

# **RW5000**

# **Configuration Guide**

**Release 5.1.56**

**Document version 1**



---

---

# Table of Contents

- Revision history..... 4
- Chapter 1: Introduction ..... 5
  - Scope of This Document ..... 5
  - Notifications..... 5
  - RADWIN 5000 Overview..... 6
    - Point-to-Multipoint Sector..... 6
    - Base Station..... 6
    - Subscriber Unit ..... 6
    - Worldwide single PN products..... 7
  - Management Tools..... 8
    - Web Interface ..... 8
    - WINTouch+ ..... 8
    - RADWIN Manager – NMS Tools ..... 9
- Chapter 2: HBS Management ..... 10
  - Scope of this Chapter ..... 10
  - Login..... 10
  - WebUI Overview ..... 12
    - SU List Filter Panel..... 13
    - Main icons ..... 15
    - Configure menu ..... 17
    - System tab..... 17
    - Services tab (HBS only)..... 19
    - Services tab (SU via HBS) ..... 43
    - Tx & Antenna tab ..... 57
    - Air Interface tab ..... 64
    - Management tab..... 83
    - Hub Site Sync tab (HBS only)..... 104
    - Inventory tab..... 104
    - Nomadic tab (HBS) ..... 107
    - Nomadic tab (SU) ..... 109

Security tab .....	110
Date & Time tab.....	120
Ethernet tab .....	121
IGMP tab (HBS only).....	128
General tab (HBS only) .....	130
Networking tab (HBS only) .....	131
WiFi tab (SU via HBS) .....	134
Events Panel .....	135
Performance monitor.....	136
Spectrum scan.....	139
Utilization monitor .....	141
Carrier Switch .....	145
Register SU .....	147
Deregister SU.....	150
Maintenance tools .....	151
Operations tools.....	157
Diagnostics tool .....	159
User profile icon .....	159
Carrier Panel.....	160
SU List Panel .....	161
Information Panel.....	167
First - Time Use.....	168
Update Connection Parameters .....	168
Select band and activate the carrier.....	170
Connect and Register Subscriber Units .....	171
Chapter 3: SU Management.....	174
Scope of this Chapter .....	174
Login.....	174
WebUI Overview .....	175
Event Panel.....	176
Main icons .....	177
Configure menu .....	178
System tab.....	178
Air Interface tab .....	180

Tx & Antenna tab .....	182
Management tab.....	184
Inventory tab.....	192
Security tab .....	193
Nomadic tab.....	196
Date & Time tab.....	197
Ethernet tab .....	198
WiFi interface tab .....	201
Spectrum scan .....	202
Maintenance tools .....	204
Diagnostics tools .....	209
Operations tools .....	212
Register button .....	212
User Profile Icon .....	212
Link Dashboard .....	213
Information Panel.....	214
Appendix A: Terminology.....	216
Appendix B: About Antennas .....	221
B.1 Scope of this Appendix .....	221
B.2 Antenna Issues.....	221
B.3 Single and Dual Antennas .....	221
B.3.1 Dual Antennas at the HBS and an SU .....	221
B.3.2 Single Antennas at Both Sites .....	222
B.3.3 Single Antenna at One Site, Dual Antennas at the Other .....	222
B.4 Considerations for Changing Antenna Parameters .....	223
Appendix C: SSH CLI .....	224
User Handbook Notice .....	227



# Revision history

Table R-1: Revision History: RADWIN 5000 Configuration Guide for the Web UI

Release & Doc.Rev	Date	Description
5.1.56	July 2024	<ul style="list-style-type: none"> <li>SU ECO</li> <li>WW SU-AIR, ALPHA-PRO</li> </ul>
Release 5.1.53	March 2024	<ul style="list-style-type: none"> <li>SU management IP via DHCP</li> <li>HW accelerated VLAN tagging mode</li> <li>SU firewall</li> <li>AES256 for 5000L HBS</li> </ul>
Release 5.1.45	June 2023	<i>New world-wide single PN products: JET AIR / JET AIR DUO</i>
Release 5.1.44	Feb 2023	<ul style="list-style-type: none"> <li>Software Defined Sector (SDS) for JET DUO 5GHz</li> </ul>
Release 5.1.42	Sep 2022	<i>New product: RADWIN 5000L HBS</i> <ul style="list-style-type: none"> <li>Enable / Disable maintenance without IP (indirect)</li> <li>Self-Registered SU Mode</li> <li>SU Interconnection</li> <li>Forgot VLAN / IP address recovery (SU-Air/Pro)</li> <li>Set Management IP &amp; VLAN in the same tab</li> </ul>
Release 5.1.30	Feb 2022	<ul style="list-style-type: none"> <li>Enhanced RADIUS Authorization</li> <li>Preserve sector ID in SU deregister operation</li> <li>Preserve Management VLAN in factory default</li> <li>SSH CLI</li> </ul>
DQ0266620/B.02 Release 5.1.10	Jun 2021	<i>New products: NEO, NEO DUO, SU Connectorized</i> <ul style="list-style-type: none"> <li>Carrier Switching - configure criteria separately</li> </ul>
DQ0266620/B.01 Release 5.0.70	Oct 2020	<i>New product: MultiSector Connectorized</i> <ul style="list-style-type: none"> <li>IGMP snooping</li> </ul>
DQ0266620/B.00 Release 5.0.70	Sep 2020	<i>New product: MultiSector Integrated</i> <ul style="list-style-type: none"> <li>Automatic Carrier Switching for JET DUO 5GHz</li> </ul>
Release 5.0.50	Jun 2020	<ul style="list-style-type: none"> <li>RADIUS AAA functions</li> <li>802.1x authentication</li> <li>Nomadic functionality</li> <li>Utilization feature</li> <li>Quality detection feature</li> <li>Bridge table</li> <li>DHCP (Option 82)</li> </ul>
Release 4.9.80	Mar 2020	<ul style="list-style-type: none"> <li>Initial release for Web managed HBS</li> </ul>

# Chapter 1: Introduction

## Scope of This Document

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

This guide applies for Linux based products, including JET PRO, JET DUO, JET AIR, JET AIR DUO, NEO\*, NEO-DUO\*, MultiSector, 5000L, SU-Air, SU-Pro, Alpha-PRO, SU-ECO, as well as 2000 Alpha when used in SU mode.

For configuration guidelines of VxWorks based products such as legacy JET, LFF HBS 5200, SFF HBS 5050 base stations, or LFF/SFF HSU subscribers - please refer to Configuration Guide of release 4.9.95.

For a detailed description of how to physically install RADWIN 5000 radios, see the RADWIN 5000 Installation Guide.

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

\* These products are discontinued for some countries, please advise local RADWIN professional services engineer.

## Notifications

Notifications consist of Notes, Cautions, and Warnings:



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



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



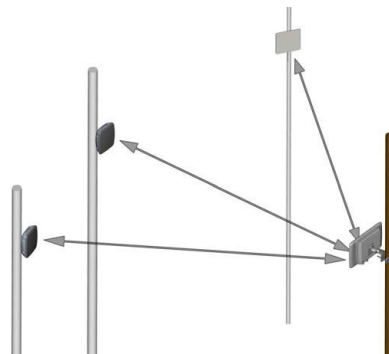
Warning: Risk of danger to persons operating near the equipment.

---

# RADWIN 5000 Overview

## Point-to-Multipoint Sector

The RADWIN 5000 point-to-multipoint system consists of “sectors”. Each sector includes a base station and multiple subscriber units. Subscriber units establish and maintain high-capacity secure wireless connection to base stations.



## Base Station

The following models of RADWIN 5000 High-Capacity Base Stations (HBS) are available at the time of release of this document:

- **5000L** - Base station with an integrated or external passive sector antenna
- **JET PRO, JET AIR, NEO\*** - Beamforming single-carrier sector base station
- **JET DUO, JET AIR DUO, NEO DUO\*** - Beamforming dual-carrier sector base station
- **MultiSector** - Base Station with multiple integrated / external sector antennas

## Subscriber Unit

The following models of RADWIN 5000 subscriber units are currently available:

- **SU PRO Embedded\*, SU AIR Embedded\***
- **SU PRO Integrated, SU AIR Integrated, Alpha-PRO Integrated, SU-ECO**
- **SU PRO Connectorized, SU AIR Connectorized, Alpha-PRO Connectorized**

In addition, there are legacy discontinued SUs: Large Form Factor (LFF) and Small Form Factor (SFF). These SUs, with release 4.9.95.06, are compatible with the above base stations.



Products marked in (\*) are discontinued for some countries, please advise local RADWIN professional services engineer.

---

## Worldwide single PN products

RADWIN products released before 2023 have specific part numbers for each regulation domain. New RADWIN base station 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.

New RADWIN Subscriber Unit products such as SU-AIR, Alpha-PRO, SU-ECO receive their respective regulatory specifications from the base station. Consequently, a single global part number can be used to order each product type, which will then be activated according to specific country regulations.

## Enforcing Regulation Restrictions

Worldwide products include a built-in GPS/GNSS receiver. The radios 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. This functionality is intended to prevent the device from transmitting in a band forbidden by the local regulation.

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



# Management Tools

## Web Interface

Web Interface is the main configuration and management interface for all the products covered in this document. The Web Interface is integrated with the radio unit, and supports any modern Web browser. This document explains in detail the web UI based configuration.

## WINTouch+

The RADWIN WINTouch+ app is an innovative and user-friendly tool designed to streamline the installation and management of RADWIN on-site installations and tasks.

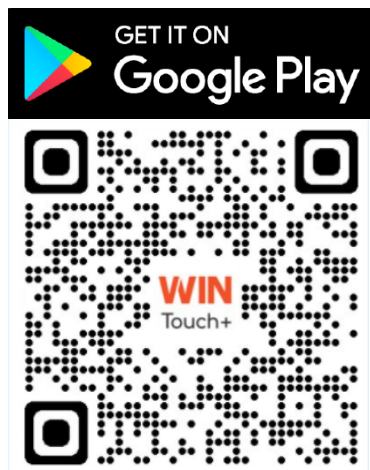
It is designed to be used with RADWIN OSS Plan & Deploy cloud-based platform in order to support a complete workflow of a typical network: site survey, network planning, installation team dispatch, deployment management, installation, documentation and maintenance.

When linked to RADWIN Web Services (RWS) account, WINTouch+ installation wizard leads you through work order processing, radio configuration, antenna alignment, and link assessment. It then generates a comprehensive report that will be uploaded to the RADWIN OSS Plan & Deploy for documentation and analysis.

Guest mode and Quick Installation mode are also available for ad-hoc SU installation when there is no need for a pre-defined work order or installation report.

Register to RADWIN OSS Tools: <https://radwin.com/oss-tools/>

Download WINTouch+:



## RADWIN Manager – NMS Tools

The RADWIN Manager is an SNMP-based management application, operating on your local computer, that was designed to manage and configure legacy units.

To support SW upgrade, backup and restore of JET AIR, JET PRO, JET DUO, JET AIR DUO, NEO\* , 5000L and MultiSector units, RADWIN Manager must be installed on the computer which is accessing the Web UI of the radio unit. SW upgrade, backup and restore operations initiated from the HBS Web UI require a Windows application **NMS Tools** supplied as of the RADWIN Manager package. See HBS Management / [Maintenance tools](#) section for details.

Latest RADWIN Manager version is available in the Support section on RADWIN Partner Portal.

---

---

# Chapter 2: HBS Management

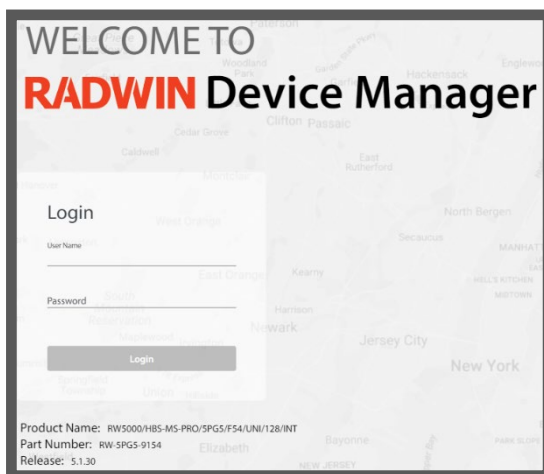
## Scope of this Chapter

This chapter covers management and operation of HBS and connected SUs via HBS Web UI.

## Login

RADWIN recommends using Google Chrome browser. Other browsers may provide basic functionality, please contact RADWIN Support for details.

Enter base station IP address in a web browser (default IP: 10.0.0.120, default protocol: HTTP). A Login screen will appear.



Enter username and password, then click **Login**.  
Default admin level credentials are:

Username:

**admin**

Password:

**netwireless**

The main window will appear.

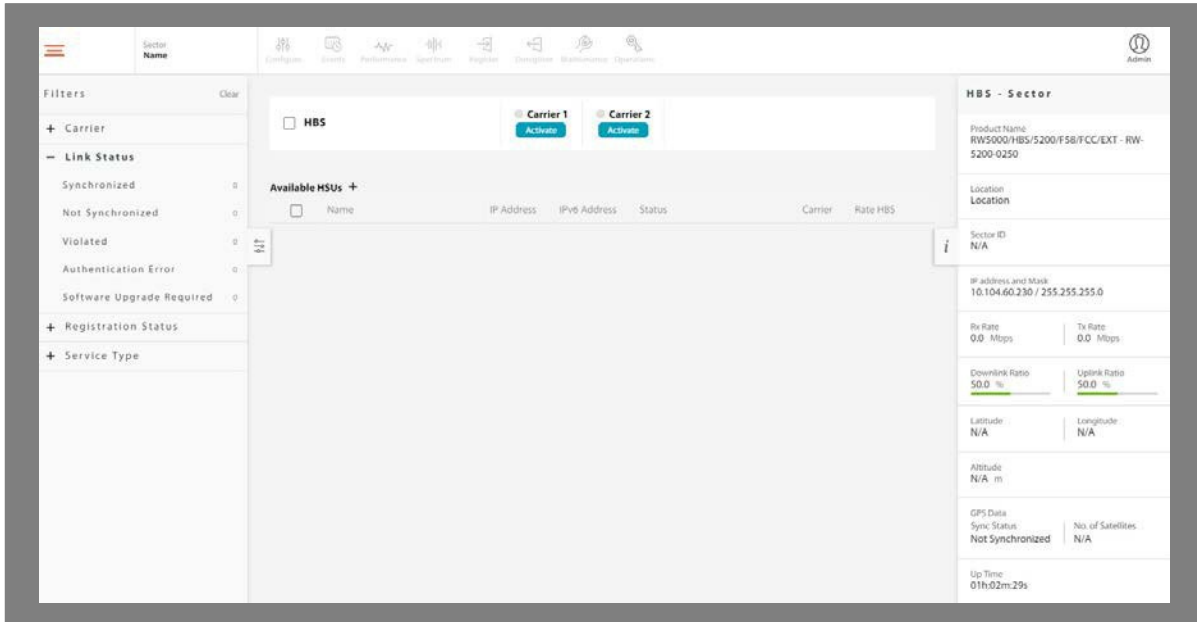


Figure 2-1: Main window for dual-carrier and multi-sector units

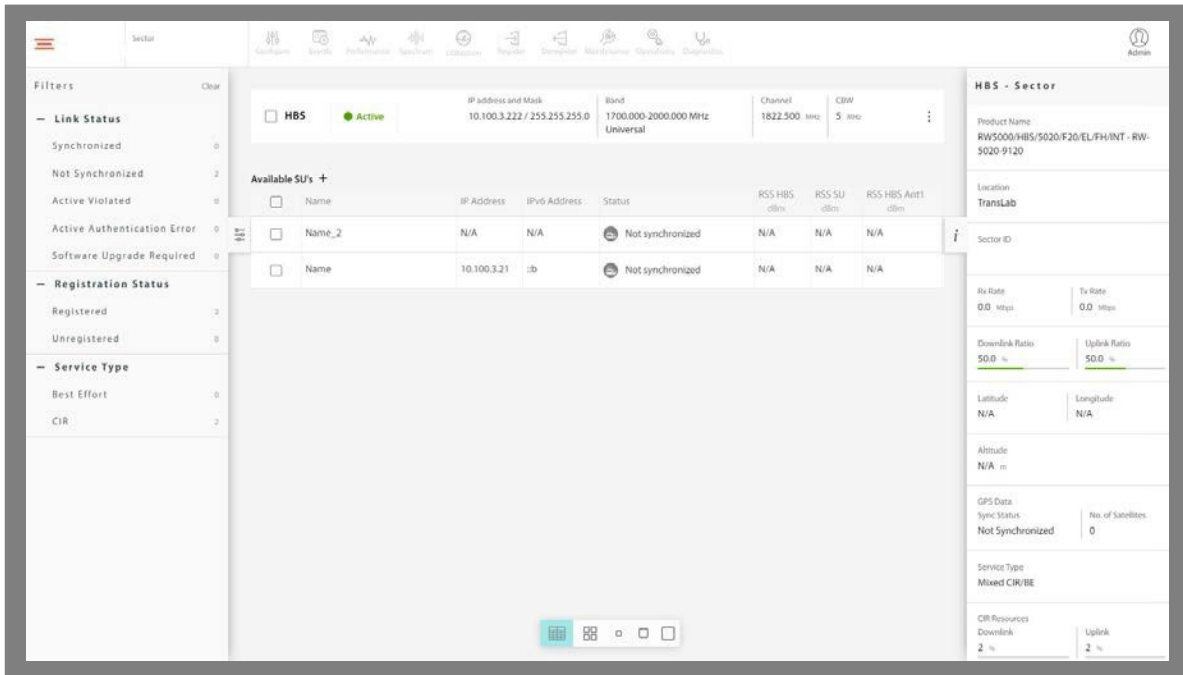


Figure 2-2: Main window for single carrier units

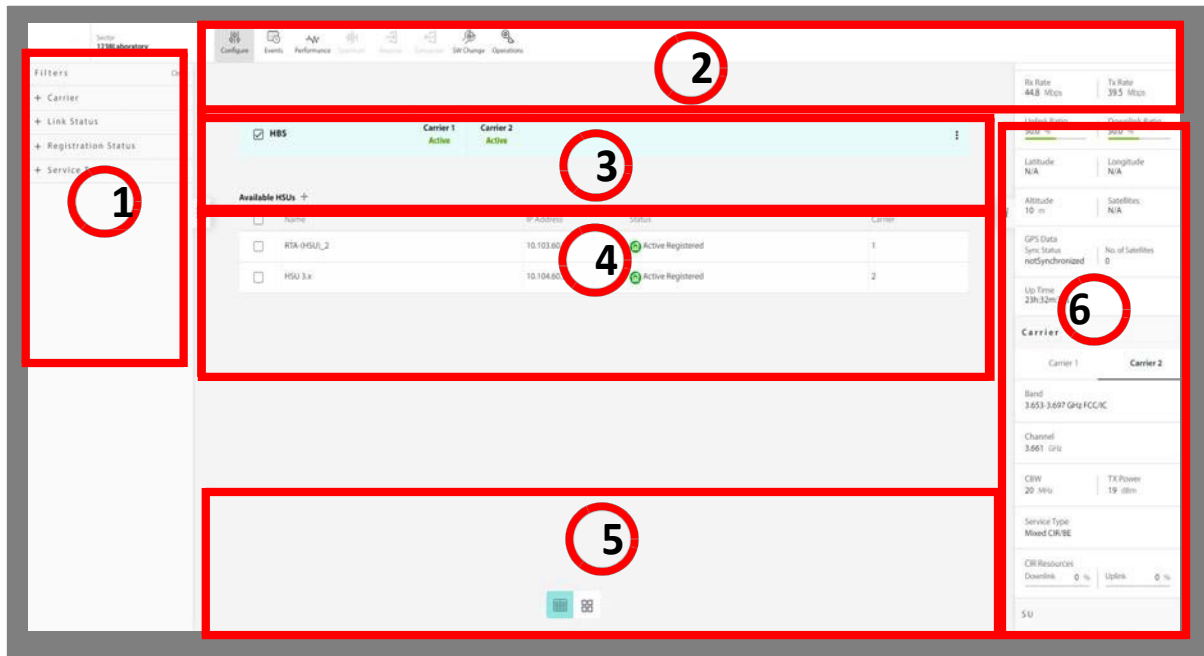
For an explanation of the Web User Interface, see [WebUI Overview](#).

For instructions on first-time use of a base station, see [First-Time Use](#).



# WebUI Overview

The WebUI shows the base station and any associated subscriber units.



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:

<b>1</b>	<i>SU List Filter Panel</i>	<b>2</b>	<i>Main icons</i>
<b>3</b>	<i>Carrier Panel</i>	<b>4</b>	<i>SU List Panel</i>
<b>5</b>	<i>SU List Views</i>	<b>6</b>	<i>Info Panel</i>

## SU List Filter Panel

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

- **Carrier:** Select Carrier 1 or Carrier 2 (in dual-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
	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.

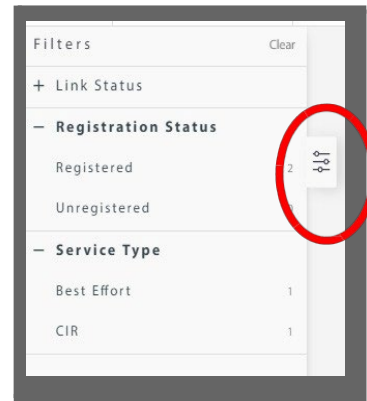
- **Registration Status:** Select Registered or Unregistered to show only devices in the indicated state.

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 hide / restore the Filters panel, click on the Filters symbol:










## Main icons






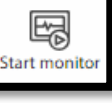
Along the top edge of the WebUI, there are icons that allow you to carry out certain tasks for the radio units.

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.



 Configure	<b>Configure</b>	View and/or modify system configuration parameters
 Events	<b>Events</b>	Shows fault conditions and events for the selected unit or units. You can also search and filter the events by severity, source, and time.
 Performance	<b>Performance</b>	The Performance Monitoring feature constantly monitors traffic and collects statistical data, whether or not the WebUI is open. Use this to see performance monitoring for the selected unit or units.
 Spectrum	<b>Spectrum</b>	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	<b>Utilization</b>	The Utilization shows how much of the available sector-wide resources of the air interface is being used.
 Carrier Switch	<b>Carrier Switch</b>	Shows Carrier Switch events, including on which unit the carrier switch was done and its cause. This icon only appears for the dual-carrier JET family products.
 Register	<b>Register</b>	Registers an SU: Enables service traffic between the SU and the HBS.



 <p>Deregister</p>	<p><b><i>Deregister</i></b></p>	<p>Deregisters an SU.</p>
 <p>Maintenance</p>	<p><b><i>Maintenance</i></b></p>	<p>Back up, upgrade or restore the software in the selected unit or units.</p>
 <p>Operations</p>	<p><b><i>Operations</i></b></p>	<p>Resets, restores to factory default configuration, and allows license-dependent upgrades on the selected unit or units.</p>
 <p>Diagnostics</p>	<p><b><i>Diagnostics</i></b></p>	<p>Creates diagnostics files, for use by RADWIN professional services and supports personnel to expedite assistance.</p>
 <p>Admin</p>	<p><b><i>User Profile Icon</i></b></p>	<p>Click this icon to log out of the HBS.</p>
 <p>Start monitor</p>	<p><b><i>Start monitor</i></b></p>	<p>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</p>

# Configure menu



Configure menu consists of tabs and sub-tabs. Most tabs are relevant for both HBSs and SUs, but some are applicable only under certain criteria, as shown in the title of each chapter, 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 is found in [Chapter 3: SU Management](#).
- SU via HBS only: Can only be carried out if you are configuring the SU via the HBS.

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

## System tab

### General

Available fields: **Description (read-only)**, **Object ID (read-only)**, **Name**, **Contact**, **Location**, and **Last Power Up (read-only)**.

Name and Location must be updated during registration. If you make any changes, click **Save** to have them take effect.

A screenshot of a web-based configuration interface. On the left, there is a sidebar with a "System" header and two sub-tabs: "General" (which is selected and highlighted in light blue) and "Coordinates". The main area displays the configuration for the "General" tab. It includes several fields: "Description" with the value "Wireless Link"; "Object ID" with the value "1.3.6.1.4.1.4458.20.5.1.1."; "Name" with the value "DUO\_PM"; "Contact" with the value "Person"; "Location" with the value "PM\_Lab"; and "Last Power Up" with the value "12/11/2018, 14:21:05". At the bottom right of the form, there are two buttons: "Cancel" and "Save".

## 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.

For 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.

The screenshot displays the 'HBS Configurations' dialog box with the 'Coordinates' section selected. The 'Coordinates' section includes fields for Latitude (-89 to +89) with a value of 32.1098 and Longitude (-180 to +180) with a value of 34.8402. There are two radio buttons for coordinate format: 'Decimal Degrees' (selected) and 'Degrees Minutes Seconds'. A 'Country' field shows 'Italy'. Below this, the 'GPS Antenna connection type' has two radio buttons: 'External' and 'Integrated' (selected). A zoomed-in view of the 'Degrees Minutes Seconds' format shows the input fields for Latitude (Degrees / Minutes / Seconds) and Longitude (Degrees / Minutes / Seconds), both set to 0 0 0.00, with directional dropdowns for 'N S' and 'E W'. 'Cancel' and 'Save' buttons are at the bottom.

## Services tab (HBS only)

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

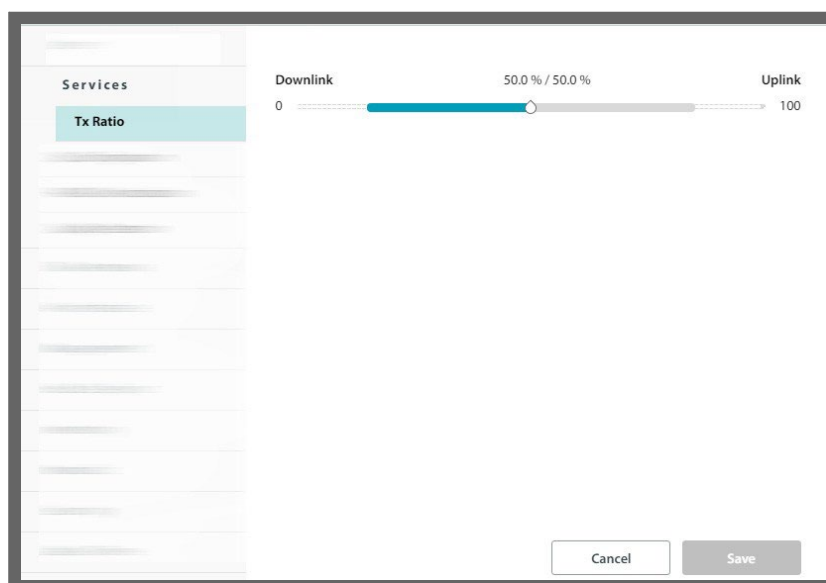
### Tx Ratio

The **Tx Ratio** (Transmission Ratio) controls the ratio of air frame resources between downlink and uplink. The adjustment range depends on channel bandwidth:

- For 20/40/80MHz channel bandwidth - 15/85% to 85/15%.
- For 10MHz – 23/77% to 77/23%
- In case of GPS Hub Site Synchronization set to Shifted phase, the Tx Ratio must be set to 50/50%

Note that changing TxRatio on the specific HBS may have a wider impact. If you use Hub Site Synchronization to collocate several HBSs (to cover adjacent sectors), they must all use the same Transmission Ratio to prevent mutual interference.

1. Move the slider to the right or left to change the Tx Ratio in 0.5% steps.
2. Click **Save** to have your changes take effect.





## 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.

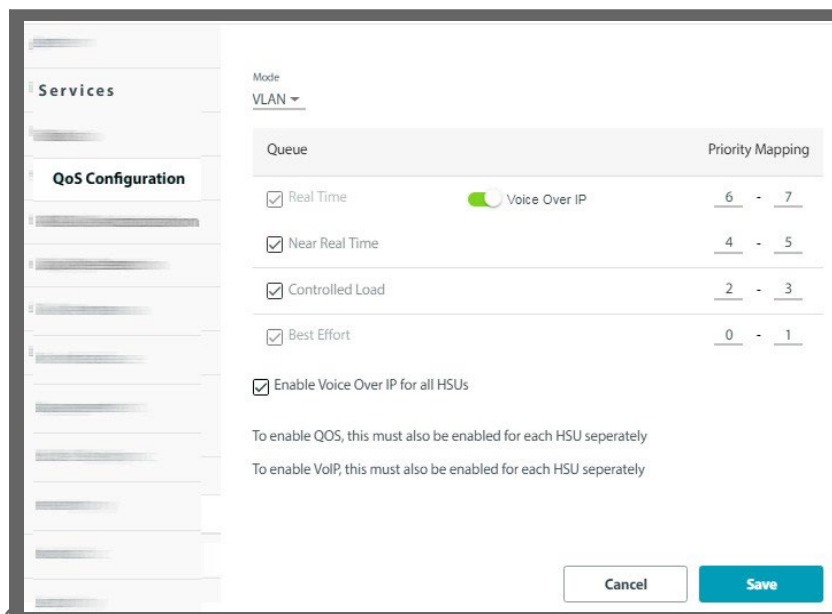
This section describes how to configure QoS for the HBS for the whole sector. However, to fully configure QoS properly, you must also configure it for each SU in turn.

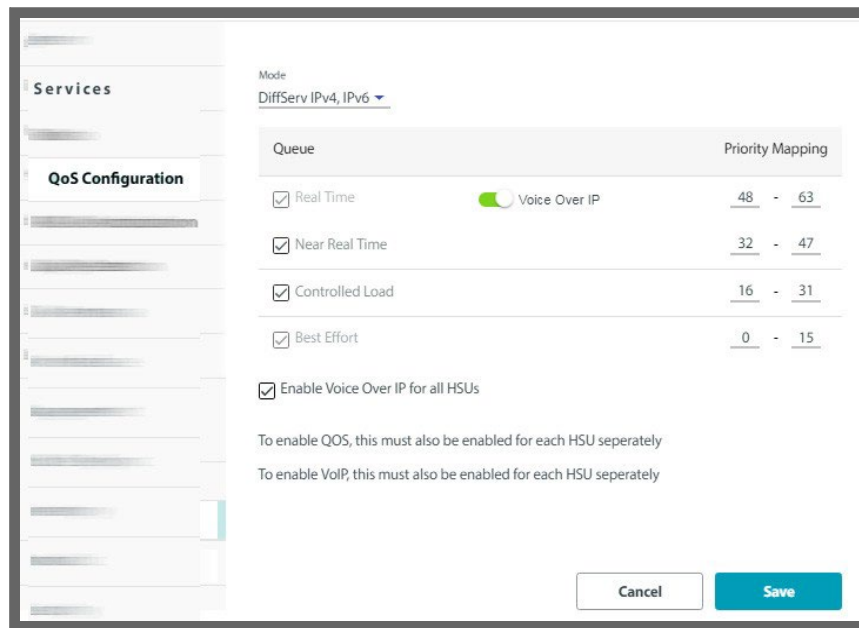
Based upon the classification criterion chosen, received packets will be mapped into one of four quality groups: real time, near real time, controlled load or best effort. You may partition the total link capacity across the four quality queues. The default weights as percentages are shown in the table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





3. When un-checking 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:

- QoS can be enabled from either the HBS or the SU. If enabled from the SU, it applies for that SU's link only.
- 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.

### **Enabling a VoIP Queue (HBS side)**

Note the following:

- VoIP queue can be enabled from either the HBS or the SU. If enabled from the SU, it applies for that SU only and its HBS. If enabled from the HBS, it applies to the whole sector. 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 the 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.



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.

---

## 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 principle

- 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 reply 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.

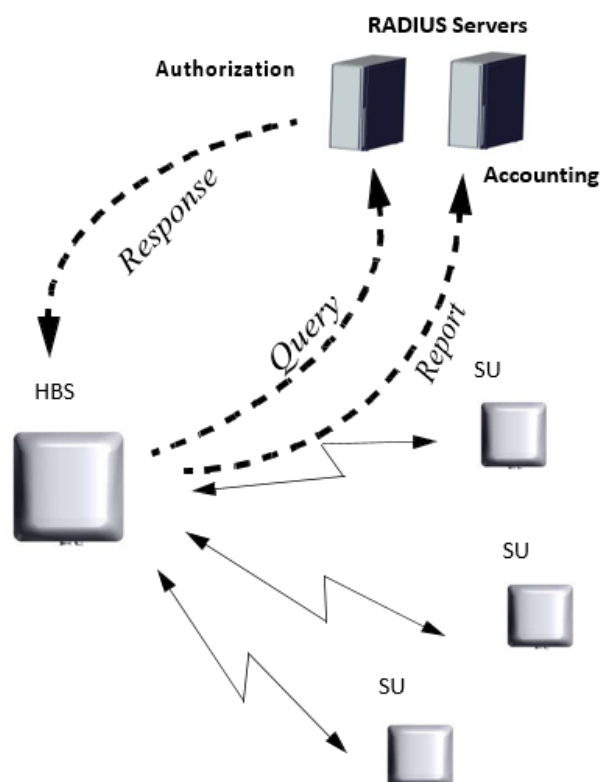


Figure 2-3: Service Validation and Authorization via a RADIUS Server

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_TVETUF_allowedVlanId_U3   Disabled      0
VALUE      RADWIN_TVETUF_allowedVlanId_U3   Enabled       1
VALUE      RADWIN_TVETUF_allowedVlanId_U4   Disabled      0
VALUE      RADWIN_TVETUF_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.



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 data 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.

Configuration Line	Parameter Value	Description
#Alpha with key ID Alpha64		
radius Cleartext-Password := "radius", RADWIN_IdentificationKeyId == "Alpha64"		SU customer ID = Alpha64
RADWIN_ServiceCategory = 5,		Service category index = 5
RADWIN_Name = "Alpha_IP_64",		Name = Alpha_IP_64
RADWIN_Location = "PSLab",		Location = PSLab
RADWIN_Vlan = 0,		VLAN TAG (prerelease 5.1.30). From release 5.1.30 should be only zero
RADWIN_ManagementIP = "20.0.0.64",		Management IP address = 20.0.0.64
RADWIN_ManagementSubnetMask = "255.255.0.0",		Management Subnet mask = 255.255.0.0
RADWIN_ManagementDefaultGateway = "20.0.0.200",		Management default gateway = 20.0.0.200
RADWIN_NTPServer = "192.168.223.37",		NTP server IP address = 192.168.223.37
RADWIN_NTPOffset = 120,		NTP offset = 120
RADWIN_SyslogServerIP = "192.168.221.90",		Syslog server IP address = 192.168.221.90
RADWIN_TrapIP_1 = "192.168.221.90",		1st Trap destination IP address = 192.168.221.90
RADWIN_TrapPort_1 = 162,		1st Trap destination port= 162
RADWIN_TrapSecurityMode_1 = 3,		1st Trap destination SNMP V mode = SNMPv3
RADWIN_TrapV3_userName_1 = "admin",		1st Trap destination SNMPv3 username = admin
RADWIN_TrapV3_userPassword_1 = "12345678",		1st Trap destination SNMPv3 password = 12345678
RADWIN_TrapIP_2 = "192.168.221.91",		2nd Trap destination IP address = 192.168.221.91
RADWIN_TrapPort_2 = 163,		2nd Trap destination port= 163
RADWIN_TrapSecurityMode_2 = 1,		2nd Trap destination SNMP V mode = SNMPv1
RADWIN_TrapIP_3 = "192.168.221.92",		3rd Trap destination IP address = 192.168.221.92
RADWIN_TrapPort_3 = 65535,		3rd Trap destination port= 65535
RADWIN_TrapSecurityMode_3 = 3,		3rd Trap destination SNMP V mode = SNMPv3
RADWIN_TrapV3_userName_3 = "Administrator",		3rdTrap destination SNMPv3 username = Administrator
RADWIN_TrapV3_userPassword_3 = "Administrator",		3rd Trap destination SNMPv3 password = Administrator
RADWIN_ContactInfo = "Yaron +97237654321",		Contact = Yar7654321on +9723
RADWIN_TrafficVlan = 1,		VLAN = Enable
RADWIN_TrafficVlanType = 1,		VLAN type = Tag
RADWIN_TVTTraffic = 1,		VLAN Ingress = Tag
RADWIN_TVTTrafficTagId = 1005,		VLAN TAG ID = 1005
RADWIN_TVTTrafficTagPriority = 3,		VLAN TAG priority = 3
RADWIN_TVTTET = 2,		VLAN Egress = Filter
RADWIN_TVTTET_allowedVlanId_1 = 100,		Allowed VLAN ID 1 = 100
RADWIN_TVTTET_allowedVlanId_2 = 200,		Allowed VLAN ID 1 = 200
RADWIN_TVTTET_allowedVlanId_3 = 300,		Allowed VLAN ID 1 = 300
RADWIN_TVTTET_allowedVlanId_4 = 400,		Allowed VLAN ID 1 = 400
RADWIN_RegisterAvailability = 1		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"
```



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)

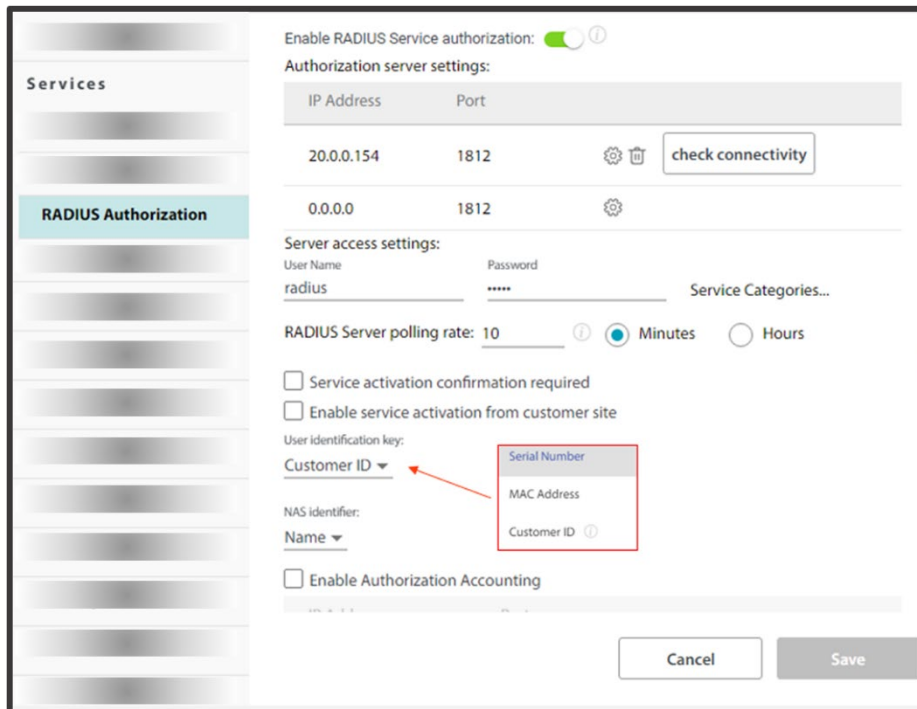
Each HBS is a radius client and should be defined as a client in the radius server. Set the IP address and secret key for each HBS in the radius client file (clients.conf).

```
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**

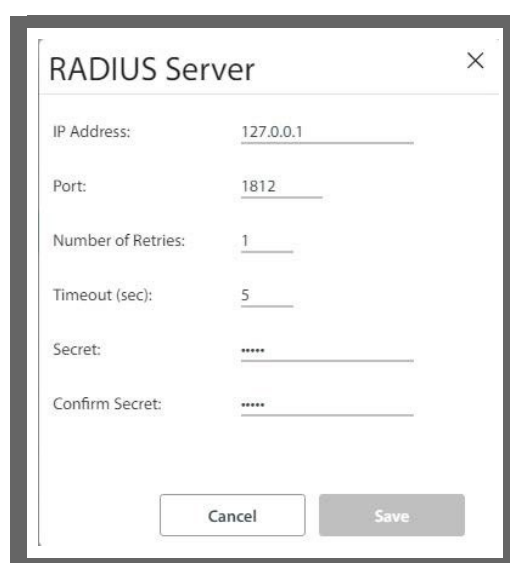
Select the HBS, click the Configure icon (  ), then from the **Services** option, select **RADIUS Authorization**.



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.



**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 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.

Category Name	Resource Type	Uplink/Downlink Resources	Maximum Information Rate Mbps	Filtering
Residential1	BE	↑ 0 ↓ 0	58 58	<input type="checkbox"/> Unlimited <input type="checkbox"/> Unlimited
Residential2	BE	↑ 0 ↓ 0	55 55	<input type="checkbox"/> Unlimited <input type="checkbox"/> Unlimited
Residential3	BE	↑ 0 ↓ 0	40 40	<input type="checkbox"/> Unlimited <input type="checkbox"/> Unlimited
Residential4	BE	↑ 0 ↓ 0	30 30	<input type="checkbox"/> Unlimited <input type="checkbox"/> Unlimited
Business1	CIR	↑ 100 ↓ 100	0 0	<input checked="" type="checkbox"/> Unlimited <input checked="" type="checkbox"/> Unlimited
Business2	CIR	↑ 90 ↓ 90	90 90	<input type="checkbox"/> Unlimited <input type="checkbox"/> Unlimited
Business3	CIR	↑ 85 ↓ 85	85 85	<input type="checkbox"/> Unlimited <input type="checkbox"/> Unlimited
Business4	CIR	↑ 80 ↓ 80	80 80	<input type="checkbox"/> Unlimited <input type="checkbox"/> Unlimited

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	<input checked="" type="checkbox"/> 0	0 <input checked="" type="checkbox"/> Unlimited
Active Voice Over IP	<input checked="" type="checkbox"/> 0	0 <input checked="" type="checkbox"/> Unlimited
Near Real Time	<input type="checkbox"/> 20	0 <input checked="" type="checkbox"/> Unlimited
Active	<input type="checkbox"/> 20	0 <input checked="" type="checkbox"/> Unlimited
Controlled Load	<input type="checkbox"/> 25	0 <input checked="" type="checkbox"/> Unlimited
Active	<input type="checkbox"/> 25	0 <input checked="" type="checkbox"/> Unlimited
Best Effort	<input type="checkbox"/> 40	0 <input checked="" type="checkbox"/> Unlimited
Active	<input type="checkbox"/> 40	0 <input checked="" type="checkbox"/> Unlimited
Total Uplink	85 %	
Total Downlink	85 %	

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

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.



Caution

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.

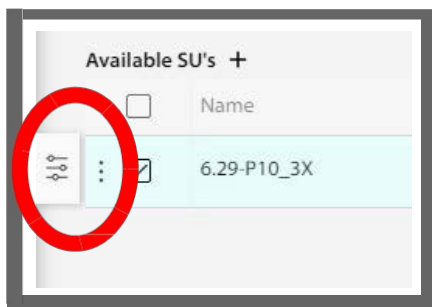
Note - When using WINTouch+ for the SU alignment, this feature must be enabled. Otherwise, the SU will immediately register to the HBS before the alignment is completed.

This option is useful if, for instance, a technician is installing an SU, and it is not quite ready to be activated.

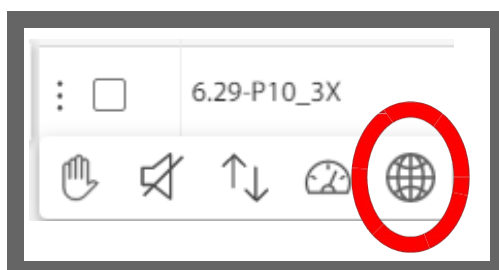
To confirm the installation from the SU side, do the following:

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.

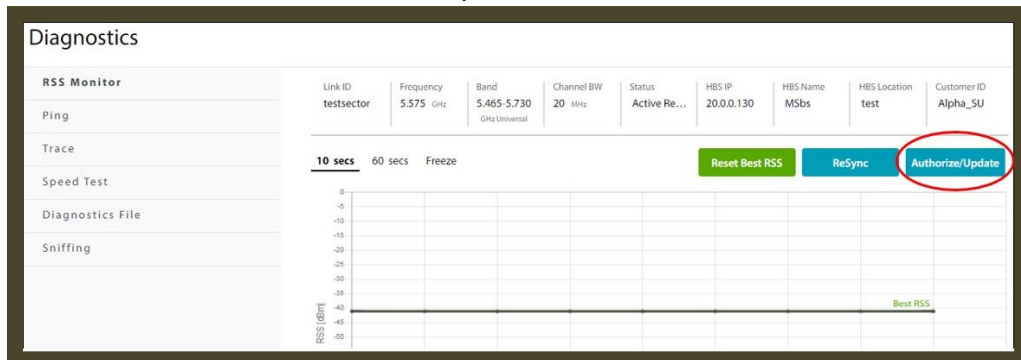


Then click on the Authorize / Update icon (looks like a globe):



**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.



**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.



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<sup>1</sup>: 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<sup>2</sup>: 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.

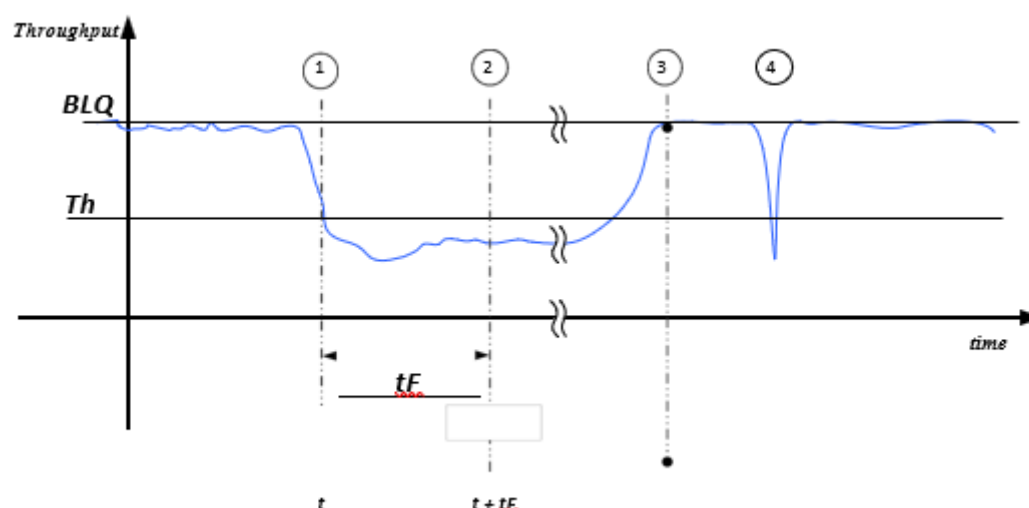


Figure 2-5: Quality Detection parameters

In [Figure 2-5, Quality Detection parameters](#), the blue line represents the real-time throughput value of the link.



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.



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.

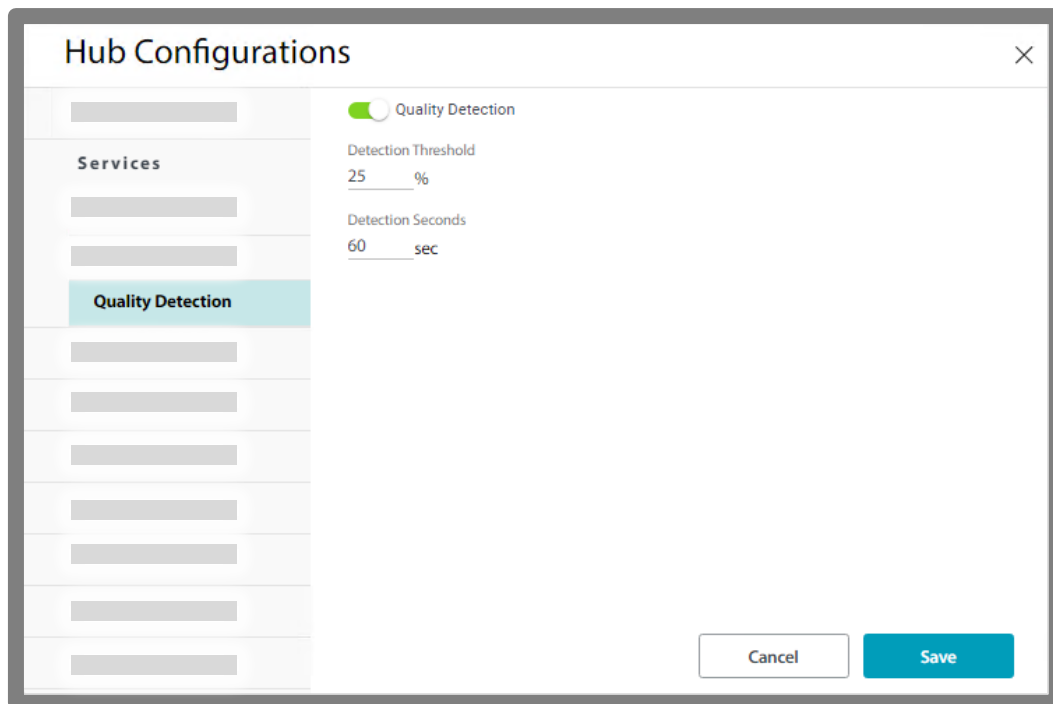
4

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

Configure Quality Detection on HBS as follows:

### **HBS side**

1. Select the HBS.
2. Click the Configuration icon (  ).
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**.





# Self-Registered SU

## Overview

In SW release 5.1.42, self-registered SU mode was introduced. This mode is very useful when the user wants to be able to register an SU from the installation site, without the need to connect to the HBS to manage the SU registration.


The user can set pre-configured settings for a self-registered SU. Any new registered SU will receive these settings. The available options include:

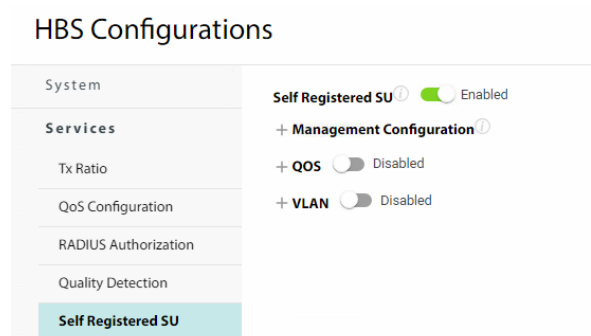
- Management IP Configuration (new in release 5.1.53)
- QOS
- VLAN

Once the self-registration is enabled in the HBS and the SU is synchronized to the BS, the installer completes the installation process and register the SU from its Web UI or WINTouch+. The SU will be configured according to self-register settings.

In case a specific SU requires a specific unique setting, after the self-registration is successful and service is established, the user can select the specific SU via the HBS Web UI and adjust the settings as required.

## Configuration

1. Select the HBS.
2. Click the Configuration icon (  ).
3. Click **Services -> Self Registered SU**.
4. Set **Self Registered SU** switch to **Enable**.
5. Click on + icons to expand sub-menus to display the available configuration sections
6. Enable and configure each relevant configuration section
7. Click **Save**.



## Management IP Configuration

Defines a management IP configuration method for a new Self Registered SU.

Note: supported only if both HBS and SU are upgraded to release 5.1.53 or higher.

– Management Configuration ⓘ

Management IP

DHCP  Static

Management VLAN

Vlan ID

100

VLAN Priority

7

### Management IP

- **Static** – default setting, SU will use static management IP. The default SU IP address is 10.0.0.120 (can be changed either from the SU or from the HBS).
- **DHCP** – SU's management IP will be set by DHCP server, the SU will send a DHCP request

### Management VLAN

- Enable the toggle switch. It will enable 802.1q VLAN tagging for SU management traffic
- Set **VLAN ID** and 802.1p **priority** to be used

Note: management VLAN will be set in any management IP mode (static / DHCP).

In the example shown here, once self-registered:

- SU management traffic will be tagged with VLAN 100, priority 7
- SU will acquire DHCP IP from a DHCP server connected to VLAN 100

## QoS

Defines service QoS configuration for a new Self Registered SU

- Toggle “Enabled” switch to provision service QoS policy on a new SU
- Adjust default QoS settings as needed - see [QoS Configuration \(SU side\)](#)

– QoS  Enabled

Queue	Strict / Weight %	Maximum Information Rate Mbps	
Real Time	↑ <input checked="" type="checkbox"/> 0	0	<input checked="" type="checkbox"/> Unlimited
Active	↓ <input checked="" type="checkbox"/> 0	0	<input checked="" type="checkbox"/> Unlimited
Voice Over IP			
Near Real Time	↑ <input type="checkbox"/> 20	0	<input checked="" type="checkbox"/> Unlimited
Active	↓ <input type="checkbox"/> 20	0	<input checked="" type="checkbox"/> Unlimited
Controlled Load	↑ <input type="checkbox"/> 25	0	<input checked="" type="checkbox"/> Unlimited
Active	↓ <input type="checkbox"/> 25	0	<input checked="" type="checkbox"/> Unlimited
Best Effort	↑ <input type="checkbox"/> 25	100	<input type="checkbox"/> Unlimited
Active	↓ <input type="checkbox"/> 40	200	<input type="checkbox"/> Unlimited
Total Uplink	70 %		
Total Downlink	85 %		

Note: HBS configuration for QoS must be enabled - see [QoS Configuration \(HBS side\)](#)

## VLAN

Defines service VLAN configuration for a new Self Registered SU

- Toggle “Enabled” switch to provision service VLAN settings on a new SU
- Adjust default VLAN settings as needed - see [VLAN Configuration](#)

The screenshot shows the VLAN configuration interface. At the top, there is a 'VLAN' section with a toggle switch set to 'Enabled'. Below this, there are two main sections: 'SU Ingress Traffic' and 'SU Egress Traffic'. The 'SU Ingress Traffic' section includes a 'Tag' dropdown menu, a 'Vlan ID' input field with the value '2', and a 'VLAN Priority' input field with the value '0'. The 'SU Egress Traffic' section includes a 'Tag' radio button selected, an 'Untag Filter...' dropdown menu, and a table for 'Allowed VLAN IDs'. The table has four columns, each with a value of '0'. Below the table, there are four checkboxes, each labeled 'Untag', with the first one checked.



Self-registered SUs will be registered as Best Effort service. If needed, after the SU is registered, service type can be modified to CIR for each SU individually, using SU service menu via HBS Web UI.



Self-registered SU mode and Radius SU Authorization mode cannot be both enabled on the same HBS.



## Services tab (SU via HBS)

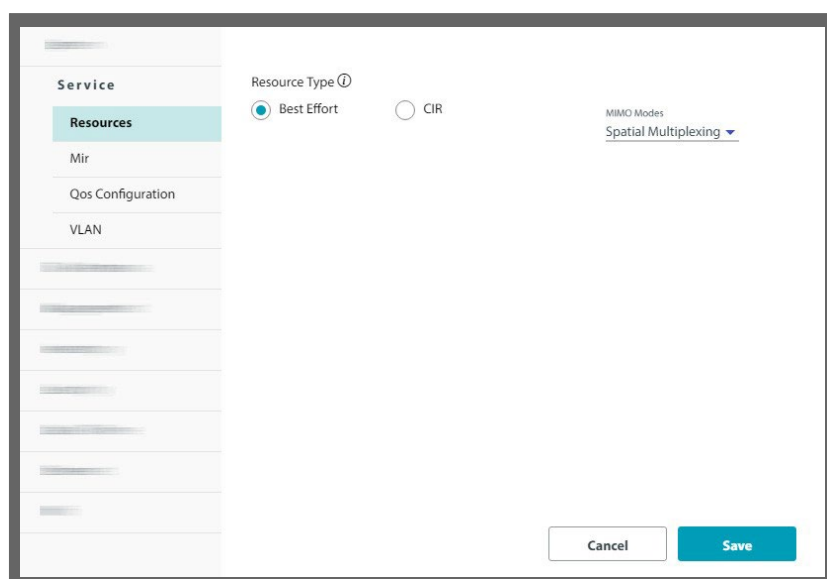
Do not confuse this with the “*Services (HBS only)*” tab.

This tab has five sub-tabs:

- Resources** - set the resource type (CIR or BE) Mir (Maximum Information Rate)
- QoS Configuration (SU side) VLAN**
- Quality Detection**

### Resources

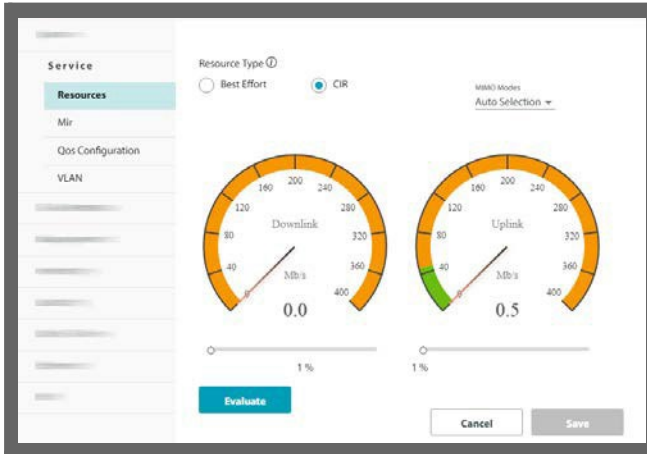
- Select the **Resource Type** for the selected SU.
  - **BE (Best Effort)** grants the SU resources as they become available in the sector.
  - **CIR (Committed Information Rate)** grants the SU with a certain guaranteed percentage of resources allocated to CIR traffic in the sector.  
Note that both the HBS and the SU must support CIR mode.
- Select a MIMO Mode for the selected SU:
  - **Spatial Multiplexing** 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.



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

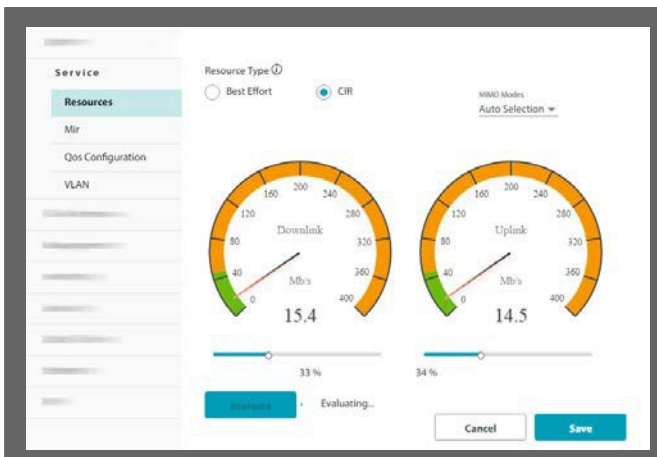


If you chose the CIR resource type, the CIR evaluate window will appear.



- Click the **Evaluate** button.

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

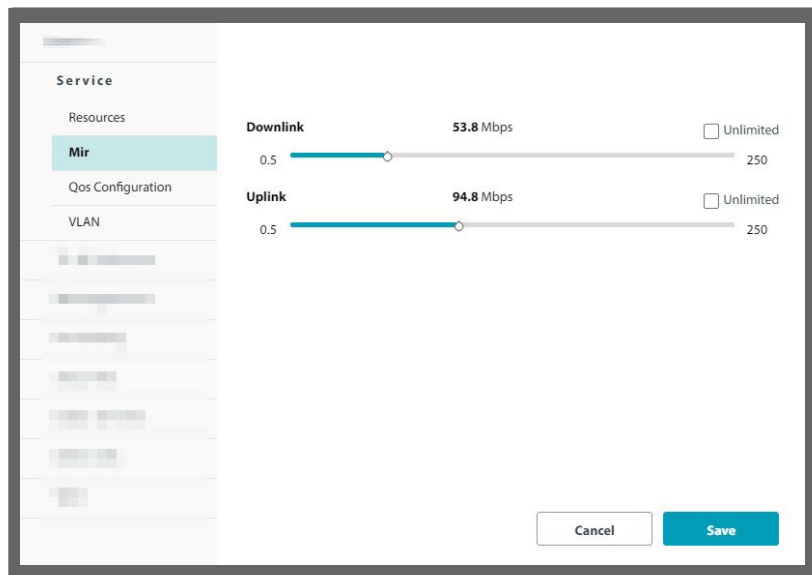


After the initial evaluation, dynamic monitoring of the sector is maintained. This allows you to add SUs in the sector, and the available resources are adjusted automatically.

- 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)

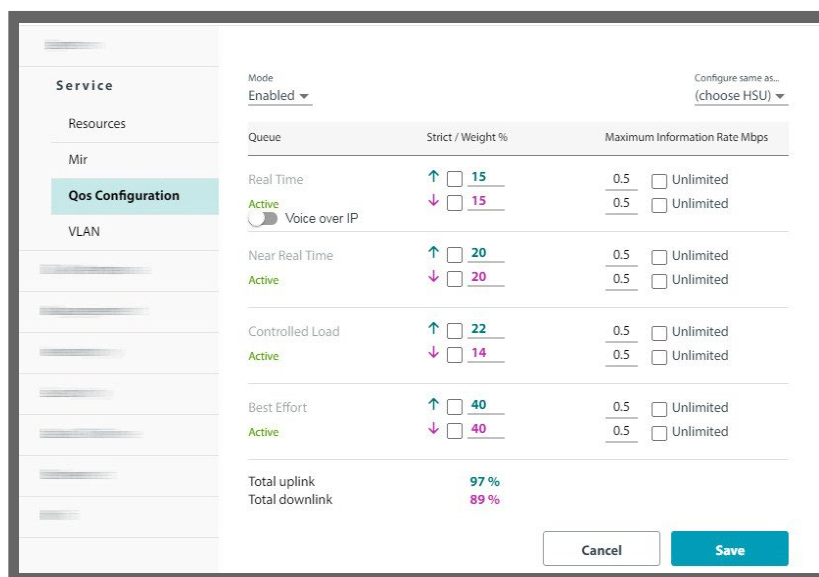
Use the sliders to set the maximum throughput rate you want for the specific SU in each direction: down link and up link. You can choose a value or click the Unlimited checkbox.



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 \(HBS side\)](#)).



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.

Resources	Queue	Strict / Weight %	Maximum Information Rate Mbps
Mir	Real Time	<input checked="" type="checkbox"/> 0	0.5 <input type="checkbox"/> Unlimited
<b>Qos Configuration</b>	<b>Active</b> Voice over IP	<input checked="" type="checkbox"/> 0	0.5 <input type="checkbox"/> Unlimited
VLAN	Near Real Time	<input type="checkbox"/> 20	0.5 <input type="checkbox"/> Unlimited
Tx & Antenna	<b>Active</b>	<input type="checkbox"/> 20	0.5 <input type="checkbox"/> 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

This section refers to VLAN tag processing for traffic. To configure the management VLAN, See [Network](#).

VLAN tag processing is configured per SU.

VLAN tag processing is disabled by default, allowing ethernet frames to pass transparently.

### **VLAN Background Information**

The standards defining VLAN Tagging are IEEE\_802.1Q and extensions.

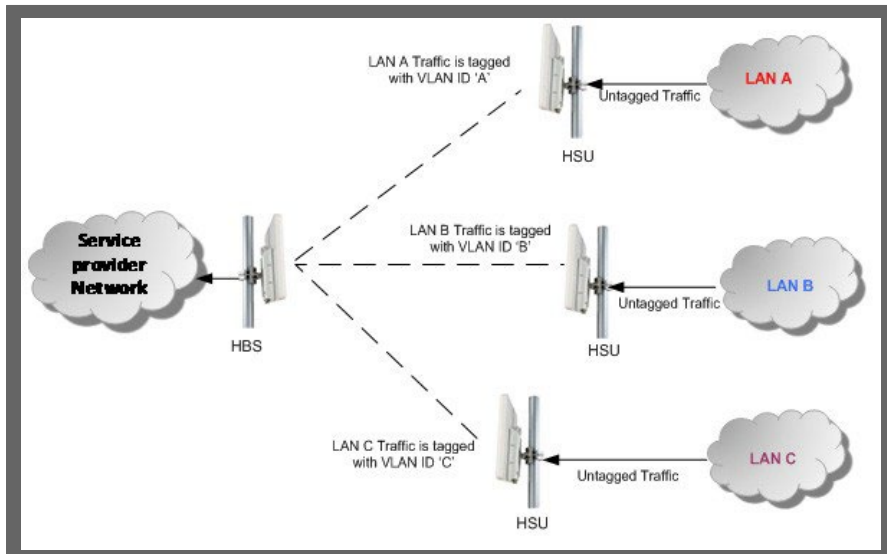
For general background information about VLAN see

[http://en.wikipedia.org/wiki/Virtual\\_LAN](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>



## 802.1q VLAN Tagging

VLAN tagging enables multiple logical networks to share a physical bridge or link.



- **Tag mode** allows for software-based 802.1q processing with separate settings for ingress and egress directions. The following table shows the possible settings:

<b>Ingress mode</b>	<b>Transparent</b>	Frames are not modified and are forwarded transparently.
	<b>Tag</b>	Tags untagged frames with specified VLAN ID and Priority

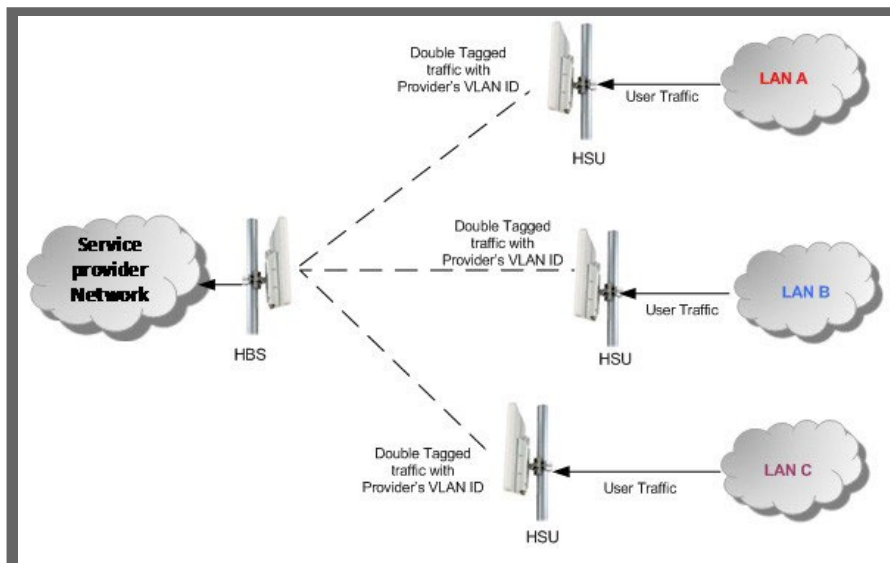
<b>Egress mode</b>	<b>Transparent</b>	Frames are not modified and are forwarded transparently.
	<b>Untag All</b>	All frames with a VLAN tag are untagged.
	<b>Filter</b>	Allow up to 4 VLAN IDs to be passed through.
	<b>Untag Filtered</b>	Allow up to 4 VLAN IDs to be passed through with optional untag of the VLAN tag from the selected VLAN ID.

- **Hardware Tag/Untag mode** (New in release 5.1.53) supports hardware accelerated 802.1q processing which provides basic tag/untag functionality while maximizing SU performance. In this case there are only two possible modes:

<b>Ingress/Egress filter = On</b>	On Ingress	Tag untagged frames with specified VLAN ID and Priority Drop any tagged frames
	On Egress	Untag frames with specified VLAN ID Drop other tagged frames
<b>Ingress/Egress filter = Off</b>	On Ingress	Tag untagged frames with specified VLAN ID and Priority Allow any tagged frames
	On Egress	Untag frames with specified VLAN ID Allow other tagged frames

## Provider Mode QinQ

QinQ is useful for service providers, allowing them to use VLANs internally in their “transport network” while adding an outer tag to VLAN-tagged frames.



When using Provider mode:

On Ingress	Add outer tag with specified VLAN ID, Priority and EtherType to any frame
On Egress	Remove outer tag with specified EtherType Drop other tagged frames

- The system always adds tags with specified VLAN ID and EtherType for each frame.
  - For a frame without a tag – the system will add a tag with specified VLAN ID and EtherType so the frame will have one tag.
  - For a frame with a VLAN tag – the system will add a tag with specified VLAN ID and EtherType 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 specified VLAN ID and EtherType so the frame will be triple-tagged and so on.

At the egress side, the SU removes the outer tag with specified EtherType no matter what the value of its VLAN ID is.

## 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.

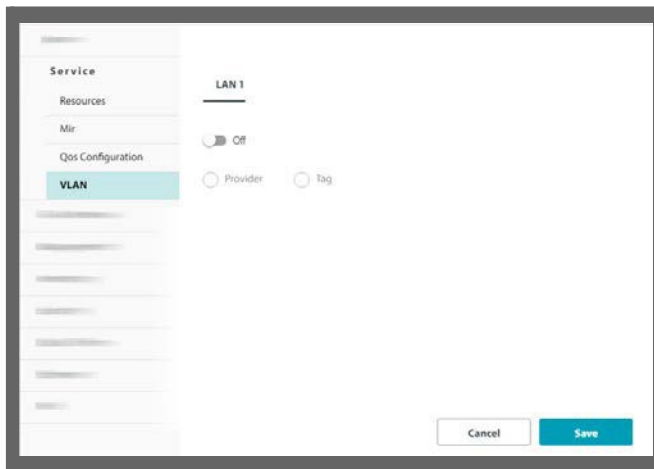


Note

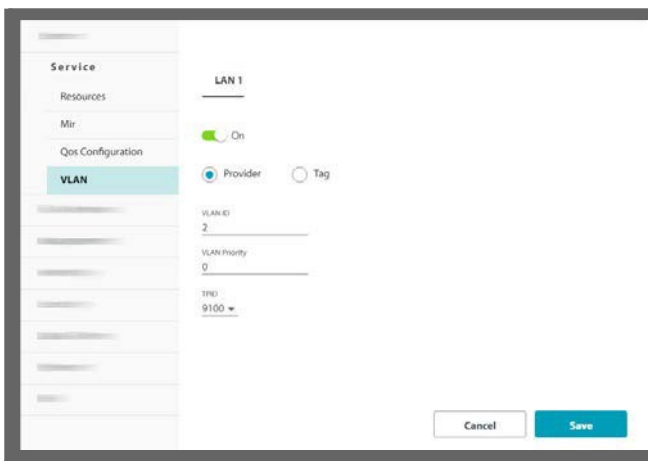
If traffic VLAN tagging is in force for the SU ingress direction and management VLAN is in use at the HBS (See [VLAN](#)), then the VLAN ID at the SU ingress direction must be the same as the VLAN ID for management at the HBS.

## VLAN Configuration

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



2. Toggle the selector switch from **Off** to **On** to enable VLAN settings.



3. Select VLAN processing mode and configure the required settings

## Provider mode

- Select **Provider** in mode selection
  - Enter **VLAN ID** (2 to 4094)
  - Enter **VLAN Priority** (0 to 7)
  - Select **TPID** (0x8100, 0x9100 or 0x88A8)
- Click **Save** to activate the settings

SU Configurations - SU-4

System

Services

Resources

MIR

QoS Configuration

**VLAN**

Quality Detection

Tx & Antenna

Management

Inventory

Security

Date & Time

Ethernet

WiFi

**LAN1**

On

Provider  Tag  Hardware Tag/Untag

Vlan ID

2

VLAN Priority

0

TPID

9100

8100

88A8

Cancel Save

## Tag mode

- Select **Tag** in mode selection
- Select the required **SU Ingress Traffic** mode
  - **Transparent**: Any frames are forwarded
  - **Tag**: Untagged frames are tagged with specified VLAN ID and Priority
    - Enter **VLAN ID** (2 to 4094)
    - Enter **VLAN Priority** (0 to 7)
- Select the required **SU Egress Traffic** mode
  - **Transparent**: Any frames are forwarded
  - **Untag All**: Any tagged frames are untagged
  - **Filter**: Allow up to 4x VLAN IDs to be forwarded
    - Enter up to 4x **Allowed VLAN IDs**
  - **Untag Filtered**: Allow up to 4x VLAN IDs and untag a selected VLAN ID.
    - Enter up to 4x **Allowed VLAN IDs**
    - Select **Untag** for a VLAN ID to be untagged.
- Click **Save** to activate the settings

The screenshot shows the 'SU Configurations - SU-4' window. On the left is a navigation menu with 'VLAN' selected. The main area is titled 'LAN1' and has a toggle switch set to 'On'. Below this are three radio buttons: 'Provider' (unselected), 'Tag' (selected), and 'Hardware Tag/Untag' (unselected). Under 'SU Ingress Traffic', there is a 'Tag' dropdown menu, a 'Vlan ID' field with '100' entered, and a 'VLAN Priority' field with '0' entered. Under 'SU Egress Traffic', there is an 'Untag Filte...' dropdown menu, a section for 'Allowed VLAN IDs' with four input fields containing '100', '101', '102', and '200', and four checkboxes labeled 'Untag' below them. The first 'Untag' checkbox is checked. At the bottom right are 'Cancel' and 'Save' buttons.



## Hardware tag/untag mode

- Select **Hardware tag/untag** in mode selection
  - Enter **VLAN ID** (2 to 4094)
  - Enter **VLAN Priority** (0 to 7)
- Select **Ingress/Egress filter** mode:

<b>Ingress/Egress filter = On</b>	On Ingress	Tag untagged frames with specified VLAN ID and Priority Drop any tagged frames
	On Egress	Untag frames with specified VLAN ID Drop other tagged frames
<b>Ingress/Egress filter = Off</b>	On Ingress	Tag untagged frames with specified VLAN ID and Priority Allow any tagged frames
	On Egress	Untag frames with specified VLAN ID Allow other tagged frames

- Click **Save** to activate the settings

### SU Configurations - SU-4 ×

System

**Services**

Resources

MIR

QoS Configuration

VLAN

Quality Detection

Tx & Antenna

Management

Inventory

Security

Date & Time

Ethernet

WiFi

**LAN1**

On

Provider  Tag  Hardware Tag/Untag

Vlan ID  
100

VLAN Priority  
3

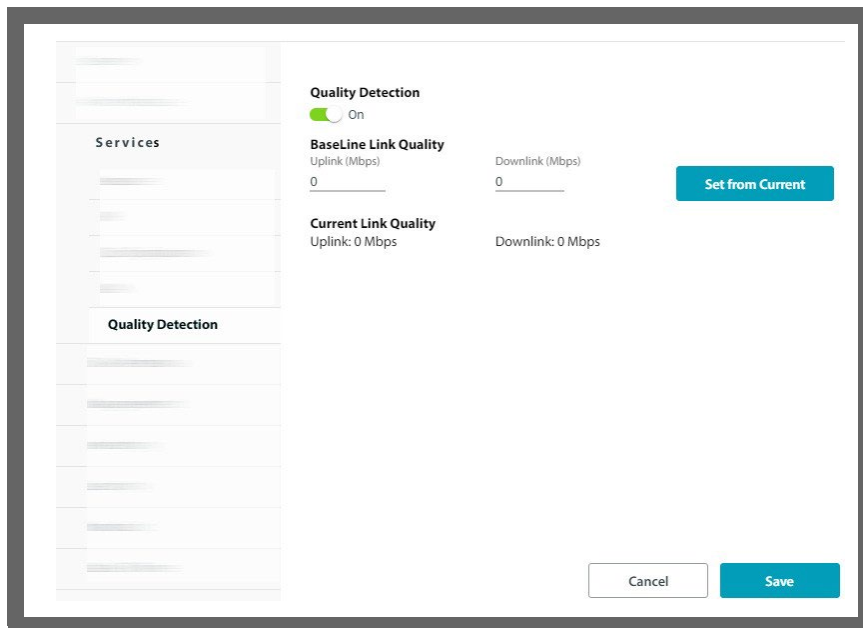
Ingress/Egress Filter

## Quality Detection (SU via HBS only)

Quality Detection must be enabled and configured both on HBS and on each monitored SU. Please refer to [Quality Detection - HBS side configuration](#).

### SU side

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



5. Select the **Baseline Link Quality** separately for uplink and for downlink in Mbps.
6. You can set this value from the current throughput of the link (shown as Current Link Quality) by clicking **Set from Current**.
7. Click **Save**.

# Tx & Antenna tab

Contents and layout of this tab vary according to the specific radio model (see sub-chapters below). Most HBS models settings are generic while others are model-specific.

## Generic Tx & Antenna settings

**Carrier tab:** (for dual-carrier HBS only) – select the carrier to configure.

Settings are for each carrier independently. Changes may affect link quality and, in the case of antenna type, cause a re-sync for the selected carrier.

**Azimuth:** Enter the sector center azimuth (in degrees).

This value does not affect operation but it's important to update it for network documentation and network monitoring. In addition, in case of JET series base station, beam steering algorithm will use the sector Azimuth value to calculate the estimated azimuth to each SU displayed in the SU List table view.

### Antenna gain:

- For an integrated antenna – read-only value, shows the typical gain of the antenna for the current operating band and channel
- For an external antenna – antenna gain value must be set correctly by the installer

### Cable loss:

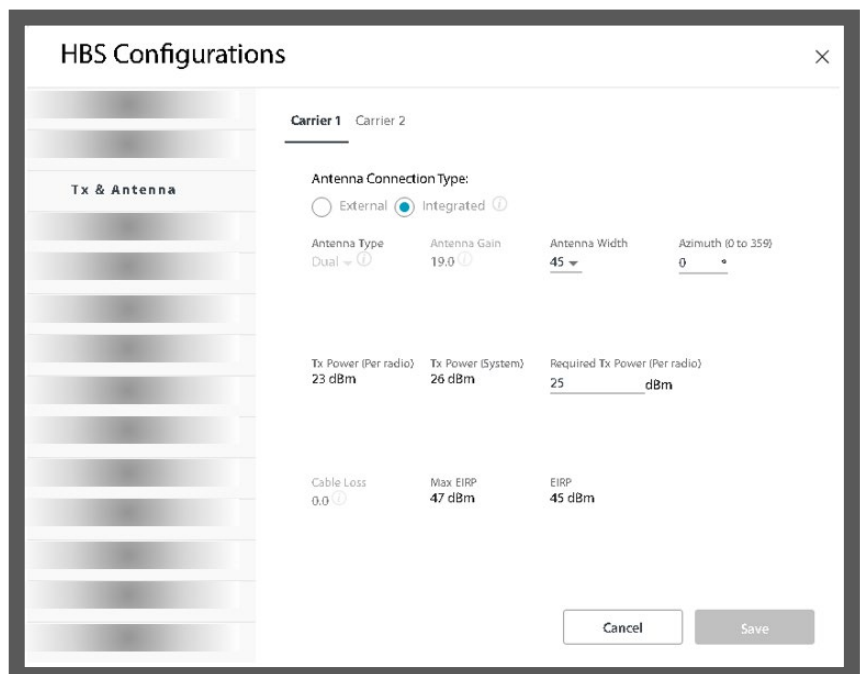
- For an integrated antenna – read-only value, fixed at 0
- For an external antenna – cable loss must be set correctly by the installer

### Required TX Power (Per radio):

by default this value is set to the maximum supported TX power, and can be adjusted within the range supported by the device.

**TX Power (Per radio):** current TX power per each radio chain, depends on:

- **Required TX Power** setting
- TX Rate / Modulation and Coding Scheme
- ATPC settings (if in use)
- **Antenna gain** and **Cable loss** (for bands which have a max EIRP limit set by regulation)



**TX Power (System)** = TX Power per radio + 3db)

**Max EIRP** = Max supported TX Power + 3db – Cable Loss + Antenna Gain

**EIRP** = TX Power (System) – Cable Loss + Antenna Gain



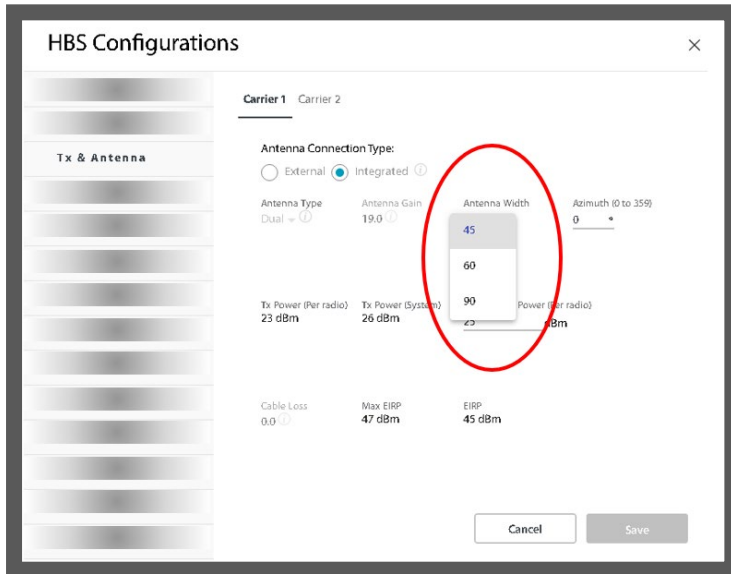
# JET DUO Software Defined Sector

Jet DUO 5GHz supports software defined sector beamwidth.

In this case, in Antenna Width field you can select the following beamwidth values:

- 90 degrees (default)
- 60 degrees
- 45 degrees

The selected beamwidth will apply to both carriers



The SDS feature allows to have up to 8 sectors at one site, with frequency reuse 2 (for each carrier) for high density deployment. This capability increases the site capacity by up to 2x without increasing the number of frequency channels required.

## SDS Examples

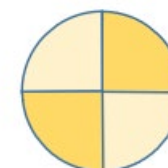
360 degree site with eight 45-degree sectors, with frequency reuse 2



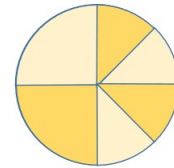
360 degree site with six 60-degree sectors, with frequency reuse 2



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



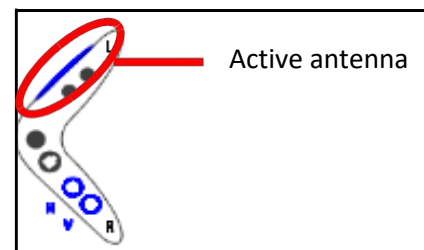
Mixed sector width with frequency reuse 2 is also an option as long as the number of sectors is even



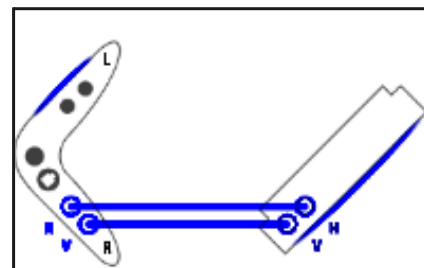
## MultiSector Integrated

- For each carrier, there are two antennas. By default, antenna name is set according to the label on external antenna connectors and can be customized.  
For Carrier 1: Ant1 (Integrated) and Ant2 (External)  
For Carrier 2: Ant3 (Integrated) and Ant4 (External)
- Antenna Type for integrated antennas is set to Master. For the external antenna, None, External, or Slave can be selected. The graphic shows the status of the antenna(s) as well as the antenna connectors location on the bottom of the unit and the recommended antenna installation orientation relative to the Multisector unit. For more details, see the RADWIN 5000 Installation Guide.

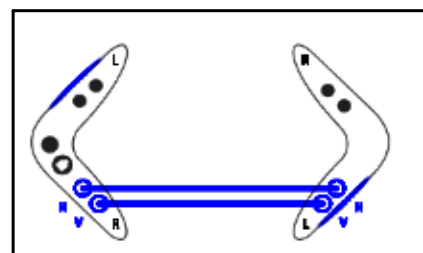
- **None:** Only integrated antenna is used. External antenna ports are disabled.



- **External:** To be used with an external sector or directional antenna. The graphic shows how the external sector antenna should be installed and connected to optimize coverage and performance.



- **Slave:** To be used with special MultiSector 180-degree antenna. Shows the MultiSector antenna installed in the opposite direction to complete 360-degree coverage.



- Port Mode can be configured for each polarization - Horizontal (H) and Vertical (V):
  - **Connected:** Select this mode when a DC-grounded antenna is connected.
  - **Termination:** Select this mode when a Termination plug is connected.
  - **Not connected:** Select this mode when nothing is connected.





---

Port Mode serves only for antenna status detection and does not affect antenna port operation.  
If the connected antenna does not have a DC ground, the port will still operate but antenna status may not be properly displayed.

---

- Beamwidth: Enter the beamwidth of the antenna being used.
- Azimuth: Enter the azimuth of the antenna being used.



Beamwidth and Azimuth values are for documentation purposes only – these values do not have any effect on operation.

	Integrated Antenna	External Antenna
Antenna Name	Ant1	Ant2
Antenna Type	Master	Slave
Port Mode	H 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:  
antenna and cables graphic is shown in **black** (when connection is detected) or in **red** (when no connection is detected)

	Integrated Antenna	External Antenna
Antenna Name	Ant3	Ant4
Antenna Type	Master	Slave
Port Mode	H 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:  
antenna and cables graphic is shown in **blue** (when connection is detected) or in **red** (when no

connection is detected)

## MultiSector Connectorized

- 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 can be configured for each polarization - Horizontal (H) and Vertical (V):
  - **Connected:** Select this mode when a DC-grounded antenna is connected.
  - **Termination:** Select this mode when a Termination plug is connected.
  - **Not connected:** Select this mode when nothing is connected.



Note

Port Mode serves only for antenna status detection and does not affect antenna port operation.

If the connected antenna does not have a DC ground, the port will still operate but antenna status may not be properly displayed.

- Beamwidth: Enter the beamwidth of the antenna being used.
- Azimuth: Enter the azimuth of the antenna being used.



Note

Beamwidth and Azimuth values are for documentation purposes only – these values do not have any effect on operation.

	Carrier 1	Carrier 2
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

## Air Interface tab

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, see [Air Interface](#).

### Radio (HBS option)

**Sector ID:** Set the Sector ID here (can be between 8 and 24 characters). The new value will be applied to all existing registered synchronized SUs.

Note: the first 4 characters of the are displayed in a separate field – this is the Network ID which should have the same value for all HBS units in the network (see [Nomadic](#) and [Secured Sync](#) features)

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

**Channel Bandwidth** and **Channel selection** may differ depending on the specific product.

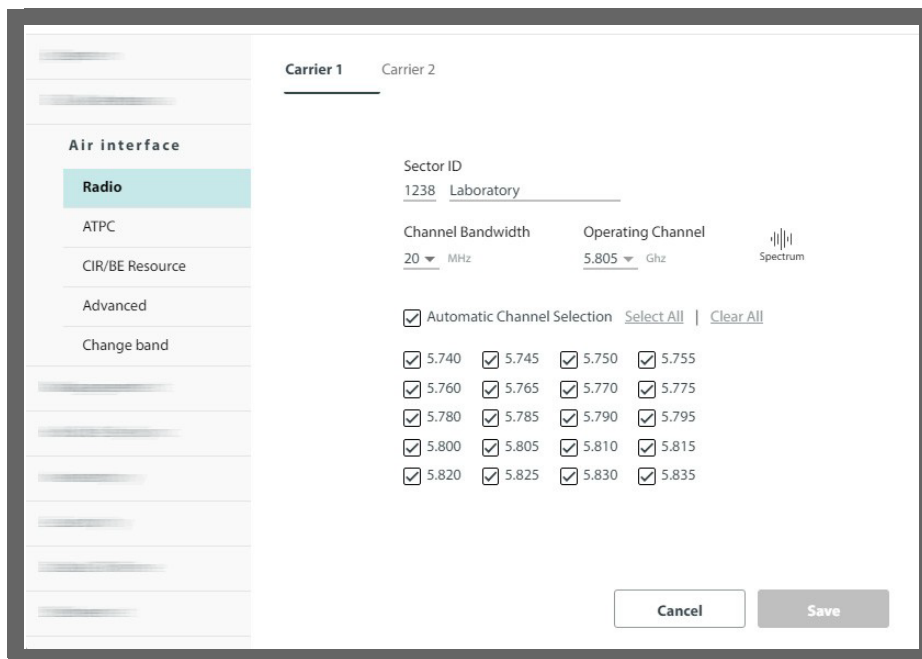


Figure 2-6: JET-DUO 3/5 GHz: Carrier 1 (5.x band)

### **JET-DUO, JET AIR DUO, NEO DUO, and MultiSector:**

- 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, Channel Bandwidth 20MHz.
- The operating channel of Carrier 1 is 5.480 GHz, Channel Bandwidth 20MHz.

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.

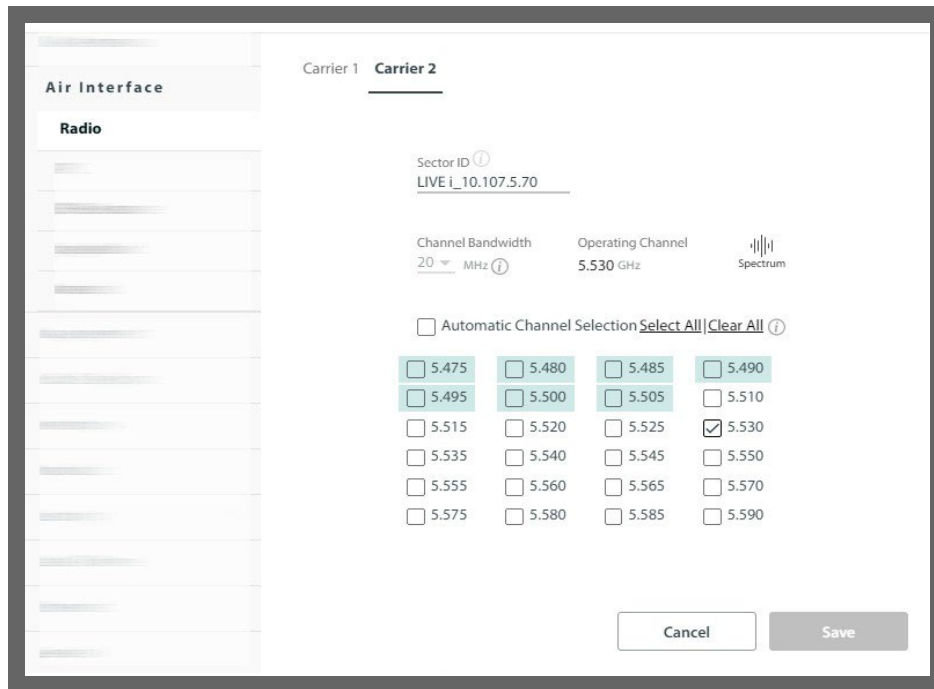
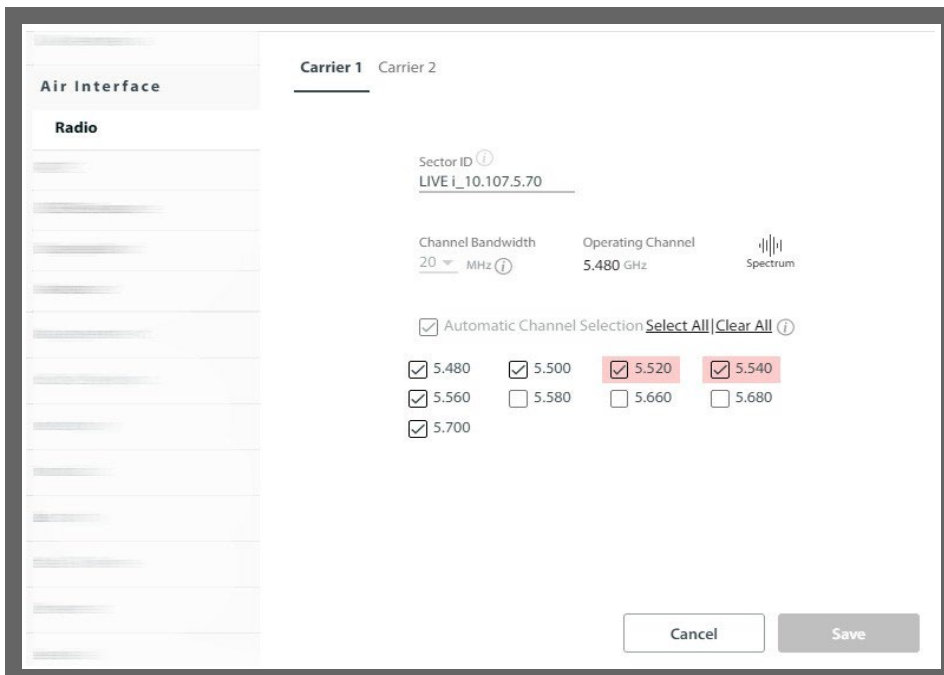


Figure 2-8: JET-DUO 5GHz and MultiSector: Carrier 2

- **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.







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

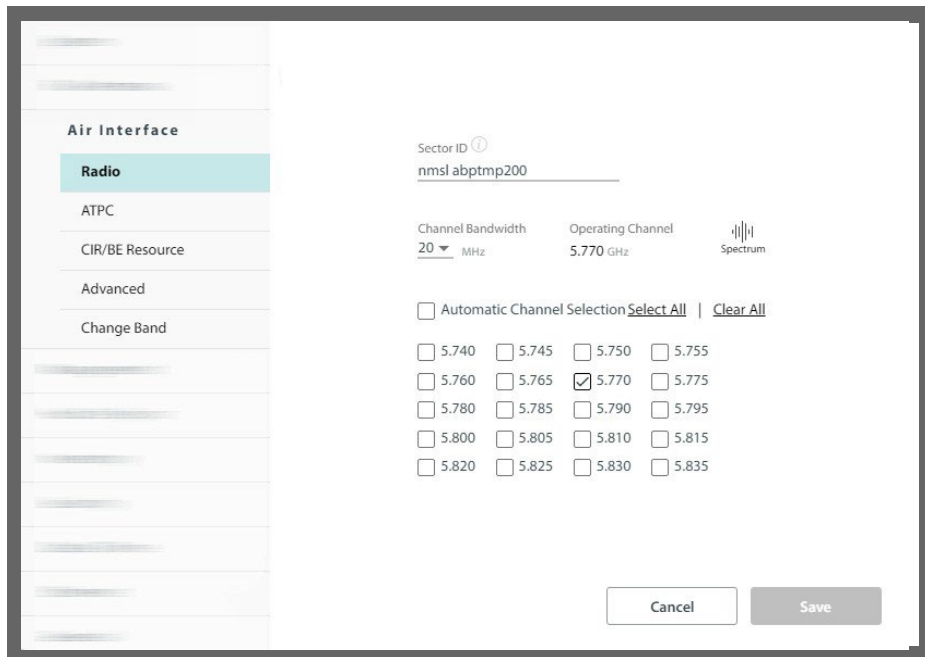
Table 2-1: Proximity Table

		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).





*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.

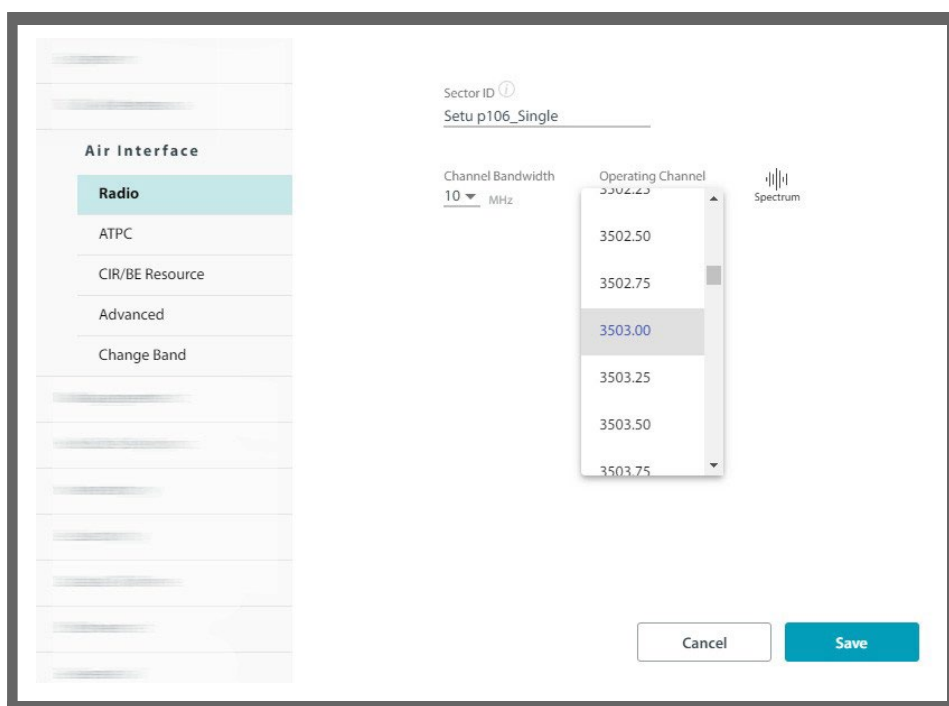


Figure 2-11: JET PRO (3.5 GHz)

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

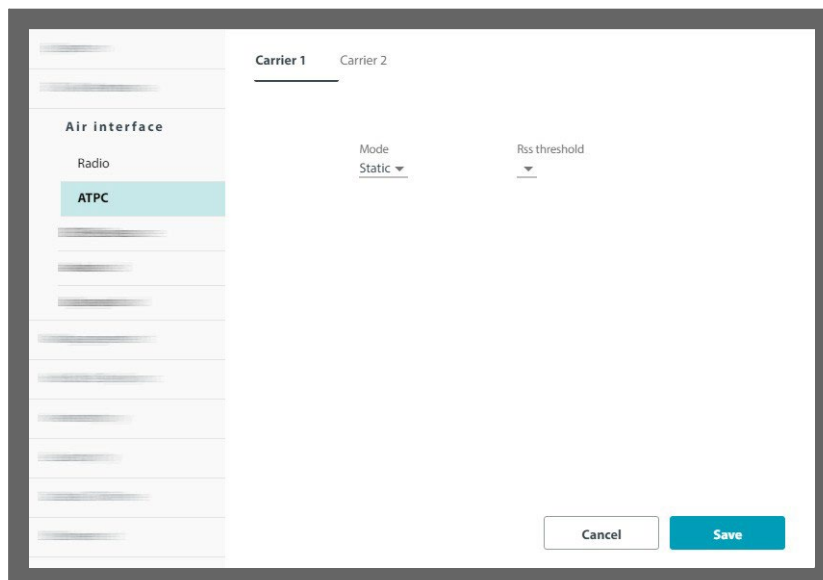
## ATPC

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.



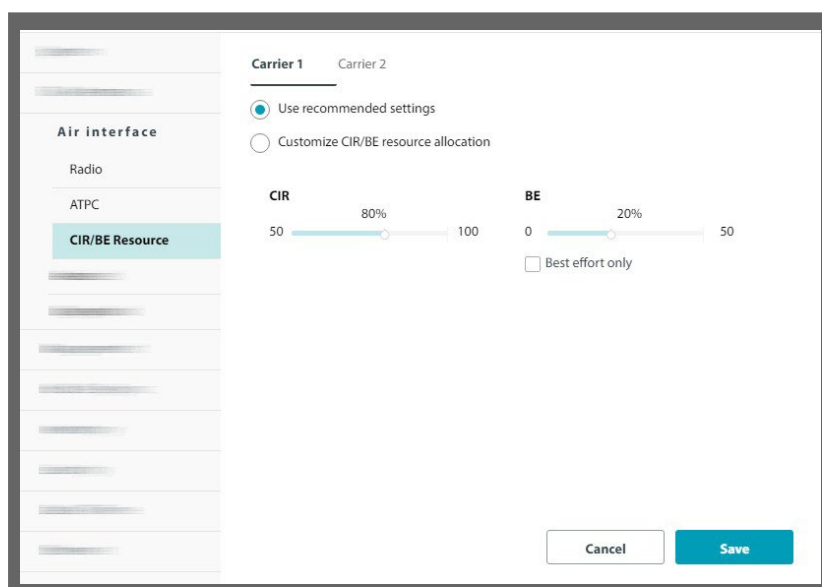
- **RSS Threshold:** The desired RSS level, which the HBS refers to in order to tune the transmission power of the SUs. The best power level depends on the radio plan, but is also influenced by your choice of Channel Bandwidth.



## 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%.



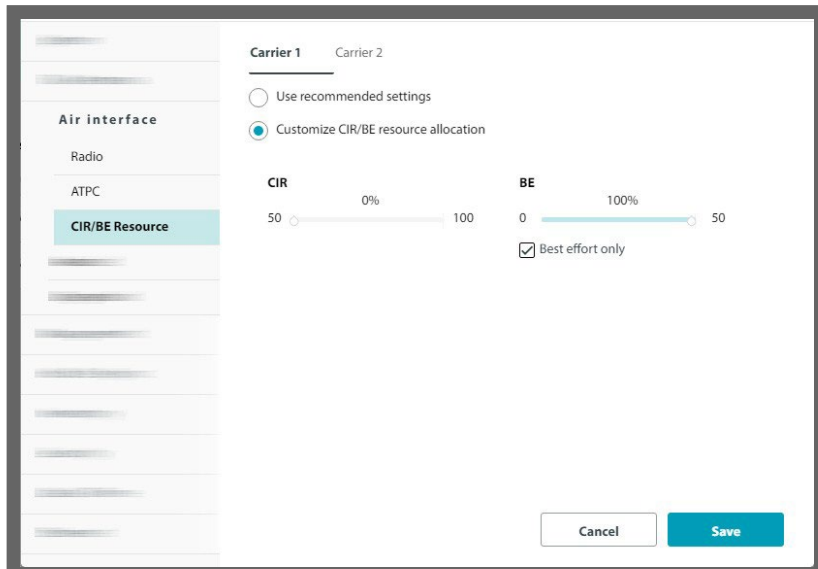
If you wish to **customize** the settings, do the following:

- If you have only BE units, check the Best Effort only box. This is like setting the CIR/Best





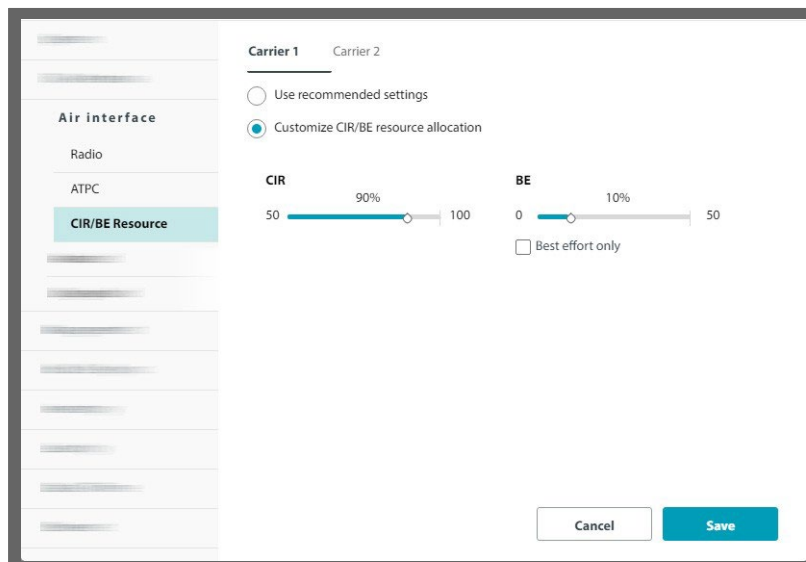
Effort Ratio to 0.0%/100.0%. If you have at least one CIR unit, this box is disabled.



- 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.



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 Uniform Single PN 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.



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



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

- 
6. Click **Yes** to continue.
  7. Click **OK**. A sector reset follows.

### HBS Configurations ×

Installation Country **Carrier 1** Carrier 2

---

Select a band from the list  
5.465-5.730 GHz Universal ▾

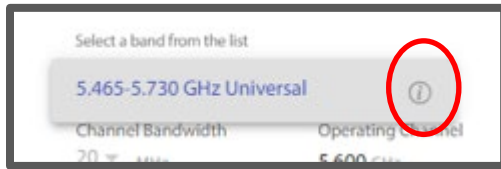
Channel Bandwidth **20** MHz      Operating Channel **5.600** GHz

Automatic Channel Selection [Select All](#) [Clear All](#) ⓘ

<input checked="" type="checkbox"/> 5.475	<input checked="" type="checkbox"/> 5.480	<input checked="" type="checkbox"/> 5.485	<input checked="" type="checkbox"/> 5.490	<input checked="" type="checkbox"/> 5.495
<input checked="" type="checkbox"/> 5.500	<input checked="" type="checkbox"/> 5.505	<input checked="" type="checkbox"/> 5.510	<input checked="" type="checkbox"/> 5.515	<input checked="" type="checkbox"/> 5.520
<input checked="" type="checkbox"/> 5.525	<input checked="" type="checkbox"/> 5.530	<input checked="" type="checkbox"/> 5.535	<input checked="" type="checkbox"/> 5.540	<input checked="" type="checkbox"/> 5.545
<input checked="" type="checkbox"/> 5.550	<input checked="" type="checkbox"/> 5.555	<input checked="" type="checkbox"/> 5.560	<input checked="" type="checkbox"/> 5.565	<input checked="" type="checkbox"/> 5.570
<input checked="" type="checkbox"/> 5.575	<input checked="" type="checkbox"/> 5.580	<input checked="" type="checkbox"/> 5.585	<input checked="" type="checkbox"/> 5.590	<input checked="" type="checkbox"/> 5.595
<input checked="" type="checkbox"/> 5.600	<input checked="" type="checkbox"/> 5.605	<input checked="" type="checkbox"/> 5.610	<input checked="" type="checkbox"/> 5.615	<input checked="" type="checkbox"/> 5.620



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 allowed power by regulation for this band.

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

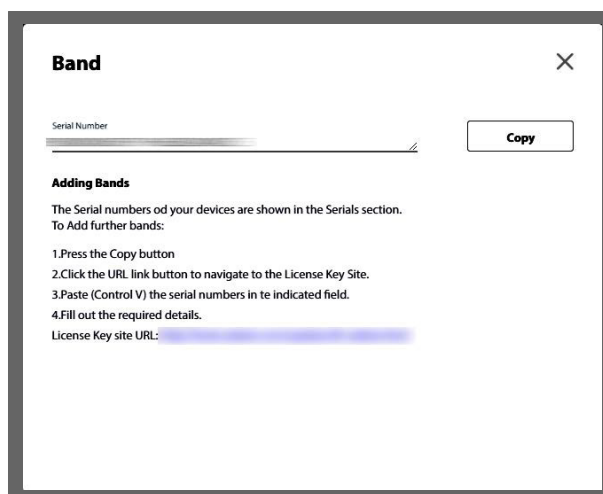
\* Power at the edge of the band might be lowered to comply to out-of-band mask requirements.

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.



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:*	<input type="text"/>	Company:*	<input type="text"/>
Address:*	<input type="text"/>	Phone:*	<input type="text"/>
End-User Email Address:*	<input type="text"/>	Confirm Email:*	<input type="text"/>
Reference:	<input type="text"/>	Enter Code (9193):*	<input type="text"/>

---

Link details

Required Band:*	<input type="text" value="2.3 GHz Universal"/>	Serial Numbers:*	<input type="text"/>
Installation Country:*	<input type="text" value="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

Close

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.



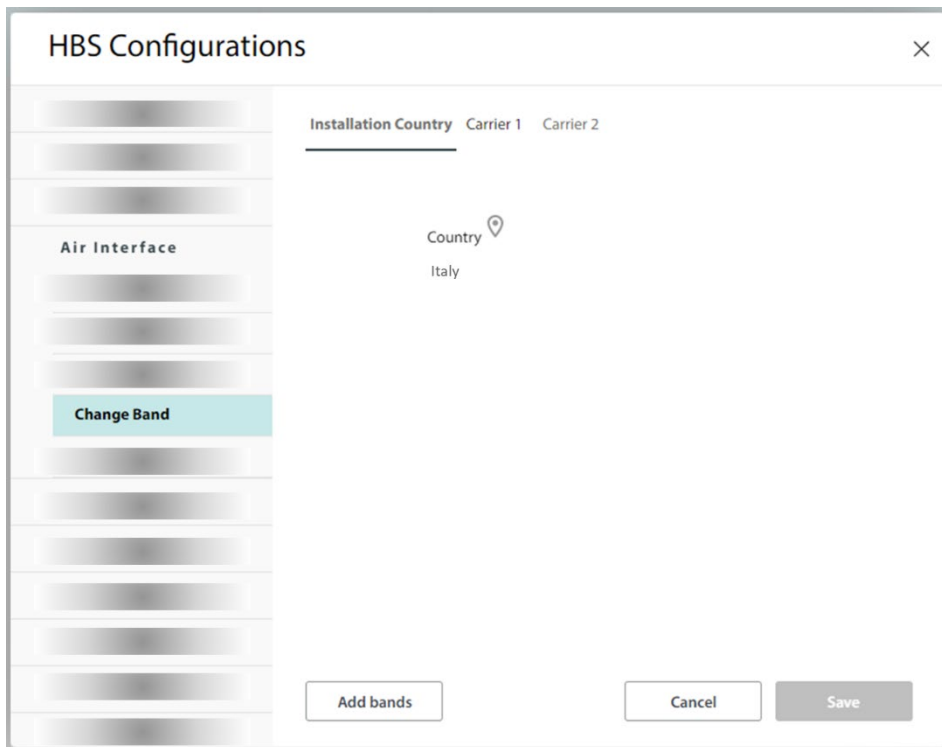
You may see error messages in the Status Column, such as Band not supported or Serial not found. Supported bands typically reflect your local regulations. Check missing serial numbers with the RADWIN Customer Service.

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.

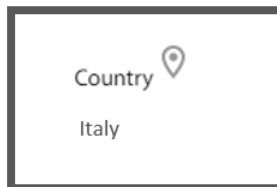
## Change country and band for Uniform Single PN Products

For single PN 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.

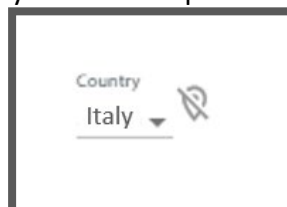
- The country setting is provided in the “**Installation country**” tab under “**Configuration -> Air interface -> change band**” screen.



- 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 country selection is disabled for the user. Example:



- 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:

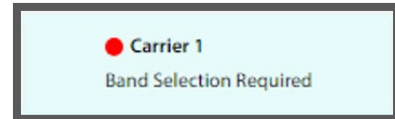


- If HBS has been activated already, the previously detected / set country will continue to be applied, and service will resume after the device boot with no need for user intervention.



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.



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 alarm "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.

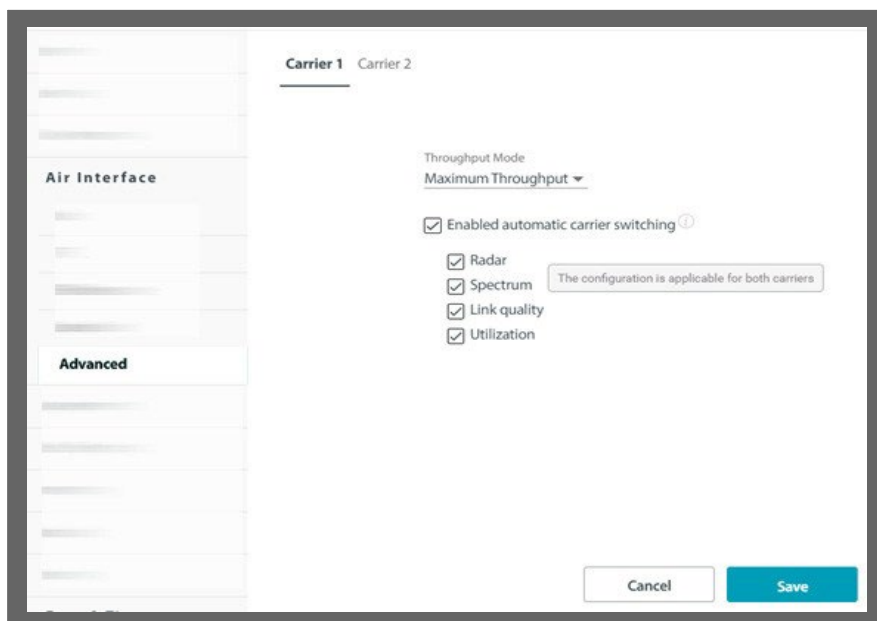
**Throughput Mode:** This determines how the Adaptive Modulation mechanism works.

- 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).



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

# Management tab

## Network (HBS)

### Configure management IP address

You may configure the unit for IPv4, IPv6, or dual-stack operation.

1. Choose IP stack operation mode (IPv4, IPv6, or IPv4+IPv6).

The screenshot shows the 'Management' tab with 'Network' selected. The configuration is for IPv4. The IP Version is set to 'IPv4'. The IPv4 section shows: IP Address: 10.103.151.23, Subnet Mask: 255.255.255.0, and Default Gateway: 10.103.151.201. The IPv6 section shows: IP Address: ::11.0.0.0, Subnet Prefix Length: 64, and Default Gateway: ::10.0.0.0. The Vlan section is set to 'On' with a VLAN ID of 2 and a VLAN Priority of 0. There are 'Cancel' and 'Save' buttons at the bottom right.

Here, we configure dual-stack mode (IPv4 + IPv6), and add the IPv6 address:

The screenshot shows the 'Management' tab with 'Network' selected. The IP Version is set to 'IPv4 + IPv6'. The IPv4 section shows: IP Address: 10.104.60.230, Subnet Mask: 255.255.255.0, and Default Gateway: 10.104.60.201. The IPv6 section shows: IP Address: 205:104:60:230, Subnet Prefix Length: 64, and Default Gateway: 205:104:60:201. There are 'Cancel' and 'Save' buttons at the bottom right. A callout box on the left shows the 'IP Version' dropdown menu with 'IPv4', 'IPv6', and 'IPv4 + IPv6' options, with 'IPv4 + IPv6' selected. A large white arrow points from the callout box to the main configuration area.

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. 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.

1. Check ON in the VLAN checkbox.
2. Enter a VLAN ID. Its value should be between 2 and 4094.
3. Enter a **Priority** value between 0 and 7.
4. 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.



## Network (SU via HBS only)

### Configure management IP address

You may configure the SU for IPv4, IPv6, or dual-stack operation.

Starting from release 5.1.53, DHCP client mode is supported (for IPv4 only).

1. Select **IP Version** (IPv4, IPv6, or IPv4+IPv6) to choose IP stack operation mode.
2. Select **Management IP** for IPv4 mode (**DHCP** or **Static**)
3. Enter IP address or addresses, including the Subnet Mask and Default Gateway (for IPv4), and/or the Subnet Prefix Length and Default Gateway (for IPv6).
4. When DHCP mode is selected:
  - a. **IPv4 Fallback** address will be used when DHCP server does not respond to DCHP Discover/Request sent by the SU.
  - b. **Current IP** will display the actual IP address (either DHCP IP or IPv4 fallback IP)
5. Click **Save**.
6. To confirm, click **OK**.

### Configure management VLAN

Note: when configured, VLAN tag will be added to any management packet sent via Ethernet or wireless interface, including DHCP transactions and IPv4 fallback address.

1. Check **On** in the VLAN checkbox.
2. Enter a **VLAN ID**. Its value should be between 2 and 4094.
3. Enter a **VLAN Priority** between 0 and 7.
4. Click **Save**.

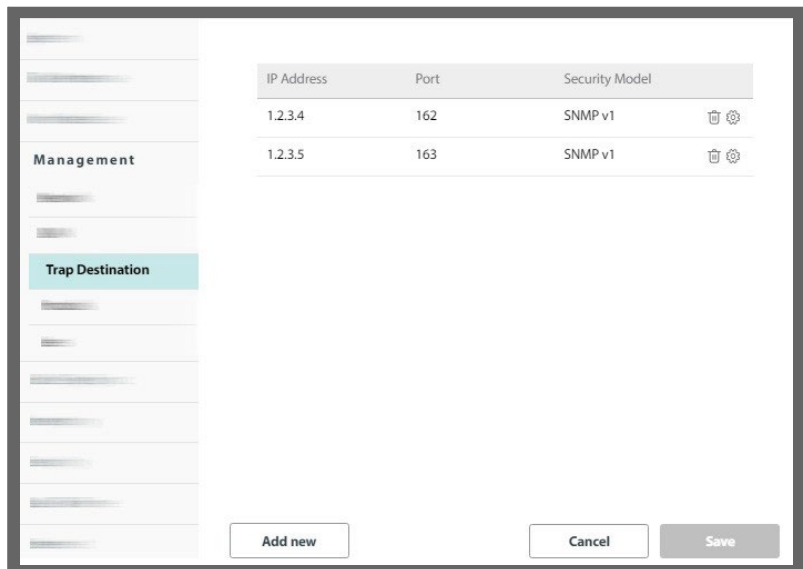
The screenshot displays the 'SU Configurations - SU-1' web interface. The left sidebar shows a navigation menu with 'Management' expanded and 'Network' selected. The main content area is divided into several sections:

- System:** IP Version is set to 'IPv4 + IPv6'.
- Management IP:** 'DHCP' is selected with a radio button, and 'Static' is unselected.
- IPv4 Fallback:** IP Address is '10.0.2.120', Subnet Mask is '255.0.0.0', and Default Gateway is '10.0.0.1'.
- IPv6:** IP Address is '::b', Subnet Prefix Length is '64', and Default Gateway is '::a'.
- Current IP:** IP Address is '10.0.100.75', Subnet Mask is '255.255.255.0', and Default Gateway is '10.0.100.254'.
- Vlan:** A checkbox is checked and labeled 'On'. Below it, 'Vlan ID [2 - 4094]' is set to '100' and 'VLAN Priority [0 - 7]' is set to '7'.

At the bottom right, there are 'Cancel' and 'Save' buttons.

## Trap Destinations

When using SNMP monitoring system such as RADWIN WINManage or a similar 3<sup>rd</sup> party system, each monitored radio unit should be configured to send SNMP traps to each server acting as SNMP trap receiver.



### 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 traps will be forwarded to the specified destinations.

**New Trap Destination**



IP Address: 1.2.3.6      Port: 162

Security Model: SNMP v1

User Name:      Password:

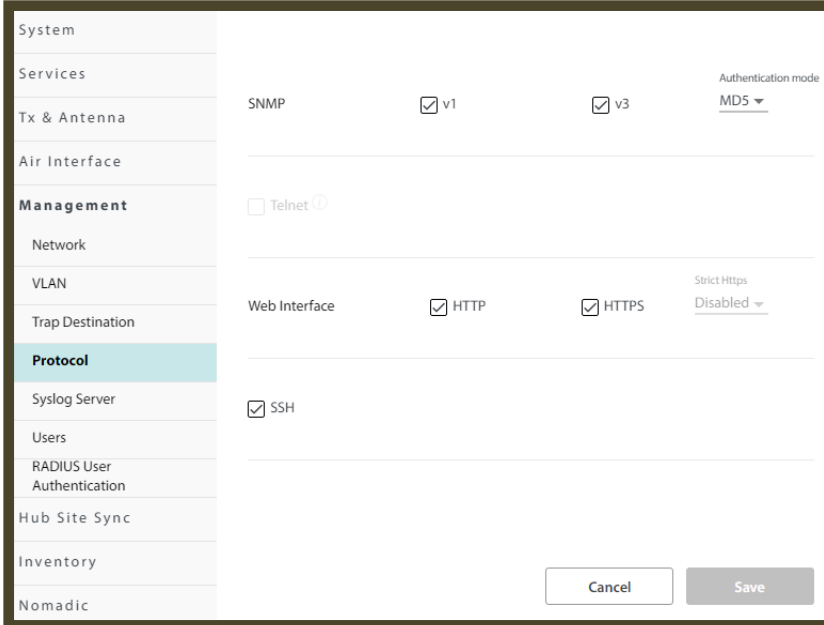
3. Once you are finished, click **Save** to have your changes take effect.

### To change (edit or delete) a trap destination:

1. To delete a trap destination, click the trash icon (  )
2. To edit a destination, click the configuration icon (  ) and update the parameters you wish to change.
3. Click **Save** to have your changes take effect.

## Protocol

You can enable/disable ODU management protocols and set specific settings.



### SNMP

- You may choose to enable SNMPv1, SNMPv3 or both.
- When configuring SNMPv3, you can leave the default authentication mode MD5 (message digest algorithm), or change it to SHA1 (secure hash algorithm).



For secure operation, as well as to be able to use some security-related features such as RADIUS User Authentication, SNMP protocol must be set to v3 only.

### Web Interface

- The unit can be configured for HTTP (port 80), HTTPS (port 443), or both.
- When HTTP is disabled, there are two options for Strict HTTPS mode:
  - Strict HTTPS Disabled: HTTP session will be redirected to HTTPS
  - Strict HTTPS Enabled (more secure): HTTP is fully disabled, user must explicitly set the browser to HTTPS to connect to the radio
- An admin user must be logged in with HTTPS to make changes in users.



For secure operation, as well as to be able to use some security-related features such as RADIUS User Authentication, HTTP must be disabled.

### **SSH**

- Command Line Interface via SSH CLI (port 22) can be enabled or disabled
- For a list of supported CLI commands, See [Appendix C](#)

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

## Syslog Server

Enter the IP address of a Syslog server to which the radio unit will send Syslog messages.

IP Address  
0.0.0.0

Clear

Cancel Save

- Enter the IP Address of the Syslog server.

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	🗑️ ⚙️

Add new Cancel Save



Possible user profiles are as follows:

Profile	Default Password	Function
<b>observer</b>	netobserver	Read Only
<b>operator</b>	netpublic	Can install and configure the sector but cannot change the frequency band/regulation.
<b>Installer</b>	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.
<b>Admin</b>	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.

The screenshot shows a 'New User' dialog box with the following fields and controls:


- User name \*
- Profile: Operator
- Change Password section:
  - New Password
  - Confirm Password
- Buttons: Cancel, Save

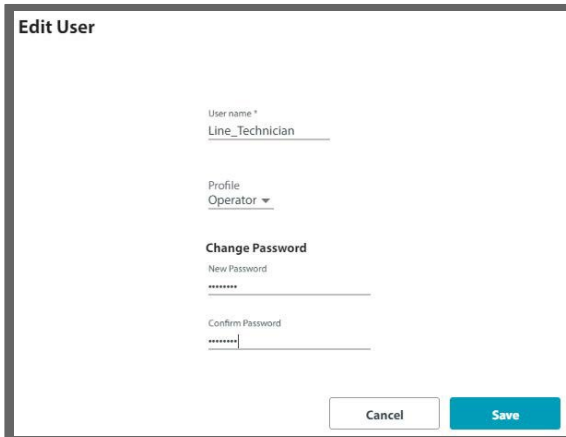
1. Enter a convenient name for the new user.
2. Choose the profile for this user. The profile determines what the user can and cannot do.
3. Set the password for this user, and confirm it.



- 
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  
\*\*\*\*\*

Cancel Save

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.

4. Click on the trash icon () to remove the user.
5. The user will be removed from the Users list.

## RADIUS User Authentication (HBS only)

---



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.

---



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<sup>1</sup>.
- » 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.

<sup>1</sup> The SNMP community may be different for the SUs, depending on your system configuration

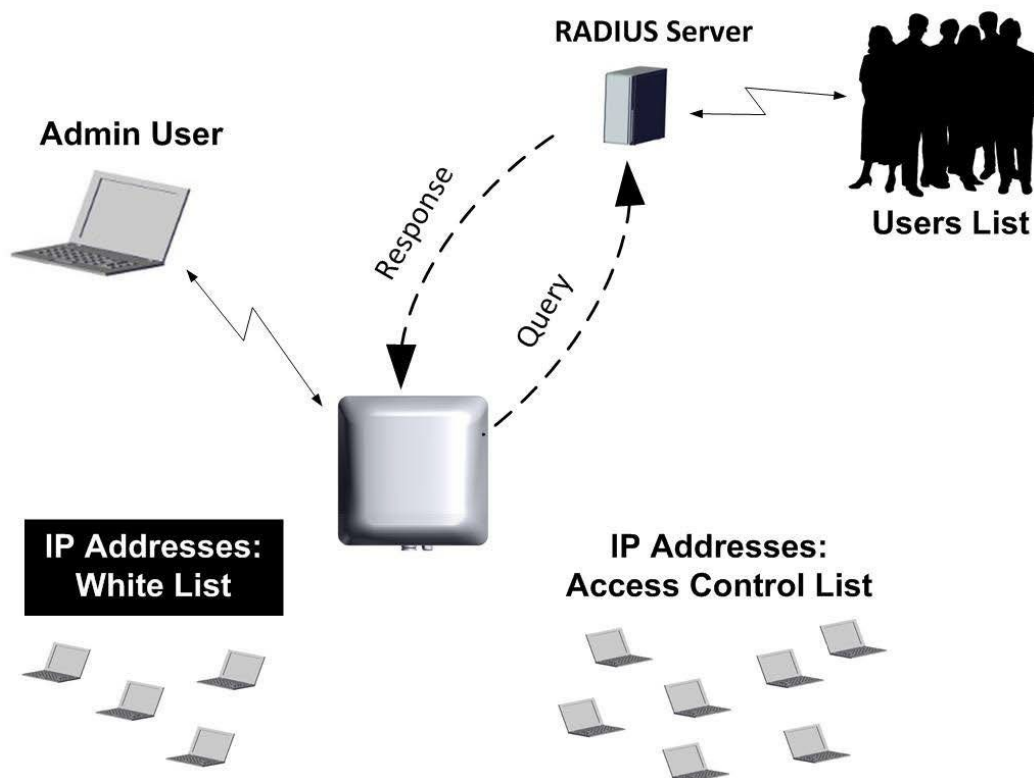



Figure 2-12: RADIUS Authentication set up

#### 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

Access Control List ⓘ White Access 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	⚙️

Cancel Save

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

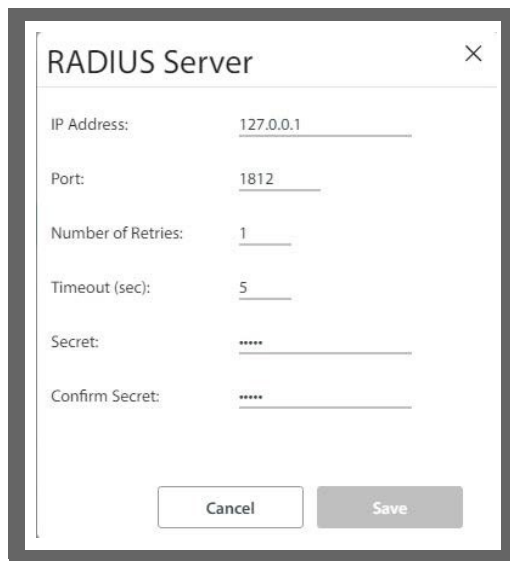


Note

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.



**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.



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:



The screenshot shows a dialog box titled "RADIUS Server" with a close button (X) in the top right corner. Inside the dialog, there are two input fields: "IP Address" with the value "10.107.4.201" and "Subnet Mask" with the value "255.255.255.0". At the bottom of the dialog, there are two buttons: "Cancel" and "Save".

- 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 (SU via HBS)

### Enable / Disable maintenance without IP (indirect)

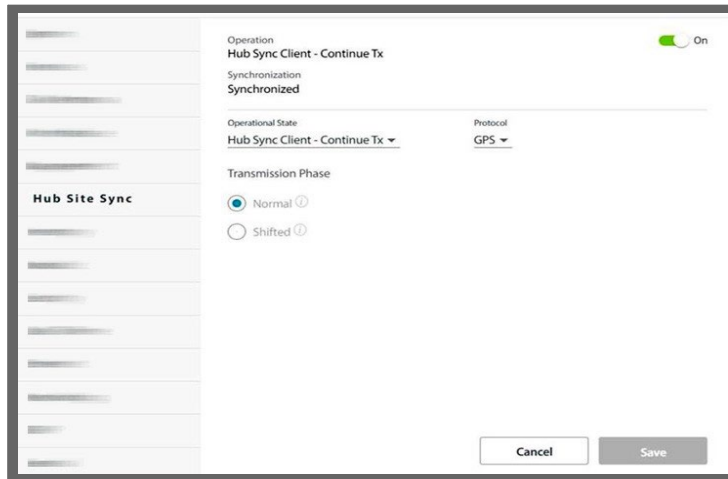
This option enables to perform SW upgrade or backup to SU devices via the BS without using the IP address of the SUs, meaning without having IP connection to the local IP address of the SU. If you don't use SW upgrade or backup without IP, or wish to disable IP forwarding, disable this option.

The screenshot displays a web configuration interface. On the left is a sidebar menu with a 'Management' section and an 'Advanced' section highlighted in light blue. The main content area shows the 'Enable/Disable Maintenance without IP (Indirect)' option, which is currently turned on (indicated by a green toggle switch and the text 'Enabled'). An information icon is visible next to the option name. At the bottom right of the main area are two buttons: 'Cancel' and 'Save'.

## Hub Site Sync tab (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.



## Inventory tab

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, hardware model type.

Dying Gasp status is also shown for supporting units (see below).



**HBS Configurations** ×

	Product RW5000/HBS-MS-PRO/SPG5/F54/UNI/128/INT - RW-SPG5-9154
	HW Version 211M
	SW Version 5.1.30_b0021_Jan 2 2022
	MAC Address 00:15:67:ec:3cd6
	Serial Number P19580IG00A00109
<b>Inventory</b>	
<b>General</b>	Aggregate Capacity 1500 Mbps
	Temperature 35 °C
	Power Consumption 12120 mW
	Supported Encryption AES 128
	HW Model Type Standard

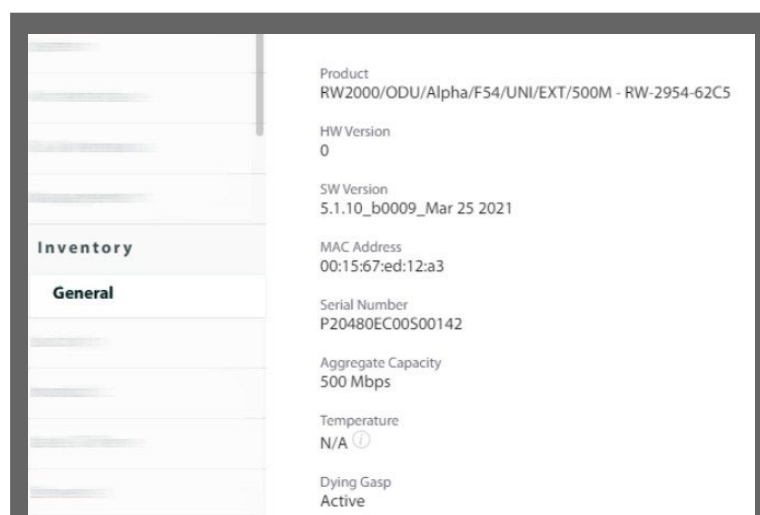
## Dying Gasp (SU only)

**Dying Gasp** feature (supported when using SU-Pro, Alpha or Alpha-PRO in PTMP SU mode):

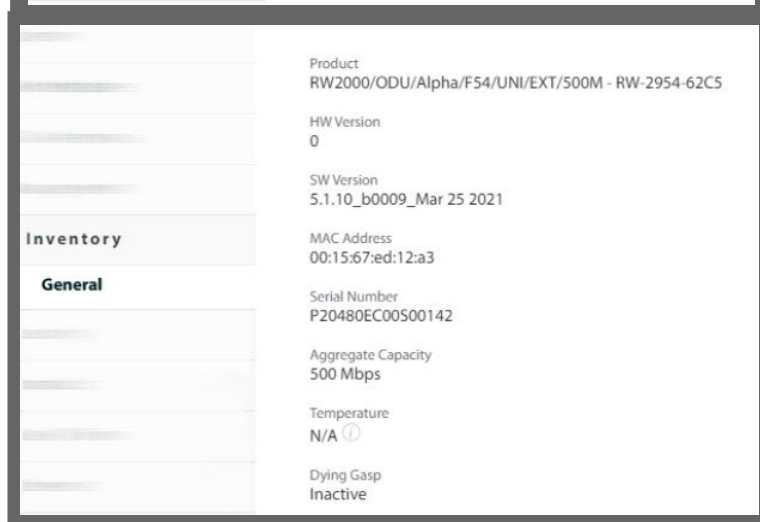
If the SU lost power, a signal is sent indicating that the reason for the sync loss is a power outage at the SU side.

### Notes:

- > You must use an appropriate PoE for the Dying Gasp feature to work. The 24V POE unit bundled with SU-Pro and Alpha-PRO does not support Dying Gasp. The PoE voltage must be  $\geq 55$  V. If the PoE voltage is lower than 50V, Dying Gasp will be inactive.
- > Dying Gasp only detects loss of AC or DC input feed of the POE injector unit. Disconnection of the POE cable cannot be detected.
- > Dying Gasp is supported for sector with up to 16 CPEs



**Dying Gasp active**



**Dying Gasp inactive**

## Nomadic tab (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.




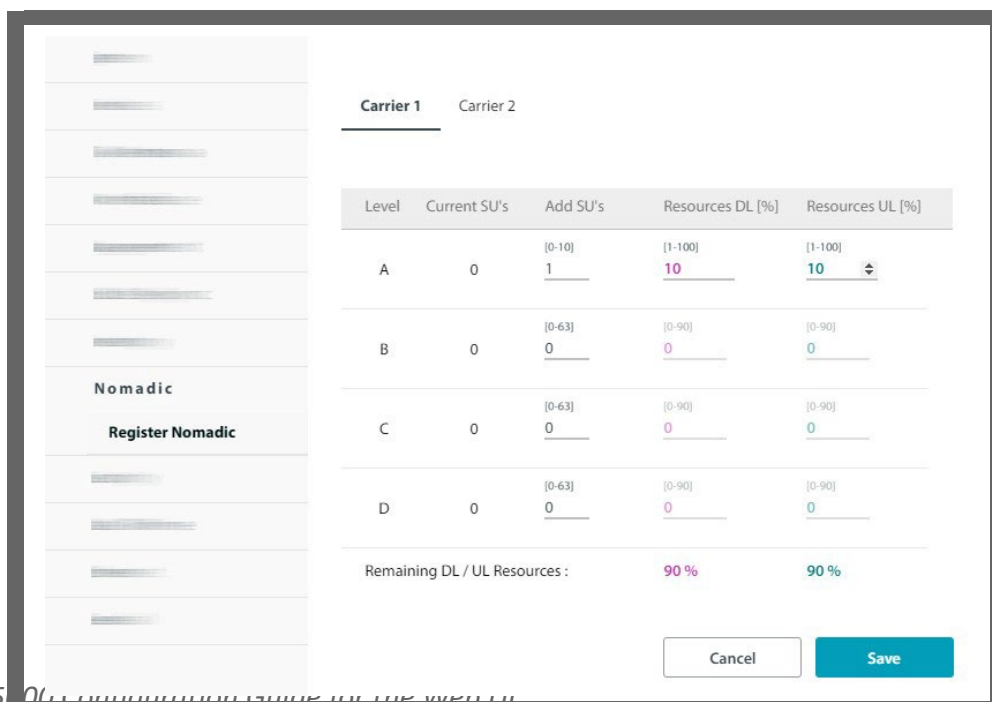
Changing the VLAN, MIR, QoS or Spatial Multiplexing/Diversity antenna mode for one configured SU at a given level changes all other SUs at that level.

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	<input type="text" value="1"/>	<input type="text" value="10"/>	<input type="text" value="10"/>
B	0	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
C	0	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
D	0	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

Remaining DL / UL Resources : 90 % / 90 %

Cancel Save

- 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.
- 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, SU-ECO 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	<u>2</u>	<u>10</u>	<u>10</u>
B	0	<u>10</u>	<u>1</u>	<u>1</u>
C	0	<u>0</u>	<u>0</u>	<u>0</u>
D	0	<u>0</u>	<u>0</u>	<u>0</u>
Remaining DL / UL Resources :			<b>70 %</b>	<b>70 %</b>

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:

Available SUs +		Name	IP Address	IPv6 Address	Status	Carrier	RSS HBS dBm	RSS SU dBm	RSS HBS Ant1 dBm	Tpout DL Mbps	Tpout UL Mbps	Eth Rx Rate Mbps	Eth Tx Mbps
<input type="checkbox"/>	6-29-P10_3X	10.107.6.29	:	Active Registered	2	-47	-42	-47	0.4	0.4	0.0	0.0	
<input type="checkbox"/>	6-24-U4C_3X	10.107.6.24	::11:0:0:0	Active Registered	2	-49	-39	-49	0.5	0.5	0.0	0.0	
<input type="checkbox"/>	Name_2	N/A	N/A	Not synchronized	1	N/A	N/A	N/A	N/A	N/A	N/A	N/A	
<input type="checkbox"/>	Name_1	N/A	N/A	Not synchronized	1	N/A	N/A	N/A	N/A	N/A	N/A	N/A	
<input type="checkbox"/>	Name_12	N/A	N/A	Not synchronized	1	N/A	N/A	N/A	N/A	N/A	N/A	N/A	
<input type="checkbox"/>	Name_11	N/A	N/A	Not synchronized	1	N/A	N/A	N/A	N/A	N/A	N/A	N/A	
<input type="checkbox"/>	Name_10	N/A	N/A	Not synchronized	1	N/A	N/A	N/A	N/A	N/A	N/A	N/A	
<input type="checkbox"/>	Name_9	N/A	N/A	Not synchronized	1	N/A	N/A	N/A	N/A	N/A	N/A	N/A	
<input type="checkbox"/>	Name_8	N/A	N/A	Not synchronized	1	N/A	N/A	N/A	N/A	N/A	N/A	N/A	
<input type="checkbox"/>	Name_5	N/A	N/A	Not synchronized	1	N/A	N/A	N/A	N/A	N/A	N/A	N/A	
<input type="checkbox"/>	Name_4	N/A	N/A	Not synchronized	1	N/A	N/A	N/A	N/A	N/A	N/A	N/A	
<input type="checkbox"/>	Name_8	N/A	N/A	Not synchronized	1	N/A	N/A	N/A	N/A	N/A	N/A	N/A	
<input type="checkbox"/>	Name_7	N/A	N/A	Not synchronized	1	N/A	N/A	N/A	N/A	N/A	N/A	N/A	

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

## Nomadic tab (SU)

SUs must be pre-configured for nomadic operation mode.  
For a full description of configuring an SU as Nomadic, see [Nomadic SU](#).

## Security tab

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

Current Read-Write Community [Forgot Community?](#)

Read-Write Community  
New  Confirm

Read-Only Community  
New  Confirm

Trap Community SNMPv1 only  
New  Confirm

Show Characters

Cancel Save

Following SNMPv1 communities are supported:

- Read-only community for polling information from the radio unit
- Read-write community to configure and control the radio unit
- Trap community for traps

#### 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.

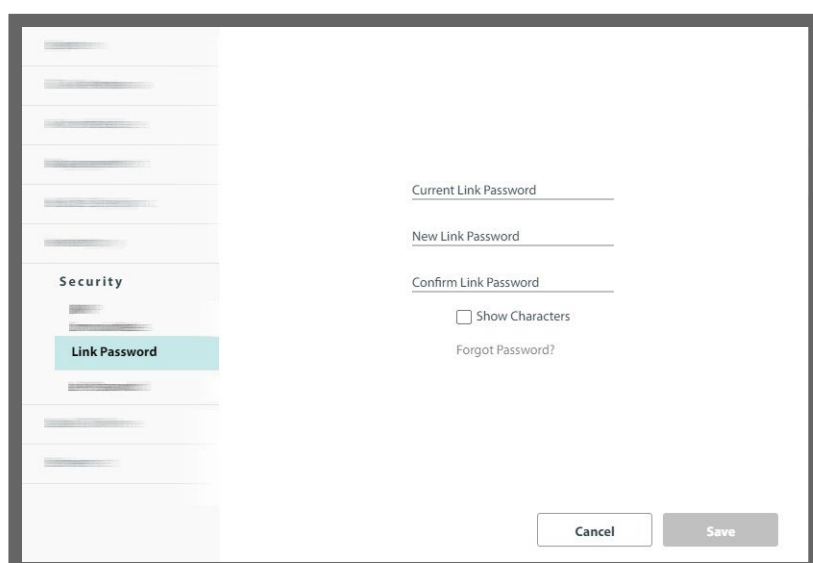
This item is available as follows:

- 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 current link password, you can enter the Alternative Key which is supplied with each radio unit.
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.



- 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-*





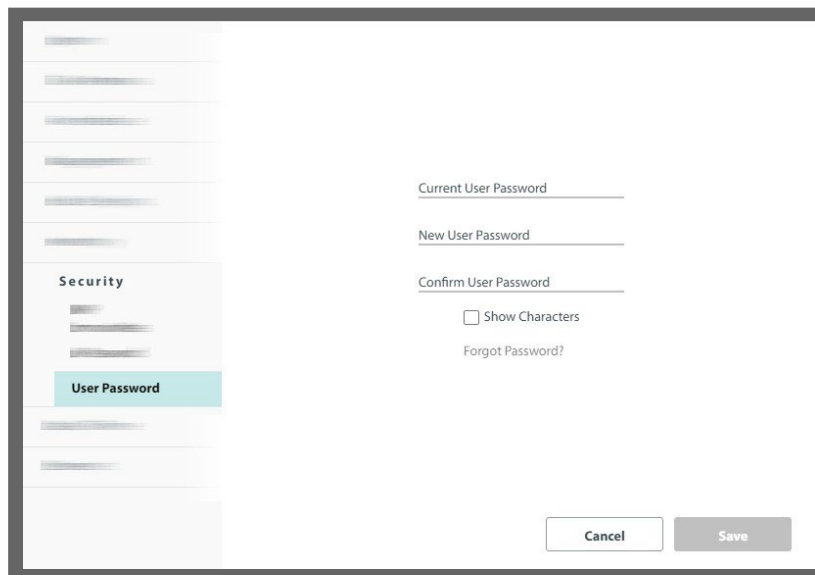
*p2mp.*

---

## 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 current link password, you can enter the Alternative Key which is supplied with each radio unit.

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.



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

## Security Mode

Security Mode controls the usage of Alternative Key which is a unique encrypted password designed as a recovery solution for cases when Link password or Admin user password are changed from the default settings, and then lost / forgotten. Alternative Key is supplied in the package with each RADWIN device, and can also be obtained by opening a support case.

Available options are:

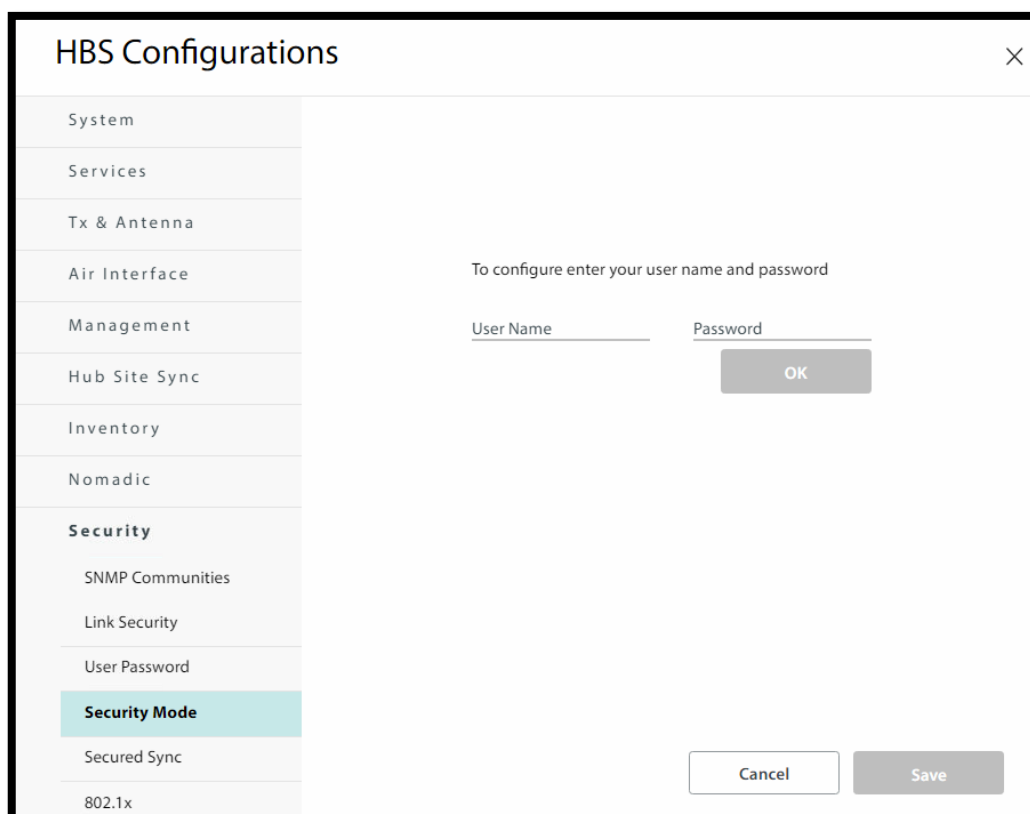
**Secured (default):** Alternative Key can always be used

**Enhanced Security\*:** Alternative key can be used only for 2 minutes after reset

**Enhanced Security:** Alternative key cannot be used. If user password is lost, the radio will have to be shipped for recovery via RMA procedure. Use only in high security environment to mitigate a concern for Alternative Key being used to gain unauthorized access to the SU.

Configure this mode as follows:

1. Make sure only SNMPv3 is allowed and HTTPs is enabled (see [Protocol](#))
2. Log in via HTTPs
3. Select **Configuration -> Security -> Security Mode**.



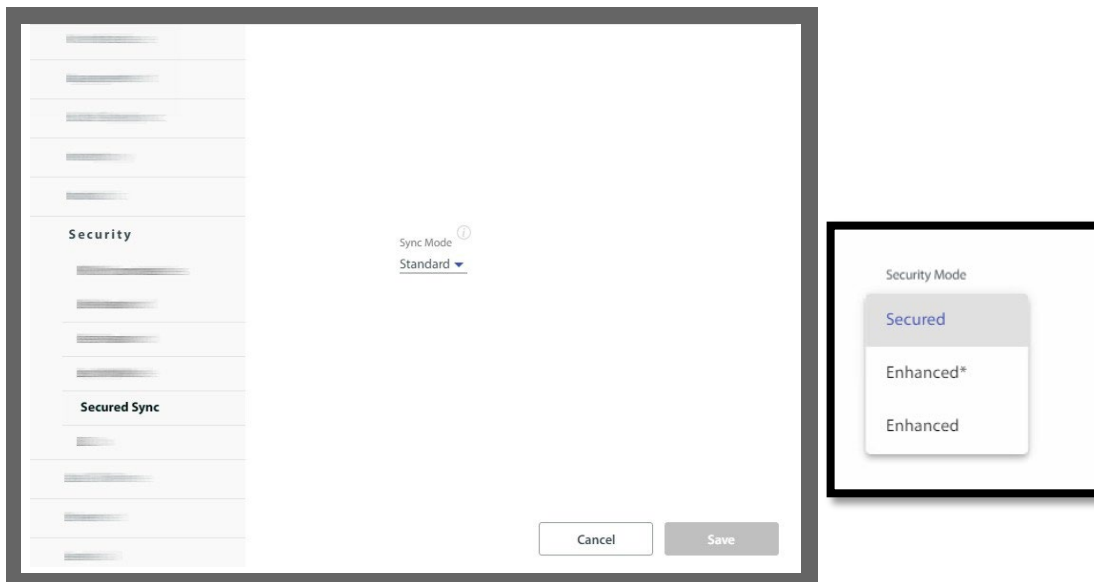
The screenshot shows the 'HBS Configurations' web interface. On the left is a navigation menu with the following items: System, Services, Tx & Antenna, Air Interface, Management, Hub Site Sync, Inventory, Nomadic, Security (expanded), SNMP Communities, Link Security, User Password, Security Mode (highlighted), Secured Sync, and 802.1x. The main content area displays a login prompt: 'To configure enter your user name and password'. Below this prompt are two input fields labeled 'User Name' and 'Password', followed by an 'OK' button. At the bottom of the main area are 'Cancel' and 'Save' buttons.

4. Enter your username and password and click **OK**.
5. Select the required security mode
6. Click **Save**.

## 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.



2. Click **Save**.



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.

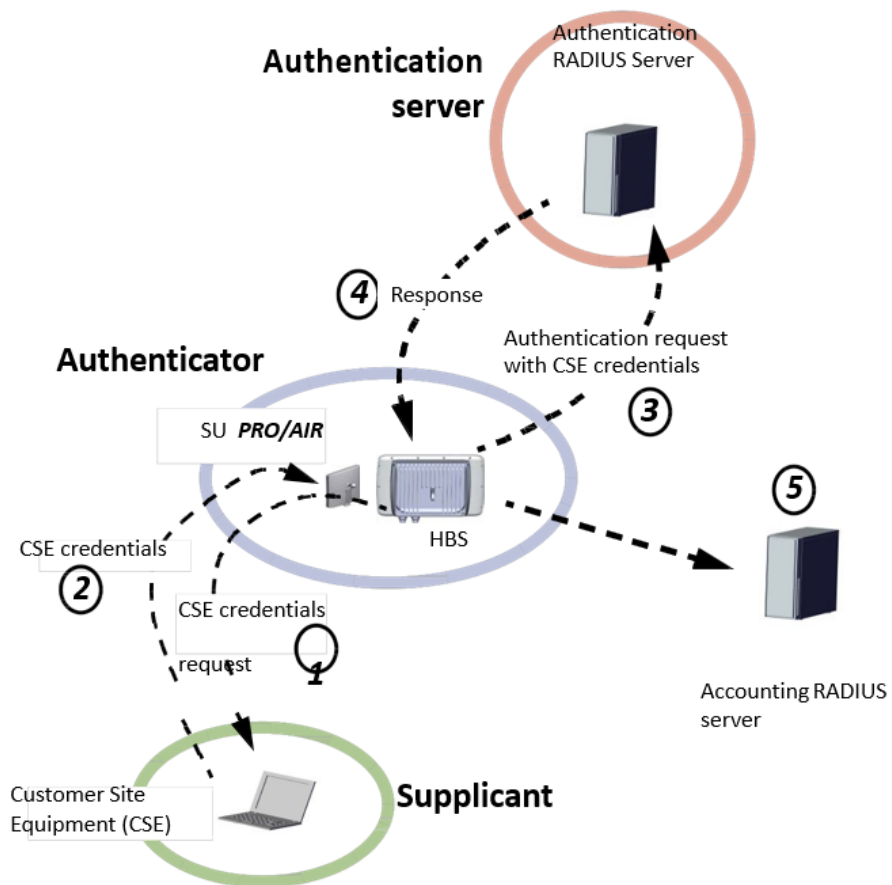
In the RADWIN implementation, the supplicant is the customer site equipment (CSE) the authenticator is the SU **PRO/AIR** EMB or SU Integrated & HBS<sup>1</sup>, and the authentication server is a customer-supplied RADIUS server. This works as follows:

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



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

---



Configure this feature as follows:

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

Enable 802.1x ⓘ

Re-authentication rate: Every  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	

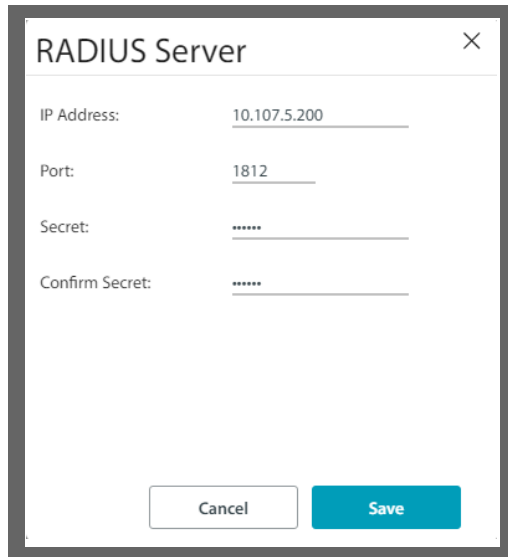
- To enable the 802.1x authentication mode, check **Enable 802.1x**.
- Next to **Re-authentication rate**, choose how often the authentication process is done (in seconds). The more often you choose to undertake this process, the better the security, but it requires more resources.
- RADIUS server settings:** 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.



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.

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





**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.



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.

# Date & Time tab

Here you can set the date and time of the selected unit manually, or synchronize it with 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.

If there is no NTP server available, you can set the date and time manually. Note that manual setting is not recommended since it will be overridden by any reset / power loss.



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

### To set date and time:

1. To manually set date and time, click the calendar icon and choose the new date, then click the spinner next to Time to choose the time.
2. To set the time based on the time of the managing computer, click **Use Computer Time**.
3. To set up NTP server as a time source:
  - a. Enter **NTP server** IP address
  - b. Set **Offset** value in minutes as per your timezone relative to UTC / GMT.
4. Click Save to have your changes take effect.

The screenshot shows a configuration window with the following elements:

- NTP Server** section:
  - NTP Server: 0.0.0.0
  - Offset: 0
- Date & Time** section:
  - Date: 11/22/2018 (with a calendar icon)
  - time: 01:58 PM (with a spinner)
  - Use Computer Time button
- Bottom buttons: Cancel and Save

# Ethernet tab

## LAN Ports

- **LAN1** refers to the RJ-45 Ethernet POE port on the radio unit (typically labeled as “POE” or “POE IN”)
- **SFP** transceiver slot is available on most HBS models (typically labeled as “LAN” or “SFP”)

**Current:** shows the current status, speed and duplex of the port

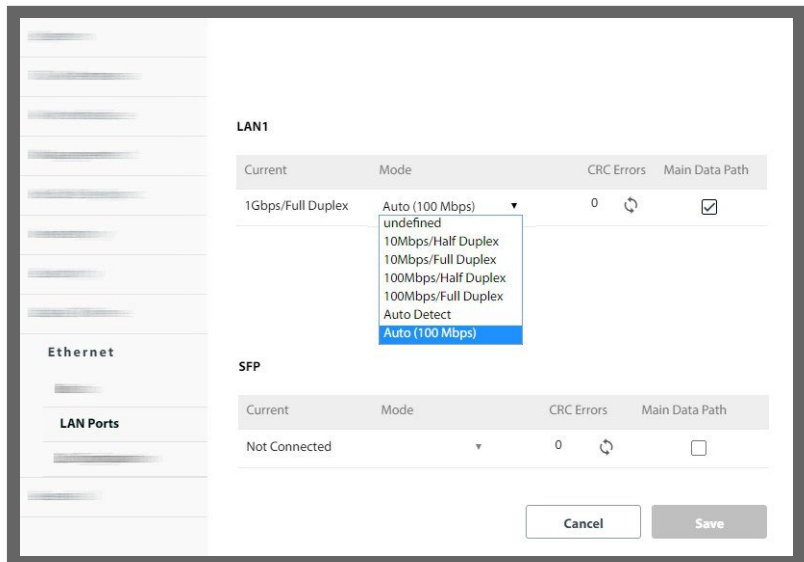
**Mode:** speed/duplex configuration (available only for LAN1 port)

- **Auto Detect:** auto-negotiate duplex and speed up to 1000 Mbps. This is the default and recommended setting
- **Auto Detect (100Mbps):** auto-negotiate duplex and speed, limited to 100 Mbps. This setting can be useful to provide a more robust Ethernet link in some cases when cable quality issues exist and 100Mbps LAN speed is good enough.
- **Manual modes - 10Mbps Half Duplex / 10Mbps Full Duplex / 100Mbps Half Duplex / 100Mbps Full Duplex**  
Manual speed/duplex can be used when connected Ethernet equipment does not support auto-negotiation, or if auto-negotiation must be disabled by design.

**CRC Errors** - Shows how many CRC errors occurred since the last reset

**Main Data Path:** selects the port for the data traffic

- 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 manage the base station itself



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

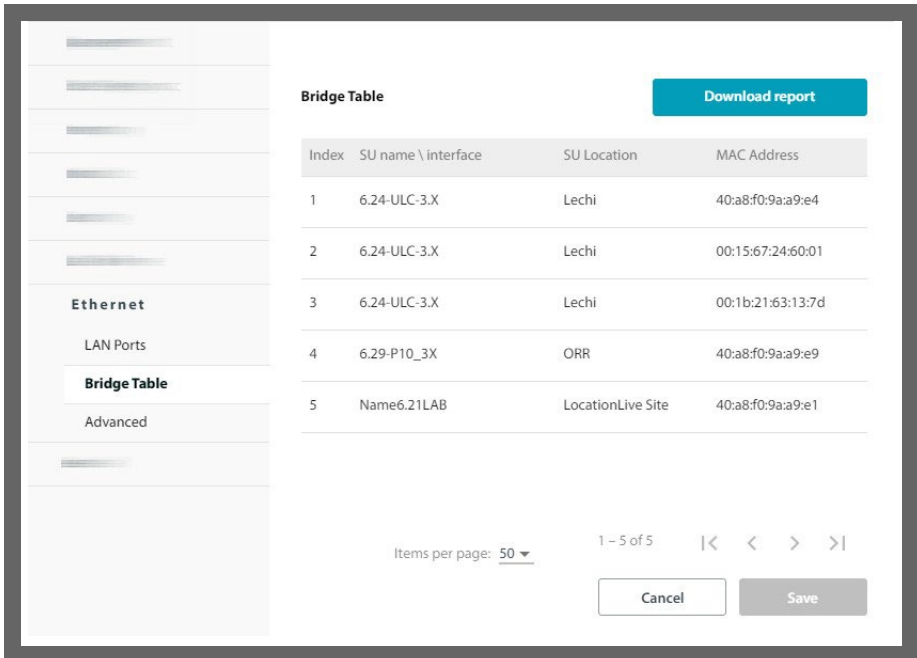
## Bridge Table

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**.



The screenshot displays the Bridge Table interface. On the left is a navigation menu with options: Ethernet, LAN Ports, Bridge Table (selected), and Advanced. The main area shows a table titled 'Bridge Table' with a 'Download report' button in the top right corner. The table contains the following data:

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

Below the table, there is a pagination control showing 'Items per page: 50' and '1 - 5 of 5' with navigation arrows. At the bottom right are 'Cancel' and 'Save' buttons.

- **Save** is not used here.

## Advanced (HBS only)

**HBS Configurations**

**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)

Advanced Cancel Save

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.

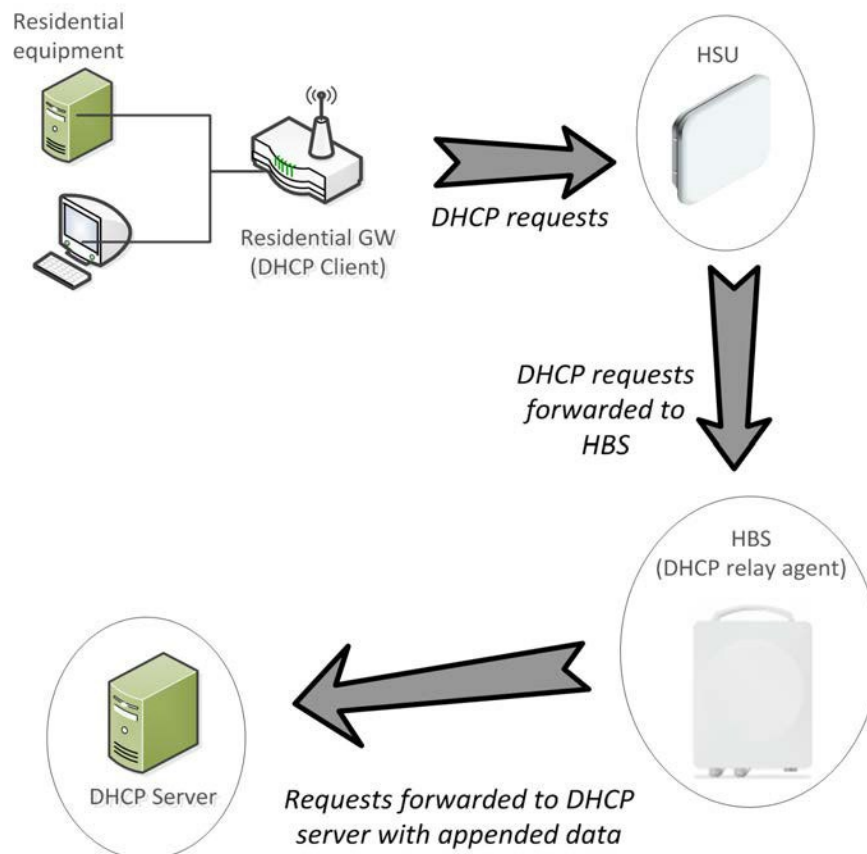


Figure 2-18: DHCP Relay Agent (Option 82): Method of operation

#### 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.



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).

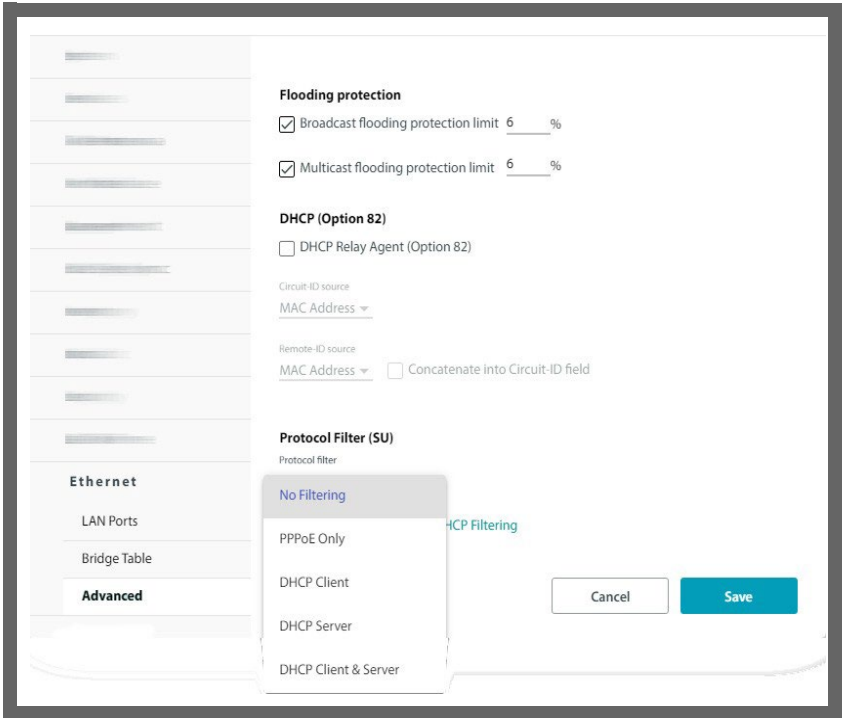
**DHCP Server:** Prevent DHCP Server responses from customer equipment from being forwarded to the HBS. DHCP Client responses can be forwarded.

**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.

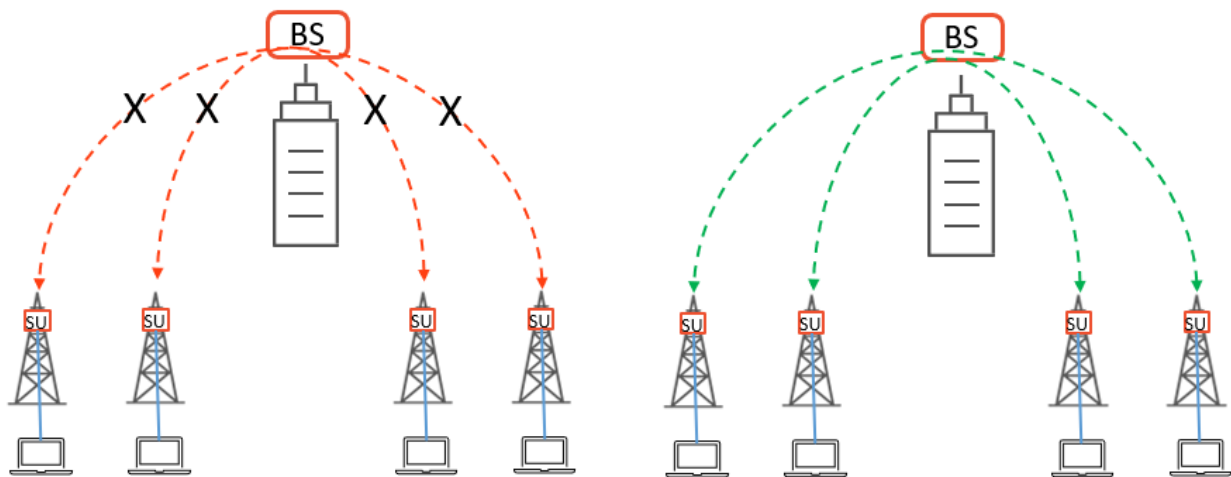




## SU interconnection

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.



## IGMP tab (HBS only)

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.

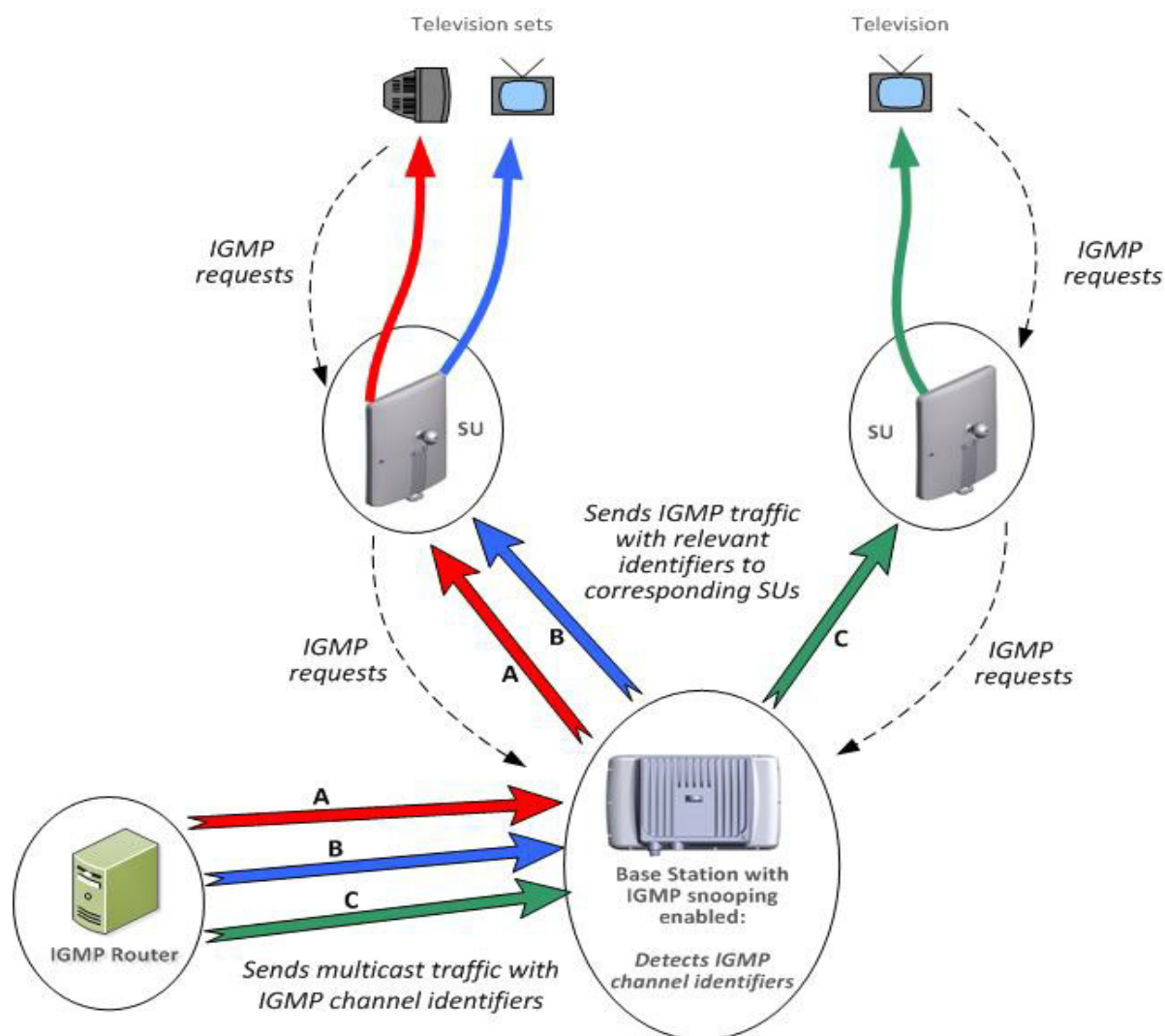


Figure 2-19: IGMP operation with the RADWIN 5000

- 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.

The screenshot displays the configuration page for IGMP. On the left, a sidebar menu contains several items, with 'IGMP' highlighted. The main content area on the right contains the following settings:

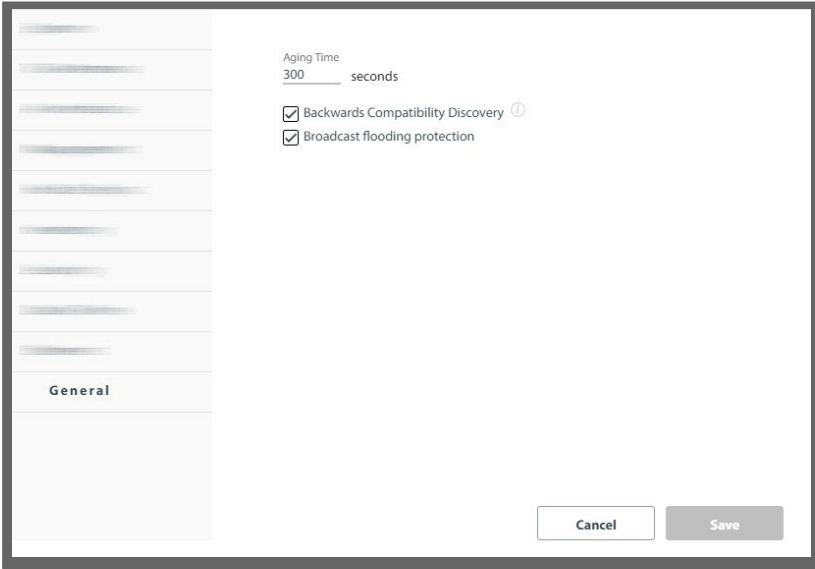
- Snooping Enabled
- Robustness:
- VLAN ID:   Off
- Total multicast groups: 5

At the bottom right of the configuration area, there are two buttons: 'Cancel' and 'Save'.

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

## General tab (HBS only)

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



The screenshot shows a configuration window with a sidebar on the left containing a 'General' tab. The main area displays the following settings:

- Aging Time: 300 seconds
- Backwards Compatibility Discovery ⓘ
- Broadcast flooding protection

At the bottom right, there are 'Cancel' and 'Save' buttons.

### ***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.

# Networking tab (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.

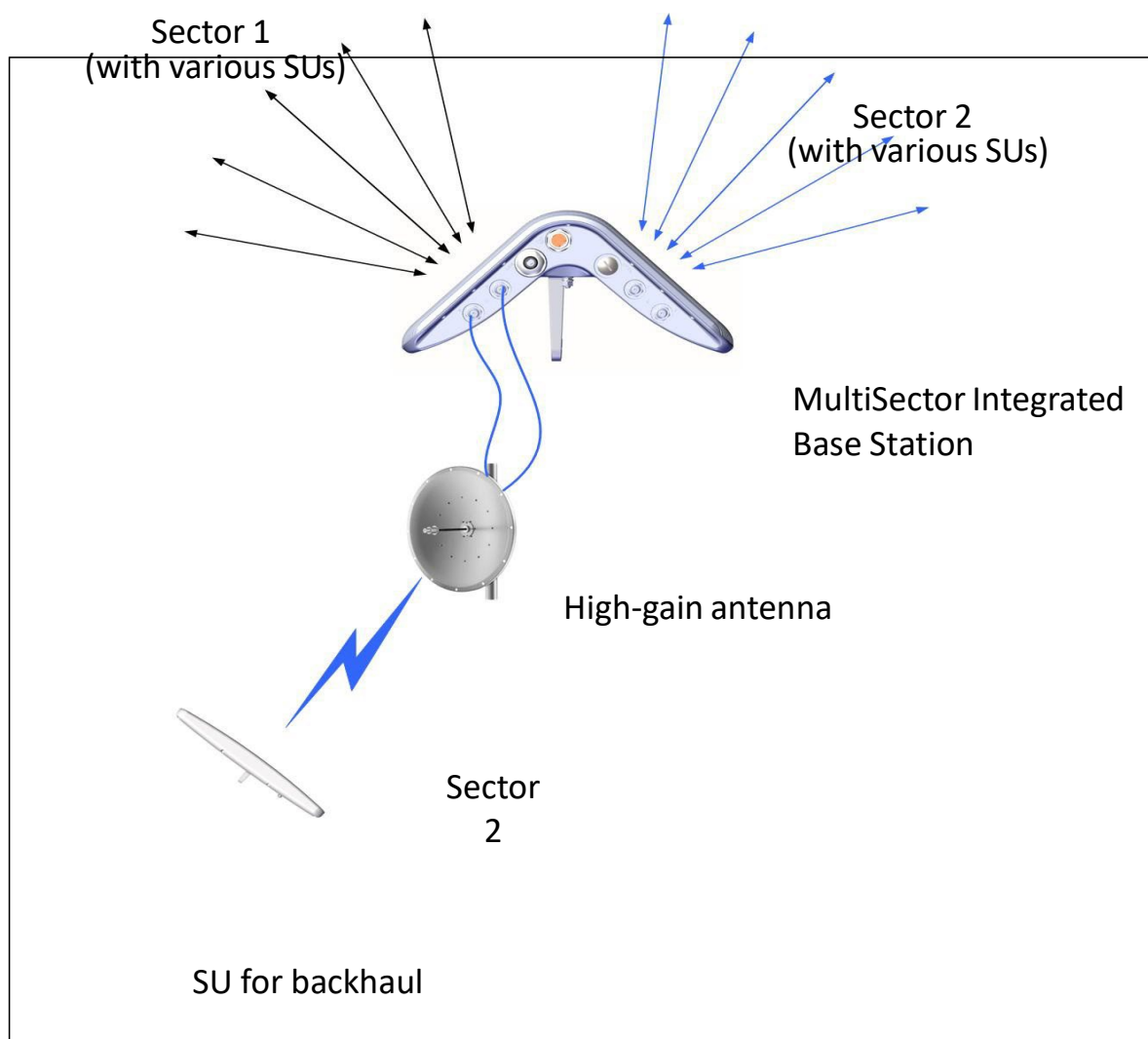


Figure 2-20: Sector Self-Backhaul: MultiSector Integrated

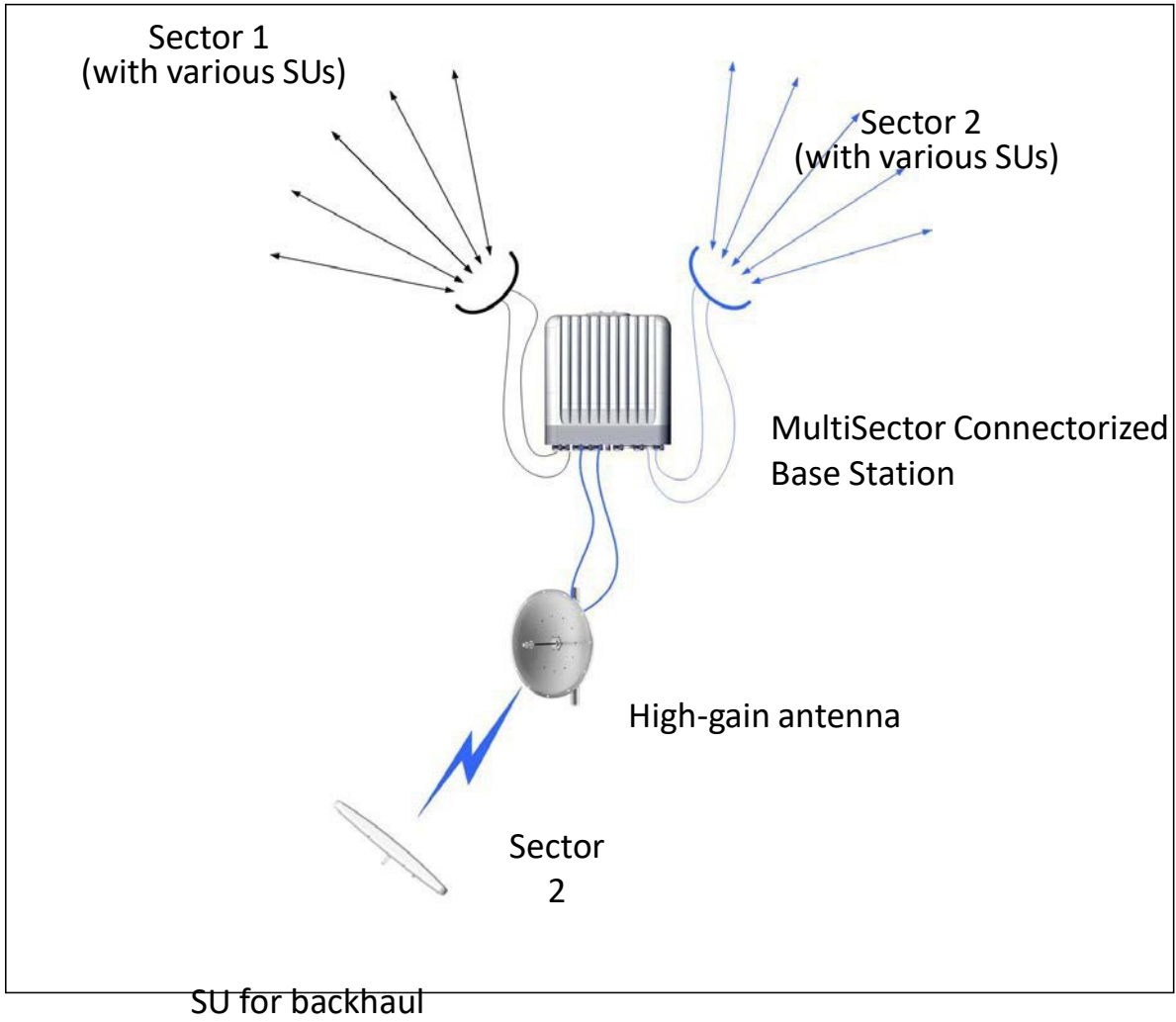
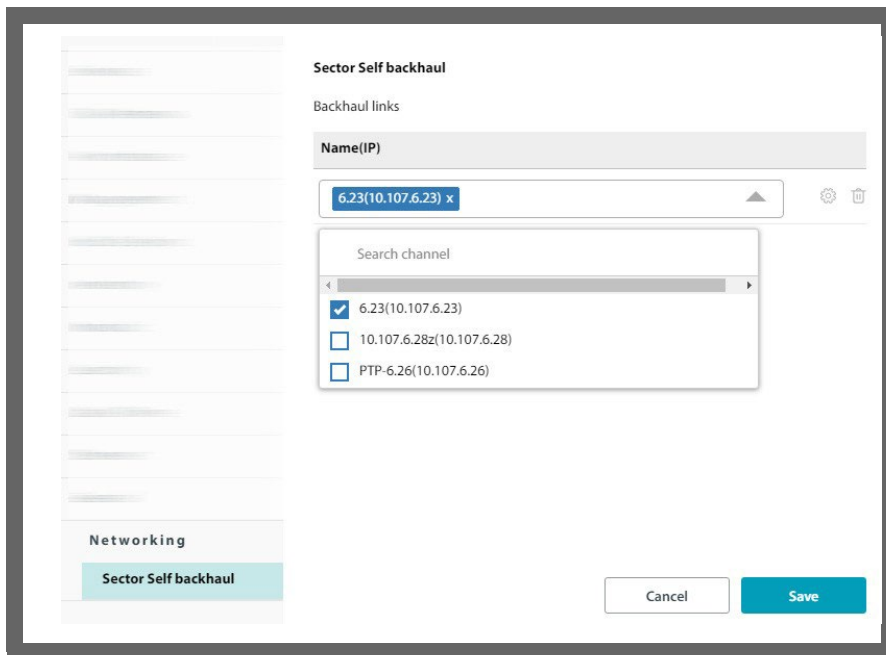


Figure 2-21: Sector Self-Backhaul: MultiSector Connectorized



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.

## WiFi tab (SU via HBS)

The screenshot shows a web-based configuration interface for WiFi. On the left is a sidebar with a 'Wifi' tab selected. The main area is titled 'SSID' and contains several configuration fields: 'Access Point Mode' (set to 'Auto'), 'Password', 'Security', 'IP Address', 'Channel', and 'TX Power'. Below these fields is a section titled 'Connected Clients' with a table showing 5 rows for client information. At the bottom right are 'Cancel' and 'Save' buttons.

#	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 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.

# Events Panel



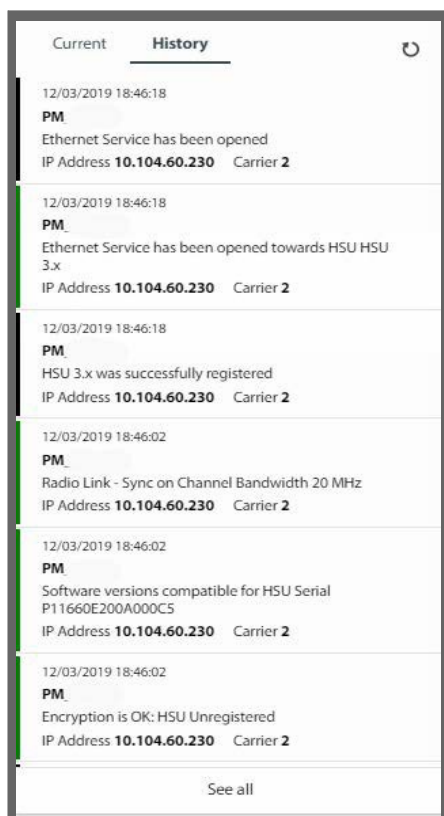
This panel allows you to see events for any or all units.

1. To display the Events Log, first select the unit or units for which you want to display events.

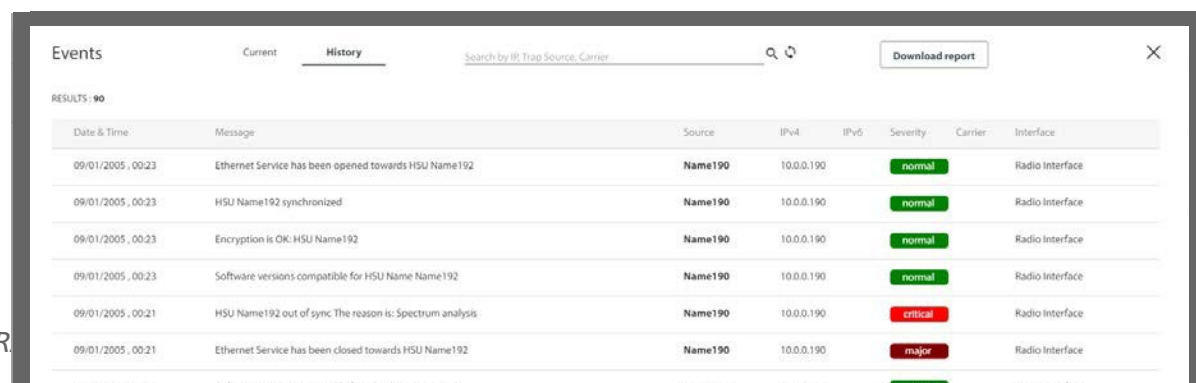
You can select any combination of units.



2. Click on the Events icon in the upper panel of the Web page ; 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.








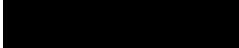
4. Click **See all** to see the full Events Log.



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

5. 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):

<b>Critical</b>	
<b>Major</b>	
<b>Minor</b>	
<b>Warning</b>	
<b>Normal</b>	
<b>Info</b>	

- » 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
  8. Click Download report to save the Events Log as a CSV or PDF file

## Performance monitor



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	Threshold	Refresh	Download report	
Integrity	Date & Time	UAS	ES	SES	BRE	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

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.

# Spectrum scan



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.

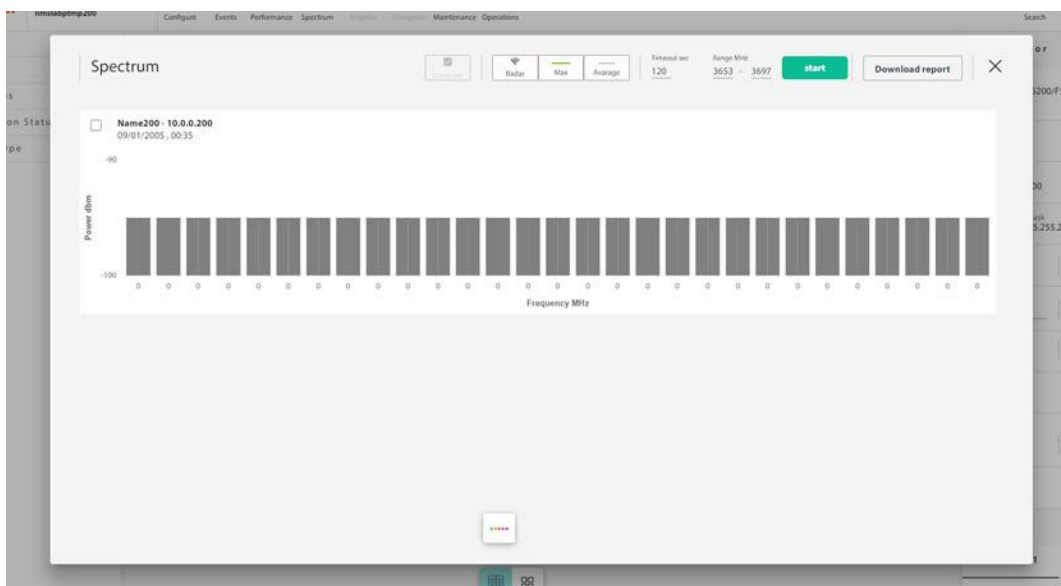
The results of the Spectrum View utility are intended for use by RADWIN Customer Service to assist with diagnosing interference related problems.

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 .
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.



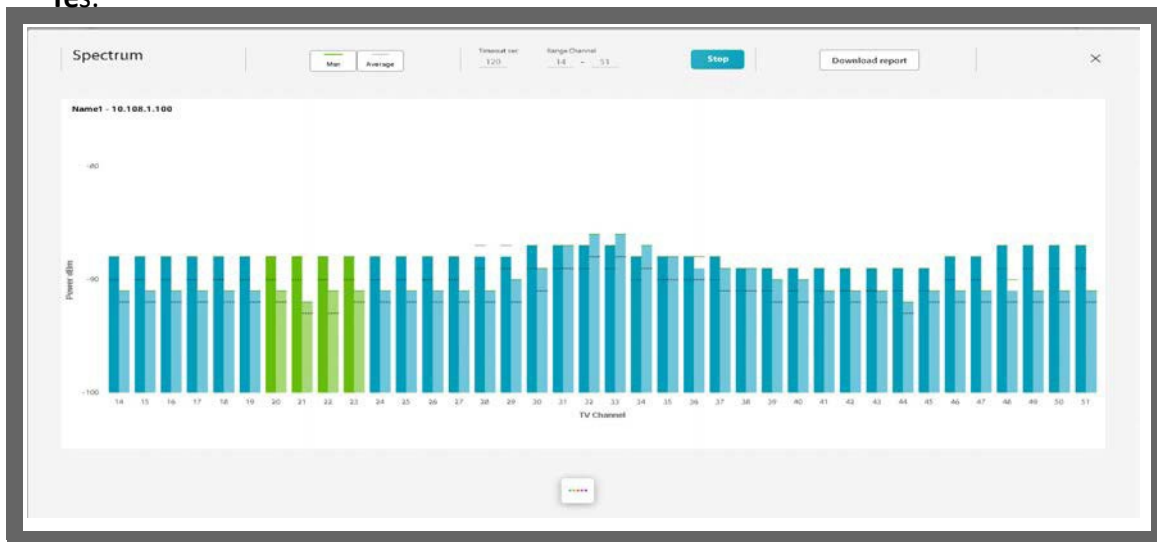
A blank Spectrum View result display will appear, where all the bars are grey.

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 **Yes**.



- 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.


## Utilization monitor



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

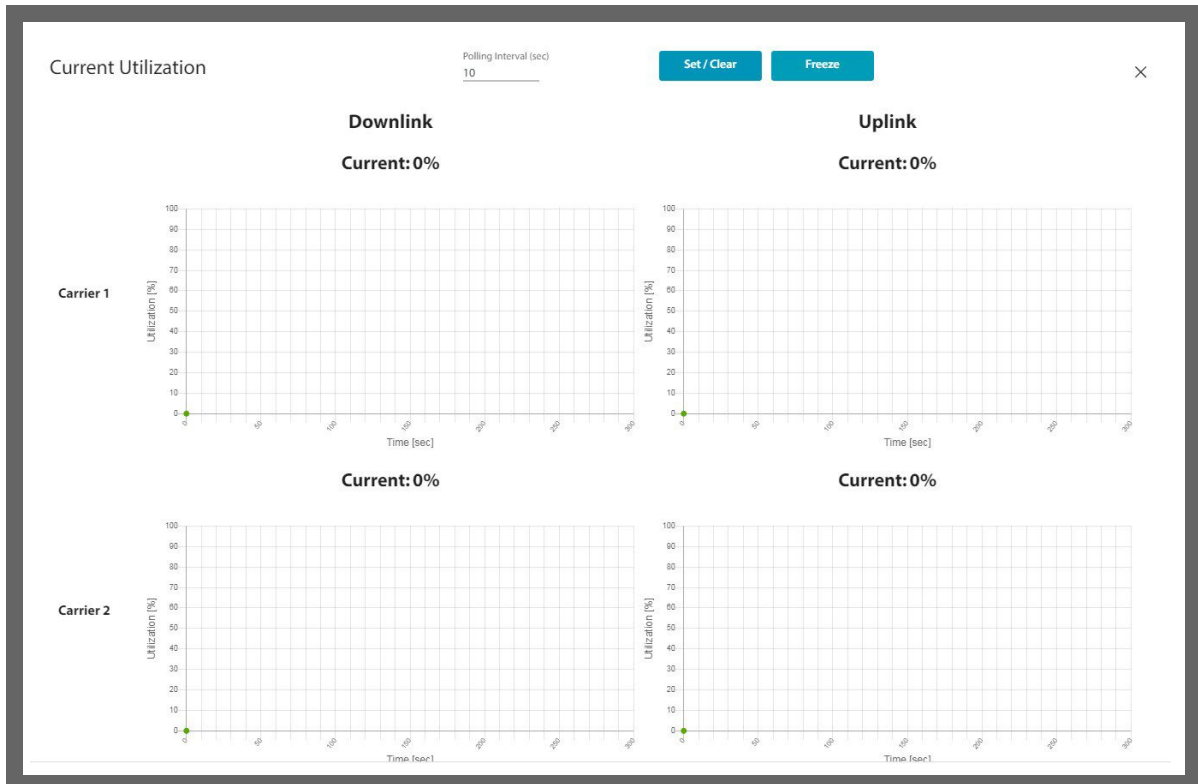
activity.

To check the utilization for the whole sector, do the following:

1. Select the HBS.
2. Click the Utilization icon (). 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 is calculated as follows:

- Set a polling interval, in seconds, then 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:

$$Utilization = \frac{CSU_{new} - CSU_{old}}{CSP_{new} - CSP_{old}}$$

- 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.

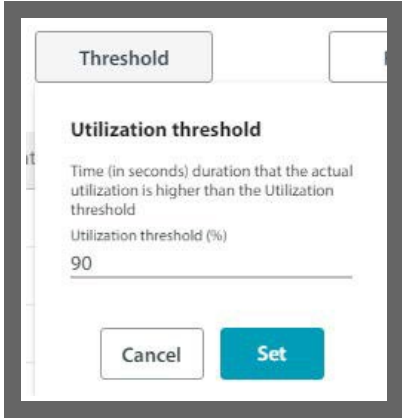
Date & Time	DL Utilization (%)	UL Utilization (%)	DL Utilization Threshold crossing seconds	UL Utilization Threshold crossing seconds
04/06/2020 13:45:00	0	0	0	0
04/06/2020 13:30:00	0	0	0	0
04/06/2020 13:15:00	0	0	0	0
04/06/2020 13:00:00	0	0	0	0
04/06/2020 12:45:00	0	0	0	0
04/06/2020 12:30:00	0	0	0	0
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.

- **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**.
- **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.



The image shows a dialog box titled "Threshold" with a sub-header "Utilization threshold". The text inside the dialog reads: "Time (in seconds) duration that the actual utilization is higher than the Utilization threshold". Below this, there is a label "Utilization threshold (%)" followed by a text input field containing the value "90". At the bottom of the dialog, there are two buttons: "Cancel" and "Set".

# 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.




The Carrier Switch only works with SU **PRO/AIR** subscriber units, and only with the NEO DUO, JET AIR DUO, 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 (  ) in the main window to open the Carrier Switch Events display:



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<sup>1</sup>.

**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<sup>1</sup>.

**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.

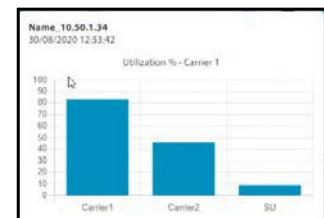
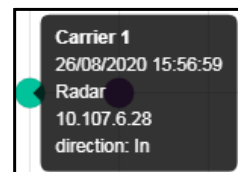
**Utilization** - If the utilization of the carrier rises above 80% while the utilization of the other carrier is less than 60%. A switch, in this case, balances the load between the carriers.

**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).
- 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 under- went 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 download the report in CSV or PDF format.

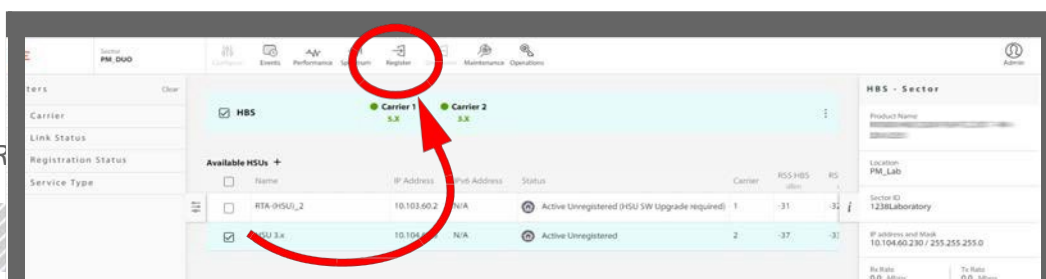
- You can filter the events shown by the IP of the SU, the cause of the event, and the direction of the event (“In” or “Out”).

## Register SU



To enable the SU to communicate with the HBS, you must *register* it.

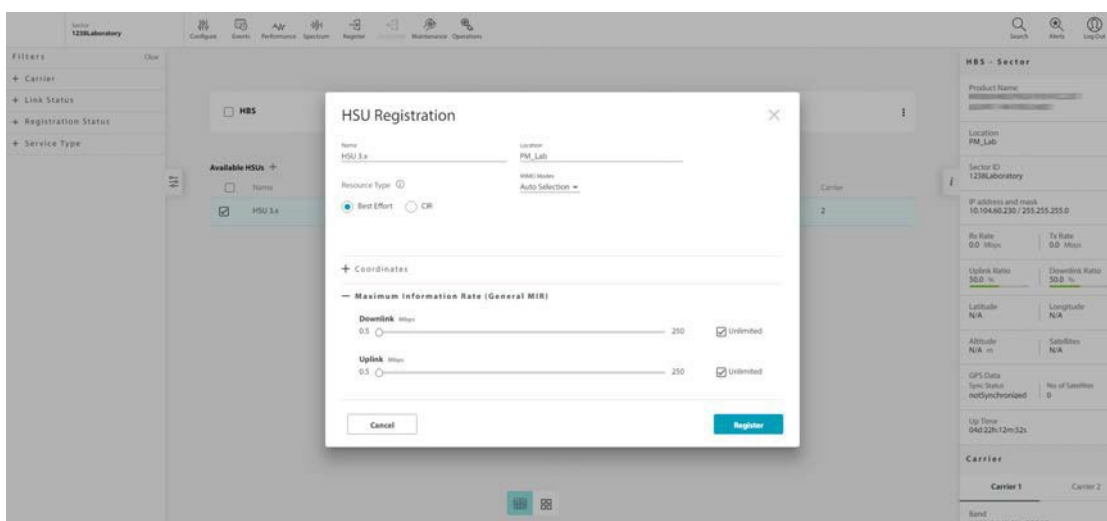
1. Select the SU you want to register by placing a checkmark next to it.



Click  
**Register**

Select HSU

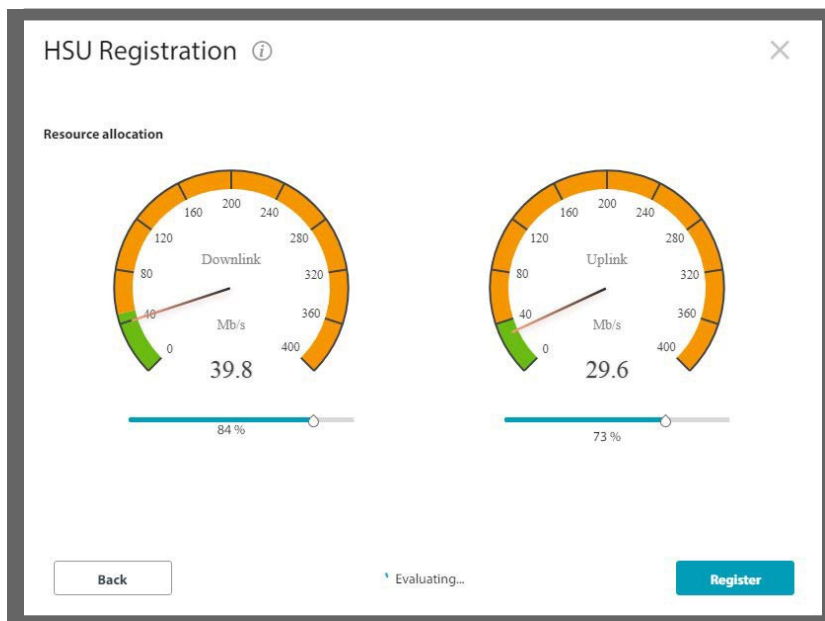
2. Click **Register**. The SU Registration window will open.



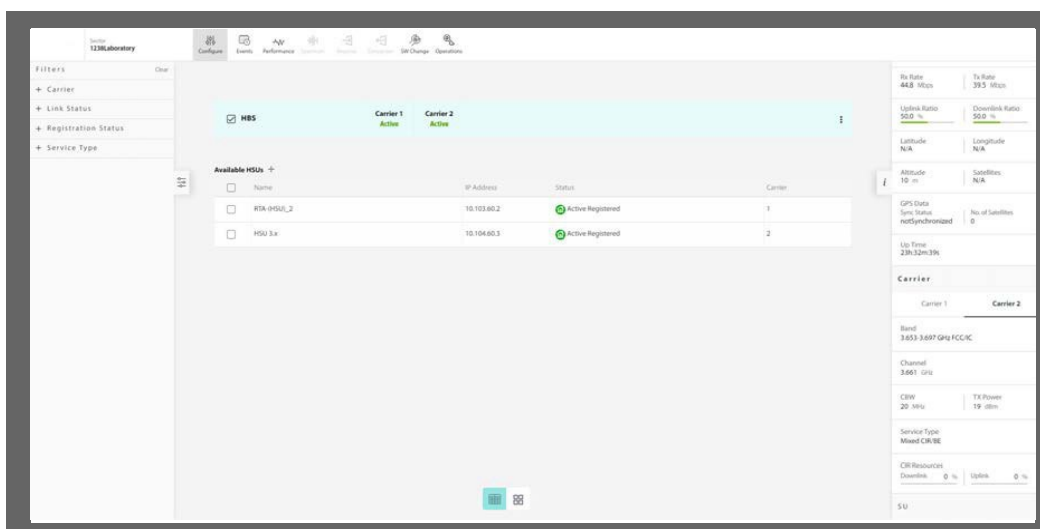
3. You may edit or add the site's name, location and coordinates.
4. Select the Resource Type for the SU. This can be CIR (Committed Information Rate), or BE (Best Effort):
  - BE grants the SU resources as they become available in the sector.
  - CIR grants the SU with a certain guaranteed percentage of resources.
5. Check a MIMO Mode for this SU:
  - **Auto Selection** (default) lets the system choose the best mode
  - **Spatial Multiplexing** 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. This mode is more reliable for nLOS or reflections, but will provide 50% lower throughput.
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 seconds, the SU will be registered.
8. If you chose the CIR resource type in Step 4 above, resource allocation must be adjusted before registration. Click **Evaluate**.
9. CIR throughput evaluation dials will appear. Use the sliders to choose the percentage of Downlink and Uplink resources to be allocated to the SU from the total resources of the sector. Dials will display the CIR throughput the SU will provide. Keep in mind that the CIR throughput depends on the current link performance and may fluctuate as the link conditions change.



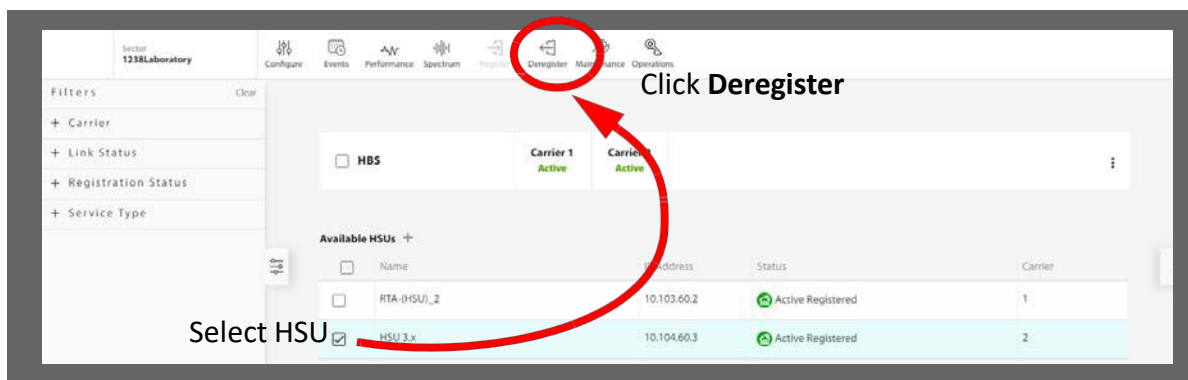
10. When a stable value is reached, the **Register** button will become enabled.
11. Click **Register**. The SU will change its status to Active Registered:



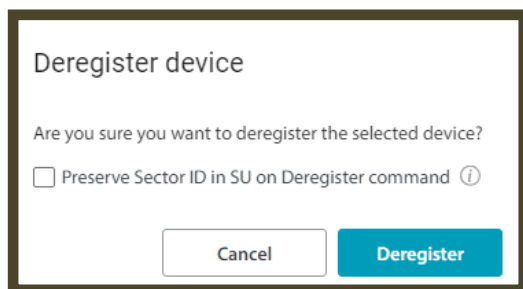
# Deregister SU



1. Select the SU you want to de-register by placing a checkmark next to it.



2. Click **Deregister**. You will be asked to confirm that you want to deregister the radio.



3. if you are sure, click **Deregister**. The device will no longer be registered.

Starting from release 5.1.30, there is an option to preserve the Sector ID on the de-registered SU, which is useful to keep the SU synchronized with the current HBS. Select the “Preserved Sector ID” before deregistering if you wish to do so.

# Maintenance tools



This allows you to perform software and configuration maintenance operations on the HBS and/or on the SUs synchronized to the sector.

2. On HBS home page, select all the relevant ODU's which you want to upgrade / backup
3. Choose the action by clicking on the Maintenance menu.

The screenshot shows the RADWIN Manager web interface. At the top, there is a navigation bar with icons for Configure, Events, Performance, Spectrum, Utilization, Carrier Switch, Register, Deregister, Maintenance, Operations, and Diagnostics. The Maintenance menu is open, showing options for Upgrade, Backup, and Restore. Below this, there is a summary for HBS with two carriers, Carrier 1 and Carrier 2, both showing 5.X. Below that is a table of Available SU's.

Available SU's +						
<input type="checkbox"/>	Name	IP Address	Status	Carrier	RSS HBS dBm	
<input checked="" type="checkbox"/>	SU-2	10.0.101.12	Active Registered	1	-69	
<input checked="" type="checkbox"/>	SU-1	10.0.101.11	Active Registered	1	-73	

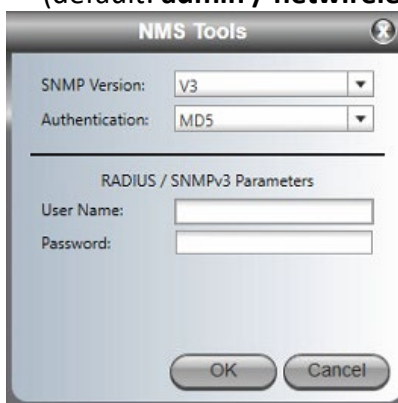
- **Upgrade:** Install a new ODU software version
- **Backup:** export current ODU software and configuration to a backup file
- **Restore:** import ODU software and configuration from a backup file

Any of these actions requires the NMSTools.exe application. This application is part of the RADWIN Manager package, which must be installed on your computer.

- Browser will request a permission to **Open NMSTools.exe** to launch the application. Approve the request.
- Select SNMP version (V1/V3) according to ODU settings
- For SNMPv1 – enter read/write community (default: **netman**)



- For SNMPv3 – select Authentication protocol (MD5/SHA), enter user name and password for a user with permissions for maintenance operations (default: **admin / netwireless**)

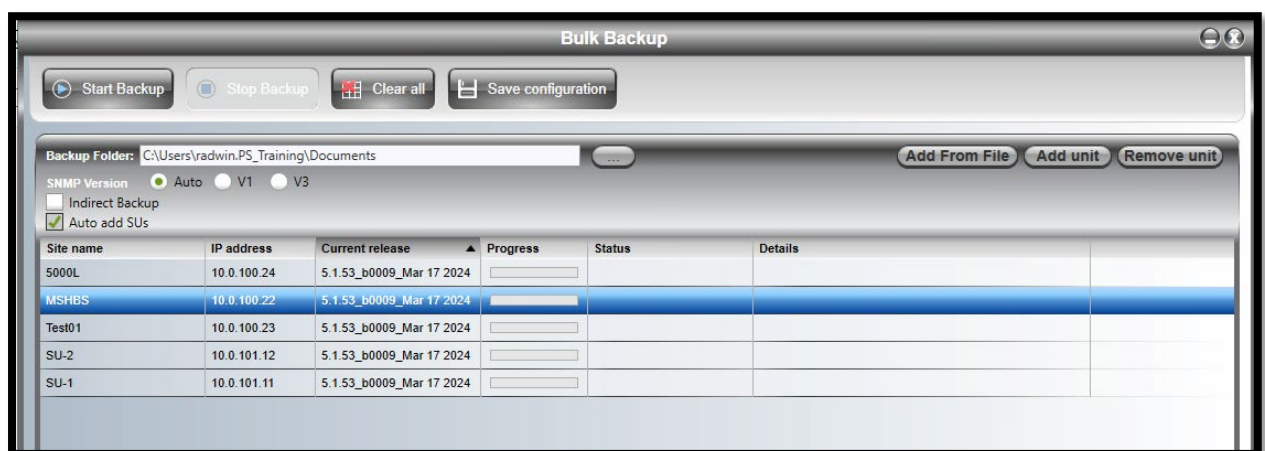


- Click OK. NMS Tools will be launched.

## Backup

If Backup was selected, NMS Tools will launch in Bulk Backup mode.

All devices previously selected in the HBS home page will be added to the Bulk Backup list.



**Backup Folder** – Windows path to the folder where backup files will be stored. By default, the current user’s Documents folder is selected. Edit the Windows path or press selection



button (...) to select a desired folder.

**Indirect Backup** - enables to backup subscriber units via the HBS without a direct IP connectivity to SUs.

- Make sure Indirect connectivity is enabled on SUs (see [Chapter 3 - Management / Advanced](#))
- Indirect mode is not supported for IPv6.

**Auto add SUs** – if Indirect Backup is selected, Software Upgrade list panel will be populated with SUs connected to the HBS.

**Add From File** – opens a Windows file dialog to upload a text file with list of devices to upgrade. Each line in the file should be in the following format:

<IP address>,<Read-Write community>,<username>,<password>

- Enter IP address for each device
- For SNMPv1, provide the Read-Write community – for example:  
**10.104.50.4,netman**
- For SNMPv3, provide the Username and password – for example:  
**10.104.50.200,,admin,netwireless**

**Add unit** – opens a dialog to enter IP and credentials for a single device. Press OK, the device will be added to the list.

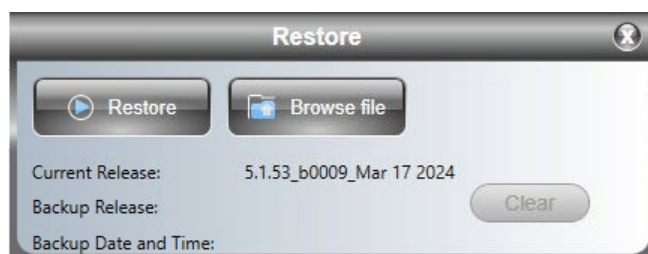
**Remove unit** - To remove a device from the list, select it by clicking on a specific line and click this button. Several devices can be selected by holding Shift and Ctrl buttons.



After devices are added to the list using one of the methods above, the tool check for connectivity and lists current software release for all devices. Once ready, click on **Start Backup** to initiate the backup operation

## Restore

If Restore was selected, NMS Tools will launch in Restore mode.



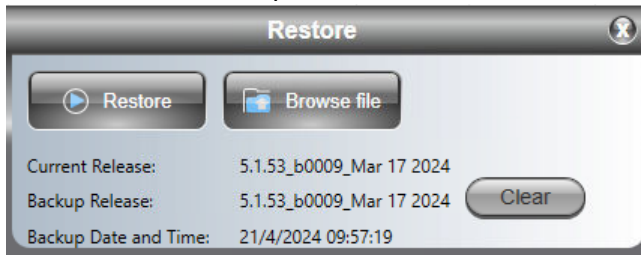
The tool will indicate the current software release of the radio unit.

**Browse File** opens Windows file selection dialog to select the backup file. Select the backup file. You will be asked if you want to preserve the current IP address of



the device. Confirm the selection. The backup file will be uploaded to the device.

After the backup file is uploaded and validated, the tool will present the software release of the backup file, as well as date and time when backup was performed:



**Clear:** remove the uploaded restore data from the device

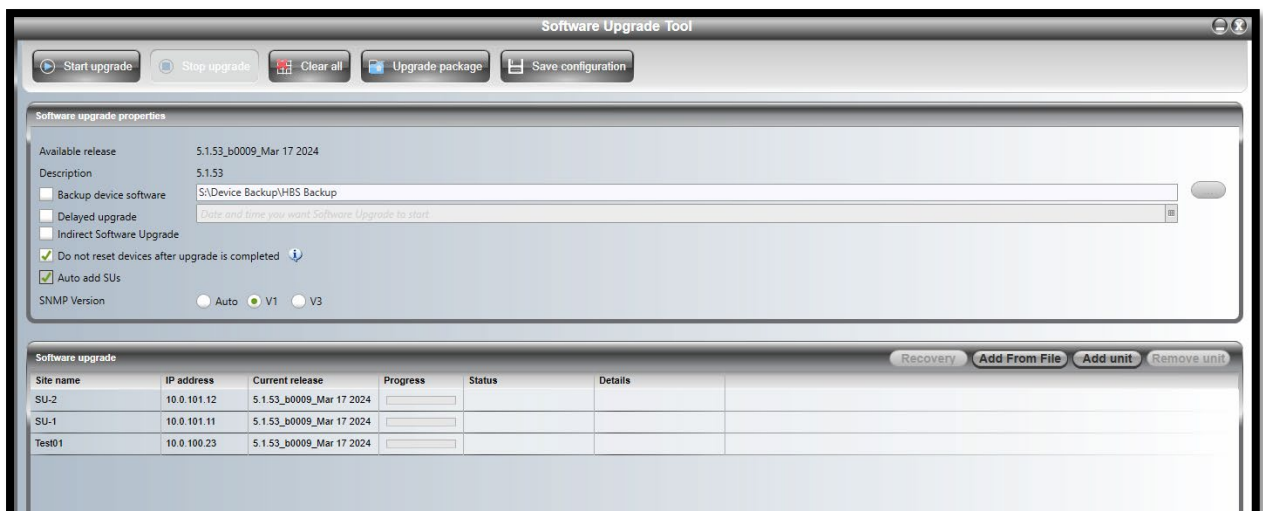
**Restore:** proceed with the restore operation (you will be asked for confirmation):



**Note:** Restore can be carried out on either the same unit from which a backup was carried out, or on a different unit. If doing a Restore on a different unit, the product part number and hardware version must be the same as that of the backup HBS unit (For more details, See [Inventory](#)).

## Upgrade

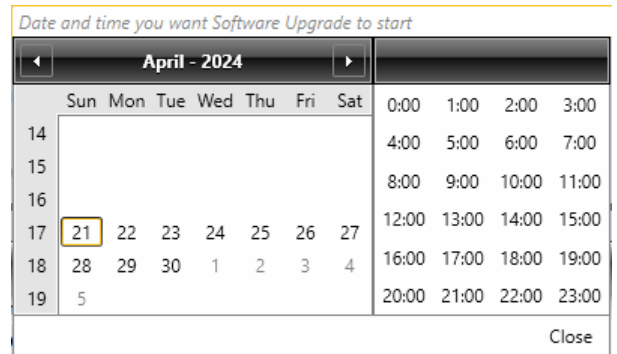
If Restore was selected, NMS Tools will launch in Software Upgrade mode. All devices previously selected in the HBS home page will be added to the Software Upgrade list.



**Backup device software** – select this option if you want to perform software backup before upgrade (recommended). By default, the current user’s Documents folder is selected as the

folder where backup files will be stored. Edit the Windows path or press selection button (...) to select a desired folder.

**Delayed Upgrade** - allows to set the date and time for scheduled upgrade. A Calendar dialog box opens:



**Indirect Upgrade** - enables to upgrade subscriber units via the HBS without a direct IP connectivity to SUs.

- Make sure Indirect connectivity is enabled on SUs (see [Chapter 3 - Management / Advanced](#))
- Indirect mode is not supported for IPv6.

**Auto add SUs** – if Indirect Backup is selected, Software Upgrade list panel will be populated with SUs connected to the HBS.

**Add From File** – opens a Windows file dialog to upload a text file with list of devices to upgrade. Each line in the file should be in the following format:

<IP address>,<Read-Write community>,<username>,<password>

- Enter IP address for each device
- For SNMPv1, provide the Read-Write community – for example:  
**10.104.50.4,netman**
- For SNMPv3, provide the Username and password – for example:  
**10.104.50.200,,admin,netwireless**

**Add unit** – opens a dialog to enter IP and credentials for a single device. Press OK, the device will be added to the list.

**Remove unit** - To remove a device from the list, select it by clicking on a specific line and click this button. Several devices can be selected by holding Shift and Ctrl buttons.

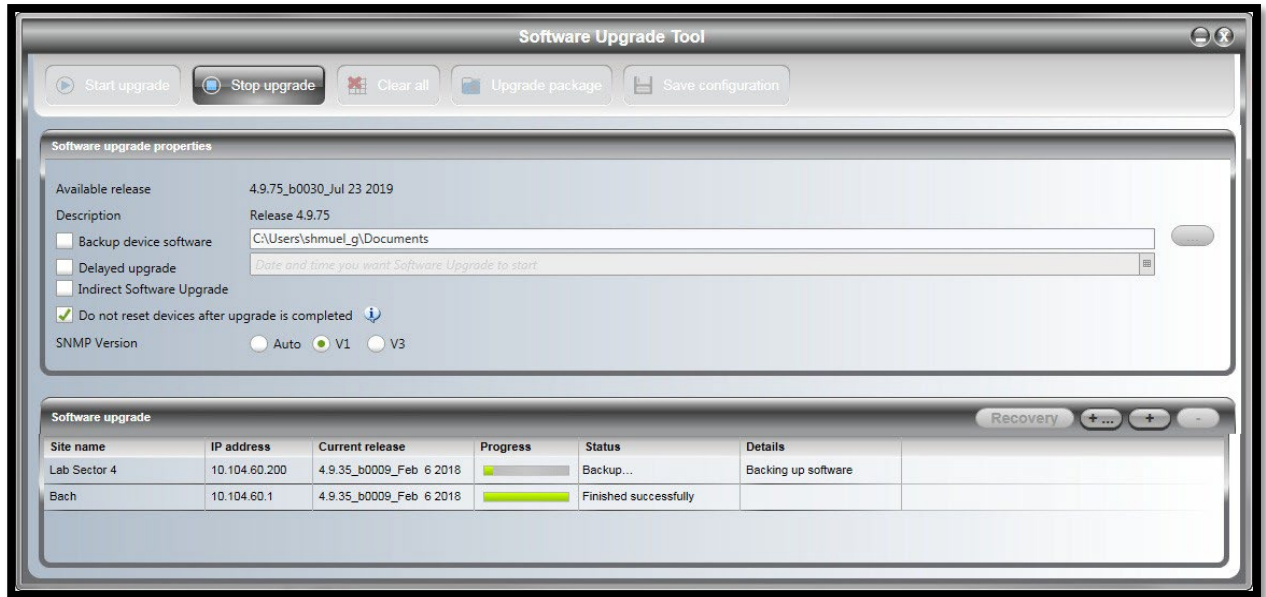


**Do not reset devices after upgrade** - this option instructs the R-Manager to not reset the HBS units after the upgrade is done. SU devices will be reset in any case.

After devices are added to the list using one of the methods above, the tool check for connectivity and lists current software release for all devices.

Once the list of devices is verified, click **Upgrade Package** to choose the SWU upgrade file.

Click **Start Upgrade** to commence the process. For an immediate upgrade you will be able to observe the upgrade progress from the green progress bars:



*Software upgrade in progress - Note the stop button*

Software upgrade					
Site name	IP address	Current release	Progress	Status	Detail
Bach@HBS.01	10.104.50.200	3.4.50_b3459_Mar 3 2013	<div style="width: 100%; height: 10px; background-color: #90EE90;"></div>	Reset done	
HFU.01.01	10.104.50.1	3.4.50_b3459_Mar 3 2013	<div style="width: 100%; height: 10px; background-color: #90EE90;"></div>	Reset done	
HNU.01.01	10.104.50.3	3.4.50_b3459_Mar 3 2013	<div style="width: 100%; height: 10px; background-color: #90EE90;"></div>	Reset done	
HFU.01.02	10.104.50.2	3.4.50_b3459_Mar 3 2013	<div style="width: 100%; height: 10px; background-color: #90EE90;"></div>	Reset done	

*Software upgrade completed successfully*

**Recovery:** If a unit has failed an upgrade, you can attempt an upgrade to a new software version, but with the factory default settings (except IP address).

Click the **Recovery** button () and follow the instructions on screen.

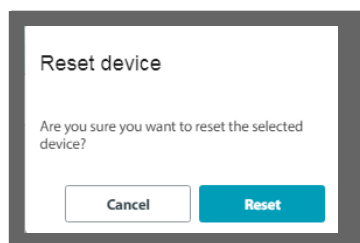
# Operations tools



This icon allows you to perform a reset, restore the factory default settings, or to enter a license for the selected device.

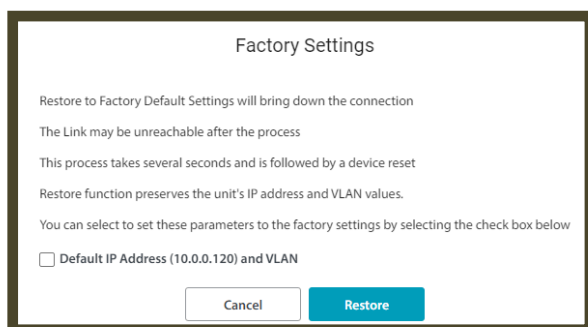
## Reset

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**.



## 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**.



## Licenses

The following features may be enabled, with the proper license:

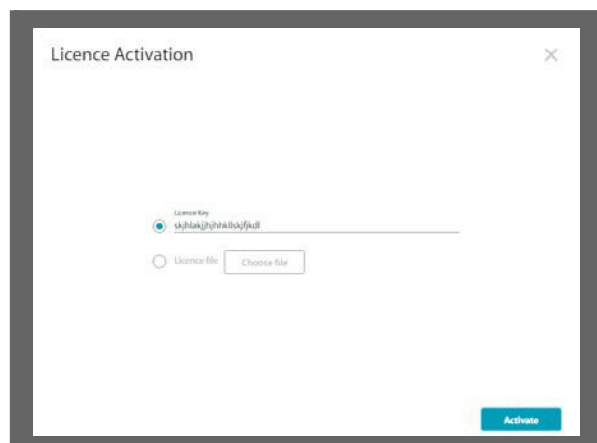
- Capacity - Throughput limit
- Max number of SUs supported by HBS
- Air interface Encryption (AES 256)

A license key is unique for each feature and a specific item of equipment.

For frequency band license please see [Change band](#) chapter.

To activate a license, you must first acquire a license key as described below:

1. Catalogue number: Contact your RADWIN representative and get a part number of the relevant license key. Purchase as many of these keys as you deem necessary.
2. You will receive a list of **License Keys** via email from RADWIN. A License Key can be used on any compatible RADWIN product; the link to a specific serial number is done in the activation stage.
3. Activate license keys.
  - a. Go to <https://tools.radwin.com/updates/LicenseKey/lk-radwin.htm>
  - b. Validate the compatibility of the license PN to a specific product (PN) or specific device (SN) in the License PN validation tab.
  - c. Open the License Activation tab. Fill in the details and submit. This will bind the license keys to serial numbers.
  - d. The License Key Application will then send you an email with a list of Activated licenses. These numbers *are* unique for the specific feature and specific item (SN) of equipment. We recommend saving this list as a text file in a secured location.
5. Select the device for which you want to apply a license.
6. Choose Operations -> License. The License Activation window will open.



7. Enter the license code in the field, or click **License file**, then **Choose file** to locate the license file.
8. Once you are ready, click **Activate**. Reset may be required to finish the process.



## Diagnostics tool

This creates diagnostic files to be used by RADWIN Professional Services and RADWIN Support.

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.

## User profile icon

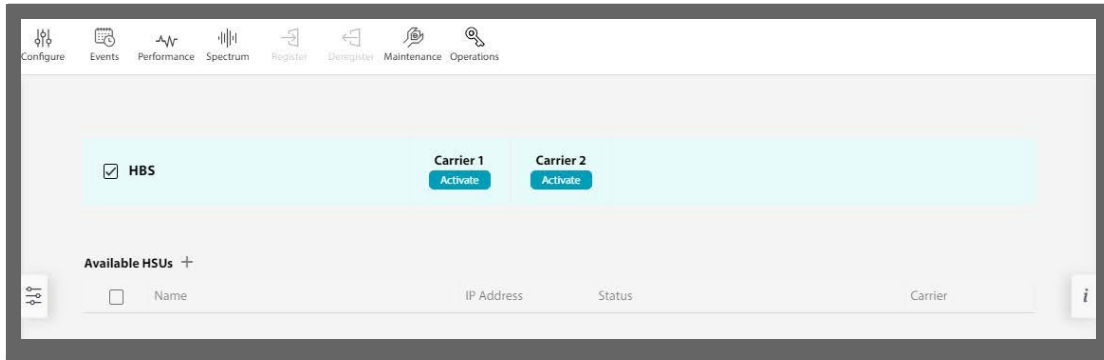


### **Admin, Observer, Operator, Installer**

The name of the user profile will appear on the icon. Click this icon to log out of the HBS.

# Carrier Panel

Near the top of the user interface, the status of the carriers is shown, together with the activation status of each Carrier.



To activate 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 ellipsis next to the Right Pane, then choose which Carrier you want to de-activate.

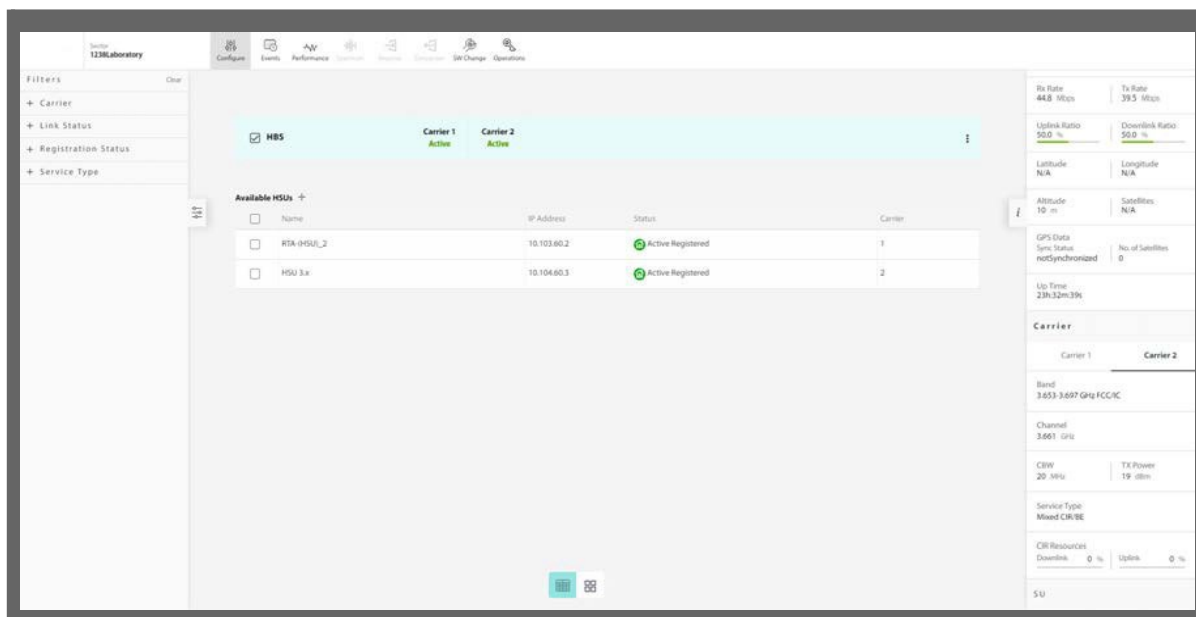




# SU List Panel

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).



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, seen when scrolling down on the list:

**Available HSUs +**

- Selection
- Name
- IP Address
- IPv6 Address
- Status
- Location
- RSS HBS [dBm]
- RSS HSU [dBm]
- RSS HBS Ant1 [dBm]
- RSS HSU Ant1 [dBm]
- RSS HBS Ant2 [dBm]
- RSS HSU Ant2 [dBm]
- Tput DL [Mbps]
- Tput UL [Mbps]

**Available HSUs +**

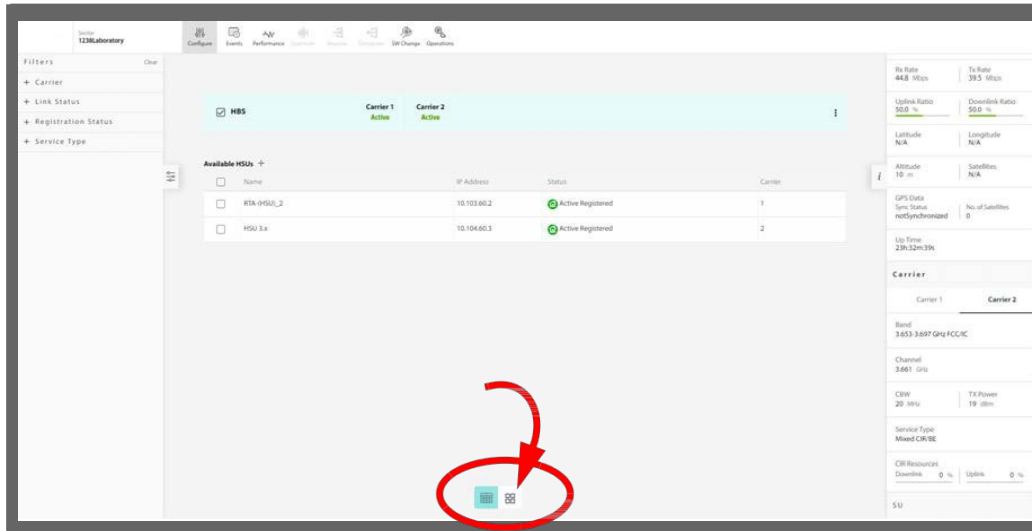
- Peak Tput DL [Mbps]
- Peak Tput UL [Mbps]
- Eth Rx Rate [Mbps]
- Eth Tx Rate [Mbps]
- Eth Rx Rate [Fps]
- Eth Tx Rate [Fps]
- Lan1 Rx Rate [Mbps]
- Lan1 Tx Rate [Mbps]
- Lan1 Rx Rate [Fps]
- Lan1 Tx Rate [Fps]
- Lan2 Rx Rate [Mbps]
- Lan2 Tx Rate [Mbps]
- Lan2 Rx Rate [Fps]
- Lan2 Tx Rate [Fps]
- Range [km]

- Range [km]
- Resources DL [%]
- Resources UL [%]
- Aggregate Capacity [Mbps]
- Rate HBS
- Rate SU
- ATPC Status
- Service Category
- Serial Number
- Modem MAC Address
- SW Version
- Resource Type
- Smart Antenna Azimuth [°]
- Level
- DL Util (%)
- UL Util (%)

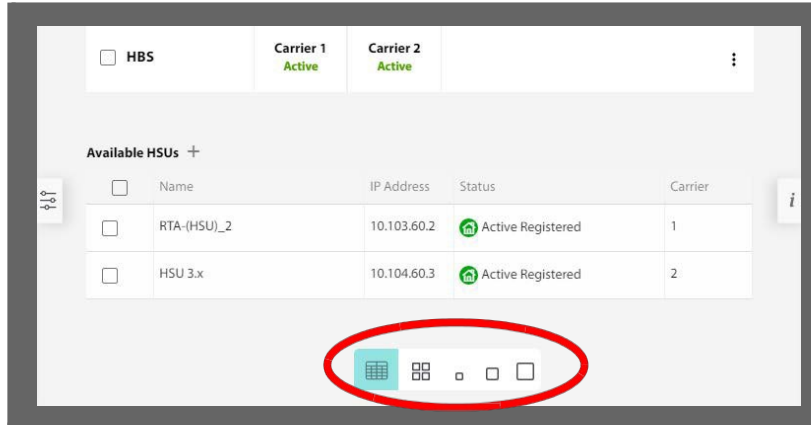
## SU List Views

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.



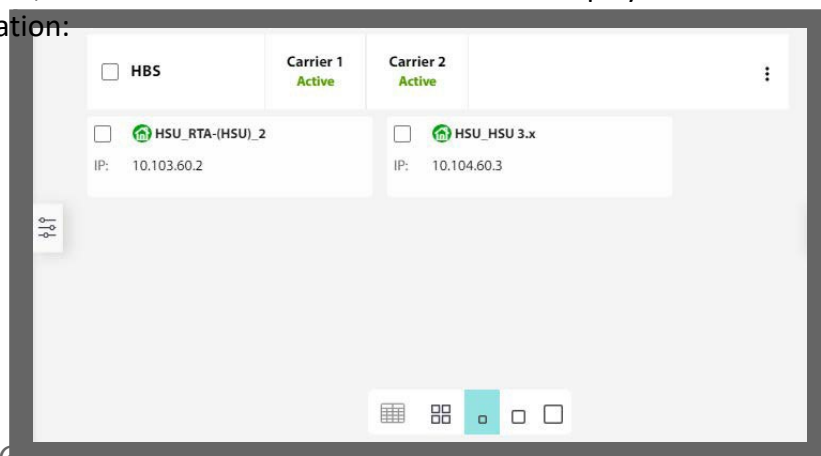
Various card size options will appear.



The size options are small, medium, and large.

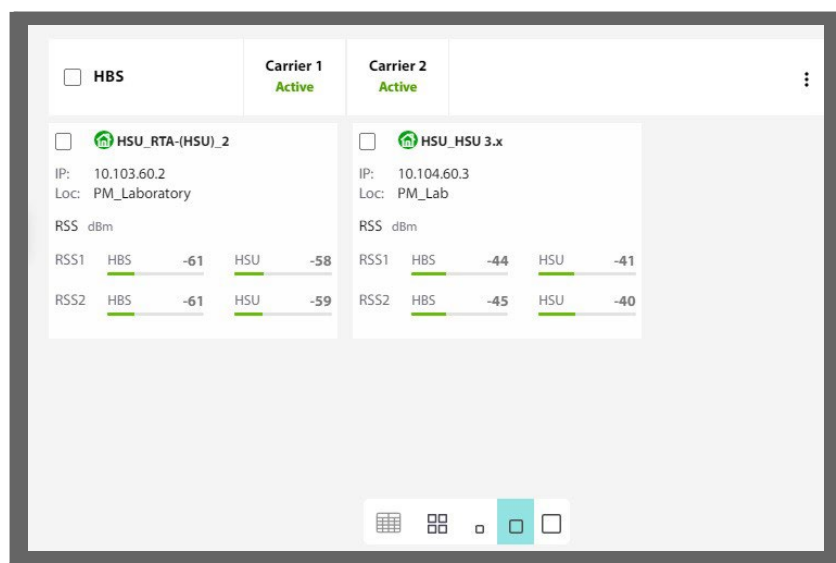
Click on the **small** card option, and the information for the SUs will be displayed in small cards with minimal information:

- Unit name, status
- IP address



Click on the **medium** card option, and the information for the SUs will be displayed in medium-sized cards with more information:

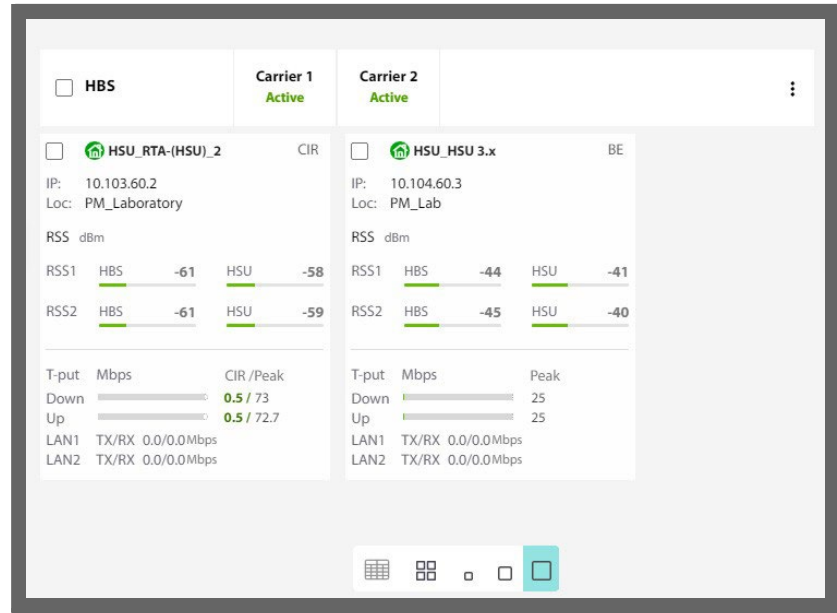
- Unit name, status
- IP address
- Location
- RSS per chain (RSS1 and RSS2), on both the HBS side and the SU side.



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.

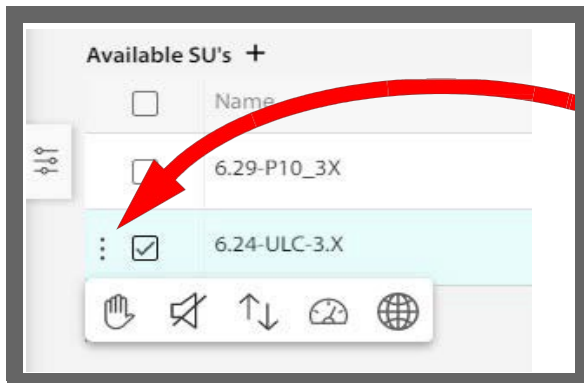
- Unit name, status
- Service category (CIR or BE) / Nomadic Level (if applicable)
- IP address
- Location
- RSS per chain (RSS1 and RSS2), on both the HBS side and the SU side
- Peak Throughput

- CIR Throughput
- Ethernet Tx/Rx traffic



## 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:

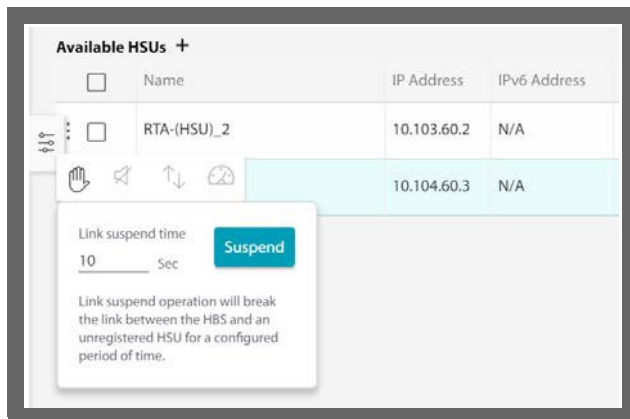
- [Suspend](#) an SU,
- Control the SU's [Buzzer](#) (if relevant for the specific model).
- [Replace](#) a defective SU with an operative SU, and transfer all configurations.
- Carry out a [Speed Test](#).
- Confirm service activation, if required by the RADIUS Authorization Server.

## Suspend

Suspends the selected subscriber from syncing with the current carrier for a specified 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:

- From the window that appears, select the amount of time for which you want to suspend the SU, then click **Suspend**.




The suspended SU will disappear from the SU list. After the time has elapsed, the SU will re- re-sync. When two carriers are active on the HBS, suspend can be used to switch the SU to the other carrier.

## 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.

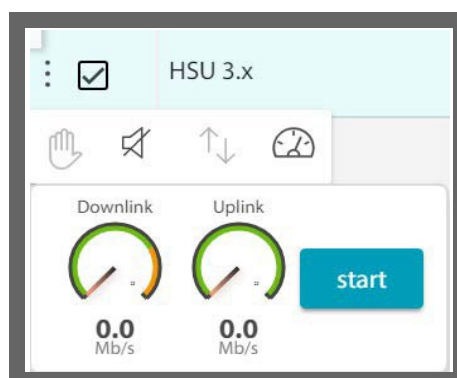
1. Click on the SU mini menu, then click on the Replace icon: 
2. You are offered a list of SUs available as replacements.
3. Select the required unit by clicking on it.
4. You are asked to confirm before proceeding, do so.
5. Once the unit was replaced successfully, a confirmation message will appear.  
Note that all of the configuration parameters from the replaced unit will appear in the new unit.

## Speed Test

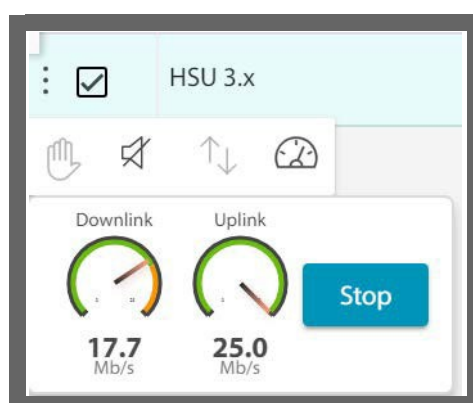
This graphically shows the real-time throughput in the downlink and uplink direction of the selected SU.

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.



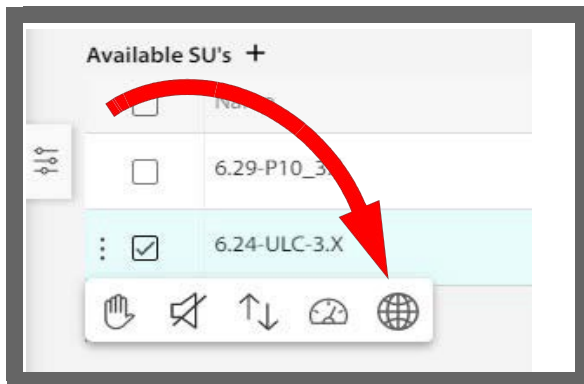
The Downlink and Uplink dials will show the speed in each direction.



3. Click **Stop** to stop the test.

## Confirm service activation

- If **Service Activation Confirmation Required** was enabled when configuring the RADIUS Authorization Server, select this to confirm the service activation.



## Information Panel

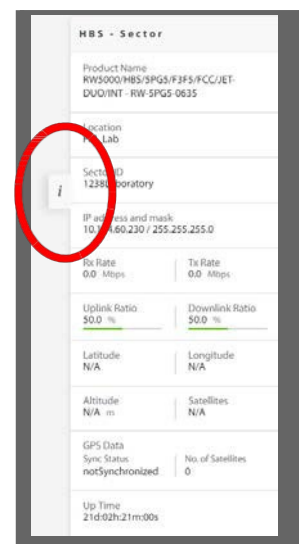
The info panel on the right pane of the user interface gives a brief overview of the sector, showing the following:

- 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 hide/restore the Info Panel, click on the minimize symbol:





# 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 and any other basic settings

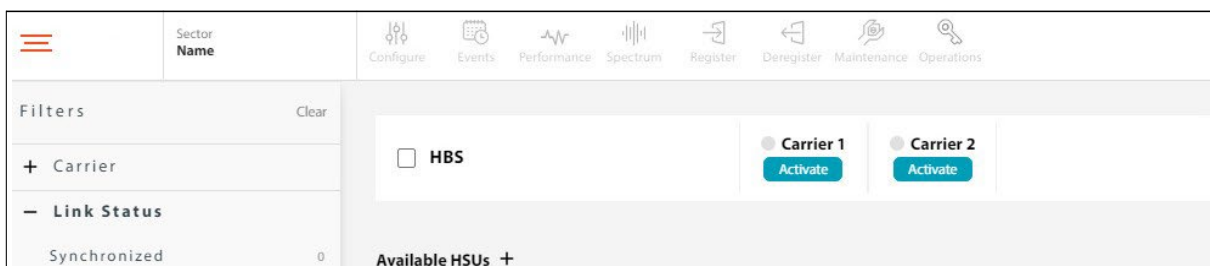
*Select operating band and activate the Base Station* - this must be done for each carrier

*Register Subscriber Units* - according to subscriber units which may have been installed

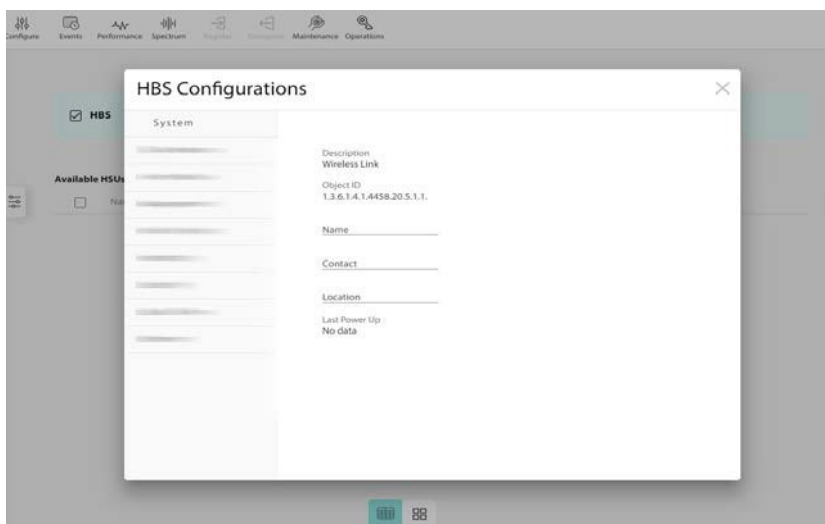
## Update Connection Parameters

When first logging on to a new base station, we recommend that you change its IP address in accordance with your network design.

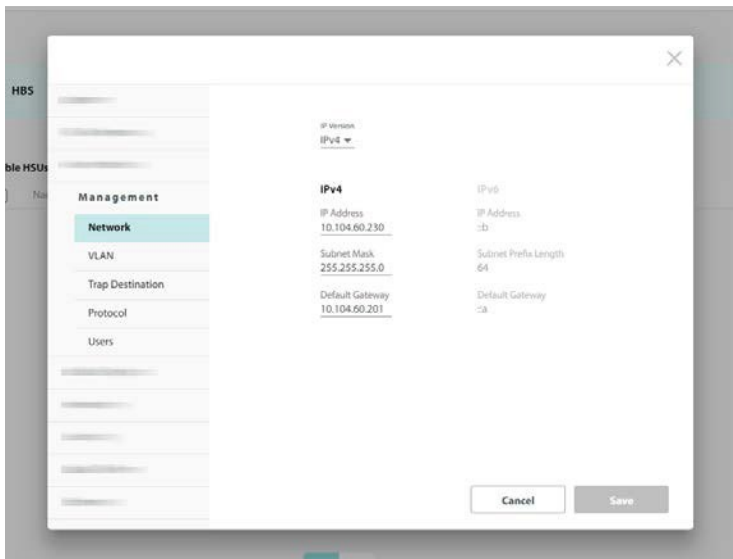
1. Connect the radio to the network and voltage via its PoE port.
2. Enter its IP address in a web browser (default value: 10.0.0.120).
3. Enter username **admin** and password **netwireless**.
4. Select the base station unit by placing a checkmark next to it, then click on **Configure**.



The **Configuration -> System** window will open.

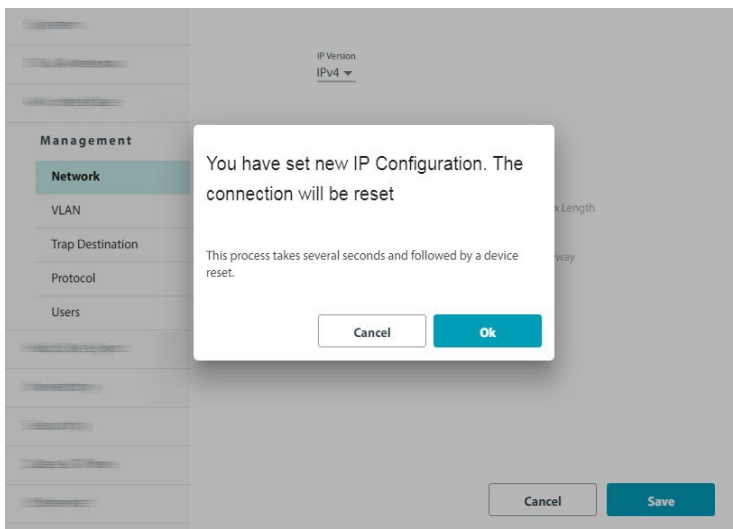


Select **Management** -> **Network**:



Enter the new IP address, Subnet Mask and Default Gateway in accordance with your network design, then click **Save**.

You will be warned that the device (HBS) will be reset. Click **OK**.



Once the HBS is reset, log in again using the new IP address.

## Select band and activate the carrier



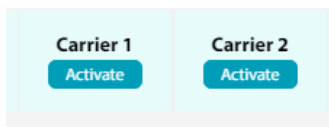
Note

For world-wide single PN products (Jet Air, Jet Air DUO), country and band 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 Uniform Single PN Products** for further information.

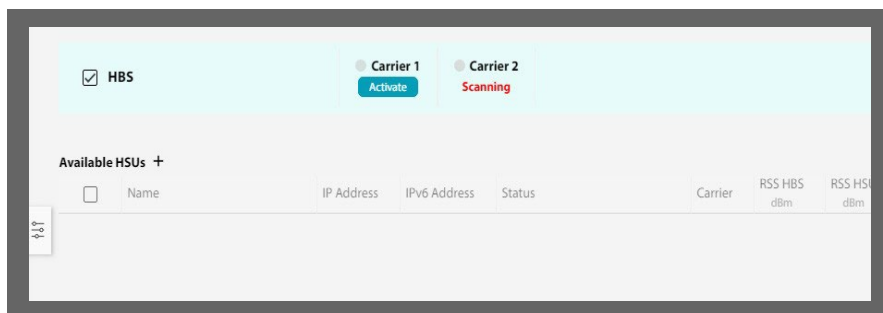
1. Click Activate button near the HBS menu



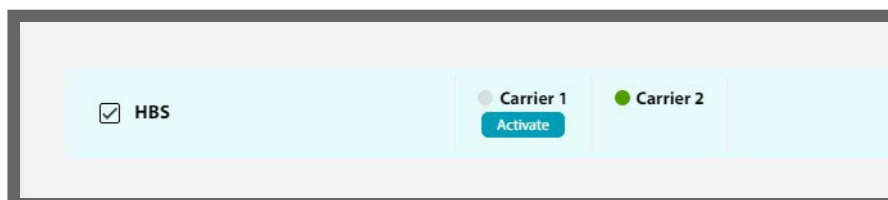
For a dual-carrier HBS, click **Activate** under **Carrier 1** or **Carrier 2**



2. Complete the Activation wizard by entering basic parameters. See [System](#) , [Air Interface](#) and [TX & Antenna](#) sections for details.
3. Click **Activate**.
4. In case of Automatic Channel Selection, the relevant Carrier will scan the channels



5. Once channel is selected, the carrier will be shown with a green bullet next to it, indicating that the carrier is Active.



6. Repeat the process for 2<sup>nd</sup> carrier if required.

Note that parameters that are common to both carriers will not appear when you run the activation wizard for the other carrier.

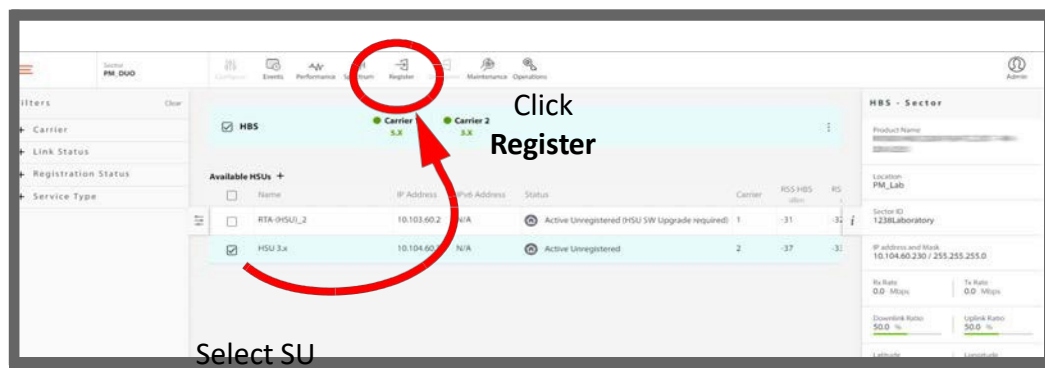
# Connect and Register Subscriber Units

1. Once SU installation and alignment is complete, it will be synchronized with the base station and will appear in the SU list as **Active Unregistered**

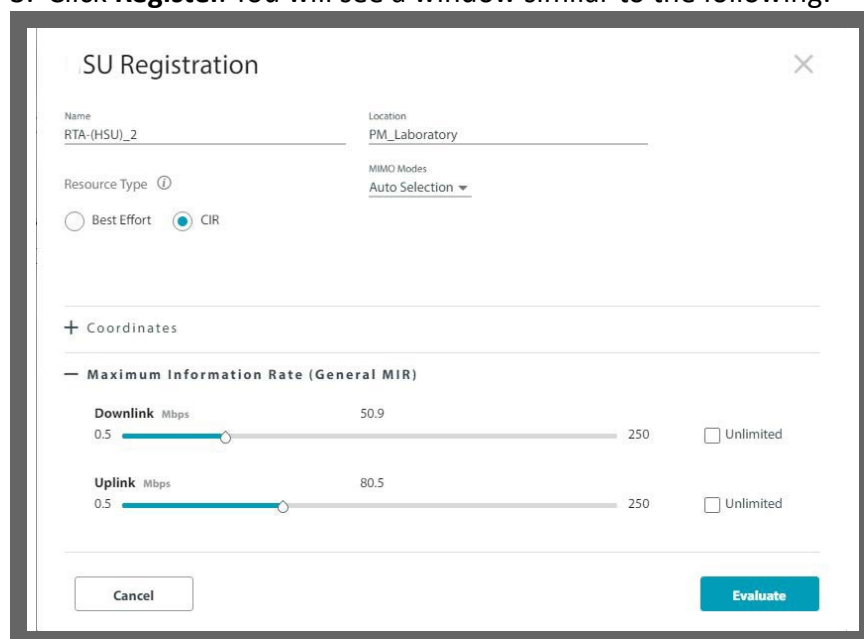


When working with dual-carrier 5 GHz base stations, since the carriers have the same Sector ID, the SU can sync to either Carrier 1 or Carrier 2. If the SU syncs to one carrier, and you wish it to sync to the other carrier, select "Suspend" for this unit, and select the time that this SU will be in suspend 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.

6. Select the SU you want to register by placing a checkmark next to it.

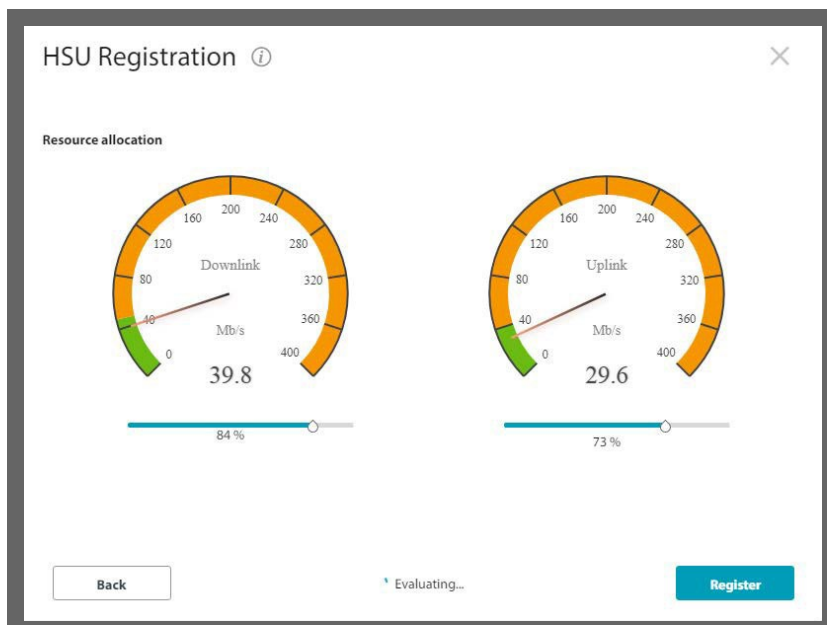


3. Click **Register**. You will see a window similar to the following:



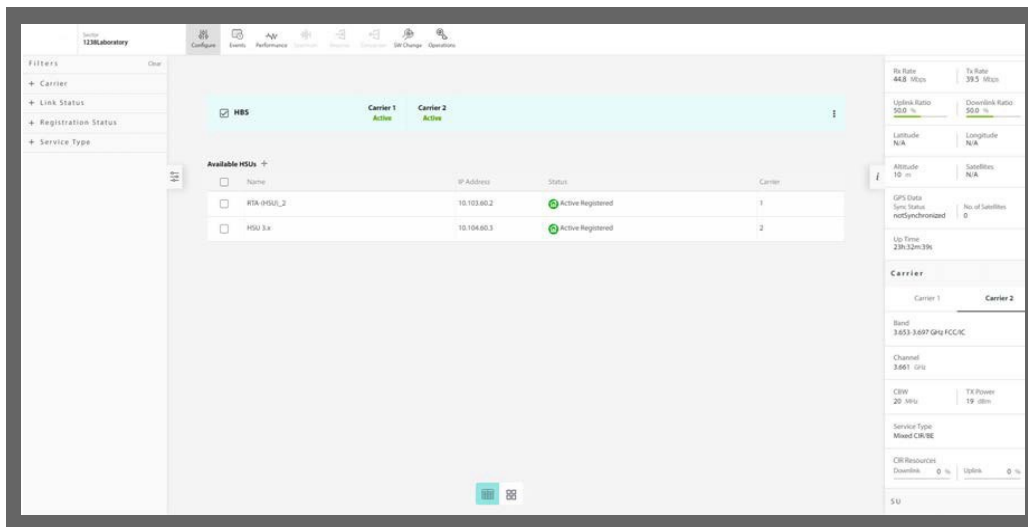
4. Enter the SU's Name and Location

5. Select the Resource Type for the SU.
  - **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 allocated to CIR traffic in the sector. Note that both the HBS and the SU must support CIR mode.
  
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 change the status to **Active Registered**.
8. If you chose the CIR resource type above, click **Evaluate** to set the resource allocation. Evaluation dials will appear. Use the sliders to choose the percentage of resources to be allocated to the SU. The dials will show Downlink and Uplink CIR throughput according to the resource allocation.



9. Once throughput is stable, the **Register** button will become enabled.

10. Click **Register** once the desired throughput is achieved.



11. The SU will be shown as **Active Registered**.

# Chapter 3: SU Management

## Scope of this Chapter

This chapter describes how to operate SU **PRO/AIR** units via SU web interface.

## Login

RADWIN recommends using Google Chrome browser. Other browsers may provide basic functionality, please contact RADWIN Support for details.

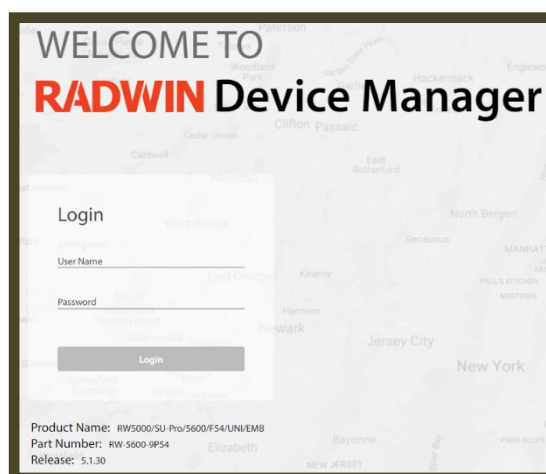
To access SU Web interface via Ethernet port:

- Make sure the SU is connected to the POE output of the POE unit
- Connect PC Ethernet interface to the LAN port of the POE unit
- Set a static IP according to SU network settings
- Default IP address for the SU via Ethernet is **10.0.0.120**

To access the SU Web interface via built-in WiFi AP (see [WiFi Interface](#) for details):

- Make sure the SU is connected to the POE output of the POE unit
- Connect to WIFI network with SSID = **R-[SU\_serial\_number]**
- Default WIFI password = **wireless**
- For mobile devices, you may have to confirm connection to a WIFI network without Internet access
- Your device will get a DHCP IP address
- Default IP for the SU via WIFI is **192.168.1.1**

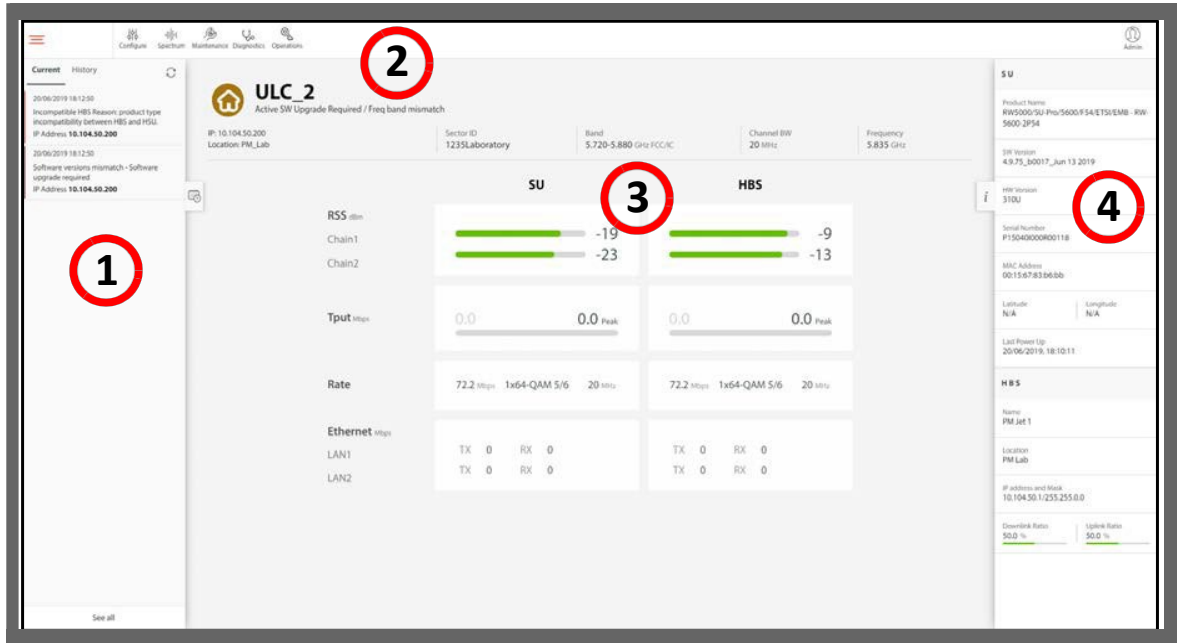
1. Enter the unit's IP address in a web browser URL. Login screen will appear:
2. Enter username and password  
Default credentials : **admin / netwireless**
3. Click **Login**





# WebUI Overview

The Web UI home page for the SU PRO/AIR series has the following layout:



Key elements of the WebUI are:

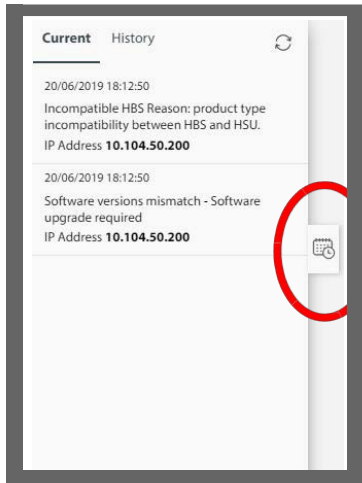
<b>1</b>	<i>Events Panel</i>	<b>2</b>	<i>Main icons</i>
<b>3</b>	<i>Link Dashboard</i>	<b>4</b>	<i>Info Panel</i>

# Event Panel

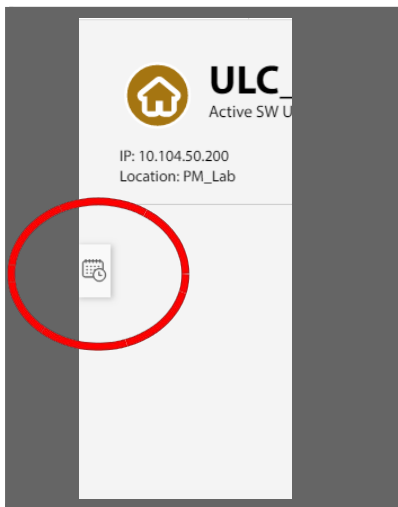
Here you can see the list of events.

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 events panel, click on the minimize symbol:

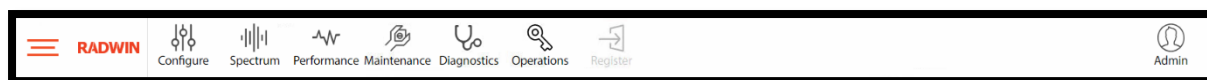



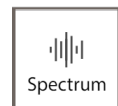



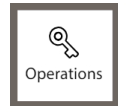
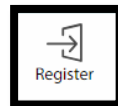

- To restore the panel, click on the minimize symbol again:



# Main icons

Along the top edge of the WebUI there are main icons.



	<b><u><a href="#">Configure</a></u></b>	Access unit configuration parameters
	<b><u><a href="#">Spectrum</a></u></b>	Spectrum view utility
	<b><u><a href="#">Performance</a></u></b>	Performance monitor utility
	<b><u><a href="#">Maintenance</a></u></b>	Back up, upgrade or restore the software
	<b><u><a href="#">Diagnostics</a></u></b>	Link monitor, ping and trace, speed test, diagnostics files, packet sniffing utilities
	<b><u><a href="#">Operations</a></u></b>	Reset, restore to factory default, add license, activate
	<b><u><a href="#">Register</a></u></b>	If the Self Register feature is enabled on the HBS, Register button will allow to register the SU.
	<b><u><a href="#">User Profile Icon</a></u></b>	Click this icon to log out of the unit.

# Configure menu

Access all parameters of the unit. Some parameters (such as inventory information) are read-only, some can be configured both directly from the SU, while others must be configured only from the HBS.

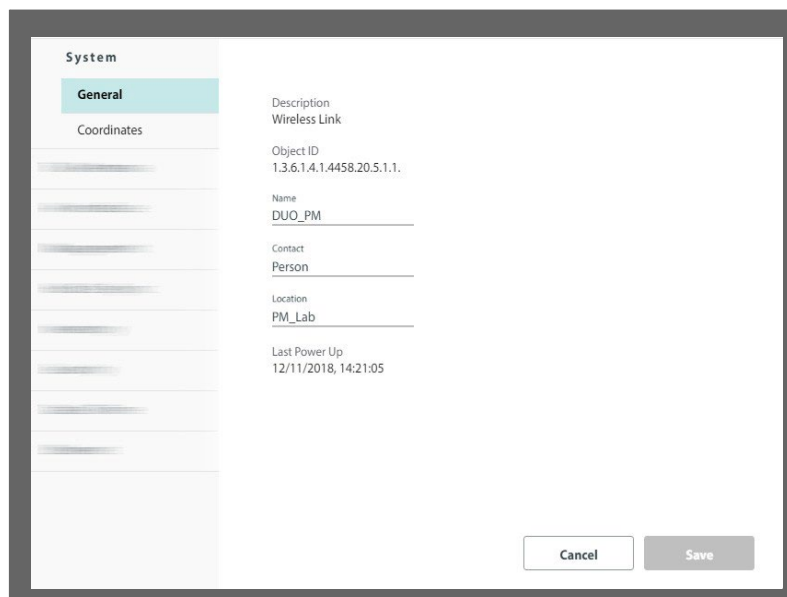
## System tab

### General

Available fields: **Description (read-only)**, **Object ID (read-only)**, **Name**, **Contact**, **Location**, and **Last Power Up (read-only)**.

Name and Location must be updated during registration.

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



The screenshot shows a web-based configuration interface for a system. On the left, there is a sidebar with a 'System' header and two tabs: 'General' (which is selected and highlighted in light blue) and 'Coordinates'. The main content area displays the following fields:

- 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

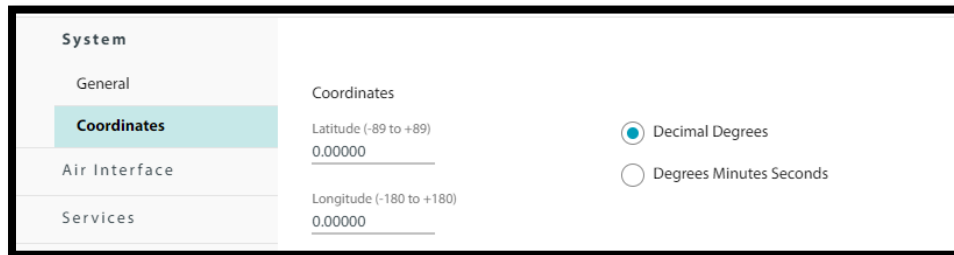
At the bottom right of the configuration area, there are two buttons: 'Cancel' and 'Save'.

## Coordinates

The coordinates (latitude and longitude) can be set in decimal degrees or degrees, minutes, and seconds.

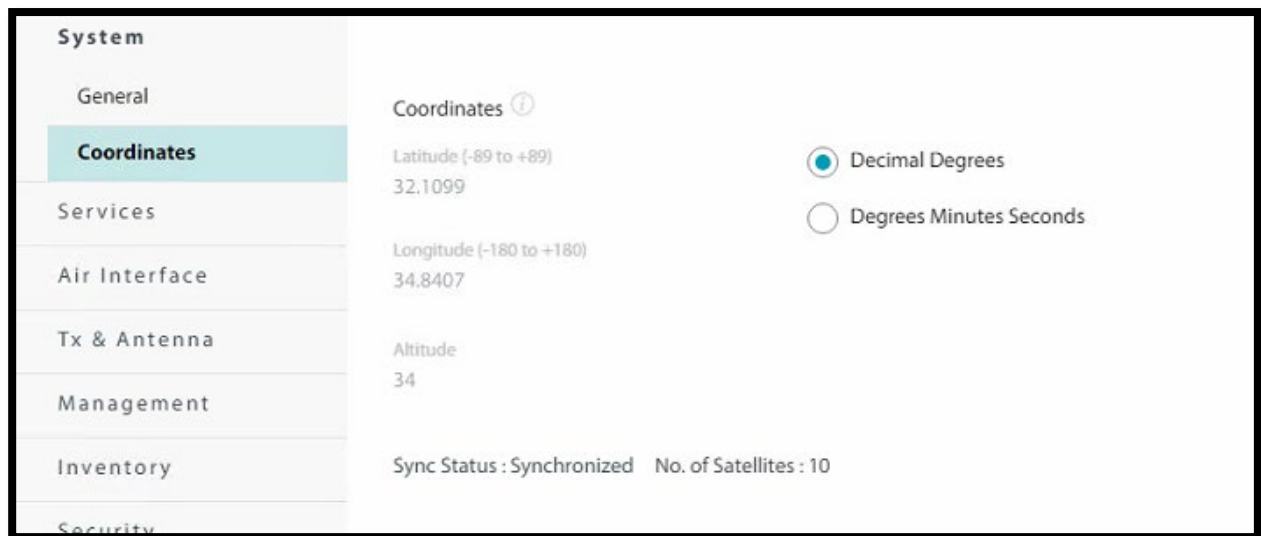
For subscriber units without a built-in GPS (such as SU-Air, SU-ECO and SU-Pro) the coordinates can be updated via Web UI.

Note: when using WINTouch+ mobile app for installation - coordinates are set based on the mobile device location data.



The screenshot shows the 'System' configuration page with the 'Coordinates' tab selected. The 'Coordinates' section is titled 'Coordinates' and contains two input fields: 'Latitude (-89 to +89)' with the value '0.00000' and 'Longitude (-180 to +180)' with the value '0.00000'. To the right of these fields are two radio buttons: 'Decimal Degrees' (which is selected) and 'Degrees Minutes Seconds'.

When using a GPS-enabled unit such as Alpha in SU mode, the coordinates are set by the GPS and are read-only. Altitude and GPS receiver status is also shown in this case:



The screenshot shows the 'System' configuration page with the 'Coordinates' tab selected. The 'Coordinates' section is titled 'Coordinates' and contains two input fields: 'Latitude (-89 to +89)' with the value '32.1099' and 'Longitude (-180 to +180)' with the value '34.8407'. To the right of these fields are two radio buttons: 'Decimal Degrees' (which is selected) and 'Degrees Minutes Seconds'. Below the input fields, the 'Altitude' is shown as '34'. At the bottom of the 'Coordinates' section, the 'Sync Status' is 'Synchronized' and the 'No. of Satellites' is '10'. The left sidebar shows the 'System' menu with 'Coordinates' selected.

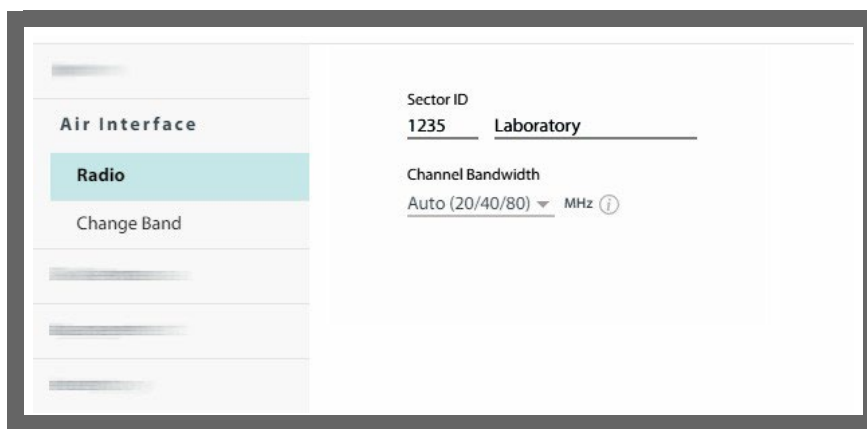
# Air Interface tab

## Radio

This tab has different settings for fixed or nomadic mode, and some settings are specific for 3.x GHz products.

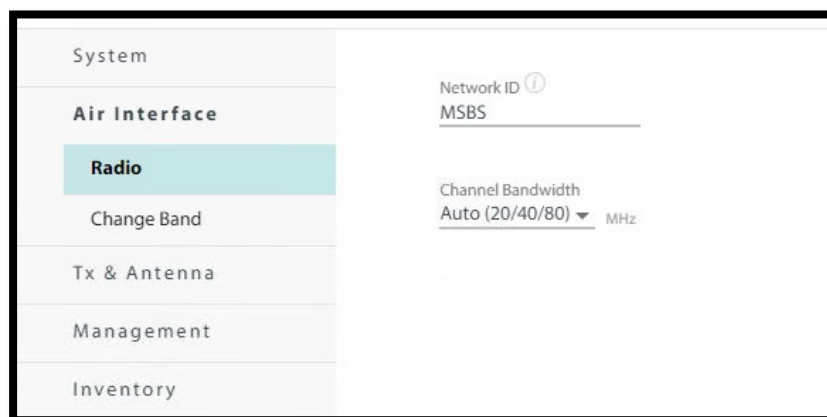
**Sector ID** (in fixed registration mode):

- Leave **empty** for the SU to be able to sync with any HBS it finds during scan
- Enter **Network ID** (4 first characters of the Sector ID) to restrict the SU to sync only with HBS units sharing the same Network ID
- Fill the complete **Sector ID** to restrict the SU to sync only with a specific HBS



**Network ID** (in nomadic registration mode):

- Enter Network ID – note it must match all the HBS units where the SU is supposed to register in nomadic mode



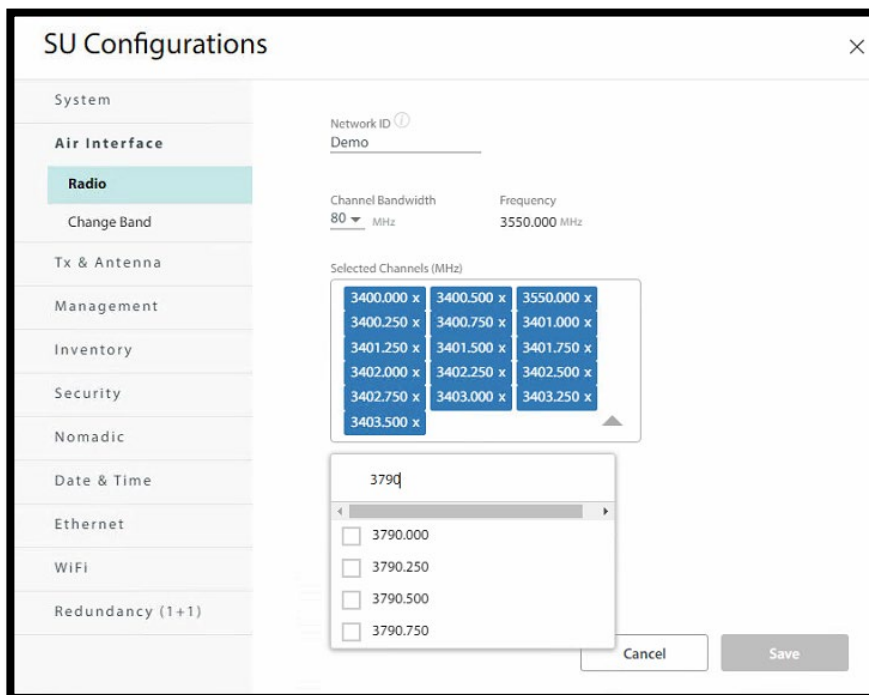
### Channel Bandwidth:

- Enter the channel bandwidth
- Selection options depend on product type:

	5.x GHz product	3.x GHz product
Channel bandwidth selection options	Auto (20/40/80 MHz) 10MHz	10MHz 20MHz 40MHz 80MHz

### Selected Channels (for 3.x GHz products):

- This setting exists only in 3.x GHz products, due to a high number of possible channels due to high resolution 250kHz channel step.
- Up to 16 channels can be selected for scanning.
- Numeric search is available – enter frequency value in MHz to find available channels.





## Change Band

Change Band operation on SU is only possible when there is no sync to a base station.

Subscriber units operating in 5.x Ghz bands, with SW release 5.1.10 and higher, will select the frequency band automatically to match the operating band of the base station.

For 3.x GHz frequency bands the band must be selected manually.



## Tx & Antenna tab

### Antenna Connection type:

- For SU Embedded models – select External or Integrated antenna according to the setup
- For SU Integrated models – read-only, Integrated antenna is selected
- For SU Connectorized models – read-only, External antenna is selected

### Antenna gain:

- For an integrated antenna – read-only value, shows the typical gain of the antenna for the current operating band and channel
- For an external antenna – antenna gain value must be set correctly by the installer

### Cable loss:

- For an integrated antenna – read-only value, fixed at 0
- For an external antenna – cable loss must be set correctly by the installer

**Required TX Power (Per radio):** by default this value is set to the maximum supported TX power, and can be adjusted within the range supported by the device.

**TX Power (Per radio):** current TX power per each radio chain, dynamic value which depends on:

- **Required TX Power** setting
- TX Rate / Modulation and Coding Scheme currently in use
- HBS ATPC settings (if ATPC is in use)
- **Antenna gain** and **Cable loss** (for bands which have a max EIRP limit set by regulation)

**TX Power (System)** = TX Power per radio + 3db)

**Max EIRP** = Max supported TX Power + 3db – Cable Loss + Antenna Gain

**EIRP** = TX Power (System) – Cable Loss + Antenna Gain

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

**Note:** changes may affect link quality

System	Antenna Connection Type:		
Air Interface	<input checked="" type="radio"/> External	<input type="radio"/> Integrated ⓘ	
<b>Tx &amp; Antenna</b>	Antenna Type Dual ▾	Antenna Gain 21.0 dBi	Beamwidth ⓘ Azimuth (0 to 359) ⓘ
Management			
Inventory			
Security	Tx Power (Per radio) 20 dBm	Tx Power (System) 23 dBm	Required Tx Power (Per radio) 20 dBm
Nomadic			
Date & Time			
Ethernet	Cable Loss 0.0 dB	Max EIRP 50 dBm	EIRP 44 dBm
WiFi			
Redundancy (1+1)			
			Cancel Save

# Management tab

## Network

IP address and management VLAN are applied to local or remote network access to the SU as part of the Ethernet network. These settings do not affect SU WiFi interface or over-the-air configuration via HBS UI.

### Configure management IP address

1. Choose IP stack operation mode (IPv4, IPv6, IPv4+IPv6).

**Note:** in case DHCP client mode is set by the HBS, IPv4 address will be acquired from DHCP server - see [Network \(SU via HBS only\)](#) for details

Field	IPv4	IPv6
IP Version	IPv4	
IP Address	10.103.151.23	::11.0.0.0
Subnet Mask	255.255.255.0	Subnet Prefix Length
		64
Default Gateway	10.103.151.201	Default Gateway
		::10.0.0.0

Vlan:  On

VLAN ID [2 - 4094]: 2

VLAN Priority [0 - 7]: 0

Buttons: Cancel, Save

Here, you can choose both, and enter the IPv6 addresses:

IP Version: IPv4 + IPv6

Field	IPv4	IPv6
IP Address	10.104.60.230	205:104:60:230
Subnet Mask	255.255.255.0	Subnet Prefix Length
		64
Default Gateway	10.104.60.201	Default Gateway
		205:104:60:201

Buttons: Cancel, Save

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**

VLAN tagging can be configured for SU management traffic.

To configure a VLAN for traffic, See [VLAN](#).

1. Check **On** in the VLAN checkbox.
2. Enter a **VLAN ID** between 2 and 4094.
3. Enter a **VLAN Priority** between 0 and 7.
4. Click **Save**.

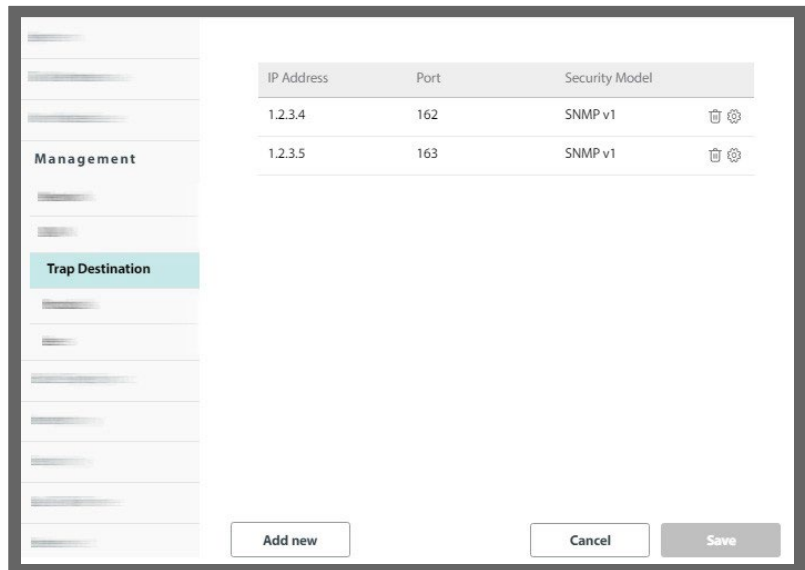
### **Lost or forgotten VLAN ID or IP Address (SU-Air/Pro/ECO)**

If the VLAN ID or IP address of the SU unit is forgotten, you can find the IP address using a sniffing tool such as Wireshark. During power-up sequence, SU sends a Gratuitous ARP packet via the Ethernet interface. Once such a packet is captured via a sniffing tool, management VLAN ID and source IP address can be discovered.

Another option is to access the unit via the WiFi interface (see [WiFi](#)) and view/modify any relevant settings in order to re-gain management access via LAN port.

## Trap Destinations

SNMP traps can be sent to up to 10 destinations, each of these can use SNMPv1 or SNMPv3.



### 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.

**New Trap Destination**

IP Address: 1.2.3.6      Port: 162

Security Model: SNMP v1

User Name:      Password:

Cancel      Save

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 (🗑️)
2. To edit a destination, click the configuration icon (⚙️)
3. 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.

The screenshot shows the 'Protocol' configuration page. On the left is a navigation menu with items: System, Air Interface, Tx & Antenna, Management, Network, VLAN, Trap Destination, Protocol (highlighted), Syslog Server, Users, Inventory, Security, Nomadic, Date & Time, and Ethernet. The main content area is divided into two sections: 'SNMP' and 'Web Interface'. In the 'SNMP' section, there are checkboxes for 'v1' (checked) and 'v3' (unchecked), and a dropdown menu for 'Authentication mode' set to 'MD5'. In the 'Web Interface' section, there are checkboxes for 'HTTP' (checked) and 'HTTPS' (checked), and a dropdown menu for 'Strict HTTPS' set to 'Disabled'. There are also checkboxes for 'Telnet' and 'SSH', both of which are unchecked. At the bottom right, there are 'Cancel' and 'Save' buttons.

### **SNMP**

- You may choose to enable SNMPv1, SNMPv3 or both.
- When configuring SNMPv3, you can leave the default authentication mode MD5 (message digest algorithm), or change it to SHA1 (secure hash algorithm).



For secure operation, as well as to be able to use some security-related features, SNMP protocol must be set to v3 only.

### **Web Interface**

- The unit can be configured for HTTP (port 80), HTTPS (port 443), or both.
- When HTTP is disabled, there are two options for Strict HTTPS mode:
  - Strict HTTPS Disabled: HTTP session will be redirected to HTTPS
  - Strict HTTPS Enabled (more secure): HTTP is fully disabled, user must explicitly set the browser to HTTPS to connect to the radio
- An admin user must be logged in with HTTPS to make changes in users.



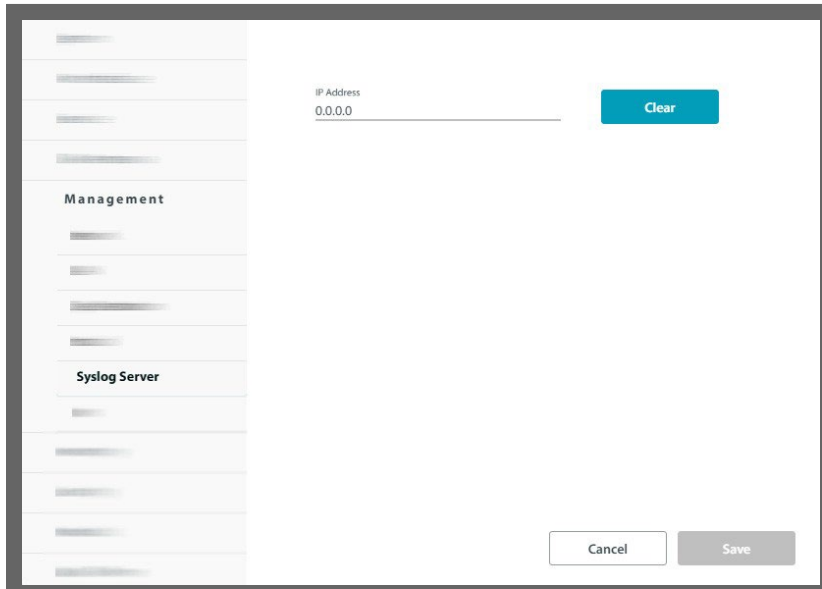
For secure operation, as well as to be able to use some security-related features, HTTP must be disabled.

### **SSH**

- Command Line Interface via SSH CLI (port 22) can be enabled or disabled
  - For a list of supported CLI commands, See [Appendix C](#)
- Once you are finished, click **Save** to have any changes take effect.

## Syslog Server

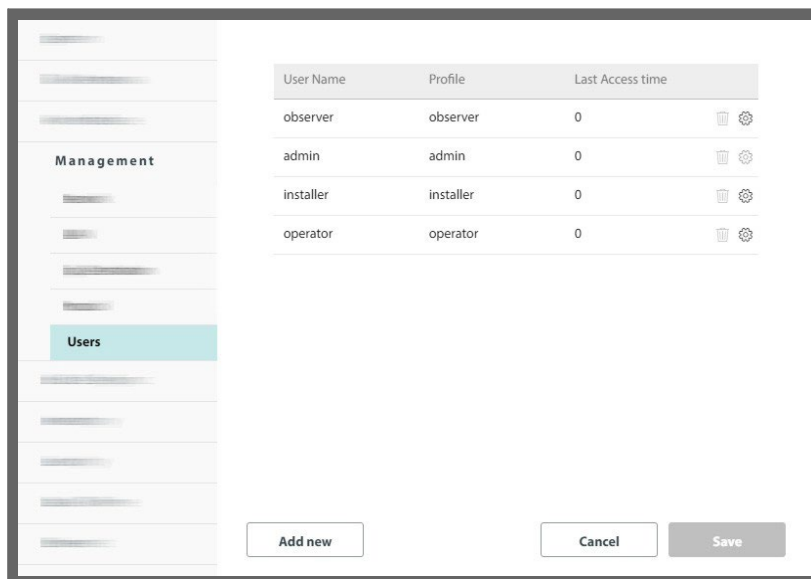
This field shows the IP address of a Syslog server to which the radio unit sends Syslog messages.



- Enter the IP address of the Syslog server and click **Save**.

## 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.





Possible user profiles are as follows:

Profile	Default Password	Function
<b>observer</b>	netobserver	Read Only
<b>operator</b>	netpublic	Can install and configure the sector, but cannot change the operating frequency or regulation.
<b>installer</b>	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.
<b>admin</b>	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.



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.


The screenshot shows a 'New User' dialog box with the following elements:

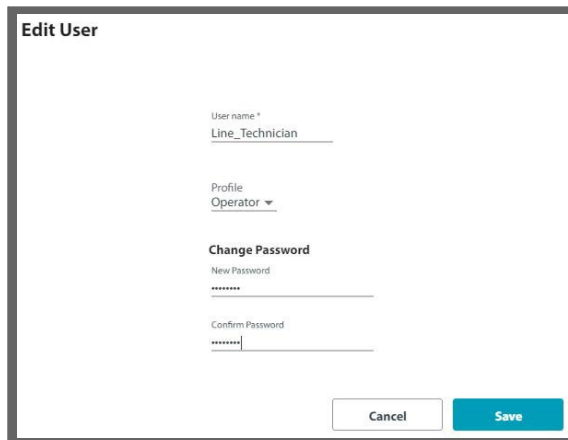
- User name \***: A text input field.
- Profile**: A dropdown menu currently showing 'Operator'.
- Change Password**: A section header.
- New Password**: A text input field.
- Confirm Password**: A text input field.
- Buttons**: 'Cancel' and 'Save' buttons at the bottom right.

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.



1. Change the name, if needed.
2. Change the profile, if needed.
3. Set the password for this user and confirm it.
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.

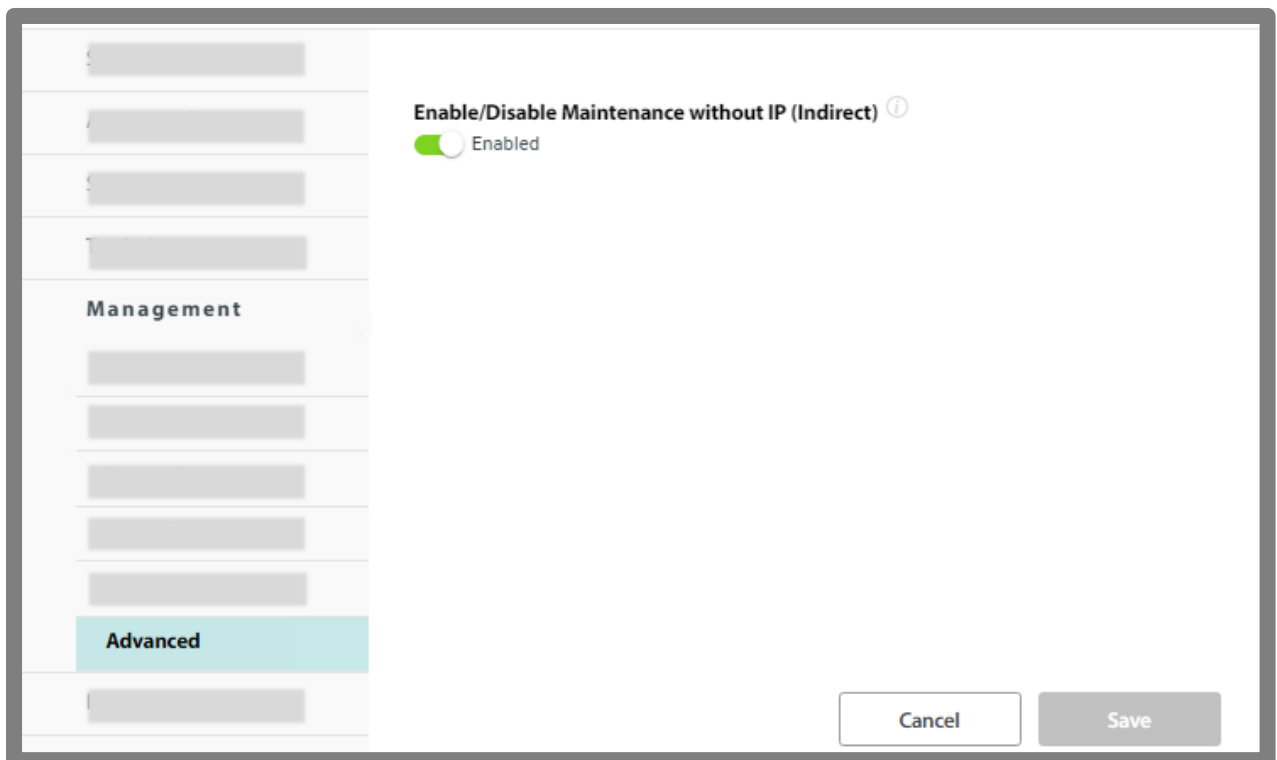
# Advanced

## Enable / Disable maintenance without IP (indirect)

By default, it is possible to perform **Indirect upgrade, backup or restore** (see [HBS configuration - Maintenance](#)) on SUs connected to an HBS, even if there is no network connectivity to SU management IP. To allow this, IP Forwarding is enabled by default on local IP management interfaces of the SU.

We recommend using a dedicated management VLAN to separate customer traffic from the SU management interface. However, in some cases network security hardening policy may require disabling IP Forwarding on all IP interfaces which are not intended to act as a router for customer traffic.

Use the toggle switch below to disable IP forwarding.



# Inventory tab

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.

HW model type special edition CBW for SUs with special hardware that don't support CBW of 10Mhz.



# Security tab

The Security dialog enables you to change the SNMP Community strings, set the Security Mode or change the current user's password.

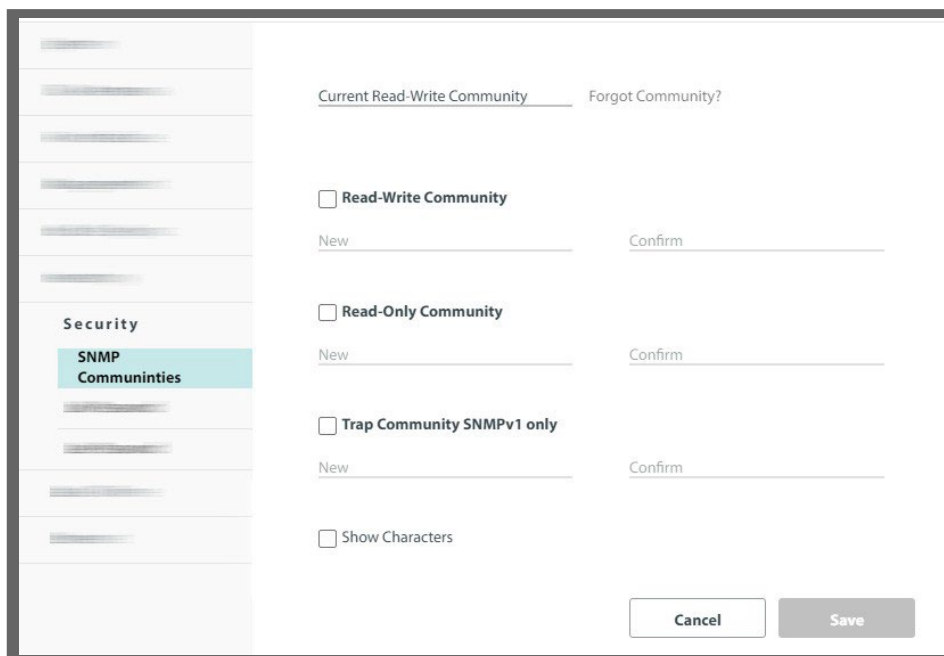
## SNMP Communities

Following SNMPv1 communities are supported:

- Read-only community for polling information from the radio unit
- Read-write community to configure and control the radio unit
- Trap community for traps

### 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

Security Mode controls the usage of Alternative Key which is a unique encrypted password designed as a recovery solution for cases when Link password or Admin user password are changed from the default settings, and then lost / forgotten. Alternative Key is supplied in the package with each RADWIN device, and can also be obtained by opening a support case.

Available options are:

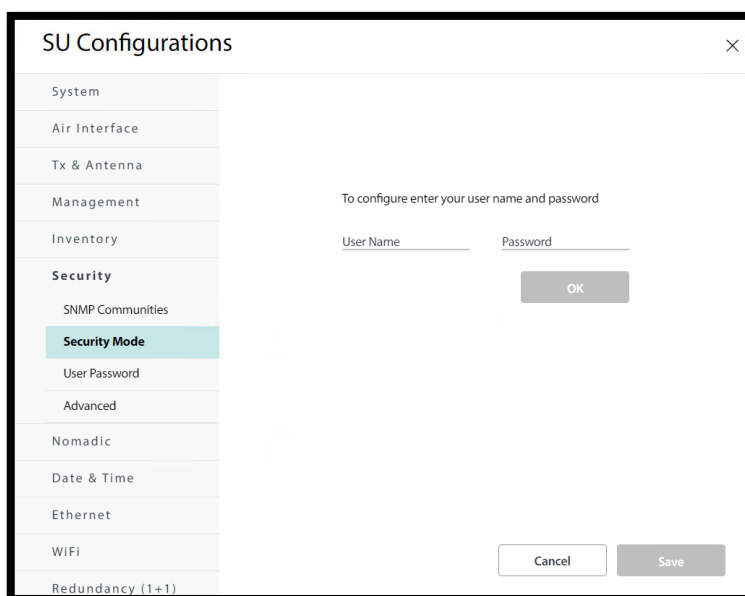
**Secured (default):** Alternative Key can always be used

**Enhanced Security\*:** Alternative key can be used only for 2 minutes after reset

**Enhanced Security:** Alternative key cannot be used. If user password is lost, the radio will have to be shipped for recovery via RMA procedure. Use only in high security environment to mitigate a concern for Alternative Key being used to gain unauthorized access to the SU.

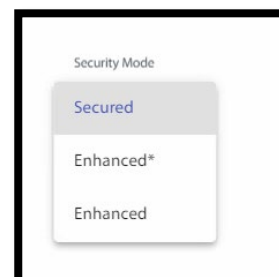
Configure this mode as follows:

1. Make sure only SNMPv3 is allowed and HTTPs is enabled (see [Protocol](#))
2. Log in via HTTPs
3. Select **Configuration -> Security -> Security Mode**.



The screenshot shows the 'SU Configurations' web interface. On the left is a navigation menu with categories: System, Air Interface, Tx & Antenna, Management, Inventory, Security, SNMP Communities, Security Mode (highlighted), User Password, Advanced, Nomadic, Date & Time, Ethernet, WiFi, and Redundancy (1+1). The main content area is titled 'To configure enter your user name and password' and contains two input fields: 'User Name' and 'Password', followed by an 'OK' button. At the bottom of the main area are 'Cancel' and 'Save' buttons.

4. Enter your username and password and click **OK**.
5. Select the required security mode
6. Click **Save**.

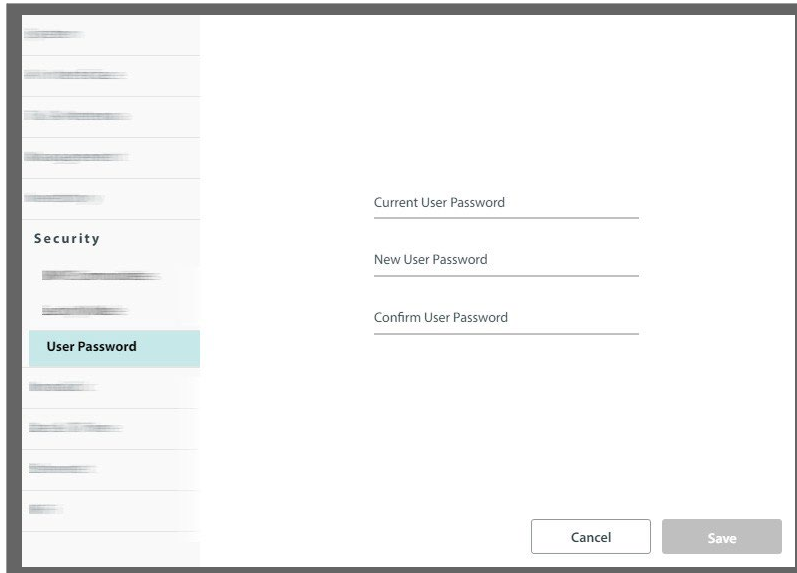


The screenshot shows a dropdown menu for 'Security Mode'. The options are: 'Secured' (highlighted in blue), 'Enhanced\*', and 'Enhanced'.

## User Password

To change the user password of the present user:

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



The screenshot shows a web application interface with a sidebar on the left and a main content area. The sidebar has a 'Security' section with a 'User Password' option highlighted in blue. The main content area contains three input fields labeled 'Current User Password', 'New User Password', and 'Confirm User Password'. At the bottom right of the dialog box, there are two buttons: 'Cancel' and 'Save'.

2. Enter the current password.
3. Enter the new password.
4. Confirm the new password.
5. Click **Save**.



## Nomadic tab

**Note** – Nomadic is not supported by SU-Air and SU-ECO models.

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.



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<sup>1</sup>:

---

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.

**Note - for 3.x GHz units only:** list of channels to scan must be set when operating in Nomadic mode (see [Radio](#))

# Date & Time tab

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.



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. 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.
2. To set the time based on the time of the managing computer, click **Use Computer Time**.
3. To set up NTP server as a time source:
  - c. Enter **NTP server** IP address
  - d. Set **Offset** value in minutes as per your timezone relative to UTC / GMT.
4. Click Save to have your changes take effect.

The screenshot shows a configuration window with the following elements:

- NTP Server** section:
  - NTP Server: 0.0.0.0
  - Offset: 0
- Date & Time** section:
  - Date: 11/22/2018 (with a calendar icon)
  - Time: 01:58 PM
  - Use Computer Time button
- Bottom buttons: Cancel and Save

# Ethernet tab

In this tab, you can configure port settings and firewall settings.

## LAN Ports

- **Current:** shows the current status, speed and duplex of the Ethernet port
- **Mode:** speed/duplex configuration of the Ethernet port
  - **Auto Detect:** auto-negotiate duplex and speed up to 1000 Mbps  
This is the default and recommended setting
  - **Auto Detect (100Mbps):** auto-negotiate duplex and speed, limited to 100 Mbps  
This setting can be useful to provide a more robust Ethernet link and solve CRC error issues due to cable quality issues, in case 100Mbps LAN speed is good enough.
  - **Manual modes - 10Mbps Half Duplex / 10Mbps Full Duplex / 100Mbps Half Duplex / 100Mbps Full Duplex**  
Manual speed/duplex can be used when connected Ethernet equipment does not support auto-negotiation, or if auto-negotiation must be disabled by design.
- **CRC Errors** - Shows how many CRC errors occurred since the last reset.

## SU Configurations



System	
Air Interface	
Tx & Antenna	
Management	
Inventory	
Security	
Nomadic	
Date & Time	
<b>Ethernet</b>	
<b>LAN Ports</b>	
Firewall	
WiFi	
Redundancy (1+1)	

LAN1		Current	Mode	CRC Errors	Main Data Path
		1Gbps/Full Duplex	Auto Detect	0	↻
Max MTU size	9216 Byte		<ul style="list-style-type: none"><li>10Mbps/Half Duplex</li><li>10Mbps/Full Duplex</li><li>100Mbps/Half Duplex</li><li>100Mbps/Full Duplex</li><li><b>Auto Detect</b></li><li>Auto (100 Mbps)</li></ul>		

Cancel Save

## Firewall (SU only)


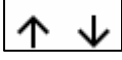

Starting from release 5.1.53, bridge mode firewall is added to SU AIR, SU PRO and Alpha.

This functionality enables packet filtering according to defined rules.

Configuration guidelines:

1. Enable the feature via **Firewall** on/off button.
2. Click **Add** to create a new firewall rule.
3. Each rule contains a set of parameters and required action.
  - a. **Name:** enter a descriptive name for the rule
  - b. **Enabled:** Displays the status of the firewall rule. All the firewall rules are saved in the system configuration file; however, only the enabled firewall rules are active on the device.
  - c. **Action:** select the required action for packets which match all the conditions in the rule.
    - i. **Accept:** allow such packets to pass through the firewall unmodified.
    - ii. **Drop:** block such packets.
  - d. **VLAN ID:** specify the VLAN ID
  - e. **Input -> Output:** traffic direction:
    - i. LAN -> WAN: uplink direction from Ethernet to Wireless
    - ii. WAN -> LAN: downlink direction from Wireless to Ethernet
  - f. **IP Type:** select Layer 3 protocol: IP, ICMP, TCP, UDP
  - g. **Source IP/Mask:** specify source IP address and CIDR mask (can be IPv4 or IPv6).  
For example, enter 192.168.1.0/24 for source IP address in the range of 192.168.1.0 to 192.168.1.255
  - h. **Destination IP/Mask:** specify destination IP address and CIDR mask (IPv4 or IPv6).
  - i. **Source Port:** Specify Layer 4 source port of the packet (enter 0 for “any port”)
  - j. **Destination Port:** Specify Layer 4 destination port of the packet (enter 0 for “any port”)

**Edit a rule**– Click on 3-point menu icon on the left side of each rule entry

-  Edit a rule entry.
-  Move the rule entry up or down to reorder.
-  Remove a firewall rule entry.

**Download / Upload CSV**- Can be used to backup and document and replication of firewall rules from a single “master” SU to other SUs

- **Download CSV:** export rules to a CSV file
- **Upload CSV:** import rules from a CSV file

### SU Configurations

- System
- Air Interface
- Tx & Antenna
- Management
- Inventory
- Security
- Nomadic
- Date & Time
- Ethernet**
  - LAN Ports
  - Firewall**
  - WiFi
  - Redundancy (1+1)

Firewall Download CSV Upload CSV

#	Name	Enabled Vlan ID	Input-> Output	Action IP Type	Source IP/Mask	Destination IP/Mask
1	Block UDP	Yes 0	LAN-> WAN	Drop UDP	0.0.0.0/32 Port: 0	0.0.0.0/32 Port: 0

🗑️ ✎ ⬆️ ⬇️

Add new Cancel Save

#### Firewall Rule - Block UDP

Name: Block UDP      Vlan ID: 0

Enabled: Yes      Input -> Output: LAN->WAN

Action: Drop      IP Type: UDP

Source IP/Mask: 0.0.0.0/32      Source Port: 0

Destination IP/Mask: 0.0.0.0/32      Destination Port: 0

Cancel Update

## WiFi interface tab

#	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

**SSID** for the WiFi AP: the format is **R-[serial number of unit]**

### 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

### Password

- WPA2 password (default: **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:

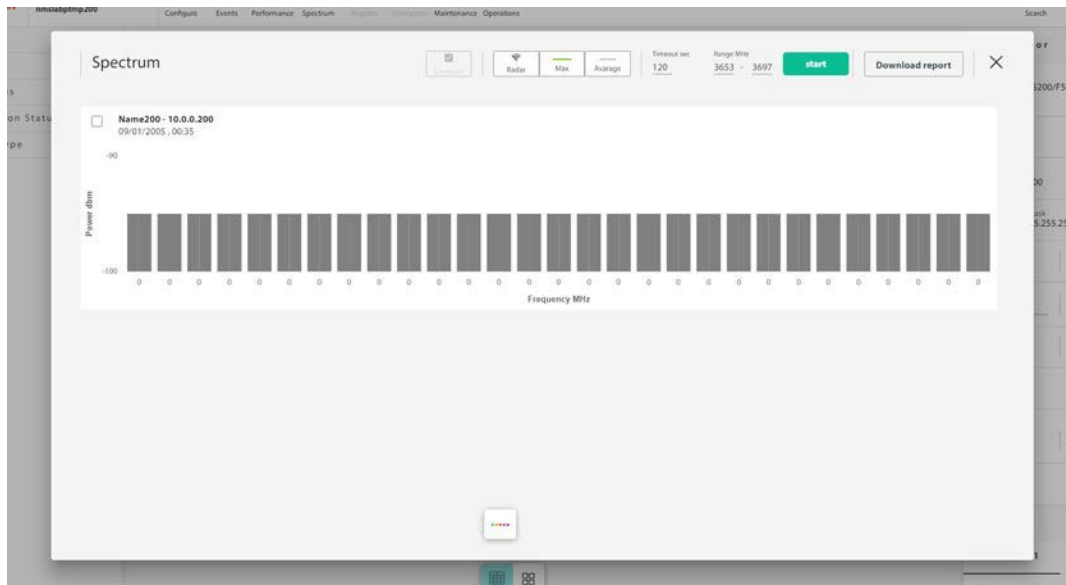
- Up to 5 clients can be connected
  - The list shows MAC addresses and signal strength (RSSI) of the connected devices
- Click **Save** to have your changes take effect.

# Spectrum scan



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.

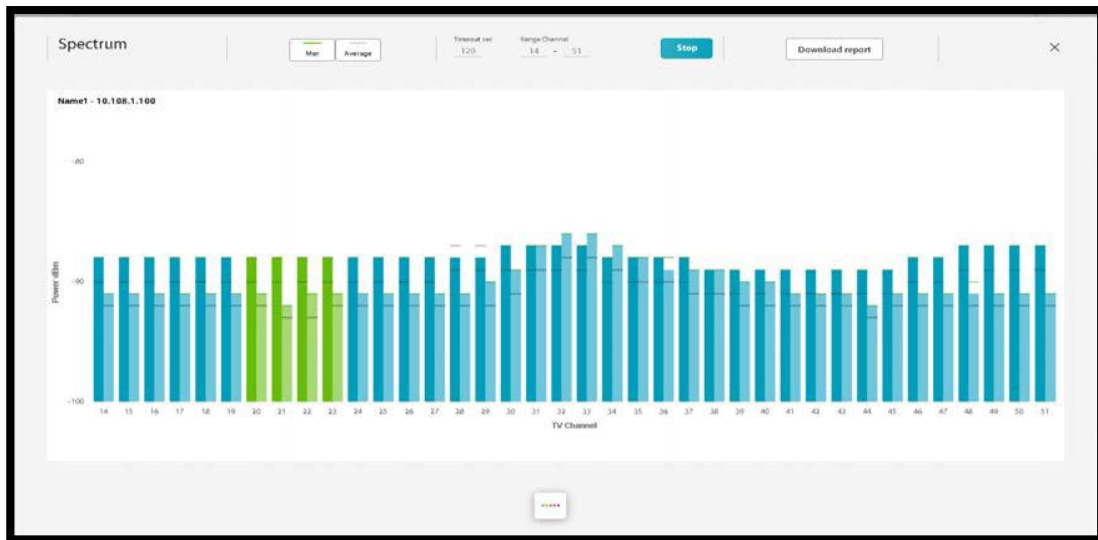
1. Click on the Spectrum View icon  . The Spectrum View window will appear.



A blank Spectrum View result display will appear.

2. Select **Scanning duration** (available values are: 1/2/5/10/15/30/60 minutes)
3. Select the frequency range (**Range MHz**, top of window). You can scan a range spanning of up to 495MHz per scan.
4. Once you are ready, click **Start** to start the scan. You will be warned that this is traffic-affecting. If this is acceptable, click **Yes**.





- 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.

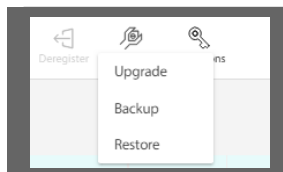


## Maintenance tools

This menu allows you to upgrade the target unit's software, as well as backup or restore software and configuration.

**Note:** Maintenance operations are not available in the first 3 minutes after bootup / reset.

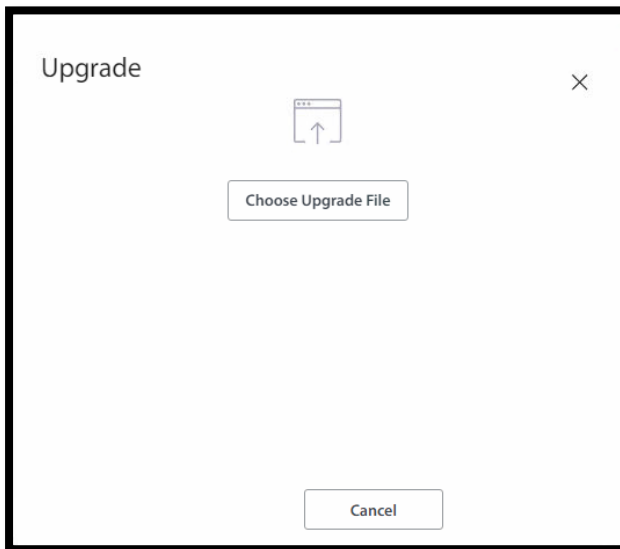
Press **Maintenance**, then choose the required action from the pull-down menu.



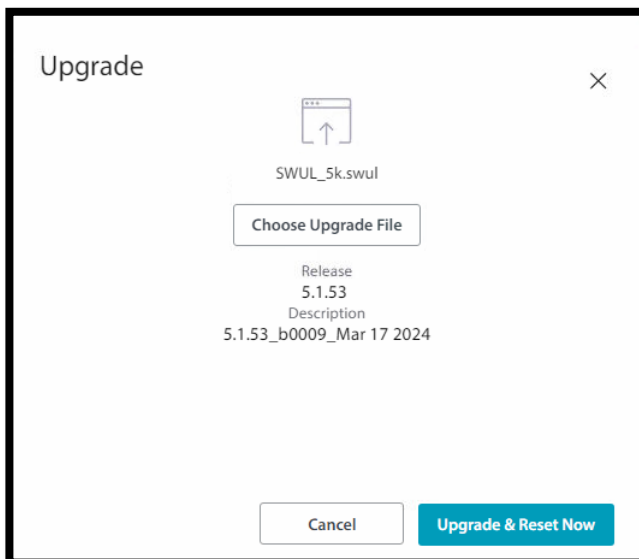
## Upgrade

To perform a SW upgrade on an SU device:

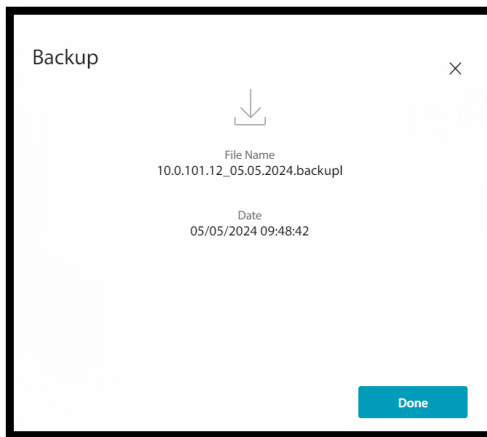
1. Download SWUL software upgrade file from Radwin Partner Portal Support section.
2. Select **Upgrade** in **Maintenance tools**
3. Press **Choose Upgrade File** to select the SWUL file from your PC for upload



4. Upload will start, showing a progress bar.
5. Once upload is done – upgrade file will be validated and release version will be shown



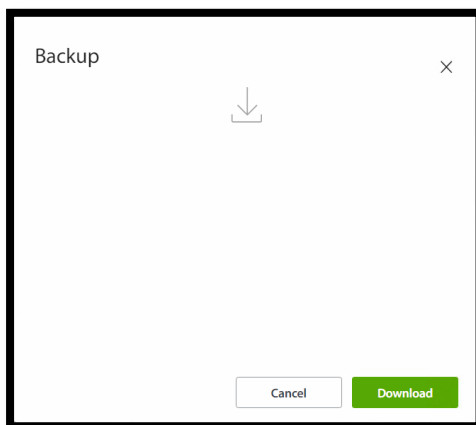
6. If the release version is correct - press **Upgrade & Reset Now** to start the upgrade. Otherwise – either select **Choose Upgrade File** to upload another file, or press **Cancel**.



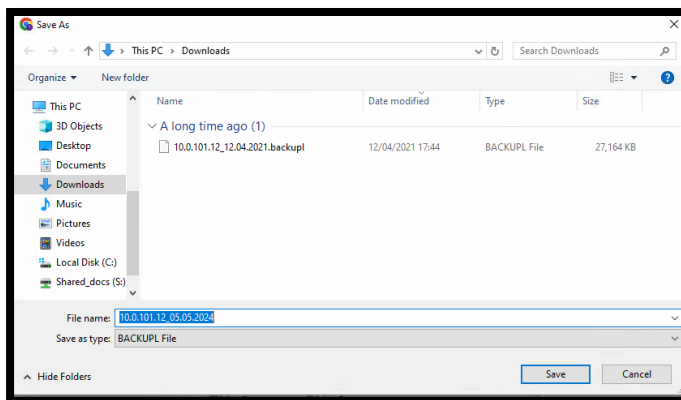
## Backup

To back up an SU device software and configuration to a file on your PC:

1. Select **Backup** in **Maintenance tools**
2. Backup dialog will open, press **Download**



3. Progress bar will be shown while backup file is prepared
4. Once ready – Windows Save As dialog will appear. Select the location on your PC to store the backup file, change the file name if needed and press Save. If required - confirm “keep the file” in browser download dialog.

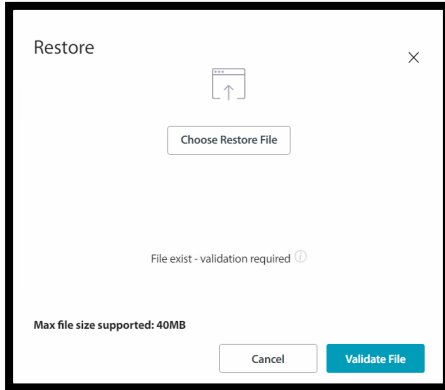


5. Finally, press **Done** to close the Backup dialog.

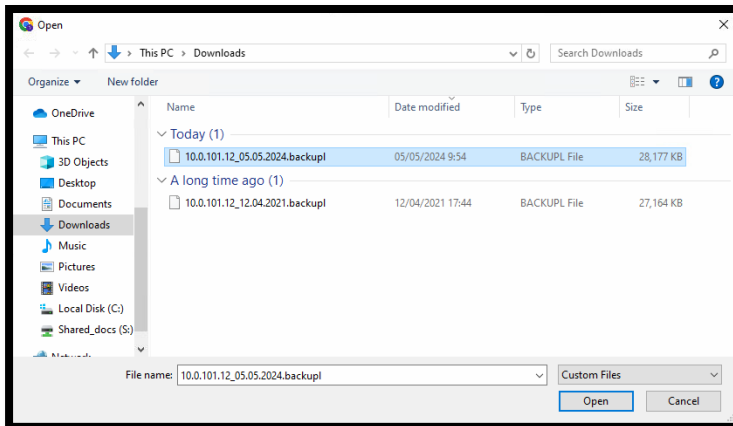
# Restore

To restore an SU device software and configuration from a backup file:

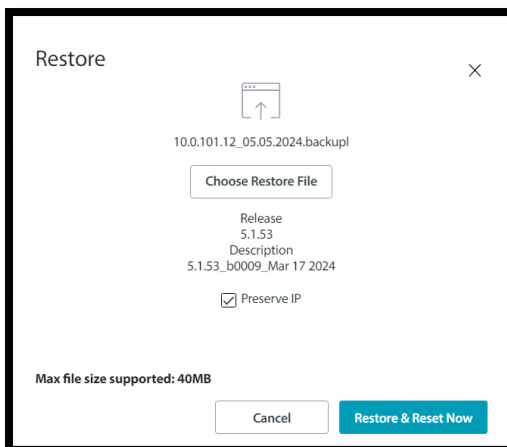
1. Select **Restore** in **Maintenance tools**, Restore dialog will open
2. In case a backup operation was done previously, the latest backup file will be available. The dialog will show “File exists – validation required”, press **Validate File**.
3. Otherwise - press **Choose Restore File** to upload a backup file from the PC file system.



4. Press **Choose Restore File**
5. Windows Open file dialog will appear. Select the backup file stored on PC, press **Open**.



6. Review the Release and Description details. De-select Preserve IP if you wish to set the IP address settings stored in the backup file. Press **Restore & Reset Now** to confirm.





# Diagnostics tools

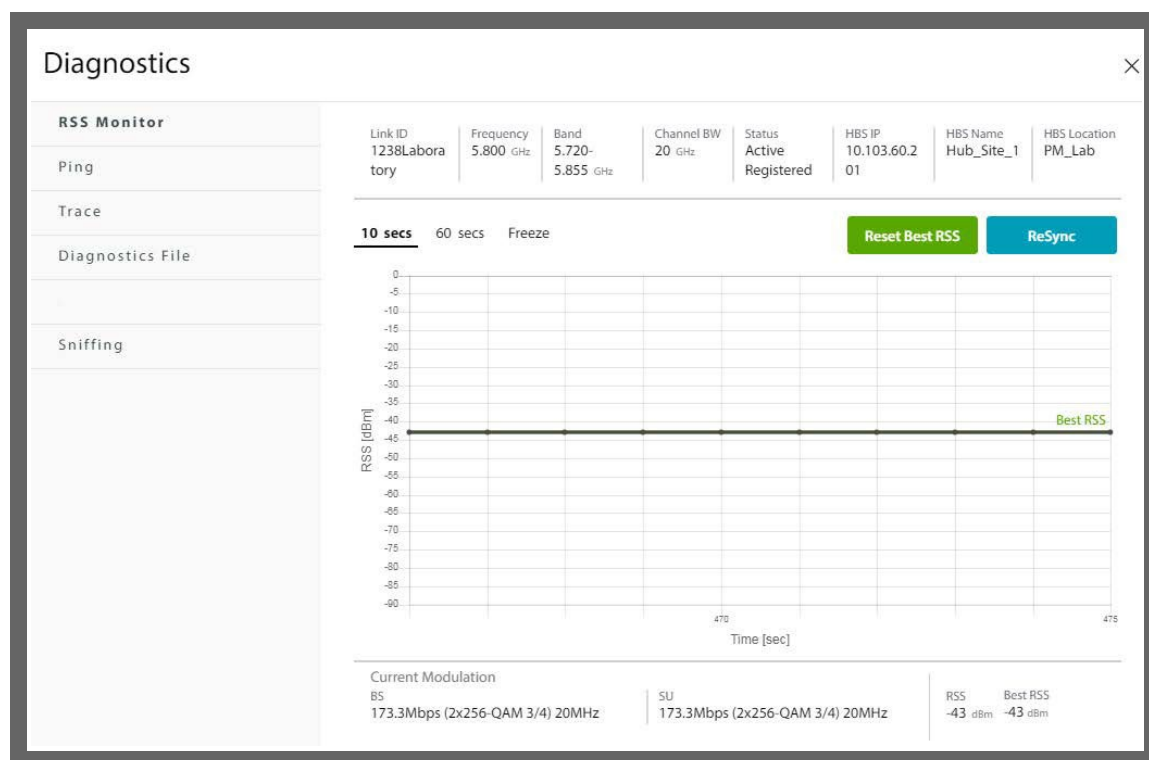


Click the icon to open the **Diagnostics** window.

There are several tabs available:

## 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.





## Ping

This is a basic ping facility that allows you to set the number of packets and the packet size to be sent.

1. Enter the target IP address in the Target IP window.
2. Enter the number of packets to be sent 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.
4. Ping results will be shown.

## Trace

This is a trace route facility.

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. Trace route results will be shown.

## 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 its 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.

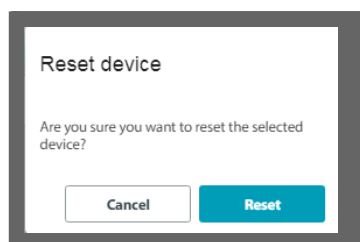


## Operations tools

This icon allows you to perform a reset, restore the factory default settings, or to perform a license activation on the selected device.

### Reset

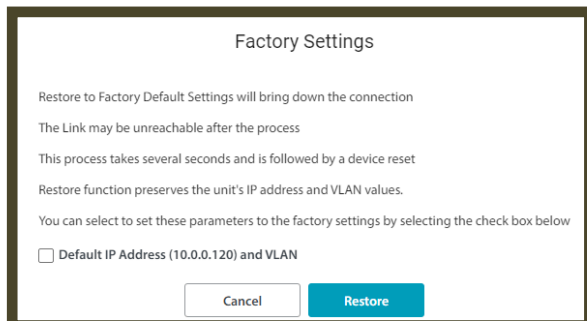
When you choose Reset, you are asked to confirm. Reset is traffic-affecting. If you are sure, click **Reset**.



### Factory Default

When you choose Factory Default, you are asked to confirm this operation. You have an option to restore the default IP address (10.0.0.120) and remove management VLAN by clicking the box next to Default IP address. Keep the box unchecked to preserve the current IP address and management VLAN.

Once you are sure, click **Restore Defaults**. Otherwise, click **Cancel**.



### Licenses

See [HBS Configuration - Licenses](#) for detailed explanation

### Register button

When SU software release is 5.1.42 and above - Self Registered SU is supported.

When the [Self Register](#) feature is enabled on the HBS, Register button will be available.

Pressing Register button will register the SU to the HBS and will activate the service according to the parameters pre-defined on HBS in Self Registered SU settings.



### User Profile Icon

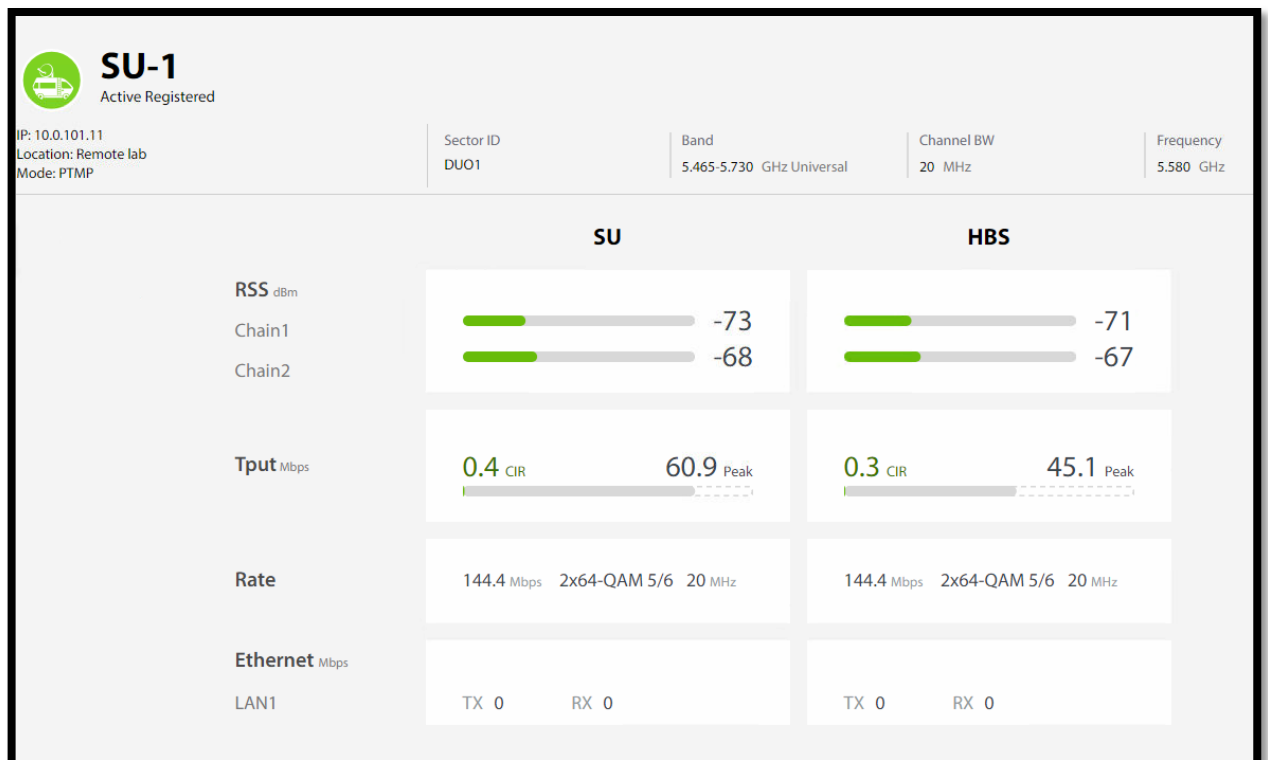


The name of the user profile will appear on the icon. Click this icon to log out.

## Link Dashboard

The following information for the subscriber unit and the wireless link is displayed:

- **SU Name and status**
- **SU IP address**
- **SU Location**
- Mode: PTMP
- **Sector ID**
- **Frequency Band**
- **Channel BW**
- **Operating Frequency**
- **RSS:** received signal per chain on both SU and HBS side
- **Tput:** Estimated net capacity in Mbps for uplink (on SU side) and downlink (on HBS side)
- **Rate:** Air rate, MCS and CBW for uplink (on SU side) and downlink (on HBS side)
- **Ethernet:** LAN TX/RX traffic in Mbps on both SU and HBS side



## Information Panel

The right pane of the user interface functions as an information panel, giving a brief overview of the sector, showing the following:

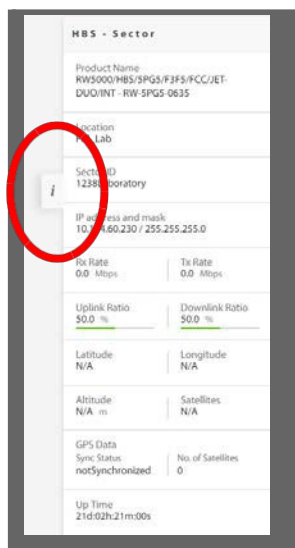
SU (above)

- 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 / restore the info panel, click on info symbol:





# 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 <a href="#">CIR</a> .
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 <a href="#">HBS</a> .
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 <a href="#">BE</a> .
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 geo-location 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, the following background information should be considered:

## B.3 Single and Dual Antennas

Each RADWIN radio has two radio chains. Most radio models such as JET series HBS or SU Integrated subscribers, come with an integrated dual-polarization antenna. Connectorized radio models may be connected to two separate antennas, or to two different connectors of the same dual-polarized antenna. The radio chains 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 radio chains used is determined by user configurations and by automatic system decisions, explained below.

### B.3.1 Dual Antennas at the HBS and an SU

When using dual antennas at both sites (single dual-polarization antenna or two single-polarization antennas), you can choose between Spatial Multiplexing Mode and Diversity Mode.

#### Spatial Multiplexing Mode

Spatial Multiplexing mode is the default operation mode and is recommended for most scenarios. In this mode, the system doubles the link capacity by transmitting two separate data streams on the same frequency channel.

To work in this mode, each port must be connected to different antenna polarization, the RSS level of both receivers should be balanced and separation (cross-polarization) between receivers must be maintained. RADWIN HBS or SU indicates RSS balance between the two antennas in the link status 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, but it will only transmit a single data stream.

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 interference and/or RSS levels are unbalanced between the two antennas
- When actual capacity with Diversity Mode is higher than with Spatial Multiplexing
- When high robustness is of importance and Diversity Mode provides enough capacity

### B.3.2 Single Antennas at Both Sites

When connectorized ODUs are installed and connected to a single antenna at each side, both ODUs must be configured for Diversity mode and will transmit a single data stream.

**Note:** termination plug with 50-ohm impedance must be installed on the unused port.

### B.3.3 Single Antenna at One Site, Dual Antennas at the Other

In this mode, one of the sites uses a single antenna while the other site uses two antennas, typically with the same polarization in a space diversity setup. The system should be configured for Diversity mode and will transmit a single data stream.



## 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:

$\text{maxAvailableTxPower} \leq \min(\text{maxRegEIRP} - \text{AntennaGain} + \text{CableLoss}, \text{maxRegTxPower})$

... (\*)

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.



- 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 all the products covered by this document. Users can enable or disable this protocol.

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 and you will be required to enter ODU user credentials.

The CLI has the same user access privileges as the users who log in to the web UI (Admin, Operator, etc..). Default credentials for admin level access are **admin/netwireless**.

Below is the list of the supported CLI commands

**Note:** the CLI supports auto completion of the command by using the tab key.

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: <b>display link reg</b> <b>display link P17300I000K00160</b>
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>	Set the trap destination index number (up to 10), IP address and port number
set syslog <server ip>	Set Syslog server IP address to <0.0.0.0> in order 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)	Send ping packets to a network device. The options for ping tests are: ping [-c count] [-i interval] [-l 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 <b>util ping 20.0.0.150 '-c' 10</b> Example 2: send pings in interval of 0.5 second (interval should be below 1) <b>util ping 20.0.0.150 '-i' 0.5</b>
util traceroute [OPTIONS] IP [BYTES] (CTRL+C To Stop, 'util traceroute' for all options)	Perform traceroute test
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  <a href="#">admin@20.0.0.130(link-Alpha IP 64)-&gt;</a>

display beamwidth	<p>Displays the current SDS beamwidth (45 / 60 / 90) for JET DUO HBS</p> <p>Output example:  <b>Sector beamwidth on carrier 1 is 45</b>  <b>Sector beamwidth on carrier 2 is 45</b></p>
set beamwidth <value>	<p>Sets the sector's SDS beamwidth (45 / 60 / 90) for both carriers on JET DUO HBS</p> <p>Output example:  <b>Sector beamwidth is set to 60</b></p>

# 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.



Last page of files

**RADWIN**

