RADWIN

RADWIN 2000 E User Manual

Release 6.1.10

Document Version 1

Contents

1 Introduction

1.1 Document Scope

This document describes how to configure and manage the RADWIN 2000E Outdoor Units (ODUs). It also describes the 2000E model, concepts of operation, a technology overview, and troubleshooting, as detailed in the following main sections:

Connecting a Laptop to the ODU
Error! Reference source not found.
Viewing Devices & Link Status
Configuring the Air Interface Parameters
Configuring ODU Management Parameters
Configuring Service Parameters

1.2 Revision History

	Date	Document Revision	SW Release	Revision details
1.	Jun. 2023	1.3	6.0.0	1st version of the user manual Includes the user manual of the 2000E version 6.0.0
2.	Dec. 2023	2.0	6.0.11	• Added QOS, protocols, management VLAN, forgot IP, SNMP, max RSS for antenna alignment • Updated screenshots with UI fixes
3.	Mar. 2024	2.1	6.0.15	• IPv6 Support • Radio Band License Management
4.	May. 2024	2.2	6.0.17	• Offline Spectrum Scan • Backup/Restore • Hub Site Synchronization
5.	July. 2024	2.3	6.0.18	• HTTPS Support • RADIUS Authentication • SNMP V3 User
6.	Sep.2024	2.4	6.0.20	• Traffic VLAN Management • Alignment Buzzer • Disable Hub Site Sync • New 6GHz products
7.	Oct.2024	2.5	6.0.22	• Syslog support
8.	Apr.2025	3.0	6.1.10	• 6GHz FCC Band support with AFC

1.3 What's New in this release

The 2000E now includes support for the 6GHz FCC/IC Band with AFC. The supported bands are 5.9-7.1 GHz and 5.9-6.4 GHz FCC/IC. These bands require the use of the FCC/IC AFC service to verify availability and allowed transmission power for different channels on these bands.

1.4 Product Family Overview

The RADWIN 2000 E Family delivers up to 2.5Gbps (depending on the regulation) in a point-to-point architecture and is the ideal choice for enterprise connectivity and for backhaul.

The RADWIN 2000 E family includes the following models:

RADWIN 2000-E Family Model Comparisons

Model Name	PN	Product Name	Max Throughput	Frequency Band	Form Factor
2000 E	RW-2U50-E2MM	RW2000/ODU/E/F50/WW/INT	2.5Gbps (universal), 1.2Gbps (FCC)	4.9-6.0 GHz	Connectorized
2000 E	RW-2U50-E1MM	RW2000/ODU/E/F50/WW/EXT	2.5Gbps (universal), 1.2Gbps (FCC)	4.9-6.4 GHz	Integrated
2000 E	RW-2U5X-E1MM	RW2000/ODU/E/F5X/WW/INT	2.5Gbps (universal), 1.2Gbps (FCC)	4.9-6.4 GHz	Connectorized
2000 E	RW-2U60-E2MM	RW2000/ODU/E/F60/WW/EXT	2.5Gbps (universal), 1.2Gbps (FCC)	5.9-7.1 GHz	Integrated

Note

Some options and models may not be available for your regulatory environment.

1.5 Technology Overview

1.5.1 Higher Capacity - Over Longer Distances

RADWIN 2000 E family products leverage the cutting-edge 802.11ax technology, building on the techniques of the market proven RADWIN 2000 PtP family to push performance to a new level.

With the ability to squeeze more bits per frequency channel and uniquely support channels of up to 160MHz and up to 4096QAM modulation, RADWIN 2000 E offers greater capacity and range than any other unlicensed PtP solution.

1.5.2 AIR Interface Mitigation Techniques

Radwin 2000E employs multiple Air interface mitigation techniques:

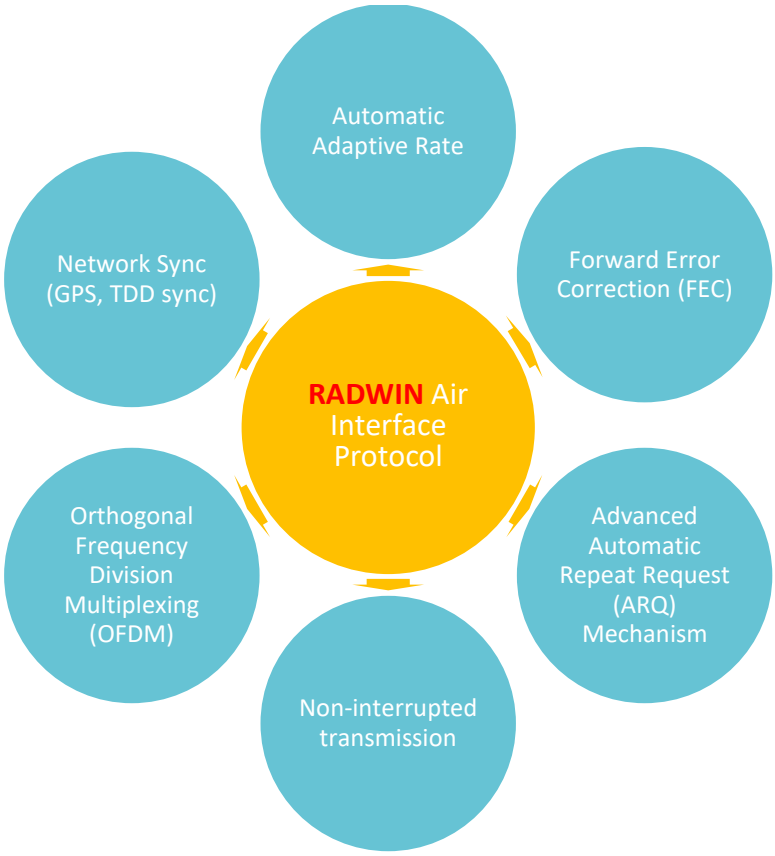


Figure 1: Multiple Air Interface Mitigation Techniques

Orthogonal Frequency Division Multiplexing (OFDM)

Orthogonal Frequency Division Multiplexing, or OFDM, is a modulation technique for effective transmission of large amounts of digital data over a radio link. It is characterized by its low overhead, low latency, and high resiliency to interference.

Selected by standards organizations and leading telecommunications providers, OFDM is the technology of choice for terrestrial radio communications that require high efficiency in difficult environments.

Based on the concept of redundant transmission, OFDM works by splitting the radio signal into multiple smaller sub-signals that are then transmitted simultaneously at different frequencies to the receiver.

By replicating the content signal using multiple narrowband sub-carriers to repeat transmissions over time, OFDM works to ensure that complete content arrives at the transmission destination.

This technique is especially effective for protecting against the effects of multipath fading deriving from the cancellation of carriers under heavy interference conditions.

When a system employing OFDM encounters RF interference, it recovers the affected signal from duplicate carriers that were not affected by the interference.

Based on these considerations, RADWIN selected OFDM as the core modulation technique for all its radio products.

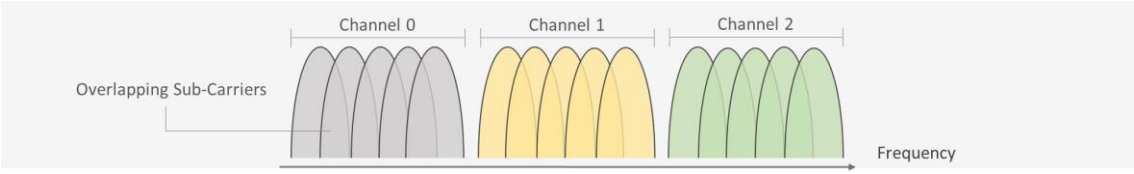


Figure 2:Orthogonal Frequency Division Multiplexing (OFDM)

Automatic Adaptive Rate - BPSK to 4096QAM

Automatic Adaptive Rate works under the RADWIN proprietary algorithm, adjusting the Modulation and Coding Scheme, and checking potential MCS without affecting the current level of service.

RADWIN 2000E product family supports the following modulation schemes: BPSK, QPSK, 16QAM, 64QAM, 256QAM, 1024QAM, 4096QAM with the following error correction rate indexes: 1/2, 2/3, 3/4, 5/6.

The automatic adaptive rate maximizes ethernet throughput while ensuring a minimum Error Rate.

The automatic adaptive rate allows enhanced robustness and better performance under interference.

RADWIN products perform independent automatic adaptive rate at each side of the link, in both the uplink and downlink.

Advanced Automatic Repeat Request (ARQ)

Advanced ARQ error-handling at the physical layer, instead of higher levels, has much lower overhead than other ARQ methods, and in many cases repeat transmission is initiated without having to wait for a request from the Client ODU, minimizing either latency or error rate to optimize performance for the type of services being delivered.

If there are unrecoverable errors in a packet, it requests retransmission automatically. RADWIN systems ensure error-free service using a proprietary quick ARQ mechanism with super-fast retransmission of errant data.

Advanced Forward Error Correction (FEC)

The Advanced FEC technique uses very little overhead, and algorithms specifically designed for the varying conditions of license-exempt frequency bands. The sender adds redundant data, enabling the receiver to detect and correct errors upon reception. Retransmissions are avoided, thus avoiding the cost of higher bandwidth requirements on average.

Non-Interrupted Transmission

The non-Interrupted transmission technique keeps transmissions regardless of changing conditions in the channel, leaving the on-the-fly corrections to operate while the communication flows remain stable and robust.

Adjustable UL/DL Ratio

RADWIN 2000E family links support an adjustable DL/UL ratio - 25%/75%, 50%/50% or 75%/25%. This capability allowed the user to optimize the transmission time allocation to the direction that contains the most data.

Adaptive MIMO/Diversity

Based on RSS levels from both paths of the dual-polarization antenna, ODUs can decide to use either MIMO or Diversity.

In most situations, MIMO represents the best option in terms of performance. However, certain conditions can affect the link, forcing the use of Diversity, such as a nearby water mirror (a lake or a bay with dense vegetation), and metal structures.

MIMO - Multiple Input Multiple Output

Multiple Input Multiple Output, or MIMO, is based on using multiple antennas per side, in our case, two antennas with opposite linear polarization. Throughput can be increased using different streams per polarity, doubling capacity over the same channel bandwidth. MIMO needs good isolation (rejection) between both polarities and a similar path performance for all the antennas. MIMO increases spectral efficiency without increasing transmission power and bandwidth. We use MIMO mode, particularly for its Rate Gain.

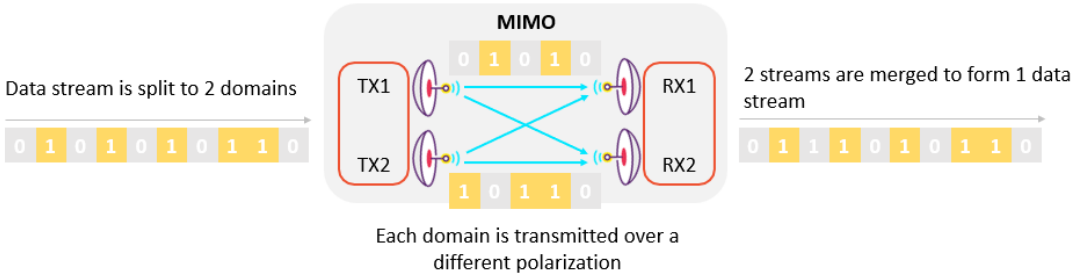


Figure 3: Multiple Input Multiple Output (MIMO)

Diversity

Diversity Mode uses two antennas to improve the quality and reliability of the link. In some scenarios, the signal is reflected along multiple paths. Each such “bounce” can introduce phase shifts, time delays, attenuations and even distortions that can destructively interfere with one another at the receiver. Antenna diversity is especially effective for mitigating multi-path situations because multiple antennas afford a receiver several parts of the same signal. Each antenna will be exposed to a different interference, thus, if one antenna is undergoing a deep fade, it is likely that another has enough signal, and collectively, such a system can provide a better link. Antenna diversity requires antenna separation, which is possible using a dual-polarization antenna or two spatially separated antennas.

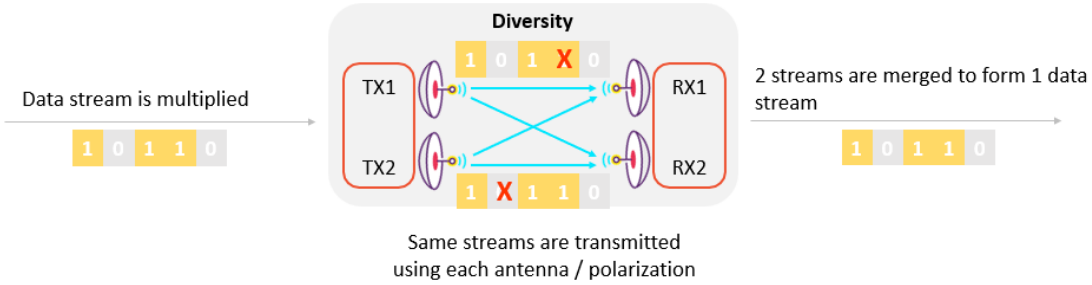


Figure 4: Diversity

1.5.3 Configurable/Adaptive Channel Bandwidth

You can configure the channel bandwidth that will be employed in the link. Supported CBWs are as follows (depending on regulation):

- 20 MHz
- 40 MHz
- 80 MHz
- 160 MHz

With the adaptive channel bandwidth feature, links that are configured to a higher channel bandwidth will automatically transfer to a lower channel bandwidth in case of interference, to optimize the throughput and provide the best service.

1.5.4 Security and Encryption

RADWIN products conform to high-security standards both in securing access to the management interface of the ODUs and in encrypting the data transmitted over the air interface.

Air Interface Security

The RADWIN 2000E platform provides a proprietary air interface that is not amenable to scanning and penetration attacks from Wi-Fi devices. RADWIN 2000E family ODUs offer standard AES 256-bit over-the-air encryption for transmitted data. The encryption is based on a user-defined link password.

1.5.5 Low Sidelobes Integrated Antenna

RADWIN 2000 E family Integrated products include a directional antenna with an exceptionally high side-lobe rejection level (≥ 22dB). This antenna provides excellent isolation in noisy environments while keeping the ODU compact and easy to install.

1.6 Mode of Operation

RW 2000 E is a Point to Point (PtP) Outdoor Unit (ODU). The PtP ODUs establish a wireless radio link between them to transmit high-capacity data.

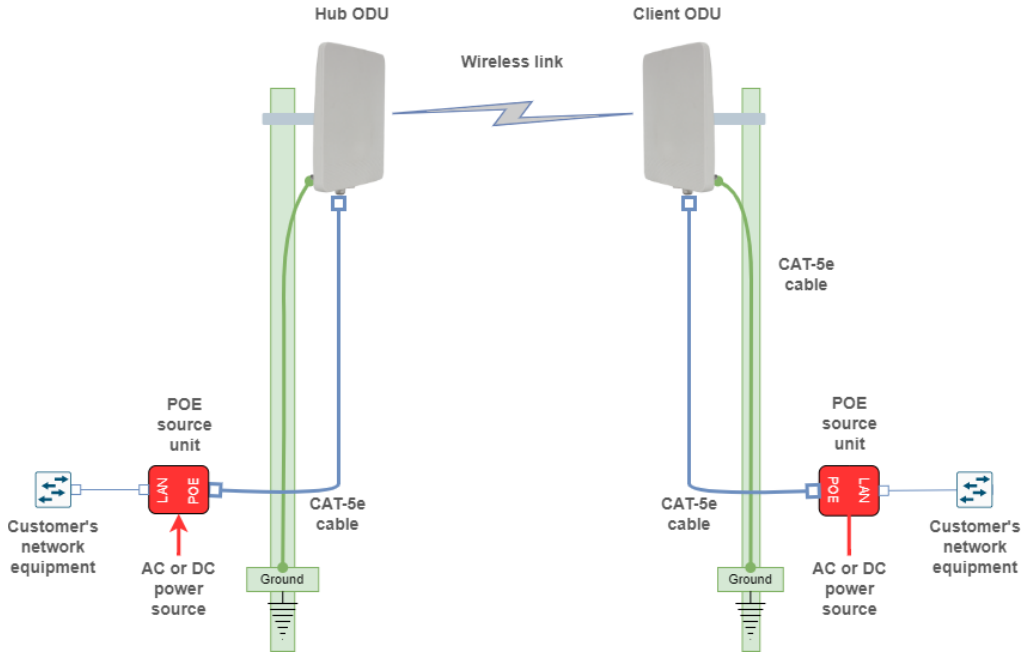


Figure 5: PtP Connection Scheme

Note

For simplicity, Lightning Protection Units (LPUs) are not shown in the following figure but are recommended.

1.6.1 Hub / Client

Any RW 2000 E ODU can be configured either as Hub or as Client.

The method of operation of the RW 2000 E link requires that one side of the link would be designated as the Hub - which will transmit a beacon, and the other side of the link would be designated as a Client which will scan for the beacon and connect to the Hub.

Due to this mode of operation, configuration of the link and service are stored in the Hub and are transferred to the Client upon link establishment.

Note

Radwin recommends that the ODU close to the operator's main network side will be configured as the Hub, while the ODU at the remote side (closer to the end customer) be configured as Client. This way, if the link between the Hub and Client is lost, you keep the connection to the Hub.

The differences between Hub and Client are summarized in the following table:

Overview of the Differences between Hub and Client

Hub	Client
Transmits beacon, waiting for Client connection	Searches for beacon and establishes a connection to the Hub
Contains some master settings for both devices	Receives settings from the Hub on link establishment
Identifies its location from GNSS and determines the country and applicable regulation	Receives the country and applicable regulation configuration from the Hub

1.6.2 Link Establishment and Starting Service

ODU Activation and Initial Setup

An ODU comes out of the box configured as a Client by default. You can change the ODU configuration between Hub and Client through the Quick Setup wizard).

To establish a link between ODUs, you need to activate the ODU by configuring essential parameters such as link ID, password, and antenna parameters for external ODUs, operating band and channels in the Hub).

Link Establishment Process

High-level process of link establishment:

1. When the Hub ODU boots, if it has been activated (essential parameters configured), it will start transmitting a beacon on configured channel and with the configured link ID.
2. When the Client ODU boots, if it has been activated (essential parameters configured), it will start scanning for a beacon.
3. Once the Client detects a beacon, the Client will attempt to connect to the Hub.
4. If the link ID matches the configured security policy, a link will be established.
5. At this point, both Hub and Client will appear in the UI, as being part of the link, but the Client is not registered yet (no service).
6. You can perform antenna alignment at this stage (the MCS is locked to be constant).
7. Once you want to start the service, register the Client to the Hub using the browser user interface.
8. Once the Client is registered, the link is fully active.

Registered/Deregistered Devices

An active link between the Hub and Client can be in either Registered or Unregistered state. When the hub and client are registered, the service is activated, and full user-data is transferred over the active link.

When they are not registered, the link will only allow limited communication between the devices during an active link and will not transfer any user-data.

When a Client is registered to a Hub, both devices are locked together and won't accept a connection to any other device if the link is lost. If they are not registered to each other, each device can create a new link with any other device if the link between them is lost.

1.6.3 Browser User Interface for Configuration and Monitoring

The RW 2000 E browser user interface allows to configure both Hub and Client settings simultaneously in a side-by-side view. The Hub is always displayed on the left side, while the Client is always displayed on the right side.

While a link between both ODUs is active, you can configure and view the status of both ODUs.

If the link is broken, or if there is a mismatch in the link (Client not registered to the Hub, link password not matching, etc.), you will only be able to configure the device to which you are directly connected (local device).

Local Device

Using a (laptop icon), the browser user interface indicates which ODU is the local device (the ODU whose IP address was entered in the browser).

Some configurations in the browser user interface are only possible for the local device (such as SW upgrade, changing user password). To configure the remote device, connect to that device's IP address directly and perform the required operation.

Note

If the link is lost, you will have a connection to only one side of the link. The other ODU becomes inaccessible. For this reason, take care when modifying the configuration that might cause the link to be lost (such as factory reset).

Link Status Indications

The browser user interface shows the status of the link. The following statuses can appear.

Status Name	Description
Not Activated	The ODU hasn't been activated. Complete the quick setup wizard to configure all the essential parameters.
Searching	The ODU is searching for a link. This can happen either if there was a link and it got disconnected, or if no link was yet established.
Not Registered	A link has been established, but the Client Hasn't been registered to the Hub. The service is not active at this link status.
Active	The link is established and is active. Full service is active over this link.
PW Mismatch	The passwords of the hub and client do not match. The service is not active at this link status.
SW Upgrade Required	A software upgrade is required for the system to function.

Status Name	Description
Spectrum Scanning	Scanning the radio spectrum to detect an optimal frequency. Service is still active during that time.
Regulation Mismatch	The regulation settings of the hub and client do not match. Service is inactive at this link status.

TDD (UL/DL) Ratio

TDD ratio determines which part of the radio frame is allocated for DL transmission and which is allocated for UL transmission. This setting is extremely useful when the data capacity is not symmetrical between the UL and the DL directions.

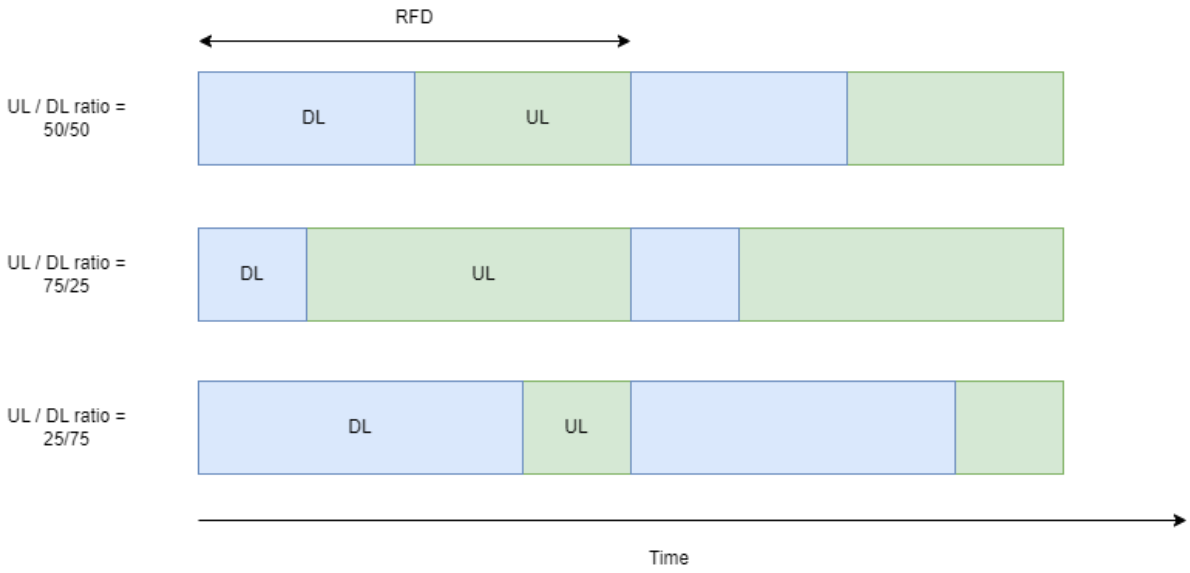


Figure 6: TDD ratio

1.7 Regulation Compliance

1.7.1 Enforcing Regulation Restrictions

RADWIN 2000 E family of ODUs include a built-in GNSS receiver. The ODUs identify their location from GNSS and determine the country in which they are located and the regulation that applies in 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.

1.7.2 GPS Mode

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

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

When the system could connect to the GNSS Signal, you could see the colored GPS icon on the upper right corner of the WebUI.

When the GNSS Signal is not reachable, this icon is greyed out.

Figure 7: GNSS Signal acquired

1.7.3 No GPS Mode

If the user wishes to test the device indoors - e.g., inside a warehouse / lab, the device will 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 will select the allowed regulation for this country, and the available frequencies will adjust to allowed frequency band in this country.

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

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

1.7.4 Dealing with AFC

AFC (Automated Frequency Coordination) is a system designed to protect licensed incumbent users (such as fixed microwave links and satellite ground stations) in the **6 GHz band** while allowing unlicensed devices (like Wi-Fi 6E and Wi-Fi 7) to operate outdoors and at higher power levels.
It is mandatory for standard-power outdoor Wi-Fi devices in **the U.S. and Canada**.

How AFC Works

1. **Device Location Reporting**:
   The ODU determines its geographic location with high accuracy (using GPS).
2. **Query to AFC System**:
   Before transmitting, the device queries an authorized AFC system over the Internet. It sends:
   - Its location
   - Technical parameters (e.g., antenna height, power capability)
3. **Frequency Allocation**:
   The AFC system checks a database of protected incumbents (managed by FCC/ISED) and calculates:
   - Which 6 GHz frequencies are safe to use
   - What power levels are allowed for each frequency
4. **Operational Authorization**:
   The AFC sends a **list of allowed channels and transmit power limits** back to each of the PtP devices.
   Each device must strictly operate within these parameters.
5. **Continuous Coordination**:
   Devices periodically re-query the AFC if they move or after a defined time window (typically every 24 hours) to maintain compliance.

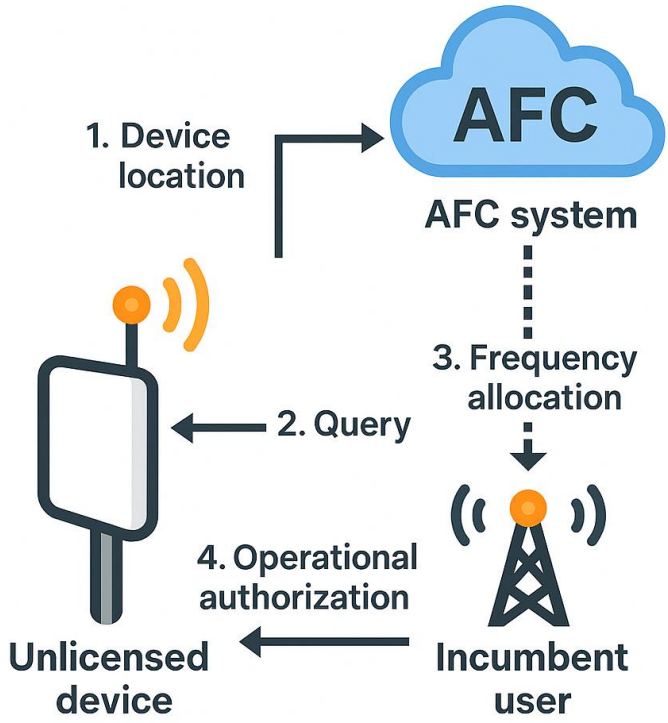


Figure 8: AFC Protocol

1.8 Management Tools

Currently, the following management tools are enabled:

Tool	Capabilities
EMS - browser UI	Configure ODU and link parameters. Monitor ODU and link status. Inspect the recent events logs. Perform SW upgrade. Perform reboot and factory reset.

1.9 Safety and Security

1.9.1 Safety

Before working on equipment connected to power lines or telecommunication lines, remove jewelry or any other metallic object that may come into contact with energized parts.

Use extreme care when working at heights.

All RADWIN products should be grounded during operation.

The use of lightning protection is dependent on regulatory and end-user requirements.

To protect against overexposure to RF energy, all persons should maintain safe distances from radio sources.
When the system is operational, avoid standing directly in front of the antenna. Strong RF fields are present when the transmitter is on.

1.9.2 Security Recommendations

Change the default user password and set a new link password

Use only SNMPv3 for monitoring and disable SNMPv1

2 Connecting a Laptop to the ODU

This section describes how to connect a laptop to an ODU and perform the initial configuration between Hub and Client ODUs using the Quick Setup wizard in the browser user interface.

2.1 Preparing a Laptop

The laptop needs to have the same subnet as the default IP of the ODU. The ODU's default IP address is 10.0.0.120.

Configuration in Windows

Configure the laptop IP address and subnet mask as follows:

1. Control Panel -> Network and Internet -> Network and Sharing Center -> Change Adapter Settings -> click Network Interface Card Name.
2. Properties -> Select Internet Protocol Version 4 (TCP/IPv4) -> Properties -> set the IP address to 10.0.0.x (any other than 120) and Subnet mask to 255.255.255.0.

Configuration in Mac

Configure the laptop IP address and subnet mask as follows:

1. System Settings -> Network -> Select network interface
2. Details -> TCP/IP -> Configure IPv4 -> Select Manually -> set the IP address to 10.0.0.x (any other than 120) and Subnet mask to 255.255.255.0.

2.2 Connecting a Laptop to RADWIN 2000 E ODUs

1. Connect the PoE (or POE switch) to a power source.
2. Connect an ethernet cable between the laptop and the PoE (or POE switch).
3. Connect an ethernet cable from the POE (or POE switch) to the ODU **PoE IN** socket.

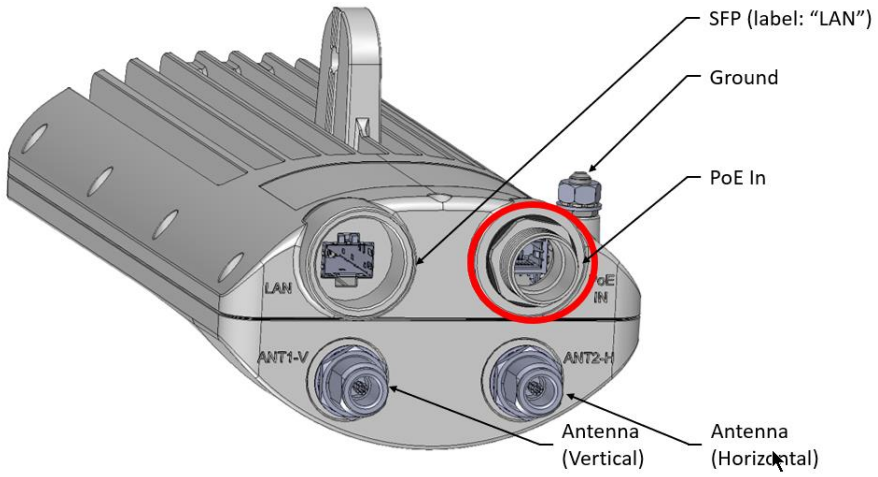


Figure 9: External ODU - POE IN socket

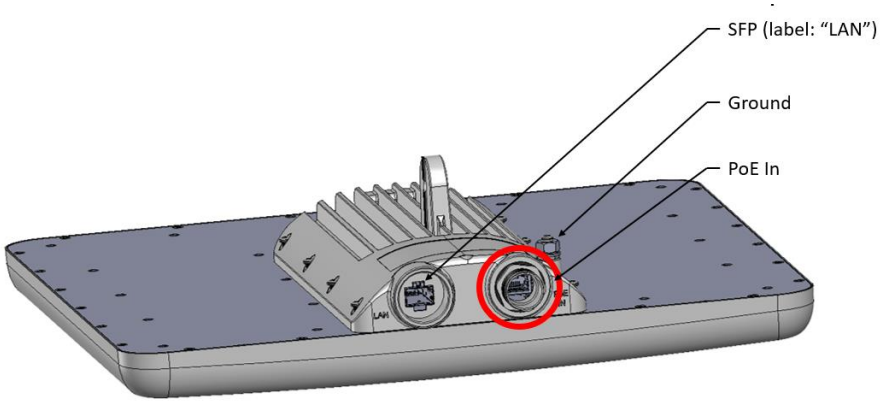


Figure 10: Integrated ODU - POE IN socket

4. In a browser, enter the ODU IP address (default value: 10.0.0.120).
5. In the login page, enter the following default credentials and click **Login**:

Figure 11: Login

After the first login:

2.3 Run quick setup to configure basic device parameters and activate the device – see Online Help – Chatbot

If the device used to configure your RADWIN 2000 E has internet connection, you could use our Chatbot to get help regarding the ODU configuration.

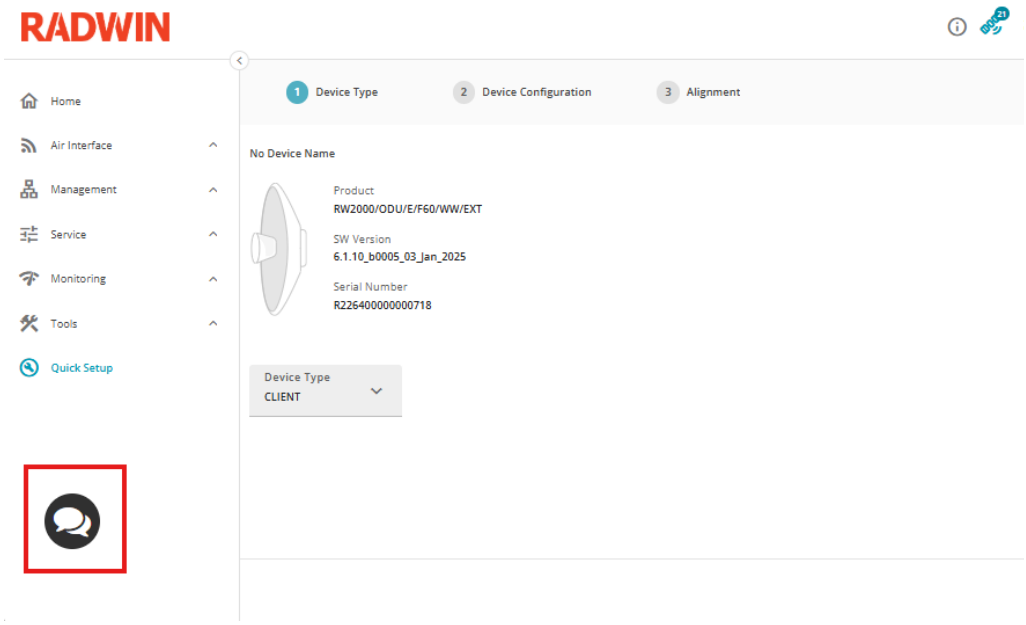


Figure 12: Chatbot Access

Clicking on the chat icon will open our chatbot.

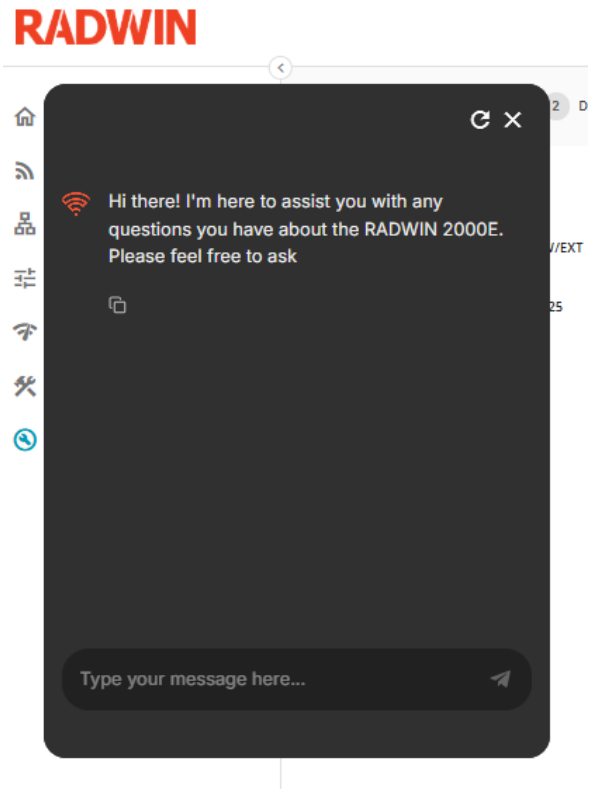


Figure 13: Chatbot Pop-up Window

Running Quick Setup for ODU Initial Configuration.

Change the IP address - see

Configuring the Management IP.

Change the default user password - see Configuring the Protocols

2.4 Online Help – Chatbot

If the device used to configure your RADWIN 2000 E has internet connection, you could use our Chatbot to get help regarding the ODU configuration.

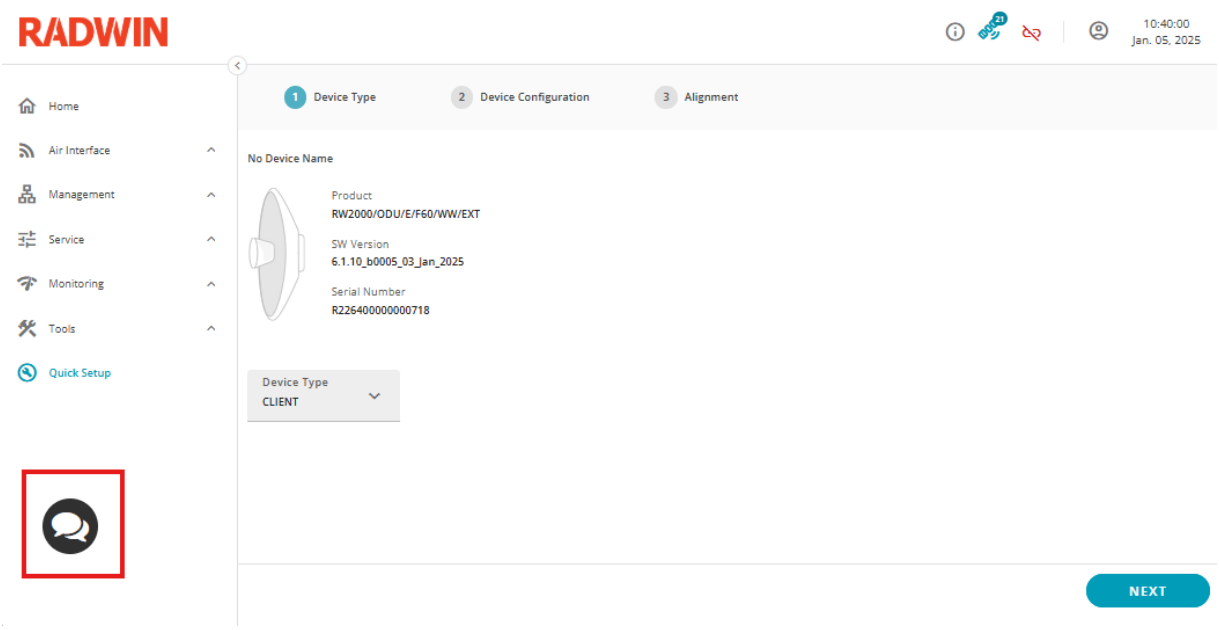


Figure 12: Chatbot Access

Clicking on the chat icon will open our chatbot.

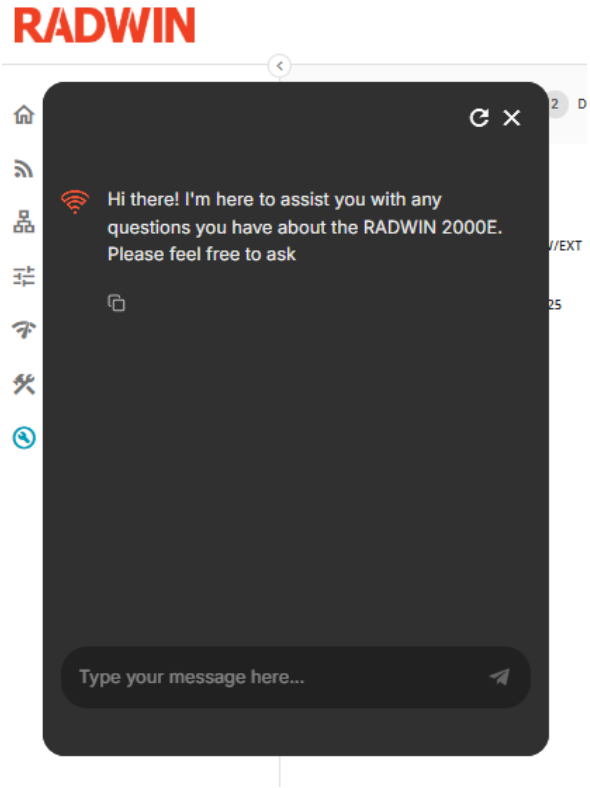


Figure 13: Chatbot Pop-up Window

2.5 Running Quick Setup for ODU Initial Configuration

1. Using a browser, log in to the ODU.
2. If this ODU hasn't yet been activated, the **Quick Setup** wizard starts automatically. Otherwise, the **Home** page appears.
3. If the **Quick Setup** wizard hasn't started, click **Quick Setup.**
4. The quick setup wizard differs between Hub and Client, some steps are relevant only on Hub side (notified in the paragraph name).

2.5.1 Device Type Selection

The wizard for configuring the ODU parameters has 2 different flows depending on the type of the device:

Hub

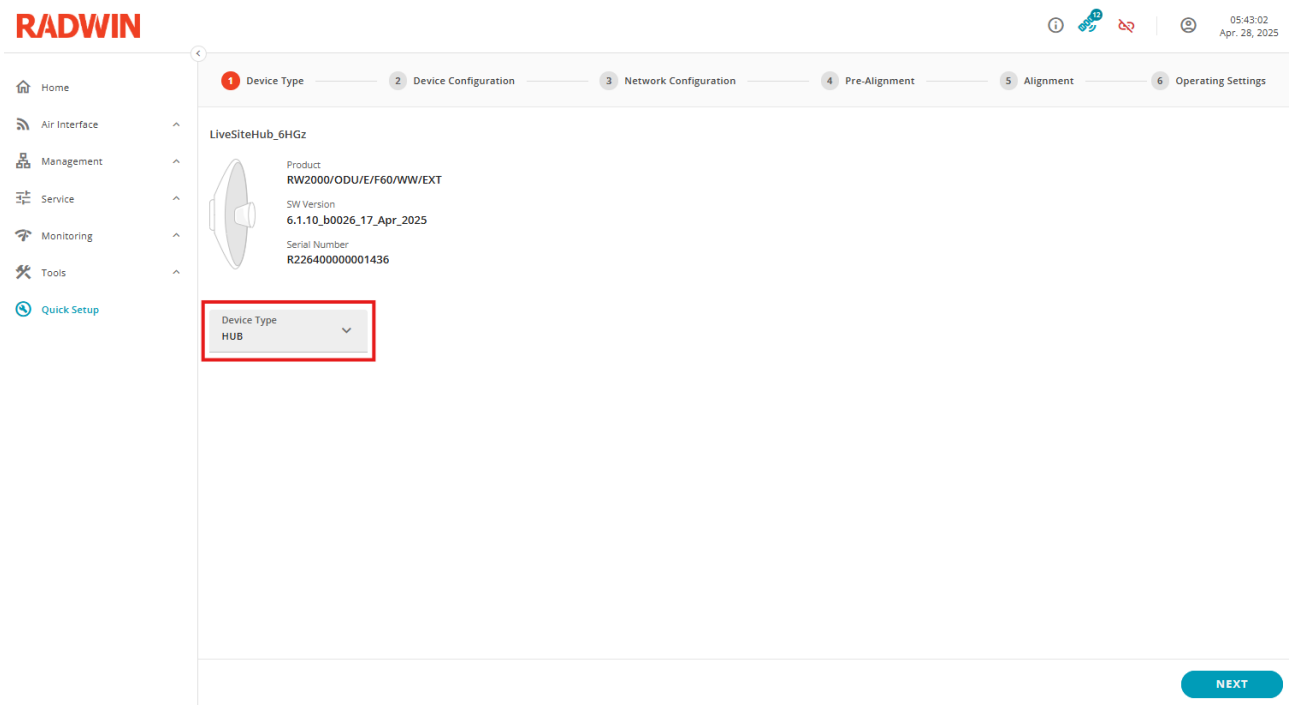


Figure 14: Define the Device Type as Hub

Client

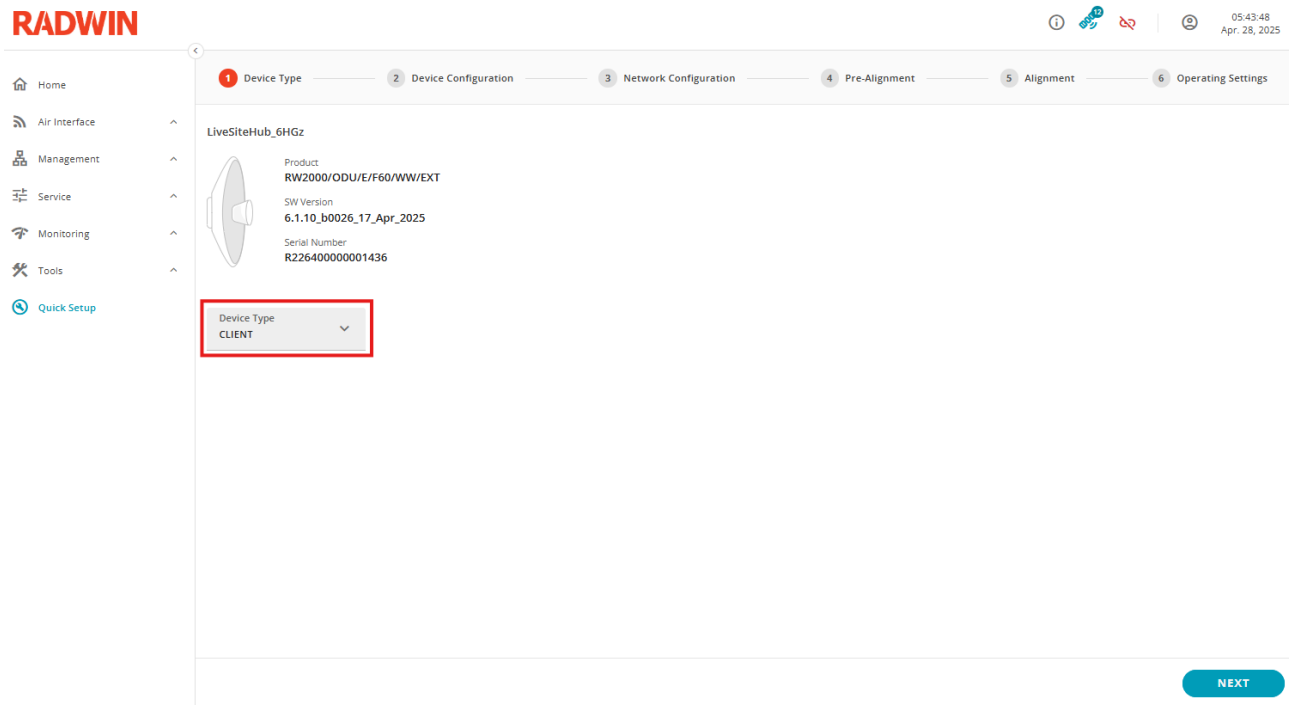


Figure 15: Define the Device Type as Client

Note

When changing device type, the ODU will perform a reboot.

When the device type is correctly set, click on NEXT.

2.5.2 Device Configuration

The ODU configuration page presents 4 sections:

1. General
2. Antenna
3. Link Management
4. Dl/UL Ratio

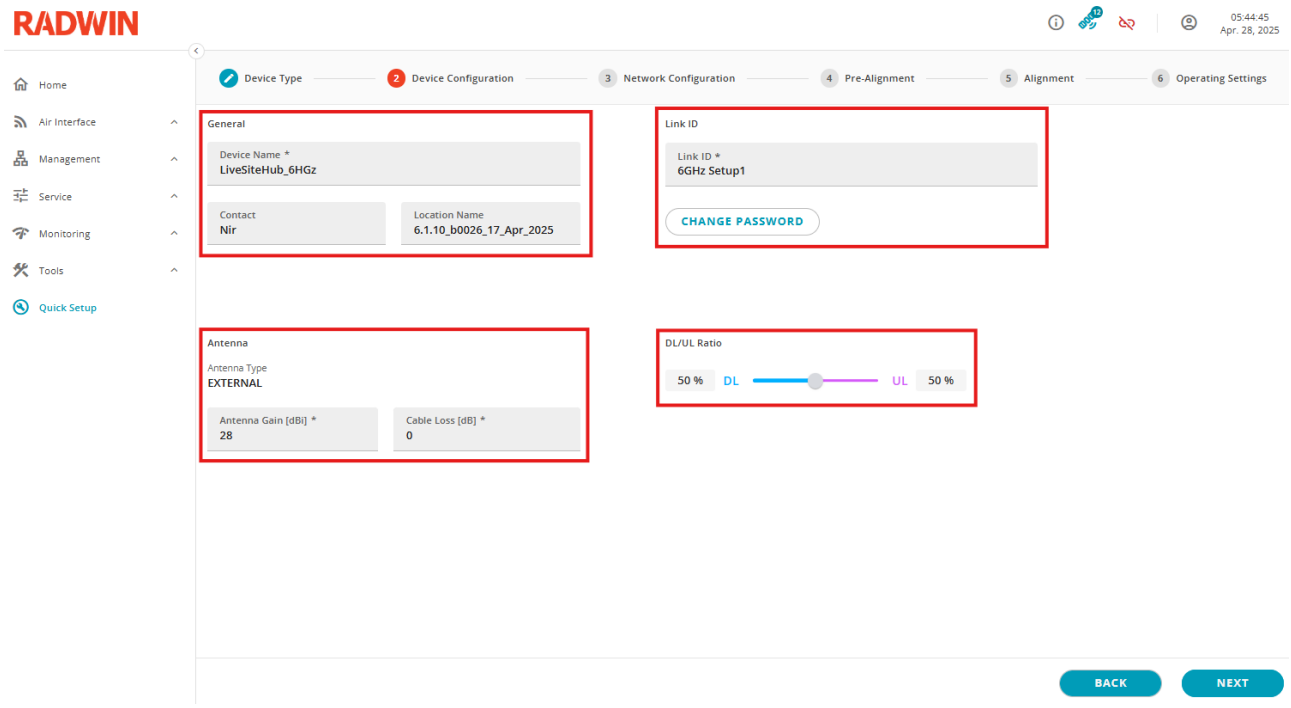


Figure 16: Device Configuration

General

Parameter	Description	Mandatory
Device Name	See Configuring General ODU Settings.	Yes
Contact	See Configuring General ODU Settings.	No
Location name	See Configuring General ODU Settings.	No

Antenna

Parameter	**Description**	**Mandatory**
Antenna Type	See Configuring the Antenna & TX Power. Antenna type could be external or Internal	Yes
Antenna Gain	See Configuring the Antenna & TX Power. For Internal antenna, antenna gain cannot be modified.	Yes
Cable loss	See Configuring the Antenna & TX Power. For Internal antenna, cable loss cannot be modified.	Yes

Link

Parameter	**Description**	**Mandatory**
Link ID	See Configuring the Link Security.	Yes
Link Password	See Configuring the Link Security.	Yes

DL/UL Ratio

The DL/UL ratio is set by default to 50/50%, you could modify it to 25/75% or 75/25%.

When finished, click on NEXT.

2.5.3 Network Configuration

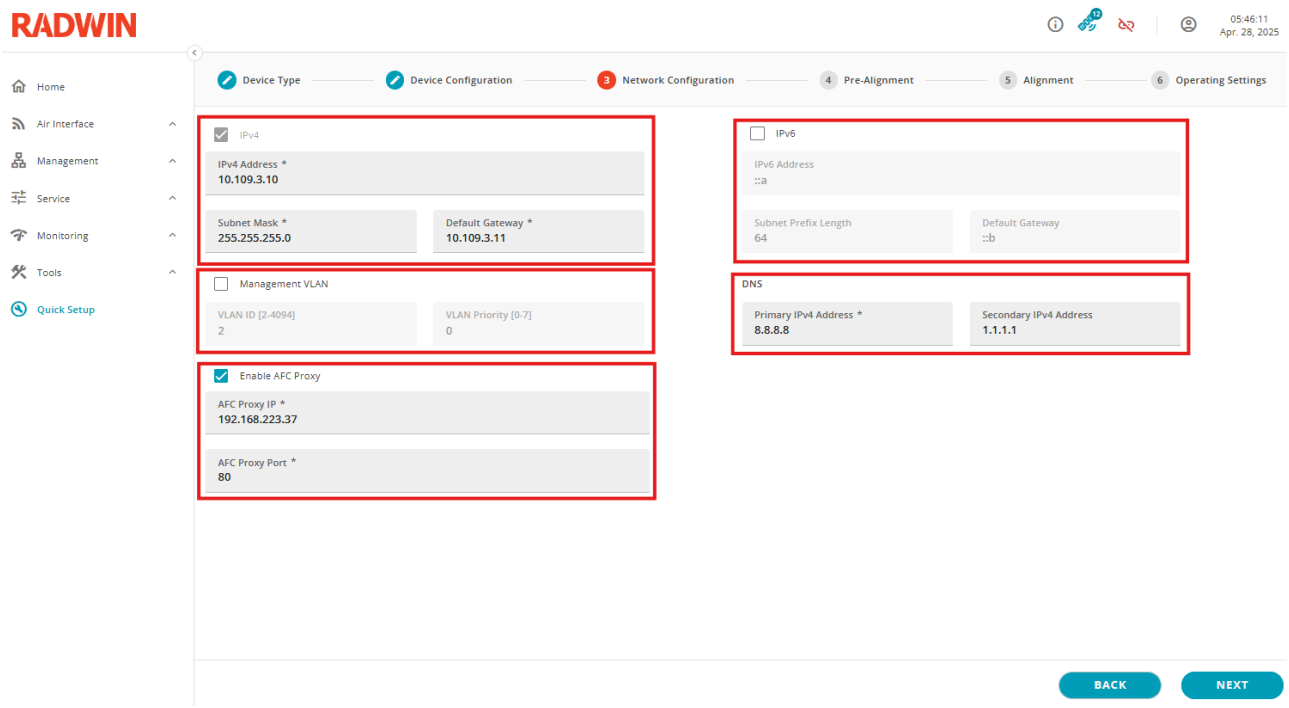


Figure 17: Network Configuration

Parameter	Description	Mandatory	Default value
IPv4 Section			
IPv4 Address	IPv4 address for management interface	Yes	**10.0.0.120**
Subnet Mask	IPv4 subnet mask for management interface	Yes	**255.255.255.0**
Default Gateway	IPv4 address default gateway for management interface	Yes	**0.0.0.0**
IPv6 Section			
IPv6 Address	IPv6 Address for management interface	No	
Subnet Prefix Length	Number of bits used by the prefix	No	**1**
Default Gateway	IPv6 address default gateway for management interface	No	
Management VLAN	Enable/disable VLAN tagging for management traffic	No	**Disabled**
VLAN ID	Supported values: 2-4094	Parameter	

Parameter	Description	Mandatory	Default value
VLAN Priority	Supported values: 0-7	Parameter	
DNS	Configure DNS servers **Mandatory with AFC when device do have direct connection to Internet**	No*	**Always visible**
Primary IPv4 Address	Address of the primary DNS server	No	8.8.8.8
Secondary IPv4 Address	Address of the secondary DNS server	No	2.2.2.2
AFC proxy (Only for US or Canada)	Enable/Disable the use of an AFC Proxy **Mandatory with AFC when device does not have direct connection to Internet**	No*	**Disabled**
AFC Proxy IP	Address of the proxy	No	0.0.0.0
AFC Proxy Port	Port for the proxy	No	80

If ODUs do not have direct access to Internet, you will need to enable the AFC Proxy feature. RADWIN offers an HTTP Proxy Docker image to enable ODUs to access the AFC Cloud Service. For more information, please refer to our HTTP Proxy – Application Note document available at RADWIN Tools Documentation or ask our support team.

When finished, click on NEXT.

2.5.4 Pre-Alignment (Hub Only)

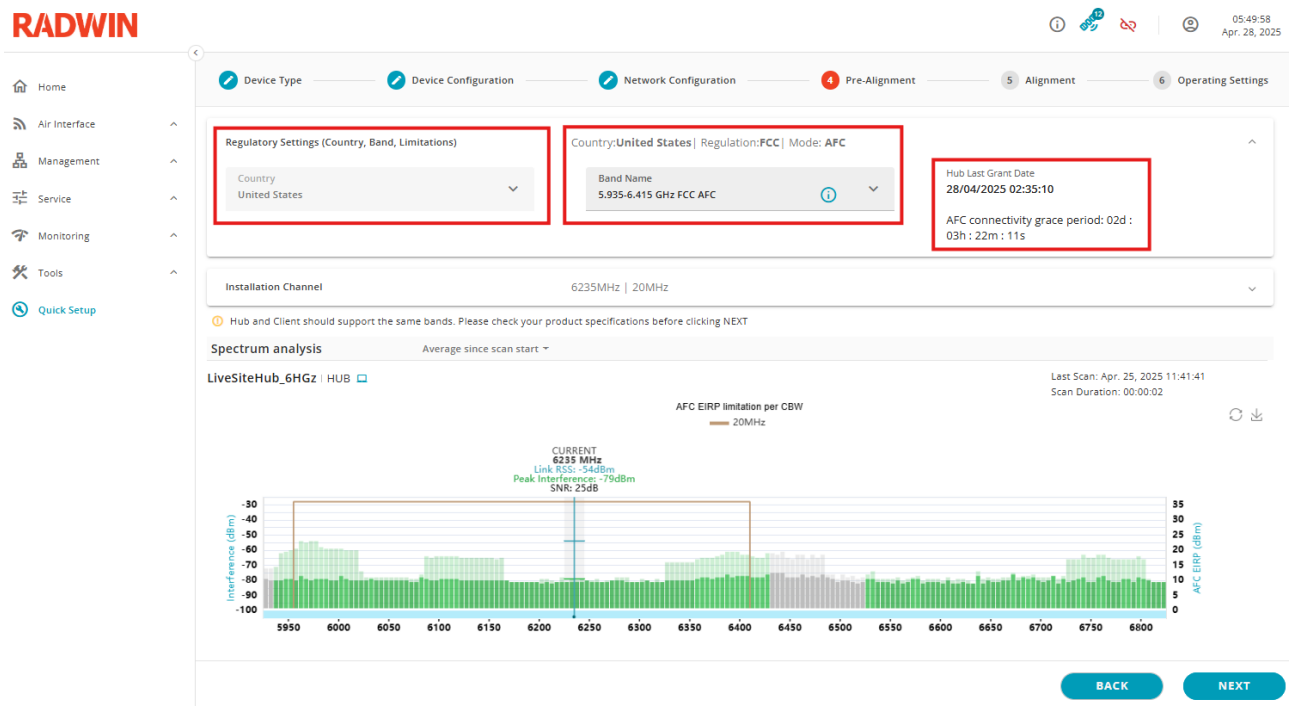


Figure 18: Installation Screen

During the first boot of the device, a spectrum scan analysis is done for 5 seconds to provide the first information regarding the environment. You can run an additional spectrum scan analysis during the quick setup if required.

Before connecting to a Client, we need to define few parameters:

Parameter	Description	Mandatory
Country	The ODU needs to know in which country it operates to use the correct regulation profile. If the ODU has a GNSS/GPS fix, the country is automatically selected by the system. If the ODU doesn't have a GNSS/GPS fix, manually select the actual country in which the ODU is installed.	Yes
Band Name	The list of bands displayed is based on the country regulations	Yes
Hub Last Grant Date (On AFC Band only)	Provides the status of the latest AFC Cloud Portal request. If succeeded, it shows the date and time of the grant.	
AFC Connectivity grace period (on AFC Band only)	Displays for how long the current AFC channel authorization could be used in case AFC server would be unreachable after the first 24h.	

After setting Country and Band, you need to select an installation channel which will be used to search for a potential Client.

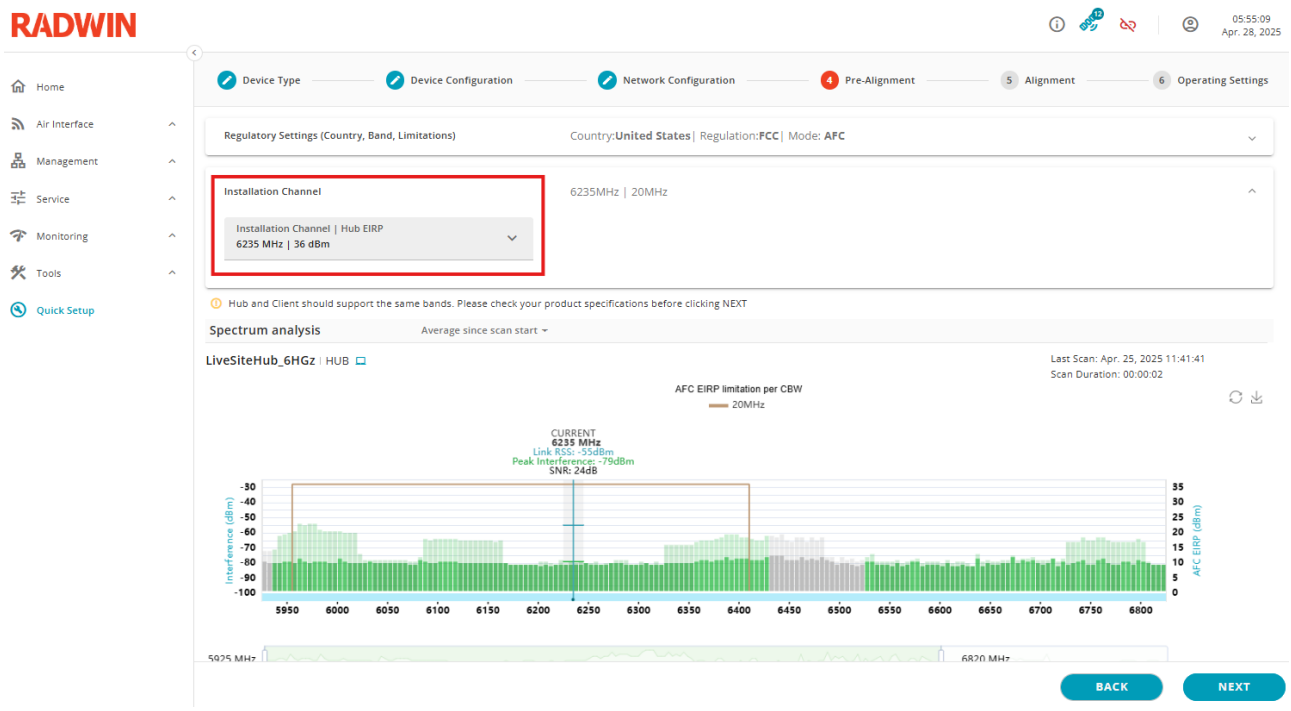


Figure 19: Installation Channel

You could select the best installation channel based on 2 parameters:

- The available maximum Tx power EIRP for this channel
- The level of interferences based on the spectrum scan

The selected channel can be previewed on the spectrum scan for more convenience.

For detailed explanation regarding the parameters on this page, see Band and Channel.

Note

Selection of a different country will result in the link being stopped if the ODU gets a GPS fix and the configured band is not permitted according to the regulation in the detected country.

When finished, you could click on NEXT.

2.5.5 Alignment

In this state, the link MCS and TX power are kept constant, allowing you to evaluate the strongest RSS while rotating the antenna to get the optimal signal level.

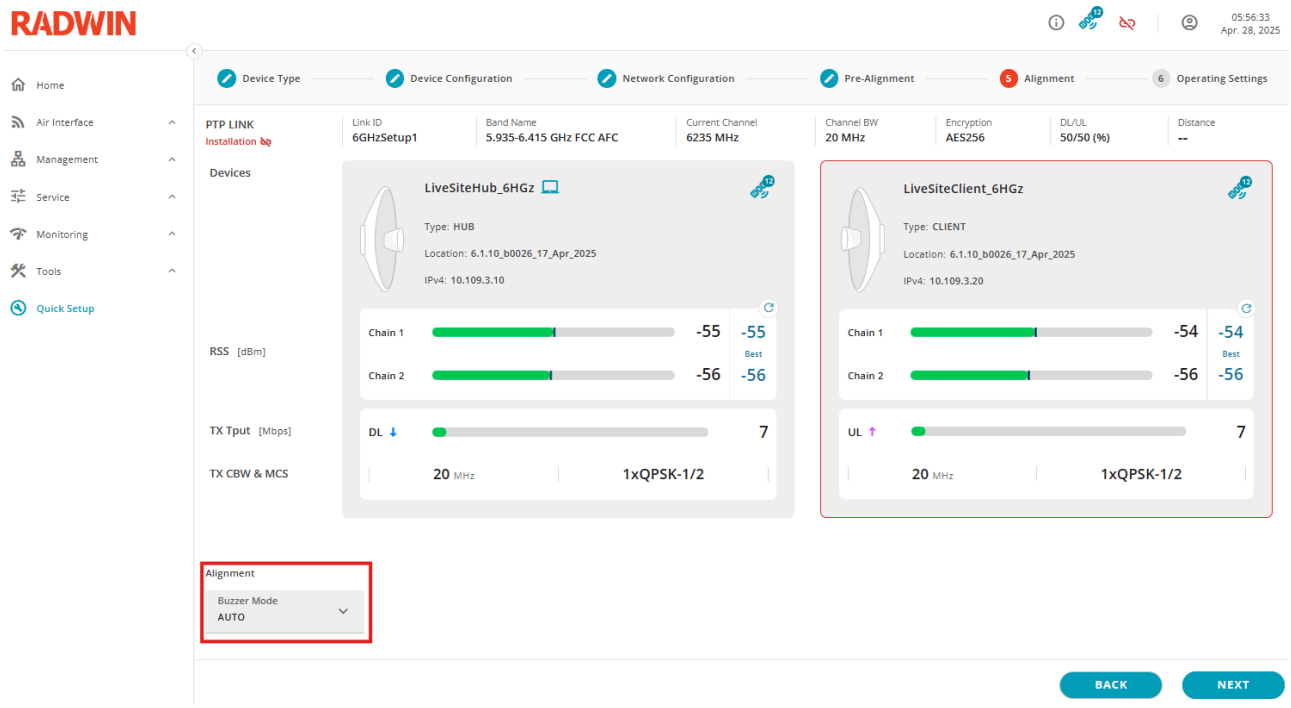


Figure 20: Aligning the Antenna

Note

When running the Quick Setup, the Buzzer is automatically set to “Auto” to help running the alignment of the antennas. For more information about the Buzzer alignment go to **Buzzer Alignment**.

1. Swivel the Client antenna from side to side.
2. Observe when the RSS in both channels reaches its maximum value.
3. When the “Best” value is the same as the current RSS value, lock the bolts. Alignment is now complete.
4. When the antenna is locked on the best RSS, click NEXT.

Note

On Client side the alignment is the final quick setup step. Next operations need to run on the Hub side.

2.5.6 Operating Settings (Hub only)

When the link between the Hub and the Client is established but not operational, the user needs to select the operating channel(s).

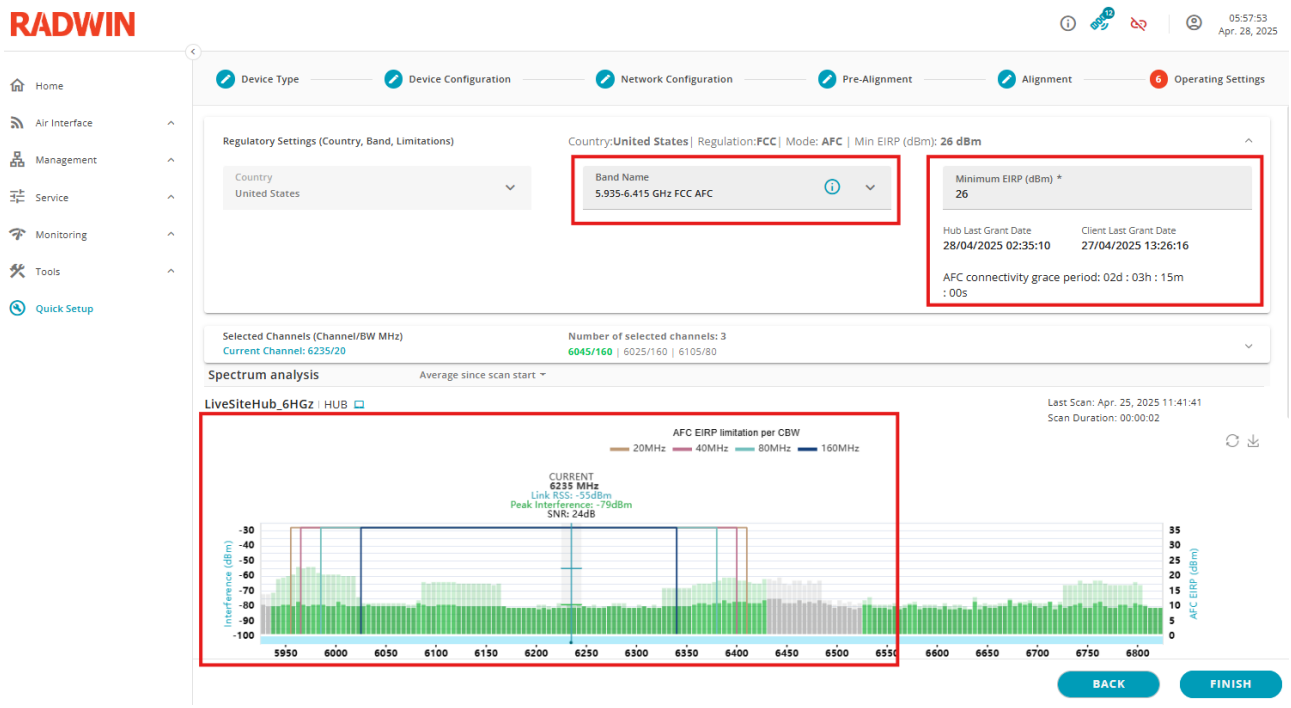


Figure 21: Operating Settings (example for AFC band)

During this phase, the user could still change the selected band.

If the selected band is an FCC/IC AFC band, then some additional information is displayed.

Parameter	Description
Country	This field shows the country in which the Hub is located. The allowed frequency bands and transmission restrictions are derived from the regulation that applies to the set country. The Client receives the operating band and channel from the Hub and doesn't require its own country setting. See Regulation Compliance for additional explanation regarding country and regulation detection. When the Hub detects a GNSS signal, it determines the country and derives the applicable regulation from that country. In this case, the county selection is disabled for the user. Once the country has been detected once, it is remembered by the Hub regardless of ODU losing GNSS signal afterwards, or of any reboots. If a GNSS signal is not detected during Hub boot, manual country selection is possible. If Hub has been activated already, the previously detected / set country will continue to be applied, and service will resume after the device boots with no need for user intervention. If the Hub hasn't been activated yet, select a country to set the frequency band for the link. This allows the Hub to start transmission.

Parameter	Description
	 After manual country selection, when GNSS signal is detected again, the Hub will automatically update the country to the one detected from GNSS. If you configured a band that now becomes not supported in the updated country, the ODU will cease transmission until you select a permitted band. Therefore, always make sure you select the correct country 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
Band Name	 The available bands are derived from the applicable regulation of the country in which the Hub is located. Each band includes a range of available channels and regulatory restrictions (TX power, max EIRP).
Minimum EIRP (AFC only)	When using an FCC AFC band, the user can define a minimum EIRP power value which ensures the link will always be available. To calculate this minimum EIRP power value, you could use our LBC inside RADWIN WinPro or our RADWIN WinPlan Cloud application.
Grant Dates and Grace Period (AFC only)	Using an FCC/IC AFC band requires the device to connect every 24h to an AFC Cloud Portal to grant a new authorization to stream on 6GHz band. This authorization is required on both sides of the link. If one or both devices failed to connect to this portal, FCC/IC authorizes the device(s) to operate on this band for an additional 24h. After these 24h, the device will need to close the link and stop any service.  When entering the AFC “grace period”, the device(s) will try to reconnect to AFC Cloud Portal every hour. A trap is generated each time the system fails to reconnect to the AFC Cloud Portal.

When the band is an FCC/IC AFC band, the AFC request results are displayed on the spectrum scan to help select the best channel. AFC information on the spectrum scan can be filtered per CBW to show only the relevant CBW information.

The user should then select the operating channel(s):

- If the band is an FCC/IC AFC, the user should select at least 2 channels to have a fallback channel in case the current channel will be forbidden by AFC Could Server in the future
- For all other bands, the user should select at least one channel

For more information about the channel selection, please refer to the paragraph Select a channel.

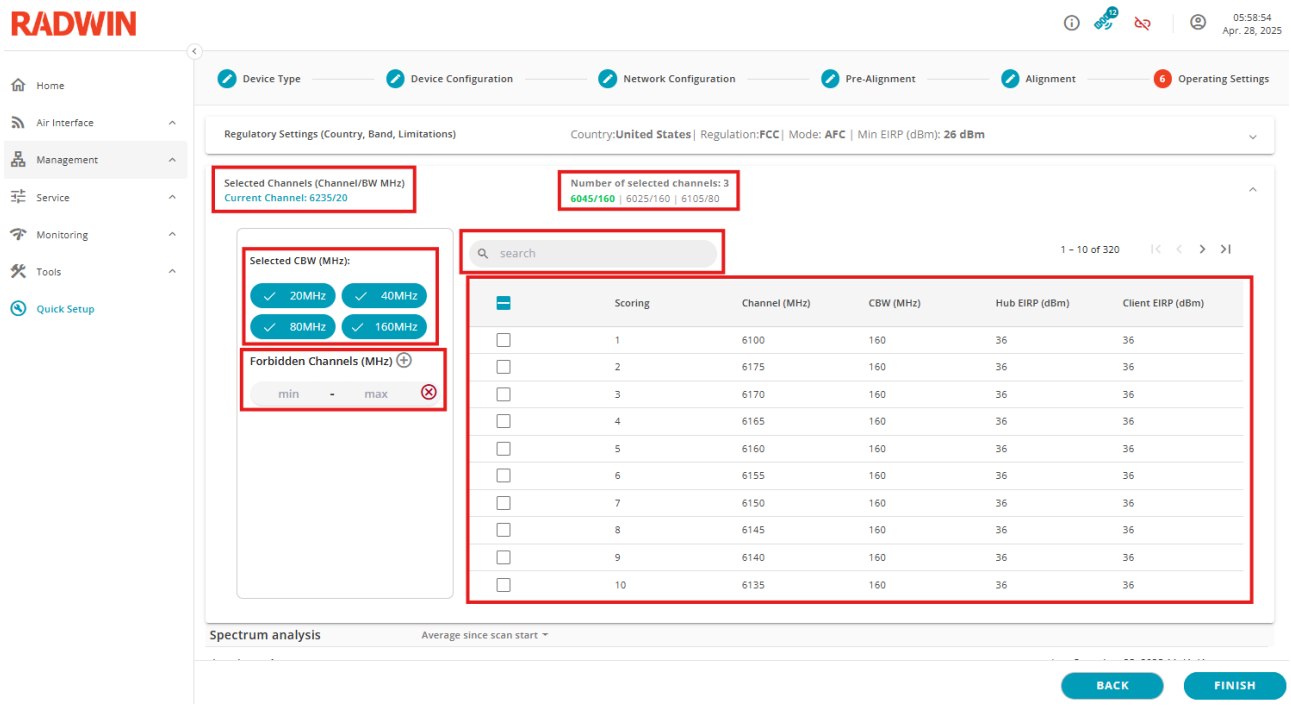


Figure 22: Selecting channels

When the operating channel(s) is(are) selected, the user could click on ‘FINISH’.

When the quick setup is finished, the user is taken to the home page.

To activate the link, the user should click on the ‘REGISTER’ button above the Client status and performance window.

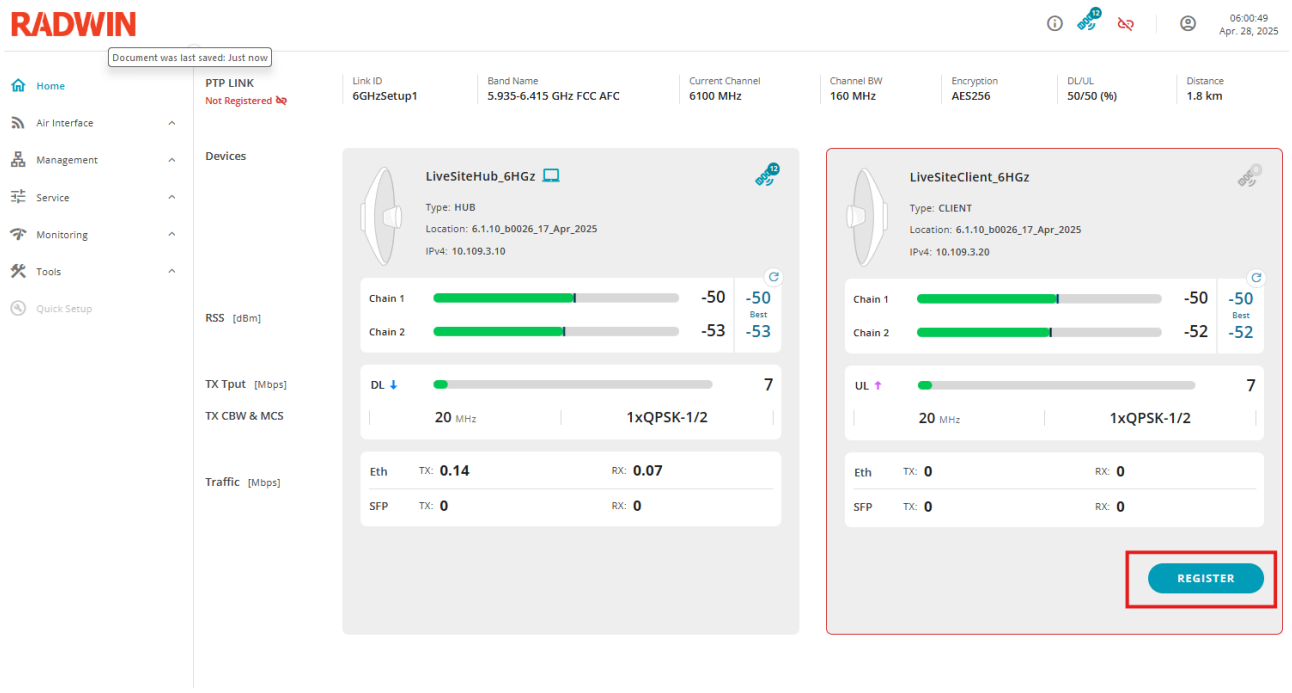


Figure 23: Register the Client

2.6 Starting and Stopping Service

For a detailed explanation regarding registered/unregistered devices, see Registered/Deregistered Devices.

To stop the service between a Hub/Client pair:

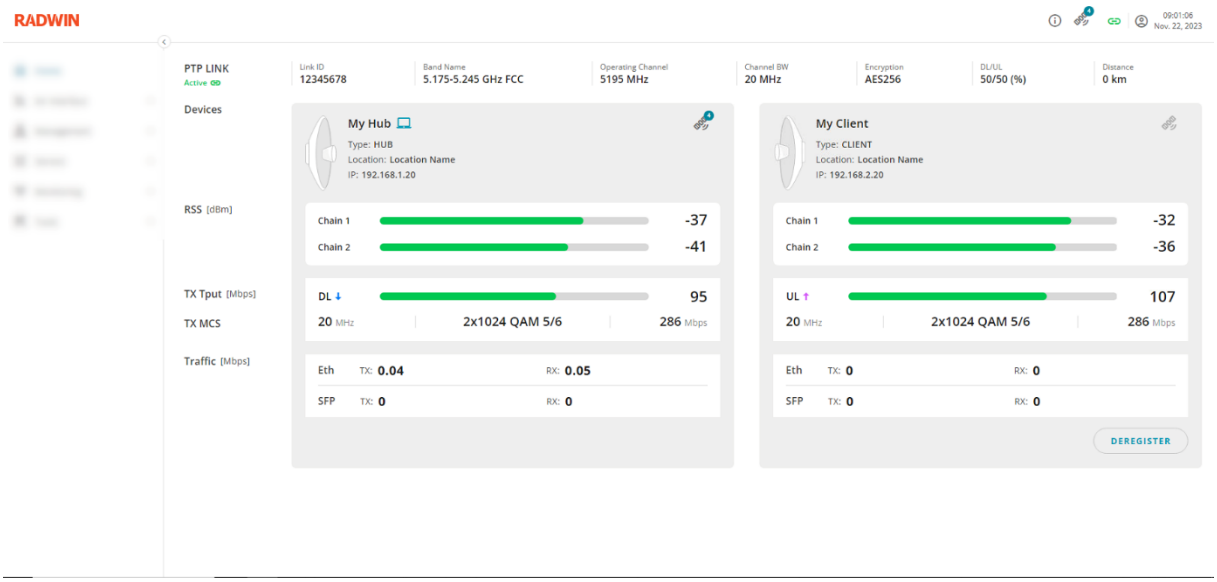


Figure 24: Starting and Stopping Service

1. On the Home page, click **DEREGISTER**:
2. Click **CONTINUE**.

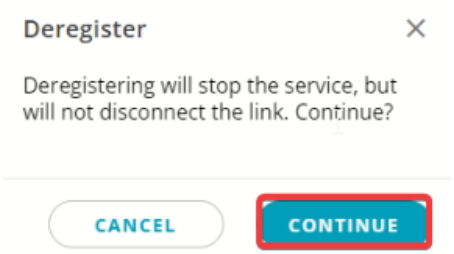


Figure 25: Deregister Client Unit

Caution

When clicking on 'DEREGISTER', the current Client will be disconnected and forgotten. The system will get back to the Quick Setup installation state.

3 Viewing Devices & Link Status

The home window is the main dashboard of the link and its devices.

In addition to a summary of general Hub/Client information displayed in other pages, the Home page displays various connection and links metrics as described below:

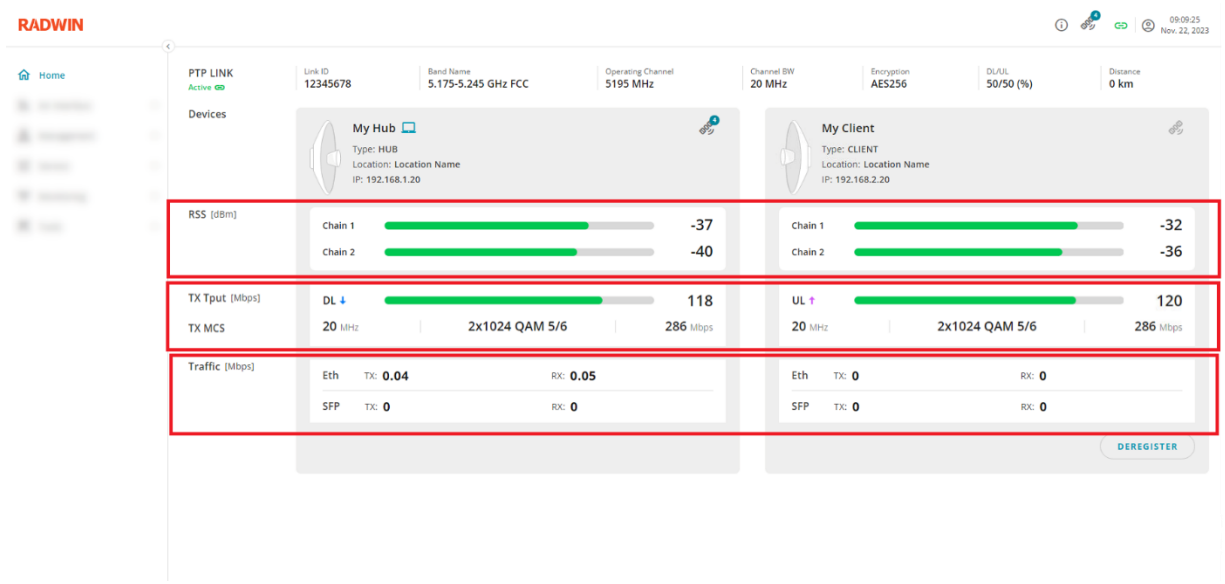


Figure 26: Viewing Devices & Link Status

Parameter	Description
RSS	Current Received Signal Strength for each RF chain (Vertical/Horizontal).
TX Tput	Displays a bar containing 2 values: Gray bar range - maximum throughput that can be achieved under current conditions (distance, CBW, UL/DL ratio) assuming highest MCS. Green bar (and number) - estimated throughput based on actual measured link conditions.
TX MCS	Displays 3 values for the last second (from left to right): Current CBW - changes dynamically according to link quality and interference. This value displays the presently used CBW. Current MCS - changes dynamically according to link quality and interference. This value displays the presently used MCS. Air interface rate - represents the modem speed over the air that corresponds to the current MCS and CBW.
Traffic	The row shows the actual traffic entering / exiting the device over the wired interface. The maximum traffic (going over the air) can reach up to the Tput (green bar) value.

4 Configuring the Air Interface Parameters

4.1 Configuring the Link Security

In the **Link Security** window, you can:

- Configure Link ID.
- Change link password

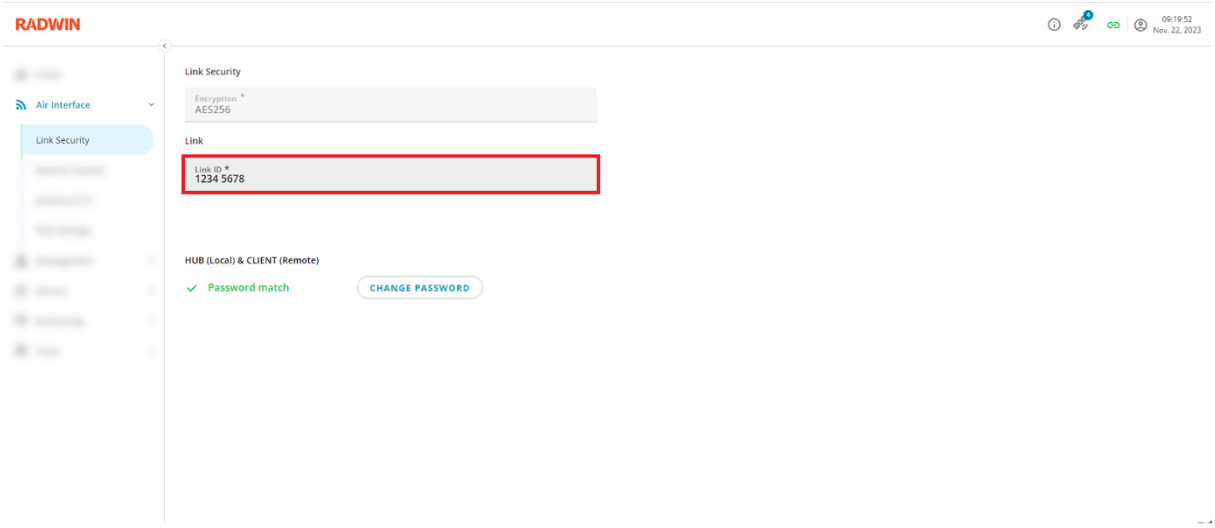


Figure 27: Configuring the Link Security

4.1.1 Changing the Link ID

The following parameters are available in the page:

Parameter	Description	Mandatory
Encryption	Displays the current air interface encryption (2000E always uses AES256)	Read only
Link ID	Enter 8-24 characters (English letters, numbers and "_" are allowed)	Yes

Link ID is similar to SSID in WiFi. During link establishment, the Hub's link ID is published in the HUB's beacon. When the Client identifies a beacon, it will attempt to connect to that beacon. The Hub will accept / reject the Client's connection based on the match between the link ID of the Client and the Hub.

If a registered link drops, the Client will only re-connect to a beacon with link ID matching its own link ID. In case the link ID of either side was changed while the link was down, the link will fail to be reestablished due to link ID mismatch.

Note

When the link is Active (the Client is registered), it is possible to change the link ID only from the Hub side – on the Client side the Link ID field is greyed out. When the Client is not registered or de-registered, you could change the Link ID also on the Client side. When the link is active and you edit the link ID from the Hub side, the link ID of Hub and Client are updated together.

The first 4 characters of the link ID are designated as the “Network ID”.

When configuring a Client unit, following options are available for Link ID setting:

Client Link ID setting	Client behavior
Empty	Client will connect to any Hub unit
Network ID (first 4 characters)	Client will only connect to Hub unit with matching Network ID
Full link ID	Client will only connect to Hub unit with matching full Link ID

4.1.2 Changing the Link Password

Changing link password will improve link security. All 2000E units are shipped with a default link password. Once the link password is updated, in order to establish a new link or to replace a unit in the existing link, the same link password must be set on both units.

Link password can be updated locally on each unit before installation.

On an existing link, from either hub or client unit.

New password should have at least 8 characters, any of the following character types can be used:

English letters

Special characters

Numbers

1. In the Link Security page, click **Change Password**.
2. Enter the old password in **Old Password** field (default password is **Wireless Bridge**)
3. Enter the new password in the **New Password** and **Confirm Password** fields.
4. Click **Change**.

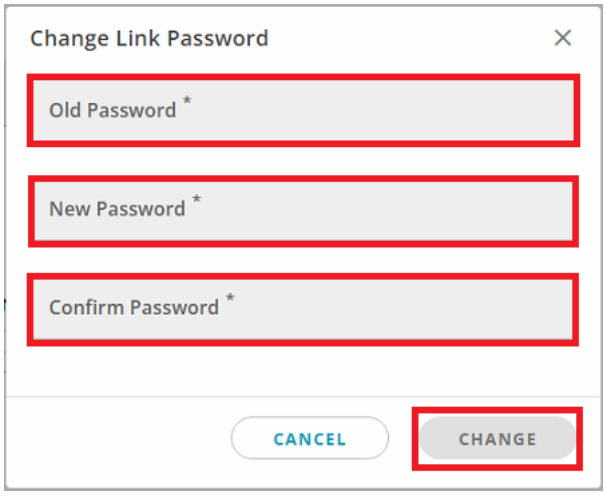


Figure 28: Changing the Link Security Password

4.2 Band and Channel

The Band and Channel window enables you to configure the Country, Band Name, Channel Bandwidth, and Operating Channel.

The Spectrum Analyzer gives you the ability to analyze the signal on the full band to use the best available frequency.

When the link between the Hub and the Client is active, each device can retrieve the spectrum scan data from the other and display it one above the other.

If you want to run a spectrum analysis, this could be done only on the local device. To run it on the second device, you will need to log into it.

Each spectrum scan is independent from the other, the zoom and scroll functions need to be used on both independently to check specific parts of the scan.

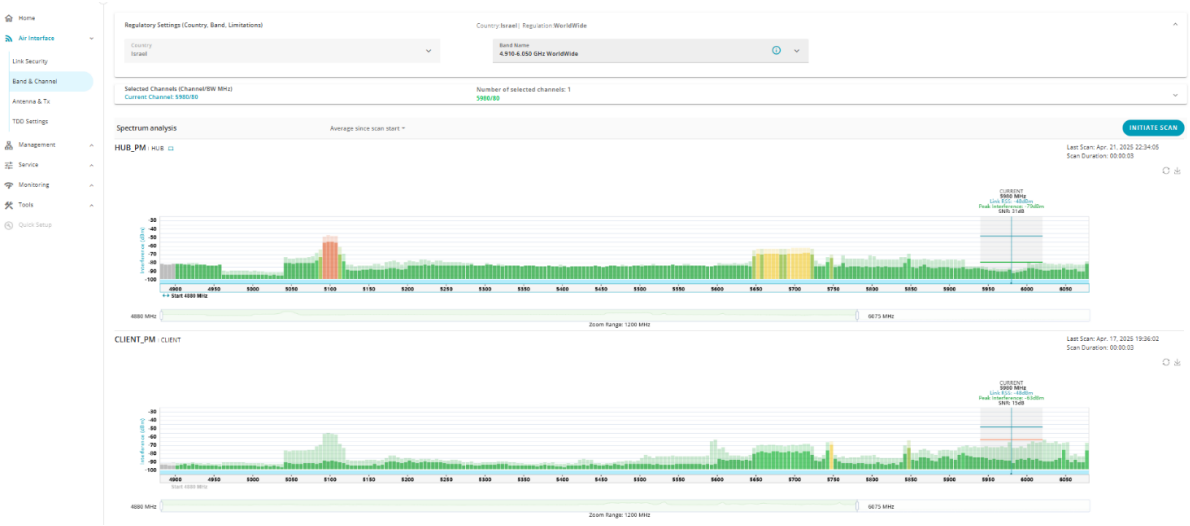


Figure 29: Band and Channel

4.2.1 Regulatory Settings

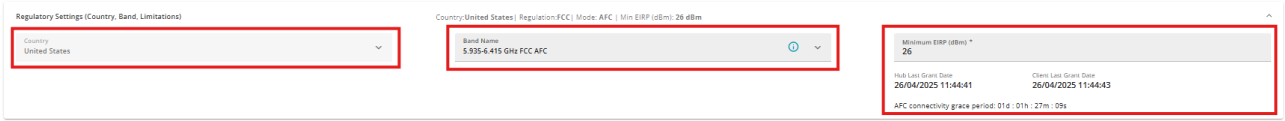


Figure 30: Regulatory Settings

The Band and Channel parameters are described in the following table:

Parameter	Description
Country	This field shows the country in which the Hub is located. The allowed frequency bands and transmission restrictions are derived from the regulation that applies to the set country. The Client receives the operating band and channel from the Hub and doesn't

Parameter	Description
	require its own country setting. See Regulation Compliance for additional explanation regarding country and regulation detection. When the Hub detects a GNSS signal, it determines the country and derives the applicable regulation from that country. In this case, the county selection is disabled for the user. Once the country has been detected once, it is remembered by the Hub regardless of ODU losing GNSS signal afterwards, or of any reboots. If a GNSS signal is not detected during Hub boot, manual country selection is possible. If Hub has been activated already, the previously detected / set country will continue to be applied, and service will resume after the device boots with no need for user intervention. If the Hub hasn't been activated yet, select a country to set the frequency band for the link. This allows the Hub to start transmission.  Caution After manual country selection, when GNSS signal is detected again, the Hub will automatically update the country to the one detected from GNSS. If you configured a band that now becomes not supported in the updated country, the ODU will cease transmission until you select a permitted band. Therefore, always make sure you select the correct country 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
Band Name	 Note The available bands are derived from the applicable regulation of the country in which the Hub is located. Each band includes a range of available channels and regulatory restrictions (TX power, max EIRP).
Minimum EIRP (AFC only)	When using an FCC AFC band, the user can define a minimum EIRP power value which ensures the link will always be available. To calculate this minimum EIRP power value, you could use our LBC inside RADWIN WinPro or our RADWIN WinPlan Cloud application.
Grant Dates and Grace Period (AFC only)	Using an FCC AFC band requires the device to connect every 24h to an AFC Cloud Portal to grant a new authorization to stream on 6GHz band. This authorization is required on both sides of the link. If one or both devices failed to connect to this portal, FCC authorizes the device(s) to operate on this band for an additional 24h. After these 24h, the device will need to close the link and stop any service.  Note When entering the FCC "grace period", the device(s) will try to reconnect to AFC Cloud Portal every hour. A trap is generated each time the system fails to reconnect to the AFC Cloud Portal.

4.2.2 Selected Channels

Through the selected channels, a user could select one of multiple channels. Currently the selection of multiple channels is used only with FCC AFC band in case the current channel or other selected channels have been removed from the authorized list or if their authorized EIRP power is less then the minimum defined by the user.

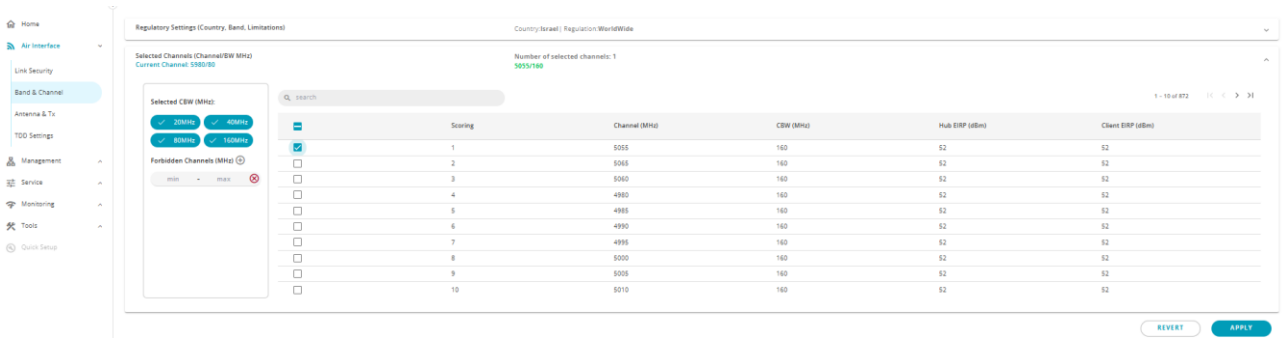


Figure 31: Selected Channels Menu

Parameter	Description
Channel Bandwidth	This is the required channel bandwidth (CBW) on which the link will operate. The actual CBW is dynamically adapted according to link conditions (Automatic CBW selection). Note: The available CBWs are determined by the selected band and are derived from the applicable regulation of the country in which the Hub is located.
Selected Channels	The actual frequency on which the link with the Client will be established is always displayed in green in the list of selected channels.

Select a channel

When selecting a channel different information is provided to help select the best possible channel.

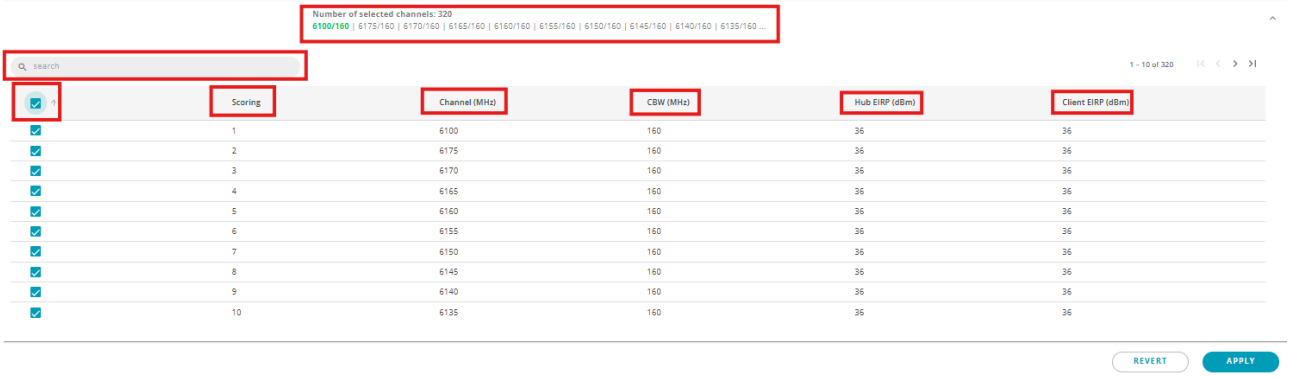


Figure 32: Select a Channel

Parameter	Description
Number of selected channels	It displays the total number of selected channels and the channel/CBW list. Only the 10 first selected channels are displayed.
Search	It allows you to search inside all the selectable channels for a specific channel.
Select all	The checkbox allows you to select all the selectable channels.
Scoring	RADWIN is providing channel scoring based on several parameters to help customers to always select the best possible channel. The scoring is based on dat from both sides of the link: local interferences, maximum modulation on this distance, authorized maximum EIRP power.
Channel (MHz)	Channel Frequency.
CBW (MHz)	Channel BandWidth.
Hub EIRP (dBm)	Required on FCC AFC band – displayed any EIRP restriction provided by the AFC Cloud Portal for a specific channel/CBW.
Client EIRP (dBm)	Required on FCC AFC band - displayed any EIRP restriction provided by the AFC Cloud Portal for a specific channel/CBW.

When finalizing the selection, the user should click on 'Apply' to validate the new channel list.

Selected CBW

The user can filter the list of channels into the right table by Channel BandWidth. The user can deselect one or several CBW to reduce the number of channels displayed in the table.

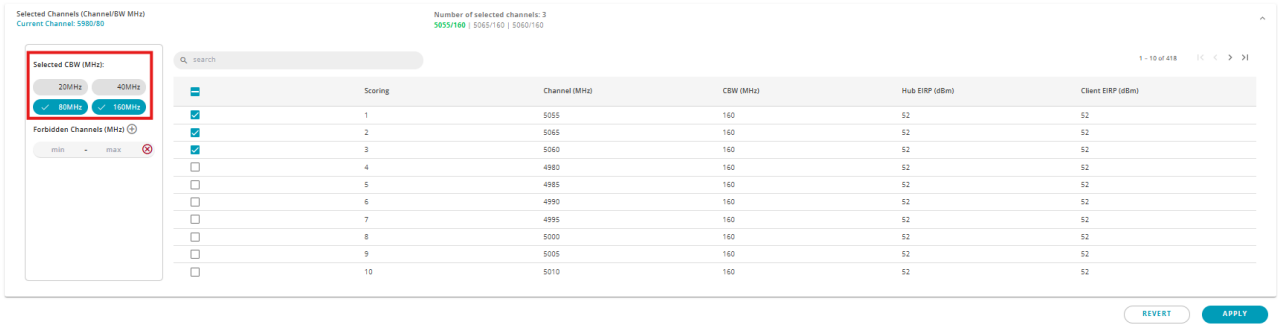


Figure 33: CBW Filter

Forbidden Channels

If some portions of the band cannot be used by the device, it is possible to add channel range filters to remove these channels from the main table.

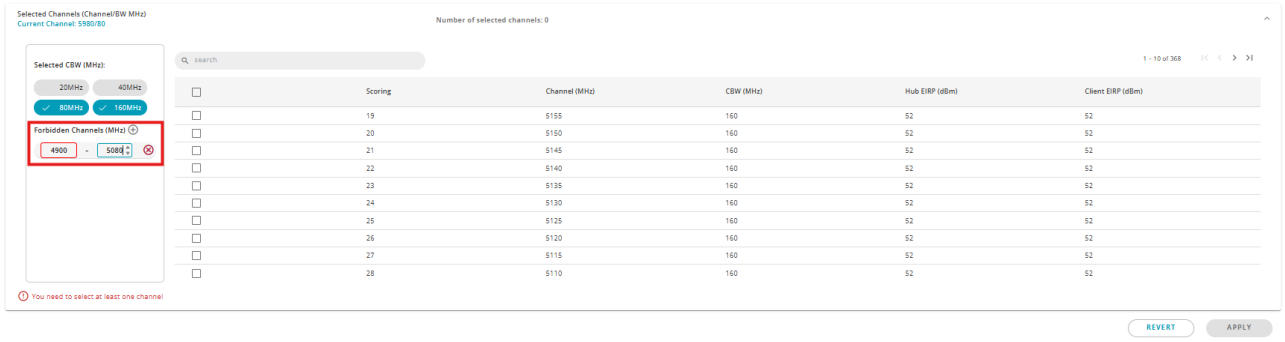


Figure 34: Forbidden Channels Filter

4.2.3 Spectrum Analysis

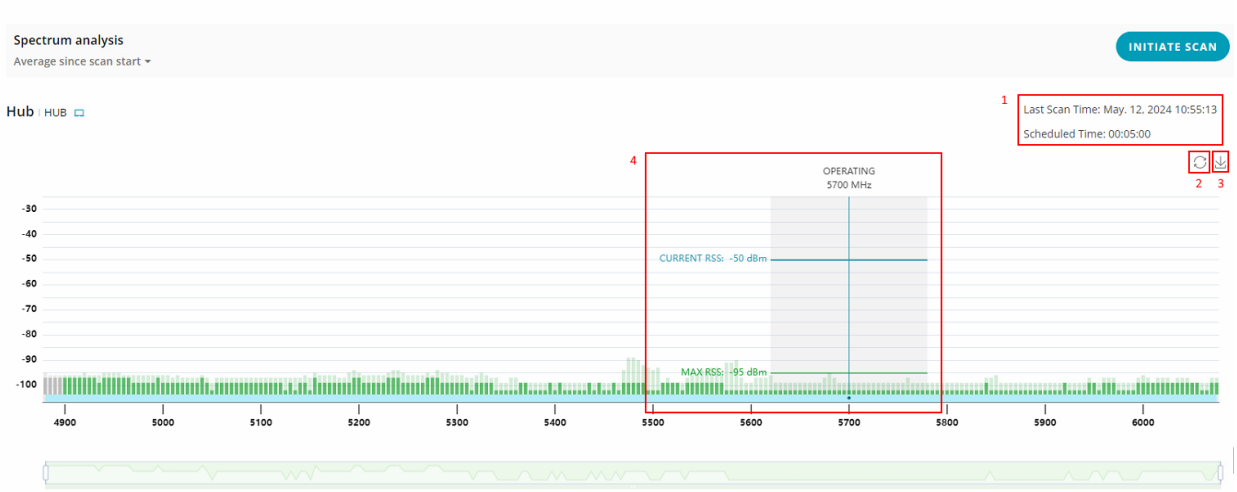


Figure 35: Offline Spectrum Scan

The spectrum analyzer allows you to analyze the hub environment to find the more suitable frequency for your operations. The spectrum analyzer is working offline which means that connection with the client/hub is suspended during the spectrum scan.

The spectrum analysis window provides several information:

1) The date of the last scan or if the scan is running, the time you started it with the elapsed time since you started or the total duration of the last scan.
2) The refresh button allows you to update the 'Current RSS' and get back to default view.
3) The download button allows you to capture the status of the present scan as a .png picture.
4) The current channel area, specifying the bandwidth (20, 40, 80 or 160Mhz) and the Current (Link) RSS and the Max RSS (=Noise RSS).

Starting a new scan

You could start at any moment a new scan by clicking on the 'Initiate Scan' button.

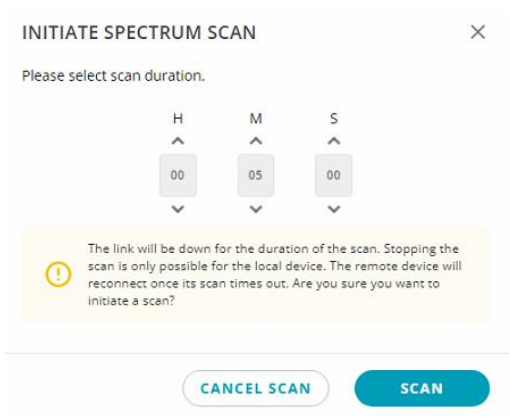


Figure 36: Start a new Spectrum Scan

In the pop-up window, you can select the duration of the scan.

Caution

Remember that starting a new scan will suspend the link for the duration of the scan.

You can then cancel the operation by clicking on the 'x' in the upper right corner or by clicking on the 'Cancel Scan' button.

To approve and launch the scan, you need to click on the 'Scan' button.

During a scan

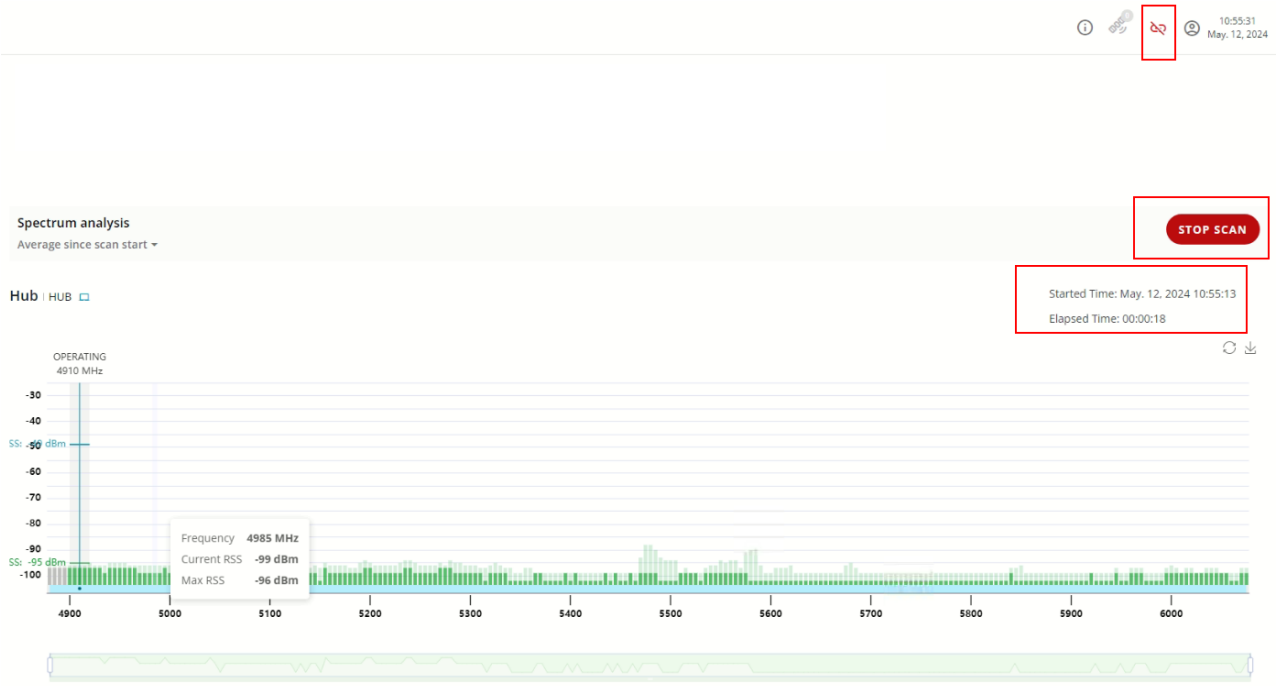


Figure 37: Running Spectrum Analysis

During the scan, the link icon in the upper right corner shows that the connection is not active.

At any moment, you can stop the scan by clicking on the 'Stop Scan' button.

You could check the progress of the scan through the 'elapsed time'.

Analyzing the Scan result

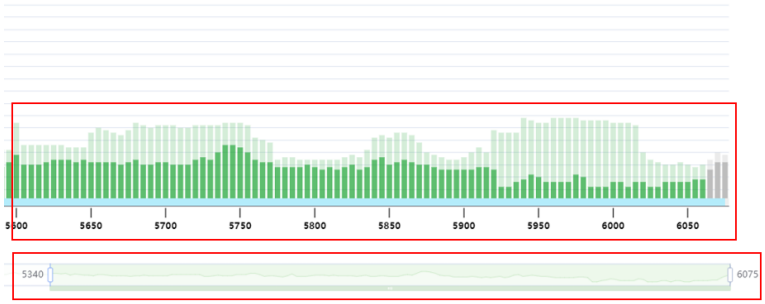


Figure 38: Spectrum Analysis Result Window

In the bottom of the spectrum analysis result, you could use the focus stretching line to zoom in and out on a specific portion of the spectrum. By clicking on refresh, you will get back to full spectrum view. When hoovering on the stretching line, you could see both ends values.

In the upper portion of the spectrum analysis result you could check the result of the spectrum scan for each frequency. The result provides a 5MHz resolution view.

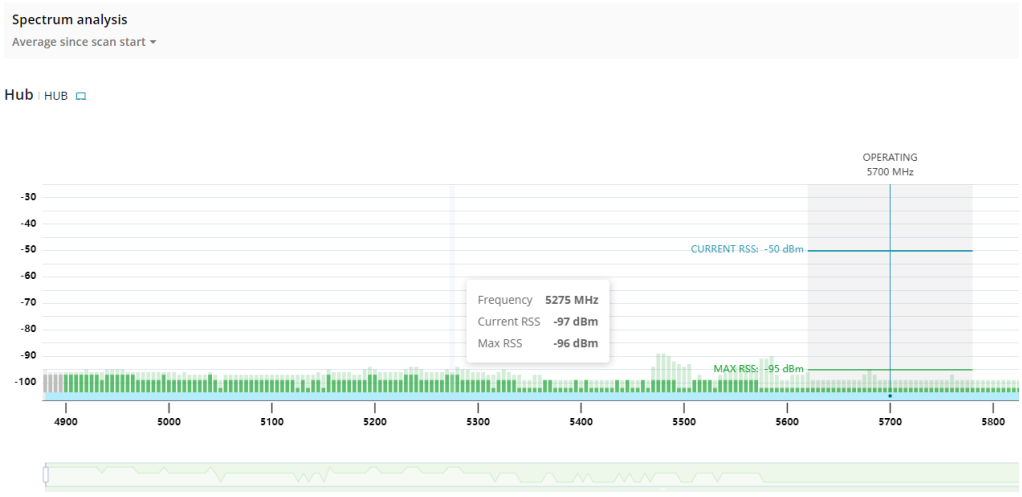


Figure 39: Analyzing the spectrum scan result

The color code used for the spectrum scan is as follow:

Color	Explanation
Ligh Green	Maximum/Peak observed during the scan

Dark Green	During scan: Current reading After scan: Average value observed during the scan
Grey	Unusable/not-scanned frequencies
AFC Results (Only for AFC band)	Per CBW, the AFC results are displayed over the spectrum results

When hoovering over the spectrum scan results, you can see the current RSS and Max RSS (interfering signals), considering 5MHz resolution.

4.3 Configuring the Antenna & TX Power

The Antenna and TX window enables you to configure Antenna gain (for external ODU), cable gain, and TX power. Based on the values you enter the system calculates the max TX power allowed that complies with the regulation limit in the selected frequency band.

Current actual TX power, the EIRP limit according to selected band regulation, and the current transmitted EIRP are displayed.

Note

The remote ODU info / settings appear only when the link is active.

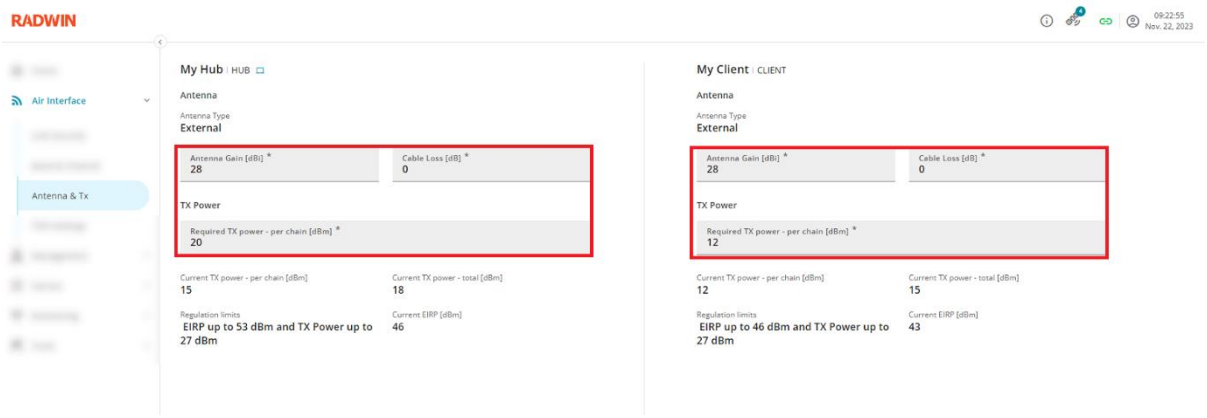


Figure 40: Configuring the Antenna & TX Power

The Antenna and TX parameters are described in the following table:

Parameter	Description	Mandatory
Antenna Type	Integrated or External	Read only
Antenna Gain	Required for External, read only for Integrated antenna	Yes
Cable Loss	For External antenna only	Yes
Max TX Power - per chain	Specify the maximum TX power per antenna chain (0 - 25dBm). The actual TX power is limited by regulation.	Yes
Current TX power - Per chain	The current TX power per chain, adjusted to support both regulation and current modulation.	Read only
Current TX power - Total	The current combined TX power (always 3db higher than TX power per chain), adjusted to support both regulation and current modulation.	Read only
Regulation limits	Maximum regulation allowed EIRP and TX power in the selected band	Read only
EIRP	Actual EIRP calculated from the current TX power, antenna gain, cable loss	Read only

4.4 Configuring TDD Settings

The TDD Setting window enables you to configure the ratio allocated for downlink (Hub->Client) and uplink (Client->Hub) and to enable/disable on the Hub side the Hub Site Sync.

For more information regarding the UL/DL ratio, see TDD (UL/DL) Ratio.

4.4.1 DL/UL Ratio

To configure the DL/UL Ratio:

1. Move the slider to select the required ratio from the following options:
    a. 75/25
    b. 50/50
    c. 25/75

Figure 41: Configuring the TDD

2. Click **APPLY**.

4.4.2 Enable/Disable the Hub Site Sync

When GPS Jamming is used in a conflict area, this could result in Hub Site clock synchronization issues.

In this case we recommend you disable the Hub Site Sync through GPS.

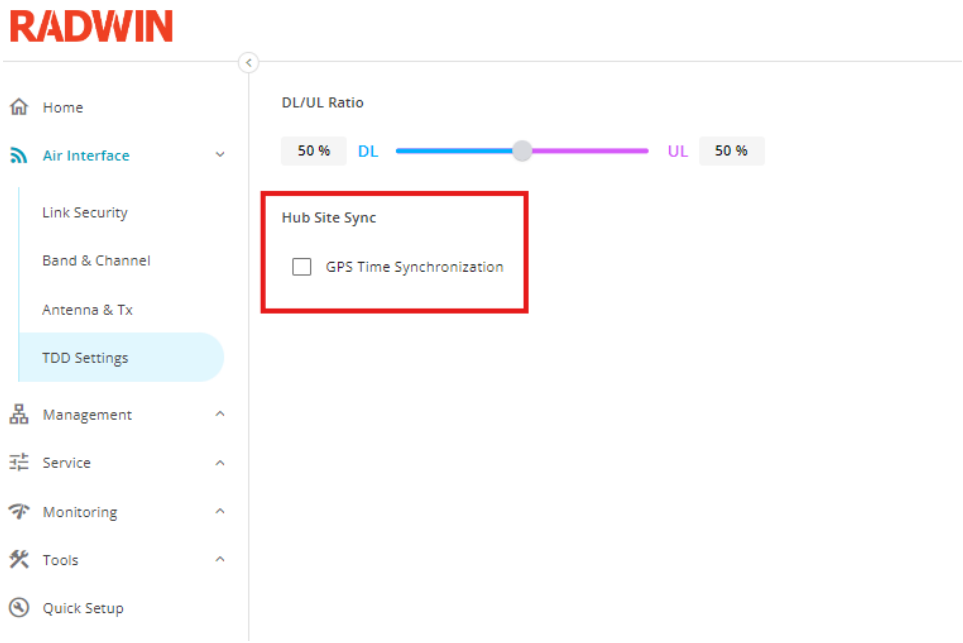


Figure 42: Disabling Hub Site Sync

5 Configuring ODU Management Parameters

5.1 Configuring General ODU Settings

Configure the following parameters for both the Hub and Client ODUs:

Note

The remote ODU info / settings appear only when the link is active.

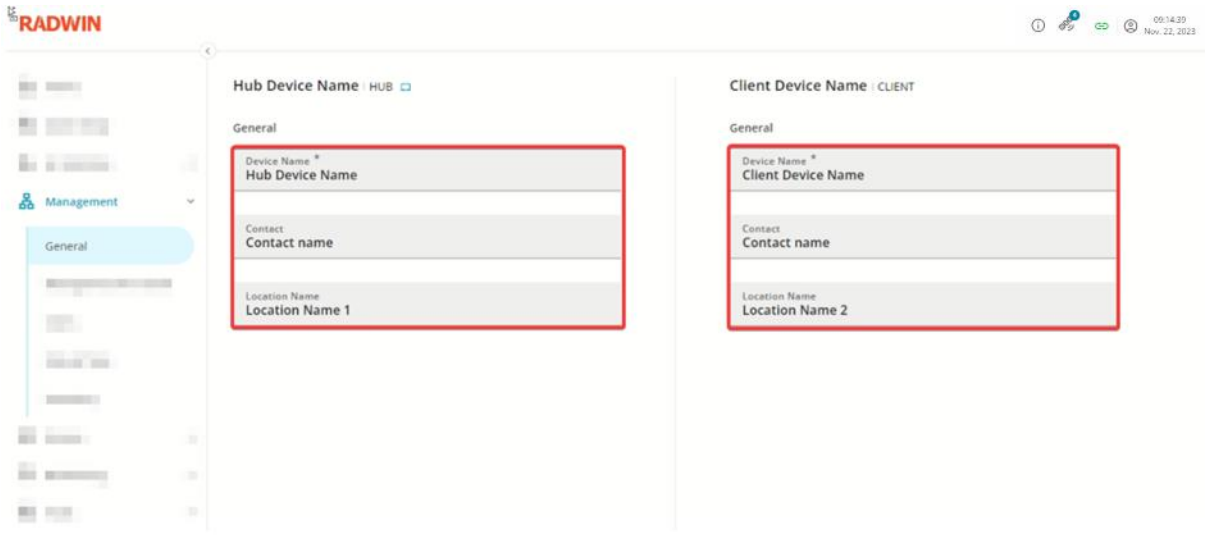


Figure 43: Configuring General ODU Settings

Parameter	Description	Mandatory
Device Name	Descriptive name to identify the device	Yes
Contact	Description to identify the person to be contacted (customer, maintenance contact etc.)	No
Location Name	Description to identify the physical location	No

5.2 Configuring the Management IP and VLAN

Configure the following parameters for both the Hub and Client ODUs:

Note

The remote ODU info / settings appear only when the link is active

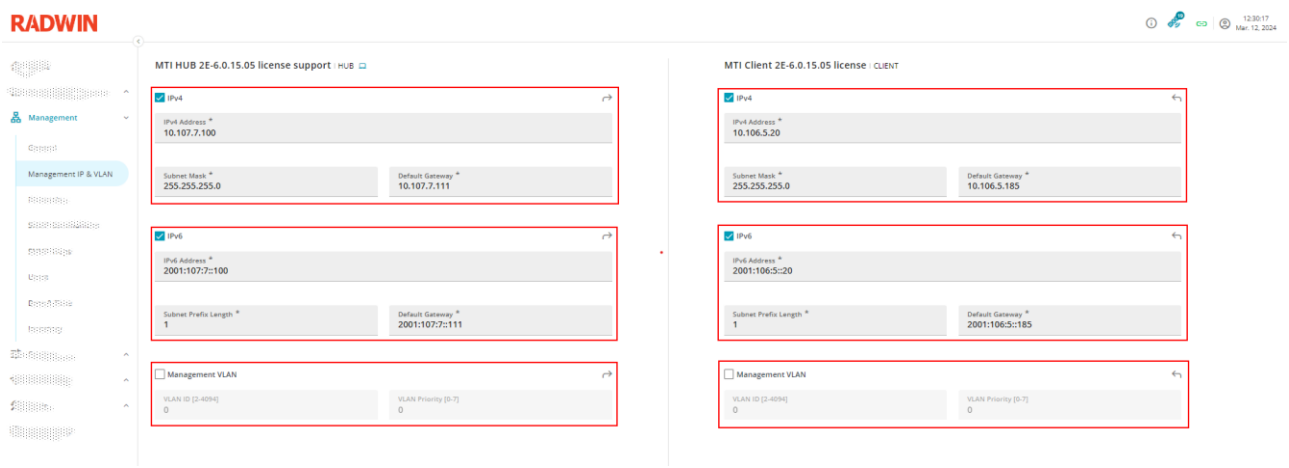


Figure 44: Configuring the Management IP and VLAN

Parameter	Description	Mandatory	Default value
IPv4 Section			
IPv4 Address	IPv4 address for management interface	Yes	**10.0.0.120**
Subnet Mask	IPv4 subnet mask for management interface	Yes	**255.255.255.0**
Default Gateway	IPv4 address default gateway for management interface	Yes	**0.0.0.0**
IPv6 Section			
IPv6 Address	IPv6 Address for management interface	No	
Subnet Prefix Length	Number of bits used by the prefix	No	**1**
Default Gateway	IPv6 address default gateway for management interface	No	
Management VLAN	Enable/disable VLAN tagging for management traffic	No	**Disabled**
VLAN ID	Supported values: 2-4094	Parameter	
VLAN Priority	Supported values: 0-7	Parameter	

Note

You can copy IPv4, IPv6 and/or VLAN values from one side of the link to the other side by clicking the Copy arrow button. Make sure you don't configure the same IP address for both devices

5.3 Configuring the Protocols

Configure the following parameters for both the Hub and Client ODUs:

Note

The remote ODU info / settings appear only when the link is active

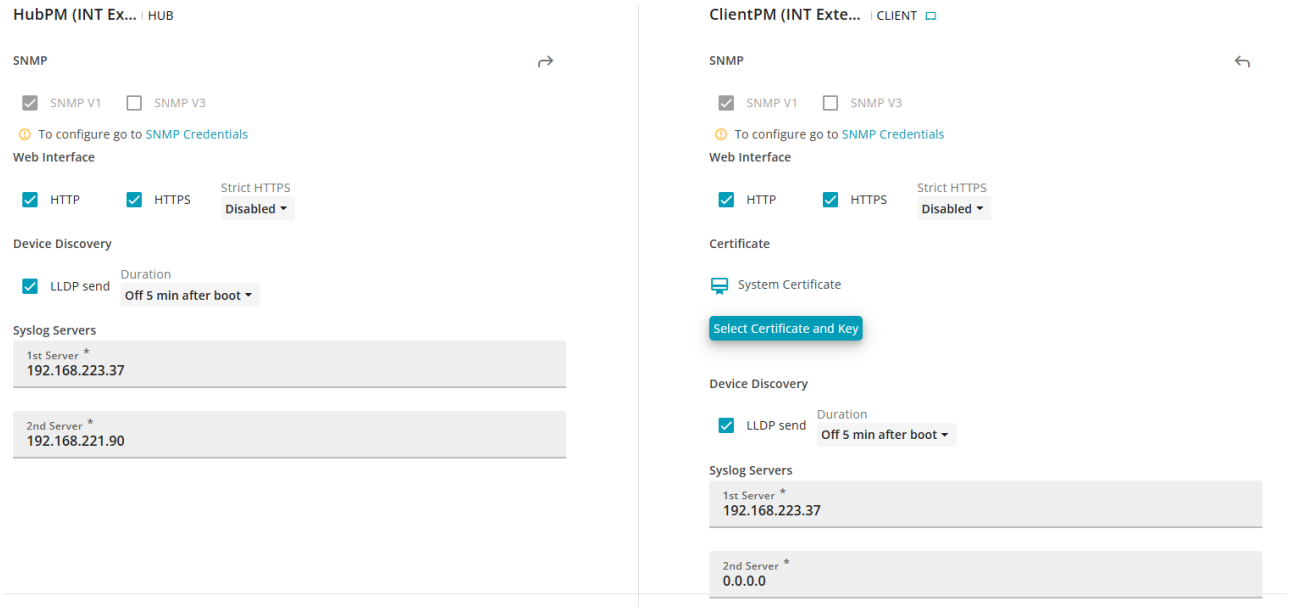


Figure 45: Configuring the Protocols

Parameter	Description	Mandatory	Default value
SNMP	**Control SNMP version and parameters**		
SNMPv1	See status of SNMPv1		**Enabled**
SNMPv3	See status of SNMPv3		**Disabled**
Link to SNMP Credentials	Configuration of SNMP parameters should be done through SNMP Credentials page		
Web Interface			
HTTP	Access web interface through HTTP		**Enabled**
HTTPS	Access web interface through HTTPS		**Disabled**
Strict HTTPS	Restrict web interface access through HTTPS only		**Disabled**
Certificate			
Select Certificate and Keys	Button to load SSL certificate and key to the web interface for HTTPS		
Device Discovery	**Control LLDP device discovery parameters**		

Parameter	Description	Mandatory	Default value
LLDP send	Enable/disable sending LLDP packets for discovery	No	**Enabled**
	Time limit for LLDP (**Always on** / **Off 5 min after boot**)	Parameter	**Off 5 min after boot**
Syslog Servers			
1st server	Can be filled with IPv4 or IPv6 address	No	**0.0.0.0 (disabled)**
2nd server	Can be filled with IPv4 or IPv6 address	No	**0.0.0.0 (disabled)**

5.3.1 Configuring and using HTTPS

To use HTTPS with your device, first enable it:

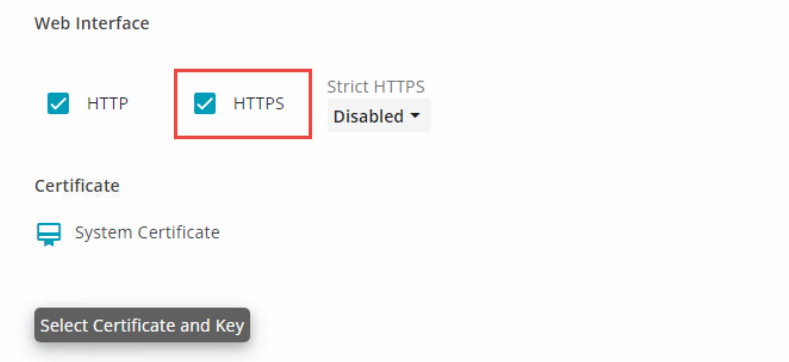


Figure 46: HTTPS with default certificate

For better security, you can disable HTTP to force the Web UI to use HTTPS only.

When HTTP is disabled, the HTTP session behavior depends on Strict HTTPS setting:

Mode	**HTTP session behavior**
Strict HTTPS disabled (default)	Session is redirected from port 80 (HTTP) to port 443 (HTTPS)
Strict HTTPS enabled	HTTP port 80 is closed

By default, RADWIN 2000 E has a factory default embedded certificate and key allowing to use HTTPS connection protocol. When using your web browser, the following message could appear when trying to connect to the device:

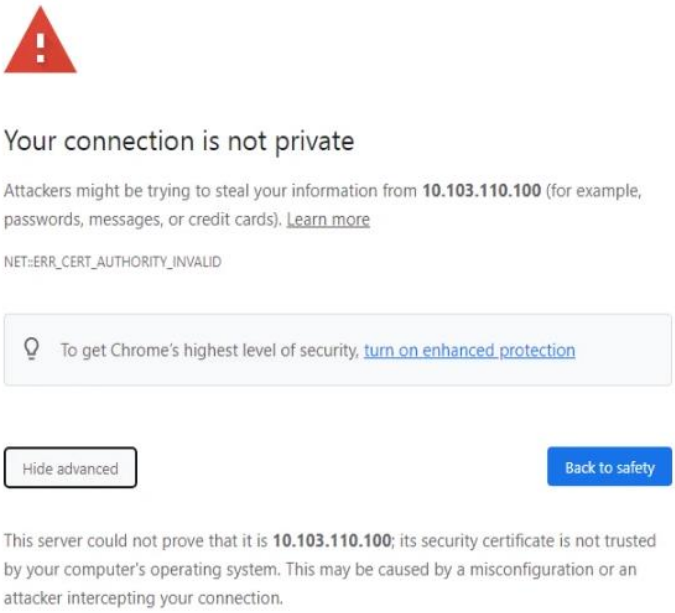


Figure 47: HTTPS with default certificate

Because the default certificate is not signed by an official certificate authority, this message could appear in your browser. Yous connection is still secured but based on unofficial authority.

If you want to avoid these messages when logging into the device or if you are using your own certificate authority, you can load your own certificate and key into the device.

You will need an SSL or TLS certificate installed on your web interface. The SSL/TLS certificate may be provided by Web Hosting Provider, or you can request it from a Certificate Authority. SSL/TLS certificates may need to be renewed periodically (according to validity set in the certificate).

Install a new certificate and key

By clicking on the "Select Certificate and Key" button, you can load your own certificate and key to the local device.

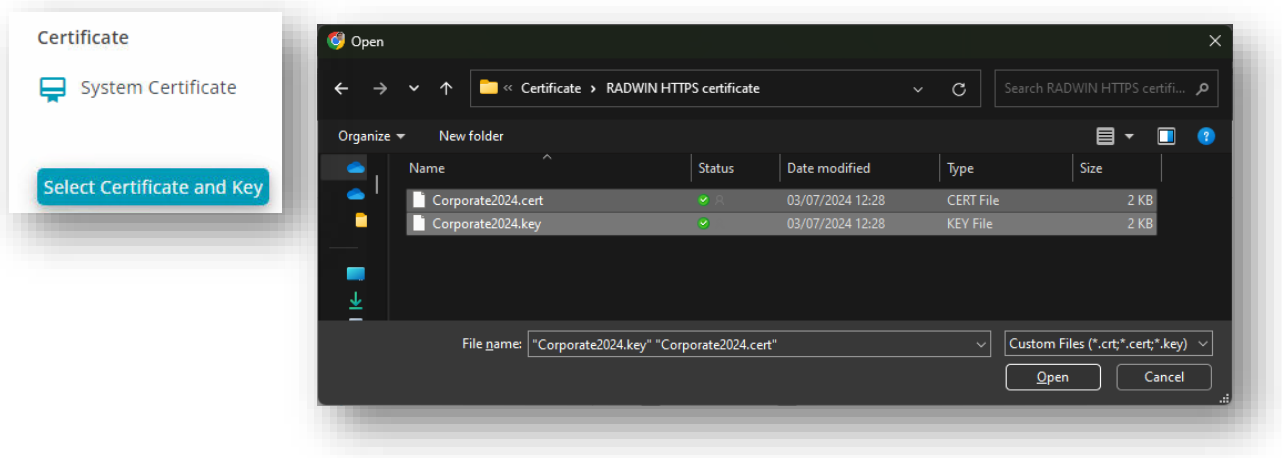


Figure 48: Select a new certificate and key

Certificate and key files must respect the following rules:

The file names should follow these naming rules:

- 1-32 characters long
- letters regular or cap allowed
- numbers allowed
- "_", "-", "." characters allowed
- The certificate file must have an extension ".cert" or ".crt"
- The key file extension must be ".key"

When loaded, the device will check the validity of the certificate and the key.

If both are validated, a validation icon will be displayed on the side of the files.

Figure 49: Approved certificate and key

Only one certificate and key can be loaded on the device. If you need to replace the certificate and the key, you should click on the bin icon to remove them from the device.

5.3.2 LLDP implementation

LLDP is a standard protocol for local discovery of network topology and devices.

RADWIN 2000E implementation of LLDP:

Each unit sends LLDP frames to Ethernet ports to advertise itself to connected devices

Link is transparent for LLDP frames sent by connected devices

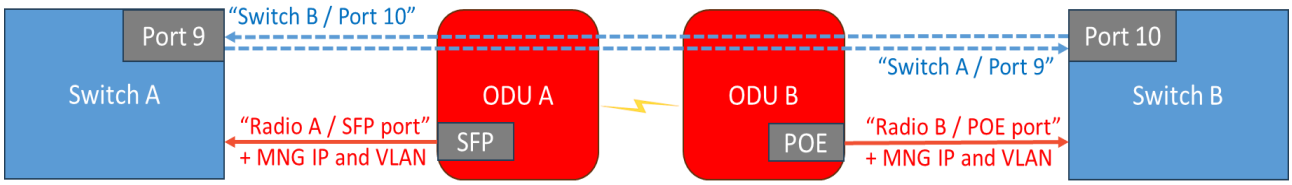


Figure 50: LLDP flow

The following information is advertised by 2000E via LLD:

LLDP TLV	Description
Chassis ID	Ethernet MAC address
Port Subtype	Interface name such as **Two_FiveGigabitEthernet0**
Port Description	Port description such as **2.5Gbps_Ethernet_VID_201** to identify the connected port and management VLAN ID (if management VLAN is configured)
System name	Device name set in General configuration screen
Management Address	Management IP address

5.3.3 Syslog Servers

The user can configure up to 2 independent syslog servers. The events sent to the syslog server are the same as the ones sent to the Web UI.

Figure 51: Syslog servers configuration

5.4 Configuring the SNMP Credentials

Configure the following parameters for both the Hub and Client ODUs:

Note

The remote ODU info / settings appear only when the link is active

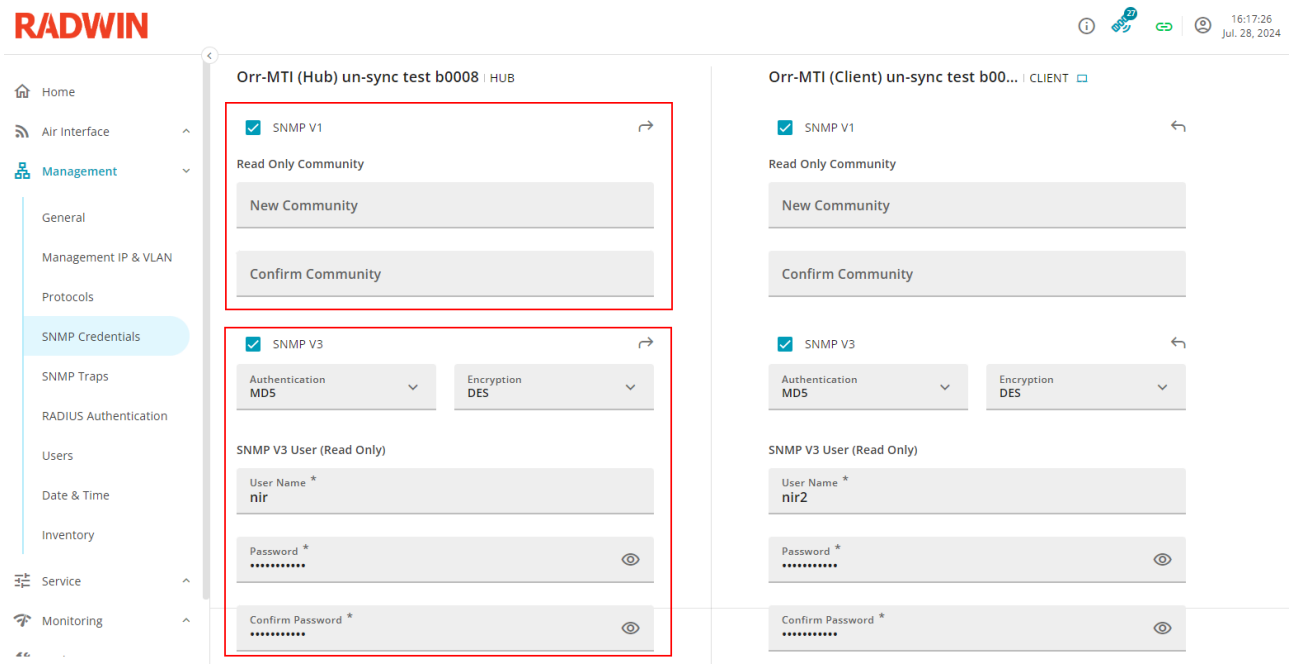


Figure 52: Configuring the SNMP Credentials

Parameter	Description	Mandatory	Default value
SNMPv1	**Control SNMP version and parameters**		
SNMPv1	Enable usage of SNMPv1		**Enabled**
Read Only Community	**Change the SNMPv1 read only community**	No	**Public**
• New Community	Enter the new value	Parameter	
• Confirm Community	Enter the same value again	Parameter	
SNMPv3			
SNMPv3	Enable usage of SNMPv3		**Disabled**
Authentication	SNMPv3 Authentication method (**MD5** / **SHA1**) Only visible when SNMPv3 is selected	Parameter	**MD5**
Encryption	SNMPv3 Encryption method (**DES** / **AES**) Only visible when SNMPv3 is selected	Parameter	**DES**
SNMPv3 User (Read Only)	**Define the SNMPv3 User**	No	
User name	Define the user name used with SNMPv3	Parameter	**Admin**

Parameter	Description	Mandatory	Default value
Password	Set SNMPv3 user password	Parameter	**Web interface Admin user password**
Confirm Password	Confirm SNMPv3 user password	Parameter	**Web interface Admin user password**

5.4.1 RADWIN MIB

RADWIN 2000E supports RFC1213 MIB-II as well as private MIB – see details in the table below.

Root OID	MIB	MIB subtree name	Description
.1.3.6.1.2.1.1	RFC1213-MIB	system	System uptime, system OID, system Name/ Contact/Location
.1.3.6.1.2.1.2	RFC1213-MIB	interfaces	Interface table for POE, SFP and wireless interfaces
.1.3.6.1.4.1.4458.1000.1.1	private	winlink1000OduAdmin	Inventory info, management IP / VLAN settings
.1.3.6.1.4.1.4458.1000.1.2	private	winlink1000OduService	QOS parameters
.1.3.6.1.4.1.4458.1000.1.5	private	winlink1000OduAir	Air interface parameters
.1.3.6.1.4.1.4458.1000.7	private	*winlink1000Genesis*	New subtree for 2000E for optimized PTP link monitoring. Presents key LAN and air interface metrics for both local and remote units

Latest MIB file is available on RADWIN partner portal

Online MIB reference tool: https://tools.radwin.com/documentation/mib-reference/

5.4.2 SNMPv1 Community Configuration

Figure 53: Configuring the SNMP Communities

SNMP community string can be anywhere from 1 to 32 characters long. Like most passwords, they're case-sensitive and can include any combination of letters, numbers, and symbols.

5.4.3 SNMPv3 User Configuration

Note

When using SNMPv3, by default the admin user credentials are used.

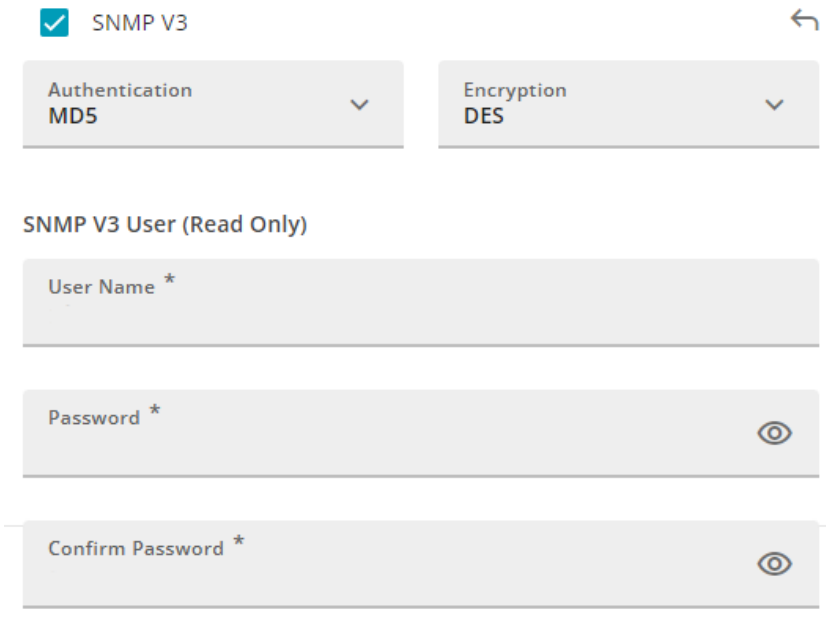


Figure 54: Configuring the SNMPv3 User

SNMPv3 provides a higher level of security. SNMPv3 is based on encrypted messages and uses authentication encryption to identify the user.

SNMPv3 requires you to set a user/password to exchange with the external server.

SNMPv3 User Name must be 8-31 characters long (uppercase letters, lowercase letters, and numbers).

SNMPv3 Password must be 8-16 characters long.

5.5 Configuring the SNMP Traps

Configure the following parameters for both the Hub and Client ODUs:

Note

The remote ODU info / settings appear only when the link is active

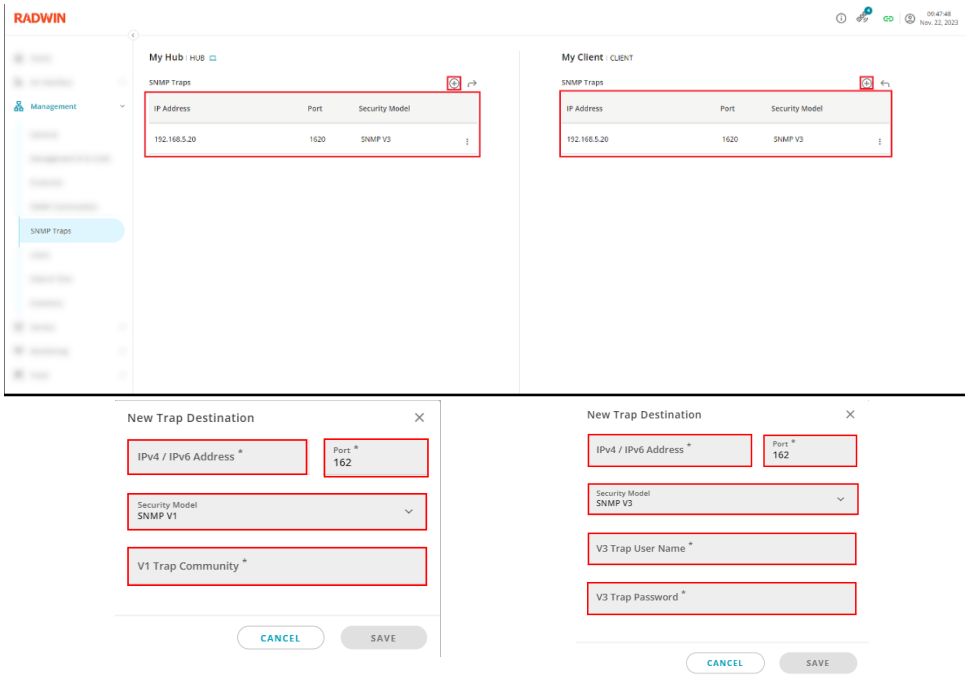


Figure 55: Configuring the SNMP Traps

The following page displays a list of the available trap destinations and enables creating additional destinations using the **+** button.

Parameter	Description	Mandatory	Default value
IP Address	**IPv4 or IPv6** destination IP address	Yes	
Port	Destination UDP port	Yes	**162**
Security Model	The security model (**SNMPv1 / SNMPv3**)	Yes	**SNMPv1**
V1 Trap Community	The community to be used for SNMPv1 traps *Only visible when SNMPv1 security model is selected*	Yes – for V1	

Parameter	Description	Mandatory	Default value
V3 Trap User Name	The username to be used for SNMPv3 traps *Only visible when SNMPv3 security model is selected*	Yes – for V3	
V3 Trap Password	The password to be used for SNMPv3 traps *Only visible when SNMPv3 security model is selected*	Yes – for V3	

5.6 RADIUS Authentication

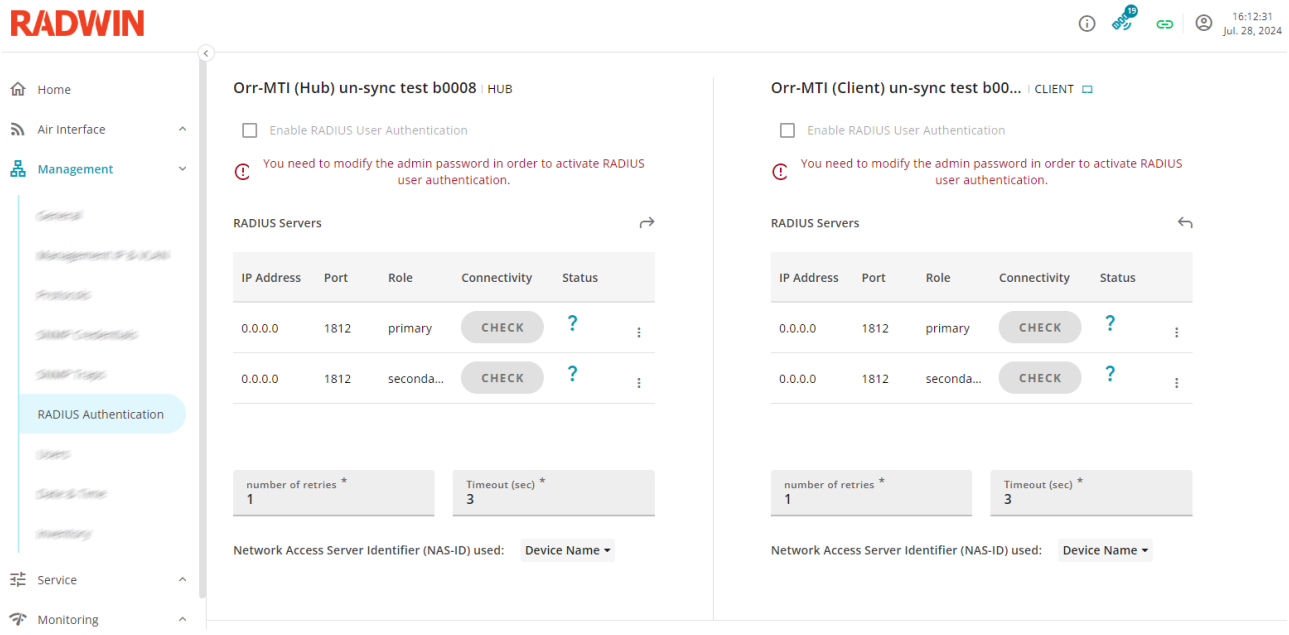


Figure 56: Configuring RADIUS Authentication

RADIUS allows you to maintain user profiles in a central database that all remote servers can share. Having a central database provides better security, enabling you to use the same identifiers to access all devices connected to your network.

Warning

The activation of the RADIUS Authentication requires changing the default password of the admin (ie. netwireless) to a more secure password.

Note

Admin user will still be active to allow access to the device even if RADIUS connection fails.

To use RADIUS Authentication, you need to first enable it.

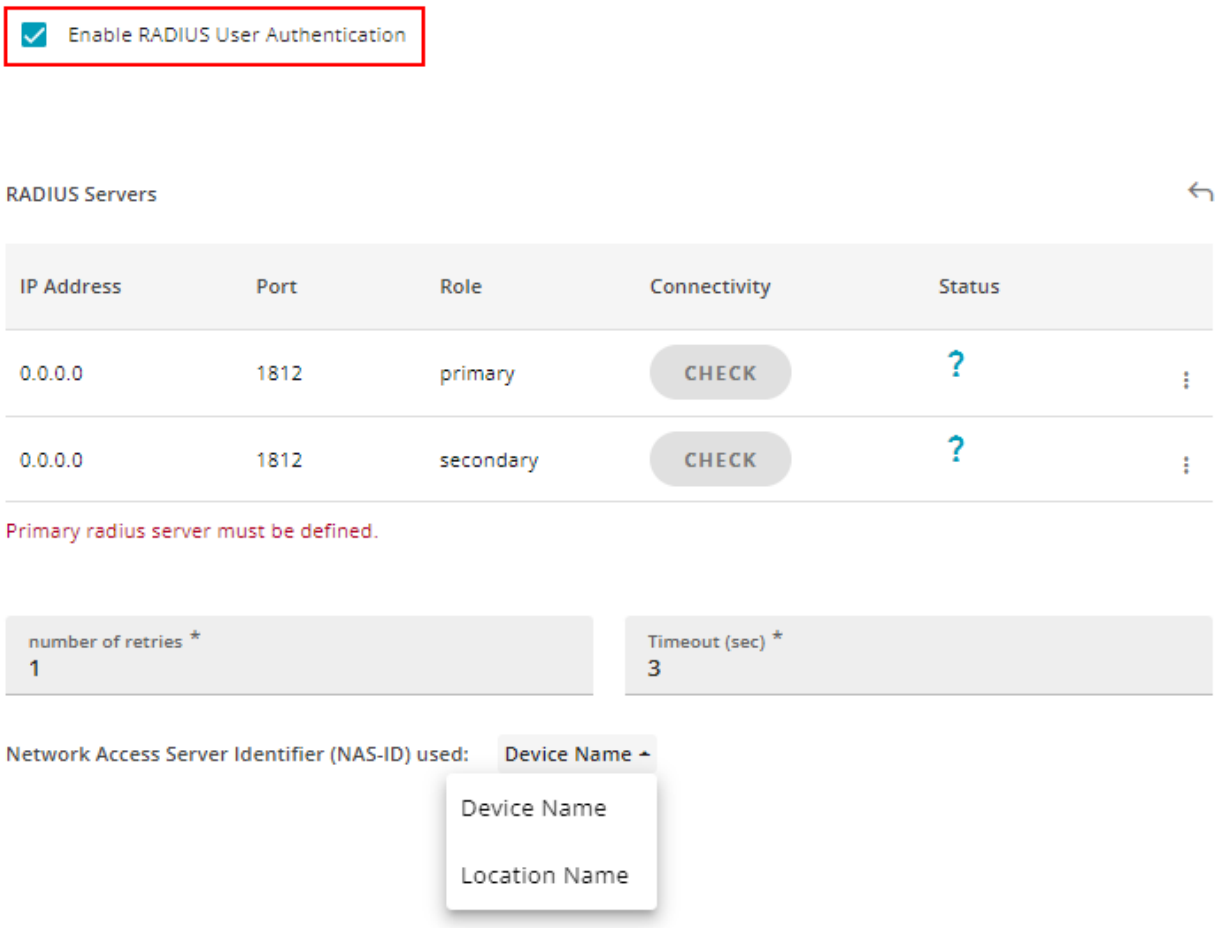


Figure 57: Enable RADIUS Authentication

RADIUS Authentication configuration proposes setting up two RADIUS servers. Only the primary is mandatory. Few parameters are required to configure the connection.

Parameter	Description	Mandatory	Default Value
RADIUS Servers			
IP Address		Yes	**0.0.0.0**
Port		Yes	**1812**
Role			**Primary or Secondary**
Connectivity	Check button to validate the entered configuration before applying it		

Parameter	Description	Mandatory	Default Value
Status	Displays the result of the check. The status could be "V" (connected) or “X" (failed)		**? (unknown)**
Options	Allows to remove or to change the configuration		
Number of retries	Number of times the device will try to connect the RADIUS server	Yes	**1**
Timeout (sec)	Timeout for the connection attempt	Yes	**3**
Network Access Server Identifier (NAS-ID)	This is the string used in the message header to identify the source of the authentication request. This could be the "device name" or the "location name"	Yes	**Device Name**

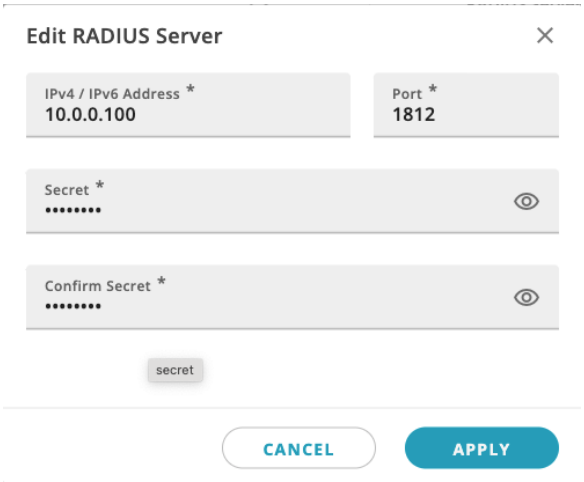


Figure 58: RADIUS Server configuration

5.7 Modifying User Passwords

On the local ODU to which you are connected, you can change the local user credentials for WEB UI access and SNMPv3 polling.

Note

To change a user password on the remote ODU, connect directly to the remote ODU IP address through the browser interface.

1. Click the options icon and click Change password.

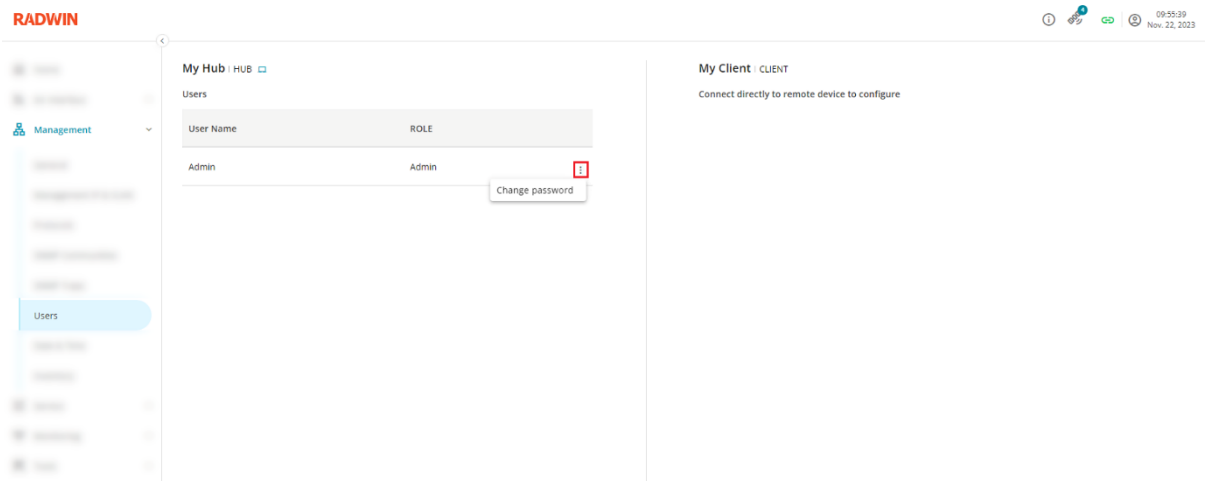


Figure 59: Modifying Passwords

Note

Password update requires current password confirmation

Note

SNMPv3 trap user name and password are set per each SNMPv3 trap destination (see **Configuring the SNMP Traps**)

5.8 Viewing the Date and Time

You can view the time source, as well as current date and time of the ODU in the **Date and Time** window.

Note

The remote ODU appears only when the link is active.

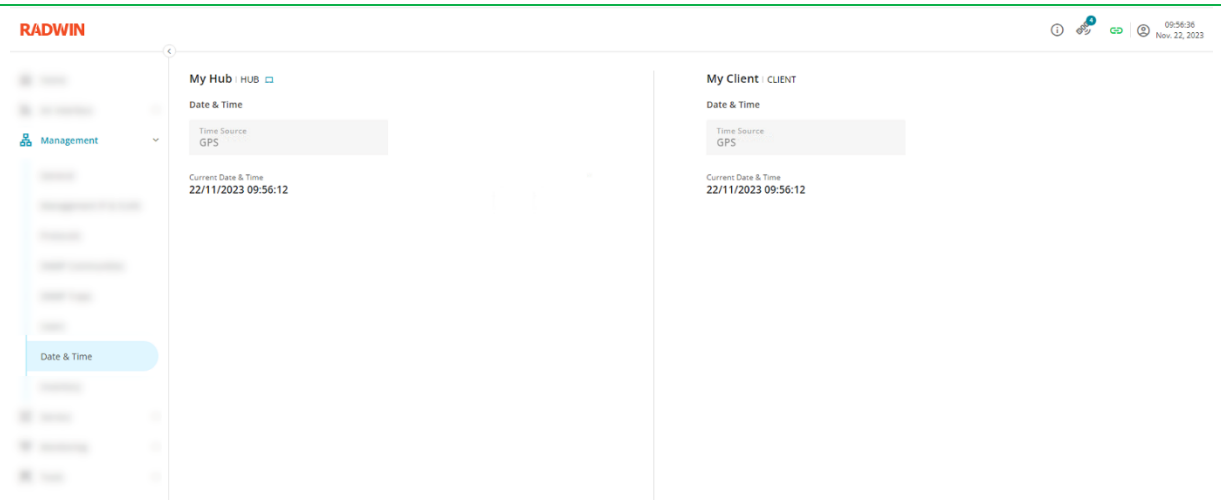


Figure 60: Viewing the Date and Time

Parameter	Description
Time Source	Time data source (**Internal / GPS**) *Note: Internal time source will only be used for several minutes after boot, until GPS signal is acquired.*
Current Date and Time	Shows the Date and Time The format is **DD/MM/YYYY HH:MM:SS** *Note: Time zone is detected automatically based on GPS location data and internal database*

5.9 Viewing the ODU Inventory

Displays information for Hub and Client ODU inventory parameters:

- Product Name
- Part Number
- HW Version
- SW Version
- MAC address
- Serial Number
- Supported Encryptions

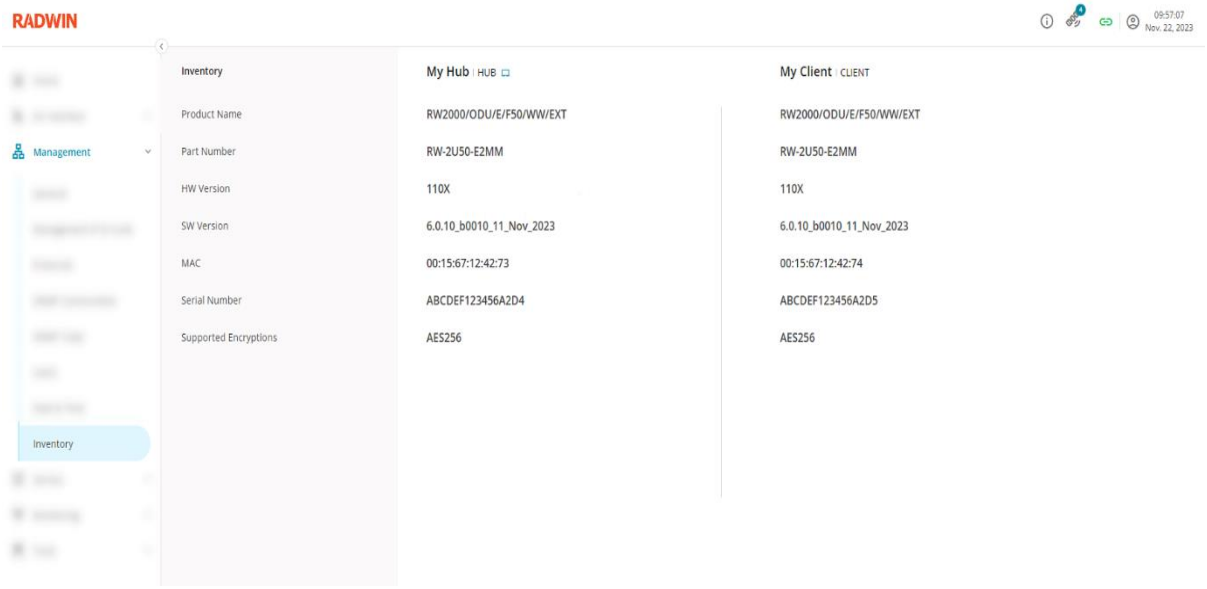


Figure 61: Viewing the ODU Inventory

6 Configuring Service Parameters

6.1 Viewing the LAN Ports Parameters

Displays the port parameters for both the Hub and Client ODUs:

Note

The remote ODU info / settings appear only when the link is active.

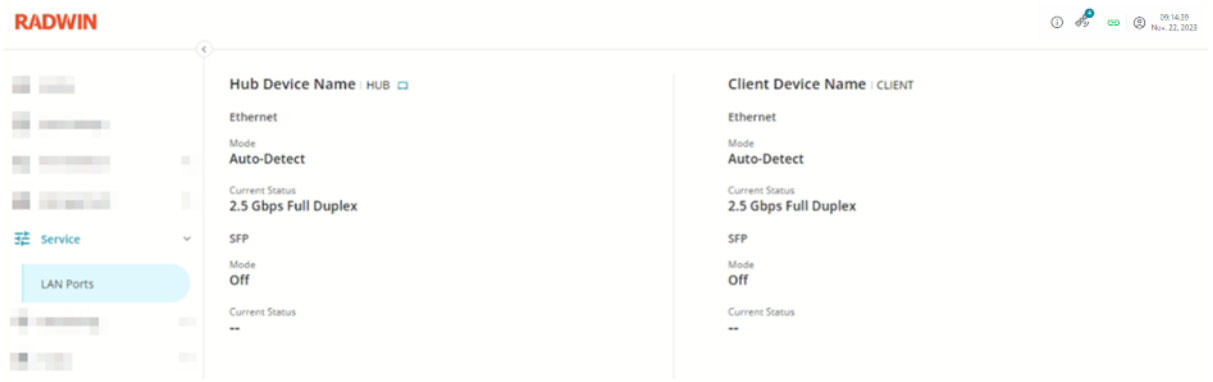


Figure 62: Viewing LAN Ports Parameters

Parameter	Description	Mandatory
Mode (Ethernet)	Only **Auto-Detect** is currently supported	Read only
Current Status (Ethernet)	Displays the current Ethernet speed and duplex mode **(100 Mbps Full Duplex / 1000 Mbps Full Duplex / 2.5 Gbps Full Duplex)**	Read only
Mode (SFP)	**Off**: no SFP module detected **Auto-Detect:** SFP module is present	Read only
Current Status (SFP)	Displays the Ethernet speed and duplex mode of the internal SFP slot interface. Only 1Gbps SFPs are supported, and **1000 Mbps Full Duplex** should be displayed. *Note: fiber / copper link status is not reflected currently*	Read only

6.2 Traffic VLAN Configuration

When Management VLAN is configured on the device on both sides, Hub and Client, it is possible to set Traffic VLAN rules.

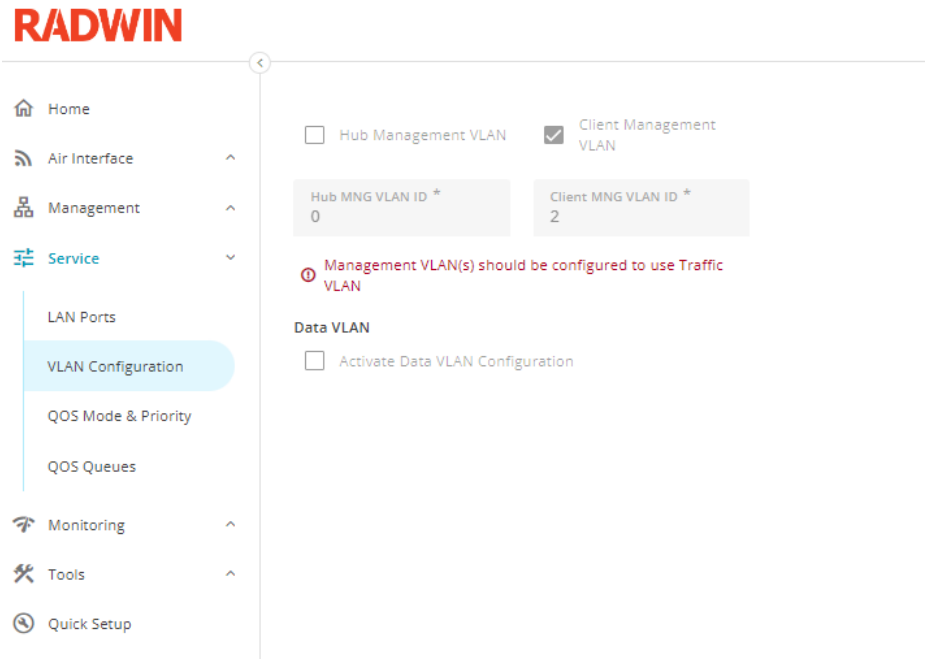


Figure 63: Traffic VLAN - No Management VLAN

2000 E supports both VLAN configurations 802.1Q and QinQ tagging.

When Traffic VLAN tagging is active, you could define which configuration you want to use:

VLAN Configuration	Tagged traffic available options	Description
802.1Q Transparent (Default)	• Transparent (Default) • Filter • Drop	All untagged traffic is untouched, tagged traffic could passthrough or be filtered on both directions.
802.1Q Tag/Untag	• Transparent • Filter • Drop	Untagged traffic is tagged with the selected VLAN ID, all other tagged traffic is managed based on the defined option on both directions.
Provider **QinQ**	N/A	The following Ethertype/TPID are supported: • 0x88a8 – by default • 0x8100 – both S-tag and C-tag will have the same Ethertype • 0x9100

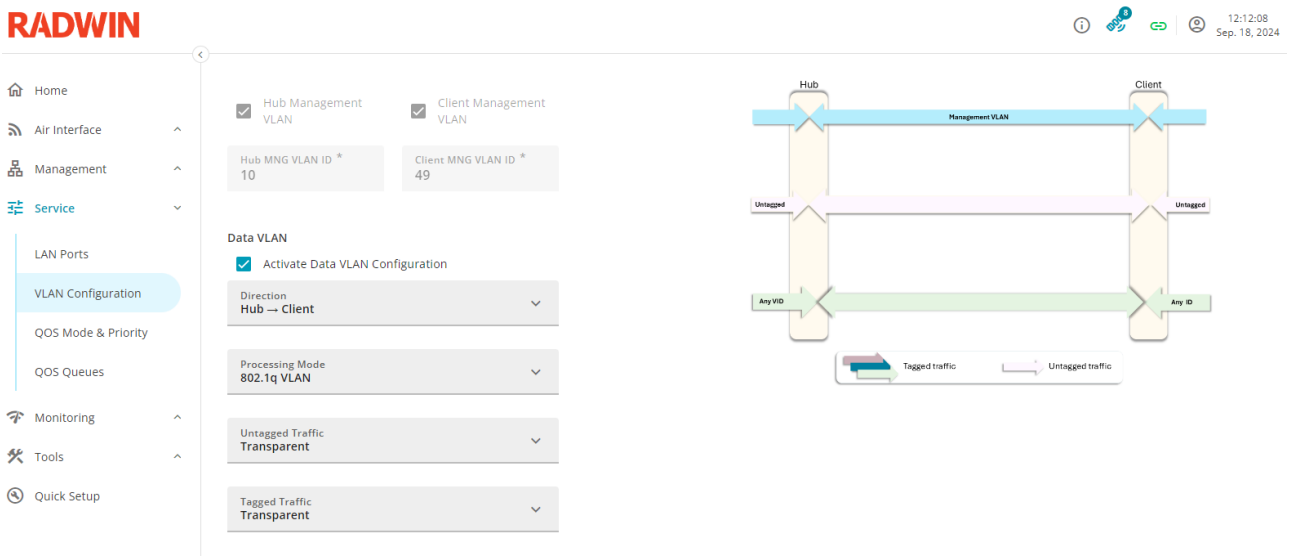


Figure 64: Traffic VLAN - With Management VLAN

The traffic direction can be also defined (Hub to Client or Client to Hub) to properly set the rules.

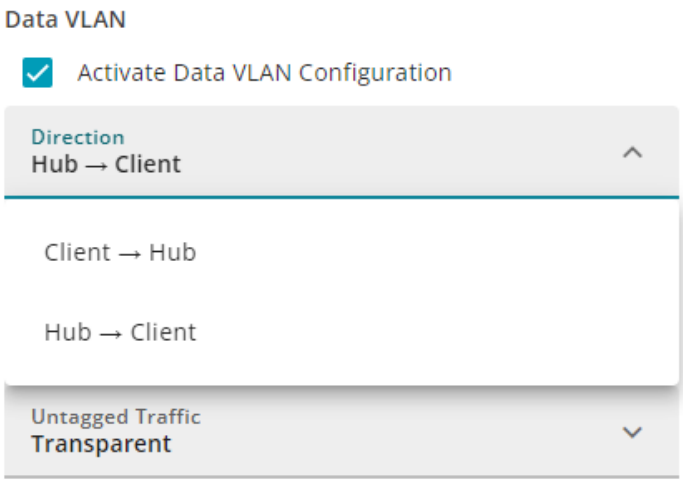


Figure 65: Traffic VLAN – Define the traffic direction

6.2.1 802.1Q VLAN

Transparent

In transparent mode, the untagged traffic is untouched in both directions.

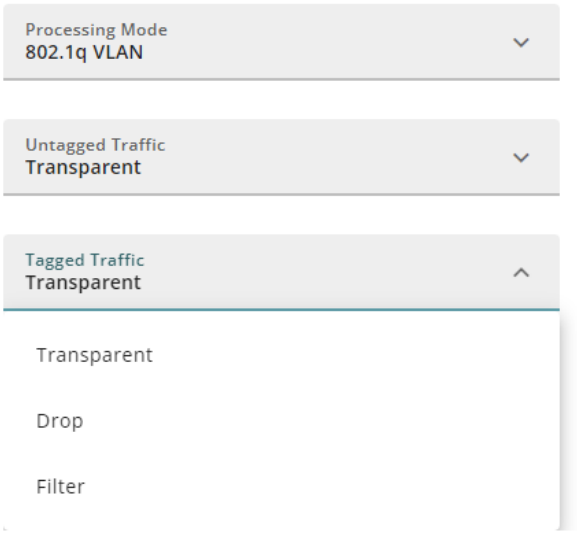


Figure 66: Traffic VLAN – 802.1Q Transparent

Transparent: Tagged traffic is passed in both directions without any manipulation.

Drop: All the tagged traffic is dropped in both directions.

Filter: Only the selected range of VLAN ID are passed in both directions.

Note

In Filter, the user can define up to 4 ranges of VLAN IDs.

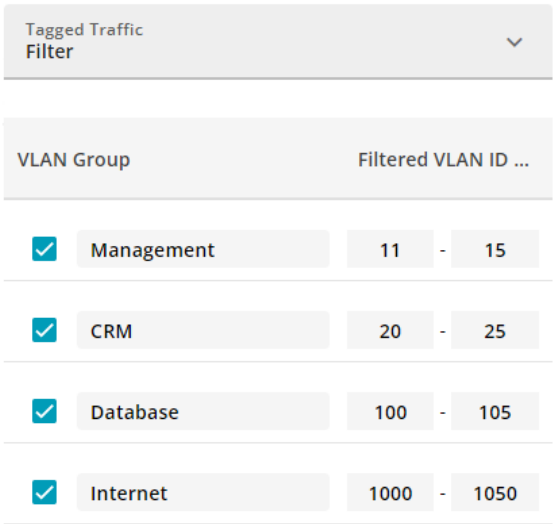


Figure 67: Traffic VLAN – Filter VLAN ID ranges

Tag/Untag

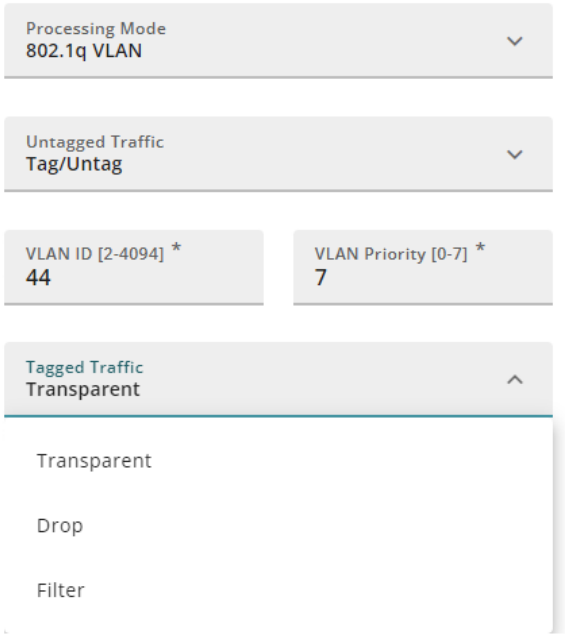


Figure 68: Traffic VLAN – 802.1Q Tag/Untag

Note

In 802.1Q Tag/Untag, on the destination side of the traffic, the untagged traffic is always discarded.

Two parameters need to be configured:

VLAN ID: The VLAN ID to be used to tag all the untagged traffic from the source and allow it from both direction all the time.

VLAN Priority: VLAN Priority to be used for the tagged traffic.

Like for Transparent mode, the user can select which option to apply on the tagged traffic:

Transparent: Tagged traffic is passed in both directions without any manipulation.

Drop: All the tagged traffic is dropped in both directions.

Filter: Only the selected range of VLAN ID are passed in both directions.

Provider QinQ

When using Provider QinQ, packets are twice encapsulated: a first type with regular VLAN ID (C-VID) and a second time with a second VLAN ID (S-VID).

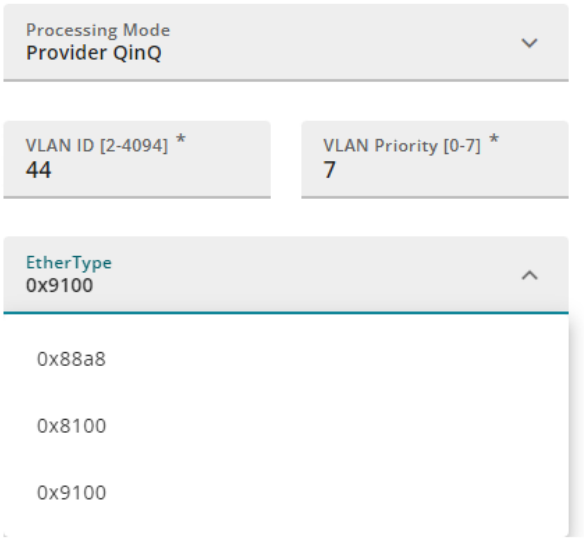


Figure 69: Traffic VLAN – Provider QinQ

In the VLAN ID field, the user should provide the S-VID which will be used in the Ethertype header.

Like for 802.1Q, the user should define also the VLAN Priority for this S-VID.

Three possible common options are proposed for the Ethertype header value:

- **0x88a8 (Default)**
- **0x8100**
- **0x9100**

Note

Other S-VID are automatically dropped. On the destination, you should take care of encapsulating the management Traffic VLAN into the same S-VID if you want to be able to control and access the destination device.

6.2.2 Traffic Stream Behavior

Each configuration and option are described in the Web UI with a scheme showing the streams behavior.

The following schemes are describing traffic from Hub to Client configurations and options:

Figure 70: Traffic VLAN – Transparent – Transparent

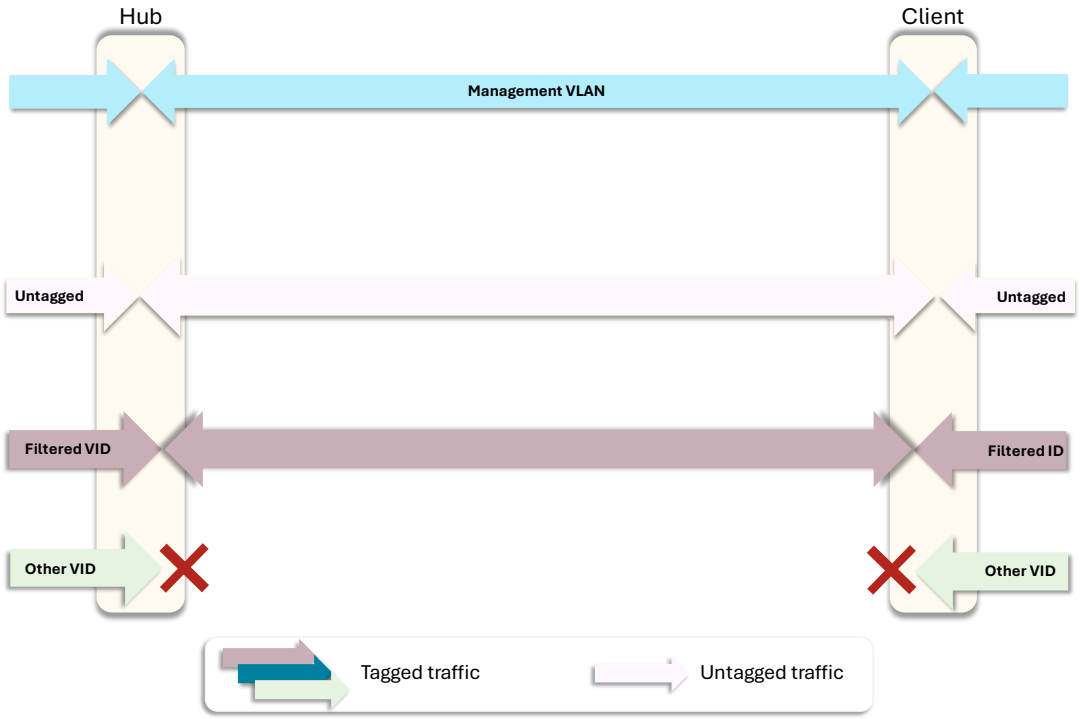


Figure 71: Traffic VLAN – Transparent – Filter

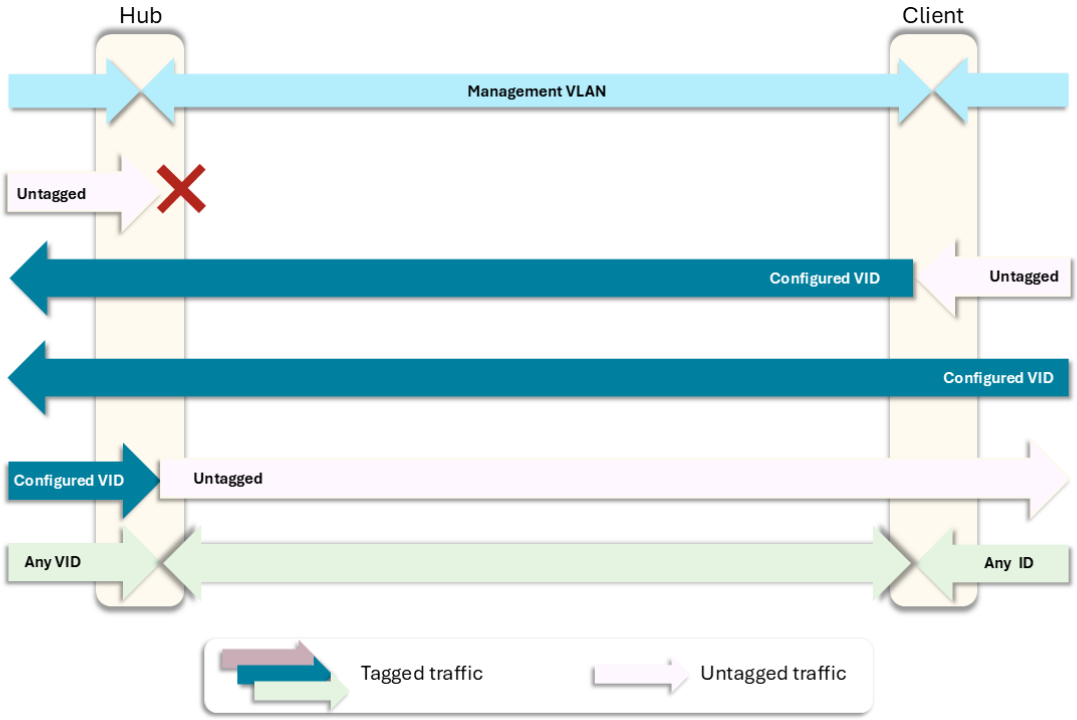


Figure 72: Traffic VLAN – Tag/Untag – Transparent

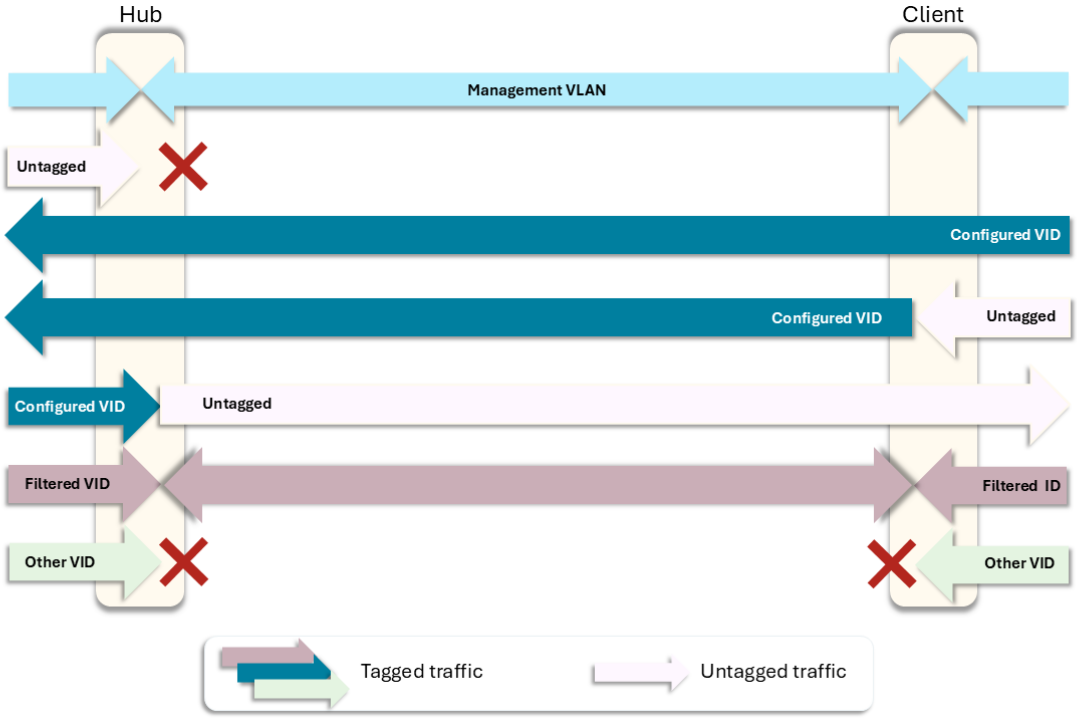


Figure 73: Traffic VLAN – Tag/Untag – Filter

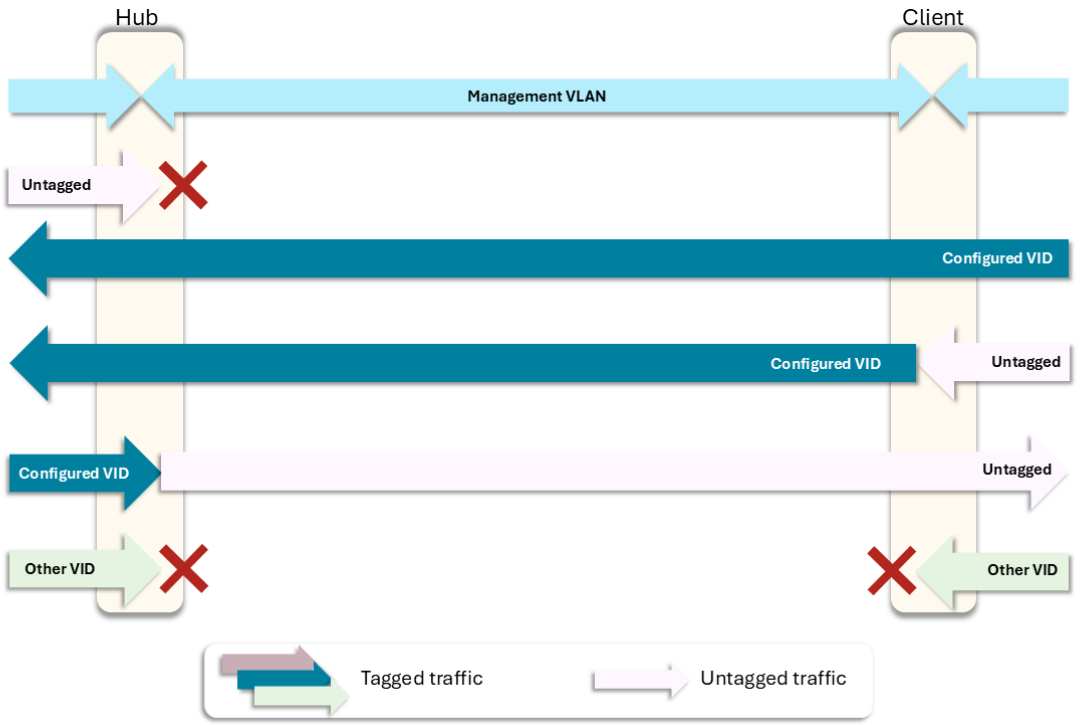


Figure 74: Traffic VLAN – Tag/Untag – Drop

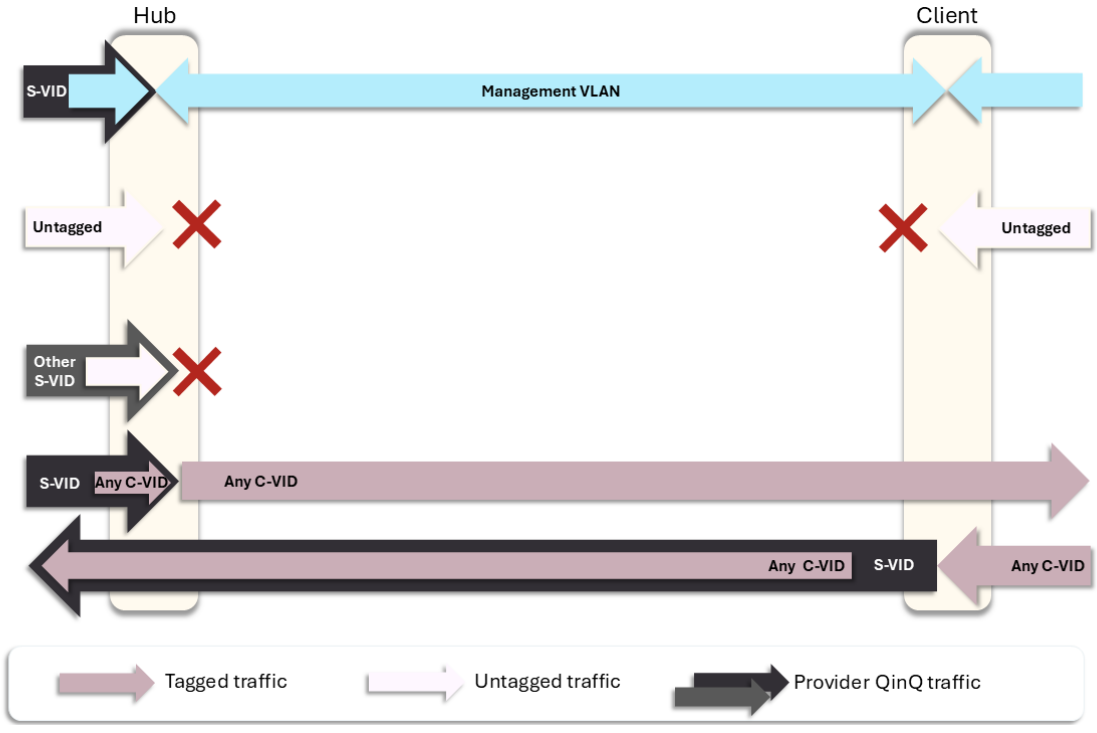


Figure 75: Traffic VLAN – QinQ

6.3 Modifying the QOS Mode and Priority

RADWIN 2000E supports QoS classification based on either 802.1p VLAN or Diffserv DSCP values. Ingress traffic is classified into up to 8 priority queues.

The QoS Mode and Priority screen enables the following operations:

- QoS mode selection
- Enable / disable queues
- Rename queues
- Set QoS priority mapping for each enabled queue

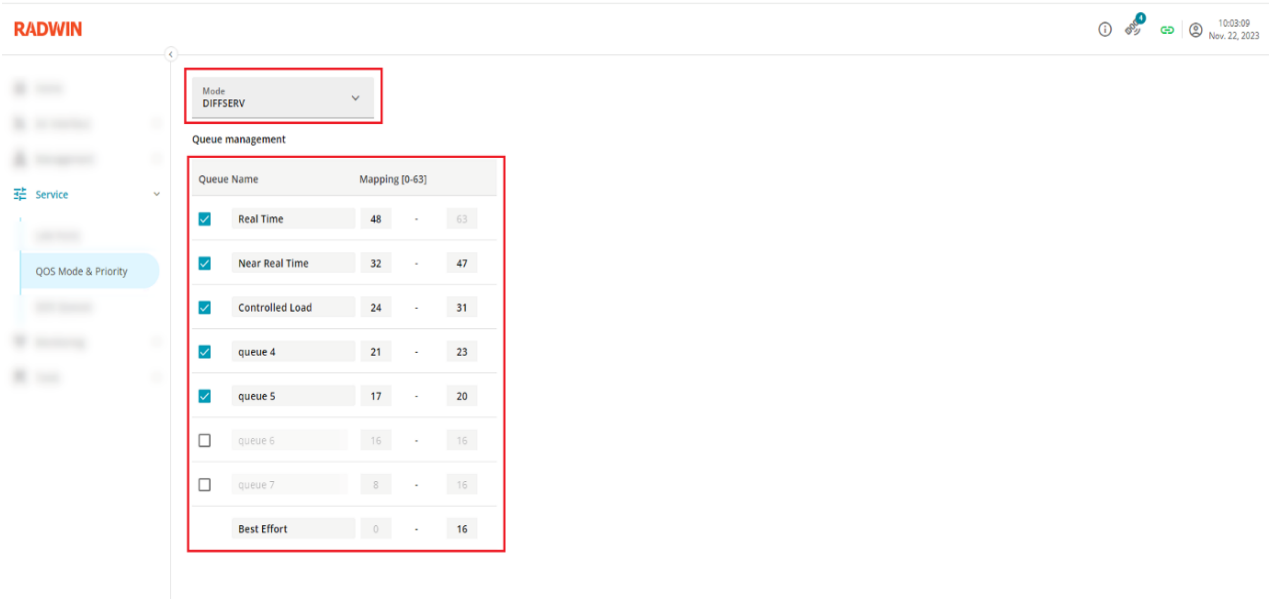


Figure 76: Modifying QOS Mode and Priority

Parameter	Description	Mandatory	Default value
Mode	**Selects the QOS mode (VLAN / DIFFSERV / Disabled) for the link**	**Yes**	**Disabled**
VLAN	801.p COS value of ingress 802.1Q frames will be used for classification	Parameter	
Diffserv	Diffserv DSCP value of ingress packets will be used for classification	Parameter	
Disabled	Traffic classification is disabled	Parameter	
Queue Management	**Enable/disable, set name and priority range**	**Yes**	
Enable / disable	Enabling and disabling the queue will affect the visible queues in the QoS Queue screen. Up to 8 queues can be enabled.	Yes	**See table below**
Queue name	Set a custom name as needed (such as **Video**)	No	**See table below**

Parameter	Description	Mandatory	Default value
Mapping	Set priority range for each queue. Available value ranges depend on the QoS mode selected: • QoS Disabled: N/A • VLAN: 0 – 7 • DIFFSERV: 0 – 63	Yes	**See table below**

If a queue is disabled/enabled, the user must adjust the mapping so it adheres to the validation rules. Priority range mapping values must be monotonic and must cover the entire range. When enabling a queue, the WFQ proportions between the queues are changed and the user must go to the Queues screen to make sure the new proportions are correctly configured.

Queue	**Queue default name**	**Default Priority**	
		Diffserv	**VLAN**
1	Real time	48-63	6-7
2	Near real time	32-47	4-5
3	Controlled load	16-31	2-3
4	Queue 4	Off	Off
5	Queue 5	Off	Off
6	Queue 6	Off	Off
7	Queue 7	Off	Off
8	Best effort	0-15	0-1

Further configuration for queue settings is available in the QoS Queues window, as described below.
The QoS configuration data is stored in the hub and sent to the client when link is established.

6.4 Modifying the QOS Queues

The QoS Queues screen controls the following:

- Strict / WFQ queue mode (per each link direction)
- Set Weight for WFQ (per each link direction)
- Set MIR mode and MIR value (per each link direction)

Link directions are as follows (also indicated by arrows on the UI):

Downlink (DL, ↓) – settings for Ethernet ingress queues of the **Hub** radio (left side panel)

Uplink (UL, ↑) – settings for Ethernet ingress queues of the **Client** radio (right side panel)

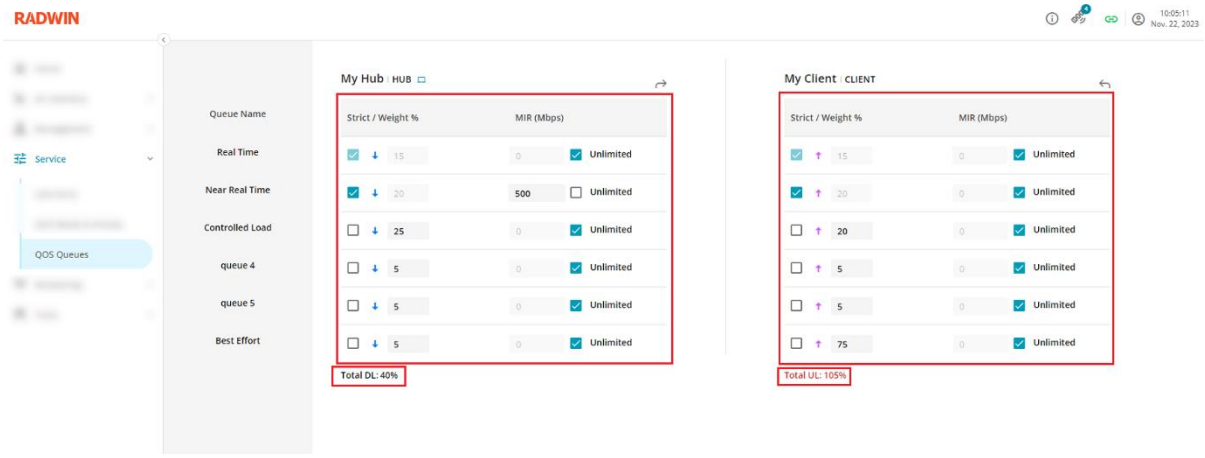


Figure 77: QoS Queues

Parameter	Description	Mandatory
Strict	• "Strict" priority packets will always be transmitted first, up to the defined MIR level. • When there are no more strict priority packets (either due to reaching the MIR or no user data available), the remaining bandwidth will be allocated to other priorities according to the WFQ • In case there are more Strict priority packets than available space in the air-frame, packets from lower priority queues will not enter this air-frame. • This ensures that high-priority traffic gets a guaranteed share of the available bandwidth and is not impacted by lower-priority traffic.	No
Weight %	• WFQ (Weighted Fair Queueing) - percent of the remaining air-frame capacity, assigned to this queue (after Strict priority packets filled the air-frame)	No

Parameter	Description	Mandatory
	• When the data channel is full, the packets of each priority transmitted in the air will be allocated according to the percent allotted for each priority • if a certain priority data channel has less data than its allotted percentage, its extra capacity will be split among the other channels corresponding to their percentage • When the data channel is not full, all packets will be transmitted without waiting The WFQ total percentage is displayed at the bottom row for the hub/client, and must be equal to 100% before you can click **APPLY**.	
MIR (Mbps) / Unlimited	• MIR - Maximum Information Rate o This is the maximum throughput limit for this queue o Note: actual MIR is limited by the selected channel bandwidth. If you modify the CBW, you might need to adjust the MIR. • Unlimited MIR. o No upper limit is set on the traffic for this queue	No

The remote ODU info / settings appear only when the link is active.

7 Viewing Monitoring Information

7.1 Counters View

The Counters window displays various statistics for traffic. The statistics are displayed for both the Hub and for the Client.

Note

The statistics are displayed only if there is an active link.

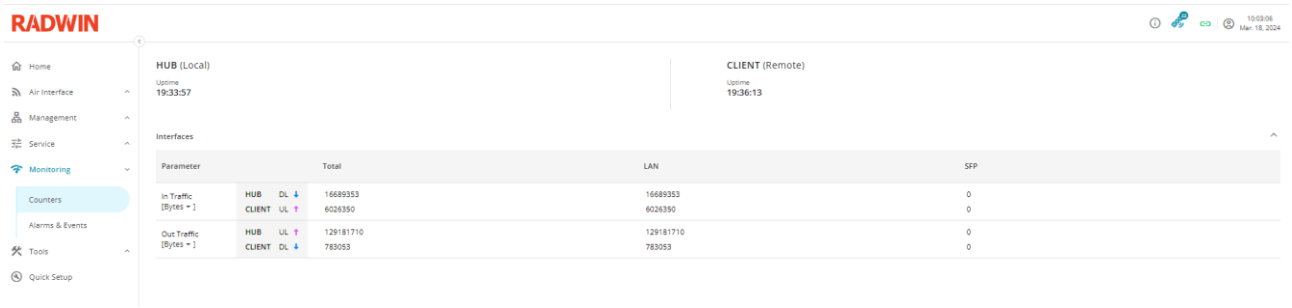


Figure 78: Counters View

The following table describes the Traffic parameters:

Parameter	Description
Uptime	Time elapsed since the reboot of the system.
In Traffic*	Traffic entering the device over the wired port. The information can be displayed in bytes or in packets. The table displays values for LAN, SFP and total traffic.
Out Traffic*	Traffic exiting the device over the wired port. The information can be displayed in bytes or in packets. The table displays values for LAN, SFP and total traffic.

Note

To select the units in which the data is displayed (bytes/packets), click the down arrow next to the current display unit:

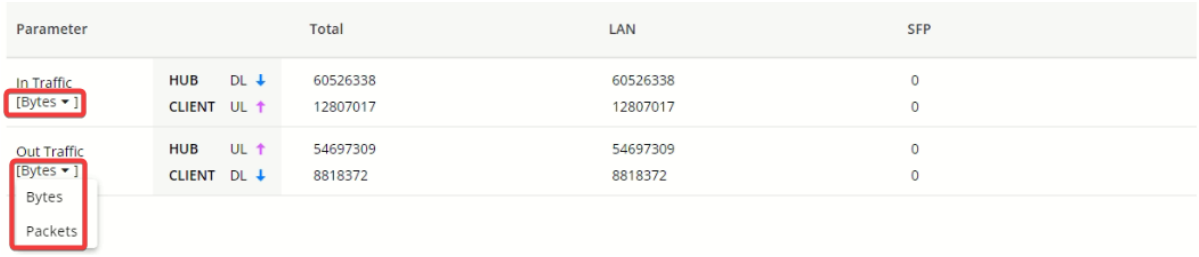


Figure 79: Traffic Parameters

7.2 Alarms and Events

The events list displays events that occurred in the system, sorted by their time of occurrence. Information provided includes:

- Date
- Time
- Type of event
- Device name
- Message

You can search for an event by text, scroll the list or skip to a specific page.

Note

For list of all supported events, see Web UI Events Table.

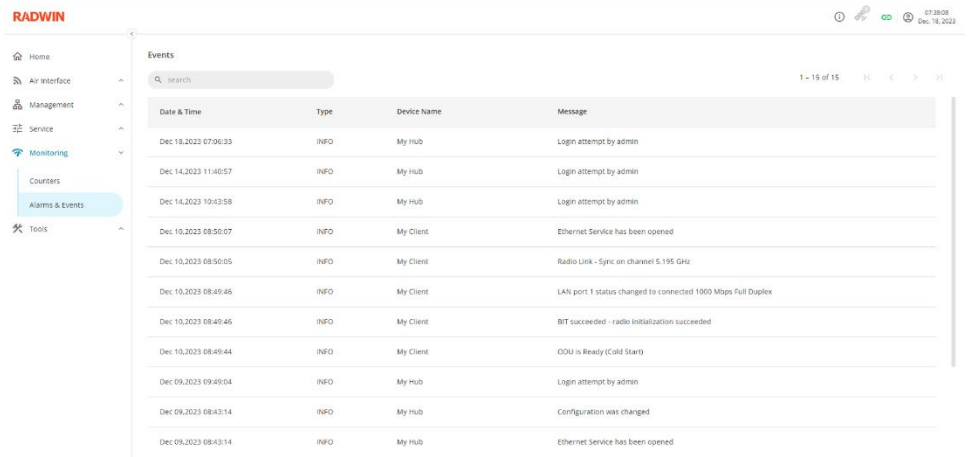


Figure 80: Alarms and Events

8 Applying Tools and Maintenance

8.1 Upgrade, Backup & Restore

Under the Upgrade/Backup/Restore tab, you could proceed to the different operations by selecting the right one.

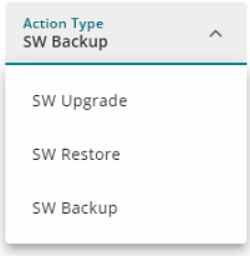


Figure 81: Operation Selection

8.1.1 Performing a Software Upgrade

Note

This operation can only be performed on the local unit to which the browser is connected. To perform this operation on the remote ODU, you must connect to its own UI.

Upgrading the software does not affect the ODU configuration.

To upgrade the software:

Download the SW Upgrade package from RADWIN Partner Portal or get it from RADWIN Partner and save it on your PC/Local Network.

1. Select the device to upgrade.

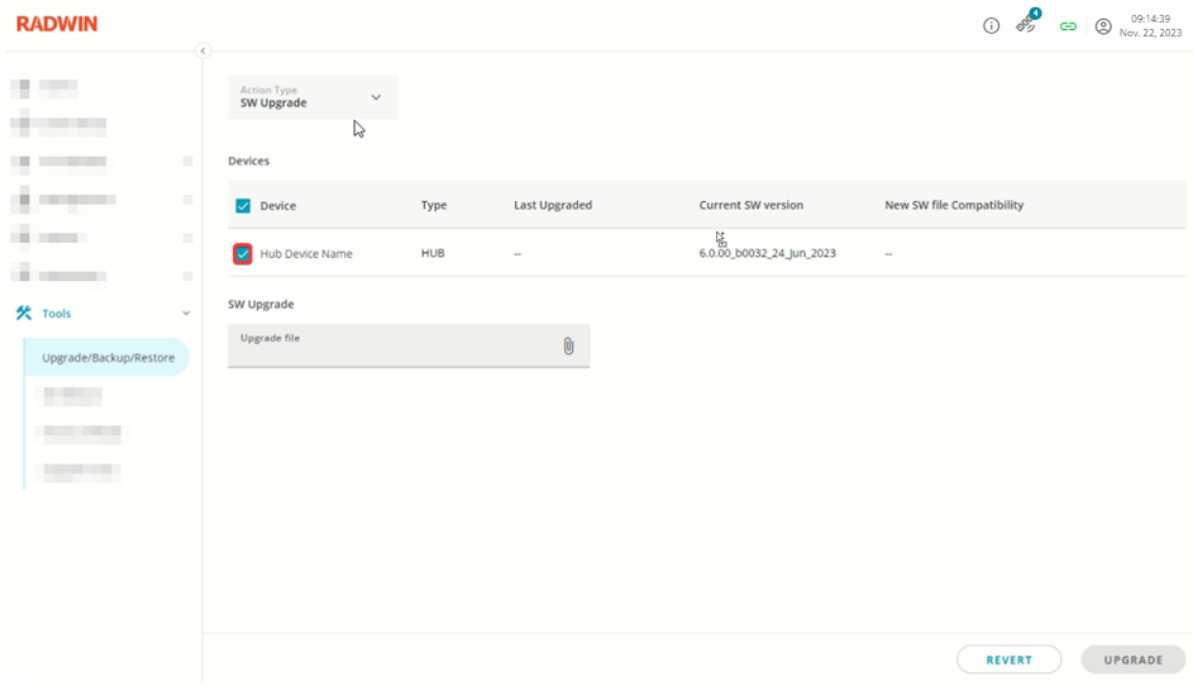


Figure 82: Performing a Software Upgrade

2. Click the **SW Upgrade** paper clip.

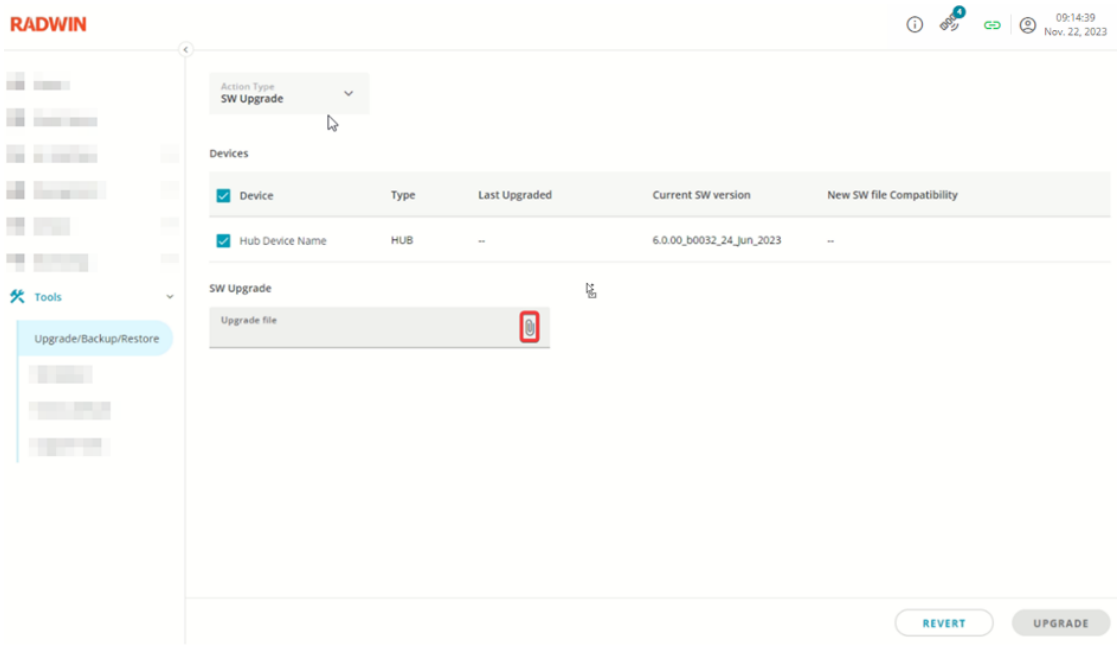


Figure 83: Software Update Paper Clip

3. Navigate to the required file, click **Open** and click **UPLOAD**.

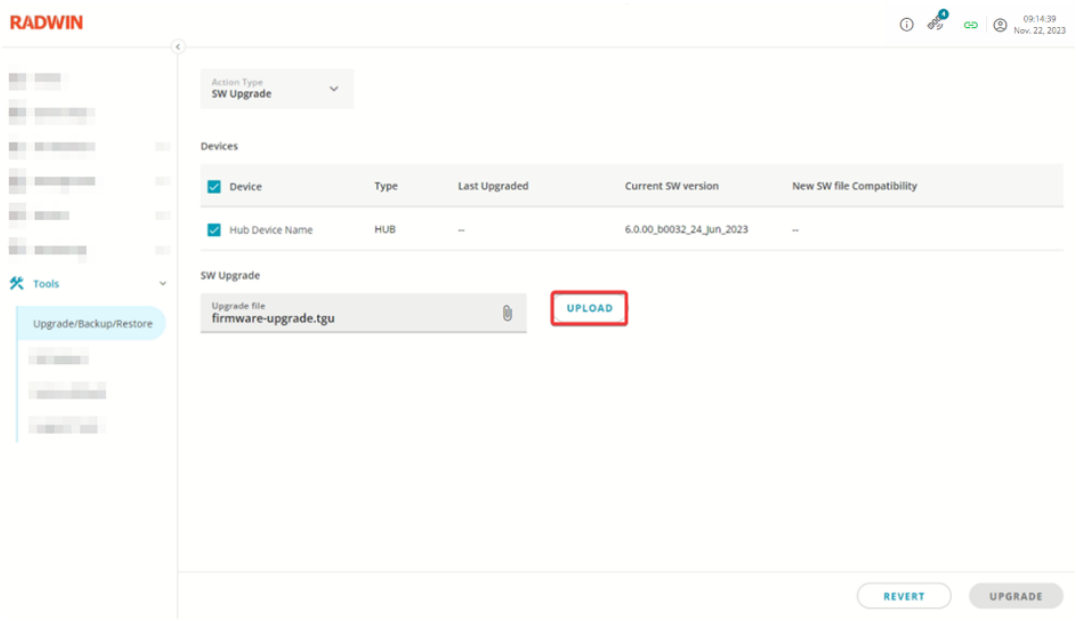


Figure 84: Navigate File

4. The file is uploaded, and its contents are validated and tested for compatibility.

   If validated, the SW version of the upgrade file is displayed, and if it is compatible with the ODU, a green checkmark is displayed.

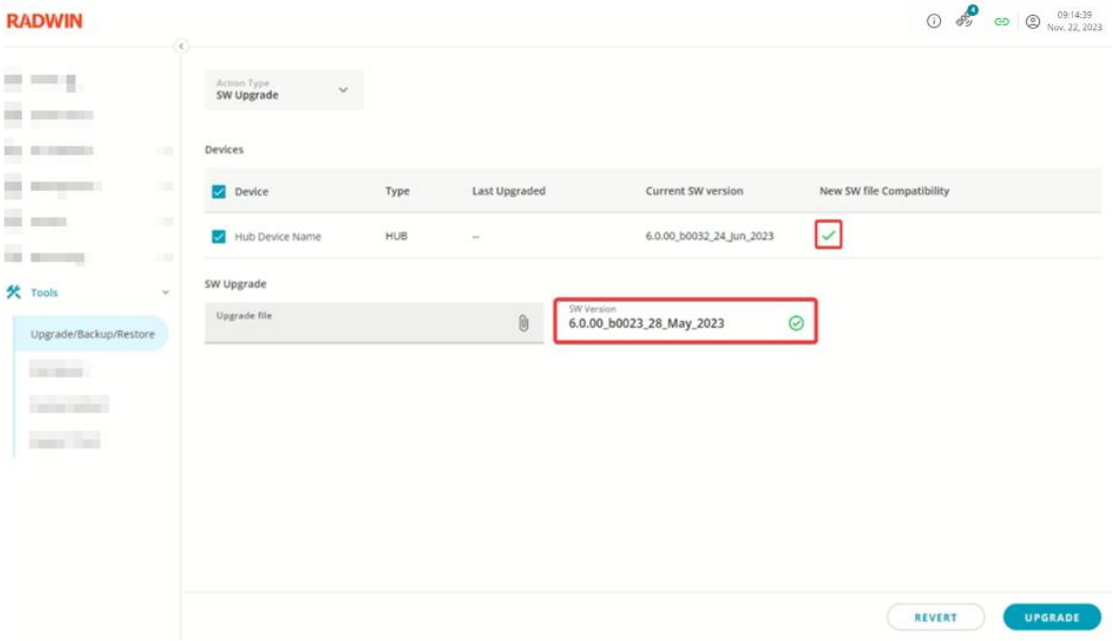


Figure 85: File Upload

Note

If the uploaded file cannot be validated or if it is not compatible with the ODU, a notification is displayed, and the upgrade cannot continue.

5. Click **UPGRADE**.

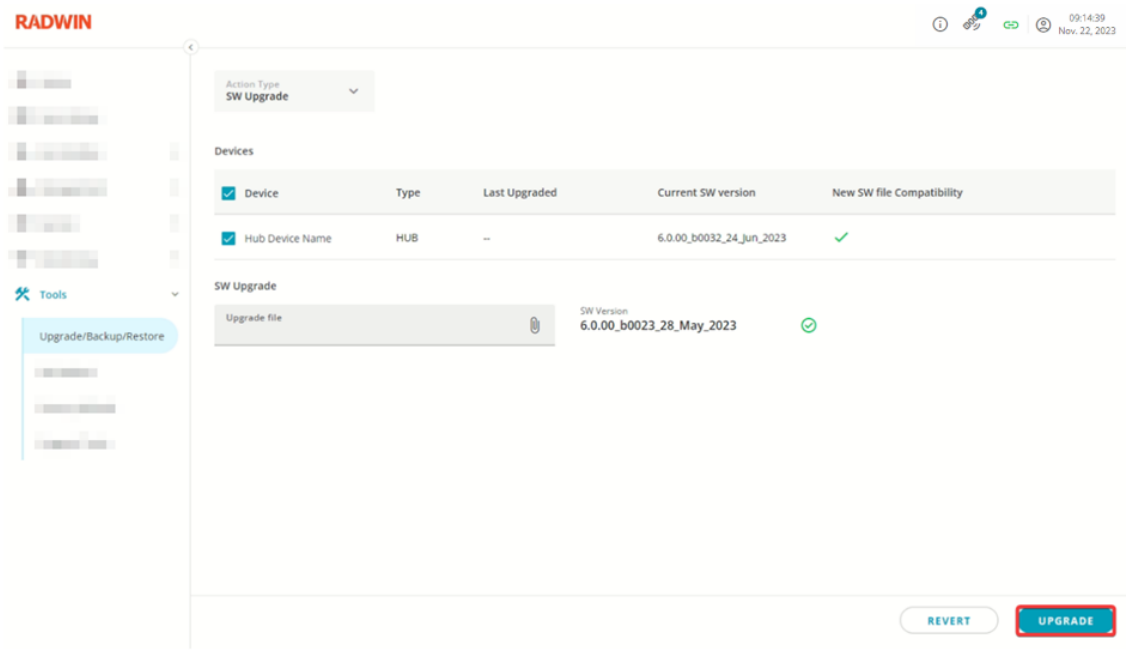


Figure 86: Upgrade

During the upgrade process, all ODU activities are frozen. Progress bars show the progress of the software upgrade and ODU restart.

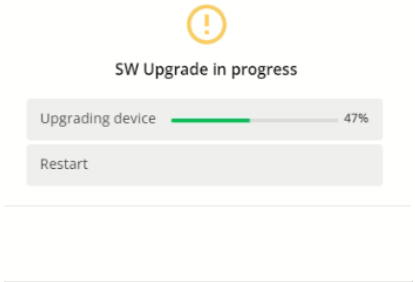


Figure 87: Upgrade in Progress

6. After the device restarts, the UI automatically will redirect to the login page.

8.1.2 Software Backup

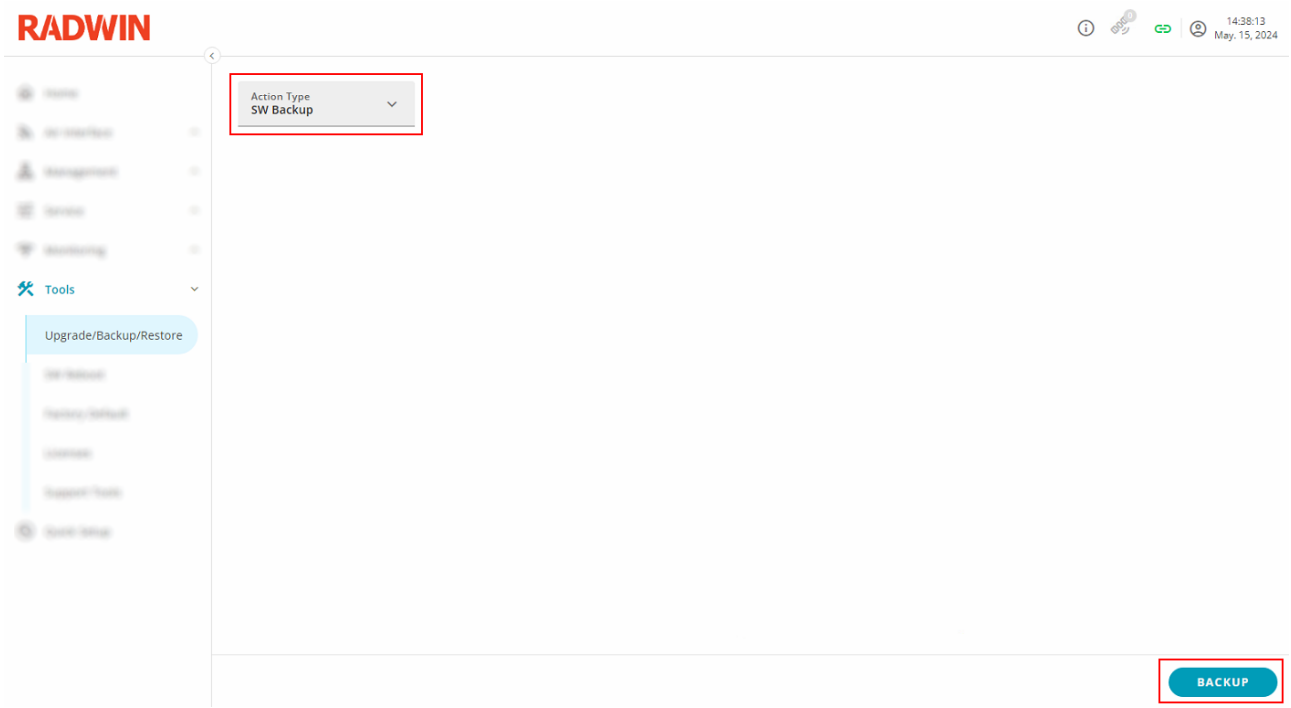


Figure 88: Start a backup

Under Action Type: SW Backup, you could proceed with a full backup of your system.

When clicking on the 'Backup' button, you will initiate the backup. The preparation of the backup could take several minutes.

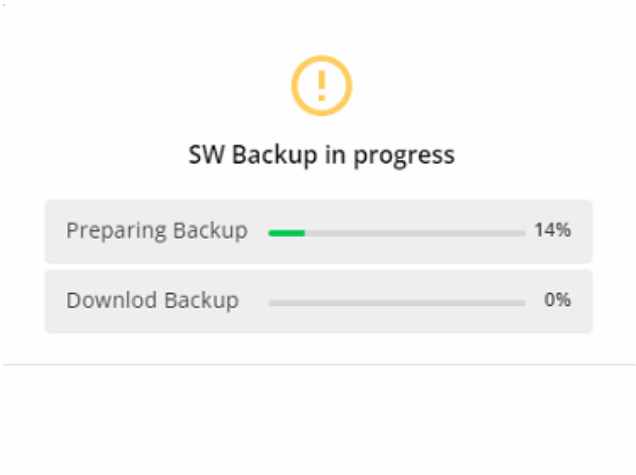


Figure 89: Running a backup

When the backup is finished, the backup pop-up tells you the backup is finished and the file will be downloaded on your device.

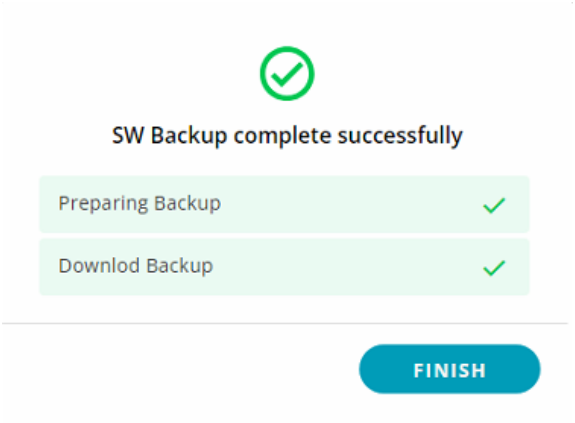


Figure 90: Backup finished

You could then retrieve the file through your browser download history or in your default download directory on your device. The name of the backup is made of:

<IP Address of the unit>_<dd-MM-yy>_<release installed on the device>.bck

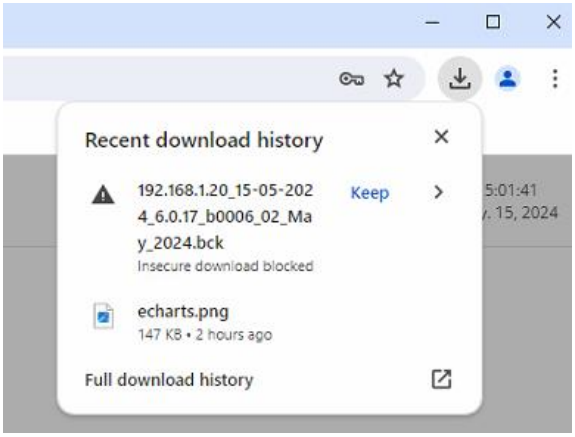


Figure 91: Locate a backup

8.1.3 Software Restore

By selecting in the Action Type, 'SW Restore' you could restore a previous backup onto the unit.

To proceed with restore on a backup file, few rules should be followed:

1. The radio unit should be a RADWIN product
2. The radio unit should be the same product where the backup has been done (i.e. here 2000 E)
3. The radio unit should have the same SW revision as the one in the backup
4. The radio unit should have the same HW revision as the one where the backup has been done
5. The radio unit should have the same licenses (open frequencies)

To start the software restore process, you should select a backup file by clicking on the paper clip.

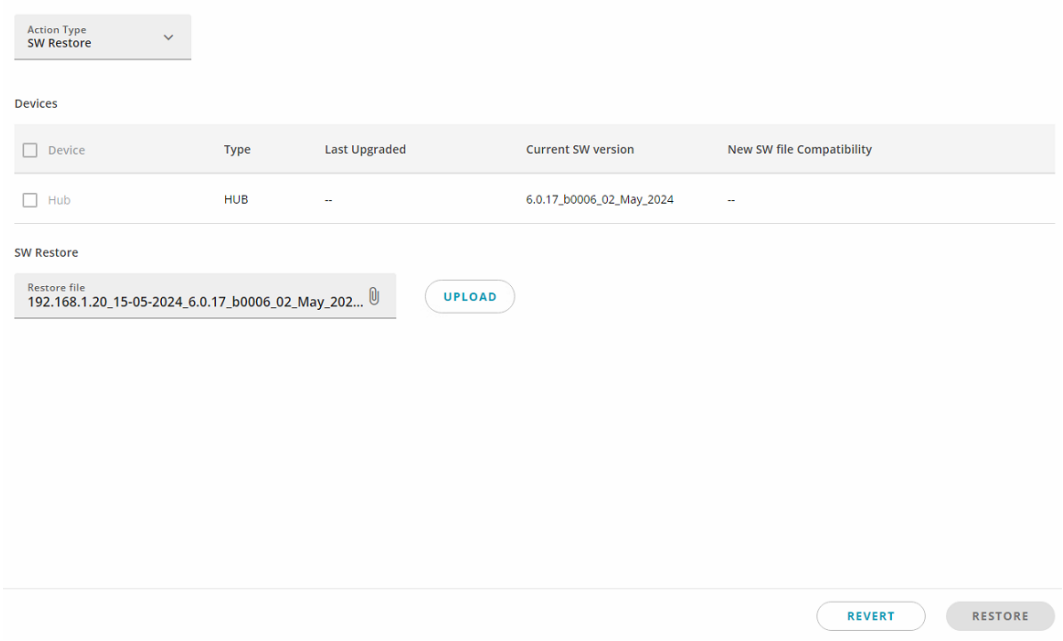


Figure 92: Select a backup file

The radio unit will then upload the file and check its compatibility based on the rules defined previously.

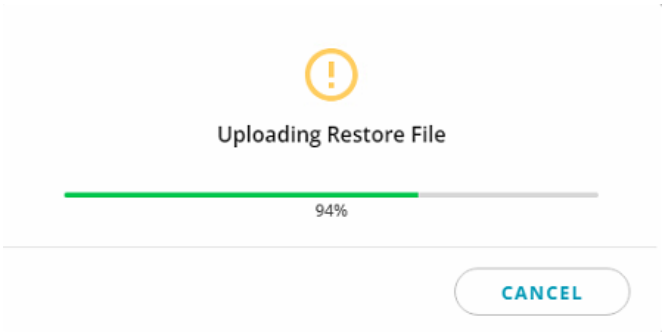


Figure 93: Uploading File

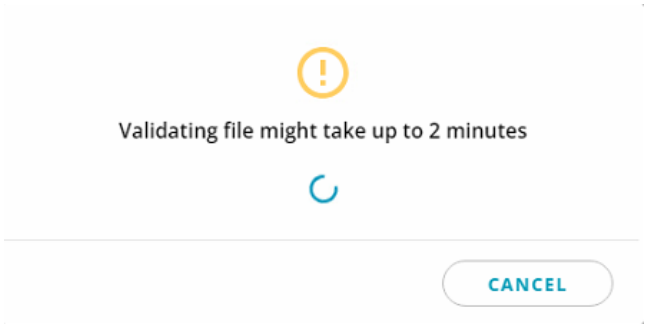


Figure 94: Validating File

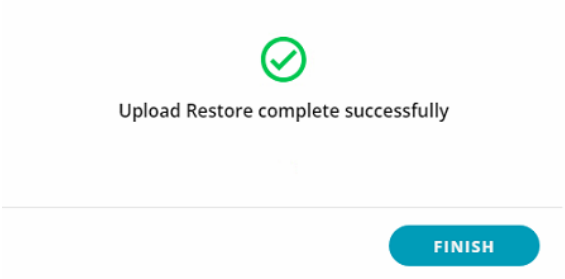


Figure 95: File validated and updated

If the file is successfully validated, then you could proceed with the software restore.

The new SW file compatibility should be checked and the file also (see screenshot below).

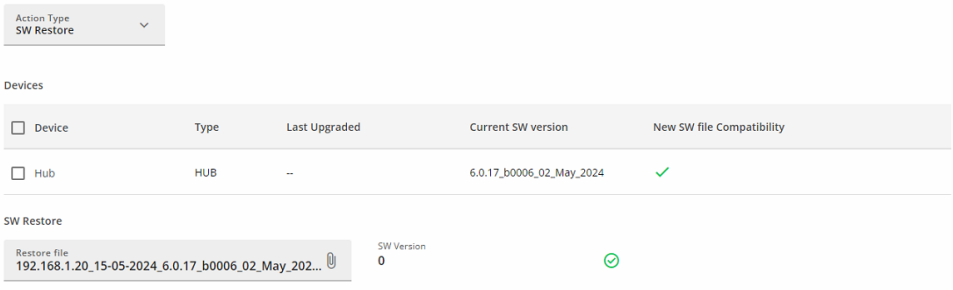


Figure 96: Ready for restore

To start the software restore operation, you need to select on which device you want to proceed and click on the 'Restore' button.

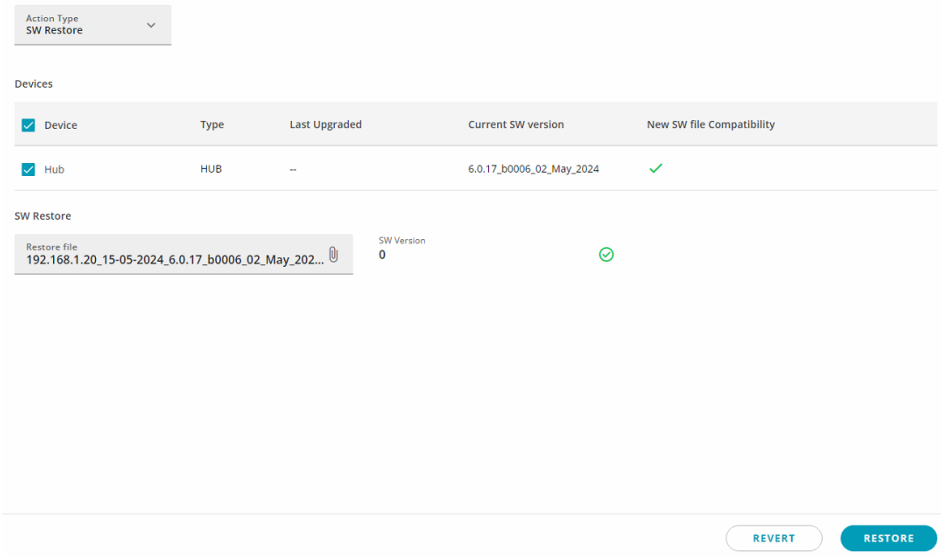


Figure 97: Device Selection

When clicking on 'Restore' a pop-up window will open to ask you validating the restore operation.

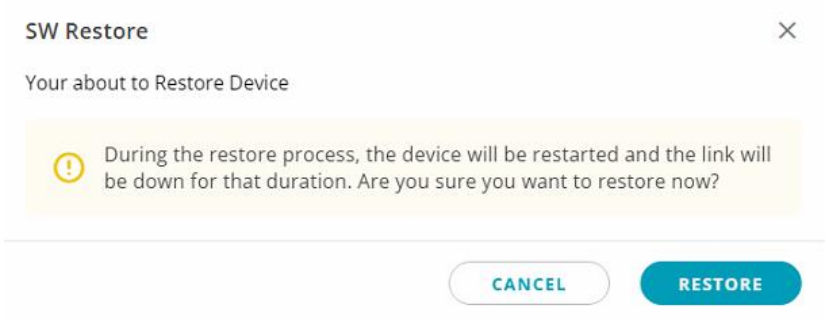


Figure 98: Restore Approval

When clicking again on 'Restore' it launches the software restore.

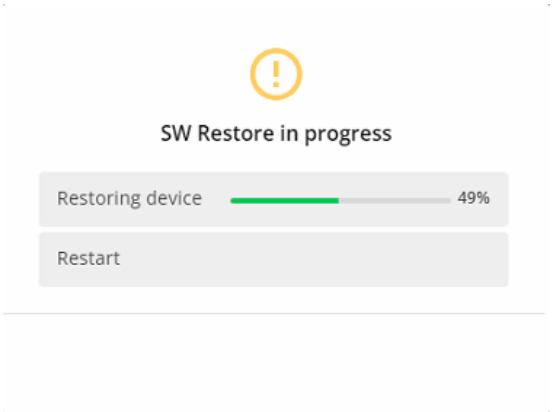


Figure 99: Restore Running

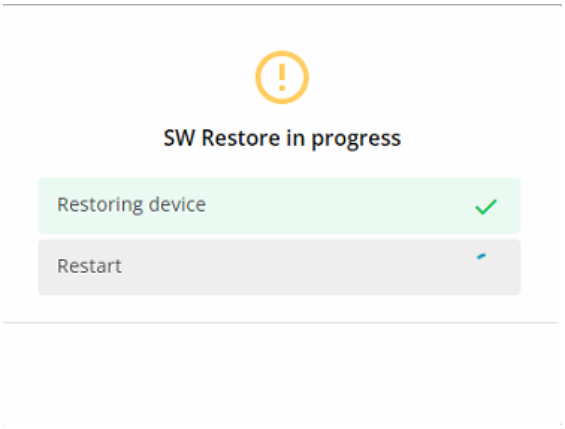


Figure 100: Restore Finished and Restart

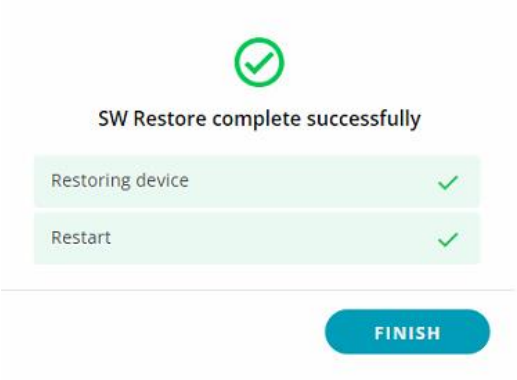


Figure 101: Restart Finished

8.2 Rebooting the ODU

You can reboot the ODU by clicking **REBOOT** for the Hub or Client ODU as required.

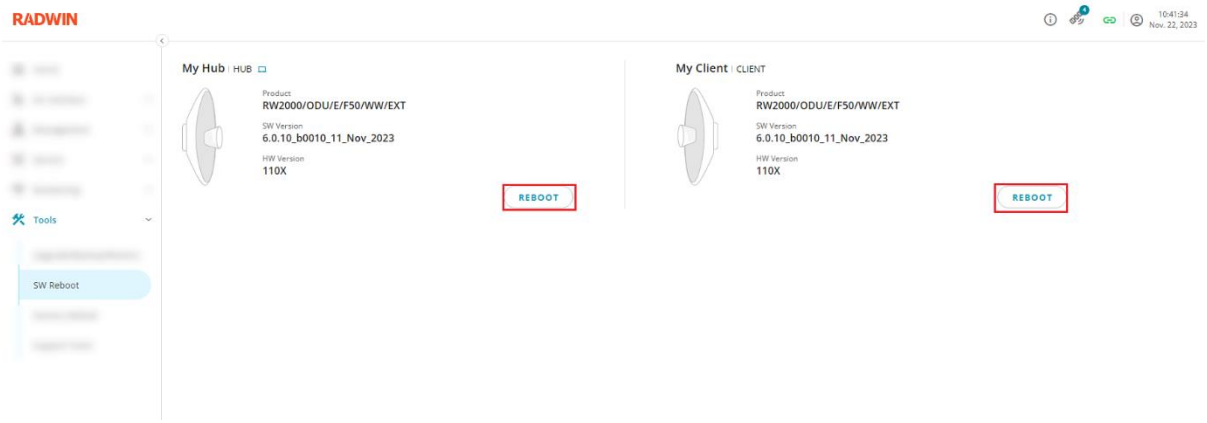


Figure 102: Rebooting the ODU

During the reboot, a timer appears. When the ODU reboots, you will need to login again.

8.3 Resetting the ODU to Factory Defaults

You can restore the ODU to factory defaults by clicking **RESET TO FACTORY DEFAULT** for the Hub or Client ODU as required.

The IP and VLAN settings can be preserved after a factory reset by checking the **Preserve IP and VLAN** checkmark.

Note

The IP address is kept unchanged after a factory reset.

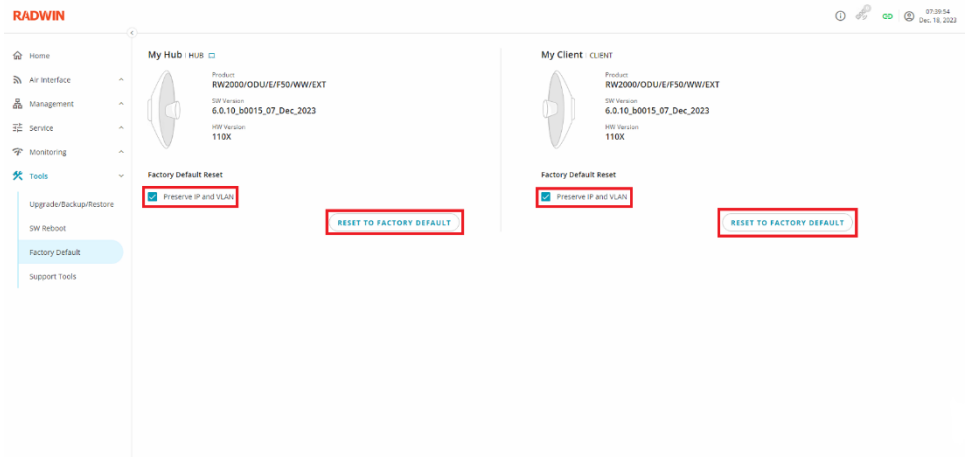


Figure 103: Resetting the ODU to Factory Defaults

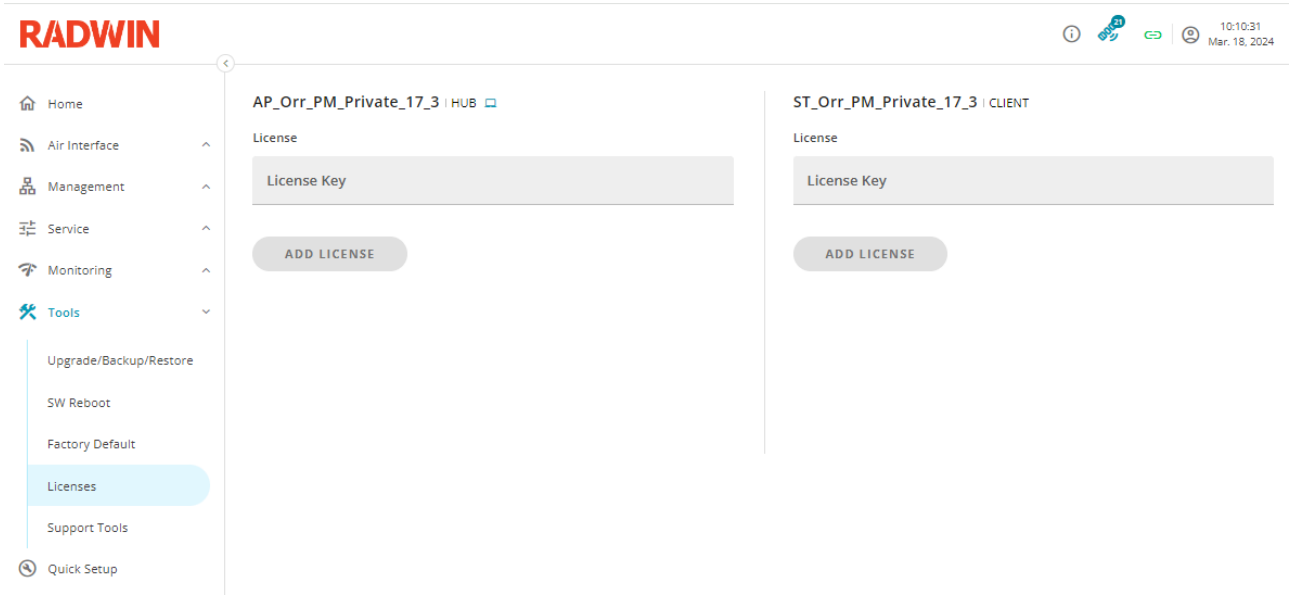
Warning

Resetting the ODU to factory default will erase all the device configuration, including Air interface parameters and user passwords. You need to make sure you will be able to connect to the device after you perform the factory reset.

8.4 Licenses

By default, bands are restricted based on GPS location. Sometimes, the device needs to be deployed in areas where the GPS antenna cannot get a signal, or the operator could have authorization to operate on unlicensed bands.

In all these cases, the device will need a license to operate.



Note

If you need a license to operate, please contact your RADWIN representative.

You need to apply for a license key on both devices, the Hub and the Client.

When you receive your license keys, you will need to enter the license key in the 'License' field and then click on the 'Add License' button to apply it.

Note

In case of reboot or upgrade/restore, the license is kept.

8.5 Support Tools

Note

These operations can only be performed on the local unit to which the browser is connected. To perform these operations on the remote ODU, you must connect to its own UI.

8.5.1 Logs

The following tool can be used to assist you when dealing with tech support:

Download Logs - download the logs that have been collected in the ODU.

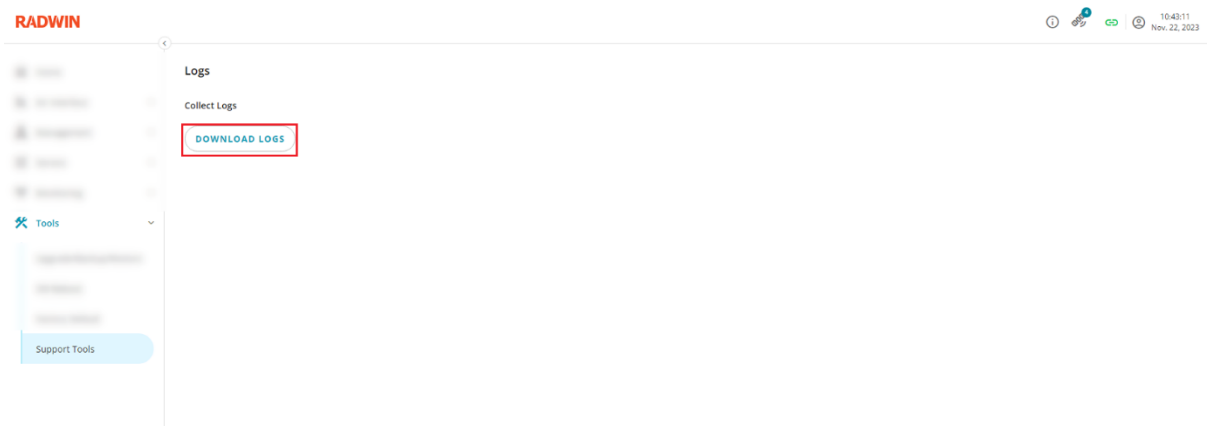


Figure 104: Supporting Tools

8.5.2 Buzzer Alignment

After the installation of the devices, the buzzer alignment tool allows to optimize the alignment on both sides of the link.

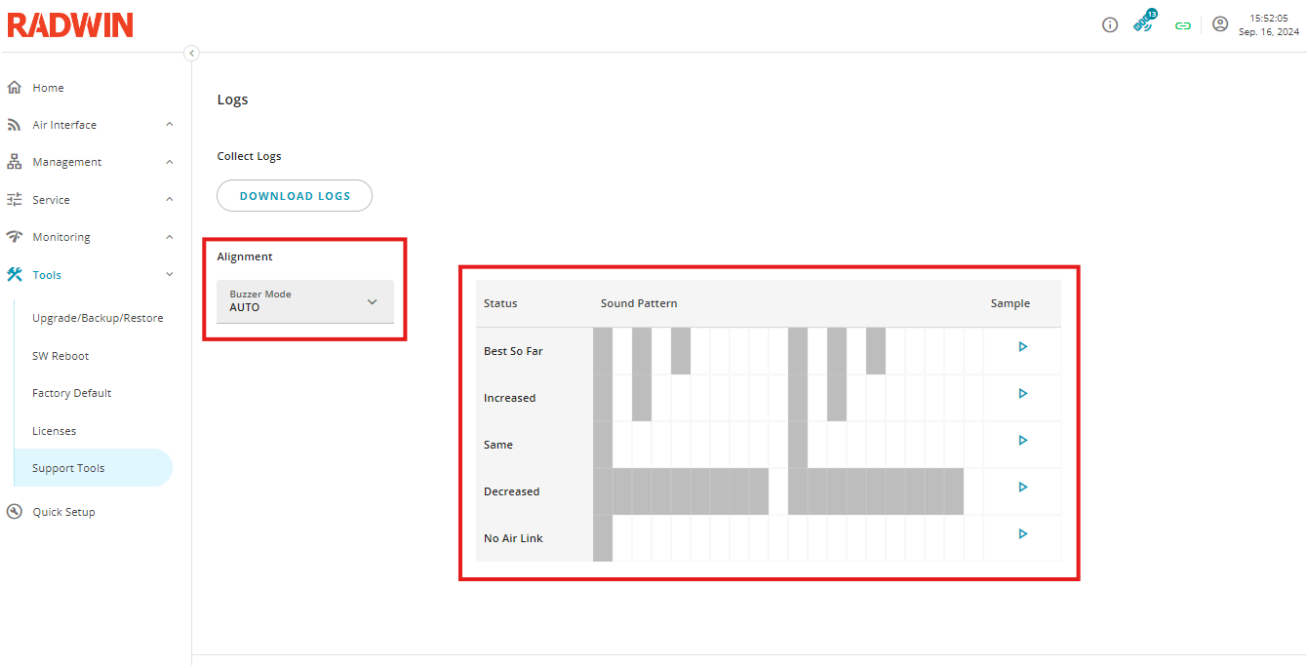


Figure 105: Buzzer Alignment

The buzzer emits different sound patterns depending on the status of the RSS:

- **Best so far**: The current alignment is the most optimized until now
- **Increased**: RSS improved compared to the previous position
- **Decreased**: RSS decreased compared to the previous position
- **Same**: No change in the RSS
- **No Air Link**: No link detected

When the buzzer is active, the RSS is measured every second and the sound pattern updated consequently.

The buzzer works in 3 different modes:

- **Off**: The buzzer is inactive.
- **On**: The buzzer is always active even after registration of the client on the Hub side.
- **Auto**: After registration of the Client on the Hub side, the buzzer goes silent but is still active.

By default, the buzzer is in Auto mode.

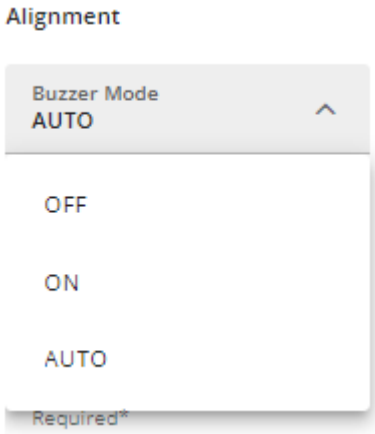


Figure 106: Buzzer Modes

Note

A sound pattern map is provided to identify the different sounds emitted by the buzzer. An audio record is also available for each sound to help identify them. By playing on the play button, you could hear each sound.

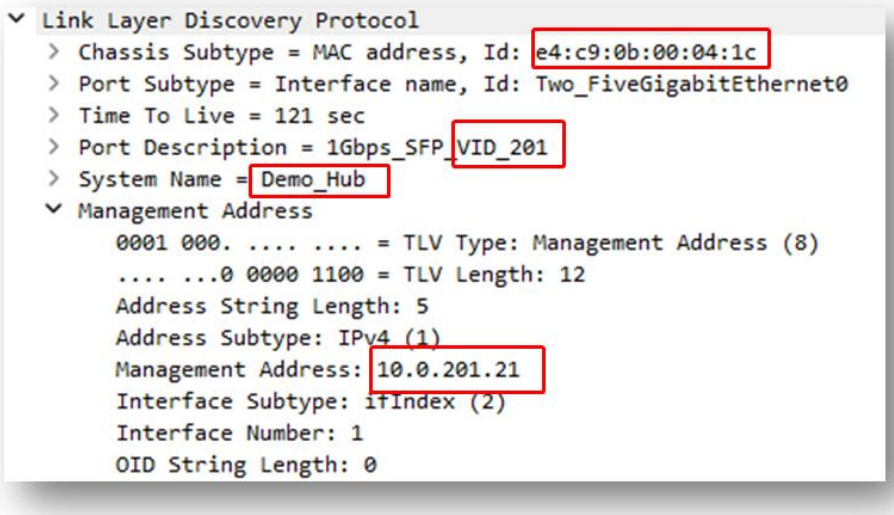
9 Troubleshooting

9.1 ODU Discovery via LLDP

By default, LLDP discovery is enabled for 5 minutes after boot (see Protocols screen). We recommend not to change this setting in order to facilitate device discovery in any scenario.

9.1.1 Discovery on local PC using Wireshark

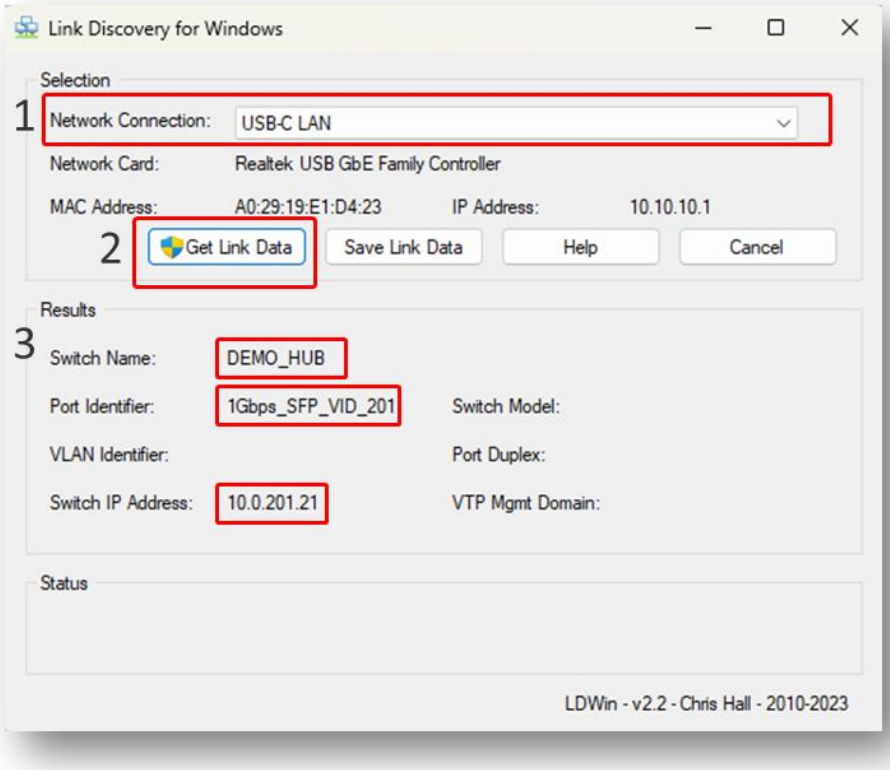
- Select your network interface and run capture
- Set capture filter for LLDP
- Connect the 2000E ODU via POE injector directly to your PC
- After up to 30 seconds, LLDP frame should appear (RADWIN MAC starts with E4:C9:0B)



- See Protocols section for details on LLDP TLVs

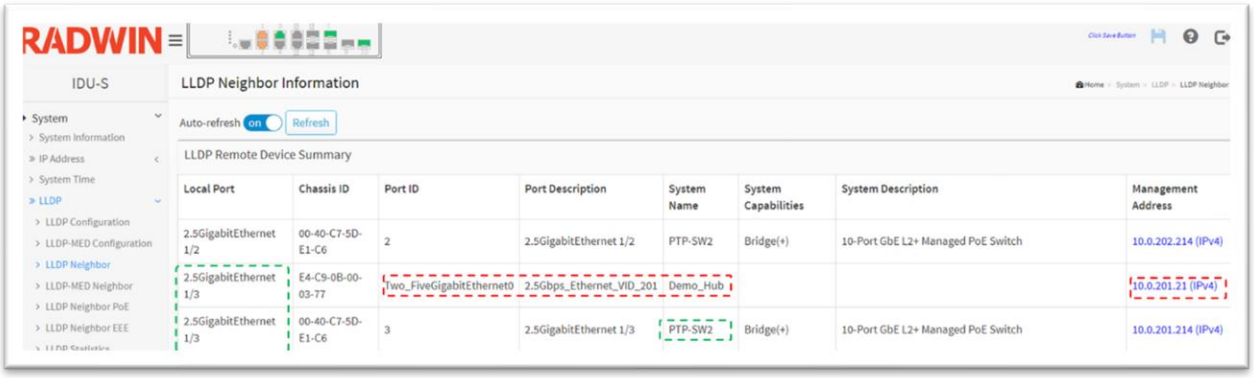
9.1.2 Discovery on local PC using LDWin

- **Download and run the open-source LDWin tool (https://github.com/chall32/LDWin)**
- Connect the 2000E ODU via POE injector directly to your PC
- Select your Network Connection **(1)**
- Press the Get Link Data button **(2)**
- After up to 30 seconds, the following data is shown **(3)**
    - Device name (as “Switch name”)
    - Port name and Management VID (as “Port ID)
    - Management IP (as “Switch IP Address”)



9.1.3 Remote discovery via managed network device

- Enable LLDP receive on IDU-S, IDU-SI or any other managed device supporting LLDP
- Power cycle the 2000E unit (on a POE switch such as RADWIN IDU-S / IDU-SI this can be done remotely by disabling and re-enabling enabling POE output on the relevant port)
- Check LLDP Neighbor Information for Chassis ID with RADWIN MAC **E4:C9:0B**
- See example below for RADWIN IDU-S



9.2 ODU Discovery via ARP

1. In a command line, `arp -a | findstr E4:C9:0B` to filter IP addresses by the MAC address. if running Linux or Mac, use `grep` instead of `findstr`.
2. The IP address of the unit is displayed.

9.3 Replacing a Device in the Link

You can substitute a different Hub or Client in a linked pair.

The devices must be in a deregistered state for them to be able to connect to a different device. For more information see Registered/Deregistered Devices.

To substitute a Hub or Client for a different one:

1. Switch ON the alternate ODU
2. Make sure the ODU is configured to be Hub / Client - according to its intended role in the link (same role as the ODU being replaced)
3. Make sure the link ID of the 2 devices between which you wish to establish a link - is identical.
4. Reset the Hub or Client that you want to replace (from tools->SW reboot->click "**REBOOT**").
5. While the device is being reset, enter the browser user interface of the other ODU in the link, and deregister the link (Home-> click "**DEREGISTER**").
6. Automatically, the Hub will rewind to Quick Setup mode.
7. Go through the whole Quick Setup until the alignment step.
8. The alternate ODU and the current ODU will now establish a link.
9. Finish the Quick Setup process to get devices in sync.
10. When a link is established between the ODUs, register the link (Home -> click "**REGISTER")**.

10 Appendixes

10.1 Web UI Events Table

The following events are supported in the system and displayed in the browser user interface.

Event text	Comments
Login attempt by <username> failed / succeeded	Login attempt to browser user interface
Ethernet Service was opened / closed	Link is active (non-active) and traffic is enabled (disabled)
Link is up	Link between Hub and Client established
Link is down due to <reason>	Link between Hub and Client dropped Possible reasons: Bad quality: link disconnected due to weak signal or high interference User request: link disconnected due to user changing air interface configuration (e.g., CBW, Channel, Tx Ratio)
Link state changed to <new state>	
LAN / SFP disconnected	LAN / SFP Cable was disconnected
LAN / SFP connected	LAN / SFP Cable was connected
Configuration was changed	
BIT succeeded - radio initialization succeeded	Internal device built-in-test on boot succeeded
ODU is Ready (Cold Start)	Device boot completed
GPS detected country is different than the user defined	User manually selected a country. The device GPS identified a different country than the user selected. The new country has the same regulation as the previous country. Service was not interrupted.
GPS detected regulation is different than user defined	User manually selected a country. The device GPS identified a different country than the user selected. The new country has different regulations than previous country. Service was stopped. User must select a band supported by the regulation of the detected country.
SW upgrade was finished successfully to unit	
Failed to upgrade unit	
1PPS synchronized	Synchronization of the frames based on the GPS is working
1PPS unsynchronized	Synchronization of the frames based on the GPS is not usable

10.2 RADIUS Server Configuration

10.2.1 Data Dictionary supplement

This is a supplement to the standard RADIUS Data Dictionary which defines the user profiles. The examples below are for FreeRADIUS configuration files but can be adapted to other RADIUS servers.

Supported parameters (attributes):

- User permissions profile (Attribute 10)

  2000 E currently does not support user profiles, this parameter cannot be used.

- User Session timeout (Attribute 11)

  This is the timeout in seconds for a connected user session.

Data dictionary supplement for RADIUS user authentication:

```
#vendor id
VENDOR RADWIN 4458
BEGIN-VENDOR RADWIN
# User Session Timeout
ATTRIBUTE RADWIN_SessionTimeout 11 integer
END-VENDOR RADWIN
```

10.2.2 User definitions

Users file example for FreeRADIUS:

```
# User Name = User_Conf, Password = SunBoss_365, Read-Write
# permissions HBS and HSU, Timeout 24h
User_Conf Cleartext-Password := "SunBoss_365" 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_SessionTimeout = 3600
```

This above example shows that there are two users with the following usernames: User_Conf and LocalTech.

For user *User_Conf*:

- Password = SunBoss_365
- Timeout value is 86,400 seconds (24-hour access from the time of log on)

For user *LocalTech*:

- Password = Moon_Crater
- Timeout value is 3600 seconds (1-hour access from the time of log on)

10.3 Terminology

ACRONYM	DEFINITION
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
ARQ	Automatic Repeat Request
BPSK	Binary Phase-shift Keying
DIFFSERV	Differentiated Services
DL	Download
EIRP	Effective Isotropic Radiated Power
FEC	Forward Error Correction
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
IP	Internet Protocol
LAN	Local Area Network
LLDP	Link Layer Discovery Protocol
MCS	Modulation Coding Scheme
MIMO	Multiple Input Multiple Output
MIR	Maximum Information Rate
ODU	Outdoor Unit
OFDM	Orthogonal Frequency Division Multiplexing
POE	Power Over Ethernet
QOS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RSS	Receive Signal Strength
SFP	Small Form-factor Pluggable
SNMP	Simple Network Management Protocol
SSID	Service Set Identifier
TCP	Transmission Control Protocol
TDD	Time-Division Duplex
TX	Transmit
UL	Upload
VLAN	Virtual Local Area Network
WFQ	Weighted Fair Queueing

10.4 User Handbook Notice

10.4.1 RADWIN 2000 Family

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 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 on 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.

10.4.2 FCC

Standard power APs and Fixed clients are prohibited on oil platforms, cars, trains, boats, and aircraft.

Transmitters in the 5.925-7.125 GHz band are prohibited from operating to control or communicate with unmanned aircraft systems.

10.4.3 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.

10.4.4 Trademarks

WinLink 1000, RADWIN 2000 are trademarks of RADWIN Ltd.

Windows 2000, XP Pro, Vista, Windows 7 and Internet Explorer are trademarks of Microsoft Inc.

Mozilla and Firefox are trademarks of the Mozilla Foundation. Other product names are trademarks of their respective manufacturers.