Wi-Fi 6 Access Point

Software Release 12.5.3

User Manual

www.edge-core.com

User Manual

Wi-Fi 6 Access Point

Cloud-Enabled Enterprise Access Points
EAP101
EAP102
EAP104
EAP104 (WL)
EAP111
OAP101

E032024-CS-R14

How to Use This Guide

This guide includes detailed information on Edgecore access point (AP) software, including how to operate and use the management functions of APs. To deploy APs effectively and ensure trouble-free operation, you should first read the relevant sections in this guide so that you are familiar with all software features.

Who Should Read This Guide?

This guide is for network administrators who are responsible for operating and maintaining network equipment. The guide assumes a basic working knowledge of LANs (Local Area Networks) and the Internet Protocol (IP).

How This Guide is Organized

The organization of this guide is based on the AP's web management interface. An introduction and initial configuration information is also provided.

The guide includes these sections:

- Section I "Getting Started" — Includes an introduction to AP management and initial configuration settings.
- Section II "Web Configuration" — Includes all management options available through the web interface.
- Section III "Appendices" — Includes information on troubleshooting AP management access.

Related Documentation

This guide focuses on AP software configuration, it does not cover hardware installation of an AP. For specific information on how to install an AP, see the following guide:

Quick Start Guide

For all safety information and regulatory statements, see the following documents:

Quick Start Guide

1Doc: Protocolo 1.943/2025 | Anexo: em 1Doc 7 Pág 5 de 321 Assinado por 1 administrador(a) em 29/12/2025 - Anexo I - WiFi 6 AP_2025_portal_v3.28.pdf (3/260) 2269/4746

Conventions

The following conventions are used throughout this guide to show information:

Note: Emphasizes important information or calls your attention to related features or instructions.

Caution: Alerts you to a potential hazard that could cause loss of data, or damage the system or equipment.

Revision History

This section summarizes the changes in each revision of this guide.

March 2024 Revision

This is the 14th revision of this guide. It is valid for software release v12.5.3 and includes the following changes:

- Minimum Signal Allowed setting for each SSID, see "Wireless Networks — General Settings" on page 69
- Added Device OS Blacklist, see "Wireless Networks — General Settings" on page 69

January 2024 Revision

This is the 13th revision of this guide. It is valid for software release v12.5.0 and includes the following changes:

- Added support for EAP111
- Added RADIUS NAS ID, see "Wireless Networks — Security Settings" on page 70
- Modified Minimum Signal Allowed default, see "Physical Radio Settings" on page 65
- Added OpenRoaming captive portal, see "OpenRoaming" on page 58
- Added OpenRoaming NAI Realm List Method/Authentication, see "OpenRoaming" on page 58
- Added Syslog Level, see "System Settings" on page 83

September 2023 Revision

This is the 12th revision of this guide. It is valid for software release v12.4.3 and includes the following changes:

- Added support for OAP101

1Doc: Protocolo 1.943/2025 | Anexo: em1_04C7D8805AD2E32AB662B8E_Solicitacao-029_2025_Anexo_Anexo_WiFi6_029_2025_pdf_6328.pdf (4/200) 2270/4746

- Added SSID isolation, see "Physical Radio Settings" on page 65
- Multiple PSK enhancement, see "Wireless Networks — Security Settings" on page 70

July 2023 Revision

This is the 11th revision of this guide. It is valid for software release v12.4.1 and includes the following changes:

- Added OpenRoaming, see "OpenRoaming" on page 58 and "Wireless Networks — OpenRoaming" on page 78
- Modified broadcast rate, see "Physical Radio Settings" on page 65
- Access Control List enhancement, see "Wireless Networks — Security Settings" on page 70
- Hostname enhancement, see "System Settings" on page 83
- Moved the language setting to the System page, see "System Settings" on page 83
- Firmware upgrade enhancement, see "Upgrading Firmware" on page 88
- Account username enhancement, see "User Accounts" on page 89

May 2023 Revision

This is the 10th revision of this guide. It is valid for software release v12.4.0 and includes the following changes:

- Added WAN port auto-detection to QR code Onboarding, see "QR Code Onboarding" on page 27
- Added automatic mesh AP configuration, see "Mesh AP Configuration" on page 30
- Removed Mark and Notrack from firewall rules, see "Firewall Rules" on page 51
- Modified Minimum Signal Allowed, see "Physical Radio Settings" on page 65
- Added RF Isolation, see "Physical Radio Settings" on page 65
- Modified Dynamic VLAN, see "Wireless Networks — Network Settings" on page 76
- Modified HotSpot 2.0 settings, see "Wireless Networks — Network Settings" on page 76
- Added Log Level, see "System Settings" on page 83

1Doc: Protocolo 1.943/2025 | Anexo: em1_04C7D8305AD2E32AB662B8E_pro_administrativo_2025_assinado_WiFi6_AP_2025_parte_8328.pdf (5/200) 2282/4726

- Added SNMPv3 User, see "SNMP" on page 94
- Modified Diagnostics and added Speed Test, see "Diagnostics" on page 98

January 2023 Revision

This is the ninth revision of this guide. It is valid for software release v12.3.0 and includes the following changes:

- Updated QR code Onboarding, see "QR Code Onboarding" on page 27
- Updated wireless status, see "Wireless Status" on page 38
- Added support for dynamic PSK, see "Wireless Networks — Security Settings" on page 70
- Updated Hotspot 2.0 settings, see "Wireless Networks — Network Settings" on page 76
- Added CAPWAP Tunnel Interface to Ethernet Settings, see "Ethernet Settings" on page 46

November 2022 Revision

This is the eighth revision of this guide. It is valid for software release v12.2.0 and includes the following changes:

- Added Airtime Fairness, see "Physical Radio Settings" on page 65
- Modified the value range of BSS Coloring, see "Physical Radio Settings" on page 65
- Modified wireless security default, see "Wireless Networks — Security Settings" on page 70
- Added 802.11v, see "Wireless Networks — Security Settings" on page 70
- Added SNMP Trap, see "SNMP" on page 94
- Added BLE Scan, see "BLE" on page 97

November 2022 Revision

This is the seventh revision of this guide. It is valid for software release v12.1.0 and includes the following changes:

- Updated SNMP read/write community settings, see "SNMP" on page 94
- Added BLE radio Tx Power, see "BLE" on page 97
- Added Interference Detection, see "Physical Radio Settings" on page 65

- Added zero-touch provisioning information, see "Zero-Touch Provisioning" on page 20
- Modified the default value for Minimum Signal Allowed, see "Physical Radio Settings" on page 65
- Added 160MHz channel bandwidth option, see "Physical Radio Settings" on page 65
- Removed uCentral cloud option from the Setup Wizard.

July 2022 Revision

This is the sixth revision of this guide. It is valid for software release v12.0.0 and includes the following changes:

- Updated Setup Wizard for uCentral cloud, see "AP Setup Wizard" on page 22
- Added Proxy ARP, see "Wireless Networks — Network Settings" on page 76
- Added Multicast-to-Unicast Conversion, see "Wireless Networks — General Settings" on page 69
- Added Bandsteering, see "Physical Radio Settings" on page 65
- Added WPA3 Enterprise 192-bit and OWE security, see "Wireless Networks — Security Settings" on page 70
- Added multiple PSK keys, see "Wireless Networks — Security Settings" on page 70
- Added Short Guard Interval (SGI), see "Wireless Networks — Advanced Radio Settings" on page 79
- Added Multicast/Broadcast Rate, see "Physical Radio Settings" on page 65
- Added UPnP, see "LAN Settings" on page 49
- Added DHCP Snooping, see "DHCP Snooping" on page 61
- Added ARP Inspection, see "ARP Inspection" on page 62
- Added DHCP Relay, see "DHCP Relay" on page 63
- Added IPv6 for Internet access, see "IPv6 Settings" on page 46
- Added Hotspot 2.0, see "Wireless Networks — Network Settings" on page 76
- Added Device Discovery Tool, see "Device Discovery" on page 99

1Doc: Protocolo 1.943/2025 | Anexo: em1_04C7D830...pdf (7/200) 2273/4726

- Added Discovery Agent settings, see "Edgecore Networks Discovery Tool" on page 91
- Added Reset button and LED enable, see "System Settings" on page 83
- Added PoE Out setting, see "Ethernet Settings" on page 46
- Added caution on firmware upgrades in uCentral mode, see "Upgrading Firmware" on page 88

April 2022 Revision

This is the fifth revision of this guide. It is valid for software release v11.6.0 and includes the following changes:

- Added Client mode, see "Physical Radio Settings" on page 65
- Added Site Survey, see "Wireless Networks — General Settings" on page 69
- Added Custom LAN, see "LAN Settings" on page 49
- Added WME configuration, see "Physical Radio Settings" on page 65
- Added BSS Coloring, see "Physical Radio Settings" on page 65
- Added OFDMA, see "Physical Radio Settings" on page 65
- Added Target Wake Time, see "Physical Radio Settings" on page 65
- Added HTTPS captive portal, see "Captive Portal Settings" on page 56
- Added HTTPS certificate upload, see "Upload Certificate" on page 88

December 2021 Revision

This is the fourth revision of this guide. It is valid for software release v11.4.0 and includes the following changes:

- Updated QR code onboarding, see "QR Code Onboarding" on page 27
- Added mesh traffic graph to the dashboard, see "Traffic Graphs" on page 40
- Added MSP mode, see "System Settings" on page 83

November 2021 Revision

This is the third revision of this guide. It is valid for software release v11.3.1 and includes the following changes:

- Updated the Setup Wizard, see "AP Setup Wizard" on page 22
- Updated the Dashboard, see "Status Information" on page 33

1Doc: Protocolo 1.943/2025 | Anexo: em1_04C7D830D2E32AB6628B_pt_administrativo_029_2025_anexo_ao_oficio_029_2025_parte_328.pdf (8/200) 2275/4726

- Added Smart Isolation, see "LAN Settings" on page 49
- Added Hotspot Settings, see "Hotspot Settings" on page 53
- Updated wireless network settings, see "Wireless Networks — Network Settings" on page 76
- Updated wireless open mesh settings, see "Wireless Networks — Open Mesh Settings" on page 78
- Added Telnet settings, see "Telnet" on page 91
- Added web server settings, see "Web Server" on page 91
- Added multicast DNS, see "Multicast DNS" on page 95
- Added firewall settings, see "Firewall Rules" on page 51
- Added a guest network, see "LAN Settings" on page 49

July 2021 Revision

This is the second revision of this guide. It is valid for software release v11.2.0 and includes the following changes:

- Added WPA3-Personal transition, WPA3-Enterprise, and WPA3-Enterprise transition. See "Wireless Networks — Security Settings" on page 70
- Support for IEEE 802.11 k/r, see "Wireless Networks — Security Settings" on page 70
- Added Minimum signal allowed (RSSI Threshold), see "Physical Radio Settings" on page 65
- Support for Open Mesh, see "Wireless Networks — Open Mesh Settings" on page 78
- SNMP v2 support, see "SNMP" on page 94
- Support for remote Syslog, see "Remote System Log Setup" on page 92
- Support for LLDP, see "LLDP" on page 96
- Support for management by an EWS-Series Controller, see "System Settings" on page 83

April 2021 Revision

This is the first revision of this guide. It is valid for software release v11.1.1.

1Doc: Protocolo 1.943/2025 | Anexo: em1_D4C7D830D2E32AB6628E_pt_administrador_v2_Anexo_WiFi6_029_2025_pt_0328.pdf (9/200) 2276/4746

1Doc: Protocolo 1.943/2025 | Anexo: em_1Doc_7B8D5AD8E32AB662B9E_processo_administrativo_029_2025_Anexo_I_MiFi6_029_2025_Part_0328.pdf (10/200) 1276/4746

Contents

1Doc: Protocolo 1.943/2025 | Anexo: em1D4C7D8805AD8E32AB062B9E... Assoc_atamis... 8/9/2025 ...Anexo_atamis_WiFi6_AP_2025_part_0328.pdf (11/200) 2237/4746

1Doc: Protocolo 1.943/2025 | Anexo: em_04C7D8805AD8E32AB6628B6E_Assoc_Administrativo_029_2025_Anexo_I_MiFi6_029_2025_Part_0328.pdf (12/200) 2939/4746

1Doc: Protocolo 1.943/2025 | Anexo: em_04C7B8805AD8E32AB662B9E_pdf_Edgecore_Administrador_Web_Anexo_MiFi6_029_2025_Parte_0328.pdf (13/200) 2270/4746

Figures

1Doc: Protocolo 1.943/2025 | Anexo: em_04C7B8805AD8E32AB662B9E_processo_administrativo_02_2025_Anexo_Anexo_VI_6_29_2025_14_03_28.pdf (15/200) 1292/4746

Figures

1Doc: Protocolo 1.943/2025 | Anexo: em_04C7B8805AD8E32AB062B9E_pdf_Termo_de_Referência_029_2025_Anexo_I_MiFi_029_2025_Part_0328.pdf (16/200) 1292/4746

Tables

1Doc: Protocolo 1.943/2025 | Anexo: em_1_04C7D8805AD8E32A1B662B9E_processo_administrativo_2025_Anexo_Anexo_MVF_6_29_2025_14_03_28.pdf (17/200) 2993/4726

Section I

Getting Started

This section provides an overview of the access point, and introduces some basic concepts about wireless networking. It also describes the basic settings required to access the management interface.

This section includes these chapters:

1Doc: Protocolo 1.943/2025 | Anexo: em_1_04C7D8805AD8E32AB662B9E_pdf_Termo_de_Referência_e_Anexos_Anexo_I_-_MiFi_6_429_2025_Part_0328.pdf (18/200) 2995/4746

1 Introduction

The access point (AP) runs software that includes a network management agent. The agent offers a variety of management options, including a web-based interface. The AP can also be accessed through Secure Shell (SSH) for configuration using a command line interface (CLI).

Note: This manual describes the configuration interface for stand-alone mode. Refer to the Edgecore *ecCLOUD Controller User Manual* for information on configuring the AP through the cloud interface.

This chapter includes the following sections:

1Doc: Protocolo 1.943/2025 | Anexo: em1_04C7B8805AD8E32AB062B9E_pdf_Termo de Referência_Processo Administrativo_Pregão Eletrônico_Anexo I_Edital_ANEXO I_ECW6-629_2025_Part_0328.pdf (19/200) 2996/4746

Configuration Options

The access point's web agent allows you to configure AP parameters, monitor wireless connections, and display statistics using a standard web browser. The AP's web management interface can be accessed from any computer attached to the network.

The CLI program can be accessed remotely by a Secure Shell (SSH) connection over the network. The CLI is used primarily for technical support.

The AP's web interface allows you to perform management functions such as:

- Set management access user names and passwords
- Configure IP settings
- Configure 2.4 GHz, and 5 GHz radio settings
- 5 GHz, and 6 GHz radio settings
- Control access through wireless security settings
- Filter packets using Access Control Lists (ACLs)
- Download system firmware
- Download or upload configuration files
- Display system information

Zero-Touch Provisioning

APs can be automatically managed by the Edgecore ecCLOUD controller or an EWS-Series controller. If an AP is already registered with the ecCLOUD controller, it will be automatically managed when the WAN port of the AP is connected to the Internet.

When an AP is connected to a local LAN with an EWS-Series controller, the AP can be configured with the controller IP address through DHCP Option 138 and then automatically managed by the controller.

As an alternative to zero-touch provisioning, you can manually set the preferred management method from the web interface, see "System Settings" on page 83.

1Doc: Protocolo 1.943/2025 | Anexo: em_04C7B8805AD8E32AB062B6E_pt_Termo de Referência 029_2025_Anexo I_MiFi 6_029_2025_Part_0328.pdf (20/200) 2096/4746

Connecting to the Web Interface

For first-time access to the AP's web management interface, you can connect a PC directly to one of the AP's LAN ports or use the quick-setup QR code (printed on a label next to the AP's ports). The first-time you access the web interface, it automatically runs the Setup Wizard for initial AP configuration.

For information on the Setup Wizard, see "AP Setup Wizard" on page 22.

For information on using the QR code, see "QR Code Onboarding" on page 27.

LAN Port Connection

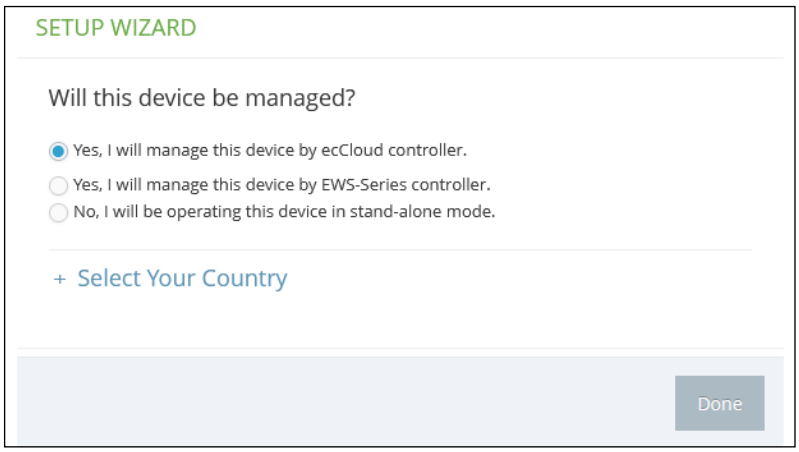
When connecting to the web management interface through one of the AP's LAN ports, the AP has a default management IP address of 192.168.2.1 and a subnet mask of 255.255.255.0. Therefore, you must set your PC IP address to be on the same subnet as the AP (that is, the PC and AP addresses must both start with192.168.2.x).

Note: To connect to the web interface using the Uplink(PoE) port, the IP address is automatically assigned through DHCP by default. If a DHCP server is unreachable, the Uplink(PoE) port reverts to a fallback IP address of 192.168.1.10.

To access the AP's web management interface, use your web browser to connect to the management interface by entering the default IP address of 192.168.2.1.

For first-time access, there is no user login and the Setup Wizard starts automatically. Follow the steps described in "AP Setup Wizard" on page 22.

Figure 1: Web Management Login



Note: To configure the AP with a different management IP address that is compatible with your network, see "LAN Settings" on page 49.

1Doc: Protocolo 1.943/2025 | Anexo: em_04C7B805AD8E32AB62B6E_proc_admin_822_2025_anexo_1_MiFi6_UG_2025_04_0328.pdf (21/200) 2997/4746

AP Setup Wizard

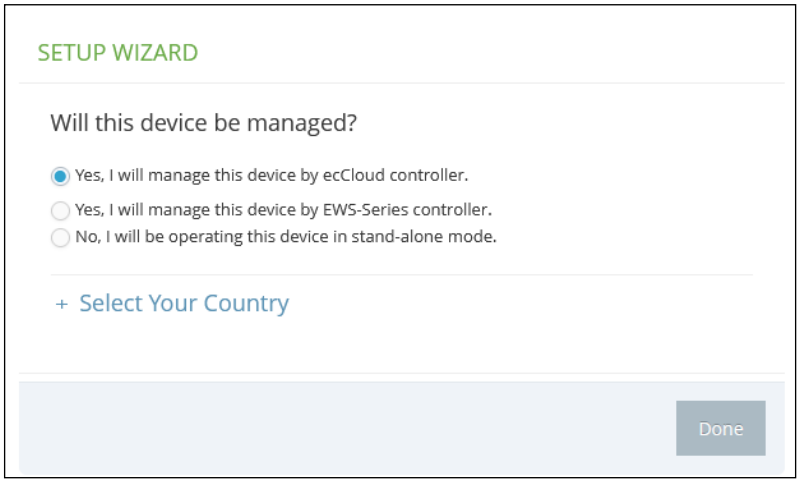
The Setup Wizard is designed to help you configure the basic settings required to get the AP up and running.

Step 1 Select How the AP will be Managed — To manage the AP using the Edgecore ecCLOUD controller, select "Yes, I will manage this device by ecCloud controller," and then continue to Step 6.

To manage the AP using the an Edgecore EWS-series controller, select "Yes, I will manage this device by EWS-Series controller," and then continue to Step 2.

Otherwise, select "No, I will be operating this device in stand-alone mode" and continue to Step 3.

Figure 2: Select ecCloud, EWS Controller, or Stand-Alone



If you select to manage the AP using the Edgecore ecCLOUD controller, go to cloud.ignitenet.com to register your AP. Log in and select Devices from the menu. Click Add Device and enter the AP serial number and MAC address to register the AP with your cloud network. The serial number and MAC address can be found on the product packaging or label.

Note: This manual describes the configuration interface for stand-alone mode. Refer to the Edgecore *ecCLOUD Controller User Manual* for information on configuring the AP through the cloud interface or the *EWS-Series Controller User Manual* for information on managing the AP through an EWS controller.

1Doc: Protocolo 1.943/2025 | Anexo: em branco - Termo de referência - Anexo I - Minuta_ARP_2025_04_0328.pdf (22/200) 2999/4746

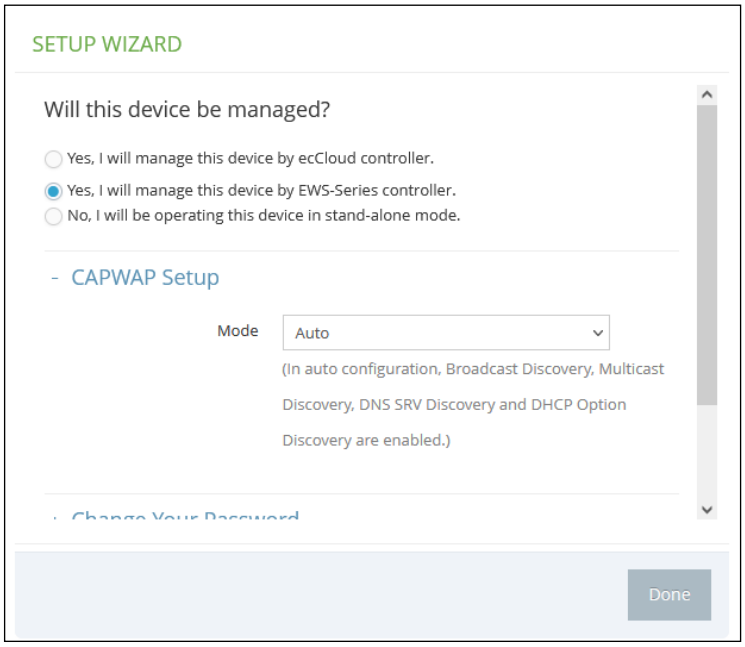
Step 2 CAPWAP Setup — When EWS-Series Controller management is selected, you can set the mode for discovering the controller. Once the AP has discovered the controller on the network it can then send a CAPWAP (Control And Provisioning of Wireless Access Points) join request.

In Auto mode, the AP uses four methods to discover the controller. These methods require no further configuration.

In manual mode, two options are available. Specify the Domain Name Suffix so that the AP can use DNS server records to discover the EWS controller. Or, just specify a static IP address for the controller.

For more information on CAPWAP setup, see "System Settings" on page 83.

Figure 3: CAPWAP Setup



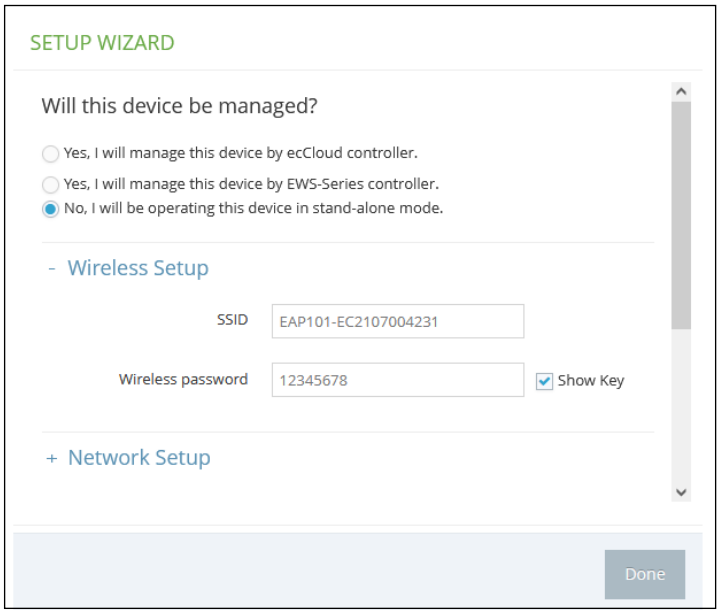
After completing the CAPWAP setup, continue with Step 5.

Step 3 Wireless Setup — If you select to manage the AP in stand-alone mode, you can configure the default wireless network.

The default wireless network name (SSID) consists of the AP model and its serial number, and there is a default wireless password. You have the option to modify the wireless network name and password to your preferred configuration. The wireless name must be 1-32 ASCII characters, and the password must be 8 to 63 ASCII characters (no special characters are allowed).

1Doc: Protocolo 1.943/2025 | Anexo: em_04C7B80D5AD8E32AB062B6E_Solicitação_de_Credenciamento_e_Processo_Licitatório_029_2025_Parte_0328.pdf (23/200) 1200/4746

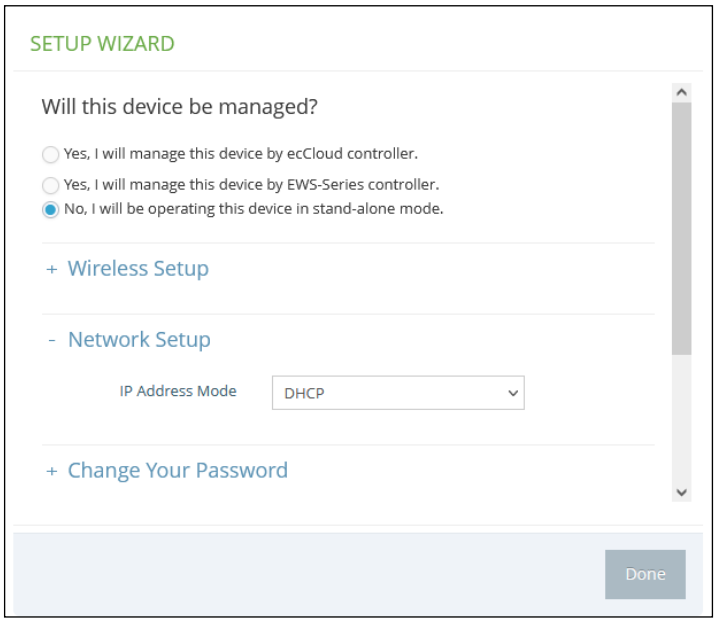
Figure 4: Wireless Setup



Step 4 Network Setup — For AP stand-alone mode, you also have the option to configure the IP address mode used to provide an IP address for the Internet access port.

The default IP Address Mode is DHCP and other options include Static IP and PPPoE. For more information, see "Internet Settings" on page 43.

Figure 5: Network Setup



1Doc: Protocolo 1.943/2025 | Anexo: em1_04C7B8805AD8E32AB6B2B6E_pdf_Termo_de_Referência_2025_Anexo_I_Wi-Fi_6_AP_2025_04_0328.pdf (24/200) 3200/4746

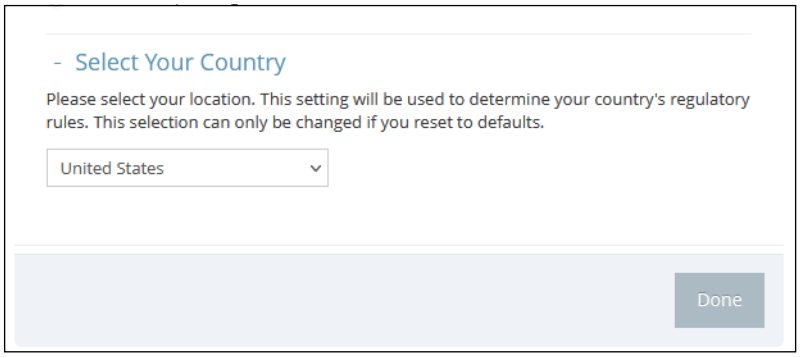
Step 5 Change Your Password — Set a new password for management access to the AP (the default user name is "admin" with password "admin"). The password must be 6-20 ASCII characters (case sensitive with no special characters).

Figure 6: Change Password

Note: For information on changing user names and passwords, see "User Accounts" on page 89.

Step 6 Select Your Country — Select the access point's country of operation from the drop-down menu. You must set the AP's country code to be sure that the radios operate according to permitted local regulations. That is, setting the country code restricts operation of the AP to the radio channels and transmit power levels permitted for wireless networks in the specified country.

Figure 7: Select Country



Caution: You must set the country code to the country of operation. Setting the country code ensures that the radios operate within the local regulations specified for wireless networks.

1Doc: Protocolo 1.943/2025 | Anexo: em_D4C7B8B5AD8E32AB62B6E_pdf_Termo_de_Referência_029_2025_Anexo_I_MiFi_6_029_2025_Part_0328.pdf (25/200) 1202/4726

Note: The country code selection is for non-US models only and is not available to any US models. Per FCC regulation, all Wi-Fi products marketed in the US must be fixed to US operation channels only.

Step 7 After completing the Setup Wizard, click "Done."

1Doc: Protocolo 1.943/2025 | Anexo: em_branco_Manual_Usuario_Processo_Licitatorio_829_2025_Anexo_I_WiFi6_AP_2025_04_0328.pdf (26/200) 1202/4746

QR Code Onboarding

For quick set up and registration of your AP with the ecCLOUD controller, you can scan the QR code on the AP using a phone.

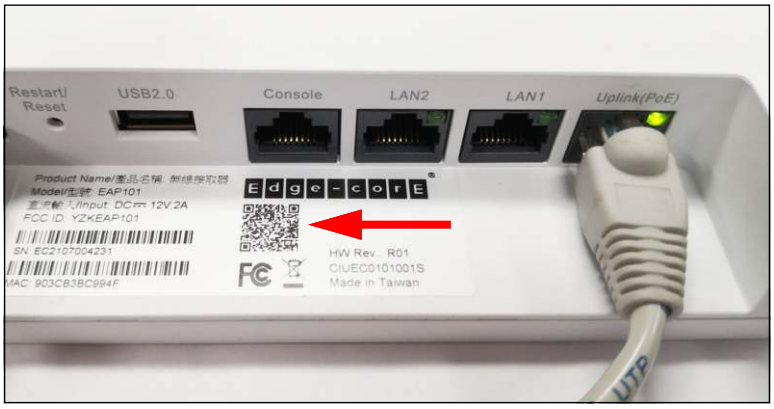
Follow these steps:

1. Power on the AP.

2. Connect the AP to the Internet. Connect your network or Internet access device to the AP's RJ-45 Uplink port.

3. Use the camera or a barcode app on your phone to scan the AP's QR code. The QR code is printed on a label next to the AP's ports.

Figure 8: Scanning the AP QR Code



4. When a message pops up, tap "yes" to join the Wi-Fi network. (iPhone requires you to go to Settings > Wi-Fi or open the browser for the message to pop up.)

   The web browser should open and redirect to the Setup Wizard page.

Note: If the phone cannot connect to the Wi-Fi network, type the SSID (network name) and password manually. The SSID name is the AP serial number (for example, EC0123456789), and the password is the AP MAC address (for example, 903CB3BC1234).

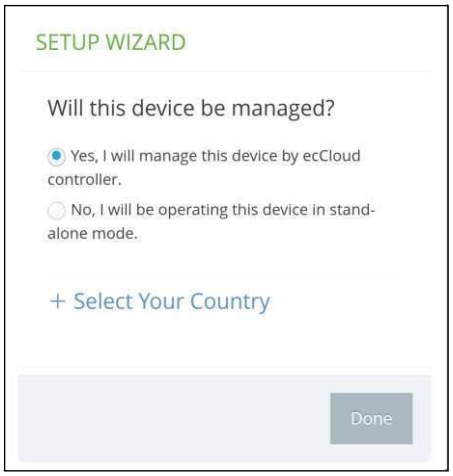
5. Wait for the auto-detection of the WAN port configuration (DHCP, Static IP, or PPPoE).

   When DHCP is detected, the AP automatically continues with the Setup Wizard.

Figure 9: Setup Wizard - Detect Network

6. Select to manage the AP using the ecCLOUD controller or to manage the AP in stand-alone mode.

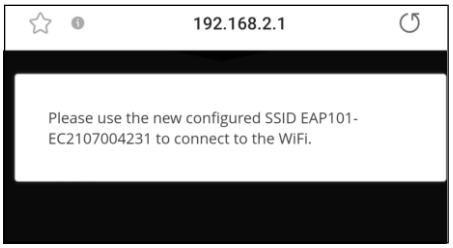
Figure 10: Setup Wizard - Device Management



a. Stand-Alone Mode: Use the default wireless network setting or customize the network name and password. Change the login password and set the country of operation. Tap "Done" to finish the setup wizard.

Wait about two minutes for the AP configuration to update, and then connect to the wireless network name configured in the Setup Wizard.

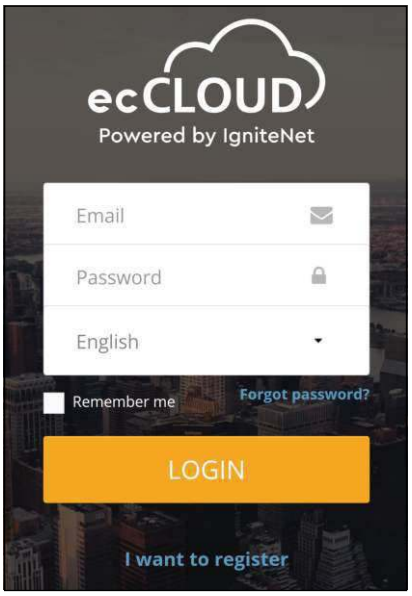
Figure 11: Connect to New SSID



b. Cloud-Managed Mode: Set the country of operation and then tap "Done" to finish the Setup Wizard. The browser is redirected to the ecCLOUD login page.

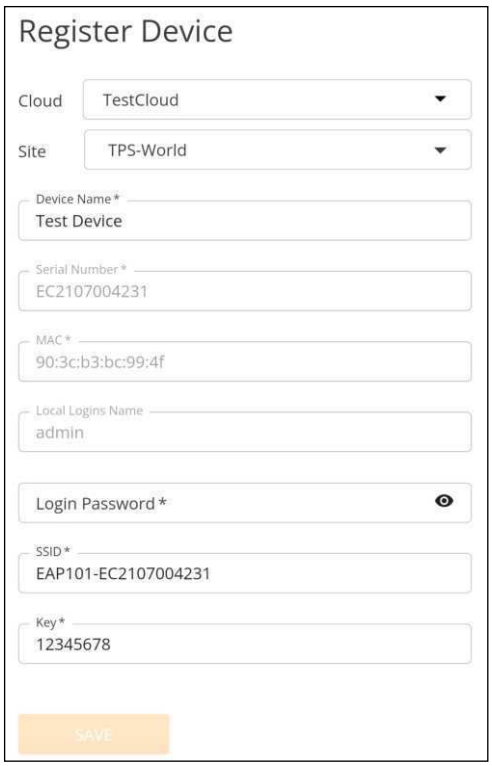
1Doc: Protocolo 1.943/2025 | Anexo: em_04C7B80D5AD8E32AB062B9E_pdf_Termo_de_Referência_029_2025_Anexo_I_WiFi6_029_2025_Part_0328.pdf (28/200) 1295/4746

Figure 12: ecCLOUD Login Page



If you already have an ecCLOUD account, log in and select a site for the AP. The AP is automatically registered for cloud management. Modify the device name, login password, SSID, and security key. After you tap "Save," wait about five minutes for the cloud controller to configure the AP.

Figure 13: ecCLOUD Device Registration



If you do not have an ecCLOUD account, tap "I want to register" and set up an account. Create a cloud and site before confirming the regulatory

1Doc: Protocolo 1.943/2025 | Anexo: em_04C7B8805AD8E32AB062B9E_proc_administrativo_029_2025_Anexo_MiFi6_029_2025_pt_0328.pdf (29/200) 1296/4746

country. After tapping “Next,” the AP is then automatically registered for cloud management.

After you tap “Save,” wait about five minutes for the cloud controller to configure the AP.

Note: Refer to the Edgecore *ecCLOUD Controller User Manual* for more information on setting up and configuring APs through ecCLOUD.

Mesh AP Configuration

The first AP can be managed either through ecCLOUD or in stand-alone mode. If a second AP needs to establish a mesh connection with the first AP, follow these steps:

1. Connect the LAN port of the first AP (Mesh Portal Point) to the LAN port of the second AP (Mesh Access Point), which then allows the second AP to synchronize its configuration with the first AP.
2. After unplugging the LAN port, the mesh connection will be established automatically.

Main Menu

The web interface Main Menu provides access to all the configuration settings available for the AP.

To configure settings, click the relevant Main Menu item. Each Main Menu item is summarized below with links to the relevant section in this guide where the configuration parameters are described in detail:

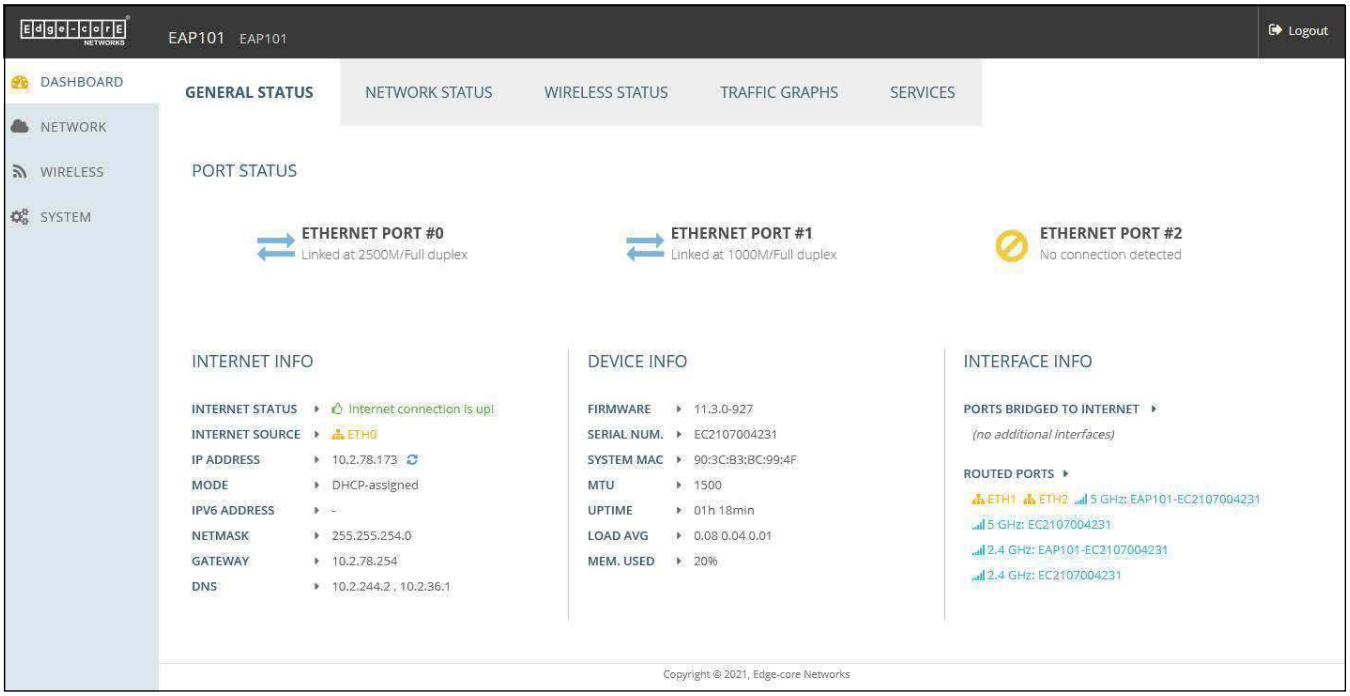
- **Dashboard** — The dashboard shows basic settings for the AP, including general status, local network settings, and wireless radio status. See “Status Information” on page 33.
- **Network** — Configures Internet, Ethernet, and LAN settings. See “Network Settings” on page 42.
- **Wireless** — Configures 2.4 GHz Radio, 5 GHz Radio, and VLAN settings. See “Wireless Settings” on page 64
- **System** — Configures System (including cloud agent and various system settings), Maintenance (such as view log, reboot, reset defaults, backup defaults, restore defaults, and firmware upgrade), User Accounts, Services (network time), and Diagnostics (including ping, traceroute).

1Doc: Protocolo 1.943/2025 | Anexo: em branco | Assinado por 1 autoridade e 1 interessado - 29/09/2025 - Anexo Interno_029_2025_Part_0328.pdf (30/200) 1296/4746

Dashboard

After logging in to the web interface, the dashboard displays. The dashboard shows basic settings for the AP, including Internet status, local network settings, and wireless radio status.

Figure 14: The Dashboard



Common Web Page Buttons

The list below describes the common buttons found on many of the web management pages:

- **Save** – Applies the new parameters and saves them to temporary RAM memory. Also displays a message at the top of the screen to inform you that the changes have not yet been saved to Flash memory. The running configuration will not be saved upon a reboot unless you click the "Save & Apply" button.

Figure 15: Saving Configuration Changes

- **Save & Apply** – Saves the changes made on a page and then applies them so that the configuration is retained after a restart.
- **Revert** – Cancels newly entered settings and restores the originals.
- **Logout** – Ends the web management session.

1Doc: Protocolo 1.943/2025 | Anexo: em_04C7B805AD8E32AB62B8E_soc_administrador_2025_processo_anexo_MiFi6_029_2025_pt_0328.pdf (31/200) 1943/4726

Section II

Web Configuration

This section provides details on configuring the access point using the web browser interface.

This section includes these chapters:

1Doc: Protocolo 1.943/2025 | Anexo: em branco Assinado por 1 pessoa: Administrador 29/09/2025 Anexo criado em 29/09/2025 14:03:28 (32/200) 1209/4746

2 Status Information

The Dashboard displays information on the current system configuration, including Internet status, local network settings, wireless radio status, traffic graphs, and services.

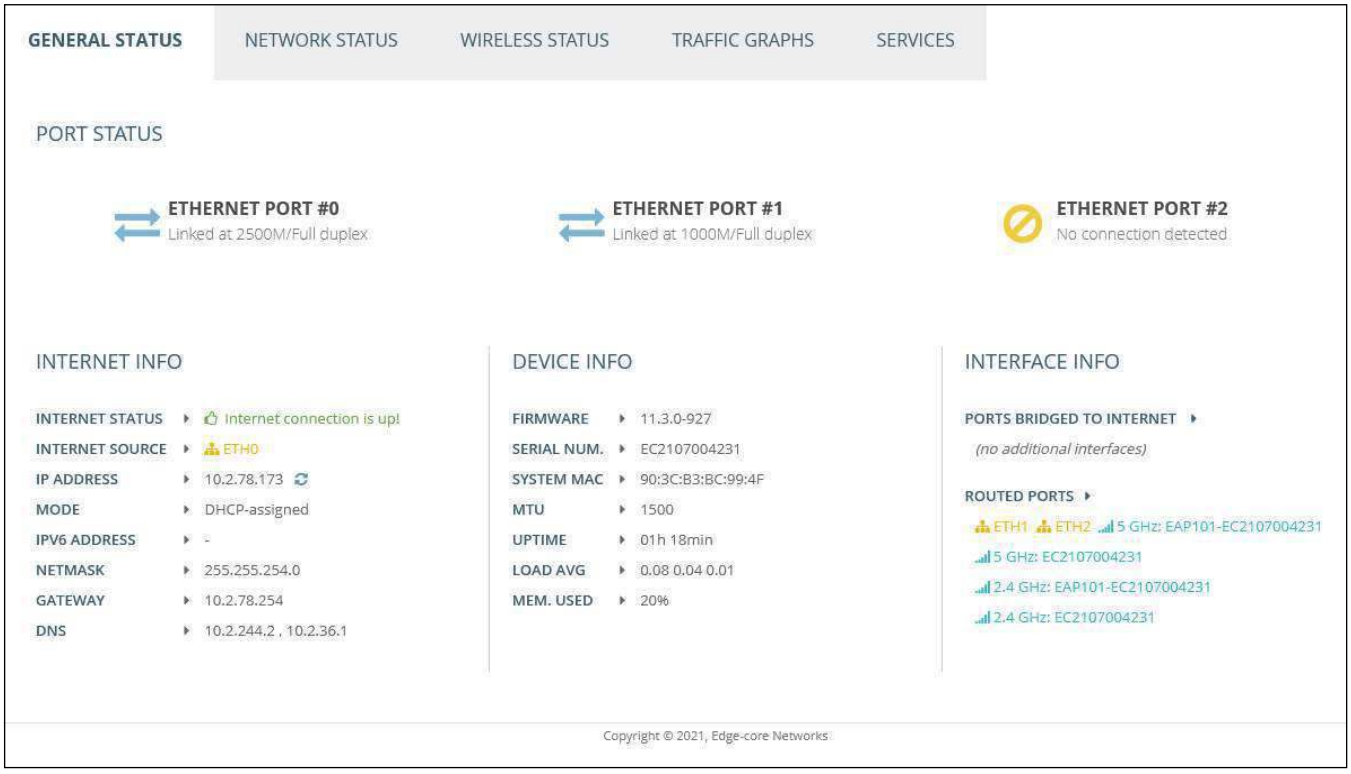
This chapter includes the following sections:

1Doc: Protocolo 1.943/2025 | Anexo: em_04C7D8805AD8E32AB062B9E_Solicitação_de_acesso_administrativo_à_rede_sem_fio_Anexo_I_MiFi6_029_2025_04_0328.pdf (33/200) 1299/4746

General Status

The General Status section shows descriptive information about the AP.

Figure 16: General Status Information



The following items are displayed in the “Port Status” section:

- **Ethernet Port #0** — Shows the status of the WAN Ethernet port, including link-up state, speed, and duplex mode.
- **Ethernet Port #1** — Shows the status of the LAN Ethernet port 1, including link-up state, speed, and duplex mode.
- **Ethernet Port #2** — Shows the status of the LAN Ethernet port 2, including link-up state, speed, and duplex mode.

The following items are displayed in the “Internet Info” section:

- **Internet Status** — Shows whether or not the Internet connection is up.
- **Internet Source** — The Ethernet port connected to the Internet. By default, this is Ethernet Port 0.
- **IP Address** — IP address of the Internet connection.

1Doc: Protocolo 1.943/2025 | Anexo: em1_04C7B8B5AD8E32AB62B6E_Solicitação_de_Acesso_Administrativo_Anexo_I_-_Termo_de_Referência_v6_29_2025_04_0328.pdf (34/200) 3000/4726

- **Mode** — Shows if the IP address is a static setting or set by DHCP.
- **IPv6 Address** — The IPv6 address of the Internet connection.
- **Netmask** — The subnet mask of the IP address.
- **Gateway** — The IP address of the gateway router that is used when a destination address is not on the local subnet.
- **DNS** — The IP address of the Domain Name Server on the network. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses.

The following items are displayed in the “Device Info” section:

- **Firmware** — The software version number.
- **Serial Number** — The serial number of the physical access point.
- **System MAC** — The system MAC address of the access point.
- **MTU** — The maximum transmission unit for packets sent on the network.
- **Uptime** — Length of time the management agent has been up.
- **Load Average** — The last 1-minute, 5-minute and 15-minute CPU load average.
- **Memory Used** — The percentage of memory being used.

The following items are displayed in the “Interface Info” section:

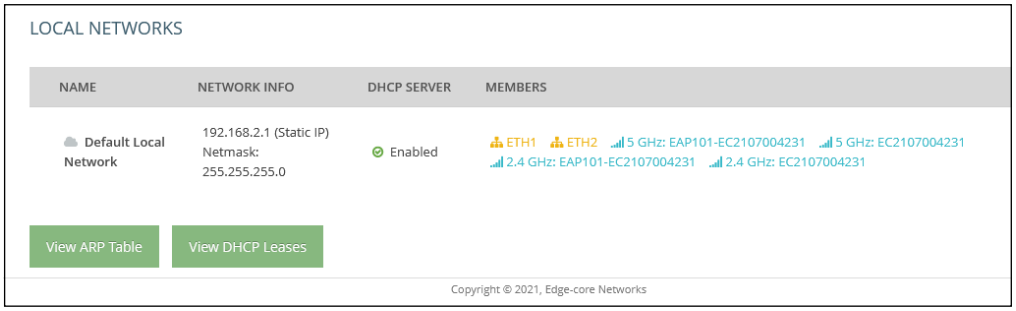
- **Ports Bridged to Internet** — Additional interfaces attached directly to the Internet. Lists interfaces attached to the WAN (that is, the Internet).
- **Routed Ports** — By default, all interfaces are configured as a member of the LAN. Traffic from these interfaces is routed across the access point through Ethernet Port 0 to the Internet. (This is also called route to Internet.)

1Doc: Protocolo 1.943/2025 | Anexo: em_1_04C7D8805AD8E32AB6628B6E_Solicitação_de_acesso_administrativo_a_pessoa_jurídica_Anexo_I_MiFi6_029_2025_04_0328.pdf (35/200) 1002/4746

Network Status

The Network Status section shows information about local network connections.

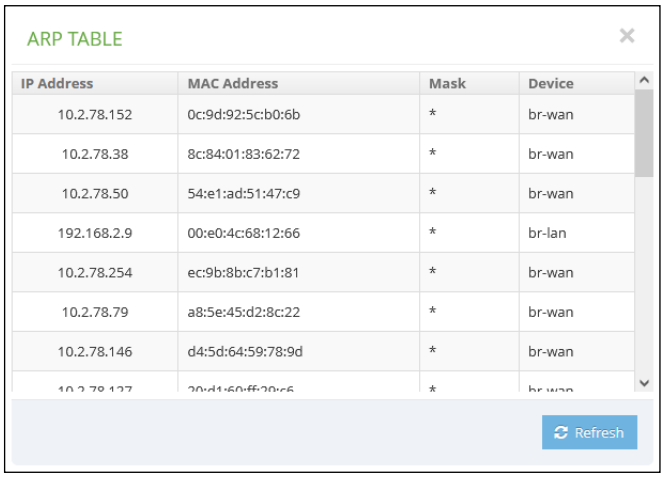
Figure 17: Local Networks



The following items are displayed in this section:

- **Name** — Shows information on the name of the local network.
- **Network Info** — Shows whether the local network uses static or dynamic configuration, and the network mask.
- **DHCP Server** — Shows if DHCP service is enabled on this network.
- **Members** — Shows the ports and wireless radios attached to this network. (Click on any of these interfaces to open the corresponding configuration page.)
- **View ARP Table** — Shows the ARP cache.

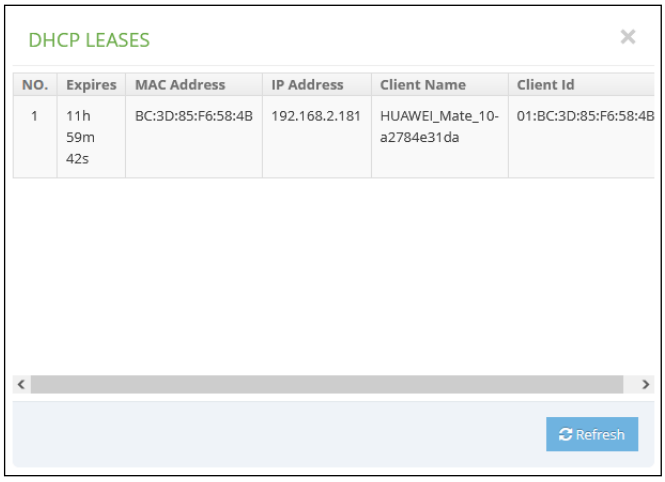
Figure 18: ARP Table



1Doc: Protocolo 1.943/2025 | Anexo: em_04C7B8805AD8E32AB6628B5E_Protocolo_Termo_de_Referencia_029_2025_Pregao_0328.pdf (36/200) 1002/4746

- **View DHCP Leases** — Shows DHCP leases.

Figure 19: Active DHCP Leases

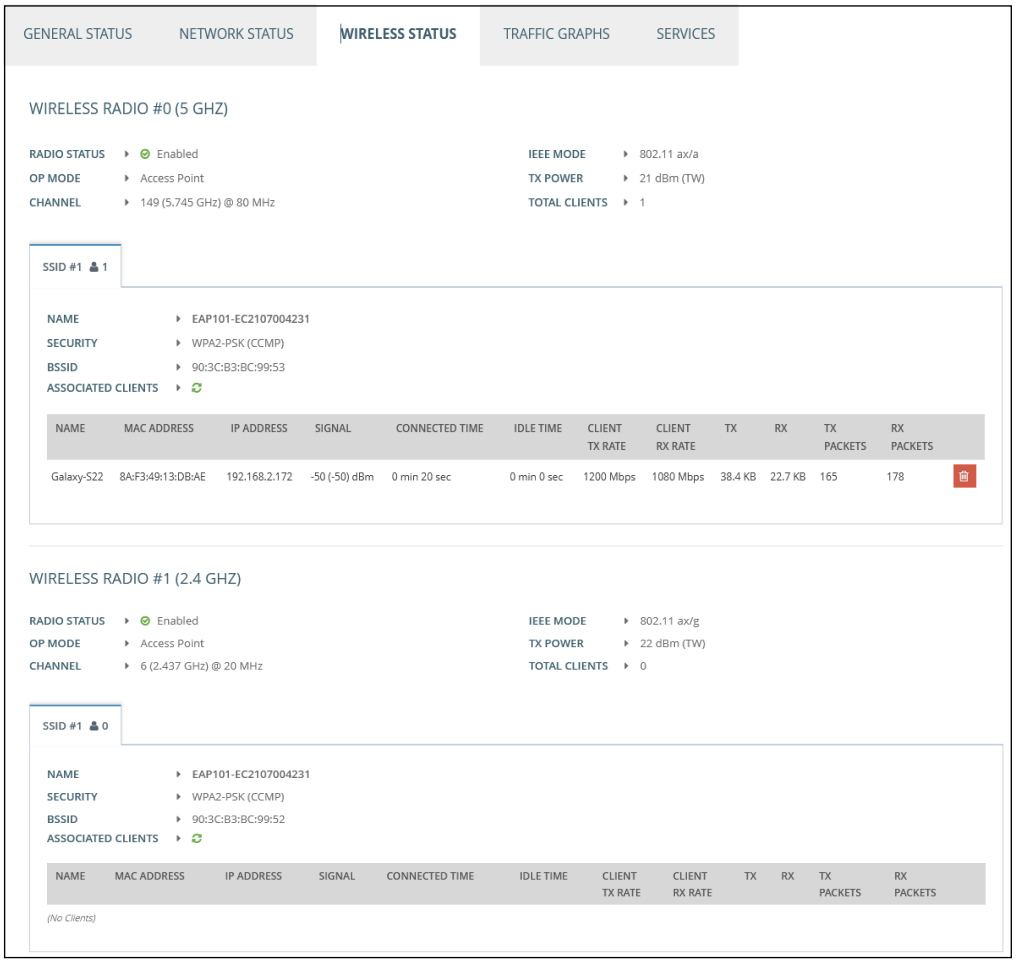


1Doc: Protocolo 1.943/2025 | Anexo: em_Doc_7_Relatorio_Tecnico_Administrativo_Processo_Licitatorio_Anexo_I_MiFi_6_29_2025_Parte_1_3_28.pdf (37/200) 1003/4746

Wireless Status

The Wireless Status section shows information about the radio settings and associated clients.

Figure 20: Wireless Status



Note that you can click the red button next to an associated client to force disconnection.

The following items are displayed in this section:

- **Wireless Radio 5 GHz/2.4 GHz** — Indicates the 2.4 GHz or 5 GHz wireless interface.
  - **Radio Status** — Shows if the wireless interface is enabled or disabled.
  - **IEEE Mode** — The 802.11 wireless LAN standards supported by the AP.
  - **Op Mode** — Shows if the wireless interface is configured to operate in an access point mode or client mode.

1Doc: Protocolo 1.943/2025 | Anexo: em1_04C7D8805AD8E32AB6B2B6E_Solicitação_de_Acesso_Administrativo_2025_Anexo_Anexo_WiFi6_029_2025_04_0328.pdf (38/200) 3005/4726

- **Tx Power** — The power of the radio signals transmitted from the AP.
- **Channel** — The radio channel the access point uses to communicate with wireless clients. The available channels depend on the 802.11 Mode, Channel Bandwidth, and Country Code settings.
- **Total Clients** — The total number of clients attached to this interface.

- **SSID #** — Service set identifier. Clients that want to connect to the wireless network through an access point must set their SSIDs to the same as that of the access point.
  - **Name** — A unique identifier for the local wireless network.
  - **Security** — Shows whether or not security has been enabled.
  - **BSSID** — The basic service set identifier. This is the MAC address of the AP generated by combining the 24 bit Organization Unique Identifier (OUI, the manufacturer's identity) and the manufacturer's assigned 24-bit identifier for the radio chipset in the AP.
  - **Associated Clients** — Shows detailed information about associated wireless clients.
    - **Name** — Client name.
    - **MAC Address** — The MAC address of the wireless client.
    - **IP Address** — The IP address assigned to the wireless client.
    - **Signal** — The signal strength (TX/RX) in dBm.
    - **Connected Time** — The time the wireless client has been associated.
    - **Idle Time** — The time the wireless client has been inactive.
    - **Client TX Rate** — The data transmit rate to the wireless client.
    - **Client RX Rate** — The data receive rate from the wireless client.
    - **TX** — The number of bytes transmitted to the wireless client.
    - **RX** — The number of bytes received from the wireless client.
    - **TX Packets** — The number of packets transmitted to the wireless client.
    - **RX Packets** — The number of packets received from the wireless client.

1Doc: Protocolo 1.943/2025 | Anexo: em_D4C7B8D5AD8E32AB62B6E_Solicitação_de_Credenciamento_e_Processo_Licitatório_829_2025_Anexo_I_MR6_029_2025_04_0328.pdf (39/200) 1006/4746

Traffic Graphs

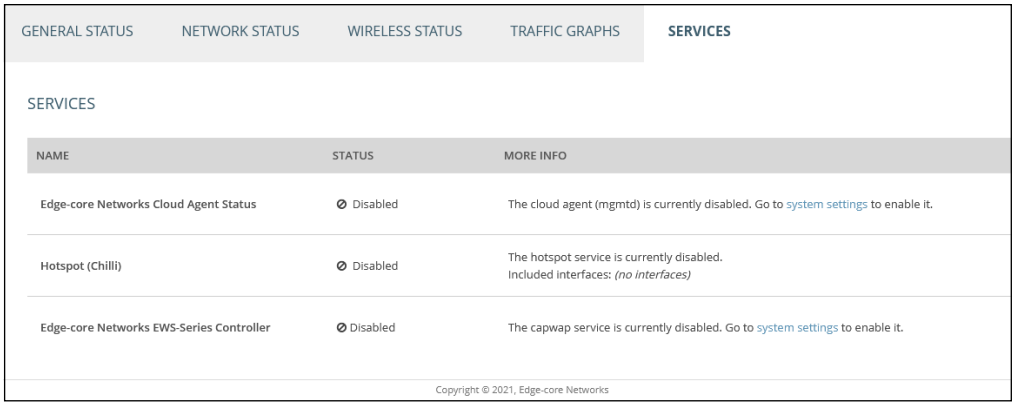
The Traffic Graphs section shows the data rate for the Ethernet ports, wireless interfaces, and mesh interface.

Figure 21: Traffic Graphs

Services

The Services section shows the status of the Edgecore cloud management agent.

Figure 22: Services



- **Edge-core Networks Cloud Agent Status** — Shows whether or not the agent for the cloud controller is enabled.

1Doc: Protocolo 1.943/2025 | Anexo: em_04C7B805AD8E32AB62B6E_ass_cationis_ad20_025_ces_Anexo_WiFi6_029_2025_04_0328.pdf (40/200) 3006/4746

- **Hotspot (Chilli)** — Shows whether or not hotspot services are enabled. Click on this field to open the Hotspot Settings menu.

- **Edge-core Networks EWS-Series Controller** — Shows if the CAPWAP service is enabled for management of the AP through an EWS-Series controller.

1Doc: Protocolo 1.943/2025 | Anexo: em_04C7B8805AD3E32AB6628B6E_Edge_Controller_Administrador_20_2025_Anexo_Manual_WiFi6_29_2025_14_0328.pdf (41/200) 3007/4746

3 Network Settings

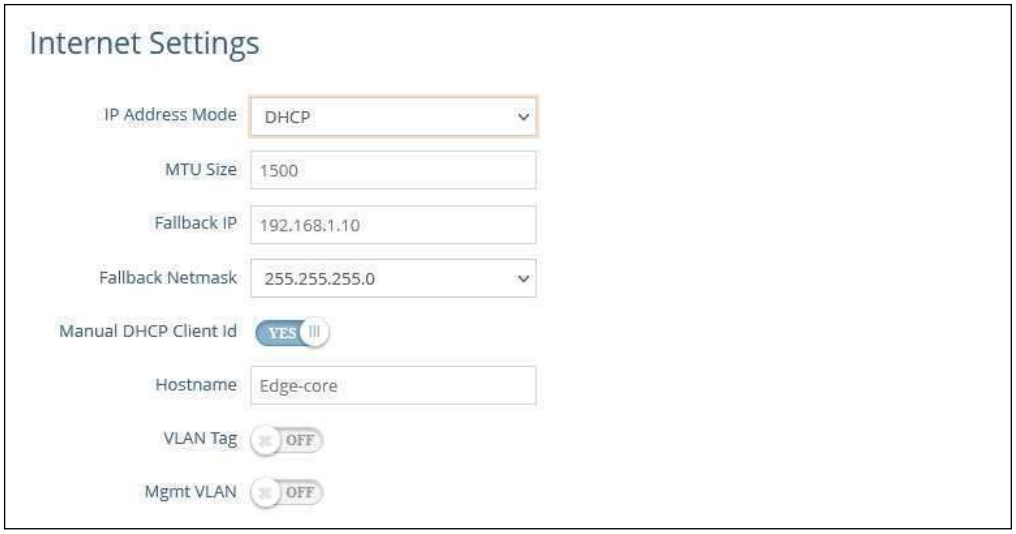
This chapter describes basic network settings on the access point. It includes the following sections:

1Doc: Protocolo 1.943/2025 | Anexo: em1_04C7B8805AD8E32AB062B9E_proc_administrativo_029_2025_Anexo_I_MiFi6_029_2025_Part_0328.pdf (42/200) 3009/4746

Internet Settings

The Internet Settings page configures the basic Internet settings for the AP, such as the source port, IP aliases, as well as the host name and maximum MTU size.

Figure 23: Internet Settings



The following items are displayed on this page:

- **IP Address Mode** — The method used to provide an IP address for the Internet access port. (Default: DHCP; Options: DHCP, Static IP, PPPoE)
  - **DHCP** — Configuration options displayed for DHCP are shown in Figure 23.
    - **Fallback IP** — This IP address is used if the DHCP service is unavailable or fails. (Default: 192.168.1.10)
    - **Fallback Netmask** — The network mask associated with the fallback IP address. (Default: 255.255.255.0)
    - **Manual DHCP Client Id** — An option to manually enter the hostname for the DHCP client.

1Doc: Protocolo 1.943/2025 | Anexo: em1_04C7B8805AD8E32AB062B6E_Solicitação_de_Credenciamento_e_Autorização_para_Uso_de_Radiofrequência_-_Anexo_I_-_Informações_Técnicas_-_Parte_1_6328.pdf (43/200) 1020/4726

Figure 24: IP Address Mode – Static IP

- **Static IP** — To configure a static IP address for the selected Ethernet interface, the following items must be specified.
  - **IP Address** — Specifies an IP address for the access point. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. (Default: 192.168.1.1)
  - **Subnet Mask** — Indicates the local subnet mask. (Default: 255.255.255.0)
  - **Default Gateway** — The IP address of the default gateway, which is used if the requested destination address is not on the local subnet.

    If you have management stations, DNS, RADIUS, or other network servers located on another subnet, type the IP address of the default gateway router in the text field provided.
  - **DNS Servers** — The IP address of Domain Name Servers on the network. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses.

    If you have a DNS servers located on the local network, type the IP address in the text fields provided.

1Doc: Protocolo 1.943/2025 | Anexo: em_D4C7B8805AD8E32AB6B2B6E_Solicitação_de_acesso_à_Internet_6_29_2025_14_03_28.pdf (44/200) 3020/4726

Figure 25: IP Address Mode – PPPoE

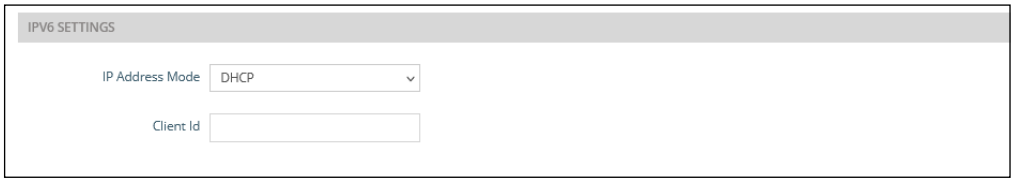
- **PPPoE** — To obtain an IP address for the selected Ethernet interface using PPPoE, the following items must be specified.
  - **Service Name** — The service name assigned for the PPPoE connection. The service name is normally optional, but may be required by some service providers. (Range: 1-32 alphanumeric characters)
  - **User Name** — The user name specified by the service provider. (Range: 1-32 characters)
  - **Password** — The password specified by the service provider. (Range: 1-32 characters)
- **MTU Size** — Sets the size of the maximum transmission unit (MTU) for packets sent on this interface. (Range: 1400-1500 bytes; Default 1500 bytes)
- **VLAN Tag** — Enable to activate tagging on this port and choose a tagging ID value between 2 and 4094, inclusive.
- **Mgmt VLAN** — Select this option to enable a management VLAN on this device. Once you enable this option, you will no longer be able to access this device on any of built-in the local networks (like 192.168.2.1 for example). You will only be able to access the device from the specified VLAN network. If this device's IP mode is set to DHCP, it will also request a new IP address in the subnet range assigned to the VLAN network.

1Doc: Protocolo 1.943/2025 | Anexo: em1_04C7B8805AD8E32AB062B8E_Solicitação_de_Homologação_Anexo_Manual_6_029_2025_Pt_0328.pdf (45/200) 1022/4726

IPv6 Settings

Enables you to configure the method used to provide an IPv6 address for the Internet access port.

Figure 26: IPv6 Settings



The following items are displayed on this section of the page:

- **IP Address Mode** — The method used to provide an IPv6 address for the Internet access port. (Default: DHCP; Options: DHCP, Static IP)
  - **DHCP** — If you configure DHCP, the Client Id must be specified.
    - **Client Id** — Manually enter the client ID for the DHCP client.
  - **Static IP** — To configure a static IPv6 address for the Internet access port, the following items must be specified.
    - **IP Address** — Specifies an IPv6 address for the access point. An IPv6 address must be configured according to RFC 2373 using 8 colon separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
    - **Default Gateway** — The IPv6 address of the default gateway, which is used if the requested destination address is not on the local subnet.
    - **DNS** — The IPv6 address of Domain Name Servers on the network. A DNS maps numerical IPv6 addresses to domain names and can be used to identify network hosts by familiar names instead of the IPv6 addresses. If you have a DNS server located on the local network, type the IPv6 address in the text field provided.

Ethernet Settings

The Ethernet Settings page configures the network behavior of the Ethernet ports, indicating that a port provides an Internet connection for wireless clients attached to the local network (routed to the Internet), or is bridged directly to the Internet.

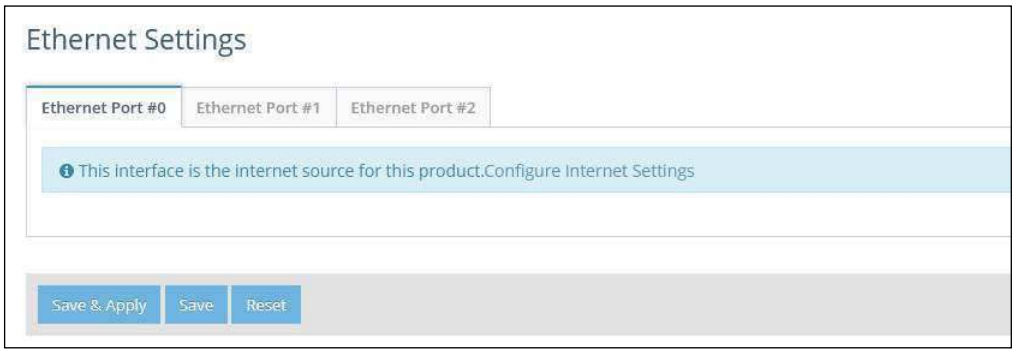
The following items are common for all pages under Ethernet Settings:

- **Ethernet Port #0** — Shows the status of the WAN Ethernet port.

1Doc: Protocolo 1.943/2025 | Anexo: em_04C7B8805AD8E32AB6628B5E_pt_Administrador_Acesso_Local_MiFi6_029_2025_04_0328.pdf (46/200) 1022/4726

- **Ethernet Port #1** — Shows the status of the LAN Ethernet port 1.
- **Ethernet Port #2** — Shows the status of the LAN Ethernet port 2.

Figure 27: Ethernet Settings – Internet Source

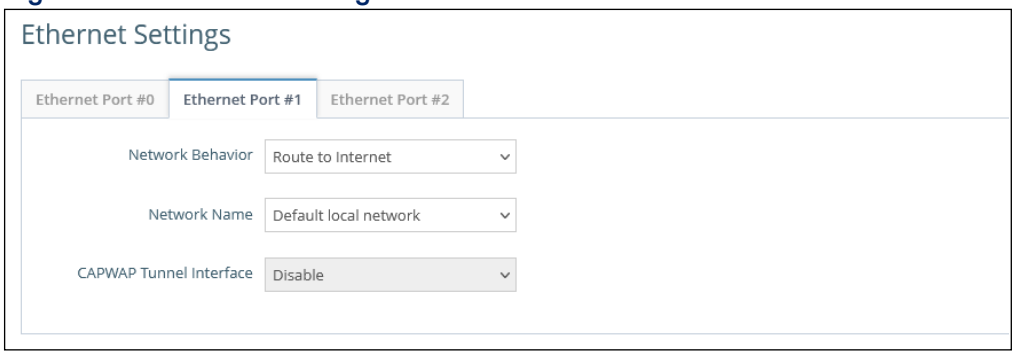


The following status message is displayed if an interface is set as the Internet source:

- "This interface is the internet source for this product. Configure Internet Settings"

  If more than one interface is connected to the Internet, only the last configured interface is used.

Figure 28: Ethernet Settings – Network Behavior



The following items are displayed on this page:

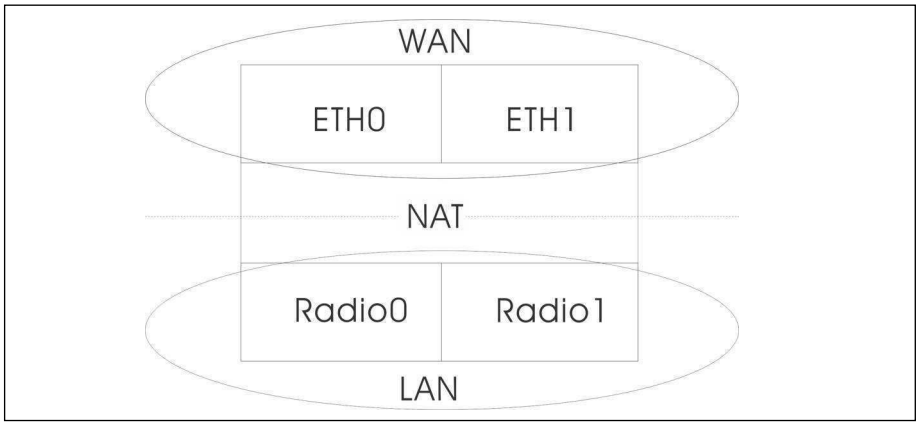
- **Network Behavior** — For the Ethernet port which is not providing Internet access, one of the following connection methods must be specified. (Default: Route to Internet)

  - **Bridge to Internet** — Configures an interface to be attached to the WAN. Traffic from this interface is directly bridged into the Internet. If an Ethernet port is bridged to the Internet, management access cannot be made by a direct connection to this port. However, if another Ethernet port or radio interface is within the LAN (routed to the Internet) the access point can be managed through this interface by a PC which is configured with an IP address in the same subnet.

1Doc: Protocolo 1.943/2025 | Anexo: em_D4C7B80D5AD8E32AB62B6E_Solicitação_de_acesso_administrativo_Anexo_Anexo_MiFi_6_29_2025_Port_0328.pdf (47/200) 1023/4726

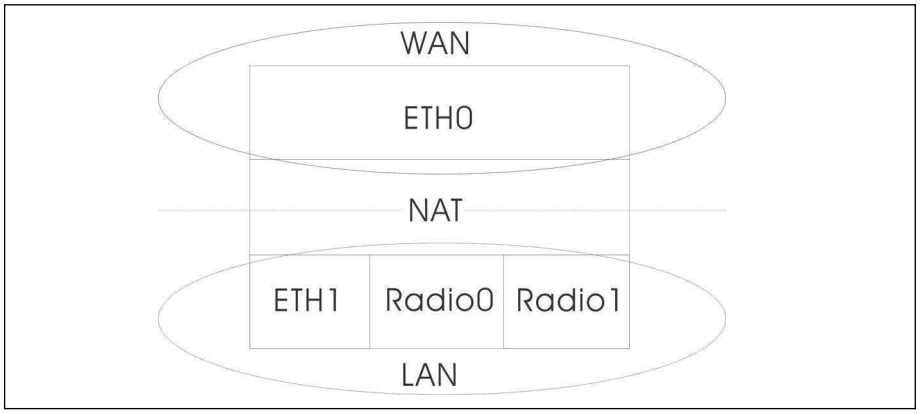
In the following figure, Ethernet Port 0 and Ethernet Port 1 are both attached to the WAN.

Figure 29: Bridge to Internet



- **Route to Internet** — Configures an interface to be a member of the LAN. Traffic from this interface is routed across the access point and out through an interface which is bridged directly to the Internet. By default, Ethernet Port 1 is routed to Internet, allowing management access via a direct connection to a PC configured with an address in the same subnet.

Figure 30: Route to Internet



  - **Network Name** — The network to be routed. The default is "Default local network" as displayed under LAN Settings – Local Networks.

- **Add to Guest Network** — This port can only support the guest network.

- **Hotspot Controlled** — This port can only access hotspot services. Click the link to open the Hotspot Settings page. See "Hotspot Settings" on page 53.

- **VLAN Tag Traffic** — This port transmits tagged traffic from a specified VLAN. Select the VLAN ID from the configured list, or click the link to open

1Doc: Protocolo 1.943/2025 | Anexo: em_04C7B8805AD8E32AB662B9E_Associations_Administrador_2025_Anexo_Manual_6_29_2025_pt_6328.pdf (48/200) 3025/4726

the Wireless VLAN Settings page and create a VLAN ID. See "VLAN Settings" on page 80.

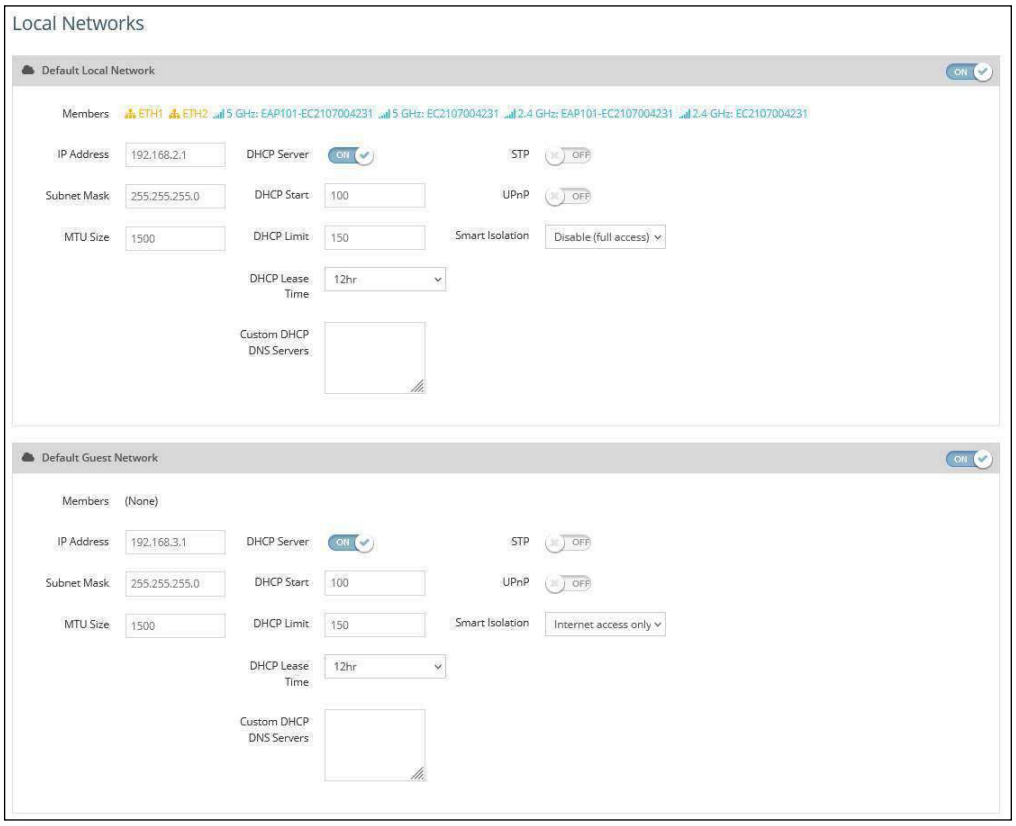
- **PoE Out** — (EAP104 only) Enables the PoE Out feature when the PoE source is detected as 802.3at, otherwise the PoE Out feature is disabled. When set to "Off," PoE Out is always disabled. (Default: On)

- **CAPWAP Tunnel Interface** — When the AP system management is set to EWS-Series Controller mode (see "System Settings" on page 83), the CAPWAP (Control And Provisioning of Wireless Access Points) protocol tunnel mode can be configured for the Ethernet port from the controller template. The options are "Disable" or "Complete." A Complete tunnel sends all management, authentication, and data traffic from the AP back to the controller. (Default: Disable)

LAN Settings

The LAN Settings page configures the LAN settings for the local and guest networks, including IP interface setting, DHCP server settings, and STP administrative status.

Figure 31: Network – LAN Settings



The following items are displayed on this page:

- **IP Address** — Specifies the IP address for the local network or guest network. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. (Default: 192.168.2.1)
- **Subnet Mask** — Indicates the local subnet mask. (Default: 255.255.255.0)
- **MTU Size** — Sets the size of the maximum transmission unit (MTU) for packets sent on this network. (Range: 1400-1500 bytes; Default 1500 bytes)
- **DHCP Server** — Enables/disables DHCP on this network. (Default: Enabled)
  - **DHCP Start** — First address in the address pool. (Range: 1-256; Default: x.x.x.100)
  - **DHCP Limit** — Maximum number of addresses in the address pool. (Range: 1-254; Default: 150)
  - **DHCP Lease Time** — The duration that an IP address is assigned to a DHCP client.
  - **Custom DHCP DNS Servers** — Specify the addresses or hostnames of custom DNS servers to be used.
- **STP** — Enables or disables processing of Spanning Tree Protocol messages. (Default: Disabled)
- **UPnP** — Enables or disables Universal Plug-and-Play broadcast messages. (Default: Disabled)
- **Smart Isolation** — Enables network traffic to be restricted to the specified network:
  - **Disable (full access)** — There is no traffic isolation. Clients can access the Internet and other devices on the local LAN.
  - **Internet access only** — Traffic from this network can only be routed to and from the Internet.
  - **LAN access only** — Traffic from this network is restricted to local LAN devices only.
  - **Internet access strict** — Traffic from this network can only be routed to and from the Internet, but with the additional restriction that users cannot access resources or devices on any private network (such as 192.168.0.0, 172.16.0.0, 10.0.0.0 etc.).
- **Add Custom LAN** — Click this button to create additional networks with their own custom settings. You can create up to 5 custom LANs.

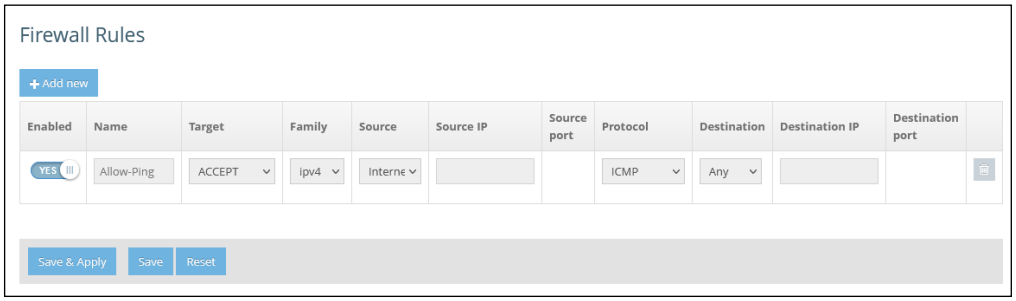
1Doc: Protocolo 1.943/2025 | Anexo: em_04C7D80D5AD8E32AB062B6E_Associação_Administrativa_de_Processo_Anexo_MiFi6_029_2025_04_0328.pdf (50/200) 1026/4726

Firewall Rules

Firewall filtering restricts connection parameters to limit the risk of intrusion. The firewall settings allow you to define a sequential list of rules that filter traffic based on source and destination IP addresses and ports. Ingress packets are tested against the filter rules one by one. As soon as a packet matches a rule, the configured target action is implemented.

One rule, "Allow-Ping," is pre-configured to allow Ping packets from the Internet. You can enable or disable this rule, but it cannot be modified or deleted. Click the "Add new" button to add a new firewall rule.

Figure 32: Firewall Rules



The following items are displayed on this page:

- **Enabled** — Enables or disables the rule.
- **Name** — A user-defined name for the filtering rule. (Range: 1-30 characters)
- **Target** — The action to take when a packet is matched. (Options: Accept, Reject, Drop; Default: Accept)
  - **Accept** — Accepts matching packets.
  - **Reject** — Drops matching packets and returns an error packet in response.
  - **Drop** — Drops matching packets.
- **Family** — The IP address family. (Options: Any, IPv4; Default: Any)
- **Source** — The source interface. (Options: Guest Network, Hotspot Network, Default Local Network, Internet, Any)
- **Source IP** — The source IPv4 address in CIDR notation. Includes an IPv4 address followed by a slash (/) and a decimal number to define the network mask.
- **Source port** — The source protocol port. (Range: 0-65535)

1Doc: Protocolo 1.943/2025 | Anexo: em_04C7B805AD8E32AB62B8E_processo_administrativo_n_029_2025_Anexo_I_MFG_029_2025_Part_0328.pdf (51/200) 1028/4746

- **Protocol** — The protocol type. (Options: Any, TCP+UDP, TCP, UDP, ICMP; Default: TCP+UDP)
- **Destination** — The destination interface. (Options: Guest Network, Hotspot Network, Default Local Network, Internet, Any)
- **Destination IP** — The destination IP address.
- **Destination port** — The destination protocol port. (Range: 0-65535)

Port Forwarding

Port Forwarding can be used to map an inbound protocol type (TCP/UDP) and port to an "internal" IP address and port. The internal (local) IP addresses are the IP addresses assigned to local devices at the edge of a network, and the external IP address is the IP address assigned to the AP interface. This allows remote users to access different servers on your local network using your single public IP address.

Remote users accessing services such as web or FTP at your local site through your public IP address, are redirected (mapped) to other local server IP addresses and TCP/UDP port numbers. For example, if you set Type/Public Port to TCP/80 (HTTP or web) and the Private IP/Port to 192.168.3.9/80, then all HTTP requests from outside users are forwarded to 192.168.3.9 on port 80. Therefore, by just using your external IP address provided by your ISP, Internet users can access the services they need at the local addresses to which you redirect them.

Figure 33: Port Forwarding

The following items are displayed on this page:

- **Enabled** — Enables port forwarding.
- **Name** — User defined name. (Range: 1-30 characters)
- **Protocol** — Set the protocol to which port forwarding is applied. (Options: TCP, UDP, TCP+UDP)
- **External Port** — The TCP/UDP port number. (Range: 1-65535)

  The more common TCP service port numbers include: HTTP: 80, FTP: 21, Telnet: 23, and POP3: 110.

1Doc: Protocolo 1.943/2025 | Anexo: em1_04C7D8805AD8E32AB062B6E_pt_Administração_Processo_Anexo_MiFi6_029_2025_04_0328.pdf (52/200) 1028/4746

- **Internal IP address** — The internal destination IP address.
- **Internal Port** — The internal destination protocol port. (Range: 1-65535)

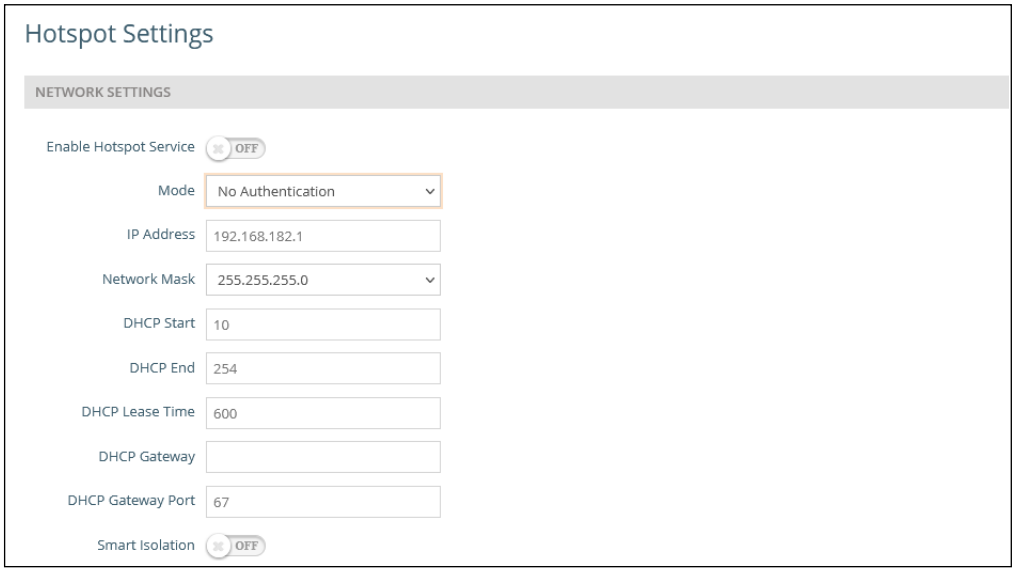
Hotspot Settings

The Hotspot Settings page can configure Internet access to the general public in places such as coffee houses, libraries and hospitals. Specific access rights may also be defined through a RADIUS server.

Network Settings

This section includes the option to enable or disable hotspot service, hotspot mode options, and network settings.

Figure 34: Hotspot Settings (Network Settings)



The following items are displayed on this page:

- **Enable Hotspot Service** — Enables or disables hotspot service. A hotspot is a physical location where people may obtain Internet access, typically using Wi-Fi technology, via a wireless local area network using a router connected to an Internet service provider.
- **Mode** — Hotspot service types include the following options:
  - **External Captive Portal Service** — This option will show the hotspot guest an externally hosted captive portal splash page and may prompt them to login, depending on how you've configured your service settings. Choose this option if you've signed up with a third-party captive portal service provider such as Cloud4Wi or HotSpotSystem.

1Doc: Protocolo 1.943/2025 | Anexo: em_04C7D8805AD8E32AB6628B8E_Processo_Administrativo_029_2025_Parte_0328.pdf (53/200) 3039/4746

- **No Authentication** — This option shows the hotspot guest your customized, locally hosted captive portal splash page, and will not require the guest to login before accessing the Internet. If you fill out the (optional) terms of service text, the guest will be required to accept these before they can access the Internet.

- **Simple Password-Only Splash Page** — This option will show the hotspot guest your customized, locally hosted captive portal splash page, and will require them to enter a simple password to login and access the Internet. If you fill out the (optional) terms of service text, the guest will be required to accept these before they can access the Internet.

- **Local Spash Page with External RADIUS** — This option shows the hotspot guest your customized, locally hosted captive portal splash page, and will require them to enter a valid RADIUS username and password to login and access the Internet. If you fill out the (optional) terms of service text, the guest will be required to accept these before they can access the Internet.

- **Network IP** — Specifies the IP address for the hotspot. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. (Default: 192.168.182.1)

  If your WAN subnet conflicts with any of the local networks (even the custom ones you create), the AP will automatically change the subnet of the local network.

- **Network Mask** — Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.

- **DHCP Start** — Starting number of (last numeric field) in address pool. (Range: 1-254; Default: 10)

- **DHCP End** — Ending number of (last numeric field) in address pool. (Range: 1-254; Default: 254)

- **DHCP Lease Time** — The duration that an IP address is assigned to a DHCP client. (Range: 600-43200 seconds; Default: 600 seconds)

- **DHCP Gateway** — Configure the DHCP gate IP address if you want to use an external DHCP server instead of the internal one.

- **DHCP Gateway Port** — The listening port used by the DHCP gateway.

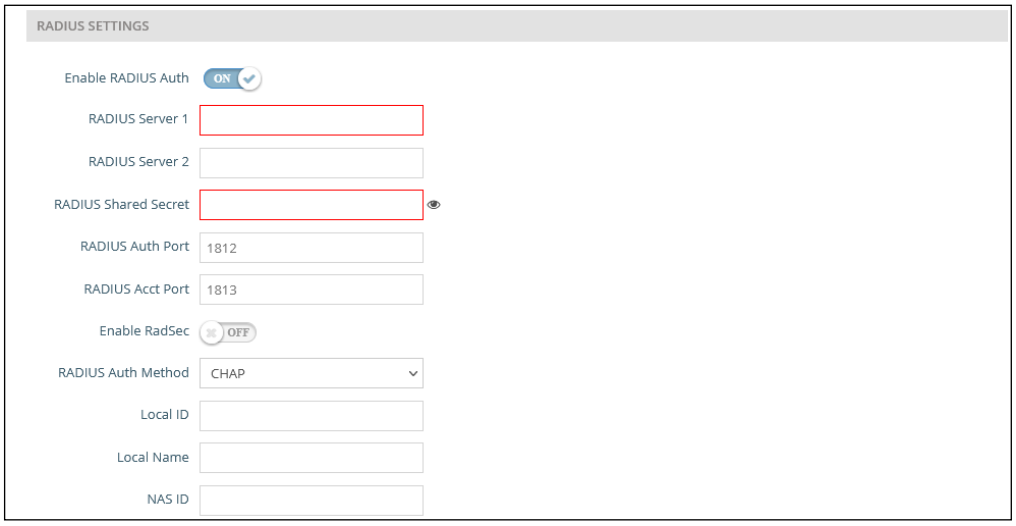
- **Smart Isolation** — Activate to prevent Hotspot users to possibly access WAN resources.

1Doc: Protocolo 1.943/2025 | Anexo: em_04C7D8805AD8E32AB062B6E_Solicitação_de_Homologação_Anexo_I_MiFi_6_029_2025_Parte_0328.pdf (54/200) 3020/4746

RADIUS Server

If you click set the mode to External Captive Portal Service or Local Splash page with External RADIUS, the following section is displayed.

Figure 35: Hotspot Settings (RADIUS Settings)



The following items are displayed on this page:

- **Enable RADIUS Auth** — Enables or disables client authentication via a RADIUS server.
- **RADIUS Server 1** — IP address or host name of the primary RADIUS server.
- **RADIUS Server 2** — IP address or host name of the secondary RADIUS server.
- **RADIUS Shared Secret** — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS server. Do not use blank spaces in the string. (Range: 1-255 characters).
- **RADIUS Auth Port** — RADIUS server UDP port used for authentication messages. (Range: 1-65535, Default: 1812)
- **RADIUS Acct Port** — RADIUS server UDP port used for accounting messages. (Range: 1-65535, Default: 1813)
- **Enable RadSec** — An authentication and authorization protocol for transporting RADIUS datagrams over TCP and TLS. RadSec replaces UDP used in the initial RADIUS design, providing a reliable transport protocol and more extensive security for the packet payload.
- **RADIUS Auth Method** — Selects the encryption method to use for messages between the AP and the RADIUS server; CHAP, PAP, or MSCHAPv2. The encryption method must match that used by the RADIUS server.

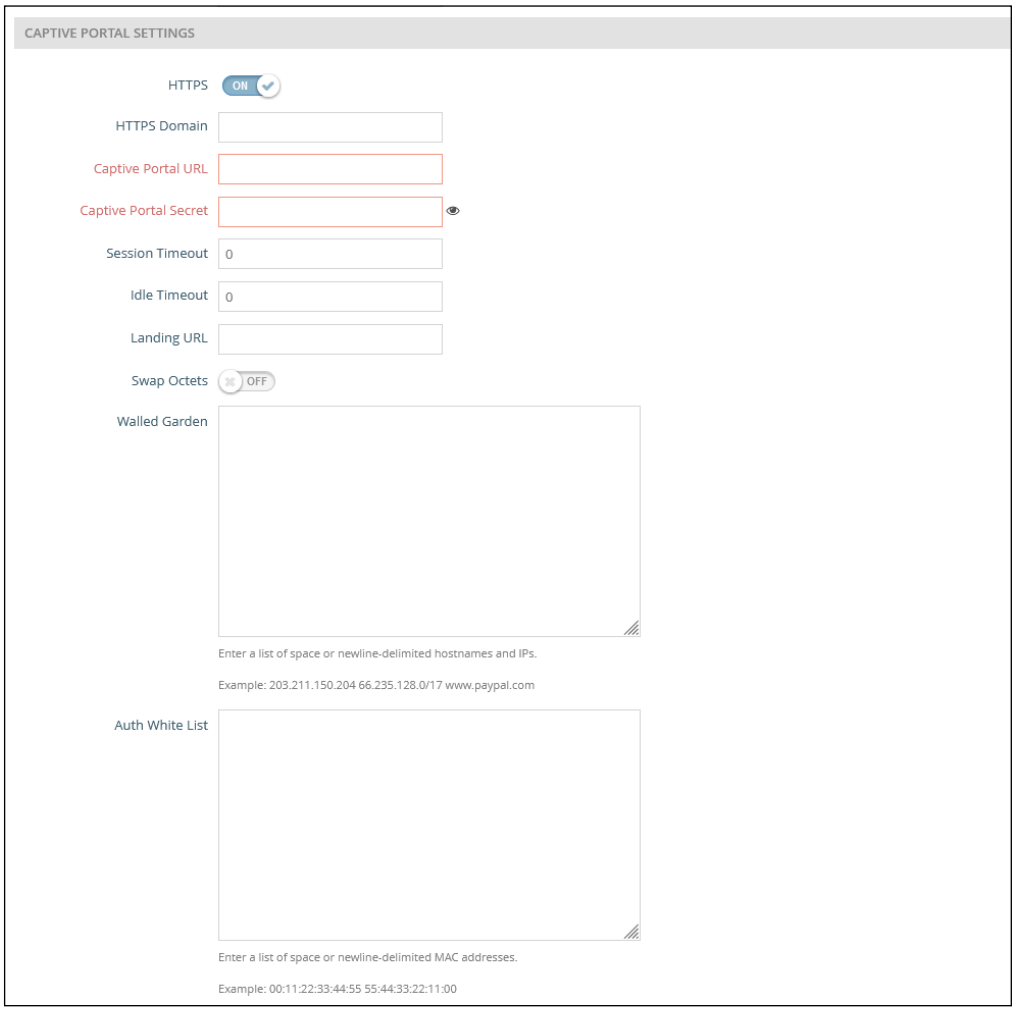
1Doc: Protocolo 1.943/2025 | Anexo: em_04C7B80D5AD8E32AB062B6E_pt_Administração_2025_Anexo_MiFi6_029_2025_04_0328.pdf (55/200) 1022/4746

- **Local ID** — Local RADIUS server identifier.
- **Local Name** — Local RADIUS server name
- **NAS ID** — Local RADIUS server operation identifier.

Captive Portal Settings

The following section is displayed for all hotspot mode options.

Figure 36: Hotspot Settings (Captive Portal Settings)



The following items are displayed on this page:

- **HTTPS** — Enables HTTPS for the captive portal. (Default: Disabled)

Note: To upload a unique security certificate from a trusted certification authority for the HTTPS captive portal, see "Upload Certificate" on page 88.

1Doc: Protocolo 1.943/2025 | Anexo: em_04C7B8805AD8E32AB6628B5E_Termo_de_Referencia_Aquisicao_de_Solucao_de_Gerenciamento_de_Acesso_Autenticado_WiFi_6_029_2025_Part_0328.pdf (56/200) 1022/4746

- **HTTPS Domain** — The domain name of the HTTPS captive portal.
- **Captive Portal URL** — Host name of Internet service portal for the hotspot.

  The captive portal forces a hotspot client to access a welcome web page (normally used for authentication) before gaining further access to the Internet. The welcome page may require authentication and/or payment.
- **Captive Portal Secret** — The password used for logging into the hotspot.
- **Customize Splash Page** — This option is shown for all hotspot service options other than External Captive Portal Service. If enabled, fill in information for the title, background color, logo image file, and optional terms and conditions.
- **Session Timeout** — The maximum time a client can stay attached to the hotspot. (Range: 0-86400 seconds)
- **Idle Timeout** — The maximum a connection can remain inactive before it is closed. (Range: 0-86400 seconds)
- **Landing URL** — Indicates the URL to which the user is directed after logging in to the captive portal.
- **Swap Octets** — Swap the values of the reported “input octets” and “output octets.” This option only appears under External Captive Portal Service.
- **Walled Garden** — A list of web sites to which unauthenticated users are allowed to navigate.
- **Auth White List** — A list of MAC addresses that are allowed to bypass the captive portal to access the Internet.

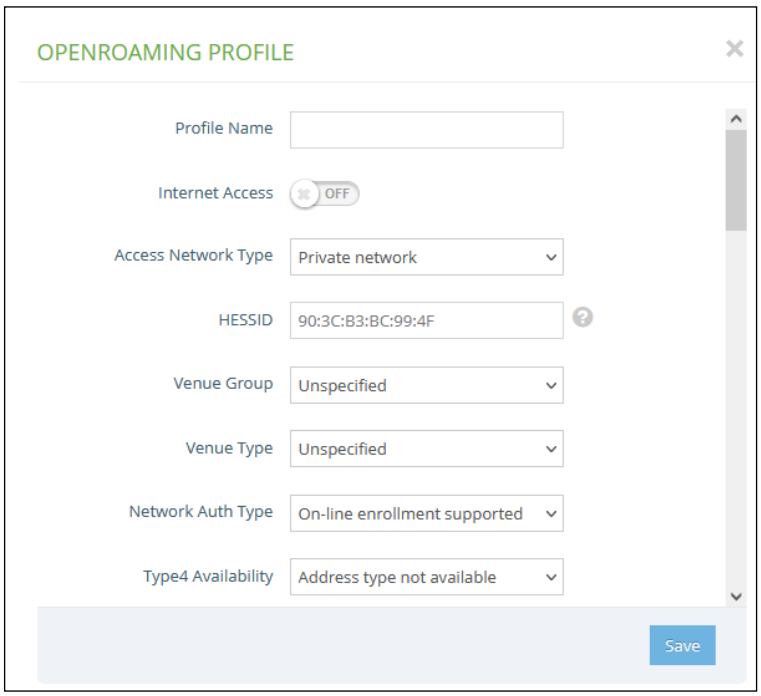
1Doc: Protocolo 1.943/2025 | Anexo: em_04C7B8805AD8E32AB062B6E_processo_administrativo_029_2025_Anexo_I_MF6_029_2025_Part_0328.pdf (57/200) 1028/4746

OpenRoaming

OpenRoaming provides a standard for public-access Wi-Fi networks to support seamless roaming between wireless networks. An OpenRoaming network advertises its public Wi-Fi capabilities and services so that clients can decide if they want to connect to the network.

Up to 32 OpenRoaming profiles can be configured and applied to specific wireless networks (see "OpenRoaming" under "Wireless Networks — Network Settings" on page 76). Click "Add New" to configure a profile.

Figure 37: OpenRoaming Profile



The following items are displayed on this page:

- **Profile Name** — A name that identifies the profile.
- **Internet Access** — Enable if this network provides access to the Internet.
- **Access Network Type** — Select one from the predefined list.
  - **Private network** — Home and enterprise networks that unauthorized users cannot access.
  - **Private network with guest access** — A private network that provides for guest access. A typical example would be an enterprise network that offers guest access.

- **Chargeable public network** — A network that is available to all users, but requires a fee.
- **Free Public Network** — A network that is available to all users without any fees.
- **Personal device network** — A network for peripheral connectivity in an ad-hoc mode. For example, a camera that connects to a printer.
- **Emergency services only network** — A network that is dedicated for access to emergency services only.
- **Test or experimental** — A network for tests or experimental work.
- **Wildcard** — When selected, the AP will reply to clients regardless of the network type requested by the client query.

- **HESSID** — The Homogenous Extended Service Set Identifier (HESSID) for the OpenRoaming network. When configured, the HESSID (a MAC address) uniquely identifies all APs belonging to the same network.
- **Venue Group** — Identifies the general class of the venue. Select from the predefined list.
- **Venue Type** — Identifies the specific type of venue within each group.
- **Network Auth Type** — Specifies the authentication required for the network. Select an option from the predefined list. (Default: "Acceptance of terms and conditions")
- **Type4 Availability** — Specifies the IPv4 address type available from the network.
- **Type6 Availability** — Specifies the IPv6 address type available from the network
- **Operating Class** — A standard index (based on IEEE Std 802.11-2012 Annex E) that specifies the AP supported operating channels.
- **Captive Portal** — Enables the Captive Portal feature. (Default: Disabled)
  - **Captive Portal URL** — Host name of Internet service portal (HTTP or HTTPS).

    A captive portal forces a client to access a welcome web page (normally used for authentication) before gaining further access to the Internet. The welcome page may require authentication and/or payment.

1Doc: Protocolo 1.943/2025 | Anexo: em1_04C7D8805AD8E32AB062B6E_Termo_de_Referencia_Anexo_I_MiFi_6_29_2025_14_0328.pdf (59/200) 1026/4746

- **Wall Garden** — A list of web sites to which unauthenticated users are allowed to navigate. Enter a list of space or newline-delimited host names and IP addresses.

- **Venue Name Information** — Configures a list of up to 10 venue names.
  - **Language Code** — Select a language from the list. (Default: English)
  - **Venue Name** — The name of the network venue. Multiple names can be added to the list.
  - **Venue URL** — Specifies a URL that provides additional venue information to users.

- **Cellular Network Information List (PLMN)** — (Optional) Identifies the 3GPP cellular networks available through the AP. Specifically, this field identifies the Public Land Mobile Network (PLMN) ID, comprised of the Mobile Country Code (MCC) and Mobile Network Code (MNC) of the mobile operator. Up to 10 PLMN IDs can be configured. Input the pair of MCC, MNC.
  For example: 400, 00
  MCC: Three decimal digits (000-999)
  MNC: Two (00-99) or three decimal digits (000-999)

- **Operator Friendly Name** — The name of the network operator and the specified language. Up to 10 names can be configured.

- **Roaming Consortium List** — (Optional) A roaming consortium is a group of service providers (SP) with which a user's credentials can be used for authentication. Each roaming consortium is identified by an organization identifier (OI) that is assigned by the IEEE. An OI is often 24 bits in length, but can also be 36 bits. Up to 10 identifiers can be configured.

- **Domain Name List** — Lists one or up to 10 domain names for the entity operating the AP. This is critical for OpenRoaming network selection policy, as it identifies the operator of the network. It indicates to the mobile device whether they are at a home hotspot or a visited hotspot.

- **NAI Realm List** — (Optional) The network access identifier (NAI) realm list identifies those service provider or other networks that are accessible through the AP. By discovering which authentication realms are supported by a network, a mobile device can selectively authenticate to its preferred network. Up to 10 identifiers can be configured.
  - **Method/Authentication** — Specifies EAP methods and authentication for each service provider added to the NAI Realm List.

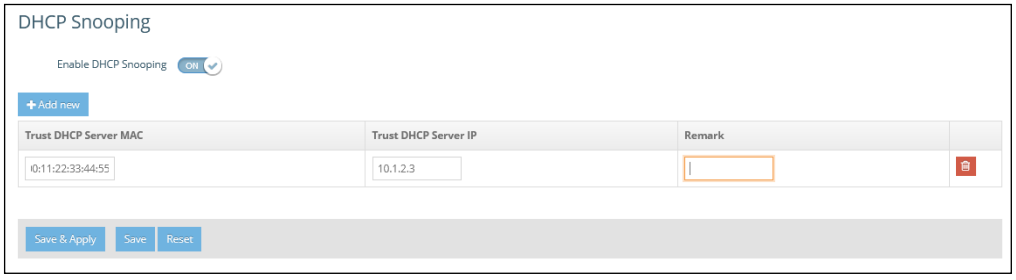
1Doc: Protocolo 1.943/2025 | Anexo: em1_04C7B8805AD8E32AB062B6E_pt_Administrativo_829_2025_Anexo_I_MR6_OD_2025_04_0328.pdf (60/200) 1026/4746

DHCP Snooping

DHCP snooping is used to validate and filter DHCP messages received by the AP. When DHCP snooping is enabled, DHCP messages received from a device not listed in the DHCP snooping table are dropped.

You can add known and trusted DHCP servers to the table by specifying their MAC and IP addresses.

Figure 38: DHCP Snooping



The following items are displayed on this page:

- **Enable DHCP Snooping** — Enables DHCP Snooping on the AP.
- **Trust DHCP Server MAC** — The MAC address of a known and trusted DHCP server.
- **Trust DHCP Server IP** — The IP address of a known and trusted DHCP server.
- **Remark** — A comment relating to the DHCP server configured.

1Doc: Protocolo 1.943/2025 | Anexo: em_04C7B8805AD8E32AB062B6E_Solicitação_de_Homologação_Anexo_Manual_6_29_2025_Part_0328.pdf (61/200) 1028/4746

ARP Inspection

ARP Inspection is a security feature that validates the MAC Address bindings for Address Resolution Protocol packets. It provides protection against ARP traffic with invalid MAC-to-IP address bindings, which forms the basis for certain "man-in-the middle" attacks. This is accomplished by intercepting all ARP requests and responses and verifying each of these packets before the local ARP cache is updated or the packet is forwarded to the appropriate destination. Invalid ARP packets are dropped.

Figure 39: ARP Inspection

The following items are displayed on this page:

- **ARP Inspection** — When enabled, ARP packets are validated against ARP spoofing.
- **Force DHCP** — Allows the AP to only learn MAC/IP pair information through DHCP packets. Since devices configured with static IP address do not send DHCP traffic, any clients with static IP addresses will be blocked by the AP unless their MAC/IP pair is listed and enabled in the Static Trust List.
- **Trust List Broadcast** — Lets other APs learn the trusted MAC/IP pairs to issue ARP requests.
- **Static Trust List** — Adds the MAC or MAC/IP pairs of devices that are trusted to issue ARP requests. Other network nodes can still send their ARP requests, but if their IP appears in the static list with a different MAC, their ARP requests will be dropped.

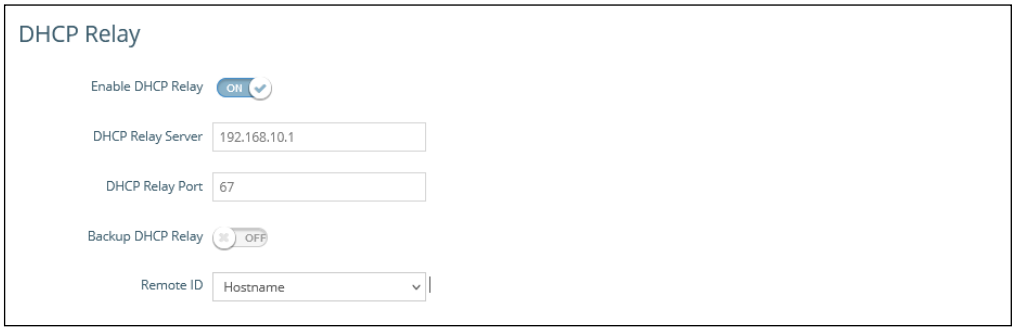
1Doc: Protocolo 1.943/2025 | Anexo: em1_04C7B8805AD8E32AB062B6E_Solicitação_de_Homologação_Anatel_MiFi_6_4G_2025_04_0328.pdf (62/200) 1029/4746

DHCP Relay

When DHCP relay is enabled, the AP as an agent for all clients and sends all broadcast DHCP requests directly to a specified DHCP server. The DHCP server IP address and port must be configured, and optionally a backup server.

With DHCP relay enabled, the circuit ID can be set on the VLAN settings or LAN settings page. IP addresses of clients are then obtained by the DHCP relay server and the IP range is determined by the remote ID and circuit ID.

Figure 40: DHCP Relay



The following items are displayed on this page:

- **Enable DHCP Relay** — Enables the DHCP relay feature on the AP.
- **DHCP Relay Server** — Specifies the IP address of the DHCP server.
- **DHCP Relay Port** — Specifies the port of the DHCP server.
- **Backup DHCP Relay** — Optionally specifies a backup DHCP server IP address and port to use if there is no response from the primary server.
- **Remote ID** — Use the hostname as the remote ID, or manually configure a text string as the remote ID.

1Doc: Protocolo 1.943/2025 | Anexo: em_04C7B8805AD8E32AB062B6E_procuradoria_2029_2025_Anexo_MiFi6_029_2025_04_0328.pdf (63/200) 1049/4746

4 Wireless Settings

This chapter describes the wireless settings on the access point. It includes the following sections:

1Doc: Protocolo 1.943/2025 | Anexo: em branco 1D4C7D8805AD8E32AB62B9E... Administração 029/2025 ... Anexo I - MiFi 6_29_2025_14_03_28.pdf (64/200) 1030/4746

Radio Settings

The IEEE 802.11 wireless interfaces include configuration options for radio signal characteristics and wireless security features.

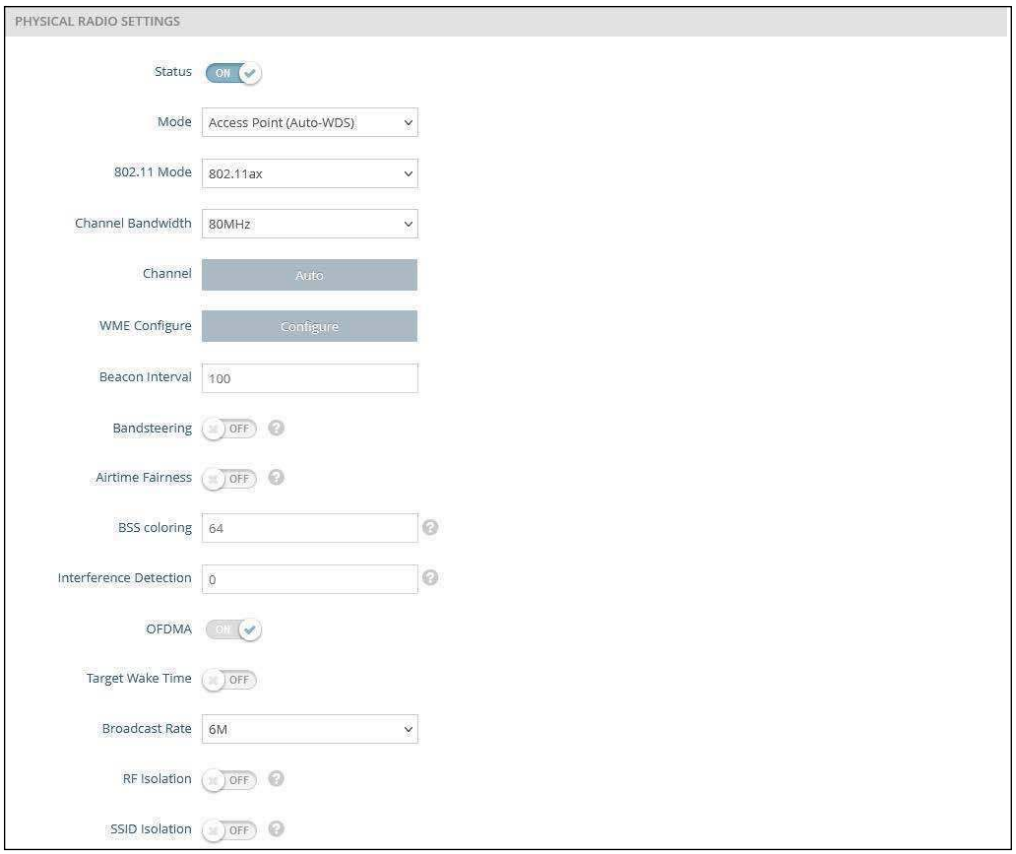
The access point can operate in several radio modes, 802.11b+g+n/ax (2.4 GHz) or 802.11a/a+n/ac+a+n/ax (5 GHz). Note that the dual-band access points can operate at 2.4 GHz and 5 GHz at the same time. The web interface identifies the radio configuration pages as:

- **Radio 2.4 GHz** — the 2.4 GHz 802.11b/g/n/ax radio interface
- **Radio 5 GHz** — the 5 GHz 802.11a/n/ac/ax radio interface

Each radio supports 16 virtual access point (VAP) interfaces based on the SSIDs, referred to as SSID1 ~ SSID16. Each VAP functions as a separate access point, and can be configured with its own Service Set Identification (SSID) and security settings. However, most radio signal parameters apply to all VAP interfaces. Traffic to specific VAPs can be segregated based on user groups or application traffic. The clients associate with each VAP in the same way as they would with separate physical access points.

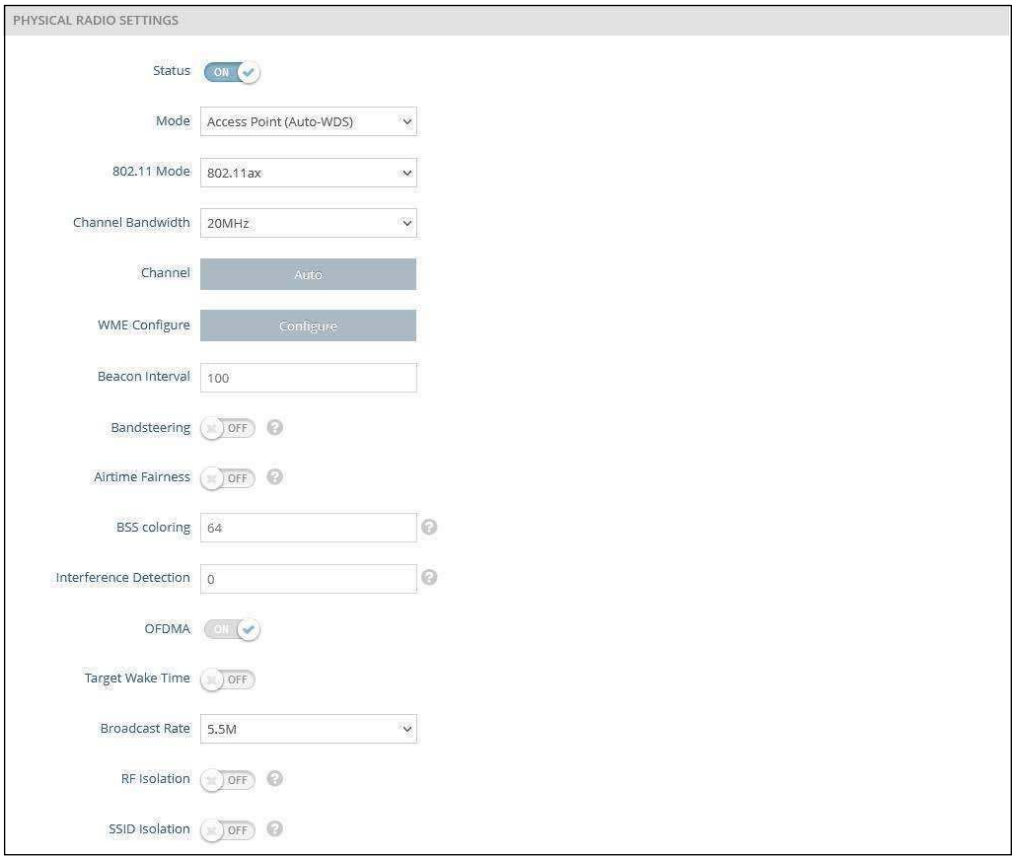
Physical Radio Settings

Figure 41: Physical Settings for Radio 5 GHz



1Doc: Protocolo 1.943/2025 | Anexo: em_D4C7B805AD8E32AB62B6_Acesso_Administrativo_Anexo_Anexo_MiFi_6_29_2025_14_03_28.pdf (65/200) 1032/4746

Figure 42: Physical Settings for Radio 2.4 GHz



The following items are displayed on this page:

- **Status** — Enables or disables the wireless service on this interface.
- **Mode** — Selects the mode in which the AP will function.
  - **Access Point (Auto-WDS)** — The AP operates as an access point in WDS mode, which accepts connections from APs in Client WDS mode. (This is the default setting.)

    In this mode, the AP provides services to clients as a normal access point. WDS is used to automatically search for and connect to other AP nodes using the same SSID and security settings.
  - **Client** — The AP can provide a wireless connection to another AP, as well as pass information from or to locally wired hosts and wireless clients.
- **802.11 Mode** — Defines the radio operation mode.
  - **Radio 2.4 GHz** — Default: 11ax; Options: 11b+g+n/ax
  - **Radio 5 GHz** — Default: 11ax; Options: 11a, 11a+n, 11ac+a+n, 11ax

1Doc: Protocolo 1.943/2025 | Anexo: em_04C7D8805AD8E32AB062B8E_pdf_Termo_de_Referencia_029_2025_Anexo_I_WiFi6_029_2025_Part_0328.pdf (66/200) 1082/4746

- **Channel Bandwidth** — The AP options for channel bandwidth include 20, 40 80, and 160 MHz. The available channel bandwidth is dependent on the 802.11 Mode. (Default: 20 MHz on 2.4 GHz Radio, 80 MHz on 5 GHz Radio; Options: 20 MHz, 40 MHz, 80MHz, 160MHz)
  - **20MHz** — For 802.11b+g+n and 802.11ax
  - **40MHz** — For 802.11b+g+n, 802.11a, 802.11a+n, 802.11ac+a+n and 802.11ax
  - **80MHz** — For 802.11ac+a+n and 802.11ax
  - **160MHz** — (Supported only on EAP104, EAP111, and OAP101 5 GHz radio) For 802.11ac+a+n and 802.11ax
- **Channel** — The radio channel that the access point uses to communicate with wireless clients. When multiple access points are deployed in the same area, set the channel on neighboring access points at least five channels apart to avoid interference with each other. For example, for 11g/n 20 MHz mode you can deploy up to three access points in the same area using channels 1, 6, 11. Note that wireless clients automatically set the channel to the same as that used by the access point to which it is linked. (The available channels are dependent on the 802.11 Mode, Channel Bandwidth, and Country Code settings.)

  Selecting Auto enables the access point to automatically select an unoccupied radio channel. (Default: Auto)
- **WME Configuration** — Wireless Multimedia Extensions (WME), also known as Wi-Fi Multimedia (WMM), is a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. It provides basic Quality of service (QoS) features for IEEE 802.11 networks. Access priority can be configured for four "Access Category"(AC) types using the following parameters:
  - **CW Min (Minimum Contention Window)** – The initial upper limit of the random backoff wait time before wireless medium access can be attempted. The initial wait time is a random value between zero and the CWMin value. Specify the CWMin value in the range 0-15 microseconds. Note that the CWMin value must be equal or less than the CWMax value.
  - **CW Max (Maximum Contention Window)** – The maximum upper limit of the random backoff wait time before wireless medium access can be attempted. The contention window is doubled after each detected collision up to the CWMax value. Specify the CWMax value in the range 0-15 microseconds. Note that the CWMax value must be greater or equal to the CWMin value.
  - **AIFS (Arbitration Inter-Frame Space)** – The minimum amount of wait time before the next data transmission attempt. Specify the AIFS value in the range 0-15 microseconds.

1Doc: Protocolo 1.943/2025 | Anexo: em_04C7D8805AD8E32AB6628B8E_pt_BR_Assessoria_Técnica_Administrativa_2025_Anexo_I_MIFI6_029_2025_v1_6328.pdf (67/200) 1033/4726

  - **TXOP Limit (Transmit Opportunity Limit)** – The maximum time an AC transmit queue has access to the wireless medium. When an AC queue is granted a transmit opportunity, it can transmit data for a time up to the TXOP Limit. This data bursting greatly improves the efficiency for high data-rate traffic. Specify a value in the range 0-8192 microseconds.

- **Beacon Interval** — The rate at which beacon signals are transmitted from the access point. The beacon signals allow wireless clients to maintain contact with the access point. They also carry power-management and other information. (Range: 100-1024 TUs; Default: 100 TUs)

- **Bandsteering** — When enabled, clients that support 2.4 GHz and 5 GHz are first connected to the 5 GHz radio. This feature helps balance the client load over the two radio bands. Note that both radios must have configured SSIDs and security settings that match for this feature to fully operate. (Default: Off)

- **Airtime Fairness** — Enabling this feature improves the overall performance of the wireless network. (Default: Disabled)

- **BSS coloring** — In 802.11ax (Wi-Fi 6) mode, BSS coloring allows nearby APs operating at the same frequency to identify traffic belonging to their own Basic Service Set (BSS). The BSS coloring enables Wi-Fi 6 networks to operate more efficiently in high-density environments where neighboring AP and client transmissions overlap. Assign a color value (a number from 1 to 63) to identify the radio BSS, or enter value 64 to allow the AP to randomly select a color value. (Range: 1-63, 64 random; Default: 64)

- **Interference Detection** — When the utilization in current channel reaches the configured threshold (as a percentage), the AP switches to a different channel. (Range: 0 - 100%; Default: 0, disabled)

- **OFDMA** — The 802.11ax (Wi-Fi 6) mode supports Orthogonal Frequency Division Multiple Access (OFDMA) and this cannot be disabled.

- **Target Wake Time** — In 802.11ax (Wi-Fi 6) mode, the AP can allow clients to request a specific Target-Wakeup Time (TWT) to transmit or receive frames, rather than rely on periodic beacons. This feature enables client devices to have much longer sleep states and results in significant power savings. In addition, the AP can control and schedule client TWTs to both manage contention in the network and accommodate delay-sensitive traffic. (Default: Disabled)

- **Broadcast Rate** — Allows a limit to be placed on the wireless bandwidth consumed by broadcast packets.

  - **Radio 2.4 Ghz** — Options: 5.5M, 6M, 9M, 11M, 12M, 18M, 24M, 36M, 48M, 54M; Default: 5.5M

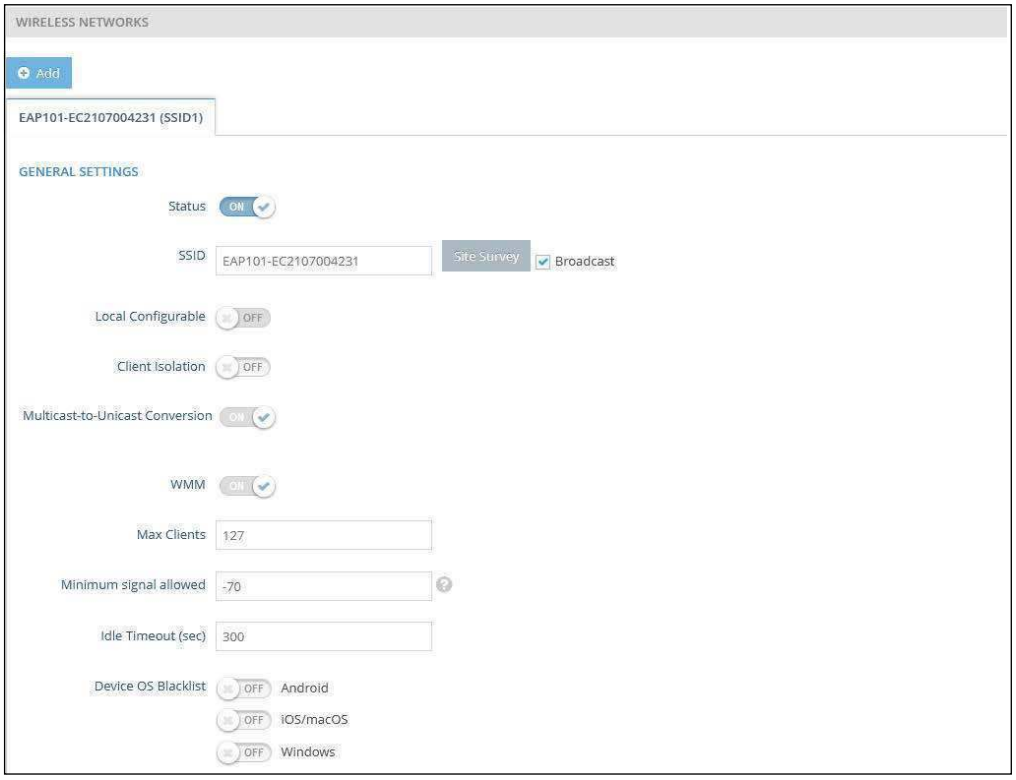
  - **Radio 5 Ghz** — Options: 6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M; Default: 6M

1Doc: Protocolo 1.943/2025 | Anexo: em_04C7D8805AD8E32AB062B6E_pt_Manual_AXE6_029_2025_04_0328.pdf (68/200) 1035/4746

- **RF Isolation** — When enabled, clients are isolated between different radio cards.
- **SSID Isolation** — When enabled, clients are isolated between different SSIDs on the same radio cards.

Wireless Networks — General Settings

Figure 43: Radio Settings (General Settings)



The following items are displayed in this section of the Wireless Settings page:

- **Status** — Enables or disables the wireless service on this VAP.
- **SSID** — The name of the basic service set provided by a Virtual Access Point (VAP) interface. Clients that want to connect to the network through the access point must set their SSID to the same as that of the access point's VAP interface. (Default: Edgecore5G-# (where # is 1-16) for 5 GHz, Edgecore2.4G-# (where # is 1-16) for 2.4 GHz; Range: 1-32 characters)
- **Site Survey** — Scans for all wireless networks that are broadcasting their SSID.
- **Broadcast** — The SSID can be broadcast at regular intervals so that wireless stations searching for a network connection can discover it. This allows wireless clients to dynamically discover and roam between WLANs. This feature also makes it easier for hackers to break into your home network. Because SSIDs are not encrypted, it is easy to grab one by snooping the WLAN looking for SSID broadcast messages coming from the AP. (Default: Enabled)

1Doc: Protocolo 1.943/2025 | Anexo: em1_04C7D8805AD8E32AB062B8E_Associations_Administrativos_2025_Processo_Anexo_WiFi6_029_2025_Part_0328.pdf (69/200) 1036/4746

- **Local Configurable** — Enables the SSID to be user configurable when the system is operating in MSP mode (see "System Settings" on page 83). (Default: Disabled)
- **Client Isolation** — When enabled, wireless clients can talk to the LAN, and reach the Internet if such connection is available, but they cannot communicate with one another. (Default: Disabled)
- **Multicast-to-Unicast Conversion** — When enabled, the AP converts multicast traffic to unicast traffic and sends it to each associated client. This feature provides a network throughput enhancement, since the AP transmits multicast traffic at a low basic rate, whereas unicast traffic can be transmitted at HT, VHT, or HE rates.
- **Max Clients** — The maximum number of clients that can associate to this SSID at the same time. (Default: 127; Range: 1-256)
- **Minimum signal allowed** — Only allows clients to connect to the radio interface if their signal strength (RSSI) is equal or greater than the specified value. Setting the value to -100 disables this feature. Clients already connected are checked periodically. (Range: -1 to -100; Default: -100)

  This forces clients to associate with an AP that has a better signal strength (also called assisted roaming). Suggested value is -70 to -80 depending on access point density and coverage.
- **Idle Timeout (sec)** — The AP disconnects a client when there is no activity for the configured amount of time. (Default: 300 seconds; Range: 60-60000 seconds)
- **Device OS Blacklist** — Denies access to the SSID from client devices with either Android, iOS/macOS, or Windows operating systems. Set to ON to prevent a client OS from connecting to the SSID. Set to OFF to allow a client OS to connect to the SSID.

Wireless Networks — Security Settings

Figure 44: Wireless Security Settings

1Doc: Protocolo 1.943/2025 | Anexo: em_04C7D8805AD8E32AB062B6E_pdf_Manual_Administrador_Processo_Anexo_MiFi6_029_2025_04_0328.pdf (70/200) 1037/4726

The following items are displayed in this section of the Wireless Settings page:

- **Method** — Sets the wireless security method for each VAP, including association mode, encryption, and authentication. (Default: WPA2-PSK)
  - **No Security** — The VAP broadcasts a beacon signal including the configured SSID. Wireless clients with an SSID setting of "any" can read the SSID from the beacon and automatically set their SSID to allow immediate connection.
  - **WPA-PSK** — For enterprise deployment, WPA requires a RADIUS authentication server to be configured on the wired network. However, for small office networks that may not have the resources to configure and maintain a RADIUS server, WPA provides a simple operating mode that uses just a pre-shared password for network access. The Pre-Shared Key mode uses a common password for user authentication that is manually entered on the access point and all wireless clients. The PSK mode uses the same TKIP packet encryption and key management as WPA in the enterprise, providing a robust and manageable alternative for small networks.
    - **Encryption** — Data encryption uses one of the following methods:
      - **CCMP (AES)** — AES-CCMP is used as the multicast encryption cipher. AES-CCMP is the standard encryption cipher required for WPA2. (This is the default setting.)
      - **Auto: TKIP + CCMP (AES)** — The encryption method used by the client is discovered by the access point.
    - **Key Method** — Uses one of the following PSK methods:
      - **Single PSK** — Enables the entry of a single PSK key.
        - **Key** — WPA is used to encrypt data transmitted between wireless clients and the VAP. WPA uses static shared keys (fixed-length hexadecimal or alphanumeric strings) that are manually distributed to all clients that want to use the network.

          String length must be 8 to 63 ASCII characters (letters and numbers). No special characters are allowed.
      - **Multiple PSK** —Enables the entry of multiple PSK keys. Up to 128 keys can be configured.
        - **Multiple Keys** — Enter multiple keys, one per line. Entering a key with a specific MAC address limits the key for use by a single client. Entering a key without a MAC address enables the key to be used by all clients.

1Doc: Protocolo 1.943/2025 | Anexo: em_04C7D8805AD8E32AB6628B6E_assoc_administrativo_029_2025_Anexo_I_MR6_029_2025_Part_0328.pdf (71/200) 1087/4746

Multiple keys are supported for WPA-PSK, WPA2-PSK, and WPA3 Personal Transition security.

- **Dynamic PSK** — Enables the use of dynamic PSK keys that are periodically generated and updated by a RADIUS authentication server. The RADIUS server IP address, UDP port, and secret text string must be specified. (See "RADIUS Settings" below for details.)

  Dynamic keys are supported only for WPA2-PSK security.

- **WPA2-PSK** — Clients using WPA2 with a Pre-shared Key are accepted for authentication.

  WPA was introduced as an interim solution for the vulnerability of WEP pending the ratification of the IEEE 802.11i wireless security standard. In effect, the WPA security features are a subset of the 802.11i standard. WPA2 includes the now ratified 802.11i standard, but also offers backward compatibility with WPA. Therefore, WPA2 includes the same 802.1X and PSK modes of operation and support for TKIP encryption.

  Refer to WPA-PSK for a description of encryption methods and the key.

- **WPA-EAP** — WPA employs a combination of several technologies to provide an enhanced security solution for 802.11 wireless networks. A RADIUS server is used for authentication, and can also be used for accounting.

  Refer to WPA-PSK for a description of encryption methods.

- **RADIUS Settings** — A RADIUS server must be specified for the access point to implement IEEE 802.1X network access control and Wi-Fi Protected Access (WPA) wireless security.

  In addition, you can configure a RADIUS Accounting server to receive user-session accounting information from the access point. RADIUS Accounting can be used to provide valuable information on user activity in the network.

Note: This guide assumes that you have already configured RADIUS server(s) to support the access point. Configuration of RADIUS server software is beyond the scope of this guide, refer to the documentation provided with the RADIUS server software.

  - **Radius Auth Server** — Specifies the IP address or host name of the RADIUS authentication server.

  - **Radius Auth Port** — The UDP port number used by the RADIUS server for authentication messages. (Range: 1024-65535; Default: 1812)

1Doc: Protocolo 1.943/2025 | Anexo: em1_04C7B8805AD8E32AB062B8E_pt_Administração_Acesso_Anexo_AWF6_029_2025_04_0328.pdf (72/200) 1039/4746

- **Radius Auth Secret** — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS authentication server. Do not use blank spaces in the string. (Maximum length: 255 characters)

- **NAS ID** — The RADIUS NAS identifier for the SSID interface This value must be between 1 and 48 characters long.

- **Backup Radius Auth** — Enables the support of a backup RADIUS authentication server.

  - **Radius Auth Server** — Specifies the IP address or host name of the backup RADIUS authentication server.

  - **Radius Auth Port** — The UDP port number used by the backup RADIUS server for authentication messages. (Range: 1024-65535; Default: 1812)

  - **Radius Auth Secret** — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the backup RADIUS authentication server. Do not use blank spaces in the string. (Maximum length: 200 characters)

- **Use Radius Accounting** — Enables the support of a RADIUS accounting server.

  - **Acct Server** — Specifies the IP address or host name of the RADIUS accounting server.

  - **Acct Port** — The UDP port number used by the RADIUS server for accounting messages. (Range: 1024-65535; Default: 1813)

  - **Acct Secret** — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS accounting server. Do not use blank spaces in the string. (Maximum length: 200 characters)

  - **Acct Interim Interval** — The time (in seconds) between each accounting update sent to the server. (Range: 60-600 seconds; Default: 60 seconds)

- **WPA2-EAP** — WPA was introduced as an interim solution for the vulnerability of WEP pending the ratification of the IEEE 802.11i wireless security standard. In effect, the WPA security features are a subset of the 802.11i standard. WPA2 includes the now ratified 802.11i standard, but also offers backward compatibility with WPA. Therefore, WPA2 includes the same 802.1X and PSK modes of operation and support for TKIP encryption.

1Doc: Protocolo 1.943/2025 | Anexo: em_04C7D8805AD8E32AB062B6E_pdf_Termo_de_Referência_029_2025_Anexo_I_MiFi_029_2025_Part_0328.pdf (73/200) 1050/4746

A RADIUS server is used for authentication, and can also be used to accounting.

Refer to WPA-PSK for a description of encryption methods.

Refer to WPA-EAP for a information on configuring the RADIUS server.

- **WPA3 Personal** — Clients using WPA3 with Simultaneous Authentication of Equals (SAE) are accepted for authentication.

  WPA3 provides more robust password-based authentication called Simultaneous Authentication of Equals (SAE), which replaces Pre-Share Key (PSK) in WPA2-Personal. This technology prevents offline dictionary attacks so that data traffic can be transmitted securely.

- **WPA3 Personal Transition** — Clients using WPA3 with SAE or clients using WPA2 with PSK are accepted for authentication. The AP negotiates the supported authentication and encryption with each client before allowing access to the network.

- **WPA3 Enterprise** — An enhanced version of WPA2-EAP security that uses more robust encryption. Clients must support one of the stronger WPA3 encryption options and use Protected Management Frames (PMF) to be able to access the network. The use of IEEE 802.1X network access control and a RADIUS server is required.

  Refer to RADIUS Settings above for information on RADIUS configuration.

- **WPA3 Enterprise Transition** — Allows WPA3 and WPA2 clients to access the network. Encryption options and the use of Protected Management Frames (PMF) are negotiated with each client before allowing access to the network.

  Refer to RADIUS Settings above for information on RADIUS configuration.

- **WPA3 Enterprise 192-bit** — WPA3 Enterprise security uses a standard 128-bit encryption. For a network handling more sensitive data, there is an option to use 192-bit encryption for additional protection.

  Refer to RADIUS Settings above for information on RADIUS configuration.

- **OWE** — Opportunistic Wireless Encryption (OWE) is the WPA3 open network security that allows users of public Wi-Fi networks to gain secure access without using a password. OWE provides individual encryption of data communications between the AP and each client, but does not provide authentication of user identities.

- **PMF** — Protected Management Frames (PMF) provide WPA2/WPA3 security for unicast and multicast management frames between the AP and clients. The "Optional" setting allows clients that do not support PMF to access the network.

1Doc: Protocolo 1.943/2025 | Anexo: em_04C7D8805AD8E32AB662B6E5_Termo_de_Referência_029_2025_Anexo_I_MiFi_6_029_2025_Part_0328.pdf (74/200) 1050/4726

The "Mandatory" setting allows only clients that support PMF to access the network. (Default: Optional)

- **802.11k** — Provides clients with information on neighbor APs when roaming. As a client is about to roam from an AP, it sends a request for a "Neighbor Report" that includes a list of available APs and associated information. The client can then quickly identify the best AP to which it can roam without having to scan all channels. (Default: Disabled)

- **802.11r** — Provides a method for fast transition roaming between APs. Before clients roam to a new AP, the initial handshake and encryption calculations are performed in advance, which results in a fast hand off without the need for re-authentication. (Default: Disabled)

- **802.11v** — Provides information to associated clients that facilitates the overall improvement of the wireless network. Also helps clients to improve battery life by setting the idle period. (Default: Disabled)

- **Radius MAC Auth** — The MAC address of the associating station is sent to a configured RADIUS server for authentication. (Default: Disabled)

- **Dynamic Authorization** — The Dynamic Authorization Extensions (DAE) to RADIUS enable a server to disconnect or change the authorization of clients that are already connected to the network. (Default: Disabled)

  - **DAE Port** — The UDP port number to use for DAE messages. (Default: 3799)

  - **DAE Client** — Specifies the IPv4 address of the RADIUS server.

  - **DAE Secret** — The shared text string used to encrypt DAE messages between the access point and the RADIUS server.

- **Access Control List** — Wireless clients can be authenticated for network access by checking their MAC address against the local database configured on the access point. (Default: OFF)

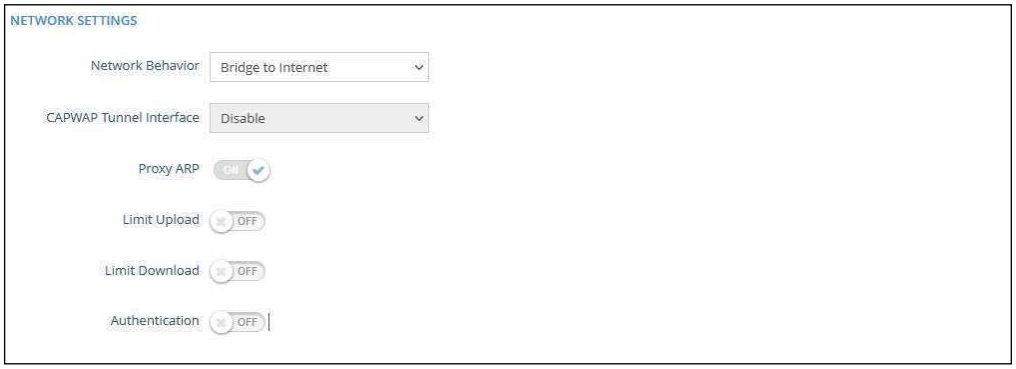
  - **Policy** — The MAC list can be configured to either allow or deny network access to specified clients. (Default: Allow all MACs on list)

  - **Filtered MACs** — List of client MAC addresses. Up to 512 MAC addresses can be configured.

1Doc: Protocolo 1.943/2025 | Anexo: em1_04C7D8805AD8E32AB6628B6E_assoc_administrativo_2025_anexo_MiFi6_029_2025_04_0328.pdf (75/200) 1052/4746

Wireless Networks — Network Settings

Figure 45: Wireless Network Settings



The following items are displayed in this section of the Wireless Settings page:

- **Network Behavior** — One of the following connection methods must be specified. (Default: Route to Internet)
  - **Bridge to Internet** — Configures an interface as attached to the WAN. Traffic from this interface is directly bridged into the Internet. (See Figure 29, "Bridge to Internet", on page 48.)
  - **Route to Internet** — Configures an interface as a member of the LAN. Traffic from this interface is routed across the access point and out through an interface which is bridged to the Internet. (See Figure 30, "Route to Internet", on page 48.)
    - **Network Name** — The network to be routed. The default is "Default local network" as displayed under LAN Settings – Local Network.
  - **Add to Guest Network** — This interface can only support the guest network.
  - **Hotspot Controlled** — This interface can only support hotspot services.
    - **Configure Hotspot** — Opens Hotspot Settings page.
    - **Walled Garden** — Configures the Walled Garden list on the Hotspot Settings page.
  - **VLAN Tag Traffic** — Tags any packets passing from this VAP (virtual access point) to the associated Ethernet port with a VLAN ID configured under "VLAN Settings" on page 80.
    - **VLAN Id** — Selects the configured VLAN ID with which to tag the VAP traffic.
    - **VLAN Settings** — Opens the VLAN Settings page.

1Doc: Protocolo 1.943/2025 | Anexo: em_04C7D8805AD8E32AB062B6E_pdf_Termo_de_Referência_829_2025_Anexo_I_MIFI_829_2025_Part_0328.pdf (76/200) 1052/4746

- **Dynamic VLAN** — The RADIUS server provides the access point with the user VLAN information. The access point assigns the associated user to the related VLAN.
  - **Default VLAN Behavior** — Specifies the behavior (Accept or Reject) when a client's VLAN ID is not defined on the RADIUS server. The default setting is Reject.
    - **Reject** — A client cannot connect to the SSID when the client's VLAN ID is not defined on the RADIUS server.
    - **Accept** — A client can connect to the SSID with an assigned or untagged VLAN ID when the client's VLAN ID is not defined on the RADIUS server.

- **CAPWAP Tunnel Interface** — When the AP system management is set to EWS-Series Controller mode (see "System Settings" on page 83), the CAPWAP (Control And Provisioning of Wireless Access Points) protocol tunnel mode can be configured. The options are "Disable," "Complete," or "Split." A Complete tunnel sends all management, authentication, and data traffic from the AP back to the controller. A Split tunnel only sends the management and authentication traffic to the controller. (Default: Disable)

- **Proxy ARP** — When Proxy ARP is enabled, the AP maintains its own ARP lookup table and replies to ARP requests on behalf of downstream stations, avoiding network inefficiencies. This feature is automatically enabled when client isolation is disabled, and disabled when client isolation is enabled. The feature cannot be configured manually. Proxy ARP is supported when the network behavior is "Bridge to Internet" or "VLAN Tag Traffic."

- **Limit Upload** — Enables rate limiting of traffic from the VAP interface as it is passed to the wired network. You can set a maximum rate in Kbytes per second. (Range: 256-10048576 Kbytes per second; Default: OFF)

- **Limit Download** — Enables rate limiting of traffic from the wired network as it is passed to the VAP interface. You can set a maximum rate in kbytes per second. (Range: 256-10048576 Kbytes per second; Default: OFF)

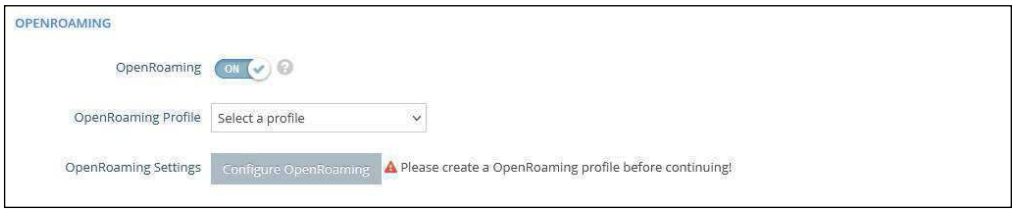
- **Authentication** — When the AP system management is set to ecCLOUD mode (see "System Settings" on page 83), this options authenticates the AP communications with the ecCLOUD controller. (Default: Disabled)

1Doc: Protocolo 1.943/2025 | Anexo: em_04C7B8805AD8E32AB062B6E_Assoc_Administrativo_Processo_Anexo_MiFi6_029_2025_04_0328.pdf (77/200) 1053/4726

Wireless Networks — OpenRoaming

Available when WPA2-EAP security is selected, OpenRoaming (Hotspot 2.0) provides a standard for public-access Wi-Fi networks to support seamless roaming between wireless networks. A OpenRoaming AP advertises its public Wi-Fi capabilities and services so that clients can decide if they want to connect to the network.

Figure 46: OpenRoaming Settings



The following items are displayed in this section of the Wireless Settings page:

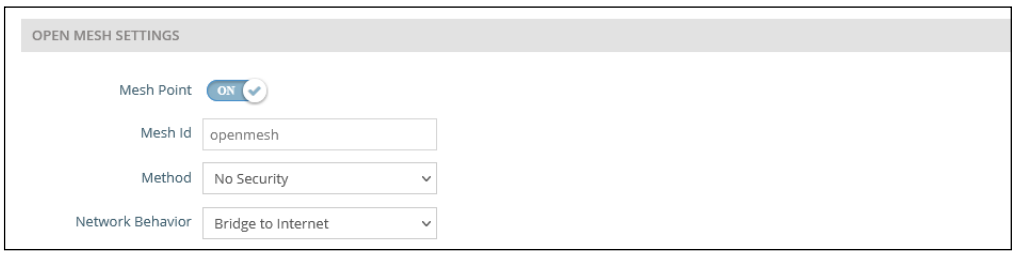
- **OpenRoaming** — Enables OpenRoaming when WPA2-EAP security is selected. (Default: Disabled)
- **OpenRoaming Profile** — Selects the profile to apply to the wireless network. See "OpenRoaming" on page 58 for profile configuration.
- **OpenRoaming Settings** — Click to access the OpenRoaming profile settings page. See "OpenRoaming" on page 58 for profile configuration.

Wireless Networks — Open Mesh Settings

Open Mesh is a network of interconnected node APs, of which only one has a wired connection to the network (and the Internet). The other AP nodes provide wireless links to each other and some support connections to wireless clients. The mesh network not only extends wireless connectivity over a greater distance, but also provides backup links should one node in the network fail.

When setting up an AP to be a node in a mesh network, select one radio interface (2.4 GHz or 5 GHz) and configure it to operate on a specific channel (do not select Auto).Set up other AP nodes to operate on the same radio interface, channel, and with the same SSID.

Figure 47: Open Mesh Settings



The following items are displayed in this section of the Wireless Settings page:

- **Mesh Point** — Enables Open Mesh support on the SSID interface.

1Doc: Protocolo 1.943/2025 | Anexo: em_04C7B805AD8E32AB62B6E_pt_Administrador_Acesso_Anexo_WiFi6_029_2025_04_0328.pdf (78/200) 3055/4726

- **Mesh ID** — Name of the mesh network.
- **Method** — Security applied on Open Mesh links.
  - **No Security** — None.
  - **WPA3-Personal** — Uses WPA3 with Simultaneous Authentication of Equals (SAE) on mesh links to other APs.
- **Network Behavior** — One of the following connection methods must be specified. (Default: Route to Internet)
  - **Bridge to Internet** — Configures an interface as attached to the WAN. Traffic from this interface is directly bridged into the Internet. (See Figure 29, "Bridge to Internet", on page 48.)
  - **Route to Internet** — Configures an interface as a member of the LAN. Traffic from this interface is routed across the access point and out through an interface which is bridged to the Internet. (See Figure 30, "Route to Internet", on page 48.)
    - **Network Name** — The network to be routed. The default is "Default local network" as displayed under LAN Settings – Local Network.

Wireless Networks — Advanced Radio Settings

Figure 48: Advanced Radio Settings

The following items are displayed in this section of the Wireless Settings page:

- **Tx Power** — Adjusts the power of the radio signals transmitted from the access point. The higher the transmission power, the farther the transmission range. Power selection is not just a trade off between coverage area and maximum supported clients. You also have to ensure that high-power signals do not interfere with the operation of other radio devices in the service area. (The range of power settings and defaults are dependent on the AP model and the Country setting.)
- **SGI** — Enables the Short Guard Interval (SGI) in the following 802.11 modes:
  5 GHz radio; 802.11a, 802.11a+ n, 802.11ac+a+n.
  2.4 GHz radio; 802.11 b g+ n.

  The 802.11n draft specifies two guard intervals: 400ns (short) and 800ns (long). Support of the 400ns Short Guard Interval is optional for transmit and receive. The purpose of a guard interval is to introduce immunity to

1Doc: Protocolo 1.943/2025 | Anexo: em_04C7D8805AD8E32AB062B6E_proc_administrativo_029_2025_Anexo_MiFi6_029_2025_Part_0328.pdf (79/200) 1056/4726

propagation delays, echoes, and reflections to which digital data is normally very sensitive. Enabling SGI sets it to 400ns. (Default: Disabled)

VLAN Settings

VLANs (virtual local area networks) are turned off by default. If turned on they will automatically tag any packets passed to the LAN port from the relevant VAP (virtual access point).

The access point can employ VLAN tagging to control access to network resources and increase security. VLANs separate traffic passing between the access point, associated clients, and the wired network. You can create up to 16 VLAN tagged networks.

Note the following points about the access point's VLAN support:

- If an Ethernet LAN port on the access point is assigned a VLAN ID, any traffic entering that port must be also tagged with the same VLAN ID.
- Wireless clients associated to the access point can be assigned to a VLAN. Wireless clients are assigned to the VLAN for the VAP interface with which they are associated. The access point only allows traffic tagged with correct VLAN IDs to be forwarded to associated clients on each VAP interface.
- When VLAN support is enabled on the access point, traffic passed to the wired network is tagged with the appropriate VLAN ID. When an Ethernet port on the access point is configured as a VLAN member, traffic received from the wired network must also be tagged with the same VLAN ID. Received traffic that has an unknown VLAN ID or no VLAN tag is dropped.
- When VLAN support is disabled, the access point does not tag traffic passed to the wired network and ignores the VLAN tags on any received frames.
- Network IP range conflict detection and resolution — The AP has two built-in local networks - one "main" network, and the more secure "guest" network. By default, the subnet ranges of these networks is set to 192.168.2.1 and 192.168.3.1, respectively.

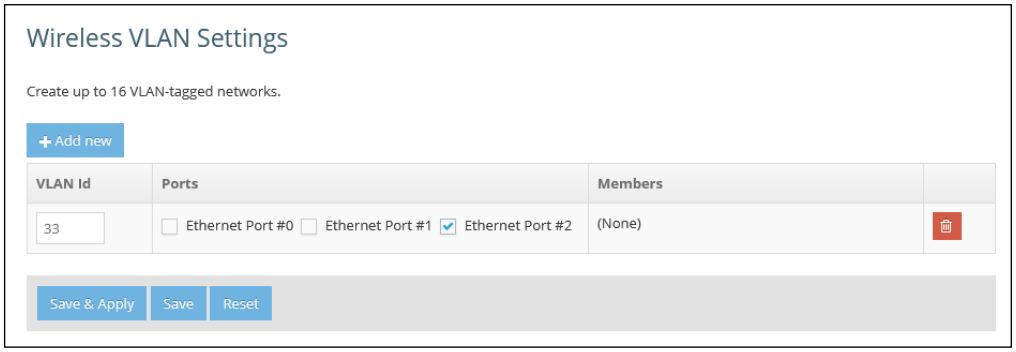
  If your network is already configured to use one of these subnets, when you plug in your network cable to the WAN port of your AP, there would normally be an IP conflict in the local AP's network and your upstream network.

  However, if your WAN subnet conflicts with any of the local networks (even the custom ones you create), the AP will automatically change the subnet of the local network.

1Doc: Protocolo 1.943/2025 | Anexo: em_04C7D8805AD8E32AB062B6E_Solicitação_de_Autorização_para_Uso_de_Radiofrequência_-_Anexo_Manual_Wi-Fi_6_AP_-_2025_04_0328.pdf (80/200) 1057/4746

Note: Before enabling VLAN tagging on the access point, be sure to configure the attached network switch port to support tagged VLAN frames for the VLAN IDs configured on the access point. Otherwise, connectivity to the access point will be lost when you enable the VLAN feature.

Figure 49: Configuring VLANs



The following items are displayed on this page:

- **VLAN ID** — A VLAN identifier to be assigned. (Range: 2-4094) (VLANs 1 is reserved for internal use.)
- **Ports** — The Ethernet ports assigned to the specified VLAN.
- **Members** — The SSID of a VAP configured to be a member of the specified VLAN. This option is configured under Radio Settings (Network Settings – Network Behavior).

1Doc: Protocolo 1.943/2025 | Anexo: em_04C7B8805AD8E32AB062B6E_Manual_Administrador_Access_Point_Intelbras_820_2025_Anexo_Manual_WiFi6_AP_2025_04_0328.pdf (81/200) 1057/4726

5 System Settings

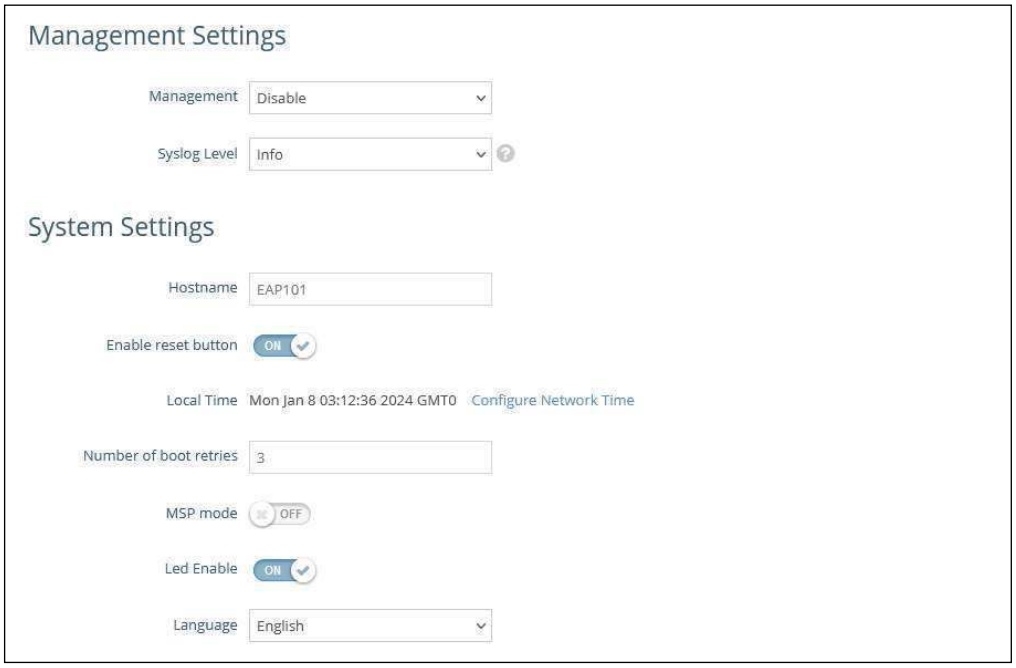
This chapter describes maintenance settings on the access point. It includes the following sections:

1Doc: Protocolo 1.943/2025 | Anexo: em_04C7B8805AD8E32AB062B9E_Solicitação_de_Credenciamento_Anexo_VI_Fi6_29_2025_14_0328.pdf (82/200) 1059/4746

System Settings

The System Settings page can be used to enable the AP to be managed from the Edgecore ecCLOUD controller or EWS-Series Controller, and configure general descriptive information about the AP.

Figure 50: System Settings



The following items are displayed on this page:

- **Management** — Set to "ecCLOUD" to manage this AP from the Edgecore ecCLOUD controller. Set to "EWS-Series Controller" to manage this AP from an Edgecore EWS-Series controller in the local network. Set to disable to manage the AP through the web interface in a stand-alone mode.
  - **ecCLOUD** — When selected, the following parameters are displayed:
    - **Controller URL** — Provides a URL link to the Edgecore ecCLOUD controller management site.
    - **Enable agent** — Enables the AP to be managed from the ecCLOUD controller.
      - **Registration URL** — Specifies the URL for device registration.
    - **Log Level** — Adjusts the system log level for the ecCLOUD daemon (mgmtd). The default value is Info. The standard ranking of log levels is as follows: Trace < Debug < Info < Warn < Error.

1Doc: Protocolo 1.943/2025 | Anexo: em1_04C7B8805AD8E32AB062B6E_Especificações_técnicas_e_Manual_MiFi6_029_2025_04_0328.pdf (83/200) 1069/4746

- **EWS-Series Controller** — When selected, the following parameters are displayed:
  - **CAPWAP** — Enables CAPWAP (Control And Provisioning of Wireless Access Points) protocol tunnel mode.
  - **DNS SRV Discovery** — The AP uses DNS server records to discover the EWS controller to which it can send a CAPWAP join request.
    - **Domain Name Suffix** — Specifies the domain suffix of the controller.
  - **DHCP Option Discovery** — The AP uses the DHCP server to obtain an IP address in the same subnet as the EWS controller, which it can then discover and send a CAPWAP join request.
  - **Broadcast Discovery** — The AP sends broadcast requests to discover the EWS controller in the same subnet.
  - **Multicast Discovery** — The AP sends multicast discover packets across the network to find the EWS controller. This option requires routing paths to be properly configured in the network.
  - **Static Discovery** — Provides a manual method to reach an EWS controller by entering IP addresses that the AP uses to send a CAPWAP join request.

- **Syslog Level** — Limits system log messages based on severity. The standard ranking of log levels is as follows: Debug < Info < Notice < Warning < Error < Critical < Alert < Emergency. (Default: Info)
- **Hostname** — An alias for the AP, enabling the device to be uniquely identified on the network. (Default: EAP101; Range: 1-63 ASCII characters. Only accepts A-Z, a-z, 0-9, and dash "-".)
- **Enable Reset Button** — Enables the AP's hardware reset button. (Default: Enabled)
- **Local Time** — The local time, given as day of week, month, time, year.
- **Number of boot retries** — The maximum number of bootup retries before switching to the next boot bank. (Range: 1-254; Default: 3)
- **MSP Mode** — Enables the Managed Service Provider (MSP) mode that prevents end-users from accessing and modifying most device settings from user-defined user accounts. Management access from "root" and "admin" accounts still provide full access to all device settings. (Default: Disabled)

  With MSP mode enabled, service providers have the option of making specific wireless SSID settings available for user configuration by enabling the "Local

1Doc: Protocolo 1.943/2025 | Anexo: em_04C7D8805AD8E32AB662B8E_Processo_Administrativo_029_2025_Anexo_MiFi6_029_2025_Part_0328.pdf (84/200) 1060/4746

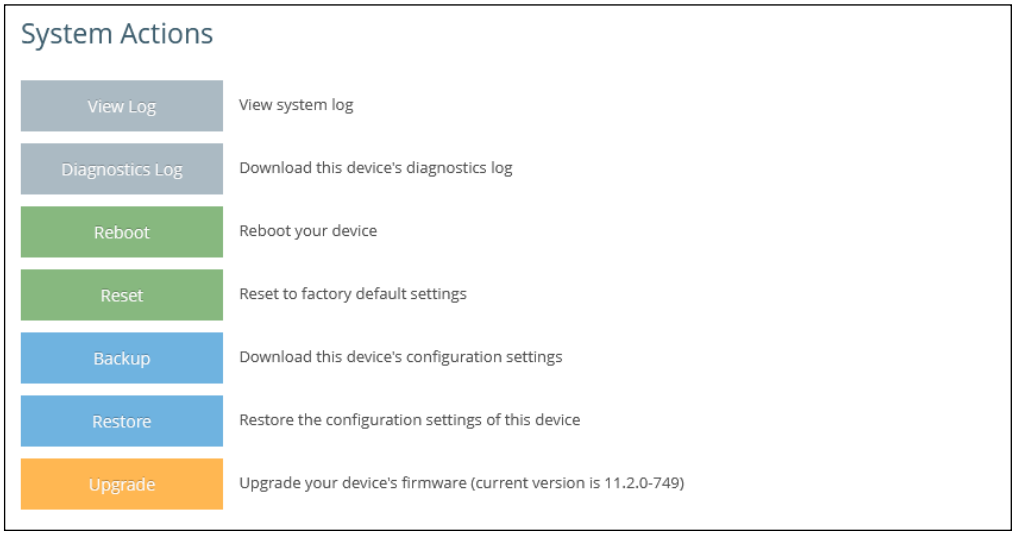
Configurable" setting. See "Wireless Networks — General Settings" on page 69.

- **LED Enable** — Enables the LED indicators on the AP. (Default: Enabled)
- **Language** — Selects the web interface language. (Options: English, Japanese; Default: English)

Maintenance

The Maintenance page supports general maintenance tasks including displaying the system log, downloading a diagnostics log, rebooting the device, restoring factory defaults, backing up or restoring configuration settings, and upgrading firmware.

Figure 51: Maintenance

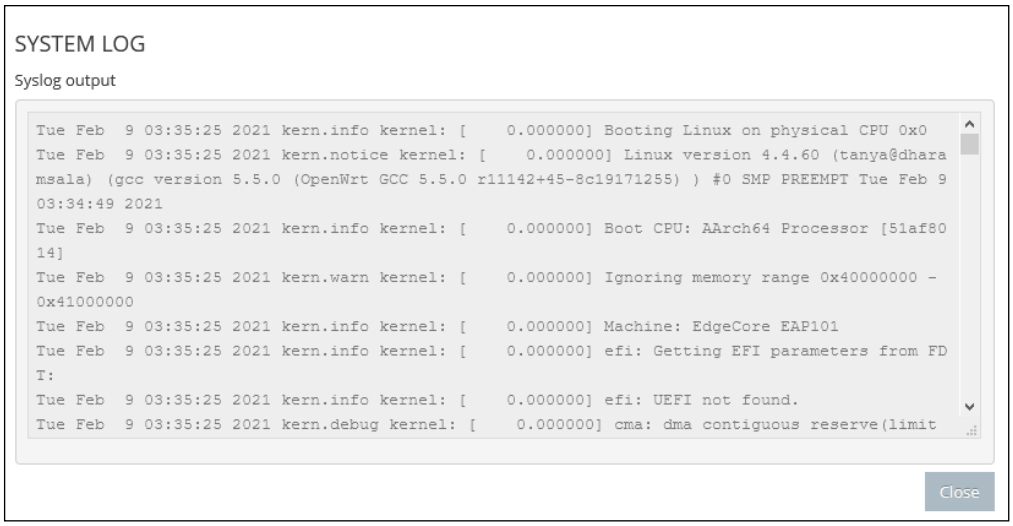


1Doc: Protocolo 1.943/2025 | Anexo: em_04C7B8805AD8E32AB062B6E_Solicitação_de_Homologação_Anatel_MiFi_6_29_2025_04_0328.pdf (85/200) 1062/4746

Displaying System Logs

The access point saves event and error messages to a local system log database. The log messages include the date and time, device name, message type, and message details.

Figure 52: System Log



Downloading the Diagnostics Log

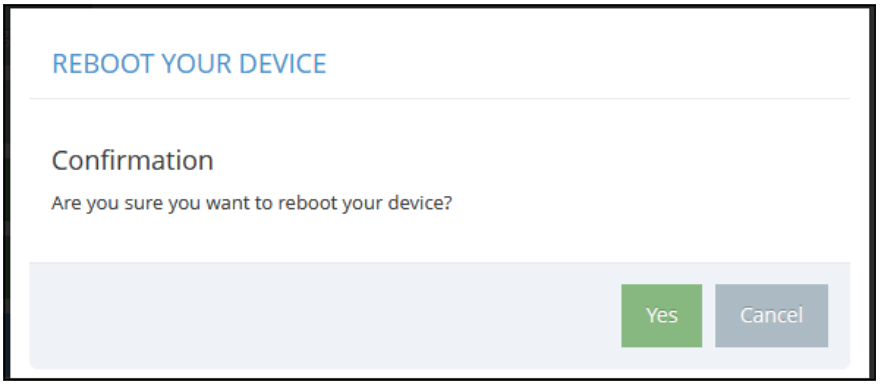
Click “Diagnostics Log” to download the log file to the management workstation. In Windows, a GNU Zip (*.tar.gz) file is stored in the Downloads folder.

The diagnostics log file contains information that can help Edgecore resolve technical issues with the AP.

Rebooting the Access Point

The Reboot page allows you to reboot the access point.

Figure 53: Rebooting the Access Point

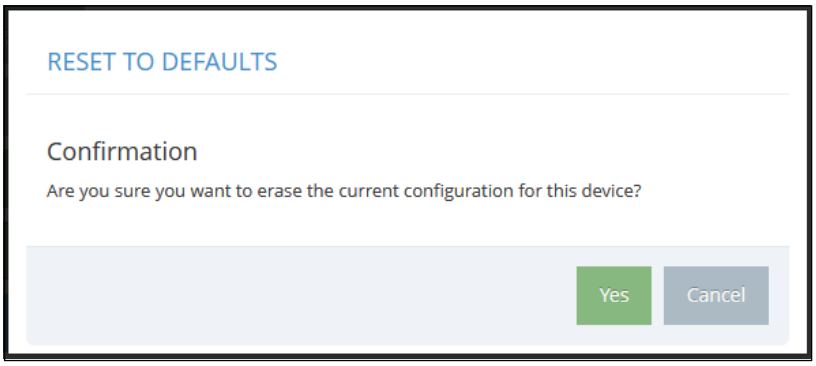


1Doc: Protocolo 1.943/2025 | Anexo: em1_04C7B8805AD8E32AB062B6E_solicitud_de_autorizacion_para_el_proceso_de_licitacion_WiFi6_29_2025_04_0328.pdf (86/200) 1062/4746

Resetting the Access Point

The Reset page allows you to reset the access point to the factory defaults. Note that all user configured information will be lost. You will have to re-enter the default user name and password to re-gain management access to this device.

Figure 54: Resetting to Defaults



Note: It is also possible to reboot or reset the access point by inserting a pin in the pin hole labeled "Reset" on the connector panel of the access point and:

- give a quick press to reboot the access point;
- press and hold for 5 seconds to reset the access point to factory defaults.

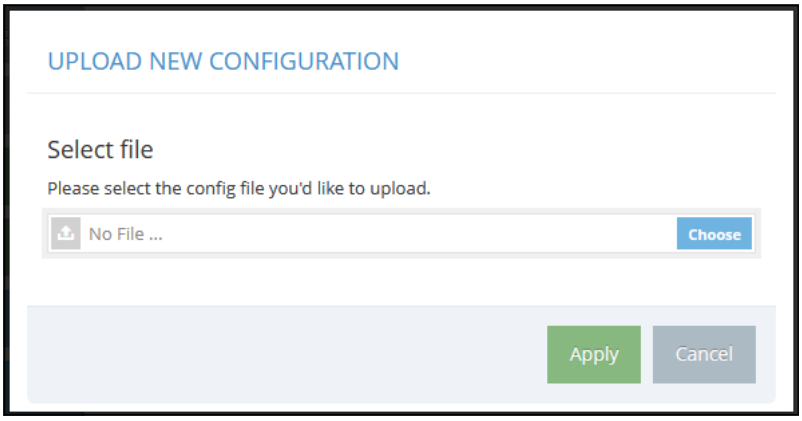
Backing Up Configuration Settings

The Backup function allows you to back up the access point's configuration to a management workstation. In Windows, a GNU Zip (*.tar.gz) file will be stored in the Downloads folder. This is a sample file name: backup-EAP101-2021-02-09.tar.gz

Restoring Configuration Settings

The Restore page allows you to upload configuration settings from a management workstation. The specified file must be one that was previously backed up from the access point.

Figure 55: Restoring Configuration Settings



1Doc: Protocolo 1.943/2025 | Anexo: em_04C7D8805AD8E32AB6628B5E_Solicitação_de_Credenciamento_Anexo_I_-_Anexo_VI_-_Art_6_29_2025_04_0328.pdf (87/200) 1063/4726

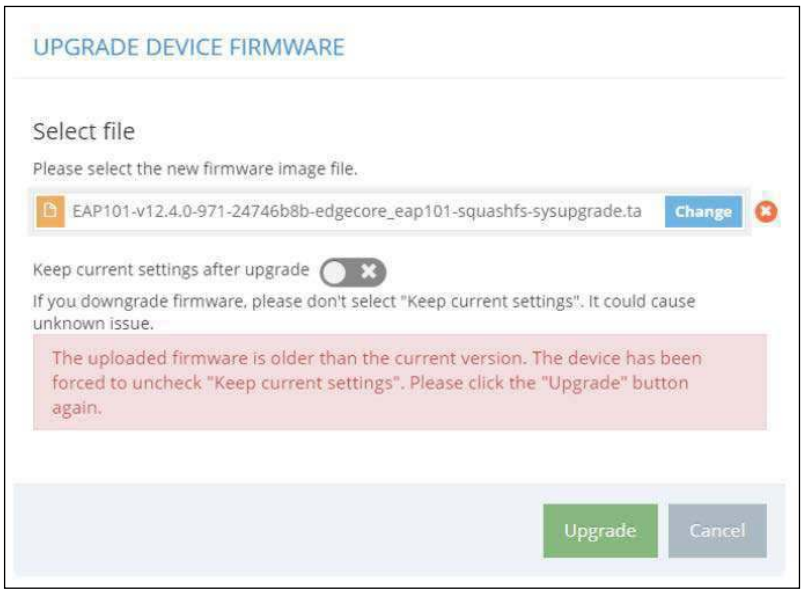
Upgrading Firmware

You can upgrade new access point software from a local file on the management workstation. New software may be provided periodically from Edgecore.

After upgrading new software, you must reboot the access point to implement the new code. Until a reboot occurs, the access point will continue to run the software it was using before the upgrade started. The access point supports dual software images, so if newly loaded software is corrupted, the alternate image will be used on the next reboot. Configuration settings are stored separately from the software, so the current settings will always be used for any new software. However, note that if the current configuration settings are corrupted, the system defaults will be used.

Note: If the uploaded firmware is older than the current version, the device forces the "Keep current settings after upgrade" option to unchecked.

Figure 56: Upgrading Firmware

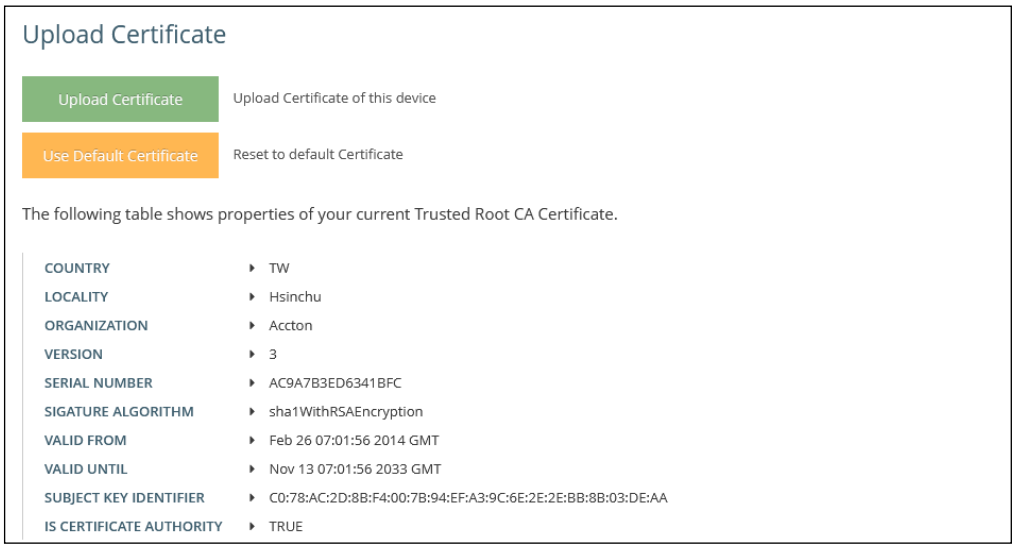


Upload Certificate

The Upload Certificate page allows you to upload a unique security certificate from a trusted certification authority for secure access (an encrypted connection) to a configured HTTPS captive portal. Alternatively, you can also reset to use the default certificate.

1Doc: Protocolo 1.943/2025 | Anexo: em1_04C7B8805AD8E32AB062B6E_Especificações_Técnicas_e_Processo_de_Aquisição_de_WiFi_6_29_2025_pt_0328.pdf (88/200) 1065/4746

Figure 57: Upload Certificate



The following items are displayed on this page:

- **Upload Certificate** — Click to upload a security certificate and private key from a trusted certification authority.
- **Use Default Certificate** — Click to reset to use the AP's default certificate.

User Accounts

The User Accounts page allows you to control management access to the AP based on manually configured user names and passwords.

Figure 58: User Accounts

The following items are displayed on this page:

- **Enabled** — Click to enable or disable the user account.
- **Username** — The name of the user. (Range: 1-32 ASCII characters. Only accepts A-Z, a-z, 0-9, period ".", underscore "_", and hyphen "-". Usernames cannot begin with a hyphen "-" or period ".".)

1Doc: Protocolo 1.943/2025 | Anexo: em_04C7D805AD8E32AB62B8E_pt_Administrador_Acesso_Administrador_Acesso_Anexo_MiFi6_029_2025_04_0328.pdf (89/200) 1066/4746

- **Password** — The user password. (Range: 6-20 ASCII characters, case sensitive, no special characters)

Services

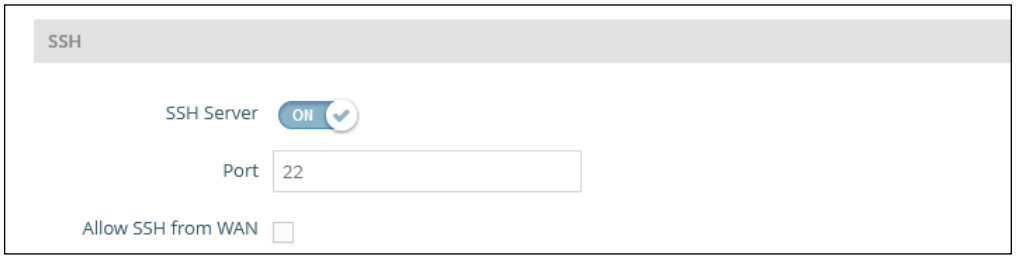
The Services page allows you to control SSH management access to the AP, configure NTP time servers, and configure iBeacon settings.

SSH

The Secure Shell (SSH) can act as a secure replacement for Telnet. The SSH protocol uses generated public keys to encrypt all data transfers passing between the access point and SSH-enabled management station clients and ensures that data traveling over the network arrives unaltered. Clients can then securely use the local user name and password for access authentication.

Note that SSH client software needs to be installed on the management station to access the access point for management via the SSH protocol.

Figure 59: SSH Settings



The following items are displayed on this page:

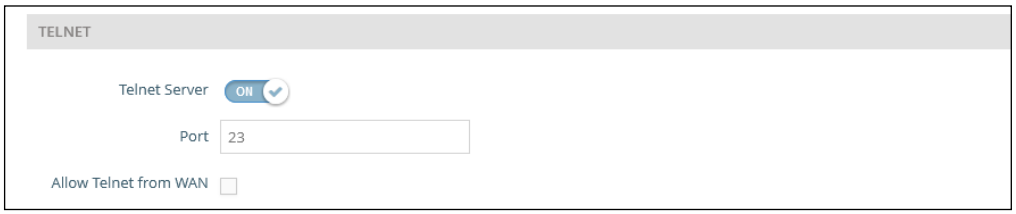
- **SSH Server** — Enables or disables SSH access to the access point. (Default: Enabled)
- **Port** — Sets the TCP port number for the SSH server on the access point. (Range: 1-65535; Default: 22)
- **Allow SSH from WAN** — Allows SSH management access from the WAN.

1Doc: Protocolo 1.943/2025 | Anexo: em1_04C7B8805AD8E32AB062B6E_Associação_Administrativa_Processo_Administrativo_2025_Anexo_Anexo_MiFi6_029_2025_04_0328.pdf (90/200) 1066/4746

Telnet

Telnet is a remote management tool that can be used to configure the access point from anywhere in the network. However, note that Telnet is not secure from hostile attacks.

Figure 60: Telnet Server Settings



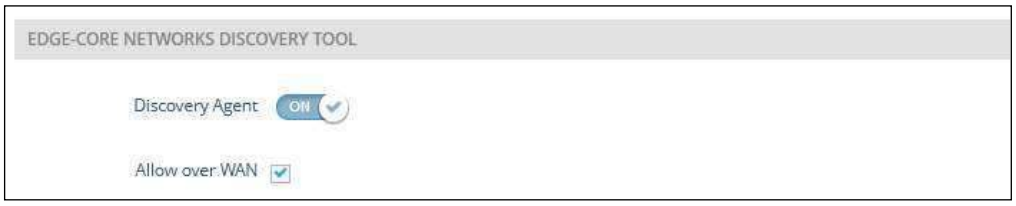
The following items are displayed on this page:

- **Telnet Server** — Enables or disables Telnet access to the access point. (Default: Enabled)
- **Port** — Sets the TCP port number for the Telnet server on the access point. (Range: 1-65535; Default: 23)
- **Allow Telnet from WAN** — Allows Telnet management access from the WAN.

Edgecore Networks Discovery Tool

The Discovery Tool agent enables the AP to find other Edgecore devices in the same Layer 2 network. See "Device Discovery" on page 99 to scan the network for devices.

Figure 61: Discovery Agent Settings



The following items are displayed on this page section:

- **Discovery Agent** — Enables the discovery agent. (Default: Enabled)
- **Allow over WAN** — Enables the discovery agent to operate over the port connected to the Internet source. (Default: Enabled)

Web Server

A Web browser provides the primary method of managing the access point. Both HTTP and HTTPS service can be accessed independently. If you enable HTTPS, you must indicate this in the URL: https://device:port_number]

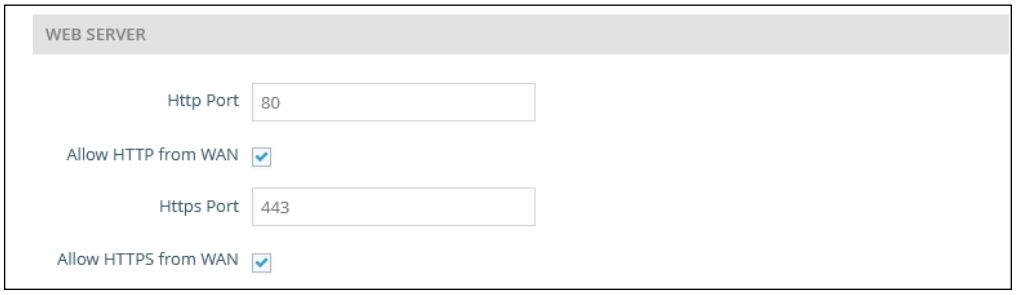
When you start HTTPS, the connection is established in this way:

- The client authenticates the server using the server's digital certificate.

1Doc: Protocolo 1.943/2025 | Anexo: em_D4C7B8B05AD8E32AB662B6E_proc_administrativo_020_2025_anexo_Anexo_MiFi6_020_2025_Part_0328.pdf (91/200) 1063/4726

- The client and server negotiate a set of security protocols to use for the connection.
- The client and server generate session keys for encrypting and decrypting data.
- The client and server establish a secure encrypted connection.
- A padlock icon should appear in the status bar for most browsers.

Figure 62: Web Server Settings



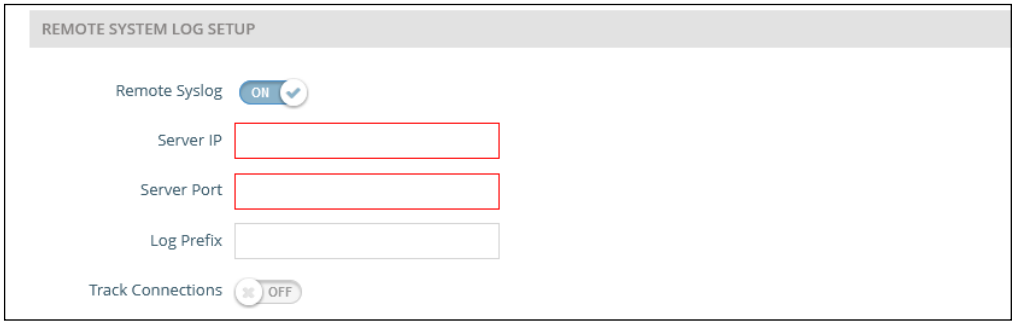
The following items are displayed on this page:

- **HTTP Port** — The TCP port to be used by the HTTP Web browser interface. (Range: 1-65535; Default: 80)
- **Allow HTTP from WAN** — Allows HTTP management access from the WAN.
- **HTTPS Port** — The TCP port to be used by the HTTPS Web browser interface. (Range: 1-65535; Default: 443)
- **Allow HTTPS from WAN** — Allows HTTPS management access from the WAN.

Remote System Log Setup

Use this feature to send log messages to a Syslog server.

Figure 63: Remote System Log Settings



The following items are displayed on this page:

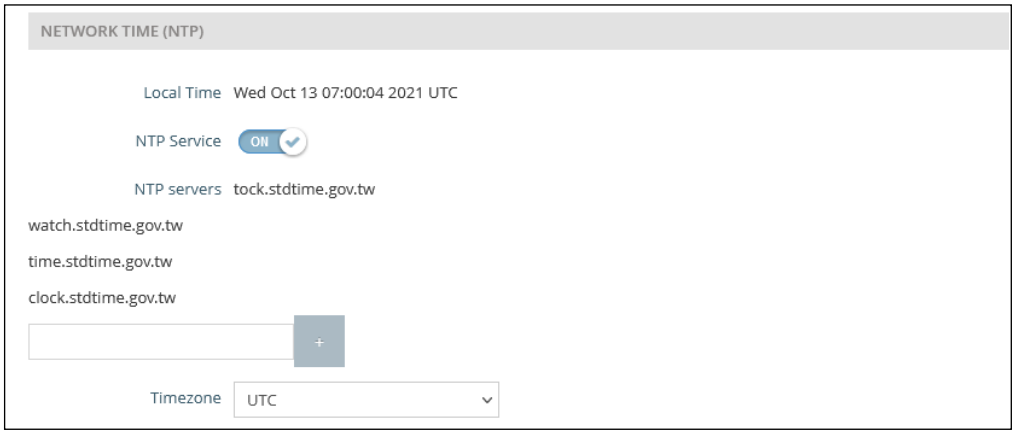
- **Remote Syslog** — Enables the logging of debug or error messages to the remote logging process. (Default: Disabled)
- **Server IP** — Specifies the IP address of a remote Syslog server that will be sent log messages.
- **Server Port** — Specifies the UDP port number used by the remote Syslog server. (Range: 1-65535)
- **Log Prefix** — Sets a prefix string for log messages sent to the specified server. The prefix can help with sorting messages on the server.
- **Track Connections** — Enables the inclusion of connection information such as source IP and port, destination IP and port in log messages.

Network Time

Network Time Protocol (NTP) allows the access point to set its internal clock based on periodic updates from a time server (SNTP or NTP). Maintaining an accurate time on the access point enables the system log to record meaningful dates and times for event entries. If the clock is not set, the access point will only record the time from the factory default set at the last bootup.

The access point acts as an NTP client, periodically sending time synchronization requests to specified time servers. The access point will attempt to poll each server in the configured sequence to receive a time update.

Figure 64: NTP Settings



The following items are displayed on this page:

- **Local Time** — Displays the local time as day of week, month, hour:minute:second, year, based on Universal Time Coordinates.
- **NTP Service** — Enables or disables sending of requests for time updates. (Default: Enabled)

1Doc: Protocolo 1.943/2025 | Anexo: em_04C7B80D5AD8E32AB062B8E_pt_Administrador_Acesso_Anexo_MiFi6_029_2025_04_0328.pdf (93/200) 1059/4746

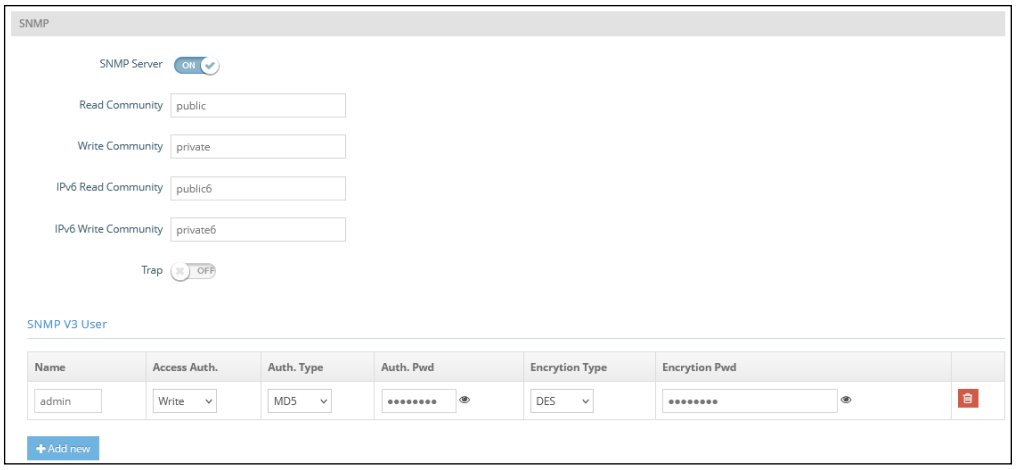
- **NTP Servers** — Sets the host names for time servers. The switch attempts to update the time from the first server, if this fails it attempts an update from the next server in the sequence. To configure additional servers, click the "+" button to open a new edit field.

- **Timezone** — To display a time corresponding to your local time, choose one of the predefined time zones from the scroll-down list.

SNMP

Simple Network Management Protocol (SNMP) is a communication protocol designed specifically for managing devices on a network. It is typically used to configure these devices for proper operation in a network environment, as well as to monitor them to evaluate performance or detect potential problems.

Figure 65: SNMP Settings



The following items are displayed on this page:

- **SNMP Server** — Enables or disables SNMP on the access point. (Default: Enabled)

- **Read Community** — A community string that acts like a password and permits read access to the access point's Management Information Base (MIB). (Range: 1-32 characters, case sensitive; Default: public)

- **Write Community** — A community string that acts like a password and permits write access to the access point's Management Information Base (MIB). (Range: 1-32 characters, case sensitive; Default: private)

- **IPv6 Read Community** — A community string for IPv6 read access to the access point's Management Information (MIB) database. (Range: 1-32 characters, case sensitive; Default: public6)

- **IPv6 Write Community** — A community string for IPv6 write access to the access point's Management Information (MIB) database. (Range: 1-32 characters, case sensitive; Default: private6)

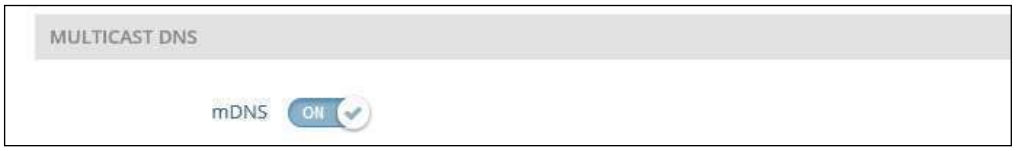
1Doc: Protocolo 1.943/2025 | Anexo: em_04C7B8805AD8E32AB6B2B8E_pt_Administração_Acesso_Anexo_MiFi6_029_2025_04_0328.pdf (94/200) 1070/4746

- **Trap** — Enables the sending of SNMP trap messages to a specified server. The access point sends the following trap messages: cold start, warm start, link up, and link down. (Default: Disabled)
  - **Server IP** — Specifies the IP address of the SNMP trap server that will be sent trap messages.
- **SNMPv3 User** — SNMP protocol version 3 provides secure access by account authentication and data encryption. An SNMP v3 user can be defined by clicking the "Add new" button.
  - **Name** — The user name used to access the SNMP service.
  - **Access Auth** — Select the access permission as "Read" or "Write."
  - **Auth Type** — Select the hash algorithm for authentication.
  - **Auth Pwd** — Configure the password for authentication.
  - **Encryption Type** — Select the encryption algorithm for data packets.
  - **Encryption Pwd** — Configure the password for data encryption.

Multicast DNS

The multicast DNS (mDNS) protocol is a zero-configuration service to facilitate connections within a local networks.

Figure 66: Multicast DNS Settings



The following items are displayed on this page:

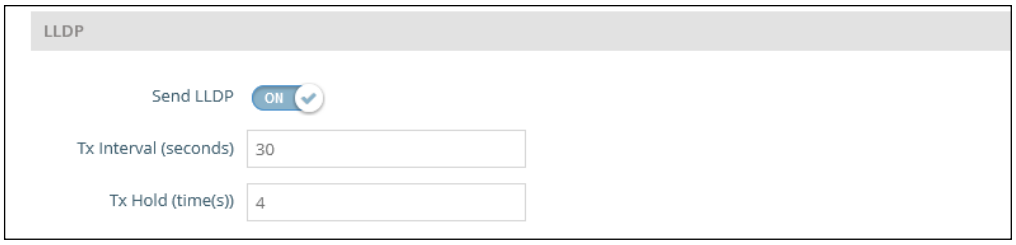
- **mDNS** — Enables or disables Multicast DNS on the access point. (Default: Enabled)

1Doc: Protocolo 1.943/2025 | Anexo: em_04C7D8805AD8E32AB6628B6E_Solicitação_de_Homologação_Anexo_Manual_6_029_2025_14_6328.pdf (95/200) 1062/4746

LLDP

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices in a network. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device.

Figure 67: LLDP Settings



The following items are displayed on this page:

- **Send LLDP** — Enables the sending of LLDP advertisements about the AP to neighboring devices in the network. (Default: Disabled)
- **Tx Interval (seconds)** — Sets the periodic transmit interval for LLDP advertisements. (Range: 5-32768 seconds; Default: 30 seconds)
- **Tx Hold (time(s))** — Configures a time-to-live (TTL) value sent in the LLDP advertisements as shown in the formula below. (Range: 2-10; Default: 4)

  The time-to-live tells the receiving LLDP agent how long to retain all information pertaining to the sending device if it does not transmit updates in a timely manner.

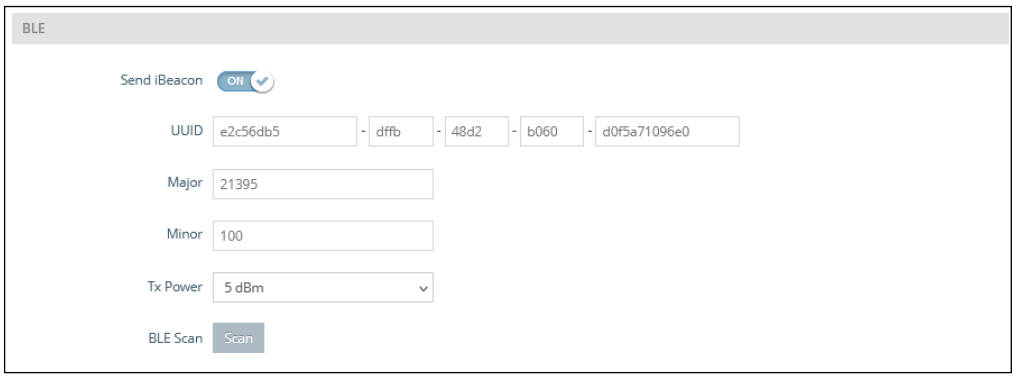
  The TTL in seconds is based on the following rule:
  minimum value ((Tx Interval * Tx Hold), or 65535)
  Therefore, the default TTL is 4*30 = 120 seconds.

1Doc: Protocolo 1.943/2025 | Anexo: em1_04C7B8805AD8E32AB662B6E_pt_Administração_Processo_Anexo_MiFi6_029_2025_04_0328.pdf (96/200) 1062/4746

BLE

The AP supports the iBeacon standard based on Bluetooth Low Energy (BLE). Devices with BLE Beacons can provide location-based services to BLE clients, such as phones, that can recognize the beacon advertisements, extract the provided information, and then take actions based on the content.

Figure 68: BLE Settings

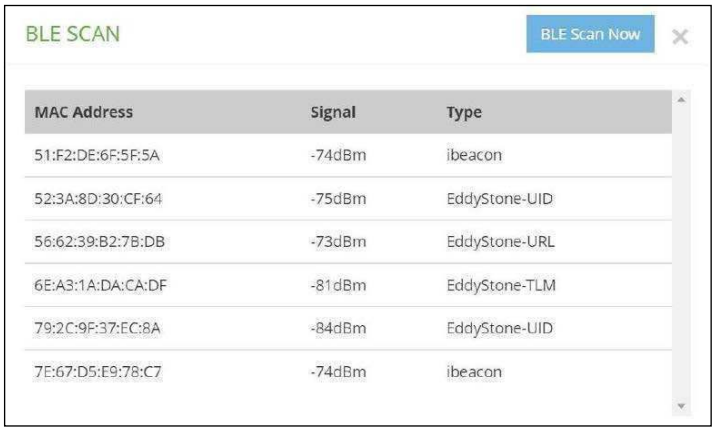


The following items are displayed on this page:

- **Send iBeacon** — Enables iBeacon support on the AP. (Default: Enabled)
- **UUID** — The iBeacon Universally Unique Identifier that advertises the beacon service. The UUID contains 32 hexadecimal digits in five groups, separated by hyphens.
- **Major** — The iBeacon value that is used to identify a beacon group. (Range: 0-65535)
- **Minor** — The iBeacon value that is used to identify individual beacons within a group. (Range: 0-65535)
- **Tx Power** — Sets the BLE radio transmit power (supported only on EAP101 and EAP104). (Range: 5 dBm to -20 dBm; Default: 5 dBm)
- **BLE Scan** — (EAP101 and EAP104 only) Scans for all BLE devices, including these four types: EddyStone-UID, EddyStone-URL, EddyStone-TLM, and ibeacon.

1Doc: Protocolo 1.943/2025 | Anexo: em_04C7B8805AD8E32AB062B6E_pt_Administrador_Acesso_Local_v6_29_2025_04_0328.pdf (97/200) 1073/4726

Figure 69: BLE Scan



Diagnostics

The Diagnostics page provides Ping, Traceroute, Nslookup, and Speed Test tools for troubleshooting connectivity problems.

Ping Enter a hostname or IP address and click to run the ping tool.

Figure 70: Network Utilities - Ping

Traceroute Enter a hostname or IP address and click to run the traceroute tool.

Figure 71: Network Utilities - Traceroute

Nslookup Enter a hostname or IP address and click to run the Nslookup tool.

1Doc: Protocolo 1.943/2025 | Anexo: em1_04C7B8805AD8E32AB662B6E_pdf_Termo_de_Referência_829_2025_Anexo_I_-_MiFi_6_429_2025_Part_0328.pdf (98/200) 1075/4746

Figure 72: Network Utilities - Nslookup

Speed Test Enter a hostname or IP address of a Netperf server to test the speed between the AP and server.

Figure 73: Network Utilities - Speed Test

Device Discovery

The Device Discovery Tool provides a method for finding other Edgecore APs within the same Layer 2 network. To function, the Discovery Agent must be enabled (see "Edgecore Networks Discovery Tool" on page 91.

Click the Scan Network button to scan for devices.

Figure 74: Device Discovery Tool

1Doc: Protocolo 1.943/2025 | Anexo: em1_04C7B8805AD8E32AB062B6E_proc_administrativo_029_2025_Anexo_I_MiFi_6_029_2025_Part_0328.pdf (99/200) 1076/4746

Section III

Appendices

This section provides additional information and includes these items:

1Doc: Protocolo 1.943/2025 | Anexo: em1_04C7B8805AD2E821B662B8E_procuradoria_e_assessoria_juridica_-_Termo_de_Referencia_-_Aquisicao_de_Switch_e_Access_Point_WiFi_6_-_Parte_1_de_3.pdf (100/200) 1076/4746

A Troubleshooting

Problems Accessing the Management Interface

Table 1: Troubleshooting Chart

Symptom	Action
Cannot connect using a web browser	■ Be sure the AP is powered up. ■ Check network cabling between the management station and the AP. ■ Check that you have a valid network connection to the AP and that intermediate switch ports have not been disabled. ■ Be sure you have configured the AP with a valid IP address, subnet mask and default gateway. ■ Be sure the management station has an IP address in the same subnet as the AP's IP. ■ If you are trying to connect to the AP using a tagged VLAN group, your management station, and the ports connecting intermediate switches in the network, must be configured with the appropriate tag. ■ If you cannot connect using SSH, you may have exceeded the maximum number of concurrent SSH sessions permitted. Try connecting again at a later time.
Forgot or lost the password	■ Reset the AP to factory defaults using its Reset button.

Using System Logs

If a fault does occur, refer to the *Quick Start Guide* to ensure that the problem you encountered is actually caused by the AP. If the problem appears to be caused by the AP, follow these steps:

1. Repeat the sequence of commands or other actions that lead up to the error.
2. Make a list of the commands or circumstances that led to the fault. Also, make a list of any error messages displayed.
3. Record all relevant system settings.
4. Display the log file through the System > Maintenance page, and copy the information from the log file.
5. Download the Diagnostics Log to a file from the System > Maintenance page.

1Doc: Protocolo 1.943/2025 | Anexo: em1_04C7B8805AD2E821B662B8E_protocolo_administrativo_029_2025_Parte_328.pdf (101/200) 1067/4746

6. Contact Edgecore and send a detailed description of the problem, along with all of the information mentioned in the above steps.

1Doc: Protocolo 1.943/2025 | Anexo: em1_04C7B8805AD2E821B662B8E_procuradoria_2025_Anexo_AWF6_029_2025_Part_0328.pdf (102/200) 1079/4746

Wi-Fi 6 Access Point

Software Release 12.5.3

User Manual

www.edge-core.com

User Manual

Wi-Fi 6 Access Point

Cloud-Enabled Enterprise Access Points
EAP101
EAP102
EAP104
EAP104 (WL)
EAP111
EAP112
OAP101

E062024-CS-R15

How to Use This Guide

This guide includes detailed information on Edgecore access point (AP) software, including how to operate and use the management functions of APs. To deploy APs effectively and ensure trouble-free operation, you should first read the relevant sections in this guide so that you are familiar with all software features.

Who Should Read This Guide?

This guide is for network administrators who are responsible for operating and maintaining network equipment. The guide assumes a basic working knowledge of LANs (Local Area Networks) and the Internet Protocol (IP).

How This Guide is Organized

The organization of this guide is based on the AP's web management interface. An introduction and initial configuration information is also provided.

The guide includes these sections:

- Section I "Getting Started" — Includes an introduction to AP management and initial configuration settings.
- Section II "Web Configuration" — Includes all management options available through the web interface.
- Section III "Appendices" — Includes information on troubleshooting AP management access.

Related Documentation

This guide focuses on AP software configuration, it does not cover hardware installation of an AP. For specific information on how to install an AP, see the following guide:

Quick Start Guide

For all safety information and regulatory statements, see the following documents:

Quick Start Guide

1Doc: Protocolo 1.943/2025 | Anexo: em_3[illegible] 1082/4746

Conventions

The following conventions are used throughout this guide to show information:

Note: Emphasizes important information or calls your attention to related features or instructions.

Caution: Alerts you to a potential hazard that could cause loss of data, or damage the system or equipment.

Revision History

This section summarizes the changes in each revision of this guide.

June 2024 Revision

This is the 15th revision of this guide. It is valid for software release v12.5.3 and includes the following changes:

- Added support for EAP112
- Added HaLow and LTE support for EAP112
- Added 3G/LTE to Internet settings, see "Internet Settings" on page 43
- Added MQTT to BLE settings, see "BLE" on page 97

March 2024 Revision

This is the 14th revision of this guide. It is valid for software release v12.5.3 and includes the following changes:

- Minimum Signal Allowed setting for each SSID, see "Wireless Networks — General Settings" on page 69
- Added Device OS Blacklist, see "Wireless Networks — General Settings" on page 69

January 2024 Revision

This is the 13th revision of this guide. It is valid for software release v12.5.0 and includes the following changes:

- Added support for EAP111
- Added RADIUS NAS ID, see "Wireless Networks — Security Settings" on page 71
- Modified Minimum Signal Allowed default, see "Physical Radio Settings" on page 65

- Added OpenRoaming captive portal, see "OpenRoaming" on page 58
- Added OpenRoaming NAI Realm List Method/Authentication, see "OpenRoaming" on page 58
- Added Syslog Level, see "System Settings" on page 83

September 2023 Revision

This is the 12th revision of this guide. It is valid for software release v12.4.3 and includes the following changes:

- Added support for OAP101
- Added SSID isolation, see "Physical Radio Settings" on page 65
- Multiple PSK enhancement, see "Wireless Networks — Security Settings" on page 71

July 2023 Revision

This is the 11th revision of this guide. It is valid for software release v12.4.1 and includes the following changes:

- Added OpenRoaming, see "OpenRoaming" on page 58 and "Wireless Networks — OpenRoaming" on page 78
- Modified broadcast rate, see "Physical Radio Settings" on page 65
- Access Control List enhancement, see "Wireless Networks — Security Settings" on page 71
- Hostname enhancement, see "System Settings" on page 83
- Moved the language setting to the System page, see "System Settings" on page 83
- Firmware upgrade enhancement, see "Upgrading Firmware" on page 88
- Account username enhancement, see "User Accounts" on page 89

May 2023 Revision

This is the 10th revision of this guide. It is valid for software release v12.4.0 and includes the following changes:

- Added WAN port auto-detection to QR code Onboarding, see "QR Code Onboarding" on page 27
- Added automatic mesh AP configuration, see "Mesh AP Configuration" on page 30

1Doc: Protocolo 1.943/2025 | Anexo: em_3[illegible] 1075/4726

- Removed Mark and Notrack from firewall rules, see “Firewall Rules” on page 51
- Modified Minimum Signal Allowed, see “Physical Radio Settings” on page 65
- Added RF Isolation, see “Physical Radio Settings” on page 65
- Modified Dynamic VLAN, see “Wireless Networks — Network Settings” on page 76
- Modified HotSpot 2.0 settings, see “Wireless Networks — Network Settings” on page 76
- Added Log Level, see “System Settings” on page 83
- Added SNMPv3 User, see “SNMP” on page 94
- Modified Diagnostics and added Speed Test, see “Diagnostics” on page 99

January 2023 Revision

This is the ninth revision of this guide. It is valid for software release v12.3.0 and includes the following changes:

- Updated QR code Onboarding, see “QR Code Onboarding” on page 27
- Updated wireless status, see “Wireless Status” on page 38
- Added support for dynamic PSK, see “Wireless Networks — Security Settings” on page 71
- Updated Hotspot 2.0 settings, see “Wireless Networks — Network Settings” on page 76
- Added CAPWAP Tunnel Interface to Ethernet Settings, see “Ethernet Settings” on page 46

November 2022 Revision

This is the eighth revision of this guide. It is valid for software release v12.2.0 and includes the following changes:

- Added Airtime Fairness, see “Physical Radio Settings” on page 65
- Modified the value range of BSS Coloring, see “Physical Radio Settings” on page 65
- Modified wireless security default, see “Wireless Networks — Security Settings” on page 71
- Added 802.11v, see “Wireless Networks — Security Settings” on page 71

1Doc: Protocolo 1.943/2025 | Anexo: em_3[illegible] 1076/4726

- Added SNMP Trap, see "SNMP" on page 94
- Added BLE Scan, see "BLE" on page 97

November 2022 Revision

This is the seventh revision of this guide. It is valid for software release v12.1.0 and includes the following changes:

- Updated SNMP read/write community settings, see "SNMP" on page 94
- Added BLE radio Tx Power, see "BLE" on page 97
- Added Interference Detection, see "Physical Radio Settings" on page 65
- Added zero-touch provisioning information, see "Zero-Touch Provisioning" on page 20
- Modified the default value for Minimum Signal Allowed, see "Physical Radio Settings" on page 65
- Added 160MHz channel bandwidth option, see "Physical Radio Settings" on page 65
- Removed uCentral cloud option from the Setup Wizard.

July 2022 Revision

This is the sixth revision of this guide. It is valid for software release v12.0.0 and includes the following changes:

- Updated Setup Wizard for uCentral cloud, see "AP Setup Wizard" on page 22
- Added Proxy ARP, see "Wireless Networks — Network Settings" on page 76
- Added Multicast-to-Unicast Conversion, see "Wireless Networks — General Settings" on page 69
- Added Bandsteering, see "Physical Radio Settings" on page 65
- Added WPA3 Enterprise 192-bit and OWE security, see "Wireless Networks — Security Settings" on page 71
- Added multiple PSK keys, see "Wireless Networks — Security Settings" on page 71
- Added Short Guard Interval (SGI), see "Wireless Networks — Advanced Radio Settings" on page 79
- Added Multicast/Broadcast Rate, see "Physical Radio Settings" on page 65
- Added UPnP, see "LAN Settings" on page 49

1Doc: Protocolo 1.943/2025 | Anexo: em_3[illegible] Edital 02/2025 - Anexo VI - 02_AP_025_Part5_062.pdf (1/204) 1076/4726

- Added DHCP Snooping, see "DHCP Snooping" on page 61
- Added ARP Inspection, see "ARP Inspection" on page 62
- Added DHCP Relay, see "DHCP Relay" on page 63
- Added IPv6 for Internet access, see "IPv6 Settings" on page 46
- Added Hotspot 2.0, see "Wireless Networks — Network Settings" on page 76
- Added Device Discovery Tool, see "Device Discovery" on page 100
- Added Discovery Agent settings, see "Edgecore Networks Discovery Tool" on page 91
- Added Reset button and LED enable, see "System Settings" on page 83
- Added PoE Out setting, see "Ethernet Settings" on page 46
- Added caution on firmware upgrades in uCentral mode, see "Upgrading Firmware" on page 88

April 2022 Revision

This is the fifth revision of this guide. It is valid for software release v11.6.0 and includes the following changes:

- Added Client mode, see "Physical Radio Settings" on page 65
- Added Site Survey, see "Wireless Networks — General Settings" on page 69
- Added Custom LAN, see "LAN Settings" on page 49
- Added WME configuration, see "Physical Radio Settings" on page 65
- Added BSS Coloring, see "Physical Radio Settings" on page 65
- Added OFDMA, see "Physical Radio Settings" on page 65
- Added Target Wake Time, see "Physical Radio Settings" on page 65
- Added HTTPS captive portal, see "Captive Portal Settings" on page 56
- Added HTTPS certificate upload, see "Upload Certificate" on page 88

December 2021 Revision

This is the fourth revision of this guide. It is valid for software release v11.4.0 and includes the following changes:

- Updated QR code onboarding, see "QR Code Onboarding" on page 27

1Doc: Protocolo 1.943/2025 | Anexo: em_3[illegible] Processo administrativo 029/2025 | Anexo WiFi 029_2025_Part5_062.pdf (18/200) 3078/4726

- Added mesh traffic graph to the dashboard, see "Traffic Graphs" on page 40
- Added MSP mode, see "System Settings" on page 83

November 2021 Revision

This is the third revision of this guide. It is valid for software release v11.3.1 and includes the following changes:

- Updated the Setup Wizard, see "AP Setup Wizard" on page 22
- Updated the Dashboard, see "Status Information" on page 33
- Added Smart Isolation, see "LAN Settings" on page 49
- Added Hotspot Settings, see "Hotspot Settings" on page 53
- Updated wireless network settings, see "Wireless Networks — Network Settings" on page 76
- Updated wireless open mesh settings, see "Wireless Networks — Open Mesh Settings" on page 78
- Added Telnet settings, see "Telnet" on page 91
- Added web server settings, see "Web Server" on page 91
- Added multicast DNS, see "Multicast DNS" on page 95
- Added firewall settings, see "Firewall Rules" on page 51
- Added a guest network, see "LAN Settings" on page 49

July 2021 Revision

This is the second revision of this guide. It is valid for software release v11.2.0 and includes the following changes:

- Added WPA3-Personal transition, WPA3-Enterprise, and WPA3-Enterprise transition. See "Wireless Networks — Security Settings" on page 71
- Support for IEEE 802.11 k/r, see "Wireless Networks — Security Settings" on page 71
- Added Minimum signal allowed (RSSI Threshold), see "Physical Radio Settings" on page 65
- Support for Open Mesh, see "Wireless Networks — Open Mesh Settings" on page 78
- SNMP v2 support, see "SNMP" on page 94

1Doc: Protocolo 1.943/2025 | Anexo: em_3[illegible] Folha nº 1039/4746

- Support for remote Syslog, see "Remote System Log Setup" on page 92
- Support for LLDP, see "LLDP" on page 96
- Support for management by an EWS-Series Controller, see "System Settings" on page 83

April 2021 Revision

This is the first revision of this guide. It is valid for software release v11.1.1.

1Doc: Protocolo 1.943/2025 | Anexo: em_8967D8805AD5821B6628907... Laboratório... 029/2025... Wi-Fi_6_AP_2205_B15_0624.pdf (110/200) 1079/4726

Contents

1Doc: Protocolo 1.943/2025 | Anexo: em_8967D8805AD2E821B6628F0E_pt-br_Laticínios_029_2025_Assistência_Técnica_WiFi_6_AP_2025_Rede_0624.pdf (114/204) 1090/4726

1Doc: Protocolo 1.943/2025 | Anexo: em_8967D8805AD5821B6628B9CE_Manual_Administrador_pdf_Anexo_WI_629_2025_Baixe_634.pdf (113 of 200) 1092/4746

1Doc: Protocolo 1.943/2025 | Anexo: em_8967D8805AD5B21B6628F0E_pt-br_Laticínios_Aparecida_de_Goiânia_GO_2025_Anexo_WiFi_6_AP2105_B15_0624.pdf (116/200) 1092/4746

Figures

1Doc: Protocolo 1.943/2025 | Anexo: em_8967D8805AD5821B6628907E9501_Manual_Administrador_Access_Point_WiFi_6_AP2025_B15_0624.pdf (114/200) 1093/4746

1Doc: Protocolo 1.943/2025 | Anexo: em_8967D8805AD2B321B6628B9CE_pt-BR_Laticínios 029/2025 - Anexo WiFi 6 AP 205_B15_0624.pdf (118/200) 3095/4726

Figures

1Doc: Protocolo 1.943/2025 | Anexo: em_8967:D8059D2E5321B6628F9CEsso_Laticínios_029/2025_Anexo_WiFi_6_AP_2025_Rev1_634.pdf (16/200) 1096/4726

Tables

1Doc: Protocolo 1.943/2025 | Anexo: em_8967D8805902E5321B6628907E5A0F0C_Laudo_Laboratorial_029_2025_Anexo_WF_629_2025_Baixo_Peso_Nascimento_Prematuridade_Gestacional_Laboratorio_Tabelas_Graficos_Anexos_Tecnicos_Apendices_Glossario_Referencias_Bibliografia_Indice_Remissivo_Sumario_Lista_Figuras_Lista_Tabelas_Lista_Abreviaturas_Lista_Siglas_Lista_Simbolos_Lista_Unidades_Lista_Medidas_Lista_Pesos_Lista_Volumes_Lista_Capacidades_Lista_Dimensoes_Lista_Areas_Lista_Perimetros_Lista_Volumes_Lista_Capacidades_Lista_Dimensoes_Lista_Areas_Lista_Perimetros.pdf (p. 17 of 200) 1096/4746

Section I

Getting Started

This section provides an overview of the access point, and introduces some basic concepts about wireless networking. It also describes the basic settings required to access the management interface.

This section includes these chapters:

1Doc: Protocolo 1.943/2025 | Anexo: em_8967D8805AD2E321B6628F9CE_pt-br_Laticínios_029_2025_Assessoria_Técnica_WiFi_6_AP_205_Base_624.pdf (18 of 20) 1098/4746

1 Introduction

The access point (AP) runs software that includes a network management agent. The agent offers a variety of management options, including a web-based interface. The AP can also be accessed through Secure Shell (SSH) for configuration using a command line interface (CLI).

Note: This manual describes the configuration interface for stand-alone mode. Refer to the Edgecore *ecCLOUD Controller User Manual* for information on configuring the AP through the cloud interface.

This chapter includes the following sections:

1Doc: Protocolo 1.943/2025 | Anexo: em_8967_Manual_Administrador_Access_Point_Edgecore_EAP102_EAP2025_Rev1_624.pdf (129/200) 1099/4746

Configuration Options

The access point's web agent allows you to configure AP parameters, monitor wireless connections, and display statistics using a standard web browser. The AP's web management interface can be accessed from any computer attached to the network.

The CLI program can be accessed remotely by a Secure Shell (SSH) connection over the network. The CLI is used primarily for technical support.

The AP's web interface allows you to perform management functions such as:

- Set management access user names and passwords
- Configure IP settings
- Configure 2.4 GHz and 5 GHz radio settings
- Configure HaLow radio settings (EAP112 only)
- Control access through wireless security settings
- Filter packets using Access Control Lists (ACLs)
- Download system firmware
- Download or upload configuration files
- Display system information

Zero-Touch Provisioning

APs can be automatically managed by the Edgecore ecCLOUD controller or an EWS-Series controller. If an AP is already registered with the ecCLOUD controller, it will be automatically managed when the WAN port of the AP is connected to the Internet.

When an AP is connected to a local LAN with an EWS-Series controller, the AP can be configured with the controller IP address through DHCP Option 138 and then automatically managed by the controller.

As an alternative to zero-touch provisioning, you can manually set the preferred management method from the web interface, see "System Settings" on page 83.

1Doc: Protocolo 1.943/2025 | Anexo: em_8967:D8059D2E321B6628907:esso_Laranjeiras_029/2025_Anexo_WiFi_6_EAP225_Brochure_pdf (120/200) 3100/4746

Connecting to the Web Interface

For first-time access to the AP's web management interface, you can connect a PC directly to one of the AP's LAN ports or use the quick-setup QR code (printed on a label next to the AP's ports). The first-time you access the web interface, it automatically runs the Setup Wizard for initial AP configuration.

For information on the Setup Wizard, see "AP Setup Wizard" on page 22.

For information on using the QR code, see "QR Code Onboarding" on page 27.

LAN Port Connection

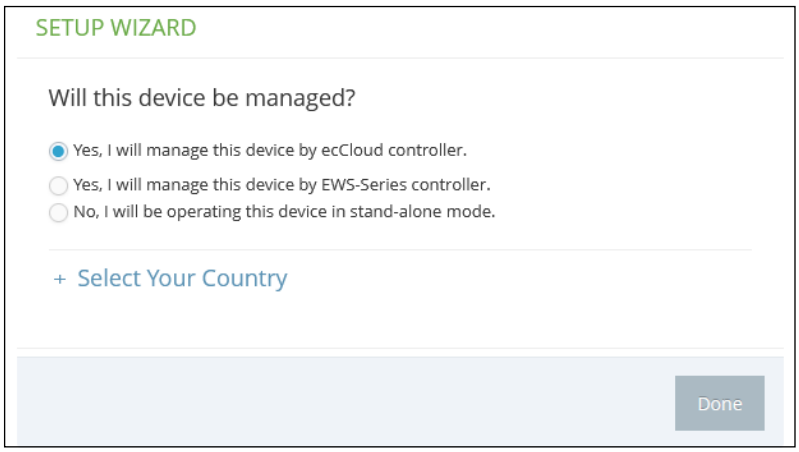
When connecting to the web management interface through one of the AP's LAN ports, the AP has a default management IP address of 192.168.2.1 and a subnet mask of 255.255.255.0. Therefore, you must set your PC IP address to be on the same subnet as the AP (that is, the PC and AP addresses must both start with192.168.2.x).

Note: To connect to the web interface using the Uplink(PoE) port, the IP address is automatically assigned through DHCP by default. If a DHCP server is unreachable, the Uplink(PoE) port reverts to a fallback IP address of 192.168.1.10.

To access the AP's web management interface, use your web browser to connect to the management interface by entering the default IP address of 192.168.2.1.

For first-time access, there is no user login and the Setup Wizard starts automatically. Follow the steps described in "AP Setup Wizard" on page 22.

Figure 1: Web Management Login



Note: To configure the AP with a different management IP address that is compatible with your network, see "LAN Settings" on page 49.

1Doc: Protocolo 1.943/2025 | Anexo: em_8407_DBS_Administration_Guide_v1.0_Portuguese_Latam_03_2025_Anexo_WiFi_6_AP_205_Brazil_624.pdf (124/200) 3390/4746

AP Setup Wizard

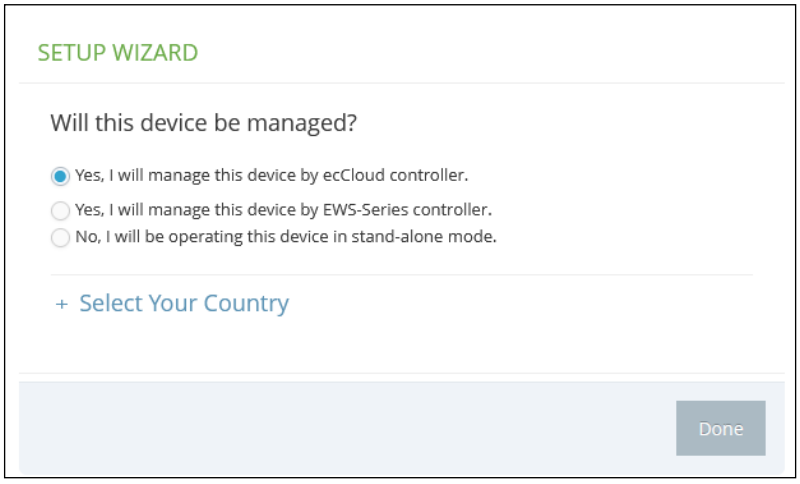
The Setup Wizard is designed to help you configure the basic settings required to get the AP up and running.

Step 1 Select How the AP will be Managed — To manage the AP using the Edgecore ecCLOUD controller, select "Yes, I will manage this device by ecCloud controller," and then continue to Step 6.

To manage the AP using the an Edgecore EWS-series controller, select "Yes, I will manage this device by EWS-Series controller," and then continue to Step 2.

Otherwise, select "No, I will be operating this device in stand-alone mode" and continue to Step 3.

Figure 2: Select ecCloud, EWS Controller, or Stand-Alone



If you select to manage the AP using the Edgecore ecCLOUD controller, go to cloud.ignitenet.com to register your AP. Log in and select Devices from the menu. Click Add Device and enter the AP serial number and MAC address to register the AP with your cloud network. The serial number and MAC address can be found on the product packaging or label.

Note: This manual describes the configuration interface for stand-alone mode. Refer to the Edgecore *ecCLOUD Controller User Manual* for information on configuring the AP through the cloud interface or the *EWS-Series Controller User Manual* for information on managing the AP through an EWS controller.

1Doc: Protocolo 1.943/2025 | Anexo: em_8967D8805AD5821B6628907... Laranjeiras 029/2025 ... 1392/4746

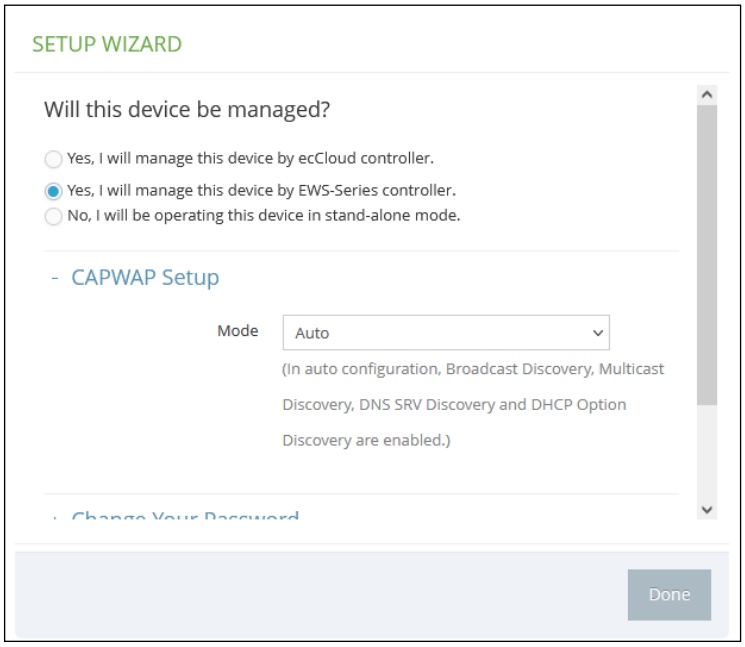
Step 2 CAPWAP Setup — When EWS-Series Controller management is selected, you can set the mode for discovering the controller. Once the AP has discovered the controller on the network it can then send a CAPWAP (Control And Provisioning of Wireless Access Points) join request.

In Auto mode, the AP uses four methods to discover the controller. These methods require no further configuration.

In manual mode, two options are available. Specify the Domain Name Suffix so that the AP can use DNS server records to discover the EWS controller. Or, just specify a static IP address for the controller.

For more information on CAPWAP setup, see "System Settings" on page 83.

Figure 3: CAPWAP Setup



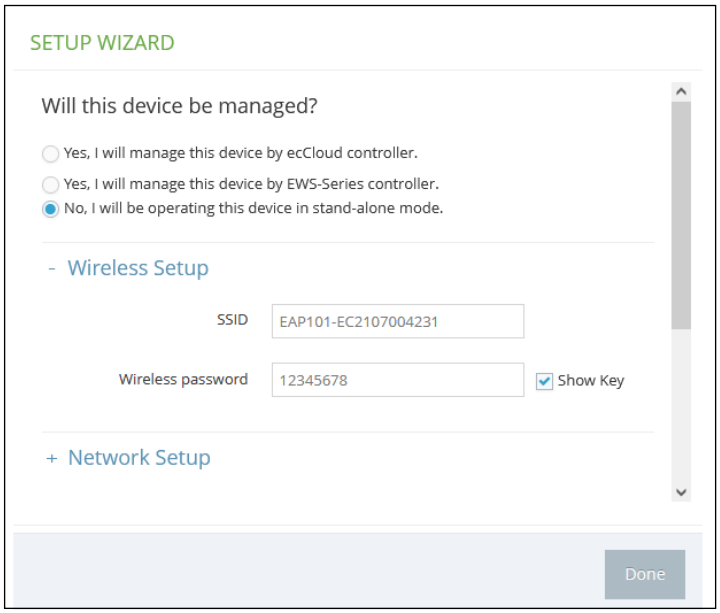
After completing the CAPWAP setup, continue with Step 5.

Step 3 Wireless Setup — If you select to manage the AP in stand-alone mode, you can configure the default wireless network.

The default wireless network name (SSID) consists of the AP model and its serial number, and there is a default wireless password. You have the option to modify the wireless network name and password to your preferred configuration. The wireless name must be 1-32 ASCII characters, and the password must be 8 to 63 ASCII characters (no special characters are allowed).

1Doc: Protocolo 1.943/2025 | Anexo: em_8967D8805D2E821B6628F9CE_Manual_Administrador_Processo_Aquisitivo_6_24_2025_Rafe_0624.pdf (126/200) 1392/4746

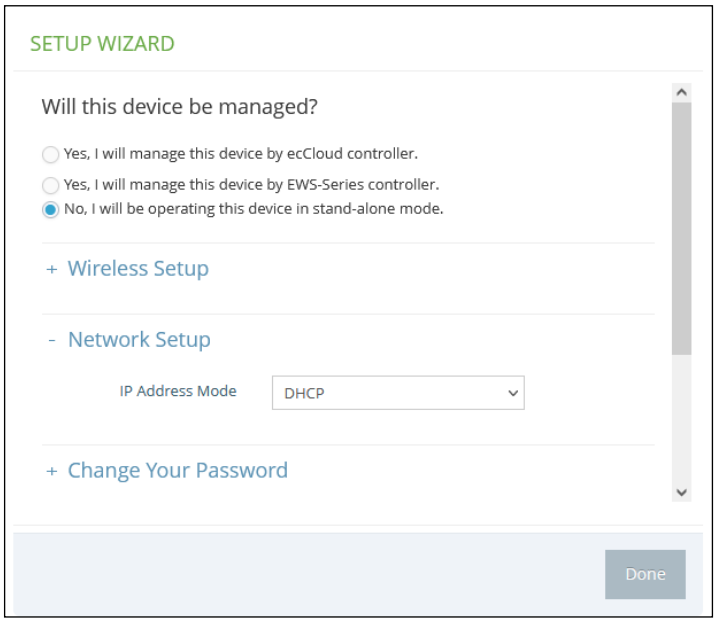
Figure 4: Wireless Setup



Step 4 Network Setup — For AP stand-alone mode, you also have the option to configure the IP address mode used to provide an IP address for the Internet access port.

The default IP Address Mode is DHCP and other options include Static IP and PPPoE. For more information, see "Internet Settings" on page 43.

Figure 5: Network Setup



1Doc: Protocolo 1.943/2025 | Anexo: em_8967DB805AD5821B6628B0E_pt_Laranjeiras_Administrativo_029_2025_Aquisicao_Wifi_6_AP_2025_Rafe_0624.pdf (124 of 200) 3394/4746

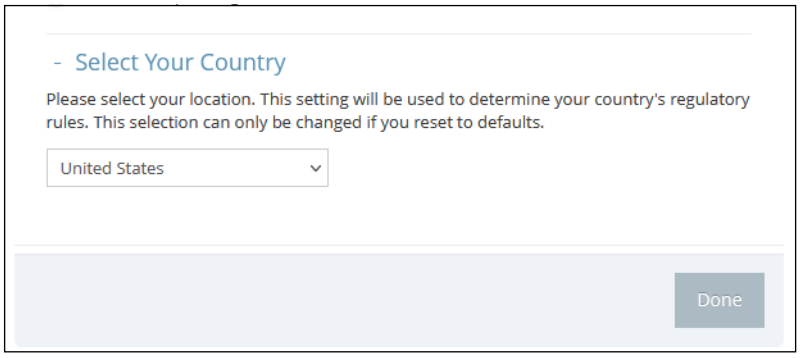
Step 5 Change Your Password — Set a new password for management access to the AP (the default user name is "admin" with password "admin"). The password must be 6-20 ASCII characters (case sensitive with no special characters).

Figure 6: Change Password

Note: For information on changing user names and passwords, see "User Accounts" on page 89.

Step 6 Select Your Country — Select the access point's country of operation from the drop-down menu. You must set the AP's country code to be sure that the radios operate according to permitted local regulations. That is, setting the country code restricts operation of the AP to the radio channels and transmit power levels permitted for wireless networks in the specified country.

Figure 7: Select Country



Caution: You must set the country code to the country of operation. Setting the country code ensures that the radios operate within the local regulations specified for wireless networks.

1Doc: Protocolo 1.943/2025 | Anexo: em_8[illegible] 1395/4726

Note: The country code selection is for non-US models only and is not available to any US models. Per FCC regulation, all Wi-Fi products marketed in the US must be fixed to US operation channels only.

Step 7 After completing the Setup Wizard, click "Done."

1Doc: Protocolo 1.943/2025 | Anexo: em_8967D8805902E5321B6628906_Gestor_Laranjeiras_029_2025_Aquisicao_WiFi_6_AP_2105_Rede_1324.pdf (126/150) 1396/4746

QR Code Onboarding

For quick set up and registration of your AP with the ecCLOUD controller, you can scan the QR code on the AP using a phone.

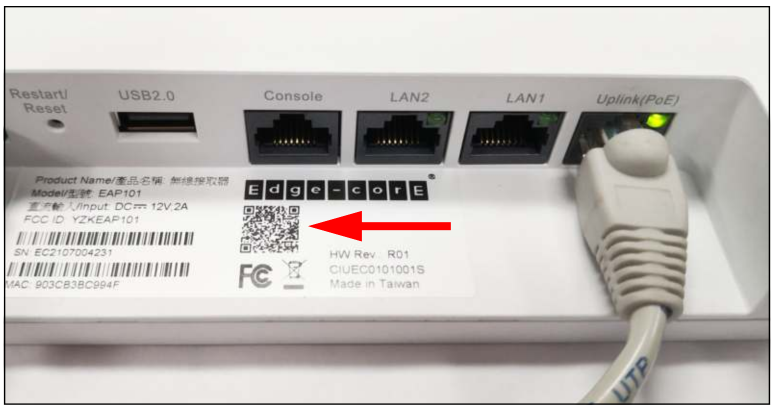
Follow these steps:

1. Power on the AP.

2. Connect the AP to the Internet. Connect your network or Internet access device to the AP’s RJ-45 Uplink port.

3. Use the camera or a barcode app on your phone to scan the AP’s QR code. The QR code is printed on a label next to the AP’s ports.

Figure 8: Scanning the AP QR Code



4. When a message pops up, tap “yes” to join the Wi-Fi network. (iPhone requires you to go to Settings > Wi-Fi or open the browser for the message to pop up.)

The web browser should open and redirect to the Setup Wizard page.

Note: If the phone cannot connect to the Wi-Fi network, type the SSID (network name) and password manually. The SSID name is the AP serial number (for example, EC0123456789), and the password is the AP MAC address (for example, 903CB3BC1234).

5. Wait for the auto-detection of the WAN port configuration (DHCP, Static IP, or PPPoE).

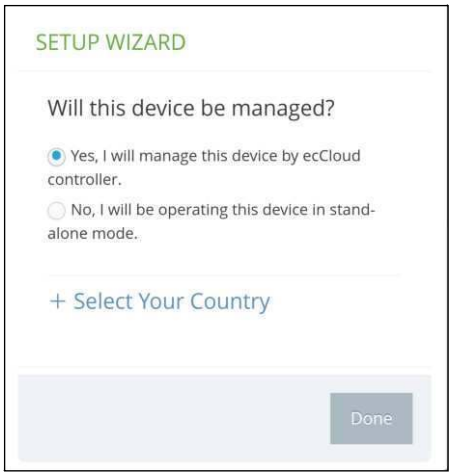
When DHCP is detected, the AP automatically continues with the Setup Wizard.

1Doc: Protocolo 1.943/2025 | Anexo: em_ [overlapping text illegible] (130/250) 3397/4721

Figure 9: Setup Wizard - Detect Network

6. Select to manage the AP using the ecCLOUD controller or to manage the AP in stand-alone mode.

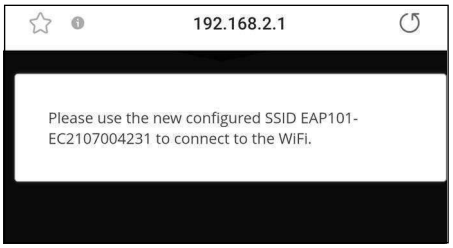
Figure 10: Setup Wizard - Device Management



a. Stand-Alone Mode: Use the default wireless network setting or customize the network name and password. Change the login password and set the country of operation. Tap "Done" to finish the setup wizard.

Wait about two minutes for the AP configuration to update, and then connect to the wireless network name configured in the Setup Wizard.

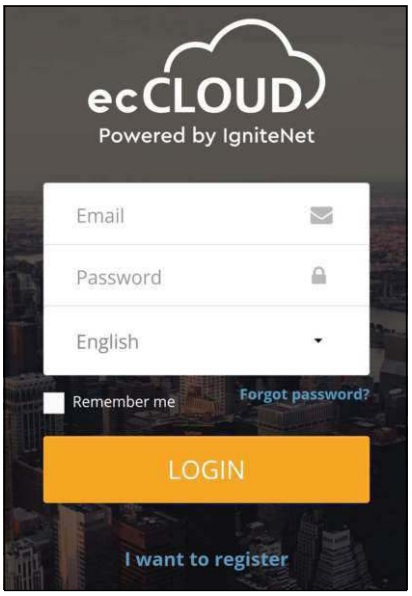
Figure 11: Connect to New SSID



b. Cloud-Managed Mode: Set the country of operation and then tap "Done" to finish the Setup Wizard. The browser is redirected to the ecCLOUD login page.

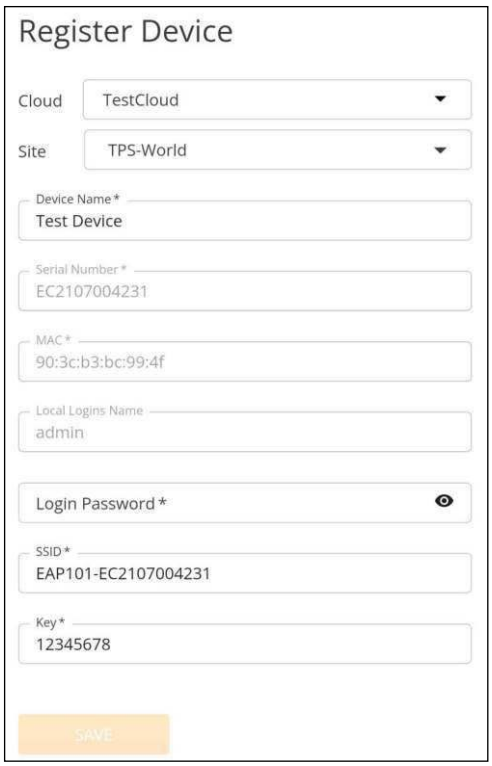
1Doc: Protocolo 1.943/2025 | Anexo: em_8967DB805AD2E321B6628B0E_pdf_Laticínio 029_2025_Anexo_WiFi_6_EAP225_Brie_624.pdf (28/28) 1397/4726

Figure 12: ecCLOUD Login Page



If you already have an ecCLOUD account, log in and select a site for the AP. The AP is automatically registered for cloud management. Modify the device name, login password, SSID, and security key. After you tap "Save," wait about five minutes for the cloud controller to configure the AP.

Figure 13: ecCLOUD Device Registration



If you do not have an ecCLOUD account, tap "I want to register" and set up an account. Create a cloud and site before confirming the regulatory

1Doc: Protocolo 1.943/2025 | Anexo: em_8967D8805AD5321B6628F0E_pt-BR_Laboratório_Processo_Aquisição_Wi-Fi_6_AP_105_Lote_0624.pdf (129/200) 3109/4746

country. After tapping “Next,” the AP is then automatically registered for cloud management.

After you tap “Save,” wait about five minutes for the cloud controller to configure the AP.

Note: Refer to the Edgecore *ecCLOUD Controller User Manual* for more information on setting up and configuring APs through ecCLOUD.

Mesh AP Configuration

The first AP can be managed either through ecCLOUD or in stand-alone mode. If a second AP needs to establish a mesh connection with the first AP, follow these steps:

1. Connect the LAN port of the first AP (Mesh Portal Point) to the LAN port of the second AP (Mesh Access Point), which then allows the second AP to synchronize its configuration with the first AP.

2. After unplugging the LAN port, the mesh connection will be established automatically.

Main Menu

The web interface Main Menu provides access to all the configuration settings available for the AP.

To configure settings, click the relevant Main Menu item. Each Main Menu item is summarized below with links to the relevant section in this guide where the configuration parameters are described in detail:

- **Dashboard** — The dashboard shows basic settings for the AP, including general status, local network settings, and wireless radio status. See “Status Information” on page 33.

- **Network** — Configures Internet, Ethernet, and LAN settings. See “Network Settings” on page 42.

- **Wireless** — Configures 2.4 GHz Radio, 5 GHz Radio, HaLow and VLAN settings. See “Wireless Settings” on page 64

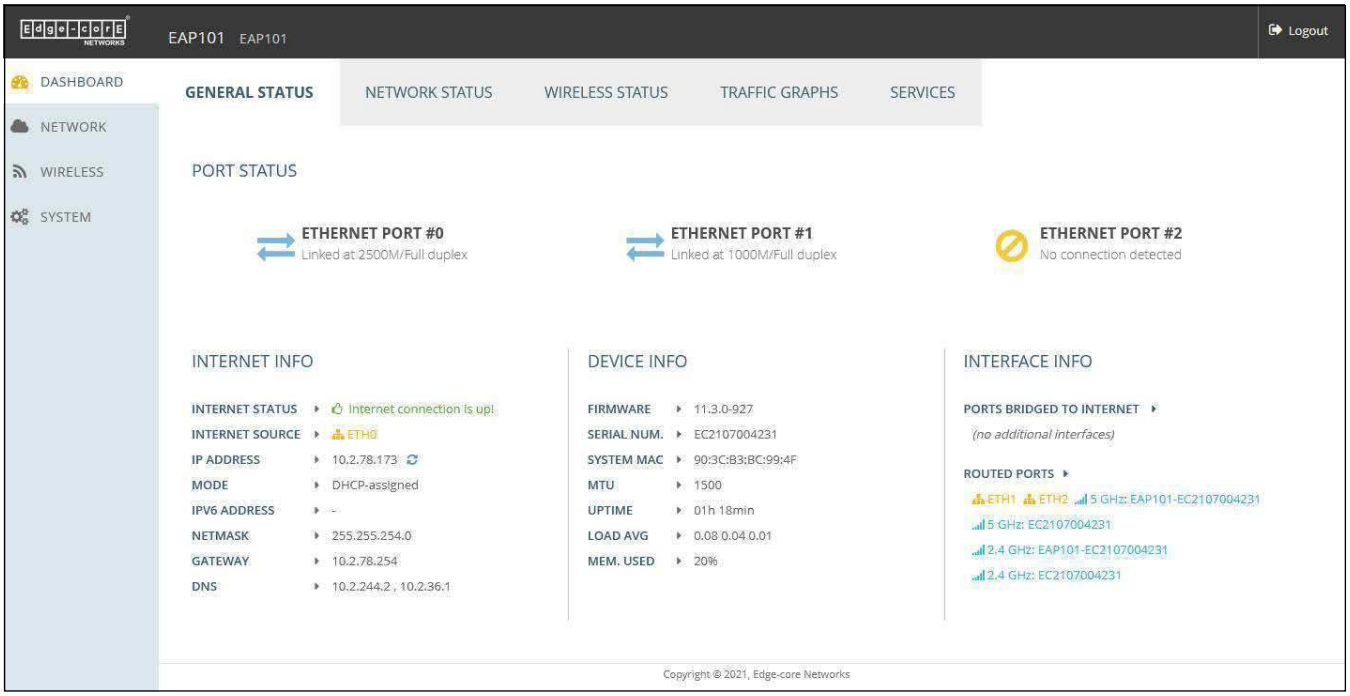
- **System** — Configures System (including cloud agent and various system settings), Maintenance (such as view log, reboot, reset defaults, backup defaults, restore defaults, and firmware upgrade), User Accounts, Services (network time), and Diagnostics (including ping, traceroute).

1Doc: Protocolo 1.943/2025 | Anexo: em_8967D8805AD5821B6628907... Laticínio 029/2025 ... 1190/4726

Dashboard

After logging in to the web interface, the dashboard displays. The dashboard shows basic settings for the AP, including Internet status, local network settings, and wireless radio status.

Figure 14: The Dashboard



Common Web Page Buttons

The list below describes the common buttons found on many of the web management pages:

- **Save** – Applies the new parameters and saves them to temporary RAM memory. Also displays a message at the top of the screen to inform you that the changes have not yet been saved to Flash memory. The running configuration will not be saved upon a reboot unless you click the "Save & Apply" button.

Figure 15: Saving Configuration Changes

- **Save & Apply** – Saves the changes made on a page and then applies them so that the configuration is retained after a restart.
- **Revert** – Cancels newly entered settings and restores the originals.
- **Logout** – Ends the web management session.

1Doc: Protocolo 1.943/2025 | Anexo: em_8407_D8059_D8532_B6628_Test_Laboratório_2025_Assessoria_WiFi_6_AP2025_Rede_624.pdf (134/200) 3400/4726

Section II

Web Configuration

This section provides details on configuring the access point using the web browser interface.

This section includes these chapters:

1Doc: Protocolo 1.943/2025 | Anexo: em_8907D8805AD5E321B6628F9CE_Manual_Administrador_Web_WiFi_6_AP_1205_Base_624.pdf (138/200) 3402/4746

2 Status Information

The Dashboard displays information on the current system configuration, including Internet status, local network settings, wireless radio status, traffic graphs, and services.

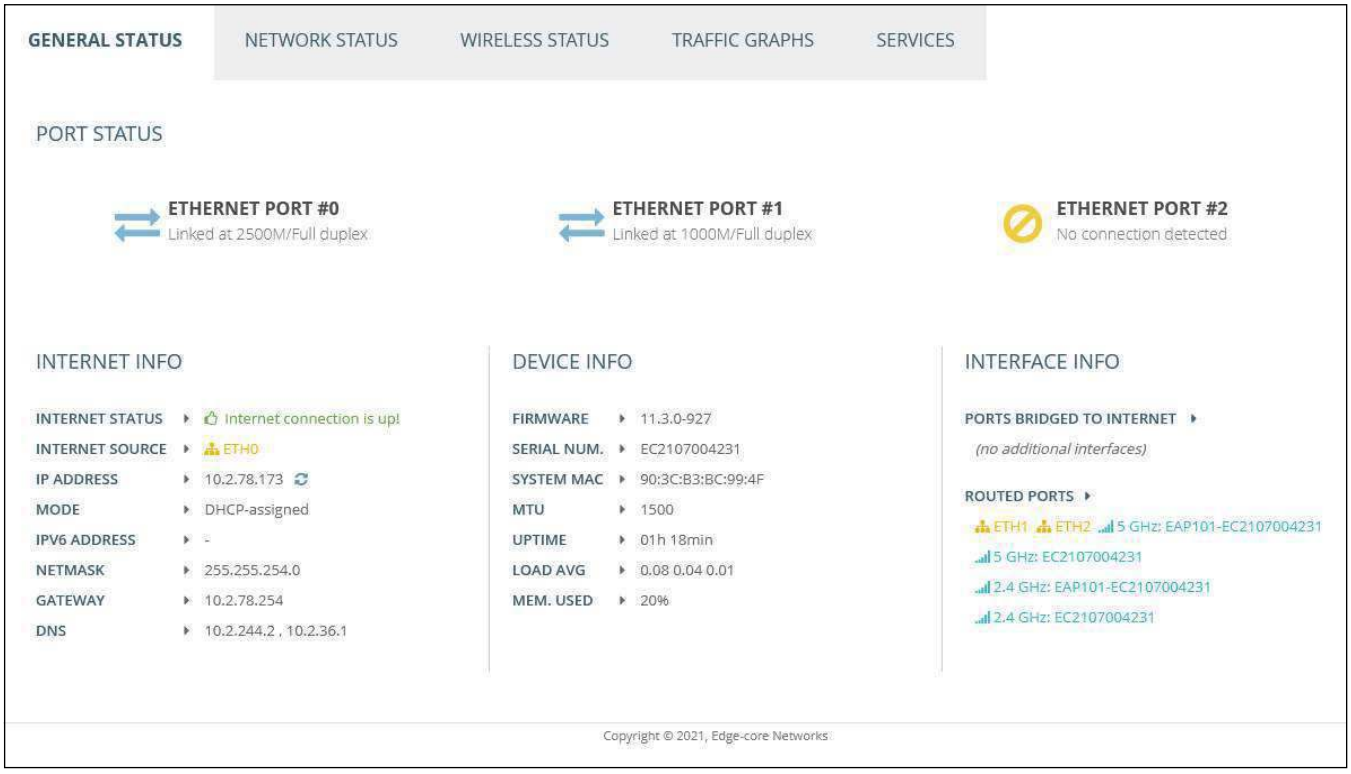
This chapter includes the following sections:

1Doc: Protocolo 1.943/2025 | Anexo: em_8967D8805AD5821B6028907E_Laudo_Laboratorial_029_2025_Anexo_WiFi_6_AP_2105_B15_0624.pdf (136/150) 3402/4746

General Status

The General Status section shows descriptive information about the AP.

Figure 16: General Status Information



The following items are displayed in the “Port Status” section:

- **Ethernet Port #0** — Shows the status of the WAN Ethernet port, including link-up state, speed, and duplex mode.
- **Ethernet Port #1** — Shows the status of the LAN Ethernet port 1, including link-up state, speed, and duplex mode.
- **Ethernet Port #2** — Shows the status of the LAN Ethernet port 2, including link-up state, speed, and duplex mode.
- **3G/LTE** — Shows the status of the 3G/LTE connection (EAP112 only).

The following items are displayed in the “Internet Info” section:

- **Internet Status** — Shows whether or not the Internet connection is up.
- **Internet Source** — The Ethernet port connected to the Internet. By default, this is Ethernet Port 0.

1Doc: Protocolo 1.943/2025 | Anexo: em_8967DB805AD5821B6628F6E_pt_Laranjeiras_do_029_2025_Anexo_WiFi_6_EAP225_Rev_1.5_624.pdf (134 of 200) 3403/4726

- **IP Address** — IP address of the Internet connection.
- **Mode** — Shows if the IP address is a static setting or set by DHCP.
- **IPv6 Address** — The IPv6 address of the Internet connection.
- **Netmask** — The subnet mask of the IP address.
- **Gateway** — The IP address of the gateway router that is used when a destination address is not on the local subnet.
- **DNS** — The IP address of the Domain Name Server on the network. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses.

The following items are displayed in the "Device Info" section:

- **Firmware** — The software version number.
- **Serial Number** — The serial number of the physical access point.
- **System MAC** — The system MAC address of the access point.
- **MTU** — The maximum transmission unit for packets sent on the network.
- **Uptime** — Length of time the management agent has been up.
- **Load Average** — The last 1-minute, 5-minute and 15-minute CPU load average.
- **Memory Used** — The percentage of memory being used.

The following items are displayed in the "Interface Info" section:

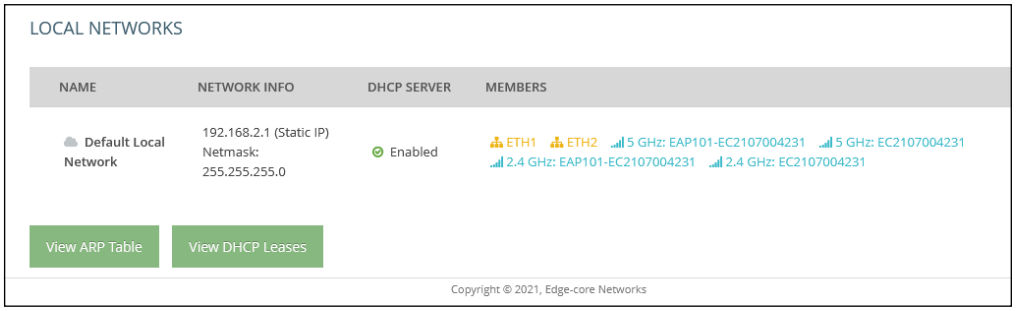
- **Ports Bridged to Internet** — Additional interfaces attached directly to the Internet. Lists interfaces attached to the WAN (that is, the Internet).
- **Routed Ports** — By default, all interfaces are configured as a member of the LAN. Traffic from these interfaces is routed across the access point through Ethernet Port 0 to the Internet. (This is also called route to Internet.)

1Doc: Protocolo 1.943/2025 | Anexo: em_8967D8805AD5321B6628907... Laticínios 029/2025 ... Anexo WI6_29_P_025_Rev_0624.pdf (138/200) 3405/4726

Network Status

The Network Status section shows information about local network connections.

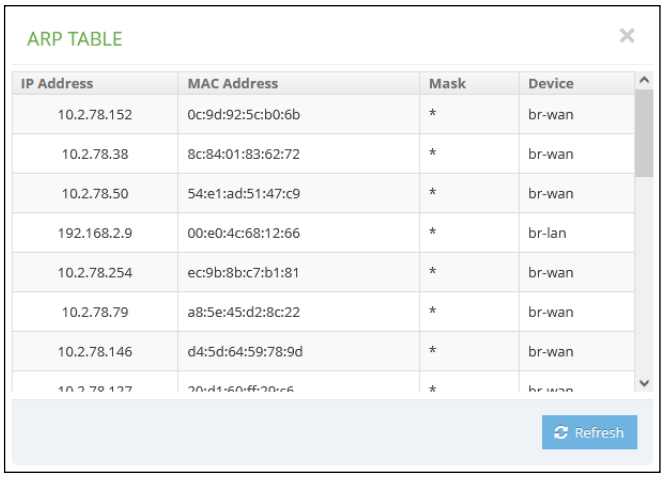
Figure 17: Local Networks



The following items are displayed in this section:

- **Name** — Shows information on the name of the local network.
- **Network Info** — Shows whether the local network uses static or dynamic configuration, and the network mask.
- **DHCP Server** — Shows if DHCP service is enabled on this network.
- **Members** — Shows the ports and wireless radios attached to this network. (Click on any of these interfaces to open the corresponding configuration page.)
- **View ARP Table** — Shows the ARP cache.

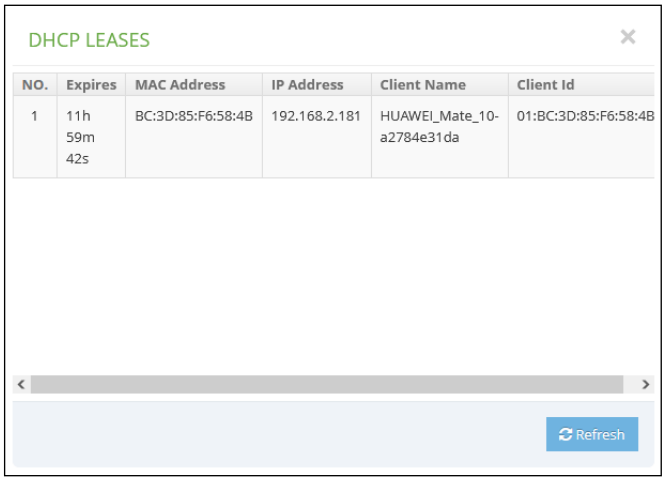
Figure 18: ARP Table



1Doc: Protocolo 1.943/2025 | Anexo: em_8967_Edge-Corp_Manual_Administrador_2025_Assistente_Web_EAP2025_Rev1_634.pdf (136/200) 3406/4726

- **View DHCP Leases** — Shows DHCP leases.

Figure 19: Active DHCP Leases

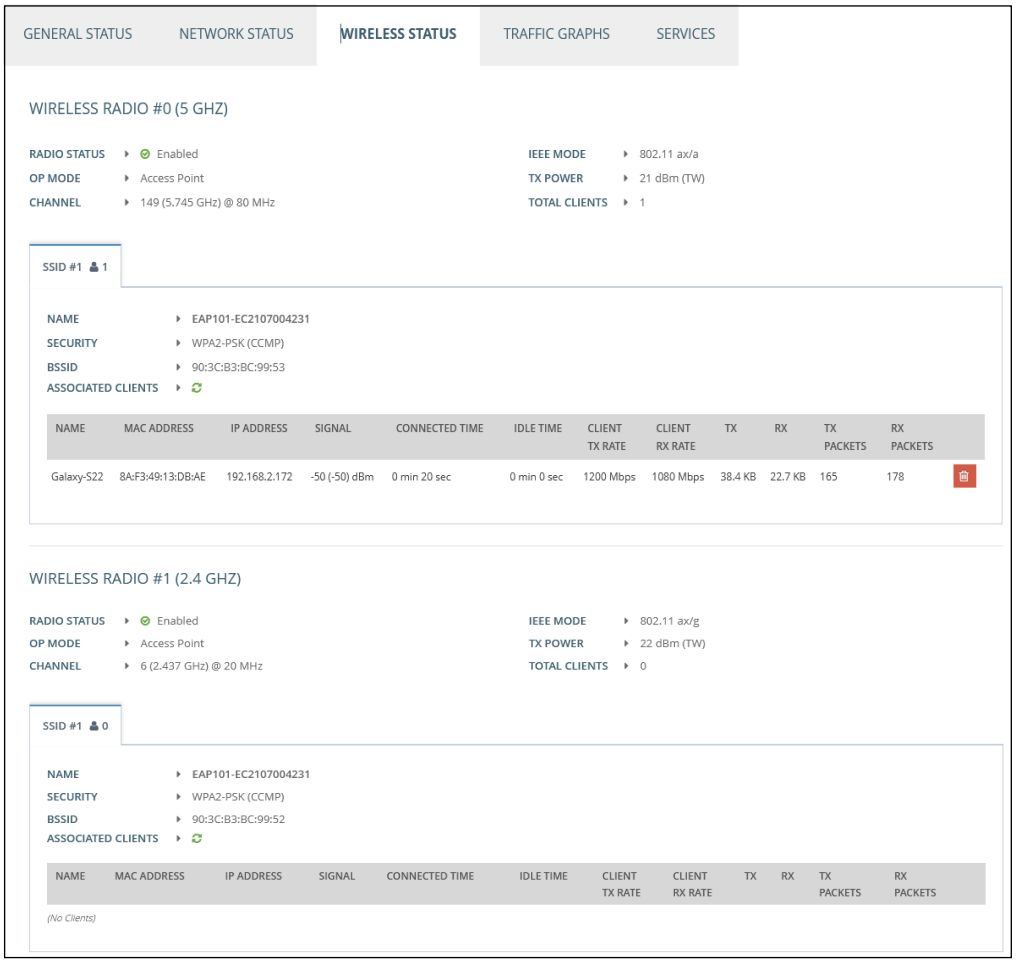


1Doc: Protocolo 1.943/2025 | Anexo: em_8967D8805AD2E82184668B9CE5D1_pdf (1).pdf (1/1) 3406/4726

Wireless Status

The Wireless Status section shows information about the radio settings and associated clients.

Figure 20: Wireless Status



Note that you can click the red button next to an associated client to force disconnection.

The following items are displayed in this section:

- **Wireless Radio 5 GHz/2.4 GHz/HaLow** — Indicates the 2.4 GHz, 5 GHz, and HaLow (EAP112) wireless interface.
  - **Radio Status** — Shows if the wireless interface is enabled or disabled.
  - **IEEE Mode** — The 802.11 wireless LAN standards supported by the AP.
  - **Op Mode** — Shows if the wireless interface is configured to operate in an access point mode or client mode.

1Doc: Protocolo 1.943/2025 | Anexo: em_8967DB805AD2E821B6628B0E_pt-br_Laranjeiras_2025_processo_Aviator_WiFi_6_EAP_105_Rate_624.pdf (38 de 204) 3403/4726

- **Tx Power** — The power of the radio signals transmitted from the AP.
- **Channel** — The radio channel the access point uses to communicate with wireless clients. The available channels depend on the 802.11 Mode, Channel Bandwidth, and Country Code settings.
- **Total Clients** — The total number of clients attached to this interface.

- **SSID #** — Service set identifier. Clients that want to connect to the wireless network through an access point must set their SSIDs to the same as that of the access point.
  - **Name** — A unique identifier for the local wireless network.
  - **Security** — Shows whether or not security has been enabled.
  - **BSSID** — The basic service set identifier. This is the MAC address of the AP generated by combining the 24 bit Organization Unique Identifier (OUI, the manufacturer's identity) and the manufacturer's assigned 24-bit identifier for the radio chipset in the AP.
  - **Associated Clients** — Shows detailed information about associated wireless clients.
    - **Name** — Client name.
    - **MAC Address** — The MAC address of the wireless client.
    - **IP Address** — The IP address assigned to the wireless client.
    - **Signal** — The signal strength (TX/RX) in dBm.
    - **Connected Time** — The time the wireless client has been associated.
    - **Idle Time** — The time the wireless client has been inactive.
    - **Client TX Rate** — The data transmit rate to the wireless client.
    - **Client RX Rate** — The data receive rate from the wireless client.
    - **TX** — The number of bytes transmitted to the wireless client.
    - **RX** — The number of bytes received from the wireless client.
    - **TX Packets** — The number of packets transmitted to the wireless client.
    - **RX Packets** — The number of packets received from the wireless client.

1Doc: Protocolo 1.943/2025 | Anexo: em_8967D8805AD2E321B6628B9CE_Manual_Administrador_Processo_Anexo_WI_629_2025_Rev1_pdf (39/204) 3409/4726

Traffic Graphs

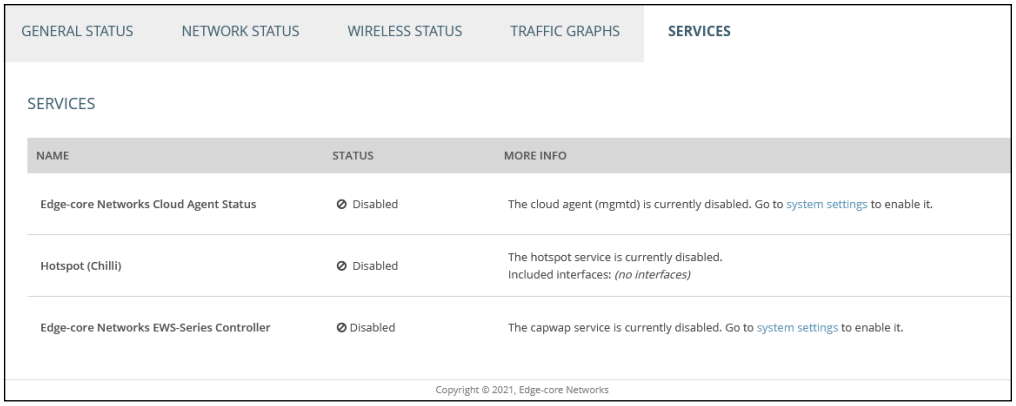
The Traffic Graphs section shows the data rate for the Ethernet ports, wireless interfaces, and mesh interface.

Figure 21: Traffic Graphs

Services

The Services section shows the status of the Edgecore cloud management agent.

Figure 22: Services



- **Edge-core Networks Cloud Agent Status** — Shows whether or not the agent for the cloud controller is enabled.

1Doc: Protocolo 1.943/2025 | Anexo: em_8967DB805AD2E821B6628B0E_pt-BR_Laticínios_029_2025_Assistência_Técnica_Wi-Fi_6_AP_025_Rede_624.pdf (140/200) 3429/4746

- **Hotspot (Chilli)** — Shows whether or not hotspot services are enabled. Click on this field to open the Hotspot Settings menu.

- **Edge-core Networks EWS-Series Controller** — Shows if the CAPWAP service is enabled for management of the AP through an EWS-Series controller.

1Doc: Protocolo 1.943/2025 | Anexo: em_8967D8805928E5821B6628907C5501_Laticínios_Processo_Administrativo_029_2025_Anexo_WiFi_6_AP_2025_Rate_0624.pdf (144/200) 3420/4726

3 Network Settings

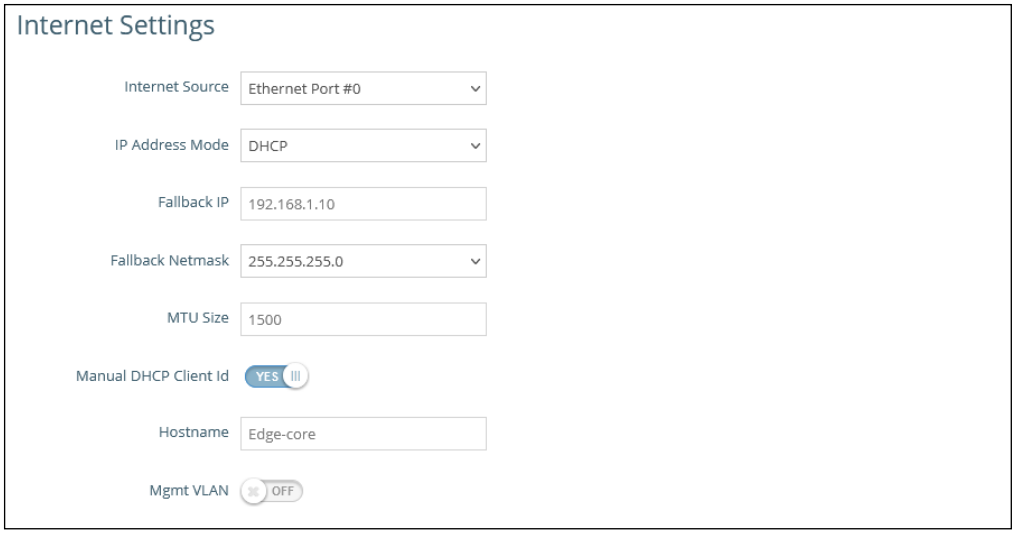
This chapter describes basic network settings on the access point. It includes the following sections:

1Doc: Protocolo 1.943/2025 | Anexo: em_8967_D80594D2E82184668B9CE_pt_Laticínios_Aleixo_WiFi_6_AP205_Base_Unit_pdf (142/200) 3422/4746

Internet Settings

The Internet Settings page configures the basic Internet settings for the AP, such as the source port, IP aliases, as well as the host name and maximum MTU size.

Figure 23: Internet Settings



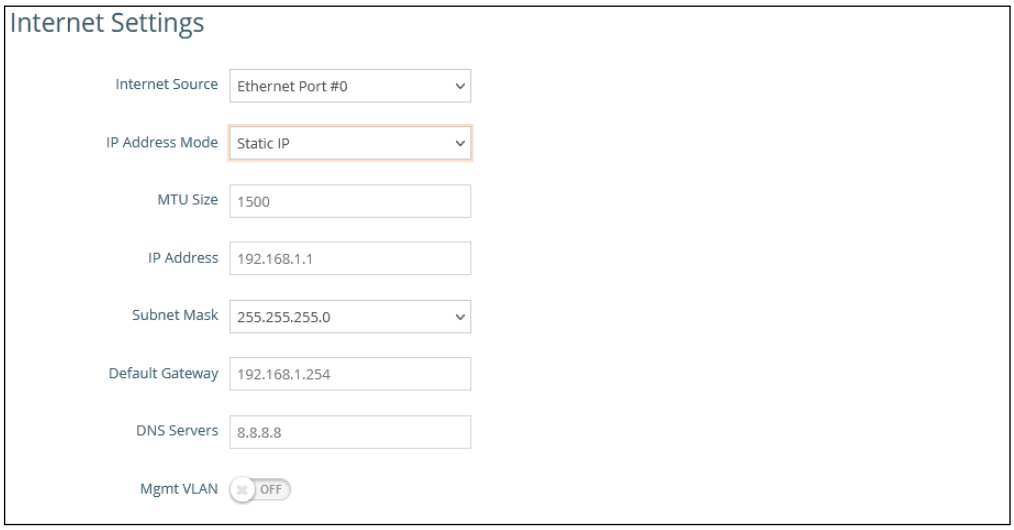
The following items are displayed on this page:

- **Internet Source** — The interface used to access the Internet.
  - **3G/LTE** — Selects the LTE interface as the Internet source. (EAP112 only.)
    - **Modem Device** — Selects the 3G/LTE modem device connected to the system.
    - **APN** — The Access Point Name (APN) used to identify this device when connected to an LTE network.
    - **PIN** — The personal identification number (PIN) of the SIM card installed in the device. The PIN authenticates use of the SIM card for access to an LTE network.
    - **Username** — The name used for LTE access.
    - **Password** — The password used for LTE access.
- **IP Address Mode** — The method used to provide an IP address for the Internet access port. (Default: DHCP; Options: DHCP, Static IP, PPPoE)
  - **DHCP** — Configuration options displayed for DHCP are shown in Figure 23.

1Doc: Protocolo 1.943/2025 | Anexo: em_8967_Edge-Corp_EAP102_EAP105_Basic_Configuration_Guide_v1.0.0.4.pdf (146/200) 1422/4726

- **Fallback IP** — This IP address is used if the DHCP service is unavailable or fails. (Default: 192.168.1.10)
- **Fallback Netmask** — The network mask associated with the fallback IP address. (Default: 255.255.255.0)
- **Manual DHCP Client Id** — An option to manually enter the hostname for the DHCP client.

Figure 24: IP Address Mode – Static IP



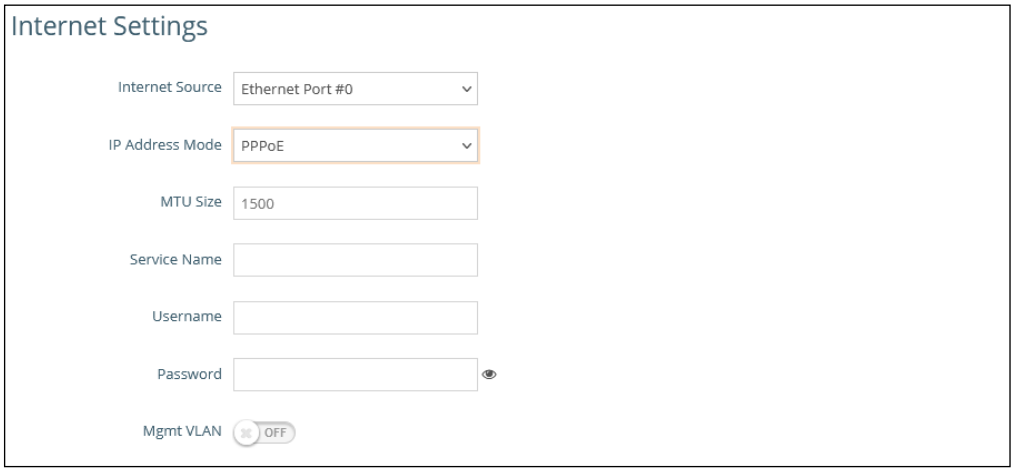
- **Static IP** — To configure a static IP address for the selected Ethernet interface, the following items must be specified.
  - **MTU Size** — Sets the size of the maximum transmission unit (MTU) for packets sent on this interface. (Range: 1400-1500 bytes; Default 1500 bytes)
  - **IP Address** — Specifies an IP address for the access point. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. (Default: 192.168.1.1)
  - **Subnet Mask** — Indicates the local subnet mask. (Default: 255.255.255.0)
  - **Default Gateway** — The IP address of the default gateway, which is used if the requested destination address is not on the local subnet.

    If you have management stations, DNS, RADIUS, or other network servers located on another subnet, type the IP address of the default gateway router in the text field provided.
  - **DNS Servers** — The IP address of Domain Name Servers on the network. A DNS maps numerical IP addresses to domain names and

can be used to identify network hosts by familiar names instead of the IP addresses.

If you have a DNS servers located on the local network, type the IP address in the text fields provided.

Figure 25: IP Address Mode – PPPoE



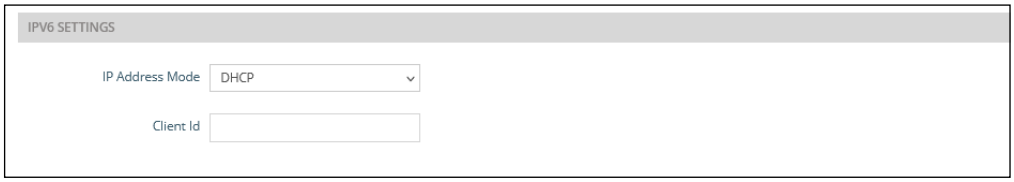
- **PPPoE** — To obtain an IP address for the selected Ethernet interface using PPPoE, the following items must be specified.
  - **Service Name** — The service name assigned for the PPPoE connection. The service name is normally optional, but may be required by some service providers. (Range: 1-32 alphanumeric characters)
  - **User Name** — The user name specified by the service provider. (Range: 1-32 characters)
  - **Password** — The password specified by the service provider. (Range: 1-32 characters)
- **MTU Size** — Sets the size of the maximum transmission unit (MTU) for packets sent on this interface. (Range: 1400-1500 bytes; Default 1500 bytes)
- **VLAN Tag** — Enable to activate tagging on this port and choose a tagging ID value between 2 and 4094, inclusive.
- **Mgmt VLAN** — Select this option to enable a management VLAN on this device. Once you enable this option, you will no longer be able to access this device on any of built-in the local networks (like 192.168.2.1 for example). You will only be able to access the device from the specified VLAN network. If this device's IP mode is set to DHCP, it will also request a new IP address in the subnet range assigned to the VLAN network.

1Doc: Protocolo 1.943/2025 | Anexo: em_8967D8805D2E821B6628907E9... (148/200) 3425/4726

IPv6 Settings

Enables you to configure the method used to provide an IPv6 address for the Internet access port.

Figure 26: IPv6 Settings



The following items are displayed on this section of the page:

- **IP Address Mode** — The method used to provide an IPv6 address for the Internet access port. (Default: DHCP; Options: DHCP, Static IP)
  - **DHCP** — If you configure DHCP, the Client Id must be specified.
    - **Client Id** — Manually enter the client ID for the DHCP client.
  - **Static IP** — To configure a static IPv6 address for the Internet access port, the following items must be specified.
    - **IP Address** — Specifies an IPv6 address for the access point. An IPv6 address must be configured according to RFC 2373 using 8 colon separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
    - **Default Gateway** — The IPv6 address of the default gateway, which is used if the requested destination address is not on the local subnet.
    - **DNS** — The IPv6 address of Domain Name Servers on the network. A DNS maps numerical IPv6 addresses to domain names and can be used to identify network hosts by familiar names instead of the IPv6 addresses. If you have a DNS server located on the local network, type the IPv6 address in the text field provided.

Ethernet Settings

The Ethernet Settings page configures the network behavior of the Ethernet ports, indicating that a port provides an Internet connection for wireless clients attached to the local network (routed to the Internet), or is bridged directly to the Internet.

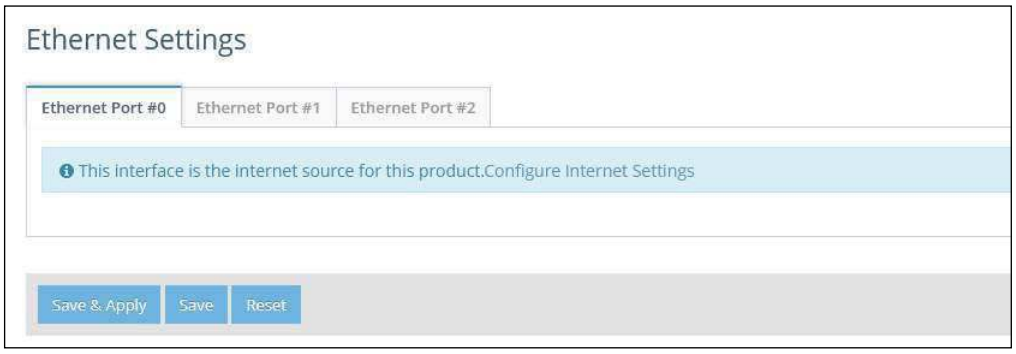
The following items are common for all pages under Ethernet Settings:

- **Ethernet Port #0** — Shows the status of the WAN Ethernet port.

1Doc: Protocolo 1.943/2025 | Anexo: em_8967:D8059:D2E321:B6628:9CE5D:Gestão_Laranjeiras_029_2025_Assessoria_Executiva_WiFi_6_AP_205_Rev_0624.pdf (146/200) 1426/4726

- **Ethernet Port #1** — Shows the status of the LAN Ethernet port 1.
- **Ethernet Port #2** — Shows the status of the LAN Ethernet port 2.

Figure 27: Ethernet Settings – Internet Source

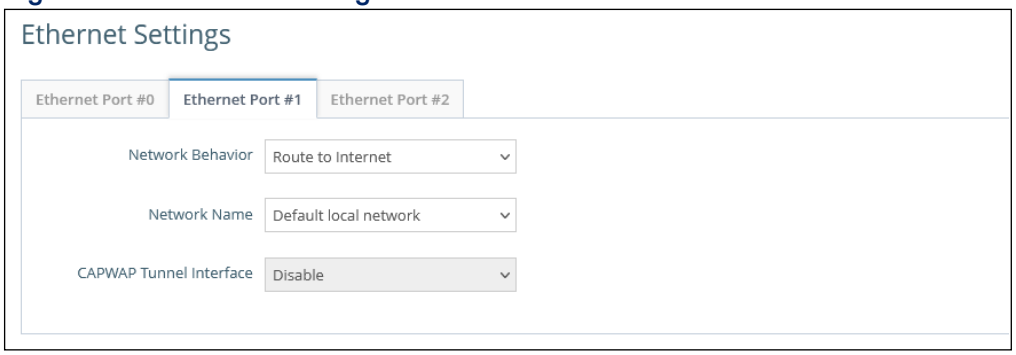


The following status message is displayed if an interface is set as the Internet source:

- "This interface is the internet source for this product. Configure Internet Settings"

  If more than one interface is connected to the Internet, only the last configured interface is used.

Figure 28: Ethernet Settings – Network Behavior



The following items are displayed on this page:

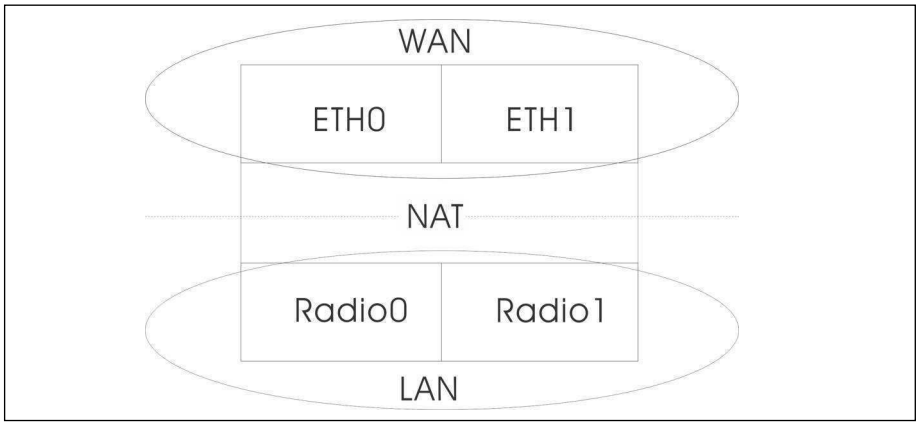
- **Network Behavior** — For the Ethernet port which is not providing Internet access, one of the following connection methods must be specified. (Default: Route to Internet)

  - **Bridge to Internet** — Configures an interface to be attached to the WAN. Traffic from this interface is directly bridged into the Internet. If an Ethernet port is bridged to the Internet, management access cannot be made by a direct connection to this port. However, if another Ethernet port or radio interface is within the LAN (routed to the Internet) the access point can be managed through this interface by a PC which is configured with an IP address in the same subnet.

1Doc: Protocolo 1.943/2025 | Anexo: em_8967DB805AD5821B6628907... Administrador 029/2025 ... 3426/4726

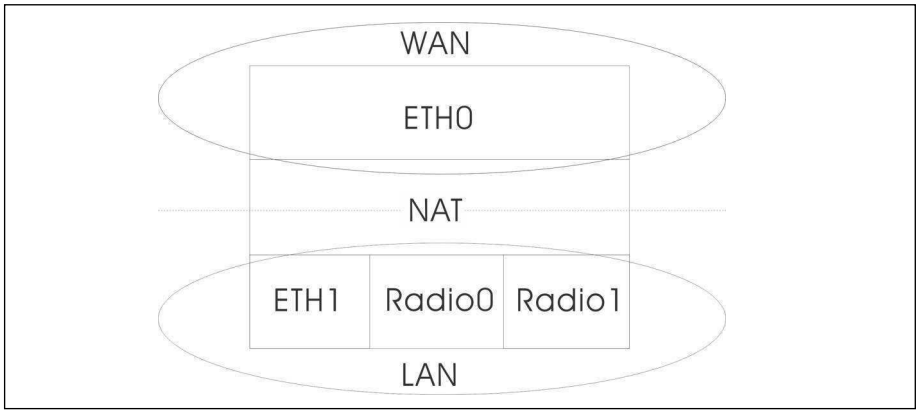
In the following figure, Ethernet Port 0 and Ethernet Port 1 are both attached to the WAN.

Figure 29: Bridge to Internet



- **Route to Internet** — Configures an interface to be a member of the LAN. Traffic from this interface is routed across the access point and out through an interface which is bridged directly to the Internet. By default, Ethernet Port 1 is routed to Internet, allowing management access via a direct connection to a PC configured with an address in the same subnet.

Figure 30: Route to Internet



  - **Network Name** — The network to be routed. The default is "Default local network" as displayed under LAN Settings – Local Networks.

- **Add to Guest Network** — This port can only support the guest network.

- **Hotspot Controlled** — This port can only access hotspot services. Click the link to open the Hotspot Settings page. See "Hotspot Settings" on page 53.

- **VLAN Tag Traffic** — This port transmits tagged traffic from a specified VLAN. Select the VLAN ID from the configured list, or click the link to open

1Doc: Protocolo 1.943/2025 | Anexo: em_8967D8805AD5821B6628B0E_pt-br_Laticínio 029_2025_Anexo_WiFi_629_2025_Rev1_634.pdf (158/200) 3428/4746

the Wireless VLAN Settings page and create a VLAN ID. See "VLAN Settings" on page 80.

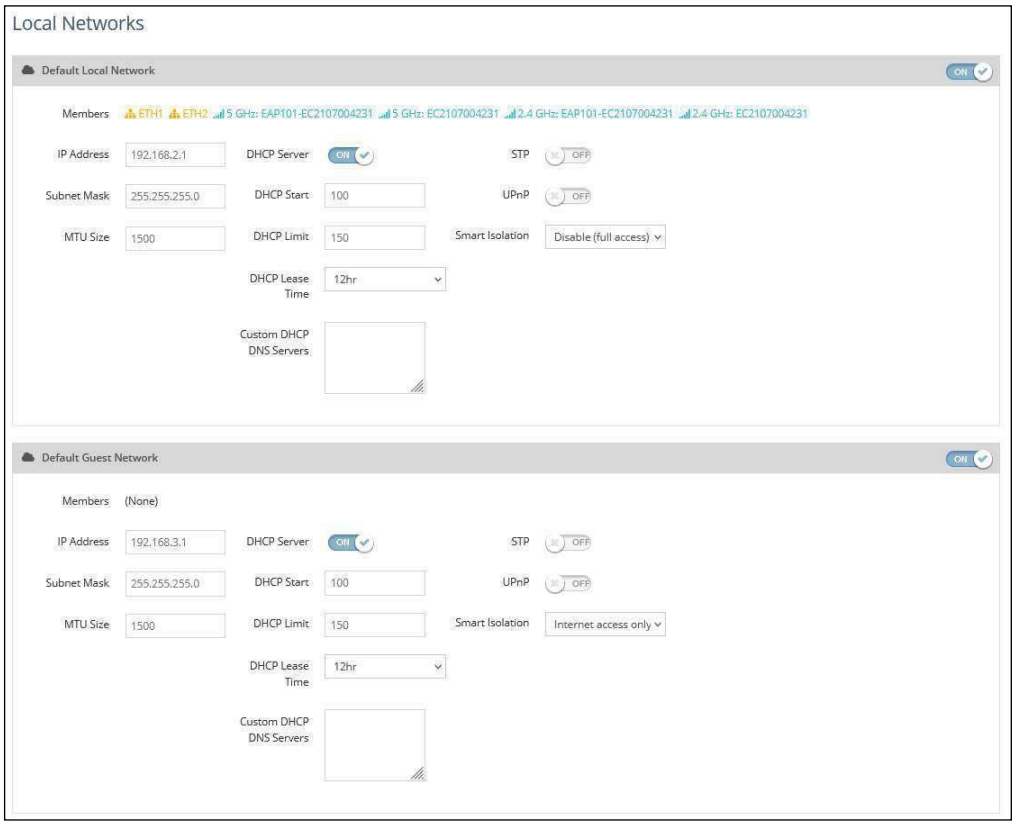
- **PoE Out** — (EAP104 only) Enables the PoE Out feature when the PoE source is detected as 802.3at, otherwise the PoE Out feature is disabled. When set to "Off," PoE Out is always disabled. (Default: On)

- **CAPWAP Tunnel Interface** — When the AP system management is set to EWS-Series Controller mode (see "System Settings" on page 83), the CAPWAP (Control And Provisioning of Wireless Access Points) protocol tunnel mode can be configured for the Ethernet port from the controller template. The options are "Disable" or "Complete." A Complete tunnel sends all management, authentication, and data traffic from the AP back to the controller. (Default: Disable)

LAN Settings

The LAN Settings page configures the LAN settings for the local and guest networks, including IP interface setting, DHCP server settings, and STP administrative status.

Figure 31: Network – LAN Settings



The following items are displayed on this page:

- **IP Address** — Specifies the IP address for the local network or guest network. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. (Default: 192.168.2.1)
- **Subnet Mask** — Indicates the local subnet mask. (Default: 255.255.255.0)
- **MTU Size** — Sets the size of the maximum transmission unit (MTU) for packets sent on this network. (Range: 1400-1500 bytes; Default 1500 bytes)
- **DHCP Server** — Enables/disables DHCP on this network. (Default: Enabled)
  - **DHCP Start** — First address in the address pool. (Range: 1-256; Default: x.x.x.100)
  - **DHCP Limit** — Maximum number of addresses in the address pool. (Range: 1-254; Default: 150)
  - **DHCP Lease Time** — The duration that an IP address is assigned to a DHCP client.
  - **Custom DHCP DNS Servers** — Specify the addresses or hostnames of custom DNS servers to be used.
- **STP** — Enables or disables processing of Spanning Tree Protocol messages. (Default: Disabled)
- **UPnP** — Enables or disables Universal Plug-and-Play broadcast messages. (Default: Disabled)
- **Smart Isolation** — Enables network traffic to be restricted to the specified network:
  - **Disable (full access)** — There is no traffic isolation. Clients can access the Internet and other devices on the local LAN.
  - **Internet access only** — Traffic from this network can only be routed to and from the Internet.
  - **LAN access only** — Traffic from this network is restricted to local LAN devices only.
  - **Internet access strict** — Traffic from this network can only be routed to and from the Internet, but with the additional restriction that users cannot access resources or devices on any private network (such as 192.168.0.0, 172.16.0.0, 10.0.0.0 etc.).
- **Add Custom LAN** — Click this button to create additional networks with their own custom settings. You can create up to 5 custom LANs.

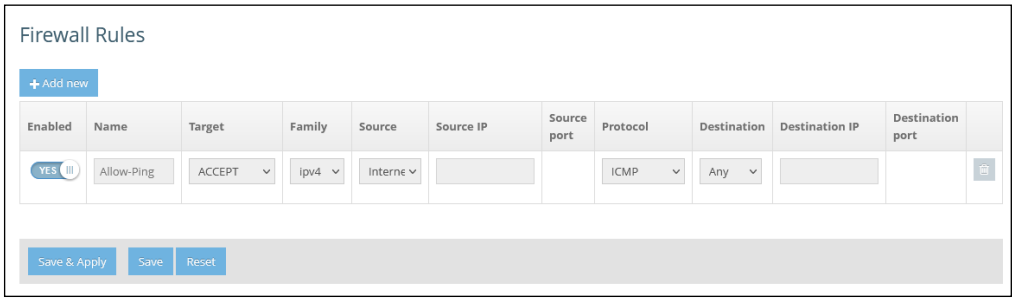
1Doc: Protocolo 1.943/2025 | Anexo: em_8967:D8059D2E321B6628B9E:esso_Laranjeiras_029/2025_Anexo_WiFi_6_AP_2025_Rev_0624.pdf (150/200) 3439/4746

Firewall Rules

Firewall filtering restricts connection parameters to limit the risk of intrusion. The firewall settings allow you to define a sequential list of rules that filter traffic based on source and destination IP addresses and ports. Ingress packets are tested against the filter rules one by one. As soon as a packet matches a rule, the configured target action is implemented.

One rule, "Allow-Ping," is pre-configured to allow Ping packets from the Internet. You can enable or disable this rule, but it cannot be modified or deleted. Click the "Add new" button to add a new firewall rule.

Figure 32: Firewall Rules



The following items are displayed on this page:

- **Enabled** — Enables or disables the rule.
- **Name** — A user-defined name for the filtering rule. (Range: 1-30 characters)
- **Target** — The action to take when a packet is matched. (Options: Accept, Reject, Drop; Default: Accept)
  - **Accept** — Accepts matching packets.
  - **Reject** — Drops matching packets and returns an error packet in response.
  - **Drop** — Drops matching packets.
- **Family** — The IP address family. (Options: Any, IPv4; Default: Any)
- **Source** — The source interface. (Options: Guest Network, Hotspot Network, Default Local Network, Internet, Any)
- **Source IP** — The source IPv4 address in CIDR notation. Includes an IPv4 address followed by a slash (/) and a decimal number to define the network mask.
- **Source port** — The source protocol port. (Range: 0-65535)

1Doc: Protocolo 1.943/2025 | Anexo: em_8967DB805AD5821B6628B0E_pdf_Laboratorio_029_2025_Assessoria_Tecnica_WiFi_6_AP_025_Rev_01_pdf (154/200) 3420/4726

- **Protocol** — The protocol type. (Options: Any, TCP+UDP, TCP, UDP, ICMP; Default: TCP+UDP)
- **Destination** — The destination interface. (Options: Guest Network, Hotspot Network, Default Local Network, Internet, Any)
- **Destination IP** — The destination IP address.
- **Destination port** — The destination protocol port. (Range: 0-65535)

Port Forwarding

Port Forwarding can be used to map an inbound protocol type (TCP/UDP) and port to an "internal" IP address and port. The internal (local) IP addresses are the IP addresses assigned to local devices at the edge of a network, and the external IP address is the IP address assigned to the AP interface. This allows remote users to access different servers on your local network using your single public IP address.

Remote users accessing services such as web or FTP at your local site through your public IP address, are redirected (mapped) to other local server IP addresses and TCP/UDP port numbers. For example, if you set Type/Public Port to TCP/80 (HTTP or web) and the Private IP/Port to 192.168.3.9/80, then all HTTP requests from outside users are forwarded to 192.168.3.9 on port 80. Therefore, by just using your external IP address provided by your ISP, Internet users can access the services they need at the local addresses to which you redirect them.

Figure 33: Port Forwarding

The following items are displayed on this page:

- **Enabled** — Enables port forwarding.
- **Name** — User defined name. (Range: 1-30 characters)
- **Protocol** — Set the protocol to which port forwarding is applied. (Options: TCP, UDP, TCP+UDP)
- **External Port** — The TCP/UDP port number. (Range: 1-65535)

  The more common TCP service port numbers include: HTTP: 80, FTP: 21, Telnet: 23, and POP3: 110.

1Doc: Protocolo 1.943/2025 | Anexo: em_8967DB805AD5821B6628B0E_pt-br_Laticínios 029_2025_Assistência Técnica_WI-629P_125_Rede_v1.pdf (152/200) 1422/4746

- **Internal IP address** — The internal destination IP address.
- **Internal Port** — The internal destination protocol port. (Range: 1-65535)

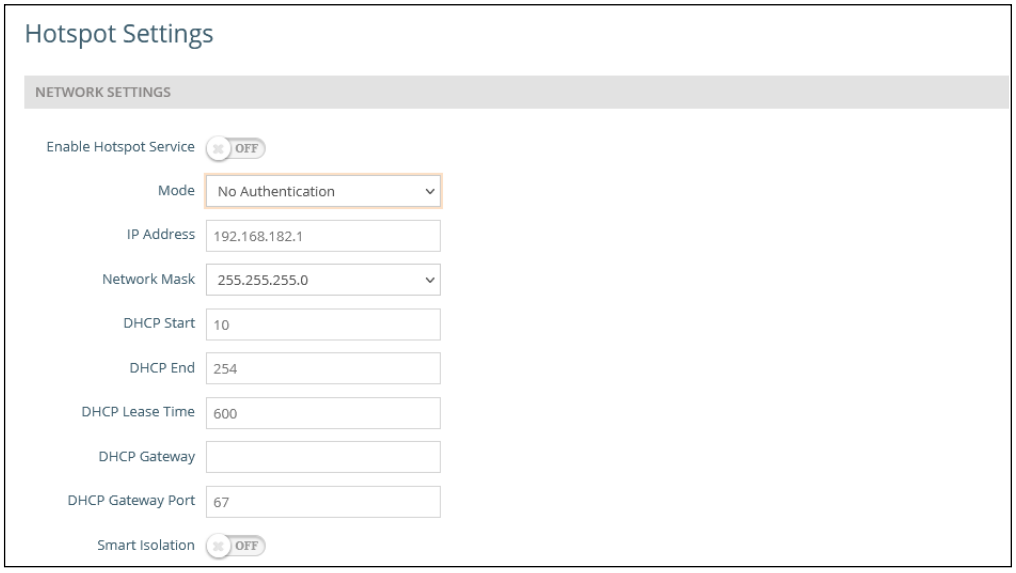
Hotspot Settings

The Hotspot Settings page can configure Internet access to the general public in places such as coffee houses, libraries and hospitals. Specific access rights may also be defined through a RADIUS server.

Network Settings

This section includes the option to enable or disable hotspot service, hotspot mode options, and network settings.

Figure 34: Hotspot Settings (Network Settings)



The following items are displayed on this page:

- **Enable Hotspot Service** — Enables or disables hotspot service. A hotspot is a physical location where people may obtain Internet access, typically using Wi-Fi technology, via a wireless local area network using a router connected to an Internet service provider.
- **Mode** — Hotspot service types include the following options:
  - **External Captive Portal Service** — This option will show the hotspot guest an externally hosted captive portal splash page and may prompt them to login, depending on how you've configured your service settings. Choose this option if you've signed up with a third-party captive portal service provider such as Cloud4Wi or HotSpotSystem.

1Doc: Protocolo 1.943/2025 | Anexo: em_8967D8805AD5821B6628907... Laticínio... 029/2025_Anexo_WiFi_6_AP_2025_Rev_0624.pdf (156/204) 1422/4726

- **No Authentication** — This option shows the hotspot guest your customized, locally hosted captive portal splash page, and will not require the guest to login before accessing the Internet. If you fill out the (optional) terms of service text, the guest will be required to accept these before they can access the Internet.

- **Simple Password-Only Splash Page** — This option will show the hotspot guest your customized, locally hosted captive portal splash page, and will require them to enter a simple password to login and access the Internet. If you fill out the (optional) terms of service text, the guest will be required to accept these before they can access the Internet.

- **Local Spash Page with External RADIUS** — This option shows the hotspot guest your customized, locally hosted captive portal splash page, and will require them to enter a valid RADIUS username and password to login and access the Internet. If you fill out the (optional) terms of service text, the guest will be required to accept these before they can access the Internet.

- **Network IP** — Specifies the IP address for the hotspot. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. (Default: 192.168.182.1)

  If your WAN subnet conflicts with any of the local networks (even the custom ones you create), the AP will automatically change the subnet of the local network.

- **Network Mask** — Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.

- **DHCP Start** — Starting number of (last numeric field) in address pool. (Range: 1-254; Default: 10)

- **DHCP End** — Ending number of (last numeric field) in address pool. (Range: 1-254; Default: 254)

- **DHCP Lease Time** — The duration that an IP address is assigned to a DHCP client. (Range: 600-43200 seconds; Default: 600 seconds)

- **DHCP Gateway** — Configure the DHCP gate IP address if you want to use an external DHCP server instead of the internal one.

- **DHCP Gateway Port** — The listening port used by the DHCP gateway.

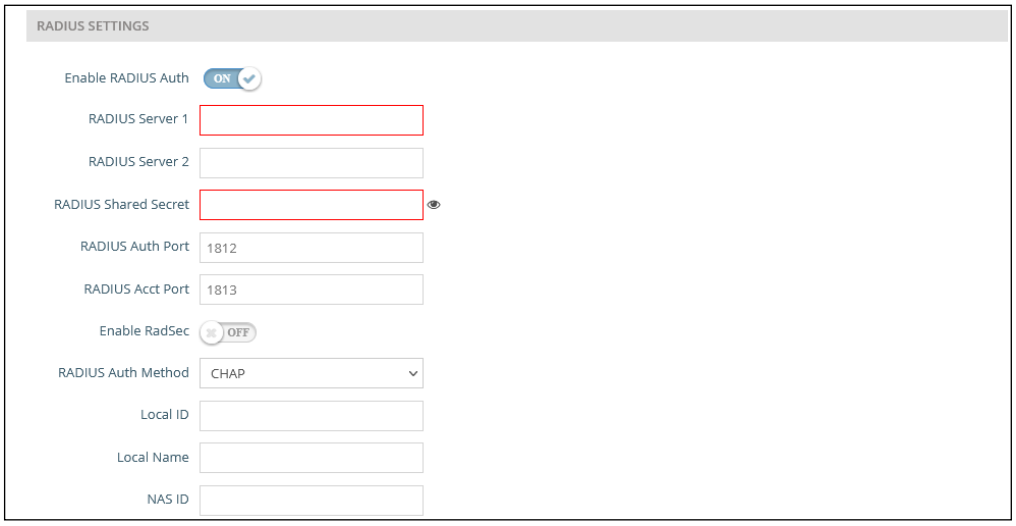
- **Smart Isolation** — Activate to prevent Hotspot users to possibly access WAN resources.

1Doc: Protocolo 1.943/2025 | Anexo: em_8907.D8059.D2E321B6628P6T_esto_Laticínio_029_2025_Anexo_WiFi_6_AP_205_Base_624.pdf (154/200) 3428/4746

RADIUS Server

If you click set the mode to External Captive Portal Service or Local Splash page with External RADIUS, the following section is displayed.

Figure 35: Hotspot Settings (RADIUS Settings)



The following items are displayed on this page:

- **Enable RADIUS Auth** — Enables or disables client authentication via a RADIUS server.
- **RADIUS Server 1** — IP address or host name of the primary RADIUS server.
- **RADIUS Server 2** — IP address or host name of the secondary RADIUS server.
- **RADIUS Shared Secret** — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS server. Do not use blank spaces in the string. (Range: 1-255 characters).
- **RADIUS Auth Port** — RADIUS server UDP port used for authentication messages. (Range: 1-65535, Default: 1812)
- **RADIUS Acct Port** — RADIUS server UDP port used for accounting messages. (Range: 1-65535, Default: 1813)
- **Enable RadSec** — An authentication and authorization protocol for transporting RADIUS datagrams over TCP and TLS. RadSec replaces UDP used in the initial RADIUS design, providing a reliable transport protocol and more extensive security for the packet payload.
- **RADIUS Auth Method** — Selects the encryption method to use for messages between the AP and the RADIUS server; CHAP, PAP, or MSCHAPv2. The encryption method must match that used by the RADIUS server.

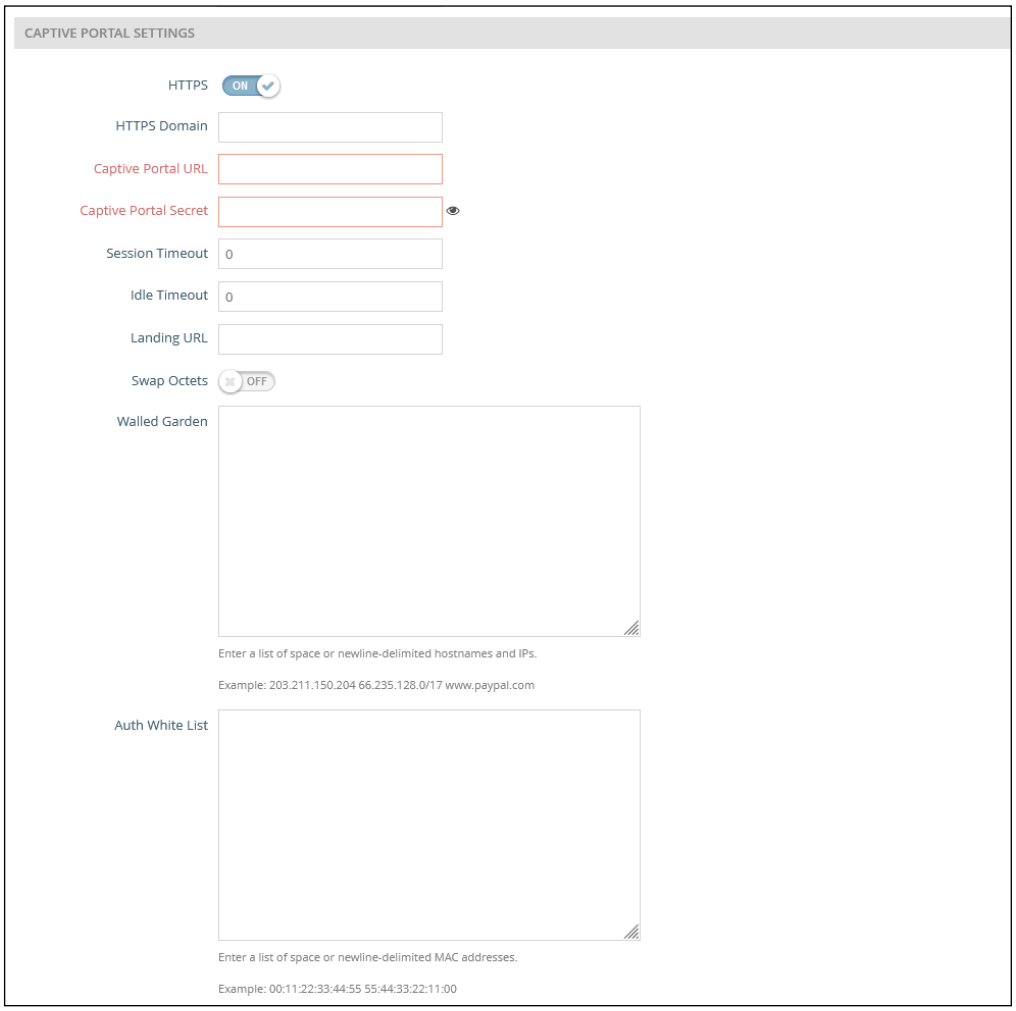
1Doc: Protocolo 1.943/2025 | Anexo: em_8967D8805AD5821B6628907... Laranjeiras 029/2025 ... 1425/4726

- **Local ID** — Local RADIUS server identifier.
- **Local Name** — Local RADIUS server name
- **NAS ID** — Local RADIUS server operation identifier.

Captive Portal Settings

The following section is displayed for all hotspot mode options.

Figure 36: Hotspot Settings (Captive Portal Settings)



The following items are displayed on this page:

- **HTTPS** — Enables HTTPS for the captive portal. (Default: Disabled)

Note: To upload a unique security certificate from a trusted certification authority for the HTTPS captive portal, see "Upload Certificate" on page 88.

1Doc: Protocolo 1.943/2025 | Anexo: em_8967:D8805D2E32B4628P0T_gest_Laranjeiras_029_2025_Assessoria_WiFi_29_P_2025_Site_0624.pdf (56/200) 1426/4746

- **HTTPS Domain** — The domain name of the HTTPS captive portal.
- **Captive Portal URL** — Host name of Internet service portal for the hotspot.

  The captive portal forces a hotspot client to access a welcome web page (normally used for authentication) before gaining further access to the Internet. The welcome page may require authentication and/or payment.
- **Captive Portal Secret** — The password used for logging into the hotspot.
- **Customize Splash Page** — This option is shown for all hotspot service options other than External Captive Portal Service. If enabled, fill in information for the title, background color, logo image file, and optional terms and conditions.
- **Session Timeout** — The maximum time a client can stay attached to the hotspot. (Range: 0-86400 seconds)
- **Idle Timeout** — The maximum a connection can remain inactive before it is closed. (Range: 0-86400 seconds)
- **Landing URL** — Indicates the URL to which the user is directed after logging in to the captive portal.
- **Swap Octets** — Swap the values of the reported “input octets” and “output octets.” This option only appears under External Captive Portal Service.
- **Walled Garden** — A list of web sites to which unauthenticated users are allowed to navigate.
- **Auth White List** — A list of MAC addresses that are allowed to bypass the captive portal to access the Internet.

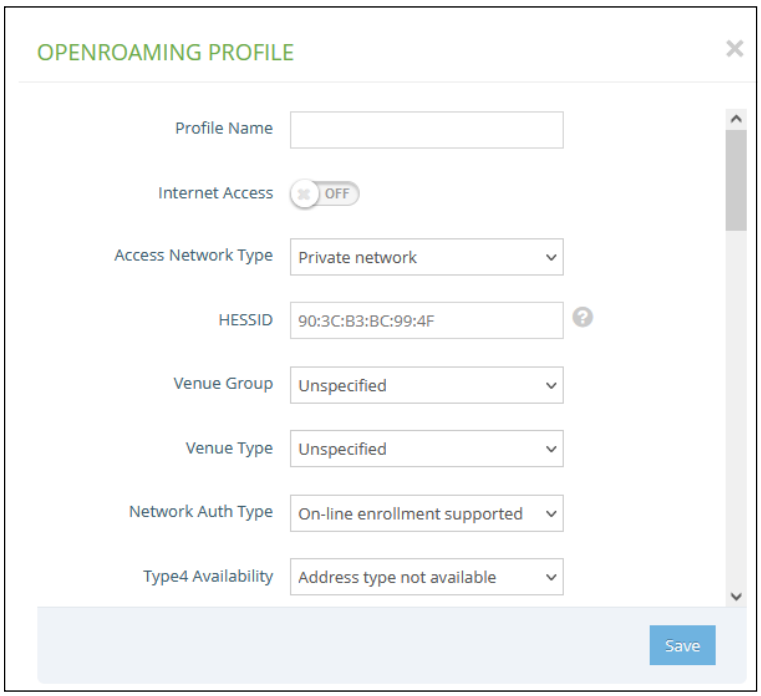
1Doc: Protocolo 1.943/2025 | Anexo: em_8967D8805AD5821B6628907... Manual_Administrador_v1_0_29_2025_Inglês_Anexo_WiFi_6_EAP225_Box_1.pdf (160/200) 1426/4746

OpenRoaming

OpenRoaming provides a standard for public-access Wi-Fi networks to support seamless roaming between wireless networks. An OpenRoaming network advertises its public Wi-Fi capabilities and services so that clients can decide if they want to connect to the network.

Up to 32 OpenRoaming profiles can be configured and applied to specific wireless networks (see "OpenRoaming" under "Wireless Networks — Network Settings" on page 76). Click "Add New" to configure a profile.

Figure 37: OpenRoaming Profile



The following items are displayed on this page:

- **Profile Name** — A name that identifies the profile.
- **Internet Access** — Enable if this network provides access to the Internet.
- **Access Network Type** — Select one from the predefined list.
  - **Private network** — Home and enterprise networks that unauthorized users cannot access.
  - **Private network with guest access** — A private network that provides for guest access. A typical example would be an enterprise network that offers guest access.

1Doc: Protocolo 1.943/2025 | Anexo: em_8967DB805AD5821B6628B9E_pt-BR_Laticínios_029_2025_Assistência_Técnica_WiFi_6_AP_205_Brite_624.pdf (168 de 204) 1428/4746

- **Chargeable public network** — A network that is available to all users, but requires a fee.
- **Free Public Network** — A network that is available to all users without any fees.
- **Personal device network** — A network for peripheral connectivity in an ad-hoc mode. For example, a camera that connects to a printer.
- **Emergency services only network** — A network that is dedicated for access to emergency services only.
- **Test or experimental** — A network for tests or experimental work.
- **Wildcard** — When selected, the AP will reply to clients regardless of the network type requested by the client query.

- **HESSID** — The Homogenous Extended Service Set Identifier (HESSID) for the OpenRoaming network. When configured, the HESSID (a MAC address) uniquely identifies all APs belonging to the same network.
- **Venue Group** — Identifies the general class of the venue. Select from the predefined list.
- **Venue Type** — Identifies the specific type of venue within each group.
- **Network Auth Type** — Specifies the authentication required for the network. Select an option from the predefined list. (Default: "Acceptance of terms and conditions")
- **Type4 Availability** — Specifies the IPv4 address type available from the network.
- **Type6 Availability** — Specifies the IPv6 address type available from the network
- **Operating Class** — A standard index (based on IEEE Std 802.11-2012 Annex E) that specifies the AP supported operating channels.
- **Captive Portal** — Enables the Captive Portal feature. (Default: Disabled)
  - **Captive Portal URL** — Host name of Internet service portal (HTTP or HTTPS).

    A captive portal forces a client to access a welcome web page (normally used for authentication) before gaining further access to the Internet. The welcome page may require authentication and/or payment.

1Doc: Protocolo 1.943/2025 | Anexo: em_8967D8805AD5821B6628907E_pdf_Laticínios_Termo_de_Referência_029_2025_Aquisição_de_Wi-Fi_6_AP_205_Lote_1_624.pdf (159/200) 1429/4746

- **Wall Garden** — A list of web sites to which unauthenticated users are allowed to navigate. Enter a list of space or newline-delimited host names and IP addresses.

- **Venue Name Information** — Configures a list of up to 10 venue names.
  - **Language Code** — Select a language from the list. (Default: English)
  - **Venue Name** — The name of the network venue. Multiple names can be added to the list.
  - **Venue URL** — Specifies a URL that provides additional venue information to users.

- **Cellular Network Information List (PLMN)** — (Optional) Identifies the 3GPP cellular networks available through the AP. Specifically, this field identifies the Public Land Mobile Network (PLMN) ID, comprised of the Mobile Country Code (MCC) and Mobile Network Code (MNC) of the mobile operator. Up to 10 PLMN IDs can be configured. Input the pair of MCC, MNC.
  For example: 400, 00
  MCC: Three decimal digits (000-999)
  MNC: Two (00-99) or three decimal digits (000-999)

- **Operator Friendly Name** — The name of the network operator and the specified language. Up to 10 names can be configured.

- **Roaming Consortium List** — (Optional) A roaming consortium is a group of service providers (SP) with which a user's credentials can be used for authentication. Each roaming consortium is identified by an organization identifier (OI) that is assigned by the IEEE. An OI is often 24 bits in length, but can also be 36 bits. Up to 10 identifiers can be configured.

- **Domain Name List** — Lists one or up to 10 domain names for the entity operating the AP. This is critical for OpenRoaming network selection policy, as it identifies the operator of the network. It indicates to the mobile device whether they are at a home hotspot or a visited hotspot.

- **NAI Realm List** — (Optional) The network access identifier (NAI) realm list identifies those service provider or other networks that are accessible through the AP. By discovering which authentication realms are supported by a network, a mobile device can selectively authenticate to its preferred network. Up to 10 identifiers can be configured.
  - **Method/Authentication** — Specifies EAP methods and authentication for each service provider added to the NAI Realm List.

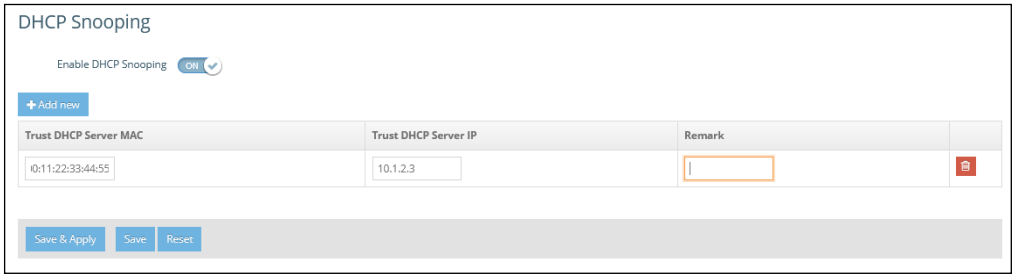
1Doc: Protocolo 1.943/2025 | Anexo: em_8967D8805AD5E821B6628B9CE_Laticínios_Processo_Licitatório_029_2025_Anexo_WiFi_6_AP_205_Rate_624.pdf (160/200) 1429/4726

DHCP Snooping

DHCP snooping is used to validate and filter DHCP messages received by the AP. When DHCP snooping is enabled, DHCP messages received from a device not listed in the DHCP snooping table are dropped.

You can add known and trusted DHCP servers to the table by specifying their MAC and IP addresses.

Figure 38: DHCP Snooping



The following items are displayed on this page:

- **Enable DHCP Snooping** — Enables DHCP Snooping on the AP.
- **Trust DHCP Server MAC** — The MAC address of a known and trusted DHCP server.
- **Trust DHCP Server IP** — The IP address of a known and trusted DHCP server.
- **Remark** — A comment relating to the DHCP server configured.

1Doc: Protocolo 1.943/2025 | Anexo: em_8967_DHCP_Snooping_Configuration_Administrator_029_2025_Assinatura_Eletronica_WiFi_6_AP_2025_Base_1324.pdf (164/200) 3430/4726

ARP Inspection

ARP Inspection is a security feature that validates the MAC Address bindings for Address Resolution Protocol packets. It provides protection against ARP traffic with invalid MAC-to-IP address bindings, which forms the basis for certain "man-in-the middle" attacks. This is accomplished by intercepting all ARP requests and responses and verifying each of these packets before the local ARP cache is updated or the packet is forwarded to the appropriate destination. Invalid ARP packets are dropped.

Figure 39: ARP Inspection

The following items are displayed on this page:

- **ARP Inspection** — When enabled, ARP packets are validated against ARP spoofing.
- **Force DHCP** — Allows the AP to only learn MAC/IP pair information through DHCP packets. Since devices configured with static IP address do not send DHCP traffic, any clients with static IP addresses will be blocked by the AP unless their MAC/IP pair is listed and enabled in the Static Trust List.
- **Trust List Broadcast** — Lets other APs learn the trusted MAC/IP pairs to issue ARP requests.
- **Static Trust List** — Adds the MAC or MAC/IP pairs of devices that are trusted to issue ARP requests. Other network nodes can still send their ARP requests, but if their IP appears in the static list with a different MAC, their ARP requests will be dropped.

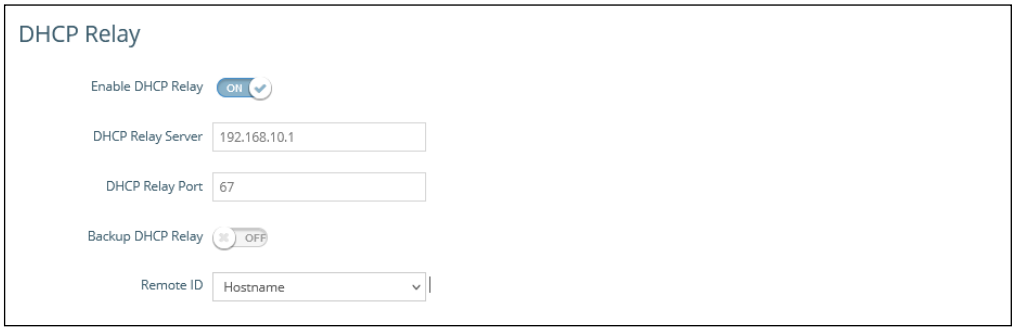
1Doc: Protocolo 1.943/2025 | Anexo: em_8967D8805AD5821B6628F9CE_Manual_Administrador_Web_Access_Point_EAP225_Wi-Fi_6_AP_1.0.5_Build_0624.pdf (162/200) 1432/4726

DHCP Relay

When DHCP relay is enabled, the AP as an agent for all clients and sends all broadcast DHCP requests directly to a specified DHCP server. The DHCP server IP address and port must be configured, and optionally a backup server.

With DHCP relay enabled, the circuit ID can be set on the VLAN settings or LAN settings page. IP addresses of clients are then obtained by the DHCP relay server and the IP range is determined by the remote ID and circuit ID.

Figure 40: DHCP Relay



The following items are displayed on this page:

- **Enable DHCP Relay** — Enables the DHCP relay feature on the AP.
- **DHCP Relay Server** — Specifies the IP address of the DHCP server.
- **DHCP Relay Port** — Specifies the port of the DHCP server.
- **Backup DHCP Relay** — Optionally specifies a backup DHCP server IP address and port to use if there is no response from the primary server.
- **Remote ID** — Use the hostname as the remote ID, or manually configure a text string as the remote ID.

1Doc: Protocolo 1.943/2025 | Anexo: em_8967D8805AD5321B6628F6E5ECA1A0F5_Proposta_Administrativa_029_2025_Aquisicao_Wifi_6_AP_205_Itens_0624.pdf (166/200) 3432/4726

4 Wireless Settings

This chapter describes the wireless settings on the access point. It includes the following sections:

1Doc: Protocolo 1.943/2025 | Anexo: em_8907D8805AD5821B6628907C_Manual_Administrador_Web_Access_Point_WF629_2025_Rev1.0_pdf (167/200) 3433/4726

Radio Settings

The IEEE 802.11 wireless interfaces include configuration options for radio signal characteristics and wireless security features.

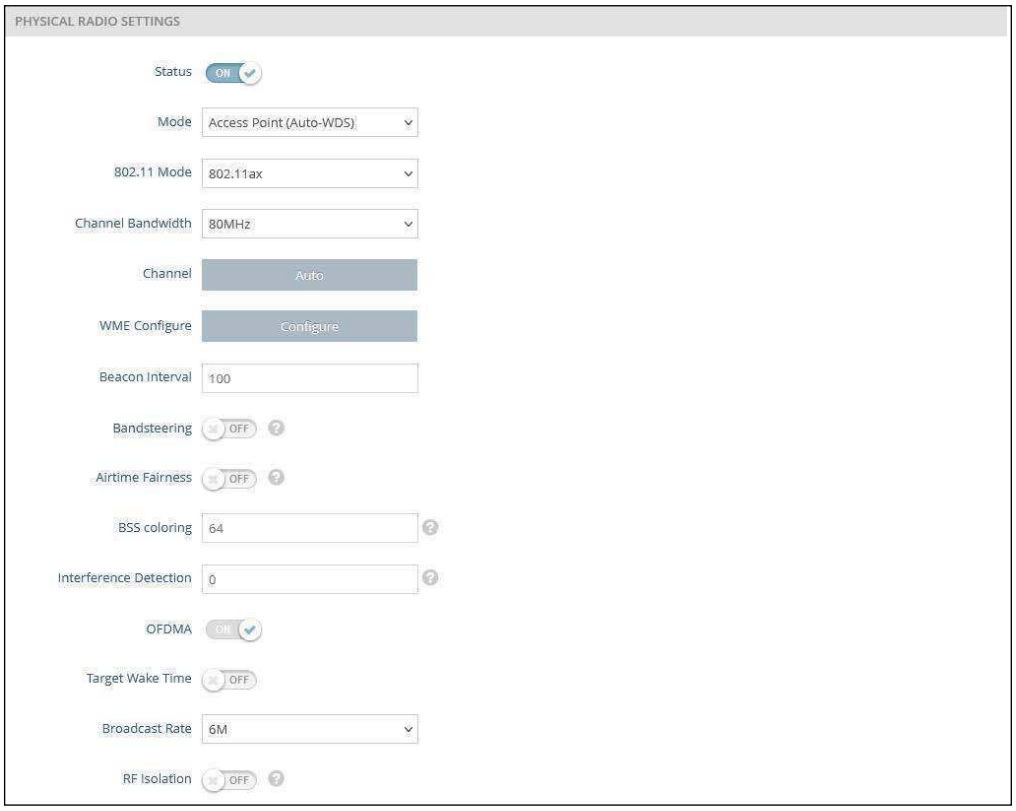
The access point can operate in several radio modes, 802.11b+g+n/ax (2.4 GHz) or 802.11a/a+n/ac+a+n/ax (5 GHz). Note that the dual-band access points can operate at 2.4 GHz and 5 GHz at the same time. The web interface identifies the radio configuration pages as:

- **Radio 2.4 GHz** — the 2.4 GHz 802.11b/g/n/ax radio interface
- **Radio 5 GHz** — the 5 GHz 802.11a/n/ac/ax radio interface
- **HaLow** — the HaLow (863-928 MHz) radio interface (EAP112 only)

Each radio supports 16 virtual access point (VAP) interfaces based on the SSIDs, referred to as SSID1 ~ SSID16. Each VAP functions as a separate access point, and can be configured with its own Service Set Identification (SSID) and security settings. However, most radio signal parameters apply to all VAP interfaces. Traffic to specific VAPs can be segregated based on user groups or application traffic. The clients associate with each VAP in the same way as they would with separate physical access points.

Physical Radio Settings

Figure 41: Physical Settings for Radio 5 GHz



1Doc: Protocolo 1.943/2025 | Anexo: em_8467_D8059_D2E321B6628B9E_pt-br_Laranjeiras_2025_Assessoria_Externa_WiFi_6_EAP225_Box_1_v1.0.24.pdf (168/200) 3435/4726

Figure 42: Physical Settings for Radio 2.4 GHz

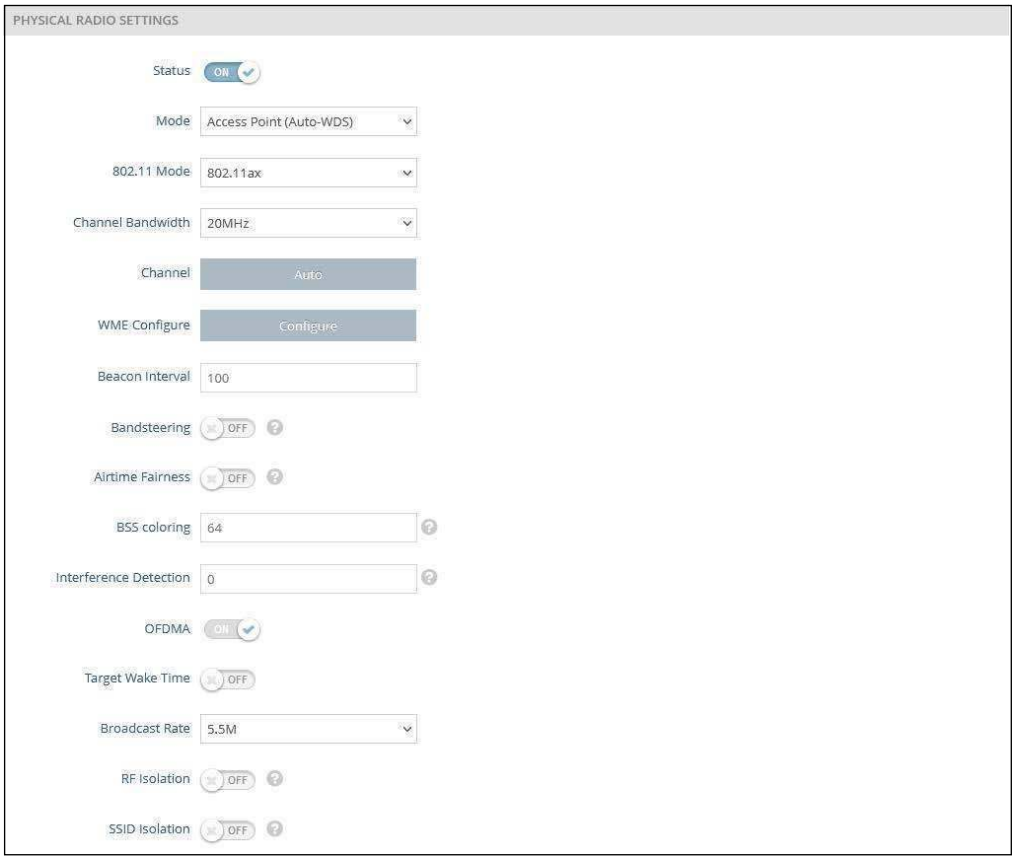
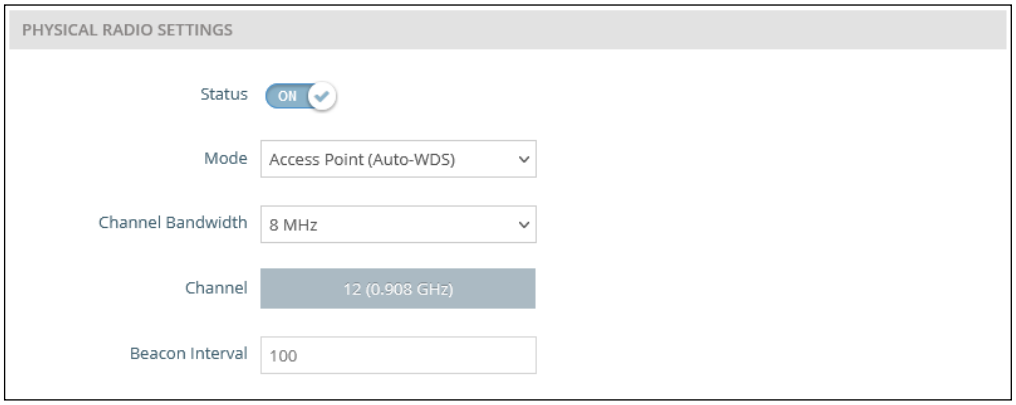


Figure 43: Physical Settings for HaLow (EAP112)



The following items are displayed on this page:

- **Status** — Enables or disables the wireless service on this interface.
- **Mode** — Selects the mode in which the AP will function.
  - **Access Point (Auto-WDS)** — The AP operates as an access point in WDS mode, which accepts connections from APs in Client WDS mode. (This is the default setting.)

1Doc: Protocolo 1.943/2025 | Anexo: em_8967DB805AD5821B6628907... Laranjeiras 029/2025 ... EAP112_EAP225_Datasheet_(169/200) 3435/4726

In this mode, the AP provides services to clients as a normal access point. WDS is used to automatically search for and connect to other AP nodes using the same SSID and security settings.

- **Client** — The AP can provide a wireless connection to another AP, as well as pass information from or to locally wired hosts and wireless clients.

- **802.11 Mode** — Defines the radio operation mode.
  - **Radio 2.4 GHz** — Default: 11ax; Options: 11b+g+n/ax
  - **Radio 5 GHz** — Default: 11ax; Options: 11a, 11a+n, 11ac+a+n, 11ax

- **Channel Bandwidth** — The AP options for channel bandwidth include 20, 40 80, and 160 MHz. The available channel bandwidth is dependent on the 802.11 Mode. (Default: 20 MHz on 2.4 GHz Radio, 80 MHz on 5 GHz Radio; Options: 20 MHz, 40 MHz, 80MHz, 160MHz)
  - **1–8 MHz** — For 802.11ah HaLow (EAP112 only)
  - **20MHz** — For 802.11b+g+n and 802.11ax
  - **40MHz** — For 802.11b+g+n, 802.11a, 802.11a+n, 802.11ac+a+n and 802.11ax
  - **80MHz** — For 802.11ac+a+n and 802.11ax
  - **160MHz** — (Supported only on EAP104, EAP111, EAP112 and OAP101 5 GHz radio) For 802.11ac+a+n and 802.11ax

- **Channel** — The radio channel that the access point uses to communicate with wireless clients. When multiple access points are deployed in the same area, set the channel on neighboring access points at least five channels apart to avoid interference with each other. For example, for 11g/n 20 MHz mode you can deploy up to three access points in the same area using channels 1, 6, 11. Note that wireless clients automatically set the channel to the same as that used by the access point to which it is linked. (The available channels are dependent on the 802.11 Mode, Channel Bandwidth, and Country Code settings.)

  Selecting Auto enables the access point to automatically select an unoccupied radio channel. (Default: Auto)

- **WME Configuration** — Wireless Multimedia Extensions (WME), also known as Wi-Fi Multimedia (WMM), is a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. It provides basic Quality of service (QoS) features for IEEE 802.11 networks. Access priority can be configured for four "Access Category"(AC) types using the following parameters:
  - **CW Min (Minimum Contention Window)** – The initial upper limit of the random backoff wait time before wireless medium access can be attempted. The initial wait time is a random value between zero and the

1Doc: Protocolo 1.943/2025 | Anexo: em_8967DB805AD5821B6628B0E_pt-br_Administrador_Web_Interface_Manual_v1.0_EAP225_BR_1.5.0_1.624.pdf (67 de 204) 3437/4726

CWMin value. Specify the CWMin value in the range 0-15 microseconds. Note that the CWMin value must be equal or less than the CWMax value.

- **CW Max (Maximum Contention Window)** – The maximum upper limit of the random backoff wait time before wireless medium access can be attempted. The contention window is doubled after each detected collision up to the CWMax value. Specify the CWMax value in the range 0-15 microseconds. Note that the CWMax value must be greater or equal to the CWMin value.

- **AIFS (Arbitration Inter-Frame Space)** – The minimum amount of wait time before the next data transmission attempt. Specify the AIFS value in the range 0-15 microseconds.

- **TXOP Limit (Transmit Opportunity Limit)** – The maximum time an AC transmit queue has access to the wireless medium. When an AC queue is granted a transmit opportunity, it can transmit data for a time up to the TXOP Limit. This data bursting greatly improves the efficiency for high data-rate traffic. Specify a value in the range 0-8192 microseconds.

- **Beacon Interval** — The rate at which beacon signals are transmitted from the access point. The beacon signals allow wireless clients to maintain contact with the access point. They also carry power-management and other information. (Range: 100-1024 TUs; Default: 100 TUs)

- **Bandsteering** — When enabled, clients that support 2.4 GHz and 5 GHz are first connected to the 5 GHz radio. This feature helps balance the client load over the two radio bands. Note that both radios must have configured SSIDs and security settings that match for this feature to fully operate. (Default: Off)

- **Airtime Fairness** — Enabling this feature improves the overall performance of the wireless network. (Default: Disabled)

- **BSS coloring** — In 802.11ax (Wi-Fi 6) mode, BSS coloring allows nearby APs operating at the same frequency to identify traffic belonging to their own Basic Service Set (BSS). The BSS coloring enables Wi-Fi 6 networks to operate more efficiently in high-density environments where neighboring AP and client transmissions overlap. Assign a color value (a number from 1 to 63) to identify the radio BSS, or enter value 64 to allow the AP to randomly select a color value. (Range: 1-63, 64 random; Default: 64)

- **Interference Detection** — When the utilization in current channel reaches the configured threshold (as a percentage), the AP switches to a different channel. (Range: 0 - 100%; Default: 0, disabled)

- **OFDMA** — The 802.11ax (Wi-Fi 6) mode supports Orthogonal Frequency Division Multiple Access (OFDMA) and this cannot be disabled.

- **Target Wake Time** — In 802.11ax (Wi-Fi 6) mode, the AP can allow clients to request a specific Target-Wakeup Time (TWT) to transmit or receive frames,

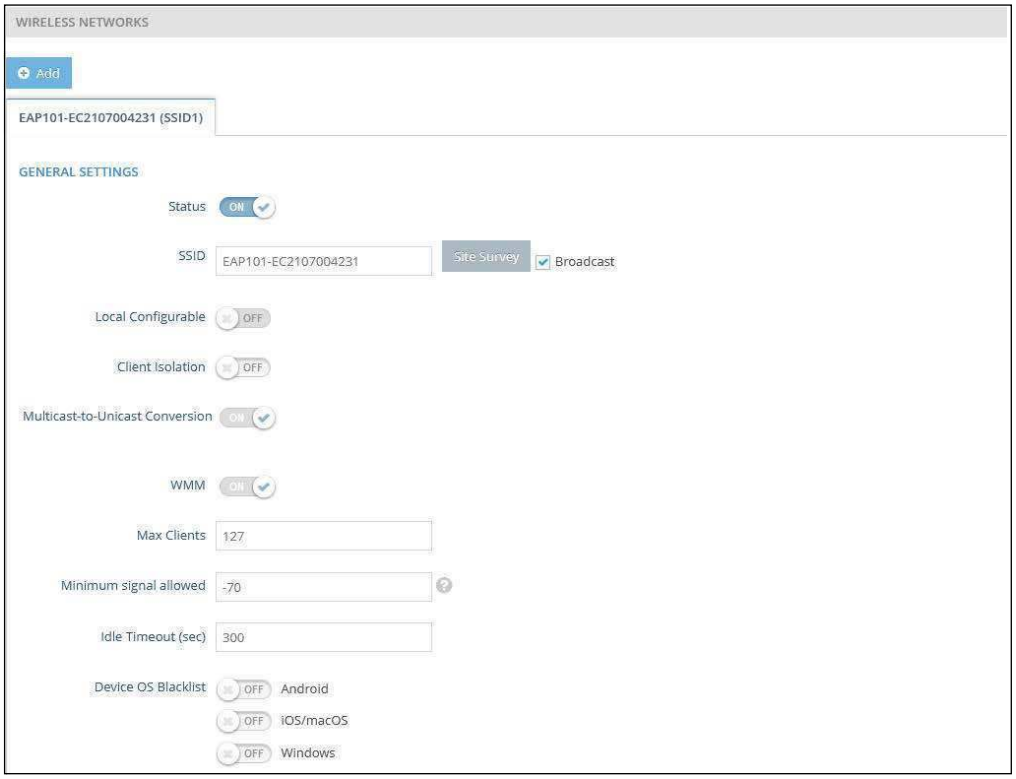
1Doc: Protocolo 1.943/2025 | Anexo: em_8407_DBS_AX3600_Gestao_Lan_Internet_v1_0_PT_Linha_Corporativa_029_2025_sem_texto_WiFi_6_AP_205_B15_0624.pdf (168/200) 3437/4726

rather than rely on periodic beacons. This feature enables client devices to have much longer sleep states and results in significant power savings. In addition, the AP can control and schedule client TWTs to both manage contention in the network and accommodate delay-sensitive traffic. (Default: Disabled)

- **Broadcast Rate** — Allows a limit to be placed on the wireless bandwidth consumed by broadcast packets.
  - **Radio 2.4 Ghz** — Options: 5.5M, 6M, 9M, 11M, 12M, 18M, 24M, 36M, 48M, 54M; Default: 5.5M
  - **Radio 5 Ghz** — Options: 6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M; Default: 6M
- **RF Isolation** — When enabled, clients are isolated between different radio cards.
- **SSID Isolation** — When enabled, clients are isolated between different SSIDs on the same radio cards.

Wireless Networks — General Settings

Figure 44: Radio Settings (General Settings)



The following items are displayed in this section of the Wireless Settings page:

- **Status** — Enables or disables the wireless service on this VAP.

1Doc: Protocolo 1.943/2025 | Anexo: em_8967DB805AD5321B6628B0E_pt-br_Administrador_Web_EAP101_EAP105_Rev_1.0.4.pdf (169/200) 3439/4726

- **SSID** — The name of the basic service set provided by a Virtual Access Point (VAP) interface. Clients that want to connect to the network through the access point must set their SSID to the same as that of the access point's VAP interface. (Default: Edgecore5G-# (where # is 1-16) for 5 GHz, Edgecore2.4G-# (where # is 1-16) for 2.4 GHz; Range: 1-32 characters)

- **Site Survey** — Scans for all wireless networks that are broadcasting their SSID.

- **Broadcast** — The SSID can be broadcast at regular intervals so that wireless stations searching for a network connection can discover it. This allows wireless clients to dynamically discover and roam between WLANs. This feature also makes it easier for hackers to break into your home network. Because SSIDs are not encrypted, it is easy to grab one by snooping the WLAN looking for SSID broadcast messages coming from the AP. (Default: Enabled)

- **Local Configurable** — Enables the SSID to be user configurable when the system is operating in MSP mode (see "System Settings" on page 83). (Default: Disabled)

- **Client Isolation** — When enabled, wireless clients can talk to the LAN, and reach the Internet if such connection is available, but they cannot communicate with one another. (Default: Disabled)

- **Multicast-to-Unicast Conversion** — When enabled, the AP converts multicast traffic to unicast traffic and sends it to each associated client. This feature provides a network throughput enhancement, since the AP transmits multicast traffic at a low basic rate, whereas unicast traffic can be transmitted at HT, VHT, or HE rates.

- **Max Clients** — The maximum number of clients that can associate to this SSID at the same time. (Default: 127; Range: 1-256)

- **Minimum signal allowed** — Only allows clients to connect to the radio interface if their signal strength (RSSI) is equal or greater than the specified value. Setting the value to -100 disables this feature. Clients already connected are checked periodically. (Range: -1 to -100; Default: -100)

  This forces clients to associate with an AP that has a better signal strength (also called assisted roaming). Suggested value is -70 to -80 depending on access point density and coverage.

- **Idle Timeout (sec)** — The AP disconnects a client when there is no activity for the configured amount of time. (Default: 300 seconds; Range: 60-60000 seconds)

- **Device OS Blacklist** — Denies access to the SSID from client devices with either Android, iOS/macOS, or Windows operating systems. Set to ON to prevent a client OS from connecting to the SSID. Set to OFF to allow a client OS to connect to the SSID.

1Doc: Protocolo 1.943/2025 | Anexo: em_8907_D8059_D8532_B8628_Edgecore_Administrador_Processo_Aquisitivo_029_2025_Anexo_WiFi_6_AP2125_Rev_0624.pdf (170/200) 3450/4726

Wireless Networks — Security Settings

Figure 45: Wireless Security Settings

The following items are displayed in this section of the Wireless Settings page:

- **Method** — Sets the wireless security method for each VAP, including association mode, encryption, and authentication. (Default: WPA2-PSK)
  - **No Security** — The VAP broadcasts a beacon signal including the configured SSID. Wireless clients with an SSID setting of "any" can read the SSID from the beacon and automatically set their SSID to allow immediate connection.
  - **WPA-PSK** — For enterprise deployment, WPA requires a RADIUS authentication server to be configured on the wired network. However, for small office networks that may not have the resources to configure and maintain a RADIUS server, WPA provides a simple operating mode that uses just a pre-shared password for network access. The Pre-Shared Key mode uses a common password for user authentication that is manually entered on the access point and all wireless clients. The PSK mode uses the same TKIP packet encryption and key management as WPA in the enterprise, providing a robust and manageable alternative for small networks.
    - **Encryption** — Data encryption uses one of the following methods:
      - **CCMP (AES)** — AES-CCMP is used as the multicast encryption cipher. AES-CCMP is the standard encryption cipher required for WPA2. (This is the default setting.)
      - **Auto: TKIP + CCMP (AES)** — The encryption method used by the client is discovered by the access point.
    - **Key Method** — Uses one of the following PSK methods:
      - **Single PSK** — Enables the entry of a single PSK key.
        - **Key** — WPA is used to encrypt data transmitted between wireless clients and the VAP. WPA uses static shared keys (fixed-length hexadecimal or alphanumeric strings) that are manually distributed to all clients that want to use the network.

1Doc: Protocolo 1.943/2025 | Anexo: em_8967D8805AD2E321B6028907E_pdf_Laticínios_Processo_Administrativo_029_2025_Anexo_WiFi_6_AP_2105_Base_624.pdf (174/200) 3450/4726

String length must be 8 to 63 ASCII characters (letters and numbers). No special characters are allowed.

- **Multiple PSK** —Enables the entry of multiple PSK keys. Up to 128 keys can be configured.

  - **Multiple Keys** — Enter multiple keys, one per line. Entering a key with a specific MAC address limits the key for use by a single client. Entering a key without a MAC address enables the key to be used by all clients.

    Multiple keys are supported for WPA-PSK, WPA2-PSK, and WPA3 Personal Transition security.

  - **Dynamic PSK** — Enables the use of dynamic PSK keys that are periodically generated and updated by a RADIUS authentication server. The RADIUS server IP address, UDP port, and secret text string must be specified. (See "RADIUS Settings" below for details.)

    Dynamic keys are supported only for WPA2-PSK security.

- **WPA2-PSK** — Clients using WPA2 with a Pre-shared Key are accepted for authentication.

  WPA was introduced as an interim solution for the vulnerability of WEP pending the ratification of the IEEE 802.11i wireless security standard. In effect, the WPA security features are a subset of the 802.11i standard. WPA2 includes the now ratified 802.11i standard, but also offers backward compatibility with WPA. Therefore, WPA2 includes the same 802.1X and PSK modes of operation and support for TKIP encryption.

  Refer to WPA-PSK for a description of encryption methods and the key.

- **WPA-EAP** — WPA employs a combination of several technologies to provide an enhanced security solution for 802.11 wireless networks. A RADIUS server is used for authentication, and can also be used for accounting.

  Refer to WPA-PSK for a description of encryption methods.

- **RADIUS Settings** — A RADIUS server must be specified for the access point to implement IEEE 802.1X network access control and Wi-Fi Protected Access (WPA) wireless security.

  In addition, you can configure a RADIUS Accounting server to receive user-session accounting information from the access point. RADIUS Accounting can be used to provide valuable information on user activity in the network.

Note: This guide assumes that you have already configured RADIUS server(s) to support the access point. Configuration of RADIUS server software is beyond the

1Doc: Protocolo 1.943/2025 | Anexo: em_8967:D8059D2E821B6628907:esso_Laranjeiras_029_2025_Anexo_WiFi_6_AP_205_B15_0624.pdf (173/200) 1452/4726

scope of this guide, refer to the documentation provided with the RADIUS server software.

- **Radius Auth Server** — Specifies the IP address or host name of the RADIUS authentication server.
- **Radius Auth Port** — The UDP port number used by the RADIUS server for authentication messages. (Range: 1024-65535; Default: 1812)
- **Radius Auth Secret** — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS authentication server. Do not use blank spaces in the string. (Maximum length: 255 characters)
- **NAS ID** — The RADIUS NAS identifier for the SSID interface This value must be between 1 and 48 characters long.
- **Backup Radius Auth** — Enables the support of a backup RADIUS authentication server.
  - **Radius Auth Server** — Specifies the IP address or host name of the backup RADIUS authentication server.
  - **Radius Auth Port** — The UDP port number used by the backup RADIUS server for authentication messages. (Range: 1024-65535; Default: 1812)
  - **Radius Auth Secret** — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the backup RADIUS authentication server. Do not use blank spaces in the string. (Maximum length: 200 characters)
- **Use Radius Accounting** — Enables the support of a RADIUS accounting server.
  - **Acct Server** — Specifies the IP address or host name of the RADIUS accounting server.
  - **Acct Port** — The UDP port number used by the RADIUS server for accounting messages. (Range: 1024-65535; Default: 1813)
  - **Acct Secret** — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS accounting server. Do not use blank spaces in the string. (Maximum length: 200 characters)

1Doc: Protocolo 1.943/2025 | Anexo: em_8967:D8059D2E821B6628907:esso_Laranjeiras_029_2025_Anexo_WiFi_6_AP_205_Lite_624.pdf (176/200) 3452/4726

- **Acct Interim Interval** — The time (in seconds) between each accounting update sent to the server. (Range: 60-600 seconds; Default: 60 seconds)

- **WPA2-EAP** — WPA was introduced as an interim solution for the vulnerability of WEP pending the ratification of the IEEE 802.11i wireless security standard. In effect, the WPA security features are a subset of the 802.11i standard. WPA2 includes the now ratified 802.11i standard, but also offers backward compatibility with WPA. Therefore, WPA2 includes the same 802.1X and PSK modes of operation and support for TKIP encryption.

  A RADIUS server is used for authentication, and can also be used to accounting.

  Refer to WPA-PSK for a description of encryption methods.

  Refer to WPA-EAP for a information on configuring the RADIUS server.

- **WPA3 Personal** — Clients using WPA3 with Simultaneous Authentication of Equals (SAE) are accepted for authentication.

  WPA3 provides more robust password-based authentication called Simultaneous Authentication of Equals (SAE), which replaces Pre-Share Key (PSK) in WPA2-Personal. This technology prevents offline dictionary attacks so that data traffic can be transmitted securely.

- **WPA3 Personal Transition** — Clients using WPA3 with SAE or clients using WPA2 with PSK are accepted for authentication. The AP negotiates the supported authentication and encryption with each client before allowing access to the network.

- **WPA3 Enterprise** — An enhanced version of WPA2-EAP security that uses more robust encryption. Clients must support one of the stronger WPA3 encryption options and use Protected Management Frames (PMF) to be able to access the network. The use of IEEE 802.1X network access control and a RADIUS server is required.

  Refer to RADIUS Settings above for information on RADIUS configuration.

- **WPA3 Enterprise Transition** — Allows WPA3 and WPA2 clients to access the network. Encryption options and the use of Protected Management Frames (PMF) are negotiated with each client before allowing access to the network.

  Refer to RADIUS Settings above for information on RADIUS configuration.

- **WPA3 Enterprise 192-bit** — WPA3 Enterprise security uses a standard 128-bit encryption. For a network handling more sensitive data, there is an option to use 192-bit encryption for additional protection.

1Doc: Protocolo 1.943/2025 | Anexo: em_8967D8805D2E821B6628F6E_Laudo_Administrativo_029_2025_Anexo_WiFi_6_AP_025_Rev_01_pdf (174/200) 1453/4726

Refer to RADIUS Settings above for information on RADIUS configuration.

- **OWE** — Opportunistic Wireless Encryption (OWE) is the WPA3 open network security that allows users of public Wi-Fi networks to gain secure access without using a password. OWE provides individual encryption of data communications between the AP and each client, but does not provide authentication of user identities.

- **PMF** — Protected Management Frames (PMF) provide WPA2/WPA3 security for unicast and multicast management frames between the AP and clients. The "Optional" setting allows clients that do not support PMF to access the network. The "Mandatory" setting allows only clients that support PMF to access the network. (Default: Optional)

- **802.11k** — Provides clients with information on neighbor APs when roaming. As a client is about to roam from an AP, it sends a request for a "Neighbor Report" that includes a list of available APs and associated information. The client can then quickly identify the best AP to which it can roam without having to scan all channels. (Default: Disabled)

- **802.11r** — Provides a method for fast transition roaming between APs. Before clients roam to a new AP, the initial handshake and encryption calculations are performed in advance, which results in a fast hand off without the need for re-authentication. (Default: Disabled)

- **802.11v** — Provides information to associated clients that facilitates the overall improvement of the wireless network. Also helps clients to improve battery life by setting the idle period. (Default: Disabled)

- **Radius MAC Auth** — The MAC address of the associating station is sent to a configured RADIUS server for authentication. (Default: Disabled)

- **Dynamic Authorization** — The Dynamic Authorization Extensions (DAE) to RADIUS enable a server to disconnect or change the authorization of clients that are already connected to the network. (Default: Disabled)

  - **DAE Port** — The UDP port number to use for DAE messages. (Default: 3799)

  - **DAE Client** — Specifies the IPv4 address of the RADIUS server.

  - **DAE Secret** — The shared text string used to encrypt DAE messages between the access point and the RADIUS server.

- **Access Control List** — Wireless clients can be authenticated for network access by checking their MAC address against the local database configured on the access point. (Default: OFF)

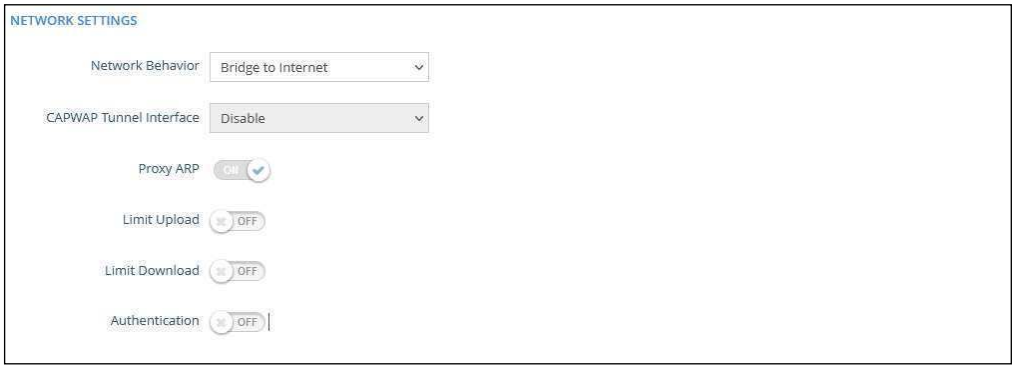
  - **Policy** — The MAC list can be configured to either allow or deny network access to specified clients. (Default: Allow all MACs on list)

1Doc: Protocolo 1.943/2025 | Anexo: em_8907D8805AD5821B6628907E5D_Laticínios_Processo_Licitatório_029_2025_Anexo_WiFi_6_AP205_B15_0624.pdf (178/200) 3455/4726

- **Filtered MACs** — List of client MAC addresses. Up to 512 MAC addresses can be configured.

Wireless Networks — Network Settings

Figure 46: Wireless Network Settings



The following items are displayed in this section of the Wireless Settings page:

- **Network Behavior** — One of the following connection methods must be specified. (Default: Route to Internet)
  - **Bridge to Internet** — Configures an interface as attached to the WAN. Traffic from this interface is directly bridged into the Internet. (See Figure 29, "Bridge to Internet", on page 48.)
  - **Route to Internet** — Configures an interface as a member of the LAN. Traffic from this interface is routed across the access point and out through an interface which is bridged to the Internet. (See Figure 30, "Route to Internet", on page 48.)
    - **Network Name** — The network to be routed. The default is "Default local network" as displayed under LAN Settings – Local Network.
  - **Add to Guest Network** — This interface can only support the guest network.
  - **Hotspot Controlled** — This interface can only support hotspot services.
    - **Configure Hotspot** — Opens Hotspot Settings page.
    - **Walled Garden** — Configures the Walled Garden list on the Hotspot Settings page.
  - **VLAN Tag Traffic** — Tags any packets passing from this VAP (virtual access point) to the associated Ethernet port with a VLAN ID configured under "VLAN Settings" on page 80.
    - **VLAN Id** — Selects the configured VLAN ID with which to tag the VAP traffic.

1Doc: Protocolo 1.943/2025 | Anexo: em_8967D8805D2E821B6628B0E_pt-br_Laticínios_029_2025_Assessoria_Técnica_Wi6_AP_2025_Rev1_634.pdf (176/200) 3456/4726

- **VLAN Settings** — Opens the VLAN Settings page.

- **Dynamic VLAN** — The RADIUS server provides the access point with the user VLAN information. The access point assigns the associated user to the related VLAN.

  - **Default VLAN Behavior** — Specifies the behavior (Accept or Reject) when a client's VLAN ID is not defined on the RADIUS server. The default setting is Reject.

    - **Reject** — A client cannot connect to the SSID when the client's VLAN ID is not defined on the RADIUS server.

    - **Accept** — A client can connect to the SSID with an assigned or untagged VLAN ID when the client's VLAN ID is not defined on the RADIUS server.

- **CAPWAP Tunnel Interface** — When the AP system management is set to EWS-Series Controller mode (see "System Settings" on page 83), the CAPWAP (Control And Provisioning of Wireless Access Points) protocol tunnel mode can be configured. The options are "Disable," "Complete," or "Split." A Complete tunnel sends all management, authentication, and data traffic from the AP back to the controller. A Split tunnel only sends the management and authentication traffic to the controller. (Default: Disable)

- **Proxy ARP** — When Proxy ARP is enabled, the AP maintains its own ARP lookup table and replies to ARP requests on behalf of downstream stations, avoiding network inefficiencies. This feature is automatically enabled when client isolation is disabled, and disabled when client isolation is enabled. The feature cannot be configured manually. Proxy ARP is supported when the network behavior is "Bridge to Internet" or "VLAN Tag Traffic."

- **Limit Upload** — Enables rate limiting of traffic from the VAP interface as it is passed to the wired network. You can set a maximum rate in Kbytes per second. (Range: 256-10048576 Kbytes per second; Default: OFF)

- **Limit Download** — Enables rate limiting of traffic from the wired network as it is passed to the VAP interface. You can set a maximum rate in kbytes per second. (Range: 256-10048576 Kbytes per second; Default: OFF)

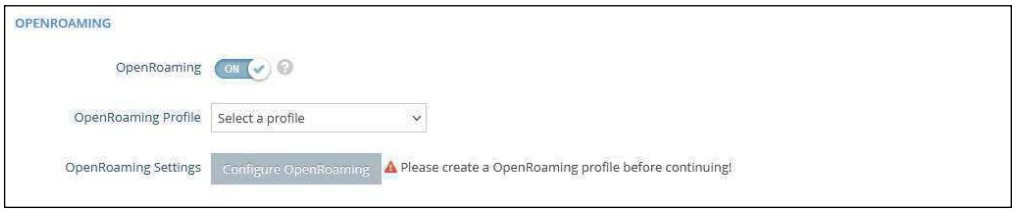
- **Authentication** — When the AP system management is set to ecCLOUD mode (see "System Settings" on page 83), this options authenticates the AP communications with the ecCLOUD controller. (Default: Disabled)

1Doc: Protocolo 1.943/2025 | Anexo: em_8967D8805AD2E821B6628907E_pt-br_Laticínios 029_2025_Assistência Técnica_EWS-AP2025_Rev1_624.pdf (187/200) 3456/4726

Wireless Networks — OpenRoaming

Available when WPA2-EAP security is selected, OpenRoaming (Hotspot 2.0) provides a standard for public-access Wi-Fi networks to support seamless roaming between wireless networks. A OpenRoaming AP advertises its public Wi-Fi capabilities and services so that clients can decide if they want to connect to the network.

Figure 47: OpenRoaming Settings



The following items are displayed in this section of the Wireless Settings page:

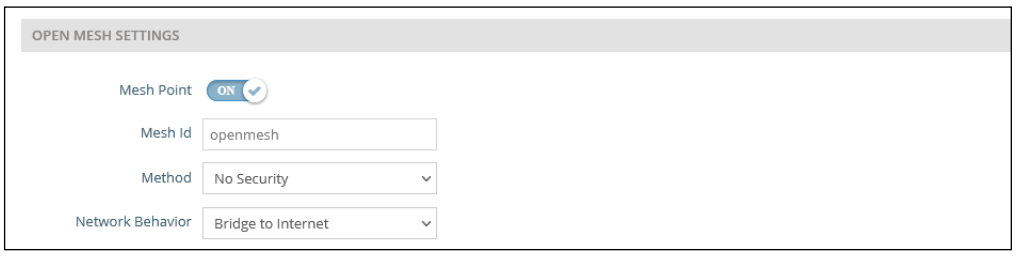
- **OpenRoaming** — Enables OpenRoaming when WPA2-EAP security is selected. (Default: Disabled)
- **OpenRoaming Profile** — Selects the profile to apply to the wireless network. See "OpenRoaming" on page 58 for profile configuration.
- **OpenRoaming Settings** — Click to access the OpenRoaming profile settings page. See "OpenRoaming" on page 58 for profile configuration.

Wireless Networks — Open Mesh Settings

Open Mesh is a network of interconnected node APs, of which only one has a wired connection to the network (and the Internet). The other AP nodes provide wireless links to each other and some support connections to wireless clients. The mesh network not only extends wireless connectivity over a greater distance, but also provides backup links should one node in the network fail.

When setting up an AP to be a node in a mesh network, select one radio interface (2.4 GHz or 5 GHz) and configure it to operate on a specific channel (do not select Auto).Set up other AP nodes to operate on the same radio interface, channel, and with the same SSID.

Figure 48: Open Mesh Settings



The following items are displayed in this section of the Wireless Settings page:

- **Mesh Point** — Enables Open Mesh support on the SSID interface.

1Doc: Protocolo 1.943/2025 | Anexo: em_8967D8805AD5821B6628B9CE_pt-br_Laticínios 029_2025_Assessoria_WiFi_6_AP_205_Base_624.pdf (178/200) 1458/4726

- **Mesh ID** — Name of the mesh network.
- **Method** — Security applied on Open Mesh links.
  - **No Security** — None.
  - **WPA3-Personal** — Uses WPA3 with Simultaneous Authentication of Equals (SAE) on mesh links to other APs.
- **Network Behavior** — One of the following connection methods must be specified. (Default: Route to Internet)
  - **Bridge to Internet** — Configures an interface as attached to the WAN. Traffic from this interface is directly bridged into the Internet. (See Figure 29, "Bridge to Internet", on page 48.)
  - **Route to Internet** — Configures an interface as a member of the LAN. Traffic from this interface is routed across the access point and out through an interface which is bridged to the Internet. (See Figure 30, "Route to Internet", on page 48.)
    - **Network Name** — The network to be routed. The default is "Default local network" as displayed under LAN Settings – Local Network.

Wireless Networks — Advanced Radio Settings

Figure 49: Advanced Radio Settings

The following items are displayed in this section of the Wireless Settings page:

- **Tx Power** — Adjusts the power of the radio signals transmitted from the access point. The higher the transmission power, the farther the transmission range. Power selection is not just a trade off between coverage area and maximum supported clients. You also have to ensure that high-power signals do not interfere with the operation of other radio devices in the service area. (The range of power settings and defaults are dependent on the AP model and the Country setting.)
- **SGI** — Enables the Short Guard Interval (SGI) in the following 802.11 modes:
  5 GHz radio; 802.11a, 802.11a+ n, 802.11ac+a+n.
  2.4 GHz radio; 802.11 b g+ n.

  The 802.11n draft specifies two guard intervals: 400ns (short) and 800ns (long). Support of the 400ns Short Guard Interval is optional for transmit and receive. The purpose of a guard interval is to introduce immunity to

1Doc: Protocolo 1.943/2025 | Anexo: em_8967_Deliberacao_Gestao_Administrativa_029_2025_Anexo_WiFi_6_AP_205_Belo_Horizonte_MG.pdf (79/200) 1459/4726

propagation delays, echoes, and reflections to which digital data is normally very sensitive. Enabling SGI sets it to 400ns. (Default: Disabled)

VLAN Settings

VLANs (virtual local area networks) are turned off by default. If turned on they will automatically tag any packets passed to the LAN port from the relevant VAP (virtual access point).

The access point can employ VLAN tagging to control access to network resources and increase security. VLANs separate traffic passing between the access point, associated clients, and the wired network. You can create up to 16 VLAN tagged networks.

Note the following points about the access point's VLAN support:

- If an Ethernet LAN port on the access point is assigned a VLAN ID, any traffic entering that port must be also tagged with the same VLAN ID.
- Wireless clients associated to the access point can be assigned to a VLAN. Wireless clients are assigned to the VLAN for the VAP interface with which they are associated. The access point only allows traffic tagged with correct VLAN IDs to be forwarded to associated clients on each VAP interface.
- When VLAN support is enabled on the access point, traffic passed to the wired network is tagged with the appropriate VLAN ID. When an Ethernet port on the access point is configured as a VLAN member, traffic received from the wired network must also be tagged with the same VLAN ID. Received traffic that has an unknown VLAN ID or no VLAN tag is dropped.
- When VLAN support is disabled, the access point does not tag traffic passed to the wired network and ignores the VLAN tags on any received frames.
- Network IP range conflict detection and resolution — The AP has two built-in local networks - one "main" network, and the more secure "guest" network. By default, the subnet ranges of these networks is set to 192.168.2.1 and 192.168.3.1, respectively.

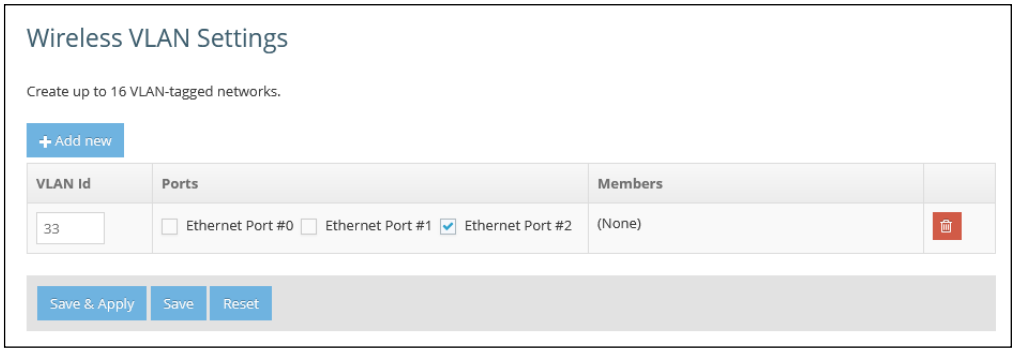
  If your network is already configured to use one of these subnets, when you plug in your network cable to the WAN port of your AP, there would normally be an IP conflict in the local AP's network and your upstream network.

  However, if your WAN subnet conflicts with any of the local networks (even the custom ones you create), the AP will automatically change the subnet of the local network.

1Doc: Protocolo 1.943/2025 | Anexo: em_8967D8805D2E821B6628F0E_Gestão_Laranjeiras_029_2025_Assessoria_Técnica_WiFi_6_AP_205_Rede_624.pdf (180/200) 3469/4726

Note: Before enabling VLAN tagging on the access point, be sure to configure the attached network switch port to support tagged VLAN frames for the VLAN IDs configured on the access point. Otherwise, connectivity to the access point will be lost when you enable the VLAN feature.

Figure 50: Configuring VLANs



The following items are displayed on this page:

- **VLAN ID** — A VLAN identifier to be assigned. (Range: 2-4094) (VLANs 1 is reserved for internal use.)
- **Ports** — The Ethernet ports assigned to the specified VLAN.
- **Members** — The SSID of a VAP configured to be a member of the specified VLAN. This option is configured under Radio Settings (Network Settings – Network Behavior).

1Doc: Protocolo 1.943/2025 | Anexo: em_8967DB805AD2E82BA6289BCE5D_Manual_Administrador_Access_Point_Wi_Fi_6_AP2025_Base_Web_pdf (184/200) 3460/4726

5 System Settings

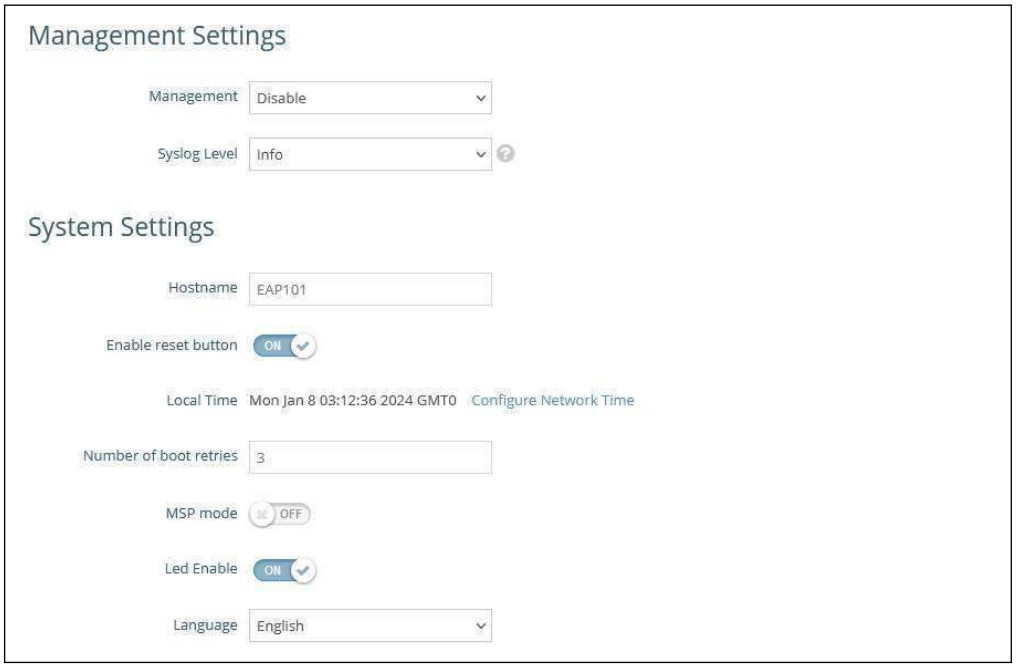
This chapter describes maintenance settings on the access point. It includes the following sections:

1Doc: Protocolo 1.943/2025 | Anexo: em_8907.D88059.D25321.B68289.T_gestor_Laranjeiras_029_2025_Anexo_WiFi_6_AP_205_Site_624.pdf (182/200) 1462/4746

System Settings

The System Settings page can be used to enable the AP to be managed from the Edgecore ecCLOUD controller or EWS-Series Controller, and configure general descriptive information about the AP.

Figure 51: System Settings



The following items are displayed on this page:

- **Management** — Set to "ecCLOUD" to manage this AP from the Edgecore ecCLOUD controller. Set to "EWS-Series Controller" to manage this AP from an Edgecore EWS-Series controller in the local network. Set to disable to manage the AP through the web interface in a stand-alone mode.
  - **ecCLOUD** — When selected, the following parameters are displayed:
    - **Controller URL** — Provides a URL link to the Edgecore ecCLOUD controller management site.
    - **Enable agent** — Enables the AP to be managed from the ecCLOUD controller.
      - **Registration URL** — Specifies the URL for device registration.
    - **Log Level** — Adjusts the system log level for the ecCLOUD daemon (mgmtd). The default value is Info. The standard ranking of log levels is as follows: Trace < Debug < Info < Warn < Error.

1Doc: Protocolo 1.943/2025 | Anexo: em_8967_Datasheet_Edgecore_Administração_Acesso_Wi-Fi_EAP101_Rev_1.0_pdf (186/204) 1462/4726

- **EWS-Series Controller** — When selected, the following parameters are displayed:
  - **CAPWAP** — Enables CAPWAP (Control And Provisioning of Wireless Access Points) protocol tunnel mode.
  - **DNS SRV Discovery** — The AP uses DNS server records to discover the EWS controller to which it can send a CAPWAP join request.
    - **Domain Name Suffix** — Specifies the domain suffix of the controller.
  - **DHCP Option Discovery** — The AP uses the DHCP server to obtain an IP address in the same subnet as the EWS controller, which it can then discover and send a CAPWAP join request.
  - **Broadcast Discovery** — The AP sends broadcast requests to discover the EWS controller in the same subnet.
  - **Multicast Discovery** — The AP sends multicast discover packets across the network to find the EWS controller. This option requires routing paths to be properly configured in the network.
  - **Static Discovery** — Provides a manual method to reach an EWS controller by entering IP addresses that the AP uses to send a CAPWAP join request.

- **Syslog Level** — Limits system log messages based on severity. The standard ranking of log levels is as follows: Debug < Info < Notice < Warning < Error < Critical < Alert < Emergency. (Default: Info)
- **Hostname** — An alias for the AP, enabling the device to be uniquely identified on the network. (Default: EAP101; Range: 1-63 ASCII characters. Only accepts A-Z, a-z, 0-9, and dash "-".)
- **Enable Reset Button** — Enables the AP's hardware reset button. (Default: Enabled)
- **Local Time** — The local time, given as day of week, month, time, year.
- **Number of boot retries** — The maximum number of bootup retries before switching to the next boot bank. (Range: 1-254; Default: 3)
- **MSP Mode** — Enables the Managed Service Provider (MSP) mode that prevents end-users from accessing and modifying most device settings from user-defined user accounts. Management access from "root" and "admin" accounts still provide full access to all device settings. (Default: Disabled)

  With MSP mode enabled, service providers have the option of making specific wireless SSID settings available for user configuration by enabling the "Local

1Doc: Protocolo 1.943/2025 | Anexo: em_8967DB805AD5821B6628B0E_pdf_Laticínios_029_2025_Anexo_WiFi_6_EAP_105_B15_0624.pdf (184/200) 1463/4726

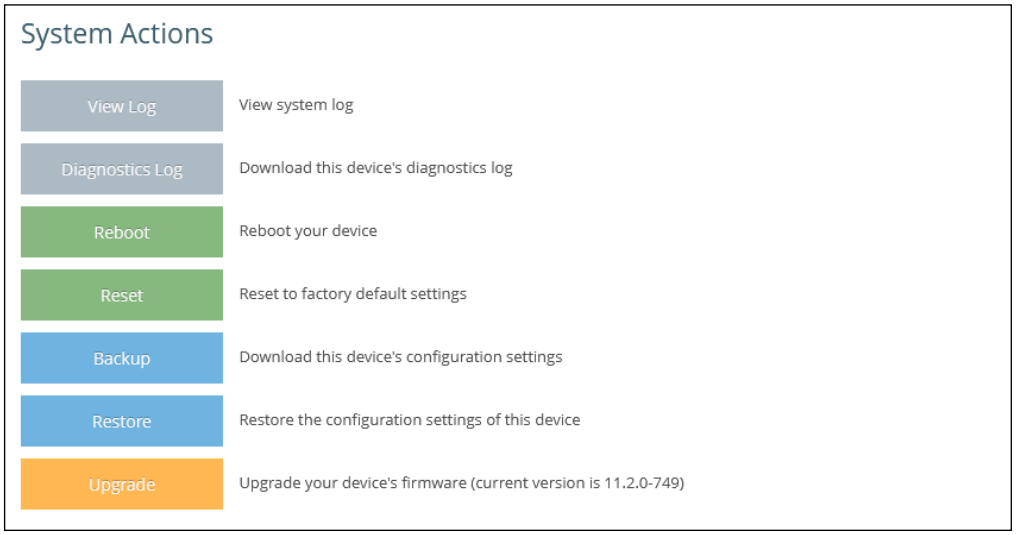
Configurable" setting. See "Wireless Networks — General Settings" on page 69.

- **LED Enable** — Enables the LED indicators on the AP. (Default: Enabled)
- **Language** — Selects the web interface language. (Options: English, Japanese; Default: English)

Maintenance

The Maintenance page supports general maintenance tasks including displaying the system log, downloading a diagnostics log, rebooting the device, restoring factory defaults, backing up or restoring configuration settings, and upgrading firmware.

Figure 52: Maintenance

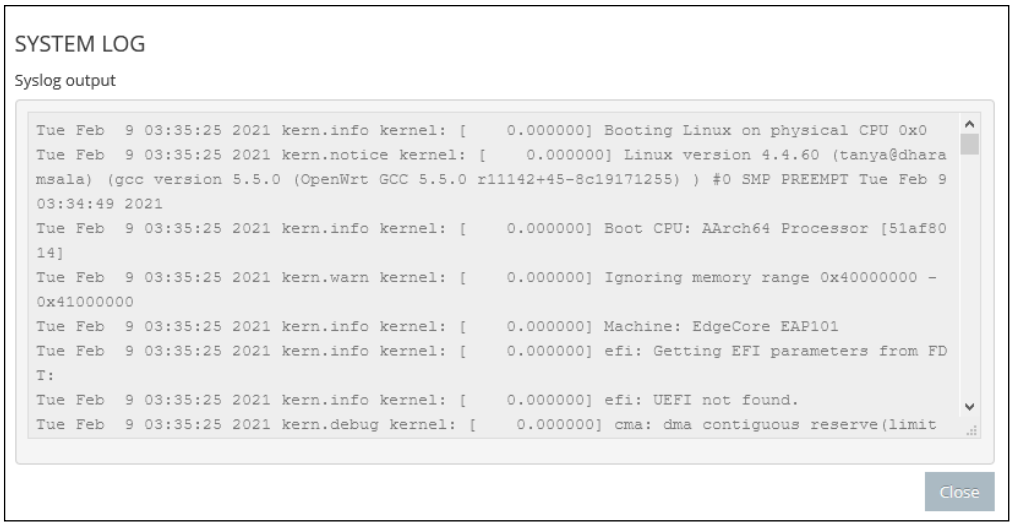


1Doc: Protocolo 1.943/2025 | Anexo: em_8967D8805AD5E321B6628F0CE_Laticínio029_2025_Anexo_WI_629_2025_Baixe_624.pdf (188/200) 3465/4726

Displaying System Logs

The access point saves event and error messages to a local system log database. The log messages include the date and time, device name, message type, and message details.

Figure 53: System Log



Downloading the Diagnostics Log

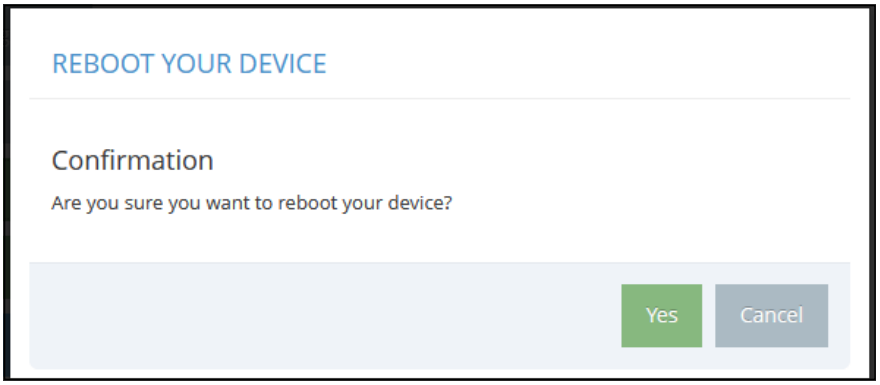
Click "Diagnostics Log" to download the log file to the management workstation. In Windows, a GNU Zip (*.tar.gz) file is stored in the Downloads folder.

The diagnostics log file contains information that can help Edgecore resolve technical issues with the AP.

Rebooting the Access Point

The Reboot page allows you to reboot the access point.

Figure 54: Rebooting the Access Point

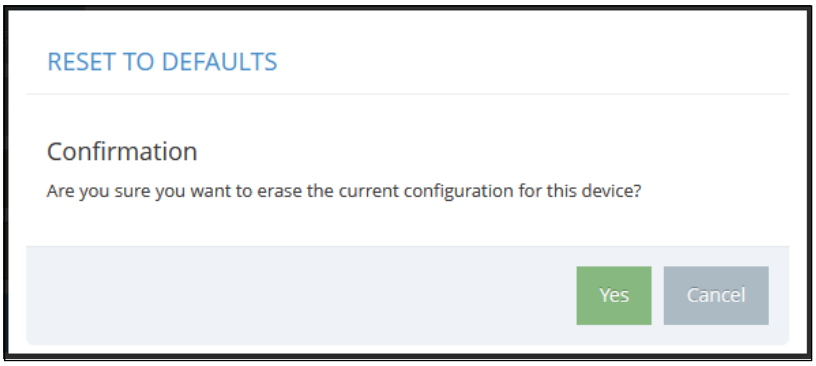


1Doc: Protocolo 1.943/2025 | Anexo: em_8967D8805AD5321B6628B9CE_Gestão_Laranjeiras_029_2025_Aquisição_Wi-Fi_6_AP_025_Item_024.pdf (86/200) 1466/4726

Resetting the Access Point

The Reset page allows you to reset the access point to the factory defaults. Note that all user configured information will be lost. You will have to re-enter the default user name and password to re-gain management access to this device.

Figure 55: Resetting to Defaults



Note: It is also possible to reboot or reset the access point by inserting a pin in the pin hole labeled "Reset" on the connector panel of the access point and:

- give a quick press to reboot the access point;
- press and hold for 5 seconds to reset the access point to factory defaults.

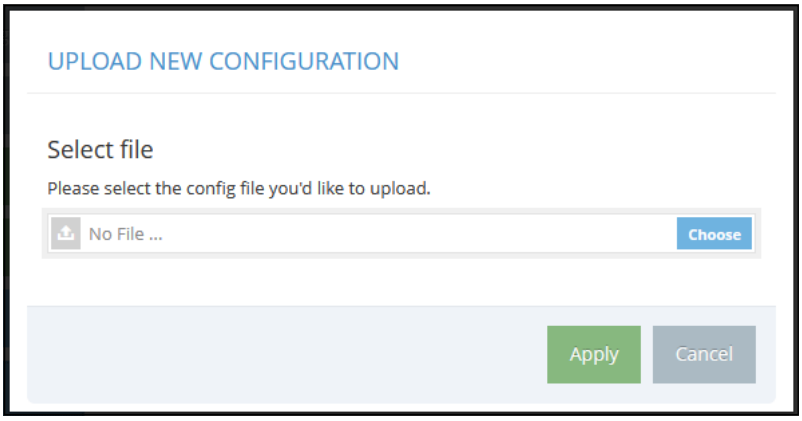
Backing Up Configuration Settings

The Backup function allows you to back up the access point's configuration to a management workstation. In Windows, a GNU Zip (*.tar.gz) file will be stored in the Downloads folder. This is a sample file name: backup-EAP101-2021-02-09.tar.gz

Restoring Configuration Settings

The Restore page allows you to upload configuration settings from a management workstation. The specified file must be one that was previously backed up from the access point.

Figure 56: Restoring Configuration Settings



1Doc: Protocolo 1.943/2025 | Anexo: em_8967DB805AD2E82B6628B9CE5D1A6F3E_Manual_Administrador_Access_Point_EAP101_Brazil_pt-br.pdf (187/200) 1466/4726

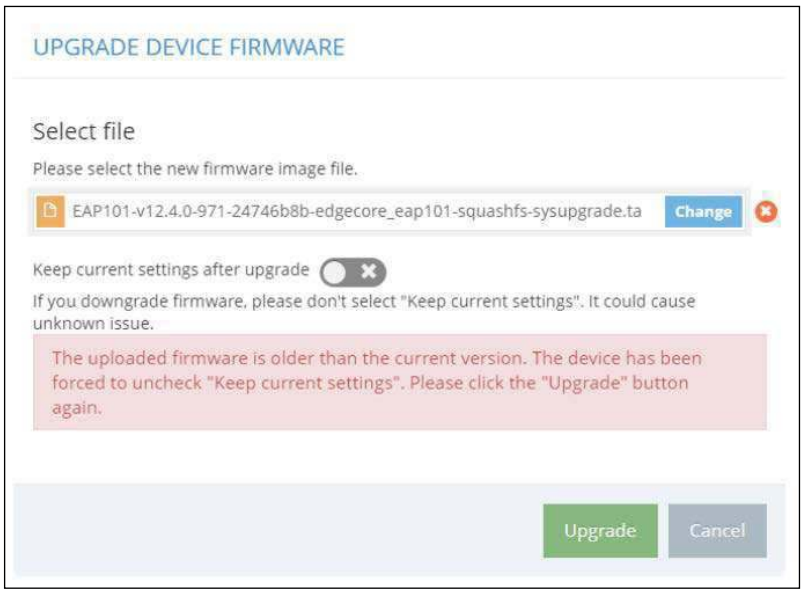
Upgrading Firmware

You can upgrade new access point software from a local file on the management workstation. New software may be provided periodically from Edgecore.

After upgrading new software, you must reboot the access point to implement the new code. Until a reboot occurs, the access point will continue to run the software it was using before the upgrade started. The access point supports dual software images, so if newly loaded software is corrupted, the alternate image will be used on the next reboot. Configuration settings are stored separately from the software, so the current settings will always be used for any new software. However, note that if the current configuration settings are corrupted, the system defaults will be used.

Note: If the uploaded firmware is older than the current version, the device forces the "Keep current settings after upgrade" option to unchecked.

Figure 57: Upgrading Firmware

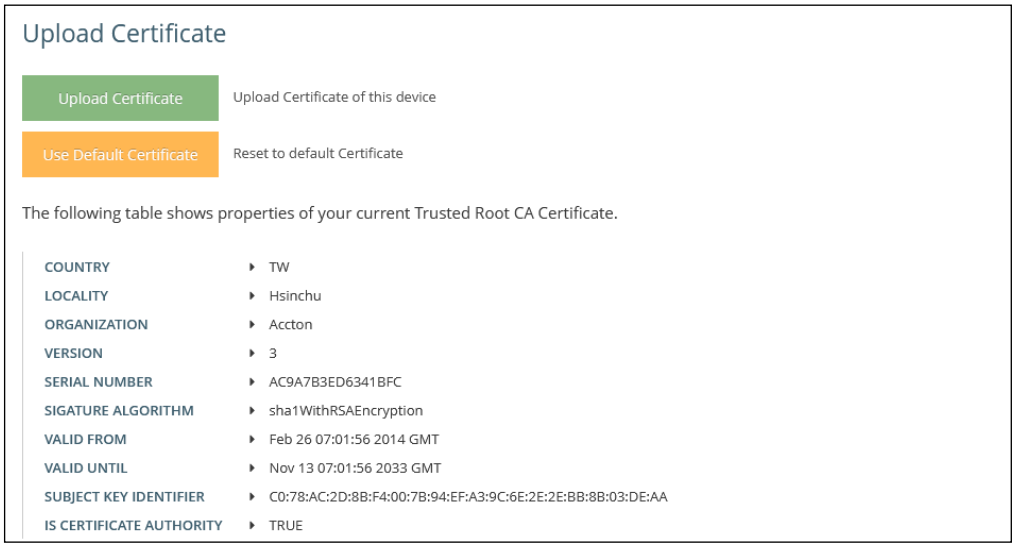


Upload Certificate

The Upload Certificate page allows you to upload a unique security certificate from a trusted certification authority for secure access (an encrypted connection) to a configured HTTPS captive portal. Alternatively, you can also reset to use the default certificate.

1Doc: Protocolo 1.943/2025 | Anexo: em_8967D8805AD5321B6628B9CE_Gestão_Laranjeiras_029_2025_Assinatura_Wi_629_2025_Rede_624.pdf (198/200) 1468/4726

Figure 58: Upload Certificate



The following items are displayed on this page:

- **Upload Certificate** — Click to upload a security certificate and private key from a trusted certification authority.
- **Use Default Certificate** — Click to reset to use the AP's default certificate.

User Accounts

The User Accounts page allows you to control management access to the AP based on manually configured user names and passwords.

Figure 59: User Accounts

The following items are displayed on this page:

- **Enabled** — Click to enable or disable the user account.
- **Username** — The name of the user. (Range: 1-32 ASCII characters. Only accepts A-Z, a-z, 0-9, period ".", underscore "_", and hyphen "-". Usernames cannot begin with a hyphen "-" or period ".".)

- **Password** — The user password. (Range: 6-20 ASCII characters, case sensitive, no special characters)

Services

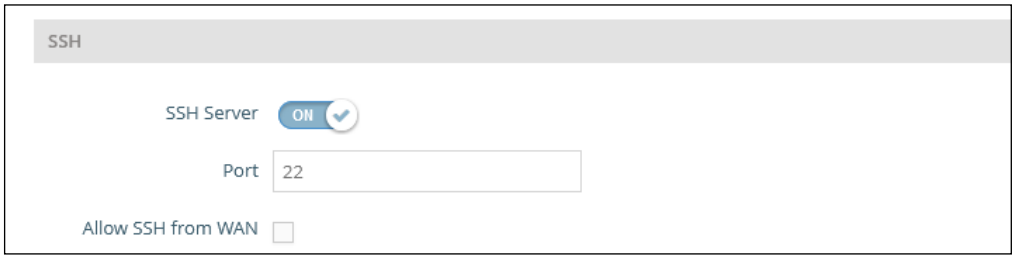
The Services page allows you to control SSH management access to the AP, configure NTP time servers, and configure iBeacon settings.

SSH

The Secure Shell (SSH) can act as a secure replacement for Telnet. The SSH protocol uses generated public keys to encrypt all data transfers passing between the access point and SSH-enabled management station clients and ensures that data traveling over the network arrives unaltered. Clients can then securely use the local user name and password for access authentication.

Note that SSH client software needs to be installed on the management station to access the access point for management via the SSH protocol.

Figure 60: SSH Settings



The following items are displayed on this page:

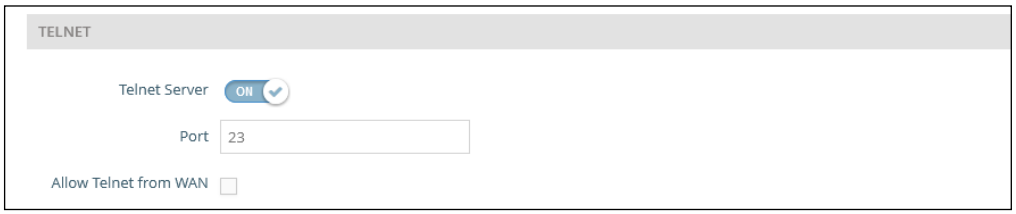
- **SSH Server** — Enables or disables SSH access to the access point. (Default: Enabled)
- **Port** — Sets the TCP port number for the SSH server on the access point. (Range: 1-65535; Default: 22)
- **Allow SSH from WAN** — Allows SSH management access from the WAN.

1Doc: Protocolo 1.943/2025 | Anexo: em_8967D8805AD5321B6628907... Laticínio... 029/2025... Anexo... WiFi_6_AP_2025_Rede_0624.pdf (190/200) 1479/4726

Telnet

Telnet is a remote management tool that can be used to configure the access point from anywhere in the network. However, note that Telnet is not secure from hostile attacks.

Figure 61: Telnet Server Settings



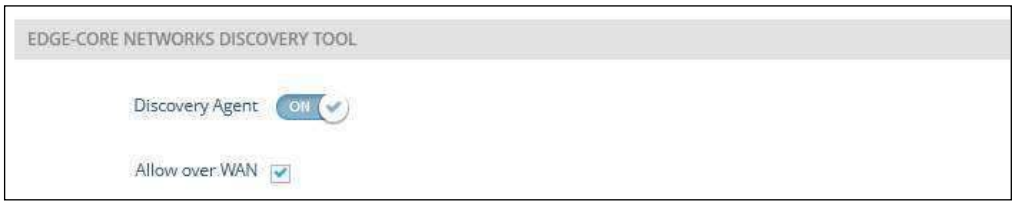
The following items are displayed on this page:

- **Telnet Server** — Enables or disables Telnet access to the access point. (Default: Enabled)
- **Port** — Sets the TCP port number for the Telnet server on the access point. (Range: 1-65535; Default: 23)
- **Allow Telnet from WAN** — Allows Telnet management access from the WAN.

Edgecore Networks Discovery Tool

The Discovery Tool agent enables the AP to find other Edgecore devices in the same Layer 2 network. See "Device Discovery" on page 100 to scan the network for devices.

Figure 62: Discovery Agent Settings



The following items are displayed on this page section:

- **Discovery Agent** — Enables the discovery agent. (Default: Enabled)
- **Allow over WAN** — Enables the discovery agent to operate over the port connected to the Internet source. (Default: Enabled)

Web Server

A Web browser provides the primary method of managing the access point. Both HTTP and HTTPS service can be accessed independently. If you enable HTTPS, you must indicate this in the URL: https://device:port_number]

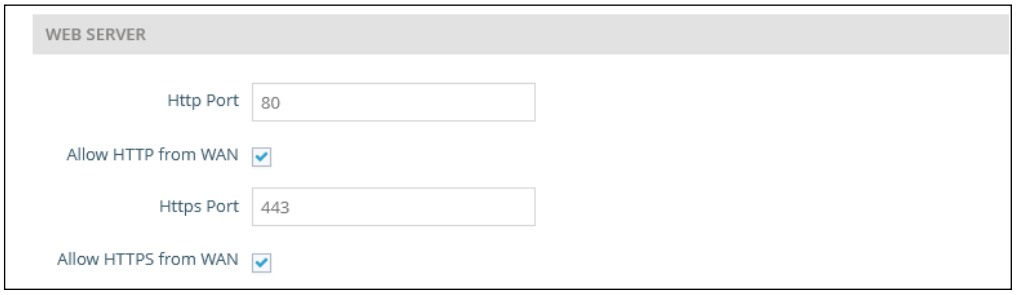
When you start HTTPS, the connection is established in this way:

- The client authenticates the server using the server's digital certificate.

1Doc: Protocolo 1.943/2025 | Anexo: em_8967DB805AD5821B6628B0E_pt-br_Laticínios 029_2025_Assistente Wi-Fi_EAP2105_Rev_0624.pdf (194/200) 1460/4726

- The client and server negotiate a set of security protocols to use for the connection.
- The client and server generate session keys for encrypting and decrypting data.
- The client and server establish a secure encrypted connection.
- A padlock icon should appear in the status bar for most browsers.

Figure 63: Web Server Settings



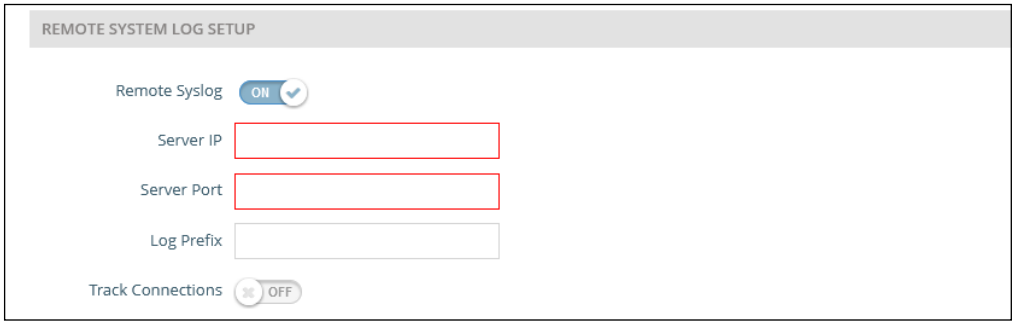
The following items are displayed on this page:

- **HTTP Port** — The TCP port to be used by the HTTP Web browser interface. (Range: 1-65535; Default: 80)
- **Allow HTTP from WAN** — Allows HTTP management access from the WAN.
- **HTTPS Port** — The TCP port to be used by the HTTPS Web browser interface. (Range: 1-65535; Default: 443)
- **Allow HTTPS from WAN** — Allows HTTPS management access from the WAN.

Remote System Log Setup

Use this feature to send log messages to a Syslog server.

Figure 64: Remote System Log Settings



The following items are displayed on this page:

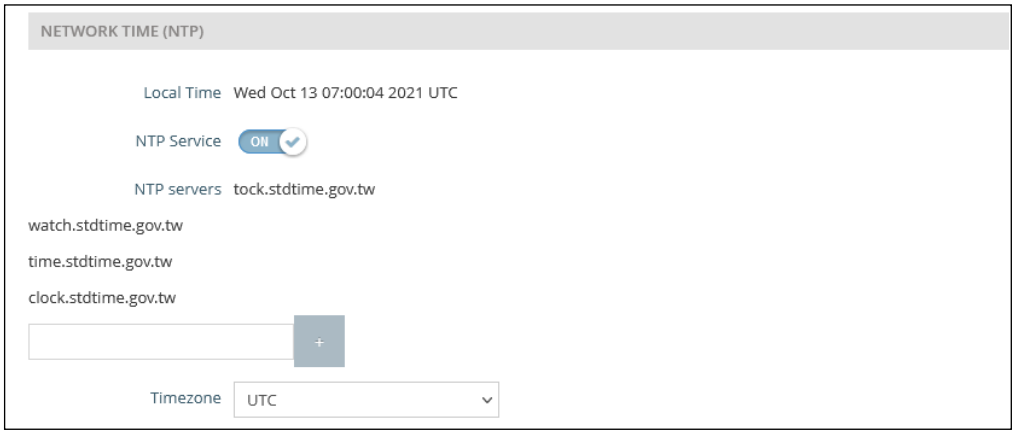
- **Remote Syslog** — Enables the logging of debug or error messages to the remote logging process. (Default: Disabled)
- **Server IP** — Specifies the IP address of a remote Syslog server that will be sent log messages.
- **Server Port** — Specifies the UDP port number used by the remote Syslog server. (Range: 1-65535)
- **Log Prefix** — Sets a prefix string for log messages sent to the specified server. The prefix can help with sorting messages on the server.
- **Track Connections** — Enables the inclusion of connection information such as source IP and port, destination IP and port in log messages.

Network Time

Network Time Protocol (NTP) allows the access point to set its internal clock based on periodic updates from a time server (SNTP or NTP). Maintaining an accurate time on the access point enables the system log to record meaningful dates and times for event entries. If the clock is not set, the access point will only record the time from the factory default set at the last bootup.

The access point acts as an NTP client, periodically sending time synchronization requests to specified time servers. The access point will attempt to poll each server in the configured sequence to receive a time update.

Figure 65: NTP Settings



The following items are displayed on this page:

- **Local Time** — Displays the local time as day of week, month, hour:minute:second, year, based on Universal Time Coordinates.
- **NTP Service** — Enables or disables sending of requests for time updates. (Default: Enabled)

1Doc: Protocolo 1.943/2025 | Anexo: em_8967DB805AD5821B6628B0E_pt-br_Laticínio 029_2025_Assistente Virtual_P2025_Rate_624.pdf (196/200) 1462/4726

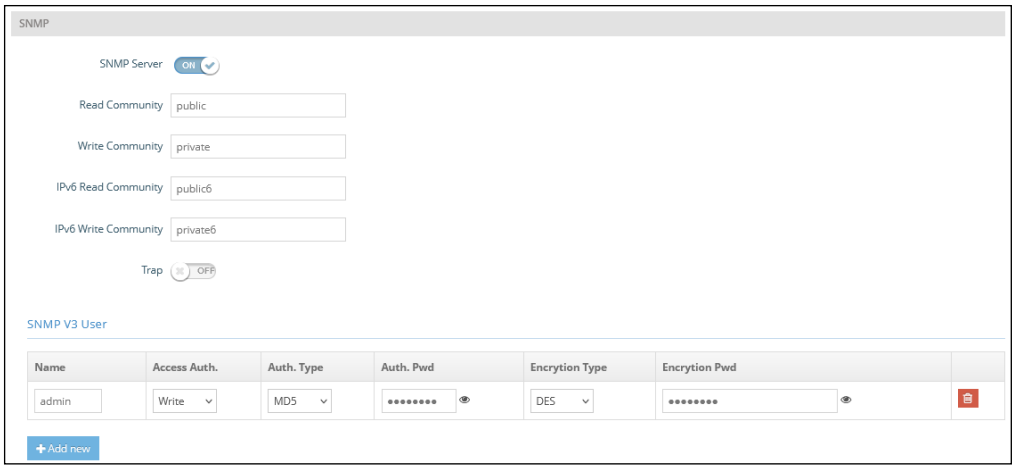
- **NTP Servers** — Sets the host names for time servers. The switch attempts to update the time from the first server, if this fails it attempts an update from the next server in the sequence. To configure additional servers, click the "+" button to open a new edit field.

- **Timezone** — To display a time corresponding to your local time, choose one of the predefined time zones from the scroll-down list.

SNMP

Simple Network Management Protocol (SNMP) is a communication protocol designed specifically for managing devices on a network. It is typically used to configure these devices for proper operation in a network environment, as well as to monitor them to evaluate performance or detect potential problems.

Figure 66: SNMP Settings



The following items are displayed on this page:

- **SNMP Server** — Enables or disables SNMP on the access point. (Default: Enabled)

- **Read Community** — A community string that acts like a password and permits read access to the access point's Management Information Base (MIB). (Range: 1-32 characters, case sensitive; Default: public)

- **Write Community** — A community string that acts like a password and permits write access to the access point's Management Information Base (MIB). (Range: 1-32 characters, case sensitive; Default: private)

- **IPv6 Read Community** — A community string for IPv6 read access to the access point's Management Information (MIB) database. (Range: 1-32 characters, case sensitive; Default: public6)

- **IPv6 Write Community** — A community string for IPv6 write access to the access point's Management Information (MIB) database. (Range: 1-32 characters, case sensitive; Default: private6)

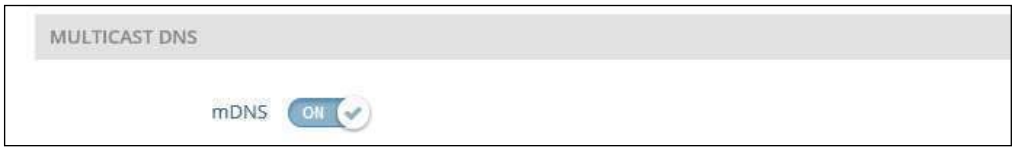
1Doc: Protocolo 1.943/2025 | Anexo: em_8967DB805AD5821B6628B0E_pt-br_Administrador_v2_2025_Assistente_Web_v2_2025_Base_0624.pdf (197 of 200) 1473/4726

- **Trap** — Enables the sending of SNMP trap messages to a specified server. The access point sends the following trap messages: cold start, warm start, link up, and link down. (Default: Disabled)
  - **Server IP** — Specifies the IP address of the SNMP trap server that will be sent trap messages.
- **SNMPv3 User** — SNMP protocol version 3 provides secure access by account authentication and data encryption. An SNMP v3 user can be defined by clicking the "Add new" button.
  - **Name** — The user name used to access the SNMP service.
  - **Access Auth** — Select the access permission as "Read" or "Write."
  - **Auth Type** — Select the hash algorithm for authentication.
  - **Auth Pwd** — Configure the password for authentication.
  - **Encryption Type** — Select the encryption algorithm for data packets.
  - **Encryption Pwd** — Configure the password for data encryption.

Multicast DNS

The multicast DNS (mDNS) protocol is a zero-configuration service to facilitate connections within a local networks.

Figure 67: Multicast DNS Settings



The following items are displayed on this page:

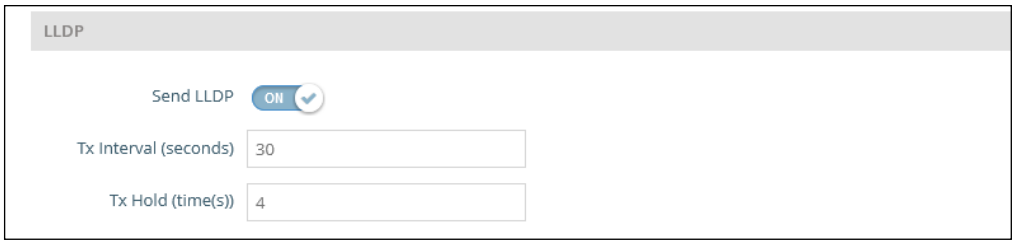
- **mDNS** — Enables or disables Multicast DNS on the access point. (Default: Enabled)

1Doc: Protocolo 1.943/2025 | Anexo: em_8967D8805AD5E821B6628907C_pt-br_Laticínios 029/2025 Assinatura Avista WI5 629P 025_Rate_0624.pdf (196/200) 1475/4726

LLDP

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices in a network. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device.

Figure 68: LLDP Settings



The following items are displayed on this page:

- **Send LLDP** — Enables the sending of LLDP advertisements about the AP to neighboring devices in the network. (Default: Disabled)
- **Tx Interval (seconds)** — Sets the periodic transmit interval for LLDP advertisements. (Range: 5-32768 seconds; Default: 30 seconds)
- **Tx Hold (time(s))** — Configures a time-to-live (TTL) value sent in the LLDP advertisements as shown in the formula below. (Range: 2-10; Default: 4)

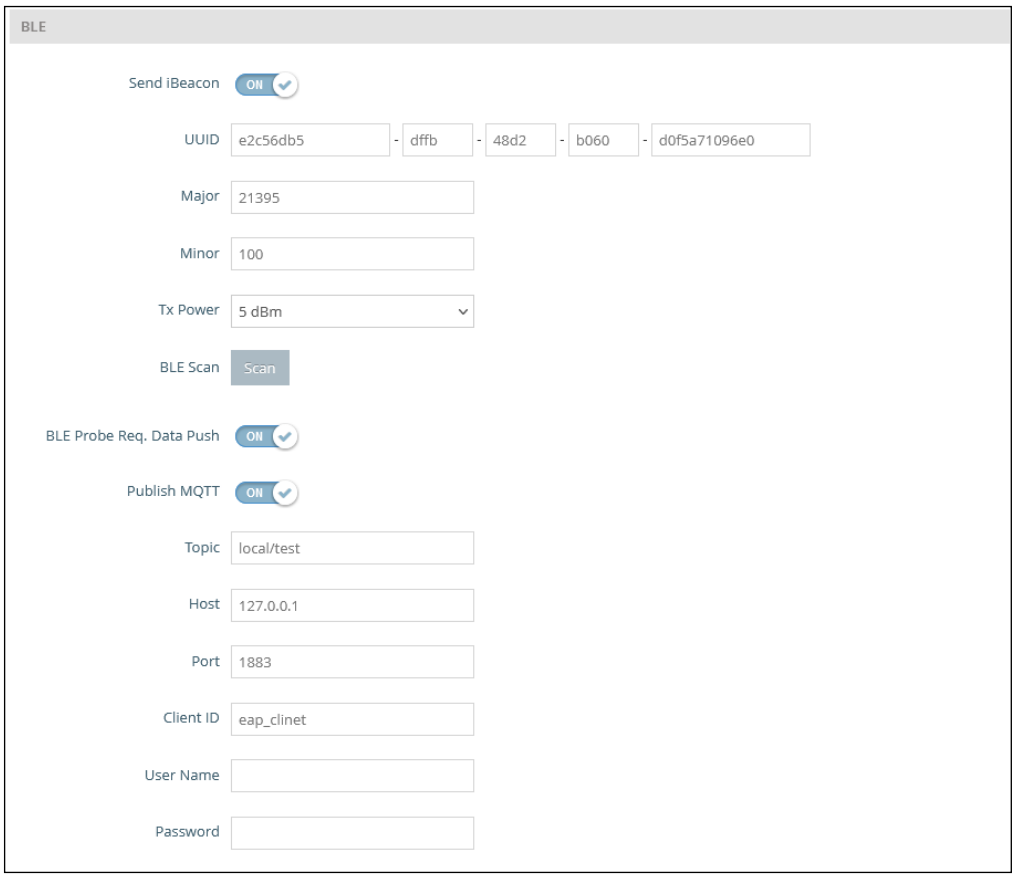
  The time-to-live tells the receiving LLDP agent how long to retain all information pertaining to the sending device if it does not transmit updates in a timely manner.

  The TTL in seconds is based on the following rule:
  minimum value ((Tx Interval * Tx Hold), or 65535)
  Therefore, the default TTL is 4*30 = 120 seconds.

1Doc: Protocolo 1.943/2025 | Anexo: em_8967:D8059D2E5321B6628906:esso_Laranjeiras_029/2025_Anexo_WiFi_6_AP_205_Rede_0624.pdf (196/200) 1476/4726

BLE The AP supports the iBeacon standard based on Bluetooth Low Energy (BLE). Devices with BLE Beacons can provide location-based services to BLE clients, such as phones, that can recognize the beacon advertisements, extract the provided information, and then take actions based on the content.

Figure 69: BLE Settings



The following items are displayed on this page:

- **Send iBeacon** — Enables iBeacon support on the AP. (Default: Enabled)
- **UUID** — The iBeacon Universally Unique Identifier that advertises the beacon service. The UUID contains 32 hexadecimal digits in five groups, separated by hyphens.
- **Major** — The iBeacon value that is used to identify a beacon group. (Range: 0-65535)
- **Minor** — The iBeacon value that is used to identify individual beacons within a group. (Range: 0-65535)
- **Tx Power** — Sets the BLE radio transmit power (supported only on EAP101 and EAP104). (Range: 5 dBm to -20 dBm; Default: 5 dBm)

1Doc: Protocolo 1.943/2025 | Anexo: em_8967DB805AD2E821B6628B0E_pt-br_Administrator_2025_05_29_15_24_25_Guia_do_Usuario_EAP225_Wi-Fi_6_AP_1.5.0.4.pdf (207/210) 1476/4726

- **BLE Scan** — (EAP101 and EAP104 only) Scans for all BLE devices, including these four types: EddyStone-UID, EddyStone-URL, EddyStone-TLM, and ibeacon.

Figure 70: BLE Scan

- **BLE Probe Req. Data Push** — Enables BLE Probe Request Data Push for the device. (EAP112 only.)
- **Publish MQTT** — Publishes pushed data as MQTT (Message Queuing Telemetry Transport) messages. (EAP112 only.)
  - **Topic** — The MQTT message topic name.
  - **Host** — The IP address of the MQTT server/broker.
  - **Port** — TCP port number.
  - **Client ID** — The identifier for this client device.
  - **User Name** — The client user name.
  - **Password** — The client password.

1Doc: Protocolo 1.943/2025 | Anexo: em_8967D8805AD5A21B6628F6E_pt-BR_Laticínio_2025_Assistência_Técnica_EAP225_Rede_Mesh_Guia_do_Usuário_v1.0_EAP225_Rede_Mesh_Guia_do_Usuário_v1.0.pdf (98 de 200) 1468/4726

Diagnostics

The Diagnostics page provides Ping, Traceroute, Nslookup, and Speed Test tools for troubleshooting connectivity problems.

Ping

Enter a hostname or IP address and click to run the ping tool.

Figure 71: Network Utilities - Ping

Traceroute

Enter a hostname or IP address and click to run the traceroute tool.

Figure 72: Network Utilities - Traceroute

Nslookup

Enter a hostname or IP address and click to run the Nslookup tool.

Figure 73: Network Utilities - Nslookup

Speed Test

Enter a hostname or IP address of a Netperf server to test the speed between the AP and server.

1Doc: Protocolo 1.943/2025 | Anexo: em_8967_Manual_Administrador_Access_Point_Corporativo_WiFi_6_AP2105_Base_v1.0.pdf (209/210) 1469/4726

Figure 74: Network Utilities - Speed Test

Device Discovery

The Device Discovery Tool provides a method for finding other Edgecore APs within the same Layer 2 network. To function, the Discovery Agent must be enabled (see "Edgecore Networks Discovery Tool" on page 91.

Click the Scan Network button to scan for devices.

Figure 75: Device Discovery Tool

Section III

Appendices

This section provides additional information and includes these items:

1Doc: Protocolo 1.943/2025 | Anexo: em1_04C7B8805AD2E821B662B8E_procuradoria_e_juridico_29_2025_15_0625.pdf (204/250) 3470/4726

A Troubleshooting

Problems Accessing the Management Interface

Table 1: Troubleshooting Chart

Symptom	Action
Cannot connect using a web browser	■ Be sure the AP is powered up. ■ Check network cabling between the management station and the AP. ■ Check that you have a valid network connection to the AP and that intermediate switch ports have not been disabled. ■ Be sure you have configured the AP with a valid IP address, subnet mask and default gateway. ■ Be sure the management station has an IP address in the same subnet as the AP's IP. ■ If you are trying to connect to the AP using a tagged VLAN group, your management station, and the ports connecting intermediate switches in the network, must be configured with the appropriate tag. ■ If you cannot connect using SSH, you may have exceeded the maximum number of concurrent SSH sessions permitted. Try connecting again at a later time.
Forgot or lost the password	■ Reset the AP to factory defaults using its Reset button.

Using System Logs

If a fault does occur, refer to the *Quick Start Guide* to ensure that the problem you encountered is actually caused by the AP. If the problem appears to be caused by the AP, follow these steps:

1. Repeat the sequence of commands or other actions that lead up to the error.
2. Make a list of the commands or circumstances that led to the fault. Also, make a list of any error messages displayed.
3. Record all relevant system settings.
4. Display the log file through the System > Maintenance page, and copy the information from the log file.
5. Download the Diagnostics Log to a file from the System > Maintenance page.

6. Contact Edgecore and send a detailed description of the problem, along with all of the information mentioned in the above steps.

1Doc: Protocolo 1.943/2025 | Anexo: em1_04C7B8805AD2E821B662B8E_pdf_Administração_de_Acesso_Autenticado_WiFi_6_29_2025_15_06_25.pdf (206/210) 1472/4726

1,Creation Road 3,
Hsinchu Science Park,
Hsinchu 30077, Taiwan, R.O.C.

Statement of Environmental Directives Compliance

Edgecore's Statement

We hereby declare that, as the date of this declaration, the products listed in this declaration are fully in compliance with following environmental laws, directives and regulations for their intended markets and applications to the best of our knowledge and belief. We acknowledge that this statement may have based on the analysis of the components and materials used in the manufacture of our products and/or supported by suppliers' furnished material declarations and/or the 3rd party test results provided by the suppliers. This is to certify that adequate information provided by the suppliers is available and accurate to the best of our knowledge.

We accept no duty to notify users of updates or changes to this declarations. We shall not be liable for any damages, direct or indirect, consequential or otherwise, suffered by users or third parties as a result of the user's reliance on information in this declaration that has been updates or changed.

Our compliance statements do not extend to, or apply to any product subjected to unintended contamination, misuse, neglect, accident, improper installation, or to use in violation of instructions.

Product Environmental Compliance Status

Attachment	Regulation	Conclusion
1	EU RoHS Directive 2011/65/EU and the amended Directive (EU) 2015/863	Complied
2	EU REACH Regulation (EC) No. 1907/2006	Complied
3	China RoHS in accordance to SJ/T 11363-2014	Complied
4	Taiwan BSMI RoHS in accordance to CNS 15663	Complied
5	EU Directive 2006/122/EC regarding Perfluorooctane Sulfonates (PFOS)	Complied
6	U.S. EPA TSCA (Toxic Substances Control Act) Section 6(h)	Complied

Product Information

Item	Accton P/N	Description	Customer P/N
1	F0PWL4125001A	??SWITCH ECS4125-10T-0724-WL US , 1 O	ECS4125-10T US

Documento Protocolo 1043/2025 || Anexo: Edgecore_Statement_of_Environmental_Directives_Compliance_R10_PRD241100010_EC84125_10T(208/256) 1475/4726

1,Creation Road 3,
Hsinchu Science Park,
Hsinchu 30077, Taiwan, R.O.C.

Attachment 1 EU RoHS Directive 2011/65/EU and the amended Directive 2015/863/EU

Product meets EU RoHS requirements with exemption(s):

Banned Substance	Threshold Limit	RoHS Exemption*
Lead (Pb)	1,000 ppm (0.1 weight %)	6(c); 7(a); 7(c)-I
Cadmium (Cd)	100 ppm (0.01 weight %)	
Mercury (Hg)	1,000 ppm (0.1 weight %)	
Hexavalent Chromium (Cr^{6+})	1,000 ppm (0.1 weight %)	
Poly Brominated Biphenyls (PBB)	1,000 ppm (0.1 weight %)	
Poly Brominated Diphenyl Ethers (PBDE)	1,000 ppm (0.1 weight %)	
Bis(2-Ethylhexyl) phthalate (DEHP)	1,000 ppm (0.1 weight %)	
Benzyl butyl phthalate (BBP)	1,000 ppm (0.1 weight %)	
Dibutyl phthalate (DBP)	1,000 ppm (0.1 weight %)	
Diisobutyl phthalate (DIBP)	1,000 ppm (0.1 weight %)	

RoHS maximum limit (ppm) does not apply to applications for which exemptions have been granted by the RoHS Directive.

Applicable within the scope of categories and expiry dates as given in Annex III of Directive 2011/65/EU as listed below:

RoHS exemption	RoHS exemption description
6(c)	Copper alloy containing up to 4 % lead by weight.
7(a)	Lead in high melting temperature type solders (i.e. lead- based alloys containing 85% by weight or more lead).
7(c)-I	Electrical and electronic components containing lead in a glass or ceramic other than dielectric ceramic in capacitors, e.g. piezoelectronic devices, or in a glass or ceramic matrix compound.

Documento Protocolo 1243/2025 || Anexo: Edge-corE_Statement_of_Conformity_RoHS_Directive_Compliance_R10_PRD241100010_Spanish.pdf (pag 1/2) 1476/4726

1,Creation Road 3,
Hsinchu Science Park,
Hsinchu 30077, Taiwan, R.O.C.

Attachment 2 EU REACH Regulation (EC) No. 1907/2006

This statement reflects Products listed below that are in compliance to Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning the Registration, Evaluation, Authorization and Restriction of Chemicals (REACH). The Candidate List of SVHCs is continually updated at https://echa.europa.eu/candidate-list-table. (substance of very high concern, 242 SVHCs as amended on November 7th, 2024.

This product contains the following REACH Substances of Very High Concern above the limits (0.1% w/w) of component article within REACH:

CAS No.	SVHCs in a concentration above 0.1% weight by weight
1303-86-2	Diboron trioxide
1317-36-8	Lead monoxide (lead oxide)
25550-51-0	Hexahydromethylphthalic anhydride
7439-92-1	Lead
71868-10-5	2-methyl-1-(4-methylthiophenyl)-2-morpholinopropan-1-one
108-78-1	Melamine
115-86-6	Triphenyl phosphate

ministrativo Proceso Protocolo 1243/2025 || Anexo: Edge-corE_Statement_of_Regulatory_Compliance_R10_PRD241100010_Spanish.pdf (pdf) (50) 3476/4726

1,Creation Road 3,
Hsinchu Science Park,
Hsinchu 30077, Taiwan, R.O.C.

Attachment 3 China RoHS in accordance to SJ/T 11363-2014

Table of toxic and hazardous substances/elements and their content:

(As required by China's management methods for controlling pollution by electronic information products)

产品内含危害物质揭露表　Products contain hazardous substances exposing table						
零部件名称 Component Name	危害物质项目 Hazardous Substances Project					
	铅 (Pb)	镉 (Cd)	汞 (Hg)	六价铬 (Cr6+)	多溴联苯 (PBB)	多溴二苯乙醚 (PBDE)
电源供应器 Power Supply	X	○	○	○	○	○
风扇 FAN	X	○	○	○	○	○
散热片Heat Sink	X	○	○	○	○	○
网络连接器 RJ45+X'FMR	X	○	○	○	○	○
二极管 Diode	X	○	○	○	○	○
突波吸收器(静电保护) TVS Array	X	○	○	○	○	○
电阻 Resistor	X	○	○	○	○	○
本表格依据 SJ/T：11364-2014 的规定编制。						

O：表示此部件使用的所有同类材料中此种有毒或有害物质的含量均低于 GB/T 26572-2011 规定的限制要求。

O：indicates the toxic or hazardous substance content of the part (at the homogenous material level) is lower than the threshold defined by Requirements for Concentration Limits for Toxic or hazardous Substances in Electronic Information Products(GB/T 26572-2011) issued by Chinese Ministry of Information Industry ("Not Contained" toxic or hazardous substances).

X:表示此部件使用的至少一种同类材料中，此种有毒或有害物质的含量高于 GB/T 26572-2011 规定的限制要求。

X: indicates the toxic or hazardous substance content of the part (at the homogenous material level) is over the threshold defined by standard of GB/T 26572-2011("Contained"toxic or hazardous substances). Suppliers can explain the technical cause of "X" according to actual situation.

...inistrativo Processo Licitatório 1.049/2025 || Anexo: ... (256) 3478/4721

1,Creation Road 3,
Hsinchu Science Park,
Hsinchu 30077, Taiwan, R.O.C.

Attachment 4 Taiwan BSMI RoHS in accordance to CNS 15663

The following tables are a declaration of the presence condition of restricted substances:

設備名稱：2.5G L2 網管型交換器 Equipment name				型號（型式）：ECS4125-10T Type designation (Type)		
單元 Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛 Lead(Pb)	汞 Mercury(Hg)	鎘 Cadmium(Cd)	六價鉻 Hexavalent chromium (Cr^{+6})	多溴聯苯 Polybrominated biphenyls (PBB)	多溴二苯醚 Polybrominated diphenyl ethers (PBDE)
電路板組件 PCBA	-	O	O	O	O	O
電源供應器 Power Supply	-	O	O	O	O	O
風扇 FAN	-	O	O	O	O	O
機殼 Chassis	O	O	O	O	O	O
組合線 Cable ass'y	O	O	O	O	O	O

備考1. 〝超出0.1 wt %〞及〝超出0.01 wt %〞係指限用物質之百分比含量超出百分比含量基準值。

Note 1：“Exceeding 0.1 wt %” and “exceeding 0.01 wt %” indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition.

備考2. 〝○〞係指該項限用物質之百分比含量未超出百分比含量基準值。

Note 2：“○” indicates that the percentage content of the restricted substance does not exceed the percentage of referenc value of presence.

備考3. 〝－〞係指該項限用物質為排除項目。

Note 3：The “–” indicates that the restricted substance corresponds to the exemption.

Documento Protocolo 1023/2025 || Anexo: Edge-84C79_Statement_of_Hazardous_Substances_Compliance_R10_PRD241100010_EC84125_10T(2).pdf (2 / 56) 3479/4726

1,Creation Road 3,
Hsinchu Science Park,
Hsinchu 30077, Taiwan, R.O.C.

Attachment 5 EU Directive 2006/122/EC regarding Perfluorooctane Sulfonates (PFOS)

The permissible maximum concentration values of hazardous substances present in electrical and electronic equipment, general requirements are as follows:

Specifications	Threshold Limit
Substance or constituent of preparations	< 0.001 weight % (10ppm)
Semi-finished products & articles & parts	< 0.1 weight % (1000ppm)
Textiles & other coated materials	< 1ug/m2

Attachment 6 Section 6(h) of US Toxic Substances Control Act (TSCA)

We hereby confirmed that the declared products do not contain the Persistent, Bioaccumulative, and Toxic (PBT) Chemicals under TSCA Section 6(h) listed below:

Substance	CAS No.
Decabromodiphenyl ether (DecaBDE)	1163-19-5
Phenol, isopropylated, phosphate (3:1) (PIP (3:1))	68937-41-7
2,4,6-Tris (tert-butyl) phenol (2,4,6-TTBP)	732-26-3
Pentachlorothiophenol (PCTP)	133-49-3
Hexachlorobutadiene (HCBD)	87-68-3

Signature:

Responsible person in charge (printed): Allen Chao
Date: December 05th,2024

1Doc: Protocolo 1.943/2025 | Anexo: em_34C7D88059D2E321B6628991_proc_administrativo_processo_licitatorio_029_2025_parte_15.pdf (2113250) 3479/4726

Proc. Administrativo Processo Licitatório - 58- 029/2025

De: Wellyngton M. - SMEAE - CTI

Para: SMA-CPL - Comissão Permanente de Licitação

Data: 07/07/2025 às 10:28:35

Setores envolvidos:

SMA, GAB, SMA-CPL, SMA-CACBS, PGM-CJL, SMEAE-CIS, SMFIN-CT, SMFIN-CCG, SMEAE, SMPLAN-CP, SMEAE - Compras, SMEAE - CTI, SMFIN-SDD, SMPLAN-GPO-ED, AP- PAF

Registro de Preço para futura e eventual aquisição de serviço de locação de firewall e segurança cibernética para atender à demanda do Município de Cáceres

Prezado Pregoeiro,

Após análise técnica minuciosa da documentação apresentada pela empresa **SH7 Proteção e Inteligência Cibernética LTDA**, no âmbito do processo licitatório em curso, informamos que foram examinados os seguintes elementos instrutórios: **Atestados de Capacidade Técnica**, **Carta de Solidariedade**, documentação referente aos **equipamentos ofertados** e **qualificação da equipe técnica**, com vistas à verificação de conformidade com os requisitos estabelecidos no Termo de Referência.

1. **Dos Equipamentos Ofertados**

   A documentação técnica dos equipamentos foi avaliada quanto à aderência às especificações exigidas no Termo de Referência. Observa-se, entretanto, que **alguns itens apresentaram omissões quanto às informações técnicas**, em razão dos **catálogos encaminhados não conterem descrições detalhadas das especificações exigidas**. Ainda assim, com base no conjunto de informações disponíveis e considerando a apresentação geral dos equipamentos, verifica-se que, **na sua maioria**, os itens ofertados **atendem aos requisitos técnicos previstos**, não comprometendo, de forma substancial, a avaliação de conformidade.

2. **Da Carta de Solidariedade**

   A **Carta de Solidariedade** emitida pelo fabricante está redigida em conformidade com as exigências legais e regulamentares, demonstrando o compromisso formal de prestar suporte técnico e fornecer insumos, peças e serviços necessários ao adequado funcionamento da solução ofertada, nos moldes exigidos pelo certame.

3. **Dos Atestados de Capacidade Técnica**

   Foram apresentados **diversos atestados de capacidade técnica**, os quais, em sua maioria, encontram-se em conformidade com as exigências editalícias, comprovando a aptidão da empresa para a execução de serviços compatíveis com o objeto licitado, conforme previsto no Termo de Referência.

   Destaca-se, ainda, que os atestados apresentados contemplam o **percentual mínimo exigido de 30% do quantitativo estimado** referente ao **item 1 – Solução de Firewall de Nova Geração e SD-WAN (Alta Disponibilidade)**, em conformidade com os itens **5.8.1.2** e **10.2.1.5.1** do Termo de Referência, o que demonstra a capacidade operacional da licitante em fornecer solução de complexidade e porte

Assinado por 3 pessoas: WELLYNGTON DE BARROS MACIEL, GIRLANE VIEIRA PEREIRA e ADEMAR ALVES TRINDADE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/E54D-A679-50A7-4318 e informe o código E54D-A679-50A7-4318

equivalentes.

Contudo, merece registro **incongruência temporal** verificada no documento intitulado **"At_SH7_assinado.pdf"**, emitido pela empresa **Inovasete Tecnologia**. O referido **Atestado de Capacidade Técnica está datado em 07 de julho de 2025**, enquanto a **assinatura nele constante está datada de 02 de julho de 2025**, o que configura um **equívoco material**, visto que a data expressa como sendo a do documento ainda não ocorreu no momento da análise.

Tal discrepância temporal, embora de natureza formal, pode ensejar dúvida quanto à exatidão das informações, razão pela qual poderá ser solicitada a retificação do documento. Importa salientar que **não há indícios de má-fé**, tampouco de tentativa de indução em erro por parte da empresa, tratando-se, portanto, de **falha sanável**.

4. **Da Qualificação da Equipe Técnica**

A licitante apresentou documentação comprobatória de que **possui, em seu quadro, pelo menos dois profissionais com certificação técnica emitida pelo fabricante da solução ofertada**, conforme exigido no **item 10.2.1.5.2** do Termo de Referência. Tal comprovação reforça a capacidade da empresa em garantir o correto funcionamento, suporte e manutenção da solução contratada, com respaldo técnico devidamente qualificado.

Diante do exposto, **opinamos favoravelmente à aceitação da documentação apresentada pela empresa SH7 Proteção e Inteligência Cibernética LTDA**, uma vez que foram demonstrados de forma satisfatória o cumprimento dos requisitos técnicos e legais exigidos para habilitação, ressalvando-se a possibilidade de correção do apontamento supra, caso julgado necessário por esta Administração.

Permanecemos à disposição para quaisquer esclarecimentos adicionais que se fizerem necessários.

–

Atenciosamente,

_____

Wellyngton de Barros Maciel
Gerente de Hardware
Decreto nº 117 de 25 de fevereiro de 2022

Coordenação de Tecnologia da Informação
Secretaria Municipal Especial de Assuntos Estratégicos Município de Cáceres – MT

Assinado por 3 pessoas: WELLYNGTON DE BARROS MACIEL, GIRLANE VIEIRA PEREIRA e ADEMAR ALVES TRINDADE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/E54D-A679-50A7-4318 e informe o código E54D-A679-50A7-4318

VERIFICAÇÃO DAS ASSINATURAS

Código para verificação: E54D-A679-50A7-4318

Este documento foi assinado digitalmente pelos seguintes signatários nas datas indicadas:

WELLYNGTON DE BARROS MACIEL (CPF 004.XXX.XXX-60) em 07/07/2025 09:29:12 GMT-04:00
Papel: Parte
Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

GIRLANE VIEIRA PEREIRA (CPF 024.XXX.XXX-66) em 07/07/2025 09:48:52 GMT-04:00
Papel: Parte
Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

ADEMAR ALVES TRINDADE (CPF 700.XXX.XXX-00) em 07/07/2025 10:14:16 GMT-04:00
Papel: Parte
Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

Para verificar a validade das assinaturas, acesse a Central de Verificação por meio do link:

https://caceres.1doc.com.br/verificacao/E54D-A679-50A7-4318

De: Igor O. - SMA-CPL

Para: SMEAE - CTI - Coordenação de Tecnologia da Informação

Data: 17/07/2025 às 09:10:26

Prezada Coordenadora,

Considerando:

- A interposição de **recurso**pela empresa F.V.B.N Construções e Tecnologia Ltda, insurgindo-se contra a **habilitação da empresa SH7 Proteção e Inteligência Cibernética Ltda** , alegando, em síntese, suposta **ilegalidade na comprovação da capacidade técnico-operacional** e **insuficiência no quantitativo mínimo exigido**;
- A apresentação, dentro do prazo legal, das **contrarrazões** pela empresa SH7, as quais argumentam pela regularidade dos documentos apresentados;
- A necessidade de apreciação técnica quanto à **validade dos atestados apresentados**, especialmente no tocante ao cumprimento do item 9.17.13 do edital e à suficiência do quantitativo exigido;

  Encaminhe-se o presente processo ao Setor Técnico competente, para que, no prazo de até **5 (cinco) dias úteis**, **emita parecer técnico.**

1. Após o parecer técnico, **encaminhe-se o processo à Procuradoria Jurídica** para emissão de **parecer jurídico** sobre a regularidade da habilitação da empresa SH7 e a legalidade da eventual manutenção ou desclassificação da mesma, com fundamento na Lei nº 14.133/2021.
2. Com o retorno dos pareceres técnico e jurídico, retornem os autos a este pregoeiro para elaboração da **decisão fundamentada quanto ao recurso interposto**.

Atenciosamente,

–

Igor de Souza Oliveira
Pregoeiro Oficial

Anexos:

CONTRARRAZOES_COMPLETA.pdf
Recurso_Administrativo_FVBN_SH7_FINAL_ass.pdf

A PREFEITURA MUNICIPAL DE CÁCERES
EDITAL PREGÃO ELETRÔNICO N° 15/2025
PROCESSO ADMINISTRATIVO N° 29/2025

SH7 PROTEÇÃO E INTELIGÊNCIA CIBERNÉTICA LTDA, Inscrita no CNPJ sob o n° 44.122.701/0001-79, por intermédio de seu representante legal abaixo assinado, com fulcro no art. 165, da Lei nº 14.133/2021, vem com fulcro no item 11.12 do instrumento convocatório, apresentar **CONTRARRAZÕES AO RECURSO** apresentado pela licitante **F.V.B.N CONSTRUÇÕES E TECNOLOGIA LTDA** quanto à habilitação desta empresa, pelos fatos e fundamentos de direito que passa a expor.

1. TEMPESTIVIDADE

1.1. A empresa tomou conhecimento do recurso apresentado pela empresa licitante F.V.B.N CONSTRUÇÕES E TECNOLOGIA LTDA em 11/07/2025, tendo o prazo de 03 (três) dias úteis, conforme disposto no item 11.12 do Edital, para apresentação de Contrarrazões.

1.2. Assim, o prazo foi iniciado em 14/07/2025, tendo como **data final 16/05/2025.** Posto isso, resta comprovada a tempestividade da presente contrarrazões.

2. SÍNTESE DO PREGÃO ELETRÔNICO

2.1. A empresa SH7 PROTEÇÃO E INTELIGÊNCIA CIBERNÉTICA LTDA participou do Pregão Eletrônico n. 015/2025, promovido pela PREFEITURA MUNICIPAL DE CÁCERES ocorrido em 03/07/2025, cujo objeto era o *Registro de Preço para futura e eventual contratação de empresa especializada para prestação de serviços de segurança cibernética com Inteligência Artificial Preditiva, garantindo alta disponibilidade, segurança, eficiência e sustentabilidade no atendimento às demandas do Município de Cáceres, conforme condições e exigências estabelecidas no instrumento convocatório.*

2.2. A empresa sagrou-se vencedora para lote único licitado e teve sua proposta analisada e aceita pelo agente de contratações.

2.3. Ocorre que a licitante F.V.B.N CONSTRUÇÕES, irresignada com o resultado da licitação, requereu a inabilitação da licitante SH7 no certame, alegando, em síntese, **irregularidade na habilitação técnica** da empresa, o que não merece prosperar.

2.4. Nesse sentido, tais alegações não merecem prosperar, pois conforme **restará esclarecido e comprovado pela empresa recorrida, não houve afronta a qualquer item do edital nem mesmo afronta a princípios basilares do direito administrativo, bem como está licitante preenche adequadamente a todos os requisitos de habilitação, especialmente em demonstrar possuir capacidade técnica, assim como apresentou proposta proporcional e exequível para execução do objeto licitado.**

2.5. Nestes termos, vem por meio deste, apresentar suas contrarrazões, tempestivamente, ao recurso administrativo interposto pela empresa F.V.B.N CONSTRUÇÕES.

3. DO CUMPRIMENTO DOS REQUISITOS DA HABILITAÇÃO – QUALIFICAÇÃO TÉCNICA

3.1. Sabe-se que a apresentação de atestado de capacidade técnica tem a finalidade de demonstrar que o licitante detém *expertise* suficiente para o cumprimento do objeto contratual. Para o TCU, é preciso diferenciar a capacidade técnico operacional da empresa (Lei 14.133/2021, Art. 67, II) e a capacidade técnico-profissional (Lei 14.133/2021, Art. 67, III):

> Art. 67. A documentação relativa à qualificação técnico-profissional e técnico-operacional será restrita a:
>
> II - certidões ou atestados, regularmente emitidos pelo conselho profissional competente, quando for o caso, que demonstrem capacidade operacional na execução de serviços similares de complexidade tecnológica e operacional equivalente ou superior, bem como documentos comprobatórios emitidos na forma do § 3º do art. 88 desta Lei;

> III - indicação do pessoal técnico, das instalações e do aparelhamento adequados e disponíveis para a realização do objeto da licitação, bem como da qualificação de cada membro da equipe técnica que se responsabilizará pelos trabalhos;

3.2. A CAPACIDADE TÉCNICO-OPERACIONAL (Lei 14.133/2021, Art. 67, II) é aquela que pertence à empresa que trata da comprovação de aptidão para desempenho de atividade compatível com o objeto da licitação. Busca identificar se a pessoa jurídica possui instalações, aparelhamento, pessoal técnico, com aptidão pertinente, adequados para a realização do objeto da licitação.

3.3. Em que pese a SH7 PROTEÇÃO E INTELIGÊNCIA CIBERNÉTICA LTDA, ter sido declarado vencedora, a empresa **F.V.B.N CONSTRUÇÕES**, inadequadamente, insurgiu contra a habilitação desta **alegando o não preenchimento dos requisitos de capacidade técnica-operacional** apresentados no Termo de Referência, em especial ao disposto no item 9.34.1.1. e 9.34.1.2.. Vejamos o que exige o edital para os licitantes:

> 9.17. **Qualificação Técnica**
> 9.17.1. Comprovação de aptidão para o fornecimento de bens em características, compatíveis com o objeto desta licitação, ou com o item pertinente, por meio da apresentação de atestados fornecidos por pessoas jurídicas de direito público ou privado.

> 9.17.13. Será exigida a comprovação da capacidade técnico-operacional da licitante, mediante a apresentação de atestados emitidos por pessoa jurídica de direito público ou privado, que comprovem a execução de serviços compatíveis em características, quantidades e prazos com o objeto deste contrato, incluindo o fornecimento e a instalação de equipamentos correlatos aos ofertados, bem como a prestação de serviços de instalação, configuração e suporte técnico. A licitante deverá comprovar, no mínimo, experiência prévia correspondente a **30% (trinta por cento)** do quantitativo estimado do **item 1 – Solução de Firewall de Nova Geração e SD-WAN (Alta Disponibilidade)**, considerado de maior relevância técnica para a consecução do objeto. Tal exigência encontra amparo no inciso III do art. 67 da Lei nº 14.133/2021, sendo justificada pela complexidade e especificidade do objeto, que demanda experiência comprovada na execução de soluções integradas de segurança cibernética, com destaque para componentes baseados em Inteligência Artificial Preditiva, visando garantir a eficiência, a continuidade dos serviços e a mitigação de riscos operacionais, em observância aos princípios da legalidade, razoabilidade, eficiência e interesse público.
>
> 9.17.13.1 A comprovação poderá ser feita por meio de um ou mais atestados que, **conjuntamente**, demonstrem a experiência da licitante de forma compatível com o objeto contratado, especialmente no que se refere ao atendimento do percentual mínimo de 30% do item de maior relevância técnica, vedada a exigência de comprovação integral do quantitativo estimado.
>
> 9.17.13.2 Os atestados deverão conter, no mínimo:
>
> 9.17.13.3 Identificação completa do emitente, com razão social, CNPJ, endereço e dados de contato;
>
> 9.17.13.4 Descrição detalhada dos serviços executados, permitindo aferir a compatibilidade em características com o objeto, incluindo fornecimento e instalação de equipamentos, implantação de soluções de segurança cibernética, configuração e suporte técnico;
>
> 9.17.13.5 Indicação de que os serviços foram executados em quantidades compatíveis, com destaque para a experiência mínima equivalente a 30% do quantitativo estimado do item de maior relevância técnica, conforme avaliação da Administração, vedada a exigência de quantidades idênticas ou desproporcionais, nos termos do art. 67, §§ 1º, 2º e 5º, da Lei nº 14.133/2021;
>
> 9.17.13.6 Período de execução dos serviços, com datas de início e de conclusão ou, se for o caso, vigência atual, para fins de comprovação da compatibilidade em prazos;

3.4. Ainda, a empresa **F.V.B.N CONSTRUÇÕES** insurge que um dos atestados técnicos apresentados não seria válido, por ter sido apresentado por empresa supostamente do mesmo grupo econômico do que a empresa licitante vencedora - atestado emitido pela **REDE EXS TELECOMUNICAÇÕES LTDA** - é plenamente válido.

3.5. Conforme já decidido em outras licitações, inclusive a ressaltar, desta mesma Municipalidade, a exemplo o Pregão Eletrônico N° 90017/2024 (SRP), em situação idêntica a esta aqui tratada, assim decidiu:

> *"II.II – DO MÉRITO Em seu recurso, a empresa recorrente "IP AMÉRICA TELECOM LTDA", alega que a empresa "NITRO MIRASSOL LTDA" descumpriu o item 9.18.1., abaixo transcrito: 9.18.1. Comprovação de aptidão para o fornecimento de bens em características, ou com o item pertinente, por meio da apresentação de atestados fornecidos por pessoas jurídicas de direito público ou privado.* ***A recorrente afirma que a recorrida apresentou Atestado de Capacidade Técnica invalido, pois o documento apresentado pela recorrida, supostamente, não é compatível com o item licitado,*** *conforme trecho transcrito: "Ao analisar os documentos apresentados pela Recorrida, notou-se que* ***o único atestado técnico por ela juntado foi emitido pela Dunet Telecom Ltda., empresa integrante do mesmo grupo econômico da vencedora do certame.*** *Deste modo, procedeu-se à realização de diligência para verificação da validade do documento apresentado, sendo requisitado à Recorrida apresentação das notas fiscais provenientes do contrato que gerou o referido atestado de capacidade técnica. (...) 2 Ibidem, p. 451. [...]*
> *A empresa prontamente atendeu ao pedido, encaminhando junto ao contrato, outros atestados de capacidade técnica assim como já havia manifestado em suas contrarrazões.* ***Quanto a qualificação técnica da empresa ficou compravado através dos atestados apresentado como já citado no parecer juridico, a empresa atendeu aos critérios editalícios.[...]***
> *Considerando os fatos narrados através do* ***parecer Nº 279/2024 - PGM e demais, referênciados acima, fica demonstrado, a priori, que a empresa recorrida cumpriu com todos os critérios estabelecidos no edital de convocação, devendo ser mantida habilitada no certame****.[...]*
> *com base nas fundamentações apresentadas, este pregoeiro, com base em suas atribuições e parecer,* ***DECIDE MANTER A HABILITAÇÃO a empresa*** *NITRO MIRASSOL LTDA inscrita no CNPJ: 49.114.343/0001-76, Local e data: Prefeitura de Cáceres-MT, 27 de junho de 2024 Igor de Souza Oliveira Pregoeiro Oficial Portaria 415-2023 Para mais informações a decisão também está disponível no site oficial da prefeitura municipal de Cáceres. Link: https://www.caceres.mt.gov.br/Licitacoes/Pregao-/1720242299/"*

3.6. Conforme o edital retificado, a comprovação técnica demandada é especificamente para o **item 1 – Solução de Firewall de Nova Geração e SD-WAN**. Ou seja, o certame exige atestados para o fornecimento de firewall, não para o switch.

3.7. Logo, a alegação do licitante recorrente de que os atestados teriam de cobrir "apenas a parte de switch" está equivocada. A exigência referia-se justamente ao firewall, como prevê expressamente o edital. Ademais, não consta no edital qualquer vedação expressa à aceitação de atestados emitidos por empresa do mesmo grupo econômico da licitante. O item invocado pela recorrente (suposto "9.17.13.9.2") não faz referência a este tipo de vedação, portanto, tal alegação é falaciosa e não merece prosperar. Assim, resta claro que não há norma editalícia que impeça o uso de atestado de empresas com vínculos societários, o que estaria em consonância com o entendimento do TCU.

3.8. Neste sentido, por ausência de vedação em Lei e por ausência de manifestação em Edital, que vincula as partes, acerca da situação em tela, é equivocada a interpretação de que os atestados não podem ser aceitos, uma vez que não há essa condição expressa.

3.9. Nesse sentido, **a validade de um atestado técnico não depende de quem é o emissor**, **mas sim das atividades efetivamente executadas** e **da sua compatibilidade com o objeto da licitação e do vínculo real da mão de obra com a empresa contratada**. Ou seja, o que importa é a demonstração da experiência e da capacidade técnica para a realização do objeto da licitação.

3.10. Não obstante, ambas as empresas, tanto esta licitante quanto a que emitiu o Atestado, são empresas de personalidade jurídica própria e que não devem ser confundidas apenas pelo fato de terem uma sócia em comum. Ressalto, novamente, que não existe nenhuma vedação expressa na Lei de Licitações quanto à tal situação de sócios em comum e inclusive acerca de empresas de um mesmo grupo econômico. Isso porque, no Brasil, via de regra, a pessoa jurídica não se confunde com seus sócios, sejam eles pessoas físicas ou outras pessoas jurídicas. No mesmo sentido, as seguintes decisões do TCU:

> "(...) Considerando tratar-se de representação, com pedido de medida cautelar, formulada por Evermobile Ltda., com fundamento no art. 113, § 1º, da Lei nº

8.666/1993, acerca de supostas irregularidades na condução do pregão Eletrônico nº 158/7855-2009, promovido pela Caixa Econômica Federal, para contratação de empresa especializada para fornecimento de solução integrada de processamento de cartões de crédito (...) Considerando que a unidade técnica, em instruções uniformes (fls. 140/143), refutou todas as irregularidades denunciadas pela representante. (...) Considerando que, **em relação à alegação de que o atestado de capacidade técnica não poderia ter sido emitido por empresa do mesmo grupo econômico, tendo sido observado que não havia vedação na Lei de Licitações nem no edital do pregão e que controlada e controladora conservam personalidade e patrimônio distintos.** (...) Os Ministros do Tribunal de Contas da União ACORDAM, por unanimidade, com fundamento nos arts. 1º, inciso II e 43, inciso I, da Lei nº 8.433, de 16 de julho de 1992, c/c os arts. 17, inciso IV; 143, inciso III; 237, inciso VII, do Regimento Interno / TCU, **nos termos dos pareceres exarados nos autos, em conhecer da presente representação, para, no mérito, considerá-la improcedente** (...).” (TCU Acórdão 451/2010-Plenário). grifo nosso

(TCU Acórdão 2241/2012-Plenário): “(...) 31. Sobre os motivos pelos quais considerou insuficiente o atestado de capacidade técnica apresentado pela empresa Connectcom Teleinformática Comércio e Serviços Ltda., a afirmação da Alive de **inviabilidade do atestado de capacidade técnica por ter sido emitido por empresa do mesmo grupo econômico não prospera.** Em primeiro lugar, porque não há vedação na Lei n° 8.666/93 e nem no edital da licitação. Em segundo lugar, porque o art. 266 da Lei 6.404/76 estabelece que as sociedades (controladora e controlada) conservam a personalidade e patrimônios distintos, além de ser um princípio da contabilidade: o princípio da entidade. Assim, não se misturam transações de uma empresa com as de outra. Mesmo que ambas sejam do mesmo grupo econômico, respeita-se a individualidade de cada uma.” grifo nosso.

3.11. Posto isso, todos os atestados apresentados pela empresa **SH7 PROTEÇÃO E INTELIGÊNCIA CIBERNÉTICA LTDA são perfeitamente legais, aptos a uso e atendem a todos os requisitos previstos no edital.**

3.12. Convém ainda observar que a mencionada exigência relativa à qualificação técnica visa assegurar a boa execução do objeto a ser contratado. Neste diapasão, vem a própria Constituição Federal, no inciso XXI, do Art. 37 parte final, afirmar que **somente é permitida às exigências de qualificação técnica indispensáveis à garantia do cumprimento das obrigações.**

3.13. Outrossim, no que tange aos quantitativos exigidos no item 9.17.13, o Edital prevê que o contrato terá vigência de 12 meses, de modo que as quantidades estimadas em cada item correspondem a fornecimentos mensais. Com efeito, o próprio quadro do Termo de Referência mostra, por exemplo, que o “Link de acesso à

internet de 35Mbps" tem 171 unidades mensais (totalizando 2.052 no ano). **De forma análoga, as 2.076 unidades estimadas para o Item 1 correspondem a 173 mensais (173×12=2.076).** Portanto, **a exigência editalícia de comprovar 30% do item de maior relevância deve incidir sobre 173 unidades mensais** (≈52), e não sobre o total anual de 2.076 (≈623). Ressalte-se que o próprio edital deixa claro que é vedada a exigência de comprovação integral do quantitativo estimado. Neste caso, **a empresa SH7 apresentou atestados que comprovam a prestação do serviço em questão (totalizando as 65 unidades do Item 1- 43 unidade atestado emitido por INOVASETE** +22 unidades no atestado emitido por REDE EXS TELECOMUNICAÇÕES LTDA +), de modo que o requisito mínimo (30% do quantitativo mensal) estaria plenamente atendido com os demais atestados anexados.

camoa telecom

ATESTADO DE CAPACIDADE TÉCNICA

A empresa **CAMOA SERVIÇOS TELECOM LTDA**, inscrita sob o CNPJ n° 28.097.989/0001-12 e no CF/DF sob o n° 07.816.367/001-01, sediada na SCLRN 711 Bloco G Sala 39, Asa Norte - Brasília-DF, atesta para os devidos fins que a empresa **SH7 PROTECAO E INTELIGENCIA CIBERNETICA LTDA**, inscrita no CNPJ: 44.122.701/0001-79, prestou os serviços de Cibersegurança e Conectividade bem como Fornecimento de equipamentos, conforme dados dos contratos abaixo:

Contrato	Objeto	Quantidade	Período
002/2022	Conectividade Multi PTT e IPTrânsito	11 Gbps	07 (sete) meses
	Conectividade FTTH	100	1 (um) ano
TA-12Mai23	Conjunto Switch / Optical Line Terminal (Terminal de Linha Óptica), portas de 1/10/25 e 100 Gbps (Edgecore e Fiberhome)	10	N/A
	Access Point	50	N/A
	Máquina de Fusão Fujikura	1	N/A
	Clivadores	3	N/A
	OTDR EXPO	1	N/A

Salientamos que a referida obra e conectividade teve desempenho a contento até seu encerramento, cumprindo rigorosamente os termos dos contratos firmados, e executando as obras de acordo os projetos executivos, não existindo fato que desabone a sua idoneidade técnica.

Brasília-DF, 22 de abril de 2.025.

gov.br Documento assinado digitalmente
SANDRO GOMES ARAUJO
Data: 22/04/2025 14:08:57 -0300
Verifique em https://validar.iti.gov.br

Inovasete
Tecnologia

ATESTADO DE CAPACIDADE TÉCNICA

ATESTAMOS para os devidos fins e a quem possa interessar que a empresa SH7 PROTEÇÃO E INTELIGENCIA CIBERNÉTICA LTDA, inscrita no CNPJ/MF sob o nº 44.122.701/0001-79, com sede no ST SRTVS QD 701 BLOCO O SALA, nº 122, NOVO CENTRO MULTIEMPRESARIAL, Bairro Asa Sul, Cep. 70.340-000 – Brasília - DF, presta serviços de Cibersegurança e Conectividade para nossa empresa INOVASETE TECNOLOGIA LTDA, inscrita no CNPJ/MF sob o nº 10.365.200/0001-00, com sede à Q SHN QUADRA 1, SN, Asa Norte, Cep. 70.701-000, Brasília – DF, detendo qualificação técnica para:

1. Serviços de Cibersegurança SDWAN e Firewall de Nova Geração, com licença de uso, subscrição (Filtro Web, IPS, Antimalware, Geolocalização e Controle de Aplicação), Suporte Técnico na modalidade 24x7, Atualização de Firmware e Assinaturas, Instalação e Configuração (43 equipamentos);

2. Serviços Gerenciados de segurança com fornecimento em comodato de Firewall NGFW Blockbit, em cluster, modelo BBX 200 com licença de uso, subscrição (Filtro Web, IPS, Anti-malware, Geolocalização e Controle de Aplicação), suporte técnico na modalidade 24x7, Atualização de Firmware e assinaturas, instalação e configuração (01 Cluster)

Informamos que a prestação dos serviços de Cibersegurança acima referidos apresentam bom desempenho operacional, tendo a empresa cumprido fielmente com suas obrigações, nada constando que a desabone técnica e comercialmente, desde janeiro de 2025 até a presente data.

Brasília, 07 de julho de 2025

gov.br Documento assinado digitalmente
SANDRO GOMES ARAUJO
Data: 02/07/2025 13:44:05-0300
Verifique em https://validar.iti.gov.br

Sandro Gomes Araújo
sandro.araujo@camoa.com.br
Sócio

ATESTADO DE CAPACIDADE TÉCNICA

Atestamos para os devidos fins que a empresa SH7 PROTECAO E INTELIGENCIA CIBERNETICA LTDA, inscrita no CNPJ: 44.122.701/0001-79, forneceu soluções incluindo equipamentos e serviços, conforme itens abaixo, cumprindo fielmente o que foi acordado, não existindo fato que desabone sua idoneidade técnica.

Objeto	Quantidade	Link
Cassini AS7716-24SC, portas client 100 Gbps, UPLINK 200 Gbps, L2/L3	6	https://www.edge-core.com/cloud-data-center-packet-optical/
ECS5550 Series	23	https://www.edge-core.com/enterprise-l3-switches/
AS5916	5	https://www.edge-core.com/service-provider-aggregation-routers/
ECS4150	57	https://www.edge-core.com/enterprise-l2-switches/
OTDR EXFO	1	n/a
Máquina de Fusão conjunto com 02(dois) clivadores	1	n/a

Brasília/DF, 22 de Abril de 2025

3.14. Reitera-se que cabe à Administração o uso da discricionariedade para **estabelecer exigências compatíveis e indispensáveis ao atendimento do objeto licitatório**, não sendo de competência da iniciativa privada, estabelecer, retirar ou mesmo questionar o mérito de tais exigências, mas sim a supremacia do interesse público para decidir e julgar sobre o contexto da matéria.

3.15. Por todo o exposto, resta claro que **(i) a exigência editalícia de 30% foi cumprida com base no quantitativo mensal e não no total anual;** (ii) os atestados apresentados dizem respeito ao item exigido (firewall) e demonstram a execução dos serviços; (iii) inexiste vedação expressa no edital ou na lei que invalidem atestados de empresa do mesmo grupo, conforme doutrina e reiterada jurisprudência do TCU;

3.16. Por todo o exposto, requer-se sejam desconsiderados os argumentos da empresa F.V.B.N. deve ser julgado improcedente, mantendo-se a habilitação da empresa SH7 e assegurando-se a continuidade regular do certame.

4. DO FORMALISMO MODERADO E A SELEÇÃO DA PROPOSTA MAIS VANTAJOSA, QUE ATENDEU ÀS FINALIDADES DAS EXIGÊNCIAS

4.1. A licitante F.V.B.N. requereu a desclassificação da empresa SH7 no certame devido apenas ao fato de que um dos atestados anexados fora emitido por empresa privada supostamente do mesmo grupo econômico da licitante vencedora, **o que não merece prosperar** como veremos a seguir.

4.2. Com base na documentação apresentada ao agente de contratações e a comissão de licitação em sede de diligências (contrato, notas fiscais e comprovantes de pagamento de uma empresa a outra), **o atestado emitido pela empresa REDE EXS,** foi comprovado sua veracidade da prestação dos serviços pela empresa SH7 PROTEÇÃO E INTELIGÊNCIA CIBERNÉTICA LTDA.

4.3. Posto isso, não há razão alguma para ser inabilitada a empresa licitante vencedora, eis que não só atende aos requisitos de habilitação técnica. Nesse sentido, merece análise as palavras de Marçal Justen Filho sobre a licitação sob o critério de julgamento do **Menor Preço**:

> A Administração Pública tem o dever de buscar o menor desembolso de recursos, a fazer-se nas melhores condições possíveis. Qualquer outra solução ofenderia aos princípios mais basilares da gestão da coisa pública. [...]. **Apenas quando o ato convocatório estabelecer que a Administração necessita do objeto de melhor qualidade é que se admitirá afastar de consideração o fator "preço"**. Excluída essa hipótese, o preço será fator decisivo na seleção da proposta mais vantajosa.

4.4. Nesse sentido, quando a Lei 8.666/93 ainda estava em vigor já era consolidado o entendimento dos Tribunais a necessidade de utilizar-se do **formalismo moderado nas contratações**, levando-se em consideração os demais **princípios constitucionais**, tais quais do interesse público, da economicidade, razoabilidade e

proporcionalidade, entendimentos esse que se estenderão para a Lei 14.133/2021 e devem ser aplicados no presente caso, vejamos:

> Além disso, **inobstante o princípio da vinculação ao edital**, consagrado no art. 41 da Lei das Licitações, **é imperativo privilegiar princípios não menos importantes, como o da economicidade, razoabilidade e proporcionalidade e, na hipótese, não seria razoável que a Administração Pública optasse, sem sopesar os custos envolvidos, pela repetição do processo licitatório, ou pela proposta muito superior ao valor do serviço licitado**, só porque a empresa com menor preço incorreu em irregularidade formal, ao não apresentar proposta digitalizada. **O que importa é se o ato, praticado em desconformidade com a regra do edital, atendeu à finalidade da sua exigência, salvaguardando os interesses públicos e privados envolvidos. Sob essa ótica, deve prevalecer a oferta da licitante vencedora, de preço inferior, fator que prepondera sobre outras formalidades, facilmente superadas por outros elementos, ou ainda passíveis de serem supridas,** com base no art. 43, § 3º, da Lei n° 8.666/93. (AC 568682. Rel. NIZETE LOBATO CARMO - TRF2 SEXTA TURMA ESPECIALIZADA E-DJF2R - Data: 25/10/2013)

4.5. Sendo assim, **o procedimento adotado pela comissão de licitações** – solicitação de documentos complementares para verificação de veracidade e aptidão técnica do atestado impugnado pelo recorrente – **é totalmente legal e segue os parâmetros previstos em lei e nos entendimentos JÁ CONSOLIDADOS pelo TCU**. Além disso, a entrega dos documentos pela licitante, confirmou e demonstrou que a empresa possui qualificação técnica para execução do objeto licitado, desse modo seria excesso de formalismo e ofensa ao princípio da economicidade e da proposta mais vantajosa, **uma vez que a empresa comprovou possuir o menor preço, inabilitá-la no certame licitatório por mera formalidade seria um grande equívoco e ofensa a primazia do interesse público.**

4.6. Ante ao exposto, requer sejam desconsideradas as alegações da recorrente F.V.B.N., uma vez que já comprovado a qualificação técnica da empresa, devendo ser mantida a sua classificação neste certame.

5. DO PODER DEVER DE PROCEDER DILIGÊNCIAS

5.1. Conforme previsto em lei, o pregoeiro ou sua Comissão de Licitações possui o poder dever de proceder com diligências a fim de verificar a veracidade das informações e documentos apresentados pelos licitantes.

5.2. É sabido que constitui boa prática em licitações o ato de diligenciar quando o julgador se depara com atestados emitidos por empresas que possuam algum tipo de relação, a exemplo de sócios em comum. Os julgados e a doutrina recomendam que a Administração aja de forma diligente e cautelosa, a fim de evidenciar que o conteúdo dos documentos apresentados exprime a real verdade dos fatos, bem como que as empresas não estão atuando em conjunto no intuito de fraudar a licitação, isto é, que uma delas (a emissora do atestado, por exemplo) não está sendo utilizada somente para dar respaldo à outra que participa do certame, através da emissão de atestado que não é condizente com a realidade.

5.3. A demonstração de fraude ou conluio, na linha do que já sinalizou o TCU:

> "(...) 46.4. Para se configurar conluio são exigidas provas ou evidências inequívocas de que tenha havido ajuste entre as partes quanto à utilização de um processo com objetivo de fraude. Esse foi o entendimento da Seção II Especializada em Dissídios Individuais do Tribunal Superior do Trabalho (SDI-2) - ROAR-79/2006-000-10-00.8. 46.5. Com efeito, para absoluta confluência probatória tendente a caracterizar conluio e fraude à licitação pública, faz-se necessário analisar todo conjunto probante, com vistas a conferir certeza de que os indícios se harmonizam com as inquinadas condutas porventura encetadas pelas sociedades empresárias." (Acórdão 5845/2013-Segunda Câmara.)

5.4. Perceba que não se trata de obter 'prova' estritamente, mas ao menos de comprovar indícios consistentes. No presente caso, o Sr. Pregoeiro já realizou diligências, ocasião em que foram enviados documentos comprobatórios da realização dos serviços, tais como contratos, comprovante de repasses econômicos, etc.

5.5. Entretanto, **caso ainda assim, deseje esta comissão verificar também o quantitativo ou os serviços descritos nos atestados emitidos pelas empresas MCD e a Inovasete**, esta deve averiguar e verificar. Nesse mesmo sentido o TCU dispõe:

(TCU - Acórdão 3.418/14-Plenário): “REPRESENTAÇÃO. POSSÍVEIS IRREGULARIDADES OCORRIDAS NA CONDUÇÃO DE CERTAME. INCERTEZAS SOBRE ATESTADO DE CAPACIDADE TÉCNICA DE LICITANTE. NÃO UTILIZAÇÃO DO PODER-DEVER DE REALIZAR DILIGÊNCIAS PARA SANEAR AS DÚVIDAS QUANTO À CAPACIDADE TÉCNICA DA EMPRESA. PRESERVAÇÃO DA CONTINUDADE DO CONTRATO QUE SE ENCONTRA EM FASE DE EXECUÇÃO. DETERMINAÇÃO. 1. O Atestado de Capacidade Técnica é o documento conferido por pessoa jurídica de direito público ou de direito privado para comprovar o desempenho de determinadas atividades. Com base nesse documento, o contratante deve-se certificar que o licitante forneceu determinado bem, serviço ou obra com as características desejadas. 2. A diligência é uma providência administrativa para confirmar o atendimento pelo licitante de requisitos exigidos pela lei ou pelo edital, seja no tocante à habilitação seja quanto ao próprio conteúdo da proposta. 3. Ao constatar incertezas sobre cumprimento das disposições legais ou editalícias, especialmente as dúvidas que envolvam critérios e atestados que objetivam comprovar a habilitação das empresas em disputa, o responsável pela condução do certame deve promover diligências, conforme o disposto no art. 43, § 3º, da Lei 8.666/1993, para aclarar os fatos e confirmar o conteúdo dos documentos que servirão de base para tomada de decisão da Administração nos procedimentos licitatórios. Observe que a decisão acima, da Máxima Corte de Contas, expressa a finalidade do Atestado e orienta que, em caso de dúvidas, deve o responsável do certame proceder a seu poder-dever de diligenciar para chegar a uma tomada de decisão justa e não arbitrária.”

5.6. Se a prestação de fato ocorreu, como prova esta empresa por sua documentação, não há razão de inabilitação.

6. REQUERIMENTOS:

6.1. Por todo o exposto requer:

a) Sejam recebidas estas contrarrazões ao recurso manejado em virtude de sua tempestividade;

b) **Seja desprovido o recurso da F.V.B.N CONSTRUÇÕES, mantendo a habilitação da <u>SH7 PROTEÇÃO E INTELIGÊNCIA CIBERNÉTICA LTDA, eis que configura a proposta mais vantajosa à administração e preencheu todos os requisitos do edital</u>**, especialmente quanto à sua qualificação técnica;

Termos em que pede deferimento.

Porto Alegre/RS, 16 de julho de 2025.

SH7 PROTEÇÃO E INTELIGÊNCIA CIBERNÉTICA LTDA

MONIQUE SIQUEIRA DA SILVA

Assinado de forma digital por MONIQUE SIQUEIRA DA SILVA
Dados: 2025.07.16 14:07:41 -03'00'

Monique Siqueira da Silva
OAB/RS 119.441

Mariana Gloria de Assis
OAB/RS 79.079

PAOLA DERRIAUX CHASTAGNIER:09387055710

Assinado de forma digital por PAOLA DERRIAUX CHASTAGNIER:09387055710
Dados: 2025.07.16 15:39:36 -03'00'

Sh7
Cyber Shield

CONTRATO DE SERVIÇOS GERENCIADOS DE SEGURANÇA – SGS

CONTRATANTE

Razão Social: REDE EXS TELECOMUNICAÇÕES LTDA
CNPJ: 23.935.457/0001-93
Endereço: Q SIG QUADRA 1 LOTE 324 - SALA 324 ED PLATINUM OFFICE, Zona Industrial, Cep. 70.610-410, Brasília – DF
Telefone: (61) 99326-4424
E-mail: roselane@redeexs.com.br
Representante Legal: Roselane Gonzalez do Nascimento Almeida – CPF 704.702.600-25

CONTRATADA

Razão Social: SH7 PROTEÇÃO CIBERNÉTICA LTDA
CNPJ: 44.122.701/0001-79
Endereço: ST SRTVS QD 701 BLOCO O SALA, nº 122, NOVO CENTRO MULTIEMPRESARIAL, Bairro Asa Sul, Cep. 70.340-000 – Brasília - DF
Telefone: (21) 99195-9540
E-mail: regis.daniel@sh7.com.br
Representante Legal: Regis Daniel Almeida - CPF 704.702-600-25

1 - OBJETO DO CONTRATO

A **CONTRATADA**, especializada em serviços de cibersegurança, prestará à **CONTRATANTE** os serviços descritos no Anexo I, compreendendo a implementação, manutenção e suporte de soluções de segurança gerenciada, fornecendo equipamentos em comodato conforme necessário, para operação por profissionais qualificados, conforme condições detalhadas nos anexos.

2 - PRAZOS

O contrato terá vigência de 12 meses, podendo ser prorrogado por igual período mediante aditivo.

c: Protocolo 1.943/2025 | Anexo Doc: 3467D8059D2E021B662B981 protocolo 1943/2025 | Acesso CONTRATO_REDE_EXS_SH7_ASSINADO.pdf (232.230) 3/8/2025 14:09:47 16

3 - INSTALAÇÕES E EQUIPAMENTOS

A **CONTRATANTE** disponibilizará instalações, infraestrutura e recursos necessários para a execução dos serviços, comprometendo-se a utilizar produtos licenciados.

4 - VALORES E PAGAMENTOS

Valores e prazos de pagamento definidos no Anexo II, pagos mediante nota fiscal, com reajuste anual pelo INPC ou índice equivalente.

5 - OBRIGAÇÕES DA CONTRATANTE

Efetuar os pagamentos nas datas acordadas, fornecer informações necessárias, zelar pelos equipamentos em comodato, garantir acesso às instalações e cumprir as condições do contrato.

6 - OBRIGAÇÕES DA CONTRATADA

Fornecer informações e suporte necessário, prestar serviços conforme legislação vigente, cumprir prazos de atendimento do SLA (Anexo III), manter habilitação e qualificação durante a vigência e devolver documentos e bens do CONTRATANTE ao término do contrato.

7 - RESCISÃO

O contrato poderá ser rescindido nas hipóteses de descumprimento contratual, falência ou por interesse de uma das partes mediante aviso prévio de 30 dias, conforme cláusulas de rescisão previstas.

8 - DISPOSIÇÕES GERAIS

O contrato regula integralmente a relação entre as partes, vedando cessão sem anuência prévia, garantindo confidencialidade e integridade das informações, sem vínculo empregatício entre as partes.

9 - FORO

Fica eleito o Foro da Comarca de Brasília/DF para dirimir questões oriundas deste contrato.

Brasília/DF, [Data] 21 JANEIRO 2025

CONTRATANTE
REDE EXS TELECOMUNICAÇÕES LTDA
Assinatura: _____

CONTRATADA
SH7 PROTEÇÃO CIBERNÉTICA LTDA
Assinatura: _____

TESTEMUNHAS:

Nome: _____
CPF: _____

Nome: _____
CPF: _____

c: Protocolo 1.943/2025 | Anexo Doc. 3467D88059D2E021B6628981.pdf | Página 3200/4726 (21/29) Acesso CONTRATO 029/2025 pelo LUIZ PAULO (21/29)

ACORDO DE COOPERAÇÃO TÉCNICA QUE ENTRE SI FAZEM A REDE EXS TELECOMUNICAÇÕES LTDA E A SH7 PROTEÇÃO CIBERNÉTICA LTDA, PARA FINS DE FORMALIZAÇÃO DA PARTICIPAÇÃO DESTA ÚLTIMA NO PROJETO DE CONECTIVIDADE E CIBERSEGURANÇA DO TRIBUNAL DE TRABALHO DA 23ª REGIÃO – MT.

DAS PARTES

REDE EXS TELECOMUNICAÇÕES LTDA, inscrita no CNPJ/MF sob nº 23.935.457/0001-93, com sede à Q SIG QUADRA 1 LOTE 324 - SALA 324 ED PLATINUM OFFICE, Zona Industrial, Cep. 70.610-410, Brasília – DF, neste ato representada por sua Sócia Diretora, **ROSELANE GONZALEZ DO NASCIMENTO ALMEIDA**, brasileira, casada, Empresária, CPF [redacted]2, doravante denominada **EXS**.

SH7 PROTEÇÃOE INTELIGÊNCIA CIBERNÉTICA LTDA, inscrita no CNPJ/MF sob nº 44.122.701/0001-79, com sede no ST SRTVS QD 701 BLOCO O SALA, nº 122, NOVO CENTRO MULTIEMPRESARIAL, Bairro Asa Sul, Cep. 70.340-000 – Brasília - DF, neste ato representada por seu Sócio, **REGIS DANIEL ALMEIDA**, brasileiro, casado, Empresário, CPF nº [redacted] doravante denominada **SH7**.

DAS DISPOSIÇÕES GERAIS

O presente **Termo Técnico de Parceria** visa atestar que as PARTES possuem **parceria técnica e operacional específica para o atendimento ao Tribunal Regional do Trabalho da 23ª Região**, no âmbito do **Contrato nº 33/2022**, publicado em 09/11/2022 no DOU, cujo objeto é a **prestação de serviços de comunicação de dados para interligação do site central do TRT23 com os sites remotos, incluindo conexão à internet**, sob regime de **empreitada por preço global**, firmado entre o TRT23 e a **REDE EXS**.

ESCOPO DA PARCERIA

1. **A REDE EXS** é a contratada pelo TRT23, sendo responsável pela entrega do serviço contratado de comunicação de dados e interligação dos sites conforme contrato supracitado.

c: Protocolo 1.943/2025 | Anexo Doc. 3467 - 8059 - 2025 - Protocolo 1.943/2025 | Anexo CONTRATO 33/2022 | Pág (235 de 239) 202/4726

2. **A SH7** atua em **parceria técnica e operacional**, fornecendo:
   - Apoio na implantação de conectividade;
   - Apoio técnico na integração e configuração de equipamentos;
   - Suporte de cibersegurança na arquitetura de rede implantada para o TRT23;
   - Monitoramento preventivo e apoio na gestão de incidentes de segurança cibernética vinculados ao ambiente operacional.

FINALIDADE

Este Termo tem por finalidade **comprovar perante o TRT23 e demais órgãos de controle que as PARTES atuam conjuntamente no cumprimento do contrato em tela**, garantindo a segurança, a continuidade e a qualidade dos serviços prestados.

VIGÊNCIA

Este Termo é válido enquanto vigorar o **Contrato 33/2022 do TRT23 (vigência: 08/11/2022 a 08/05/2025)**, podendo ser prorrogado em caso de prorrogação do referido contrato.

DECLARAÇÃO

As PARTES declaram, para os devidos fins, que possuem equipe técnica qualificada, alinhamento de processos e integração de sistemas, garantindo a execução colaborativa e integrada das atividades no referido contrato.

Brasília/DF, [DATA]. 21 JANEIRO 2025

REDE EXS TELECOMUNICAÇÕES LTDA

SH7 PROTEÇÃO CIBERNÉTICA LTDA

Comprovante de Pagamento Pix

Valor: R$ 7.460,00

Realizado em: 11/06/2025 - 14:05:17

Solicitante: ROSELANE GONZALEZ DO NASCIMENT

Cooperativa e conta origem: 3953/36087-6

Nome do destinatário: G2Z

CNPJ do destinatário: 44.122.701/0001-79

Instituição do destinatário: NU PAGAMENTOS - IP

Agência e conta do destinatário: 1 / 160626821-5

Nome do pagador: Rede Exs Telecomunicacoes Ltda

CNPJ do pagador: 23.935.457/0001-93

Instituição do pagador: BANCO COOPERATIVO SICREDI S.A.

ID da transação: E10736214202506111705O1kTrODMo1k

Autenticação Eletrônica: E107.3621.4202.5061.1170.501k.TrOD.Mo1k

Número de Controle: 12532167101

Emitido em: 03/07/2025 - 17:19:43

* A transação acima foi realizada no nosso Aplicativo Sicredi conforme as condições especificadas neste comprovante.
* Os dados digitados são de responsabilidade do usuário.
Serviços por telefone 3003 4770 (Capitais e Regiões Metropolitanas) / 0800 724 4770 (Demais Regiões)
SAC 0800 724 7220 / Ouvidoria 0800 646 25 19

Comprovante de Pagamento Pix

Valor: R$ 20.000,00

Realizado em: 03/07/2025 - 18:15:16

Solicitante: ROSELANE GONZALEZ DO NASCIMENT

Cooperativa e conta origem: 3953/36087-6

Nome do destinatário: G2Z

CNPJ do destinatário: 44.122.701/0001-79

Instituição do destinatário: NU PAGAMENTOS - IP

Agência e conta do destinatário: 1 / 160626821-5

Nome do pagador: Rede Exs Telecomunicacoes Ltda

CNPJ do pagador: 23.935.457/0001-93

Instituição do pagador: BANCO COOPERATIVO SICREDI S.A.

ID da transação: E10736214202507032114 32J8CBvC6q3

Autenticação Eletrônica: E107.3621.4202.5070.3211.432J.8CBv.C6q3

Número de Controle: 12731695532

Emitido em: 03/07/2025 - 18:15:19

* A transação acima foi realizada no nosso Aplicativo Sicredi conforme as condições especificadas neste comprovante.
* Os dados digitados são de responsabilidade do usuário.
Serviços por telefone 3003 4770 (Capitais e Regiões Metropolitanas) / 0800 724 4770 (Demais Regiões)
SAC 0800 724 7220 / Ouvidoria 0800 646 25 19

Comprovante de transferência

09 MAI 2025 - 13:56:57

Valor	R$ 35.000,00
Tipo de transferência	Pix

Destino

Nome	SH7 PROTECAO E INTELIGENCIA CIBERNETICA LTDA
Agência	0001
Conta	160626821-5

Origem

Nome	REDE EXS TELECOMUNICACOES LTDA
Agência	0001
Conta	959722940-1

Dados gerais do pagamento

Identificador	LtHhYIxLkO

Nu Pagamentos S.A. - Instituição de Pagamento
CNPJ 18.236.120/0001-58

ID da transação:
E18236120202505091656s10a4f89c0e

Estamos aqui para ajudar se você tiver alguma dúvida.

Me ajuda →

Ouvidoria: 0800 887 0463 |
ouvidoria@nubank.com.br (Atendimento das 8h

PROCURAÇÃO

A empresa **SH7 PROTECAO E INTELIGENCIA CIBERNETICA LTDA**, Inscrita no CNPJ sob o n° **44.122.701/0001-79**, sediada na Setor SRTVS Qd 701 bloco O - Sala 122, Multiempresarial, Asa Sul, Brasília-DF – Cep: 70.340-000, por intermédio de seu representante legal, Roselane Gonzalez do Nascimento Almeida, portadora da CNH sob nº [redacted], CPF sob nº [redacted], nomeia e constitui sua bastante procuradora , **Paola Derriaux Chastagnier,** inscrita no CPF sob o número [redacted], residente e domiciliado na cidade de Nova Friburgo, Rio de Janeiro, doravante denominada OUTORGADA, para representar a OUTORGANTE como se presente fosse, em qualquer instância, em portais de licitações, certames licitatórios, pregões e congêneres, de qualquer entidade de direito público ou privado, incluindo autarquias, sociedades de economia mista, fundações, empresas públicas e agências governamentais, podendo também, assinar, acordar, declarar, transigir, formular ofertas, lances e propostas verbais, assinar documentos, assinar comerciais, desistir verbalmente de formular ofertas, lances e propostas verbais, negociar redução de preços, recorrer, impugnar, esclarecer, tomar qualquer decisão durante todas as fases da licitação ou pregão, inclusive apresentar a declaração de que a OUTORGANTE licitante cumpre os requisitos de habilitação, apresentar envelopes de propostas de preços e documentação de habilitação, desistir expressamente da intenção de interpor recurso administrativo ao final da sessão, assinar a ata da sessão, prestar todos os esclarecimentos solicitados pelo pregoeiro ou pela comissão de licitação , praticando, enfim, todos os atos pertinentes permitidos em Direito, por mais especiais que seja, em nome da OUTORGANTE, em todo o território Nacional, o que tudo dará por firme, e valioso, a bem deste mandato.

A presente terá validade até 31 de dezembro de 2025.

Brasília, 03 de julho de 2025.

ROSELANE GONZALEZ DO NASCIMENTO ALMEIDA:07894477702

Assinado de forma digital por ROSELANE GONZALEZ DO NASCIMENTO ALMEIDA:07894477702
Dados: 2025.07.03 12:10:28 -03'00'

ROSELANE GONZALEZ DO NASCIMENTO ALMEIDA

CPF 078.944.777-02

ASSIS & SIQUEIRA
ADVOGADOS ASSOCIADOS

INSTRUMENTO DE PROCURAÇÃO

OUTORGANTE: SH7 PROTEÇÃO E INTELIGÊNCIA CIBERNÉTICA LTDA, Inscrita no CNPJ sob o n° 44.122.701/0001-79, com sede na St Srtvs Qd 701 Bloco O Sala 122, Novo Centro Multiemp, Asa Sul, Brasília, Df, neste ato, representada por sua sócia administradora Roselane Gonzalez do Nascimento Almeida, abaixo assinado.

OUTORGADAS: ASSIS E SIQUEIRA ADVOGADOS ASSOCIADOS, CNPJ Nº 40.960.488/0001-13, situada à Rua Coronel Aparício Borges, 1123, Porto Alegre, RS, CEP 90680-570, sociedade de advogados e suas sócias, **MARIANA GLORIA DE ASSIS**, brasileira, casada, advogada, inscrita no CPF sob o n. [redacted] e OAB/RS [redacted] e **MONIQUE SIQUEIRA DA SILVA,** brasileira, solteira, advogada, inscrita no CPF sob o n. [redacted] e OAB/RS [redacted], com endereço na Rua Coronel Aparício Borges, 1123, Porto Alegre/RS, CEP 90680-570, endereço eletrônico monique@assisesiqueira.adv.br e mariana@assisesiqueira.adv.br

PODERES: Pelo presente instrumento a outorgante confere à outorgada amplos poderes para o foro em geral, com cláusula "ad-judicia et extra", em qualquer Juízo, Instância ou Tribunal, podendo propor contra quem de direito, as ações competentes e defendê-lo nas contrárias, seguindo umas e outras, até final decisão, usando os recursos legais e acompanhando-os, conferindo-lhe ainda, poderes especiais para confessar, conhecer a procedência do pedido, desistir, renunciar ao direito sobre que se funda a ação, transigir, firmar compromissos ou acordos, podendo agir em Juízo ou fora dele, assim como substabelecer os poderes a outrem, com ou sem reservas de iguais poderes, para agir em conjunto ou separadamente com o substabelecido.

FINALIDADE: atuar administrativamente na defesa dos interesses da outorgante na via administrativa perante a Prefeitura Municipal de Cáceres.

Brasília, 15 de julho de 2025.

ROSELANE GONZALEZ DO NASCIMENTO ALMEIDA:07894477702

Assinado de forma digital por ROSELANE GONZALEZ DO NASCIMENTO ALMEIDA:07894477702
Dados: 2025.07.16 15:59:33 -03'00'

SH7 PROTEÇÃO E INTELIGÊNCIA CIBERNÉTICA LTDA

ILUSTRÍSSIMO SENHOR AGENTE DE CONTRATAÇÃO DA PREFEITURA MUNICIPAL DE CÁCERES - MT

REF.: PREGÃO ELETRÔNICO N.º 15/2025
PROCESSO ADMINISTRATIVO N. 29/2025

IRREGULARIDADE NA HABILITAÇÃO TÉCNICA DA EMPRESA SH7 PROTEÇÃO E INTELIGÊNCIA CIBERNÉTICA LTDA

F.V.B.N CONSTRUÇÕES E TECNOLOGIA LTDA, inscrita no CNPJ nº 24.148.452/0001-83, empresa licitante no âmbito do Pregão Eletrônico nº 15/2025, Processo Administrativo nº 29/2025, promovido pela Prefeitura Municipal de Cáceres - MT, vem, com fundamento no ***art. 165 da Lei nº 14.133/2021***, interpor o presente**:**

RECURSO ADMINISTRATIVO

Contra a habilitação da empresa **SH7 PROTEÇÃO E INTELIGÊNCIA CIBERNÉTICA LTDA,** inscrita no CNPJ: 44.122.701/0001-79, com base nos seguintes fundamentos:

I –DA TEMPESTIVIDADE.

O presente recurso é tempestivo visto que atende o mencionado no Art. 165, I, alínea “c” da Lei 14.133/2021, o prazo para apresentar o recurso administrativo em licitação são de 3 dias úteis, além do que consta no item 11.5 e seguintes do Edital de Licitação, tendo a habilitação do licitante ocorrida no dia **08/07/2025**, o termo final para apresentação das razões escritas será o dia **11/07/2025**.

II – DA ILEGALIDADE DO ATESTADO APRESENTADO.

Violação ao princípio da vinculação ao edital e à Lei n.º 14.133/2021

A empresa SH7 apresentou atestado técnico emitido pela empresa Rede EXS Telecomunicações Ltda, CNPJ nº 23.935.457/0001-93, cuja sócia é a mesma da SH7: Sra. Roselane Gonzalez do Nascimento Almeida, configurando, portanto, vínculo societário direto entre as duas empresas.

A existência desse vínculo afronta frontalmente o disposto no art. 67, §1º da Lei nº 14.133/2021, que exige a comprovação de aptidão por terceiros independentes e isentos. Além disso, viola o item 9.17.13.9.2 do Edital, que expressamente veda a aceitação de atestados emitidos por empresas com relação societária ou pertencentes ao **mesmo grupo econômico.**

Jurisprudência consolidada do Tribunal de Contas da União:

- Acórdão TCU nº 1.793/2011 – Plenário: “Atestados emitidos por empresas coligadas ou com sócios em comum não satisfazem a exigência legal.”

- Acórdão TCU nº 2.168/2020 – Plenário: “É inválido atestado entre empresas do mesmo grupo econômico.”

Tais precedentes reforçam o entendimento de que a comprovação técnica deve ser feita por terceiros efetivamente autônomos, sob pena de simulação de experiência e burla à competitividade.

III – DO DESCUMPRIMENTO DO ITEM 9.17.13.2 DO EDITAL.

Falta de comprovação do quantitativo mínimo exigido

O **item 9.17.13.2** do Edital estabelece que:

> “A licitante deverá comprovar, por meio de atestado(s), que executou pelo menos 30% do item de maior relevância do objeto licitado (Item 1), conforme definição do órgão.”

O objeto de maior relevância (Item 1) exige a execução de 2.076 unidades, devendo a empresa comprovar, no mínimo, 623 unidades.

Contudo, os atestados apresentados pela empresa SH7 não evidenciam a execução desse quantitativo mínimo, o que configura descumprimento expresso e objetivo do edital, violando o princípio da vinculação ao instrumento convocatório, previsto no ***art. 5º, inciso I, da Lei n.º 14.133/2021***.

Tal exigência não é meramente formal, mas essencial para garantir a capacidade técnica mínima da licitante, visando proteger o interesse público quanto à eficiência e à adequada execução contratual. A ausência dessa comprovação impõe a inabilitação da licitante, por inobservância de critério indispensável.

V – DA OBRIGATORIEDADE DE OBSERVÂNCIA AOS PRINCÍPIOS LEGAIS

A vinculação ao edital é princípio basilar das licitações públicas, consagrado expressamente na ***Lei n.º 14.133/2021, art. 5º, inciso*** I, e implica que a Administração e os licitantes devem obedecer fielmente às regras previstas no edital, não podendo inovar ou flexibilizar exigências técnicas previamente estabelecidas.

A admissão da habilitação com base em atestado irregular e quantitativo insuficiente viola os princípios da legalidade, da isonomia, da impessoalidade e da moralidade, podendo gerar:

- **Nulidade do procedimento licitatório ou do contrato (art. 147 da Lei nº 14.133/2021);**
- **Responsabilização do agente público envolvido, nos termos do art. 5º da mesma lei;**
- **Configuração de ato de improbidade administrativa (art. 11 da Lei nº 8.429/1992), por violação ao dever de legalidade e à fiel observância do edital.**

V – DOS PEDIDOS

Diante de todo o exposto, requer-se:

1. O recebimento e conhecimento deste recurso administrativo, com fundamento no ***art. 165 da Lei nº 14.133/2021;***

2. A verificação formal do vínculo societário entre a empresa SH7 PROTEÇÃO E INTELIGÊNCIA CIBERNÉTICA LTDA e a empresa Rede EXS Telecomunicações Ltda, configurando grupo econômico, o que invalida o atestado técnico apresentado;

3. A análise objetiva do não atendimento ao quantitativo mínimo de 30% do item de maior relevância, em afronta ao ***item 9.17.13.2 do edital***;

4. A inabilitação da empresa SH7, por apresentar documentação técnica incompatível com as exigências editalícias;

5. A responsabilização da Administração, em caso de inércia, pela eventual homologação indevida, com comunicação aos órgãos de controle competentes, se necessário.

Por fim, requer-se, caso não seja acolhido o presente recurso, que a decisão administrativa que o indeferir seja fundamentada de forma clara, precisa e documental, nos termos dos princípios da motivação, publicidade e legalidade, conforme exige o art. 20 da Lei nº 14.133/2021.

Cáceres - MT, 11 de julho de 2025.

F V B N CONTRUCOES E TECNOLOGIA LTDA:24148452000183

Assinado de forma digital por F V B N CONTRUCOES E TECNOLOGIA LTDA:24148452000183
Dados: 2025.07.11 08:56:36 -04'00'

F.V.B.N Construções e Tecnologia Ltda
CNPJ: 24.148.452/0001-83
Fredolino Vieira De Barros Neto
Cargo: Sócio Administrador

De: GIRLANE P. - SMEAE - CTI

Para: PGM-CJL - Coordenadoria Jurídico de Licitação

Data: 18/07/2025 às 08:52:32

Prezado(a) Procurador(a),

Cumprimentando-a cordialmente, dirijo-me a Vossa Senhoria para encaminhar parecer técnico acerca da interposição de recurso e contra razões do presente Processo Licitatório e solicitar a emissão de parecer jurídico sobre a regularidade da habilitação da empresa SH7 e a legalidade da eventual manutenção ou desclassificação da mesma, com fundamento na Lei nº 14.133/2021.

_

Girlane Vieira Pereira

Coordenadora de Informações Sistêmicas e Tecnologia de Informação

Anexos:

PARECER_17_07_2025.pdf

Assinado digitalmente (anexos) por:

Assinante	Data	Assinatura	
GIRLANE VIEIRA PEREIRA	18/07/2025 08:52:47	1Doc	GIRLANE VIEIRA PEREIRA CPF 024.XXX.XXX-66
Ademar Alves Trindade	18/07/2025 08:56:32	1Doc	ADEMAR ALVES TRINDADE CPF 700.XXX.XXX-00

Para verificar as assinaturas, acesse **https://caceres.1doc.com.br/verificacao/** e informe o código: **87DF-A0D4-4619-5447**

Prezado Pregoeiro,

Trata-se de resposta ao recurso administrativo interposto pela empresa **F.V.B.N CONSTRUÇÕES E TECNOLOGIA LTDA**, no qual são alegadas supostas irregularidades na habilitação da empresa **SH7 PROTEÇÃO E INTELIGÊNCIA CIBERNÉTICA LTDA**, especificamente quanto à legalidade dos atestados apresentados e ao cumprimento das exigências editalícias relativas à comprovação da capacidade técnico-operacional.

Após análise técnica minuciosa dos argumentos apresentados, temos a expor e considerar:

I – DA ALEGAÇÃO DE ILEGALIDADE DOS ATESTADOS APRESENTADOS PELA LICITANTE HABILITADA

A recorrente sustenta que os atestados apresentados pela empresa SH7 seriam inválidos por supostamente não atenderem ao disposto na legislação vigente, notadamente no que tange à exigência de serem emitidos por terceiros independentes e isentos.

Contudo, tal alegação não encontra amparo legal. A Lei Federal nº 14.133/2021, em seu artigo 67, §1º, dispõe que:

> *"A exigência de atestados será restrita às parcelas de maior relevância ou valor significativo do objeto da licitação, assim consideradas as que tenham valor individual igual ou superior a 4% (quatro por cento) do valor total estimado da contratação."*

A norma em referência trata da restrição quanto à **exigibilidade dos atestados**, não impondo, em momento algum, **vedação à aceitação de atestados emitidos por empresas pertencentes ao mesmo grupo econômico ou com vínculos societários**, conforme pretende fazer crer a recorrente.

Ademais, o **edital** é claro ao dispor, em seu item 9.17.1, que será aceita a **comprovação de aptidão por meio de atestados emitidos por pessoas jurídicas de direito público ou privado**, e no item 9.17.13, exige-se a **demonstração de capacidade técnico-operacional** mediante apresentação de atestados que comprovem a execução de serviços compatíveis, em características, quantidades e prazos, com o objeto licitado.

Logo, os documentos apresentados pela licitante SH7 encontram-se em conformidade com as exigências editalícias e legais, sendo **lícita e legítima sua aceitação** no presente certame.

II – DO ALEGADO DESCUMPRIMENTO DO ITEM 9.17.13.2 DO EDITAL

Assinado por 2 pessoas: GIRLANE VIEIRA PEREIRA e ADEMAR ALVES TRINDADE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/87DF-A0D4-4619-5447 e informe o código 87DF-A0D4-4619-5447

A empresa recorrente sustenta que a licitante SH7 PROTEÇÃO E INTELIGÊNCIA CIBERNÉTICA LTDA não teria atendido ao quantitativo exigido no item 1 do edital, sob o argumento de que deveria apresentar atestados comprovando a execução de, no mínimo, **623 unidades**, correspondente a **30% das 2.076 unidades** revistas.

Contudo, tal interpretação mostra-se **equivocada**, haja vista que o próprio edital é claro ao estabelecer que o contrato terá **vigência de 12 (doze) meses**, sendo que as **quantidades estimadas em cada item correspondem a fornecimentos mensais**.

Com efeito, o **quadro de itens constante no Termo de Referência** indica, de forma inequívoca, que as **2.076 unidades previstas para o Item 1** representam o somatório anual da estimativa de **173 unidades mensais** (173 × 12 = 2.076).

Importante destacar que essa interpretação já havia sido **formalmente esclarecida** no âmbito deste processo, por meio do **Despacho nº 45 datado de 05/06/2025**, constante do **Processo Licitatório n.º 029/2025**, em resposta à solicitação da empresa NET SERVICES, no qual foi **expressamente registrado que o quantitativo correto a ser considerado para fins de comprovação corresponde a 173 unidades mensais**, e não ao total anual.

Dessa forma, a exigência constante no item 9.17.13.2 do edital, que impõe a comprovação de **30% da parcela de maior relevância**, deve incidir sobre o valor mensal estimado, ou seja, **30% de 173 unidades**, o que corresponde a aproximadamente **52 unidades**.

Adicionalmente, cumpre frisar que o edital é expresso ao **vedar a exigência de comprovação integral do quantitativo estimado**, justamente com o intuito de assegurar a competitividade e a ampla participação no certame, em consonância com os princípios da **razoabilidade, proporcionalidade e isonomia**.

No caso concreto, a empresa SH7 apresentou atestados que comprovam a prestação do serviço em quantidade correspondente a **65 unidades do Item 1**, **superando, portanto, o percentual mínimo exigido no edital**. Ressalte-se que tais documentos foram devidamente analisados e aceitos pela comissão técnica responsável, conforme os critérios estabelecidos na legislação aplicável e no próprio instrumento convocatório.

Dessa forma, resta **amplamente demonstrado** que a licitante SH7 **cumpriu integralmente a exigência editalícia prevista no item 9.17.13.2**, sendo, portanto, **descabida a alegação de inabilitação por suposto descumprimento quantitativo.**

III – CONCLUSÃO

Assinado por 2 pessoas: GIRLANE VIEIRA PEREIRA e ADEMAR ALVES TRINDADE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/87DF-A0D4-4619-5447 e informe o código 87DF-A0D4-4619-5447

Diante de todo o exposto, verifica-se que **os argumentos apresentados pela empresa recorrente não possuem respaldo legal ou fático** que justifique a reforma da decisão de habilitação da empresa SH7.

Ressalta-se ainda que os documentos foram criteriosamente analisados pela equipe técnica responsável, que concluiu pela **regularidade e adequação da documentação apresentada**, em consonância com os princípios da legalidade, isonomia e competitividade que regem os processos licitatórios.

Assim sendo, opina-se pela **total improcedência do recurso interposto pela empresa F.V.B.N CONSTRUÇÕES E TECNOLOGIA LTDA**, mantendo-se inalterada a decisão que declarou habilitada a empresa SH7 PROTEÇÃO E INTELIGÊNCIA CIBERNÉTICA LTDA.

Permanecemos à disposição para prestar eventuais esclarecimentos adicionais que se fizerem necessários.

Assinado por 2 pessoas: GIRLANE VIEIRA PEREIRA e ADEMAR ALVES TRINDADE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/87DF-A0D4-4619-5447 e informe o código 87DF-A0D4-4619-5447

VERIFICAÇÃO DAS ASSINATURAS

Código para verificação: 87DF-A0D4-4619-5447

Este documento foi assinado digitalmente pelos seguintes signatários nas datas indicadas:

GIRLANE VIEIRA PEREIRA (CPF 024.XXX.XXX-66) em 18/07/2025 07:52:45 GMT-04:00
Papel: Parte
Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

ADEMAR ALVES TRINDADE (CPF 700.XXX.XXX-00) em 18/07/2025 07:56:30 GMT-04:00
Papel: Parte
Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

Para verificar a validade das assinaturas, acesse a Central de Verificação por meio do link:

https://caceres.1doc.com.br/verificacao/87DF-A0D4-4619-5447

ecCLOUD Controller

User Manual

www.edge-core.com

User Manual

ecCLOUD Controller

Cloud-Based Wired and Wireless Device Network Controller

E022025-MR-R10

How to Use This Guide

This guide includes detailed information on the Edgecore ecCLOUD Controller, including how to create Clouds and Sites, and how to manage your APs and other devices. To manage your network devices effectively and ensure trouble-free operation, you should first read the relevant sections in this guide so that you are familiar with all features.

Who Should Read This Guide?

This guide is for network administrators who are responsible for operating and maintaining network equipment. The guide assumes a basic working knowledge of LANs (Local Area Networks), the Internet Protocol (IP), and Simple Network Management Protocol (SNMP).

How This Guide is Organized

The organization of this guide is based on the ecCLOUD Controller web management interface. An introduction and initial configuration information is also provided.

The guide includes these sections:

- Section I "Getting Started" — Includes an introduction to the ecCLOUD Controller and initial access steps.
- Section II "Cloud Configuration" — Includes all management options available through the ecCLOUD Controller web site.

Conventions

The following conventions are used throughout this guide to show information:

Note: Emphasizes important information or calls your attention to related features or instructions.

Caution: Alerts you to a potential hazard that could cause loss of data, or damage the system or equipment.

Warning: Alerts you to a potential hazard that could cause personal injury.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - Edgecore ecCLOUD User Manual_v2.0_20250227.pdf (3/301) 1/96/4726

Revision History

This section summarizes the changes in each revision of this guide.

February 2025 Revision

This is the tenth revision of this guide. It includes the following change:

- Added support for EAP112-L, EAP112-H, and EAP105, see "Edgecore APs" on page 27
- Added restricted access to cloud management portal by IP ACL, see "Changing the Cloud Properties" on page 49
- Updated Site Configuration - Wi-Fi 6 to Site Configuration - Wi-Fi 6 & Newer to include WIFI-7 models, see "Wireless SSID Configuration" on page 161 and Figure 168
- Added support to 320 MHz channel bandwidth for Radio Mode “802.11 be”, see "Physical Radio Settings" on page 174 and "Physical Radio Settings" on page 233
- Added support for Hotspot RADIUS DAE Configuration, see "Dynamic Authorization" on page 193 and Figure 193
- Added support for MQTT in iBeacon, see Publish MQTT" on page 205 and Figure 206
- Added support for HaLow Open Mesh Mode, see "Mesh Radio" on page 232
- Updated LinqPath to classify links with RSSI below -70dBm as “No Link,” see "Expected RSSI" on page 253 and "Expected RSSI with rain" on page 254

July 2024 Revision

This is the ninth revision of this guide. It includes the following change:

- Added Smart NVR Add-on with support for IP Cameras, see "Using the Smart NVR Add-On" on page 88

June 2024 Revision

This is the eighth revision of this guide. It includes the following changes:

- Updated the Captive Portal and SSID configuration descriptions to include Microsoft 365 Authentication, see "SSID Configuration" on page 82 and Figure 76
- Added visibility for network topology update time, see "Locations and Maps" on page 99 and Figure 98
- Added Microsoft 365 Authentication support, see "Microsoft 365 Authentication" on page 171 and Figure 172

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - Termo de Referência - Anexo IV - Modelo de Declaração de Vistoria - 029_2025_page_27.pdf (4/301) 1409/4726

- Updated System Settings for WiFi 6 Sites to include SNMP Trap Server, see "SNMP" on page 200 and Figure 200

March 2024 Revision

This is the seventh revision of this guide. It includes the following changes:

- Added Report Management feature, see "Report Management" on page 70
- Added Aprecomm's Virtual Wireless Expert Add-on, see "Using the Aprecomm Add-On" on page 84
- Updated the LinqPath Tool to include Distance Steps and corresponding Expected MCS & Data Rate, see "Using the LinqPath Tool" on page 252 and Figure 249

December 2023 Revision

This is the sixth revision of this guide. It includes the following changes:

- Updated Supported Models, see "The following devices are supported by ecCLOUD:" on page 27
- Updated Figure 20, see "Device Configuration Changes" on page 41
- Modified Cloud Management Add-ons, see "Add-Ons" on page 74
- Modified Target Options in Firewall Settings, see WiFi-5 "Firewall Settings" on page 139 and WiFi-6 "Firewall Settings" on page 186
- Added SSID Isolation Support, see "Wireless SSID Configuration" on page 161
- Added Dynamic PSK Keys Support, see "Security Settings" on page 163
- Added Mgmtd Log and SysLog Level Capability, see "System Settings" on page 196
- Added SNMPv3 User Support for WiFi-6, see "SNMPv3 User" on page 205
- Added Site SD-WAN Settings, see "Site SD-WAN Configuration" on page 216
- Added 6 GHz Band Support, see "WiFi 6 and Newer Device Configuration" on page 228
- Added Device SD-WAN Settings, see "SD-WAN Device Configuration" on page 286

August 2023 Revision

This is the fifth revision of this guide. It includes the following changes:

- Added OpenRoaming, see "Adding an SSID" on page 162 and "OpenRoaming" on page 206

1Doc: Protocolo 1.943/2025: Anexo Administrativo nº 07/2025 - Aquisição de Solução de Gestão de Rede Wireless - 1738/4726
Anexo_Administrativo_nº_07_2025_-_Aquisicao_de_Solucao_de_Gestao_de_Rede_Wireless_-_1738_4726_20250227.pdf (5/301)

- Added RF Isolation, see "Radio Settings" on page 173
- Modified Broadcast Rate, see "Radio Settings" on page 173
- Added Site Grouping, see "Site Grouping" on page 62
- Added "Always Follow Cloud Configuration" on page 65

March 2023 Revision

This is the fourth revision of this guide. It includes the following changes:

- Added Airtime Fairness, see "Global Settings" on page 174
- Added 802.11v, see "Adding an SSID" on page 162
- Added BLE Tx Power, see "iBeacon" on page 204
- Added BLE Scan, see "iBeacon" on page 237
- Updated Channel Bandwidth, see "Physical Radio Settings" on page 174 and "Physical Radio Settings" on page 233
- Updated BSS Coloring, see "Physical Radio Settings" on page 174 and "Physical Radio Settings" on page 233
- Updated Minimum Allowed Signal, see "Adding an SSID" on page 120 and "Adding an SSID" on page 162
- Added Terragraph device configuration, see "Terragraph Device Configuration" on page 257
- Added Site Terragraph VLAN settings, see "VLAN Settings" on page 214

November 2022 Revision

This is the third revision of this guide. It includes the following changes:

- Added batch upload information, see "Creating Your First Cloud" on page 29 and "Add Devices" on page 100
- Updated Cloud menu, see "Managing Your Devices" on page 54
- Updated WiFi 5/WiFi 6 configuration, see "WiFi Configuration" on page 103
- Renamed chapter "Site WiFi 5 Configuration" on page 118
- Added Multicast/Broadcast Rate, see "Adding an SSID" on page 120
- Added OSEN, see "Adding an SSID" on page 120

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 01 - 2025 | Anistia EC processo digital Manual 029_2025_20250227.pdf (6/301) 1719/4726

- Added AuthPort External RADIUS, see "Radio Settings" on page 128
- Added Disabled W52 Channel, see "Radio Settings" on page 128
- Added IPv6 settings, see "Internet Settings" on page 132
- Added Uplink 802.1P, see "VLAN Settings" on page 135
- Added Enable RSTP, see "Local Network Settings" on page 137
- Added DNS Entries, see "Local Network Settings" on page 137
- Added ARP Inspection, see "ARP Inspection" on page 141
- Added DHCP Snooping, see "DHCP Snooping" on page 142
- Added AuthPort Remote Splash Page with External RADIUS, see "Hotspot Settings" on page 142
- Added DNS Entries and DNS Mapping, see "Hotspot Settings" on page 142
- Added Generate NAS ID, see "RADIUS Server" on page 146
- Added HTTPS Login, see "Captive Portal" on page 147
- Modified Cloud and Radio LEDs, see "System Settings" on page 149
- Added MSP Mode, see "System Settings" on page 149
- Added SNMP IPv6 Write Community and SNMP Location, see "SNMP" on page 154
- Added IGMP Snooping, see "IGMP Snooping" on page 157
- Added LLDP, see "LLDP" on page 158
- Added iBeacon, see "iBeacon" on page 158
- Added SNMPv3 User, see "SNMPv3 User" on page 159
- Added chapter "Site WiFi 6 Configuration" on page 160
- Added chapter "Site Terragraph Configuration" on page 210
- Renamed chapter "WiFi 5 Device Configuration" on page 219
- Added chapter "WiFi 6 and Newer Device Configuration" on page 228

May 2021 Revision

This is the second revision of this guide. It includes the following changes:

1Doc: Protocolo 1.943/2025 | Anexo Administrativo EC processo licitatório 029_2025_pregão 027.pdf (7/301) 3440/4726

- Added support for EAP101 and EAP102.
- Added section "QR Code Onboarding" on page 35.

December 2020 Revision

This is the first revision of this guide.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 01 - Aquisição de Licenças de Uso de Software (8/301) 1443/4726

Contents

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - 29/12/2025 | Anexo EC_ecCloud_UserMan_029_20252025227.pdf (9/301) 3742/4726

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf_Administrativo_processo_licitatorio_029_2025_pdf_3467D8B059B3E321B66283D2925AD1E0.pdf (10/301) 3445/4746

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 08059386321866289 29_2025_Administrativo_processo_licitatorio_029_2025_pdf_27.pdf (11/301) 11/4726

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 34670/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf_27.pdf (12/301) 3445/4746

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 de 2025 | Anexo Administrativo 3 de 2025 - Anistia EC_processo_licitatorio_029_2025_pdf (13/301) 13/301

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 34670880598386321866289 2025 Administrativo_processo_licitatorio_029_2025_pdf_27.pdf (14/301) 14/4746

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 08059386120256289 2025 Administrativo_processo_licitatorio_029_2025_pdf_27.pdf (15/301) 15/4746

Figures

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 08059386321866289 2025 | Anistratec_ecCloud_UserMan_029_20252026027.pdf (16/301) 1429/4746

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 08059386321866289_2025_Anexo_Administrativo_Cloud_Usuario_029_20252026227.pdf (17/301) 1750/4746

Figures

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (18/301) 1743/4746

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 08059386321866289 2025 | Anistia EC processo Distorção 029 2025 26 27.pdf (19/301) 1732/4746

Figures

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 34670808059386321866289 2025 Anistratec_procesoDistanciamiento_2025_20250627.pdf (21/301) 1736/4746

Figures

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - 2025 | Anexo Administrativo 3 - 2025 | Anexo Administrativo 3 - 2025_pdf (23/301) 1736/4726

Figures

Section I

Getting Started

This section provides an overview of the ecCLOUD Controller software and describes the initial steps required to start using the service.

This section includes these chapters:

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - Termo de Referência 29/2025 | Anistia EC_ecCLOUD_UserManual_029_2025_250227.pdf (25/301) 1758/4746

1 Introduction

This chapter includes the following sections:

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - 29/2025 | Anexo EC_processo_licitatorio_029_2025_pdf (26/301) 1759/4746

The Edgecore ecCLOUD Controller is a cloud-based network service available from anywhere through a web-browser interface.

The ecCLOUD Controller software is highly scalable and able to manage an unlimited number of networks and devices. Combining both network management and wireless controller features, it enables Edgecore access points (APs) and switches to automatically connect and be managed as one network.

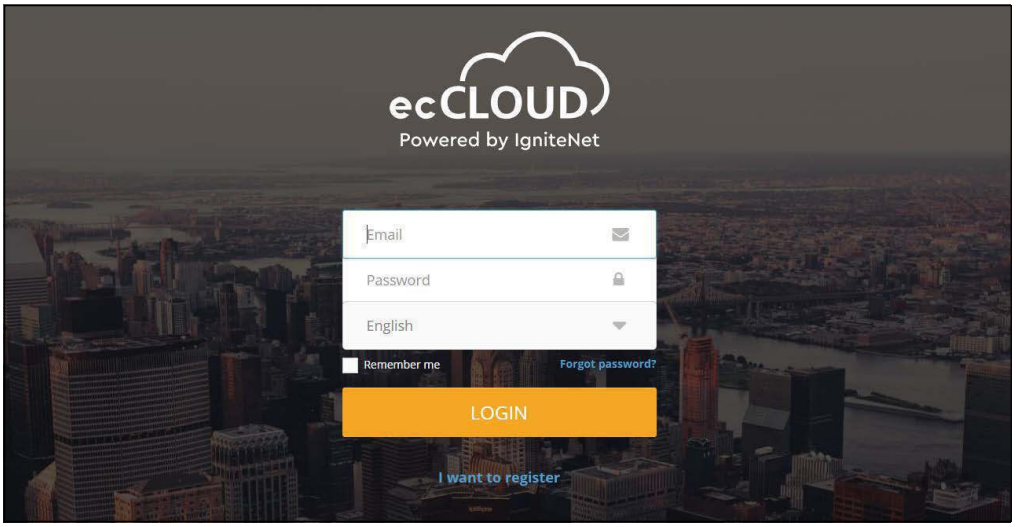
The following devices are supported by ecCLOUD:

- **Edgecore APs**: EAP101, EAP102, EAP104, EAP104 Lite, EAP112-L, EAP112-H, EAP105, ECW5211-L, ECW5410-L, ECWO5211-L, OAP100, OAP100e, OAP101, OAP101 6E, SP-W2-AC1200 (L), SP-W2M-AC1200, SP-W2M-AC1200-POE, SS-W2-AC2600
- **Edgecore Switches**: ECS2100-10P, ECS2100-10T, ECS2100-28P, ECS2100-28PP, ECS2100-28T, ECS2100-52T, ECS4100-12PH, ECS4100-12T, ECS4100-28P, ECS4100-28T, ECS4100-52P, ECS4100-52T, ECS4120-28Fv2, ECS4120-28Fv2-I, ECS4120-28T, ECS4120-52T, ECS4125-10P, ECS4150-28P
- **MLTGs**: MLTG-360, MLTG-CN, MLTG-CN LR
- **SD-WAN**: SDW102

ecCLOUD Controller Login

From a web browser, go to **cloud.ignitenet.com** to register an account and start creating your own cloud networks and sites.

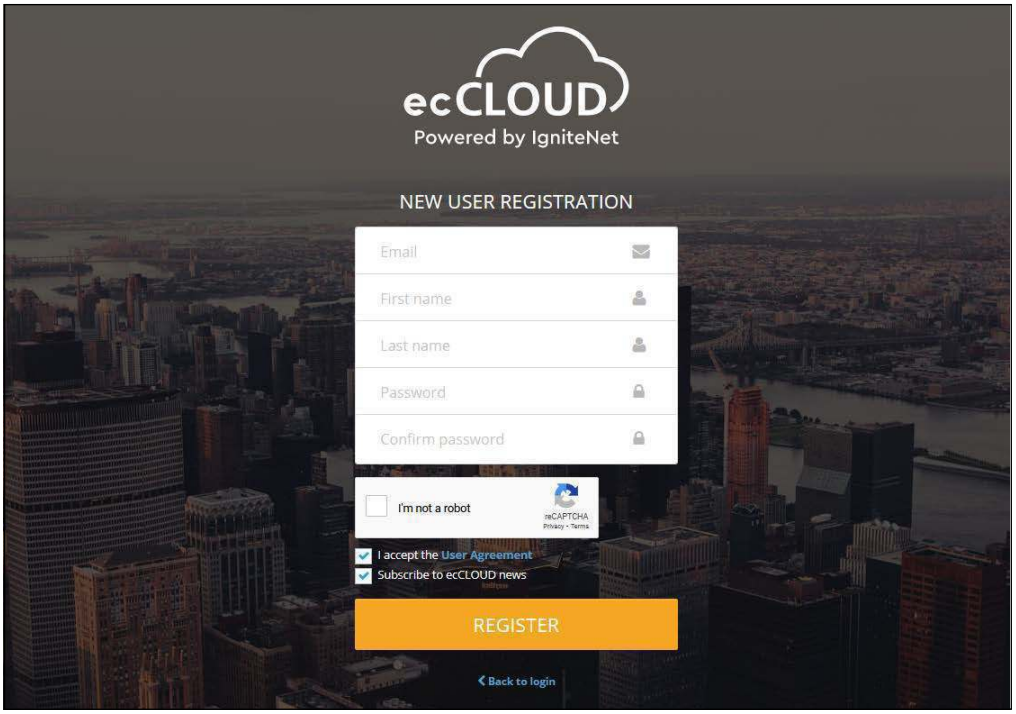
Figure 1: ecCLOUD Controller Login



1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 de 3 - 29/12/2025 | Anexo_Administrativo_3_-_Edgecore_ecCloud_Licencia_029_20252026_27.pdf (27/301) 1760/4746

Click “I want to register” to create a new account.

Figure 2: New User Registration



Enter your email address and specify a first and last name. Set a password to protect access to your account, click “I am not a robot,” and then click REGISTER.

Note: You must have a valid email address in order to create your user profile.

The ecCLOUD Controller sends a verification email to the account email address. When you receive the email, click on the provided link to activate your account.

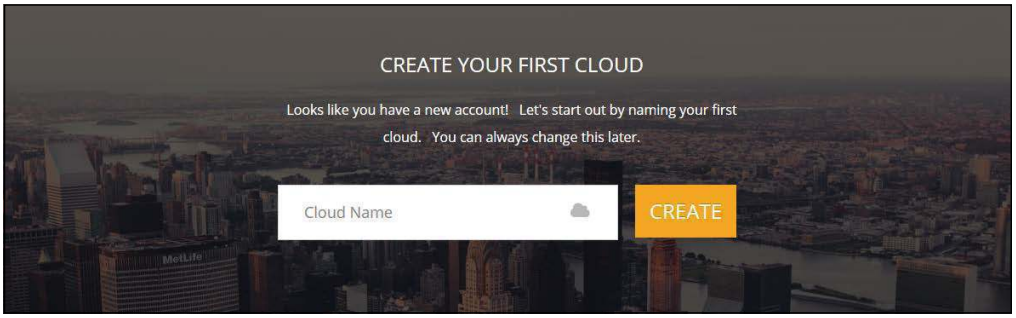
1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 de 3 - Termo de Referência - Aquisição de Licenças de Software (28/301) 1763/4726

Creating Your First Cloud

The ecCLOUD Controller uses a cloud-like account – it houses a group of sites, which are logical groupings of your managed devices. Each cloud will have its own set of users and configuration settings. As an end-user, you can join as many clouds as you want, with different roles on each cloud.

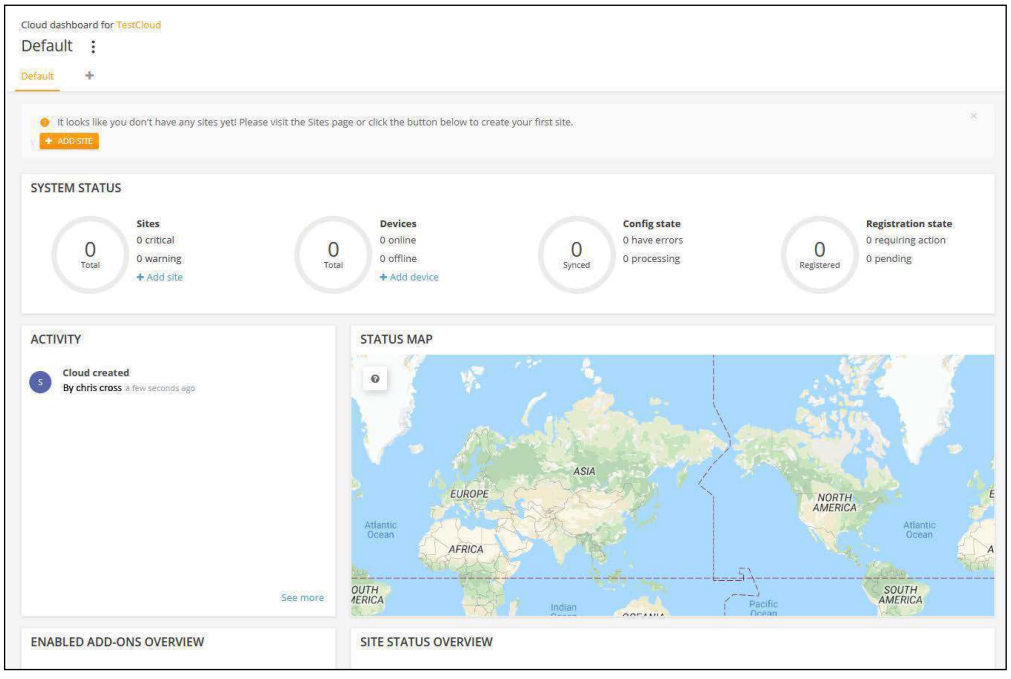
Once you are registered as a user on the ecCLOUD Controller, you are given the option to create a cloud when you first log in.

Figure 3: Creating a Cloud on First Login



After entering a name for your first cloud, click CREATE to display the Cloud Dashboard.

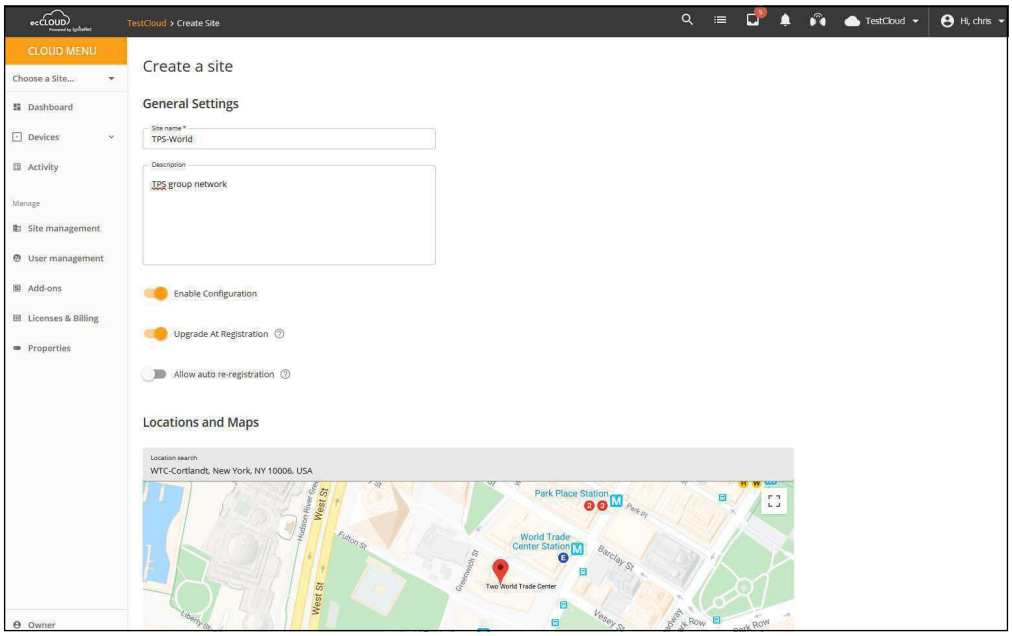
Figure 4: Create Your First Cloud



1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - Plataforma de Gestão de Dados Municipais - 2025_20250627.pdf (29/301) 1762/4746

Click ADD SITE and enter information for your first site.

Figure 5: Defining Your First Site



Set the following properties for devices at your site:

- **Enable Configuration**: This setting has the following options:
  - ON: Enables you to remotely configure your devices. (default)
  - OFF: Your devices need to be configured locally. However, you can still remotely monitor your devices and you will still receive alerts when a device goes offline.
- **Upgrade At Registration**: Enable this setting if you want your devices to be automatically upgraded to the latest firmware after registration. It is recommended that you keep this setting on.
- **Allow auto re-registration**: When this setting is enabled, your devices will automatically re-register when they are reset to defaults. If this setting is disabled, a user must log in to the cloud and manually chose the action to take when a device attempts to re-register.

After configuring all the site information, click CREATE to create the site.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 08059386321866289 2025 | Anexo EC_acesso_dados_Marco_2025_20250227.pdf (30/301) 1465/4726

After setting the regulatory country and local logins, click “Save” to save your configuration.

Figure 6: Saving the Site Configuration

When you first save the site configuration, you are prompted to add devices (wireless, switches, MeshLinqs, GLinqs) to your new site. Click “ADD DEVICES” to continue.

Figure 7: Add Devices Prompt

Alternatively, you can click Devices-Wireless or Switches on the main menu to access the device management view.

You are now ready to start adding Edgecore APs or switches to your cloud network.

Figure 8: Device Management View

Click on ADD DEVICE to access the “Register new Devices” page.

Fill in the serial number, MAC address and name, and then click SAVE. Alternatively, you can use the QR code on a device (see “QR Code Onboarding”

1Doc: Protocolo 1.943/2025 | Anexo Administrativo EC_proceso_Licitatorio_029_2025_20250627.pdf (31/301) 1486/4726

on page 35), or use a barcode scanner. Or, you can upload information for a batch of devices in a file.

Turn "Enable barcode scanning mode" ON to quickly scan barcodes and enter the serial number and MAC addresses of your devices. Once entered, turn off the barcode scanning mode and enter the names of the devices manually. Click the SAVE button when you are ready to add your new devices to the site.

Turn on the "Always follow cloud configuration" feature to ignore any local configuration changes received from a device. For more information, see "Always Follow Cloud Configuration" on page 65.

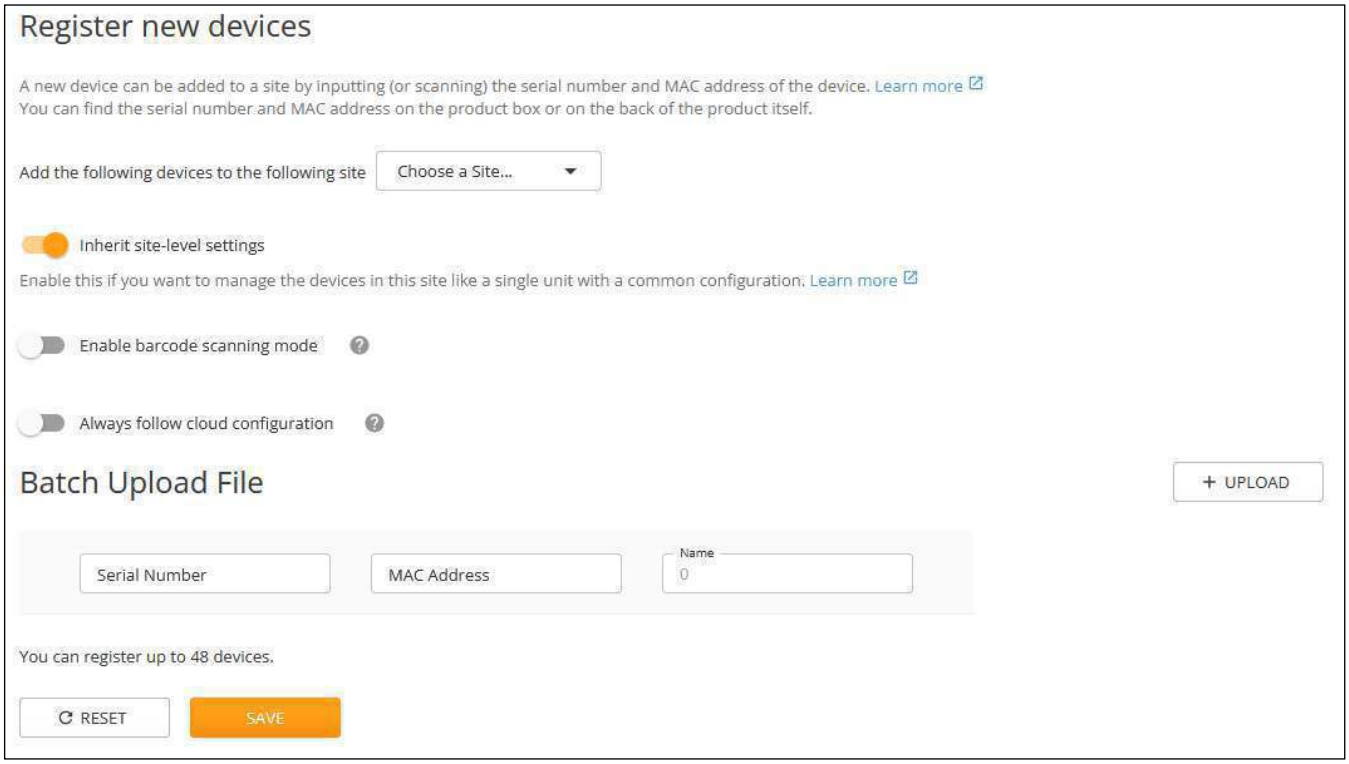
For a batch upload, prepare a list of devices in a CSV (comma-separated values) file. A CSV file is a plain text file in which information is separated by commas. For each device, the serial number, MAC address and name should be entered on one line, as in the following format.

```
<Serial Number 1>,<MAC 1>,<Device Name 1>
<Serial Number 2>,<MAC 2>,<Device Name 2>
```

Click the UPLOAD button to upload your CSV file.

For more information on registration, see "Understanding Device Registration" on page 39.

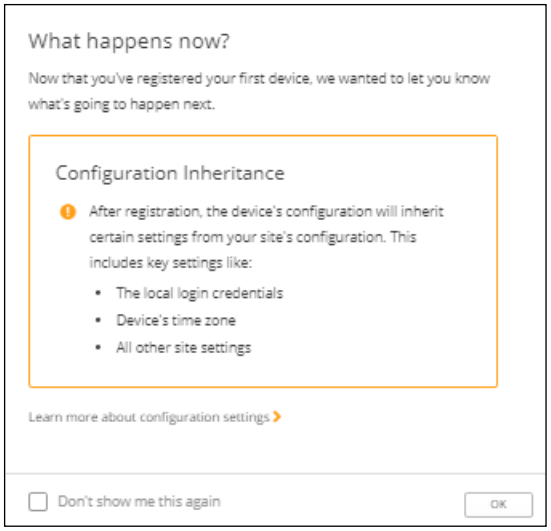
Figure 9: Adding Devices



1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3467088059838632168628937_2025_Anexo_Administrativo_EC_processo_licitatorio_029_2025_pdf.pdf (32/301) 1465/4746

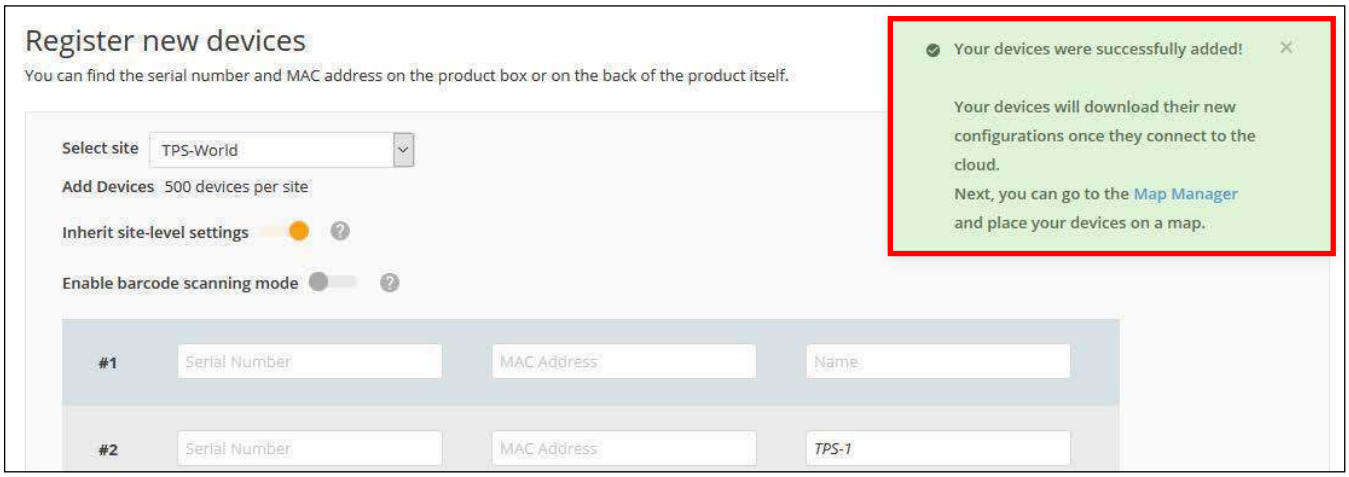
When the controller adds a device, the following pop-up window is displayed warning you that the device will inherit settings from the ecCLOUD controller site configuration. For more information on inheritance, see "Understanding Configuration Inheritance" on page 37.

Figure 10: Adding Devices Warning Message



Further, at the top of the "Register new devices" page a message appears indicating that devices have been successfully added. Click on the blue link "Map Manager" in the message to place your device on a map. See "Placing a Device on a Map" on page 35.

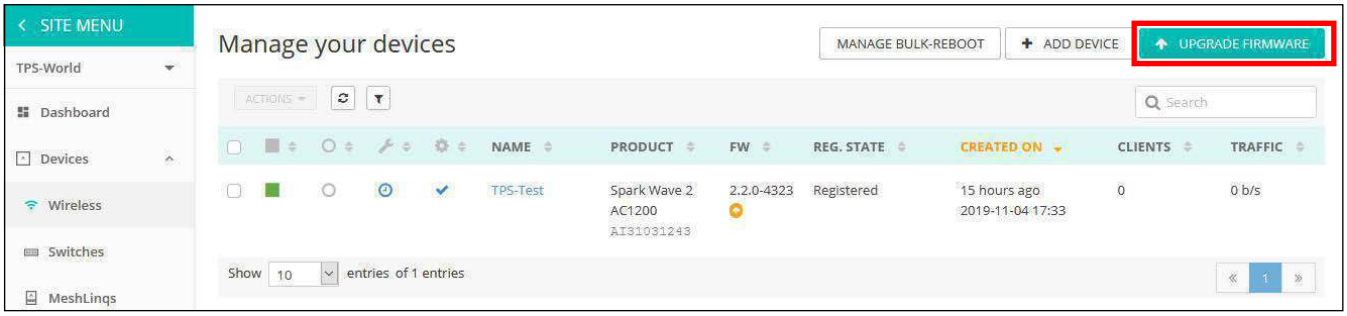
Figure 11: Adding Devices Successful Message



1Doc: Protocolo 1.943/2025 | Anexo Administrativo 08059386121866289 29/2025 Administrativo_ecCloud_Usuario_029_20252026227.pdf (33/301) 33/4726

Additionally, with the first device added to the site the “Upgrade Firmware” button appears above the device list. Refer to “Schedule Maintenance Tasks” on page 113.

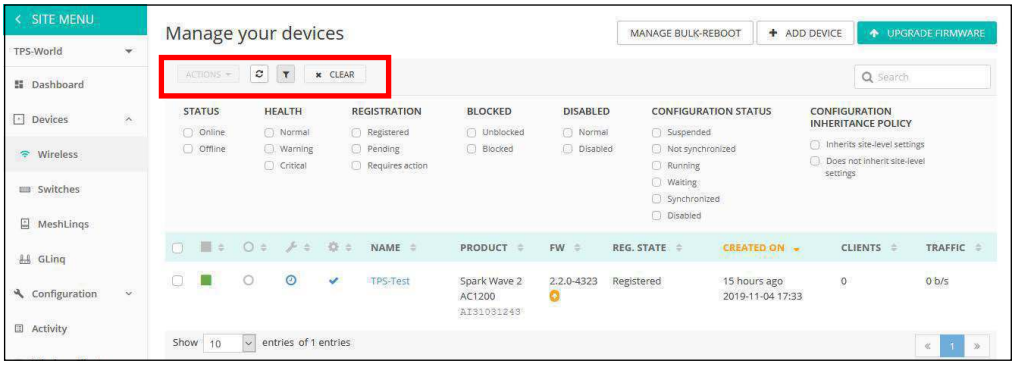
Figure 12: Firmware Upgrade Button



Clicking the filter (funnel shape) button in the upper left of the device manager view enables devices in the list to be filtered based on various properties. Chose the properties from the selection lists under Status, Health, Registration, Blocked, Disabled, Configuration Status, and Configuration Inheritance Policy.

Click the “Clear” button to reset all the filters.

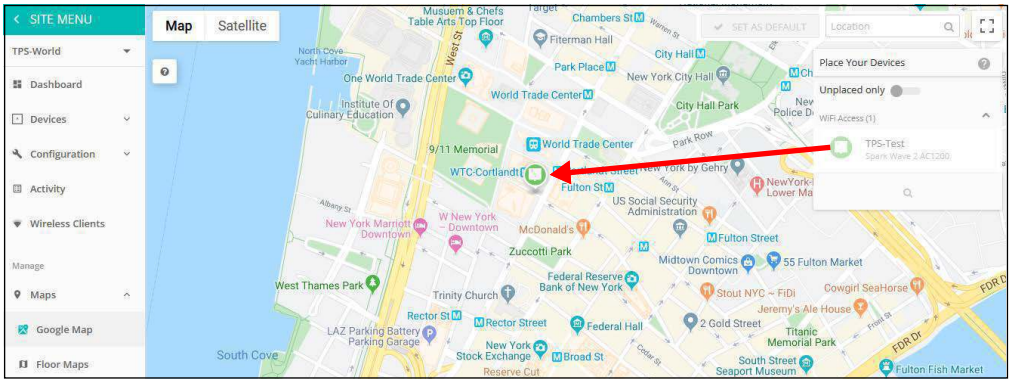
Figure 13: Filtering the Device View



Placing a Device on a Map

Clicking on the Map Manager link in the adding-devices successful message displays the map view page. Use the mouse to click-drag devices to installation locations on the map.

Figure 14: Placing a Device on a Map



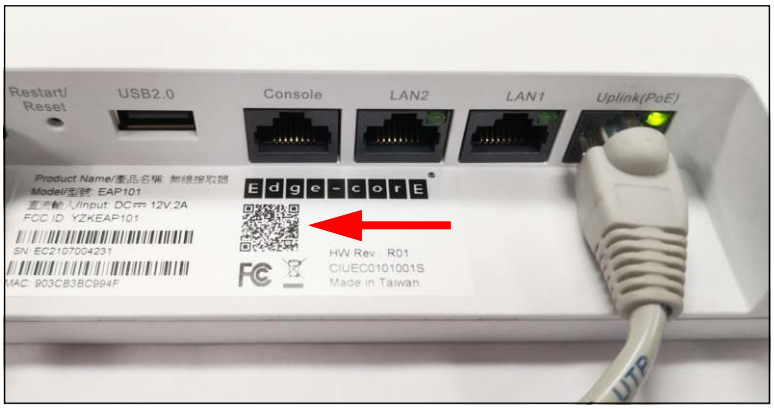
QR Code Onboarding

For quick set up and registration of your AP with the ecCLOUD controller, you can scan the QR code on the AP using a phone.

Follow these steps:

1. Power on the AP.
2. Connect the AP to the Internet. Connect your network or Internet access device to the AP's RJ-45 Uplink port.
3. Use the camera (iPhone) or a barcode app (Android) on your phone to scan the AP's QR code. The QR code is printed on a label on the AP.

Figure 15: Scanning the AP QR Code



1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - Termo de Referência 29/2025 Administrativo_proc_Sid_listaMar_029_2025_pag_227.pdf (35/301) 1468/4726

4. When a message pops up, tap "yes" to join the Wi-Fi network. (iPhone requires you to go to Settings > Wi-Fi for the message to pop up.)

   The web browser should open and redirect to the Setup Wizard page.

Note: If the phone cannot connect to the Wi-Fi network, type the SSID (network name) and password manually. The SSID name is the AP serial number (for example, EC0123456789), and the password is the AP MAC address (for example, 903CB3BC1234).

---

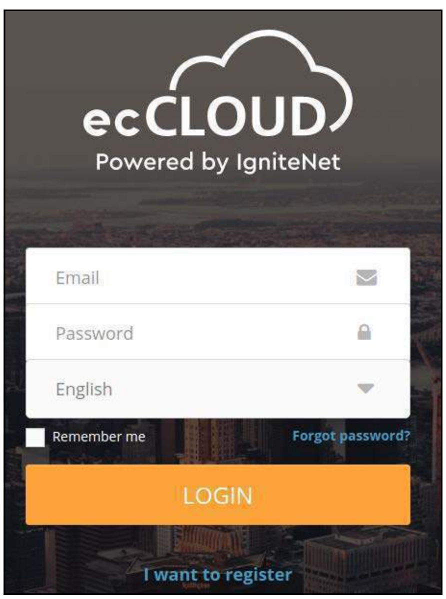
5. Select to manage the AP using the ecCLOUD controller, or to manage the AP in stand-alone mode.

   a. Stand-Alone Mode: Use the default wireless network setting or customize the network name and password. Tap "Done" to finish the setup wizard.

      Wait about two minutes for the AP configuration to update, and then connect to the wireless network name configured in the Setup Wizard. The browser is then redirected to the login page of the AP.

   b. Cloud-Managed Mode: Tap "Done" to finish the Setup Wizard and the browser is redirected to the ecCLOUD login page.

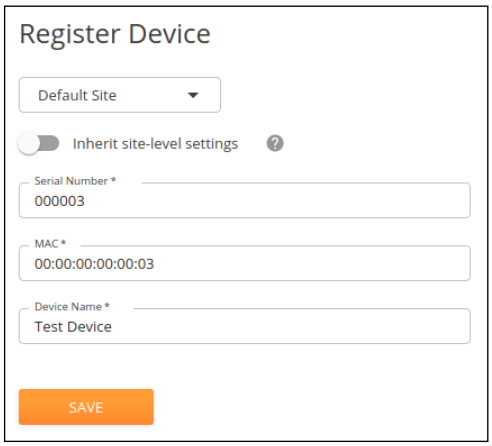
Figure 16: ecCLOUD Login Page



If you already have an ecCLOUD account, log in and select a site for the AP. The AP is automatically registered for cloud management. After you tap "Save," wait about two minutes for the cloud controller to configure the AP.

1Doc: Protocolo 1.943/2025 ... (36/301)

Figure 17: ecCLOUD Device Registration



If you do not have an ecCLOUD account, tap "I want to register" and set up an account. Create a cloud and site before confirming the regulatory country. After tapping "Next," the AP is then automatically registered for cloud management.

After you tap "Save," wait about two minutes for the cloud controller to configure the AP.

Understanding Configuration Inheritance

When a new device is added to the Cloud, the device's "Site-level configuration inheritance" behavior must also be selected. This "Inheritance Policy" determines how the Cloud configures a device. Cloud Configuration is very flexible, it allows Device-level configuration overrides to be setup when there is a need to inherit only a subset of site-level settings.

The Site-level Inheritance Policy is set when you first register a device, but this can also be changed later at any time.

There are two Inheritance Policy options for devices:

- **Inherit site-level settings** — Select this Inheritance Policy if you want to manage devices at a site like a single unit with a common configuration. This is normally the best way to configure Wi-Fi access devices. You would typically choose this Inheritance Policy for a hotel, business, or other similar application where enterprise Wi-Fi is deployed.

  Even though devices inherit most of their settings from the Site-level, you can always override any Site-level settings at the Device-level by making changes on the Device-level configuration pages.

- **Don't inherit site-level settings** — Select this Inheritance Policy if you do not want a device to inherit any settings from the Site level.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 08059386321866289 2025 Anistia EC_acesso_distancia_029_2025_pdf 27.pdf (37/301) 1470/4726

You would normally choose this Inheritance Policy if a device is used for infrastructure, backhaul, or needs to be configured independently from the other devices at a site. This is the typical choice for MetroLinq point-to-point links.

When Site-level inheritance is enabled for a device, the device's final configuration will include the following:

- Settings inherited from the Site-level device configuration.
- Settings initially inherited from the Site-level configuration that have been since been modified as a Device-level "override."
- Settings unique to the Device-level configuration. That is, device-specific settings that are not configurable at the Site level.

Note: Device-level overrides can be reset to the Site-level configuration by clicking the "Use Site Settings" button on the page where a setting has been changed.

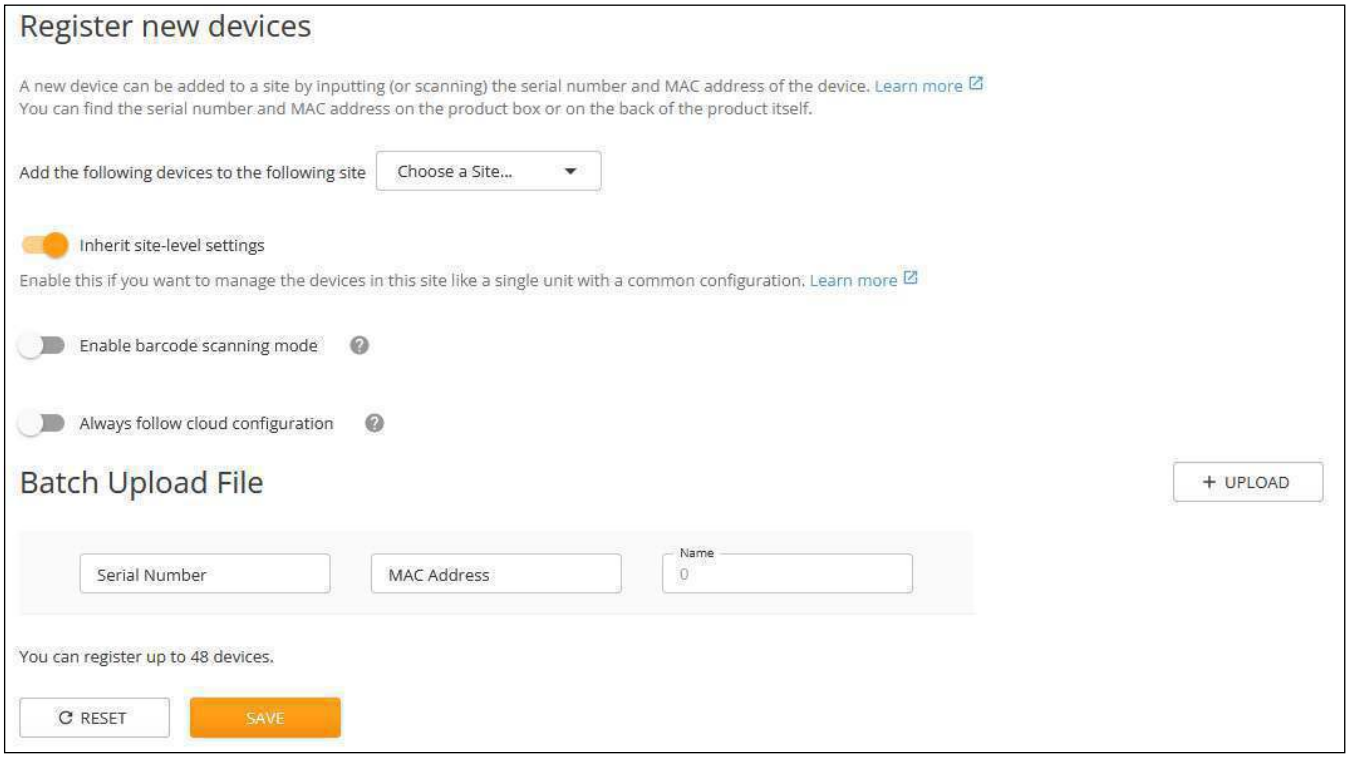
Note that some Device-level override settings, specifically those for SSIDs, local logins, and VLANs, cause all other settings for that entity to be overridden. For example, changing one setting for a Site-level configured SSID at the Device level results in all settings for that SSID being treated as an override. That is, any future changes to the SSID at the Site level will not be reflected in the Device-level configuration.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 34670805938632168289 12/2025 | Anexo EC_procesoDigitalizado_029_20252026227.pdf (38/301) 1473/4726

Understanding Device Registration

New devices can easily be added to a site by entering (or scanning) the serial numbers and MAC addresses of the devices into the “Add device” form on the Cloud.

Figure 18: Registering New Devices



Note: A device’s serial number and MAC address can be found on its product box, or on the main dashboard page of the local web configuration UI.

This is the typical process that occurs after a device is registered:

1. Once a device is added to a site, it goes into the “Pending Registration” state. At this point, the Cloud is waiting for the device to call in for the first time to fetch the credentials it will use for future communication with the Cloud.

2. After the device makes its initial connection to the Cloud and completes registration, the Cloud checks to see if the device’s site has the “auto firmware upgrade” setting enabled. If so, it checks the device’s firmware to see if it needs to be upgraded, and if so, it creates an auto firmware upgrade task for the device.

3. After the device is upgraded (or if firmware upgrade is skipped), the device will send up its current configuration to the Cloud. This generates a “Received

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - 07/08/2025 | Anexo_Administrativo_3_-_Processo_Licitatorio_029_2025_-_Pregao_-_Aquisicao_de_Licenca_de_Uso_de_Software_de_Gestao_de_Frotas_-_Assinado_-_Assinado.pdf (39/301) 1772/4726

Config" task, the details of which can be viewed on the device's Activity page. The Cloud must collect the device's initial configuration, as well as firmware version, before it can push any new configurations down to the device.

4. Next, the cloud will merge any Site-level configuration settings (assuming inheritance is enabled) with the device's configuration, and create a "Change Config" task to push the new settings down to the device. If Site-inheritance is enabled, the device's running configuration will be completely replaced with the configuration seen on the device's Configuration page on the Cloud. Any configuration settings changed through the local UI prior to registration (excluding certain wireless client settings) will be wiped once the cloud sends down the device's new configuration.

After the initial configuration task is completed, the device is finished with all registration-related activities and will commence normal operation. A device's "Activity" page can be used at any time to see the point at which the device is in the initial registration and/or configuration process.

In summary, there are four possible registration states for a device:

- **Unregistered:** There is no record of the device in the Cloud database when a device is unregistered.
- **Pending Registration:** The Cloud user has added the device record to a site by serial number and MAC, and the Cloud is waiting for the device to make an initial connection. At this point, the device has not yet made any contact with the Cloud. If you see a device in this state for a long time, check its Internet connection or your upstream firewall settings.
- **Registered:** The device has made initial contact with the Cloud, completed the registration process, and received its credentials which it will use in any further communication with the Cloud. The "registered" state is the normal operating state of a device on the cloud.
- **Re-registration:** This means the device was previously registered, but is attempting to register again. The system creates an alert for this situation as it requires the user to login to their Cloud account and choose which actions they want to take - such as to allow the device to connect again, and what to do with the device's new configuration.

Note: You can enable "auto" re-registration from the site properties page so that no manual intervention is required to resolve re-registration alerts.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 08059386/2025 | Anistia EC_processo_digital_Marcio_029_20252025_0227.pdf (40/301) 1475/4726

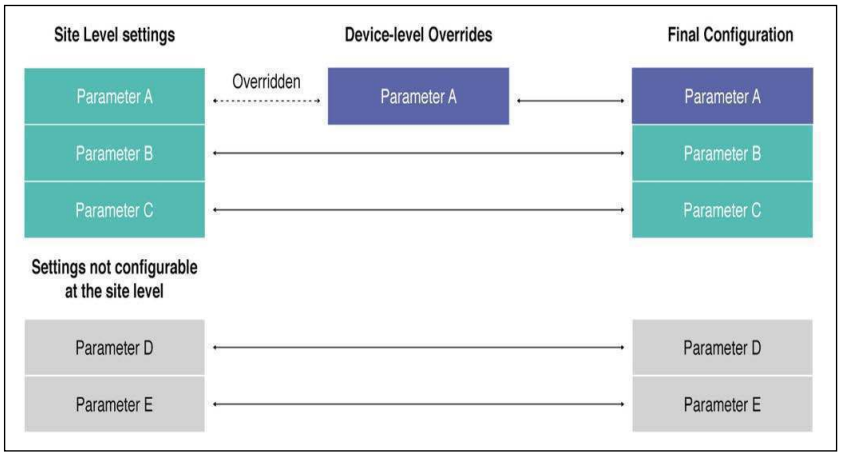
Device Configuration Changes

Any time a device's Device-level or Site-level configuration is changed, the Cloud must determine which settings should actually be changed and pushed down to a device.

When "Site-level configuration inheritance" is enabled for a device, the final configuration will be made of merging two different sets of configurations:

- The common Site-level configuration settings for that product type, and
- The device's individual configuration, which includes settings not configurable at the site level, such as advanced radio settings, features unique to a single product, and more importantly, any Device-level configuration overrides.

Figure 19: Device Configuration Overrides



Device-level configuration setting overrides can be created by changing a setting at the Device-level configuration that's currently being inherited from the site level. These overrides can always be reverted at any time by clicking the "Use Site Settings" button.

Figure 20: Reverting Device-Level Overrides

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - 2025 | Anexo I - Termo de Referência - Aquisição de Licenças de Uso de Software - 2025 (41/301) 1446/4746

After a user changes the configuration for a device, the following will happen:

1. A "Change Config" task will be created detailing exactly which settings are being changed on the device. This task can be tracked on the device's Activity page.

2. The Cloud will push the new configuration down to the device and wait for a configuration ACK from the device to acknowledge that the new configuration was successful.

3. If the ACK is received, the task is marked as complete. If the device loses connectivity after applying the new set of configuration settings, the device will revert to the previous configuration, and send a failure notification to the Cloud. This will result in an "out of sync" error.

Configuration Errors and Failures

There are two major errors that may be encountered during the configuration process:

- **Configuration out of sync error**: This error occurs when the device reverts a configuration pushed down from the Cloud because it cannot connect to the Cloud again after the change. This is what "out of sync" means; the device's running configuration does not match the configuration on the Cloud.

- **Resolution**: This error can be resolved by changing any incorrect settings in your device's configuration on the Cloud, and clicking the "Resync" button to send them back down. For example, a device is currently operating in Client mode, but is configured to use AP mode from the device's Configuration page on the Cloud. After a configuration push, the device will no longer be able to access the Internet or Cloud. The device's operating mode must be changed to Client from the Cloud configuration.

Configuration Suspended Error

Device configuration suspension means that no configurations will be pushed to the device from the Cloud, and no configurations received by the device will be processed by the Cloud.

A device's configuration may become suspended in two cases:

- **Device was downgraded**: As of 2/1/2019, if you downgraded your Cloud-connected device to an older firmware without resetting to defaults, your device's configuration will automatically be suspended. The reason for this is that the device's configuration may contain keys or other values that are not supported, or are incompatible with the older firmware version. This situation could lead to system errors and undefined behavior.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - 2025 | Anexo Administrativo 3 - 2025_processo_licitatorio_029_2025_pages 1-45 (42/301) 14/15/4746

Resolution: Reset your device to defaults and allow it to connect to the Cloud again through re-registration.

- **A system error has occurred:** Sometimes (very rarely), a system error will occur when the Cloud does not understand how to process one or more keys in the configuration sent to it by the device.

  Resolution: Most times, the system error can be cleared out by resetting the device to defaults, and choosing the "Use the device's running config" at re-registration.

Note: This will clear out any "bad" cloud-level configuration keys, but will also clear out any device-level overrides you may have created.

If that does not work, wait for support and development teams to investigate the cause of the system error. Once resolved, an email will be sent out to all Cloud account owners and admins notifying them that the device's configuration has been unsuspended.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3467D8B059B3E321B66289D2920251 | Anexo EC_acceso_Cloud_Usuario_029_20252026227.pdf (43/301) 1478/4726

Section II

Cloud Configuration

This section provides details on creating and managing clouds and sites, as well as configuring access point settings.

This section includes these chapters:

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - 1Doc 1.943/2025 | Anexo Administrativo 3 - EC_processo_licitatorio_029_2025_pagina_1449.pdf (44/301) 1449/4726

2 Cloud Management

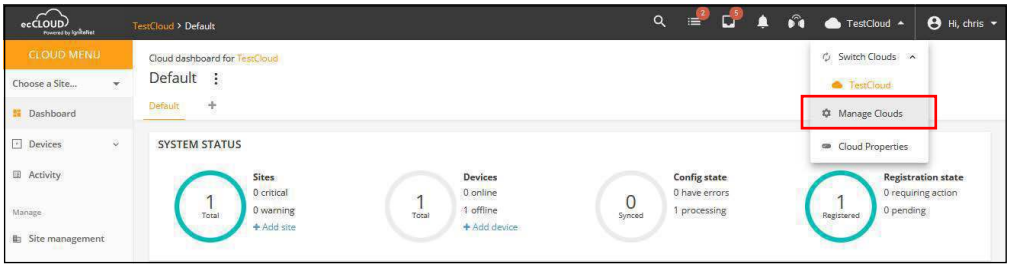
This chapter includes the following sections:

1Doc: Protocolo 1.943/2025 | Anexo ... EC_CLOUD_UserManual ... .pdf (45/301)

Managing Your Clouds

Select "Manage Clouds" from the Cloud pull-down menu in the upper right of the screen to get to the cloud management page.

Figure 21: Cloud Menu



Create a New Cloud (from an existing account)

To add a new cloud to an existing account, follow these steps:

1. Select Manage Clouds in the upper right of the screen (once logged in) to open the Cloud Memberships page.

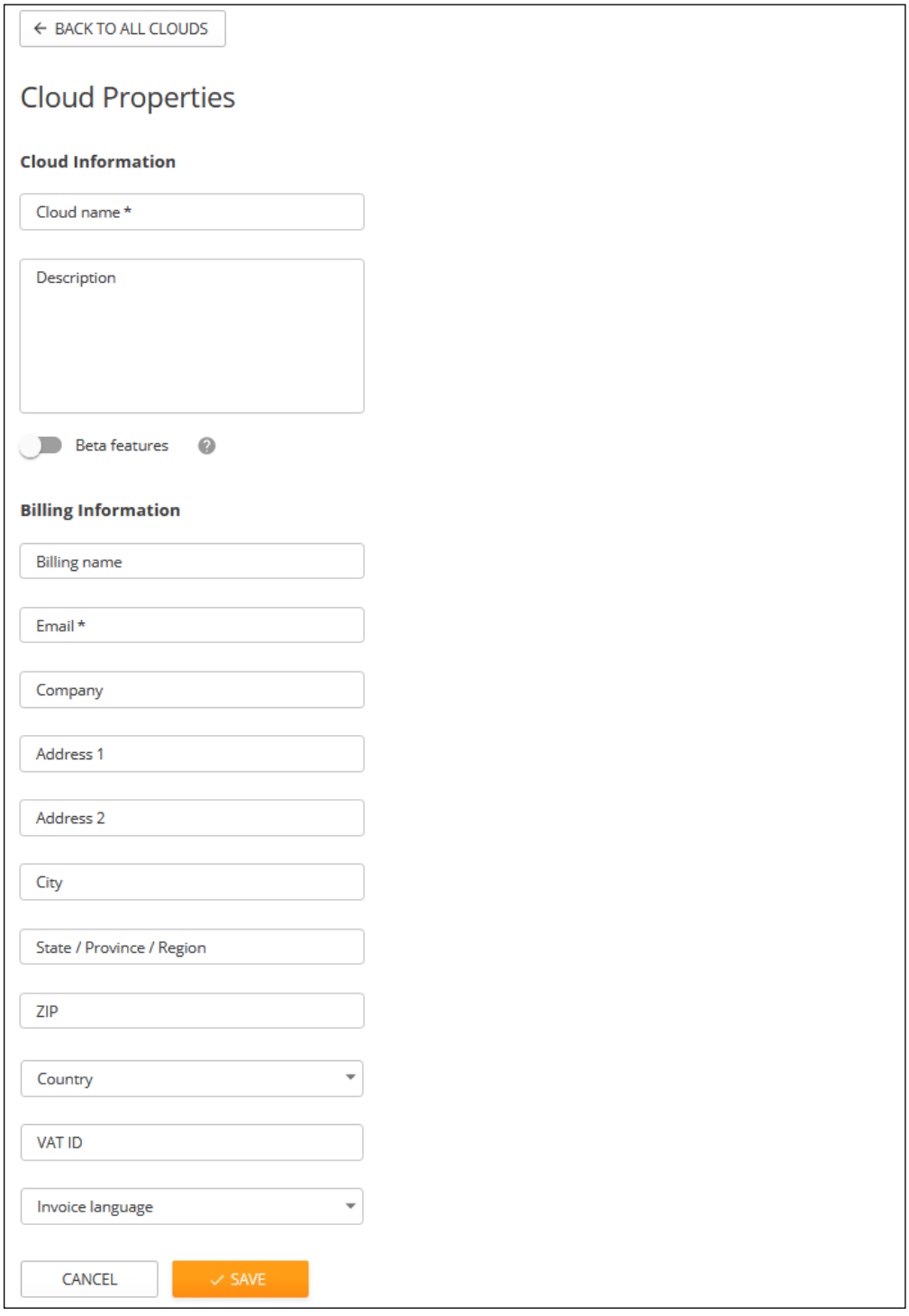
2. Click Add Cloud.

Figure 22: Displaying Cloud Membership

3. Fill in the cloud name and other descriptive information.

4. Click Save.

Figure 23: Adding Cloud Information

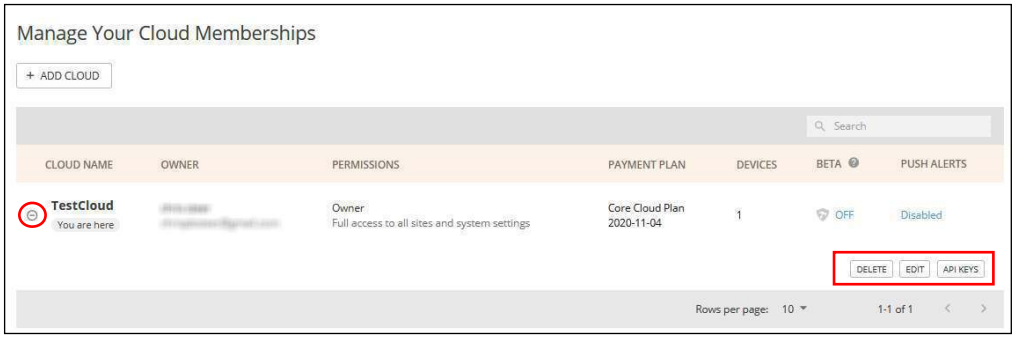


1Doc: Protocolo 1.943/2025 | Anexo Administrativo 08059386121866289 2025 Administrativo_processo_licitatorio_029_2025_pdf (47/301) 1750/4746

Editing Cloud Information

Click on the expand icon to show the DELETE and EDIT buttons.

Figure 24: Showing Cloud Actions

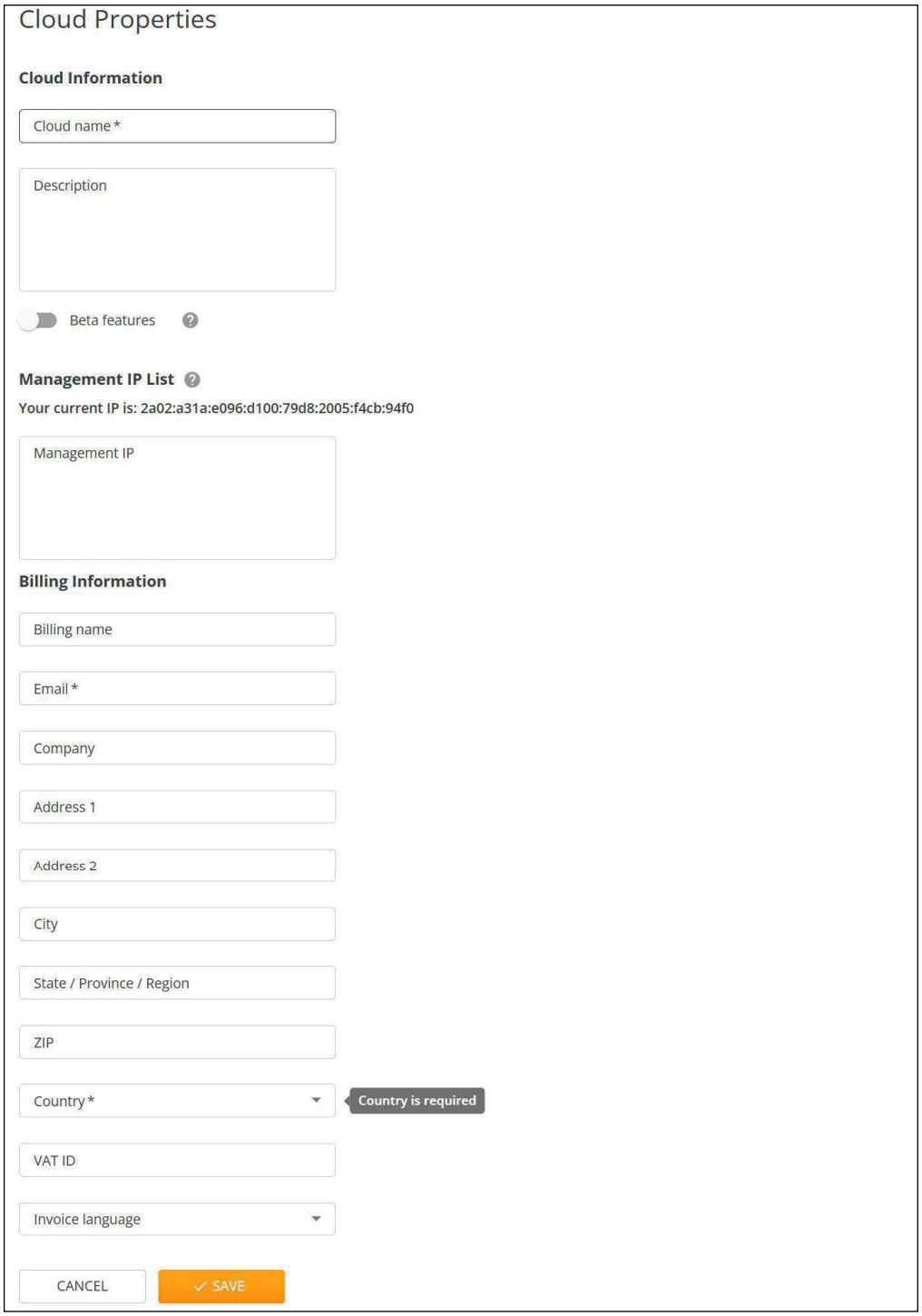


Changing the Cloud Properties

In the cloud management list with the selected cloud expanded, click on the EDIT button in the lower right of the list to display the cloud information properties. Make your changes to the cloud properties and then click the SAVE button.

To restrict cloud access, Login IP ACL allows administrators to define specific IPv4 or IPv6 addresses that are permitted to connect to the cloud management portal.

Figure 25: Changing Cloud Properties

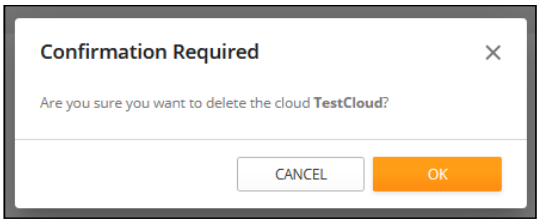


1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - TERMO DE REFERÊNCIA 29/2025 Administrativo_processo_licitatorio_029_2025_pdf_27.pdf (49/301) 1752/4726

Deleting a Cloud

In the cloud management list with the selected cloud expanded, click on the DELETE button in the lower right of the list to delete the cloud. Click OK in the confirmation window to complete deleting the cloud.

Figure 26: Delete Cloud Confirmation

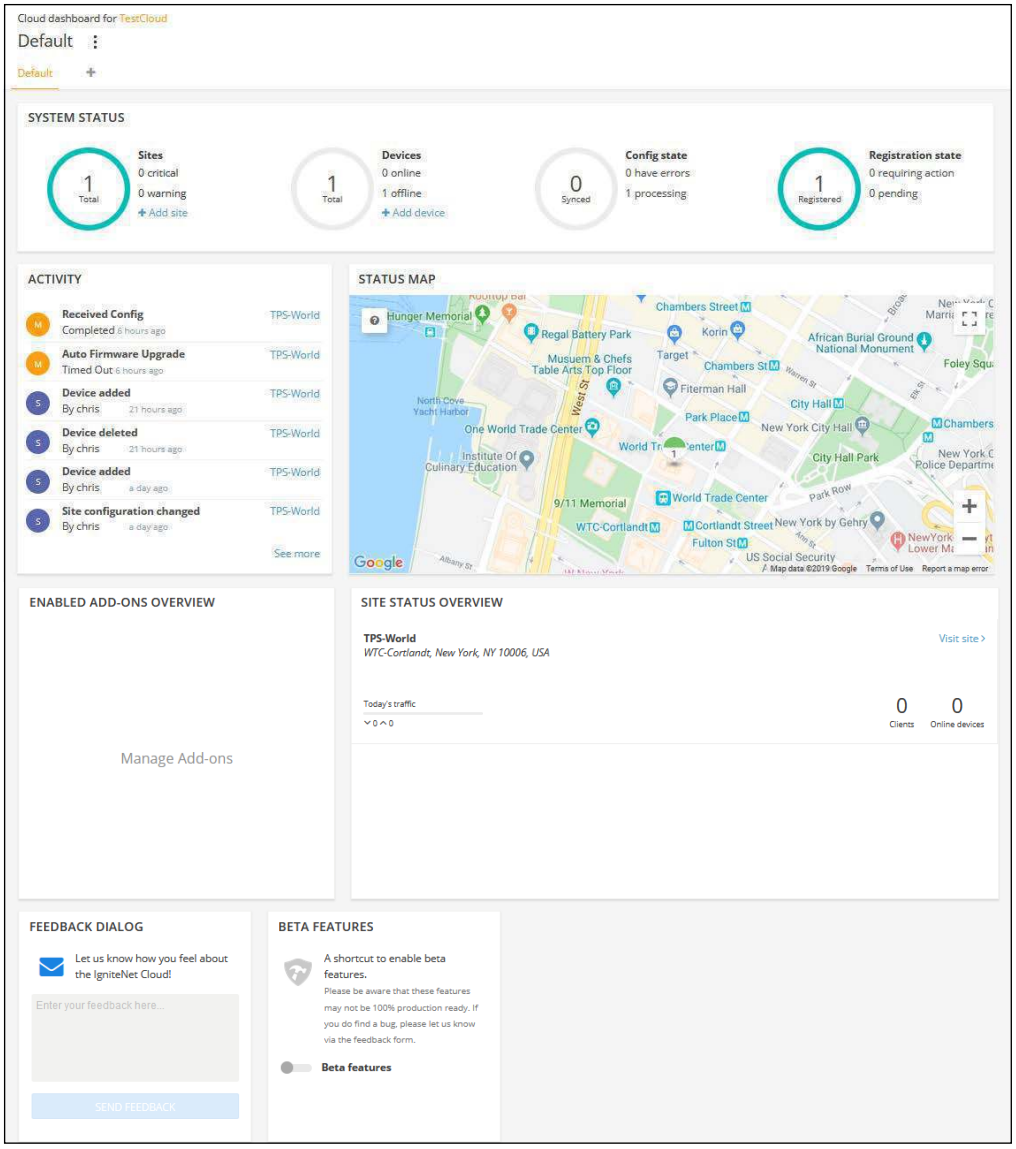


Caution: Deleting a cloud is a permanent action and will result in the deletion of all related records, such as APs, clients, sites, system activity logs, and device configurations stored for that cloud.

Displaying the Cloud Dashboard

The cloud dashboard provides an overview of system status for configured devices, recent activity information, a cloud status map, and a site status overview.

Figure 27: The Cloud Dashboard



The following items are displayed on the cloud dashboard:

- **System Status** — The four circles represent (from left to right): the number of sites, the number of devices (with online/offline counts), the number of devices with synced configurations, and the number of devices registered.

Note: Placing the mouse cursor over the four circles shows additional information.

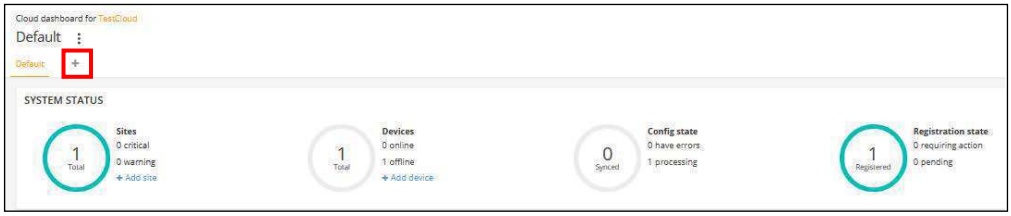
1Doc: Protocolo 1.943/2025 | Anexo Administrativo 08059386/2025 | Anexo EC_procesoDistensa_029_20252025027.pdf (51/301) 1756/4726

- **Activity** — Provides a short summary of the most recent device, network and system alerts, and maintenance notifications such as the device being unreachable or rebooted. Clicking on each entry provides further details.
- **Cloud Map** — Displays the geographical location of the cloud sites and the devices located at each site. Hovering over a device displays a pop up with further device details.
- **Enabled Add-Ons Overview** — A summary of the currently enabled Add-ons. Clicking in the box opens the Site Add-ons management view.
- **Site Status Overview** — Lists a summary of site statistics, including the day's traffic, the number of clients, and the number of online devices.
- **Feedback Dialog** — Enables you to send your comments and suggestions directly to Edgecore.
- **Beta Features** — Enables new cloud controller features that are in beta release stage.

Creating a Custom Cloud Dashboard

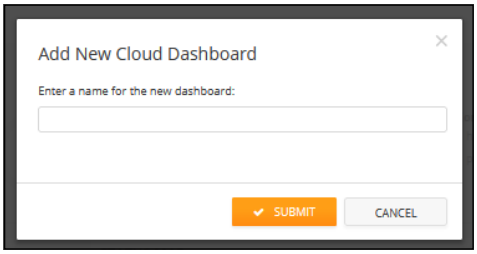
In the default cloud dashboard, click the plus sign next to the default tab at the top to create a custom dashboard suitable for your requirements.

Figure 28: Adding a Custom Cloud Dashboard



Enter a name for the new custom dashboard and click SUBMIT.

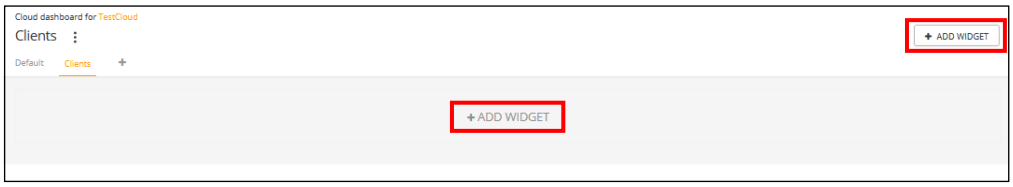
Figure 29: Naming a Custom Cloud Dashboard



1Doc: Protocolo 1.943/2025 | Anexo Administrativo 08059386 de 29/12/2025 | Anexo EC_proceso_Licitatorio_029_2025_20250627.pdf (52/301) 17/47

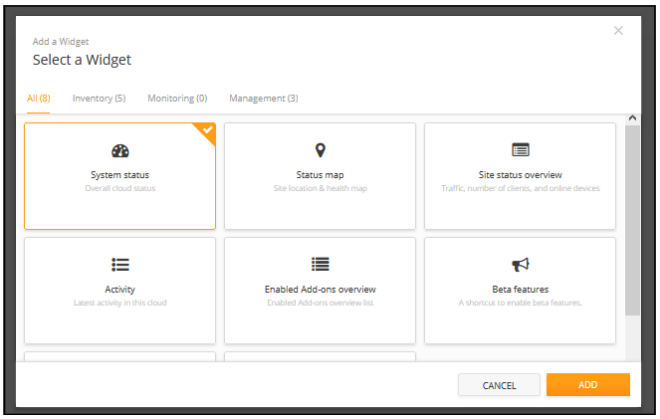
A new tab will appear next to the default dashboard tab with the custom dashboard's name. Click on one of the "+ Add Widget" buttons to add the desired item for the new dashboard.

Figure 30: Adding a Widget to a Custom Cloud Dashboard



Once a widget is selected click the "ADD" button.

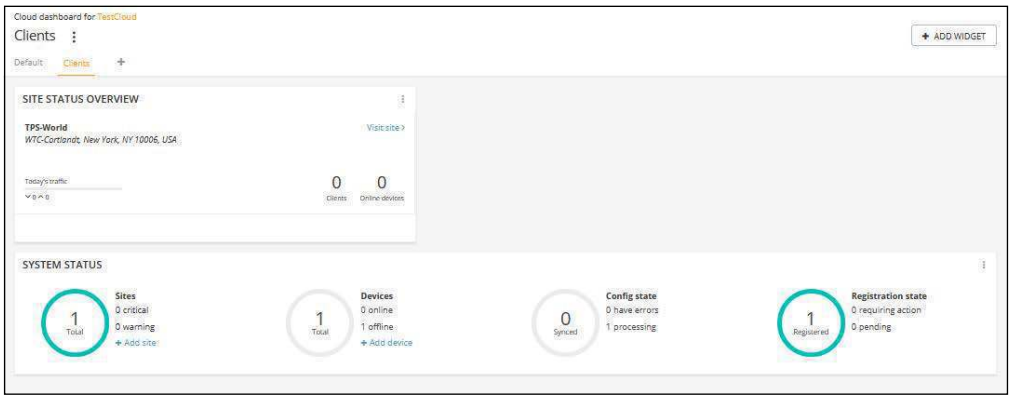
Figure 31: Selecting a Widget for a Custom Cloud Dashboard



Afterwards the widget will appear on the new custom dashboard. The widget size can be adjusted by dragging the edges of the widget box. Further, it can be renamed or removed by clicking the three dot icon in the upper right of the box.

Click the "Add Widget" button again to add additional widgets to the custom dashboard.

Figure 32: Customized Widgets Added to a Custom Cloud Dashboard

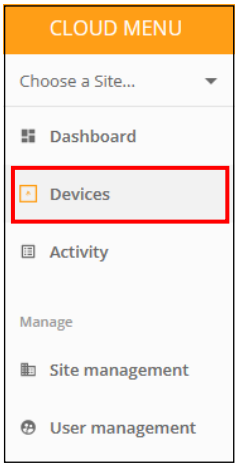


1Doc: Protocolo 1.943/2025 | Anexo Administrativo_proceso_licitatorio_029_2025_pliego.pdf (53/301) 1746/4746

Managing Your Devices

Clicking the Devices section on the Cloud menu displays all the cloud devices for all sites.

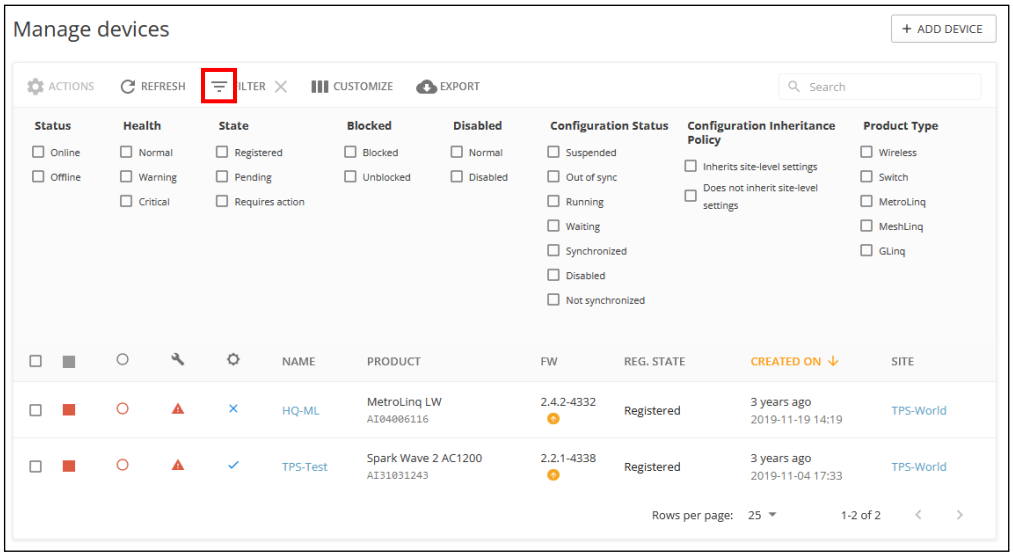
Figure 33: Cloud Menu Devices



Filtering the Device List

Click the filter (funnel) icon button in the upper left of the window to open the filtering options for the device list (Status, Health, State, Blocked, Disabled, Configuration Status, Configuration Inheritance Policy, or Product Type). The displayed devices can also be sorted by clicking on the ascending or descending arrows at the top of each column.

Figure 34: Manage Your Devices



1Doc: Protocolo 1.943/2025 | Anexo Administrativo 08059386/2025 | Anexo Administrativo_procedimento_029_20252025027.pdf (54/301) 1789/4746

Configuring Inheritance Policy

The Site-level Inheritance Policy is set when you first register a device, but this can also be changed later at any time. For more information, see "Understanding Configuration Inheritance" on page 37.

In the Cloud Devices list, the column with the gear icon indicates the devices that have the Configuration Inheritance Policy enabled. The Configuration Inheritance Policy field can be filtered and the policy for devices changed from the "Actions" list.

Figure 35: Configuration Inheritance Policy Indication

Select devices by clicking the checkmark square in the first column. The "Actions" button becomes available in the column header. Click the Actions button to display a menu of actions that can be applied to the selected devices.

Figure 36: Manage Your Devices Actions Menu

The following items are displayed on the Actions menu:

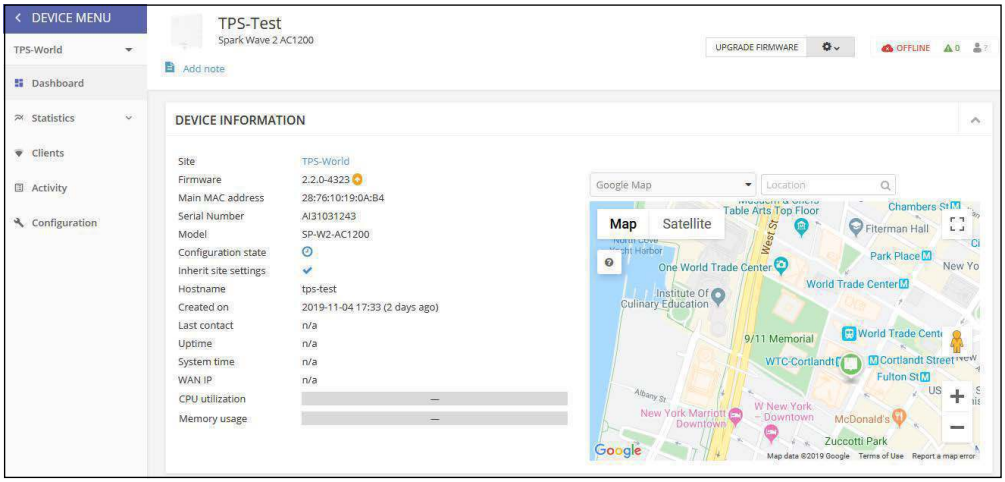
- **Change Inheritance Policy** — The selected devices will change their inheritance policy, either to "Do not inherit site-level configuration," or to "Inherit site-level configuration," depending on the current setting.
- **Move to Site** — Moves the selected devices to another site. The devices will inherit site-level configuration from the selected site.
- **Block** — Blocks the selected devices from communicating with the cloud.
- **Disable** — Blocks (prevents communication with the cloud) and hides the devices from all dashboards. The devices are no longer available, but the device history is preserved.
- **Delete** — Permanently removes the selected devices from the cloud.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 08059386321866289 2025 Anistia EC processo Distancia 029 2025 0256227.pdf (55/301) 1760/4726

Viewing Device Information

Click a device name link in the Name column to access the detailed device information.

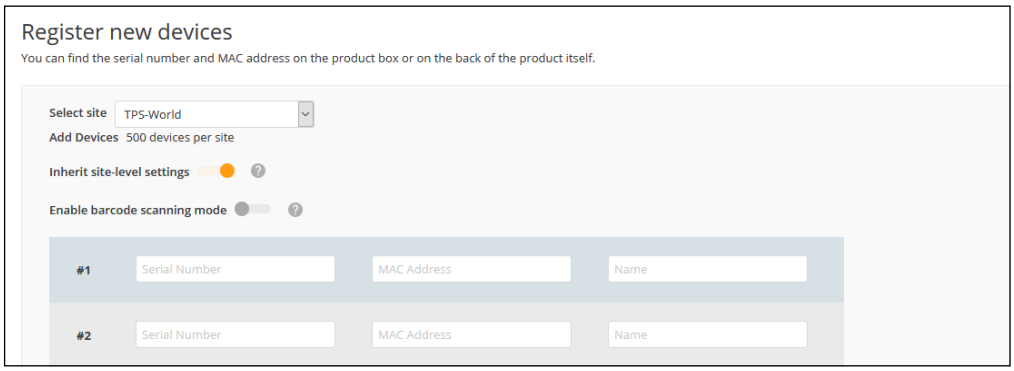
Figure 37: Accessing Device Details



Adding Devices

Click the Add Devices button to display the “Register new devices” page and add new devices to the cloud.

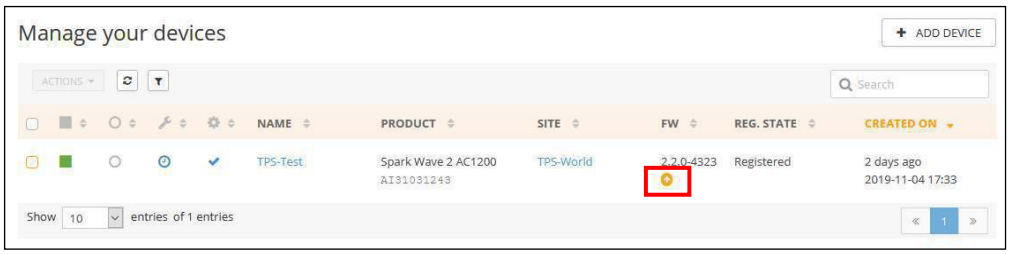
Figure 38: Adding Devices to Your Cloud



Upgrading Device Firmware

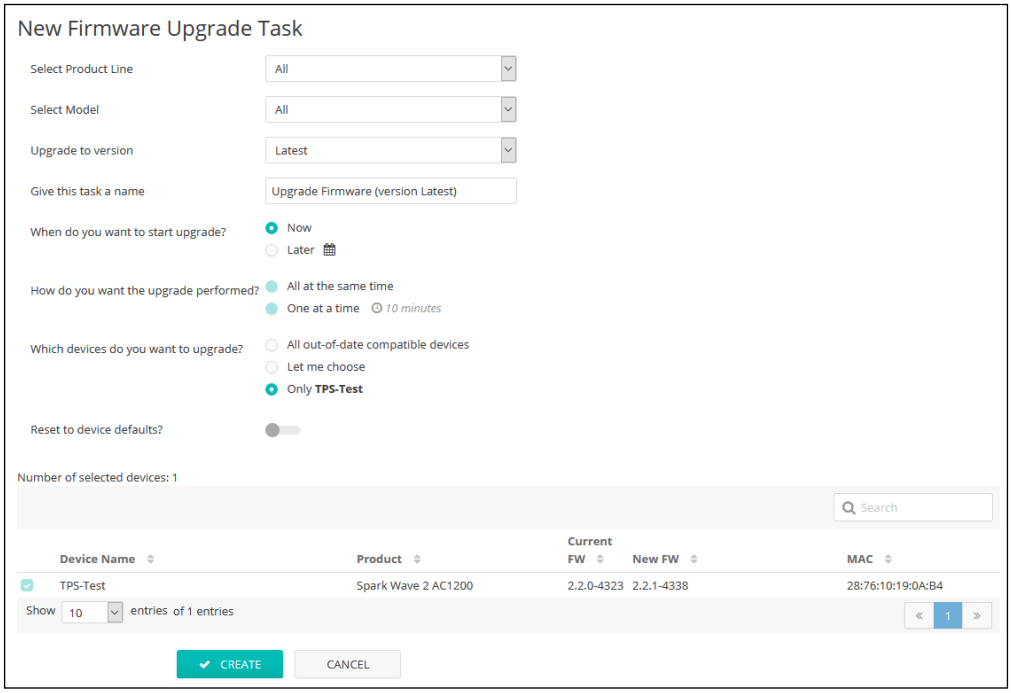
Click the upgrade icon in the FW column when new firmware is available for a device. The automated firmware upgrade page opens.

Figure 39: Firmware Upgrade Indication



Follow the selections for the firmware type and upgrade schedules, and then click the Create button to initiate the upgrade.

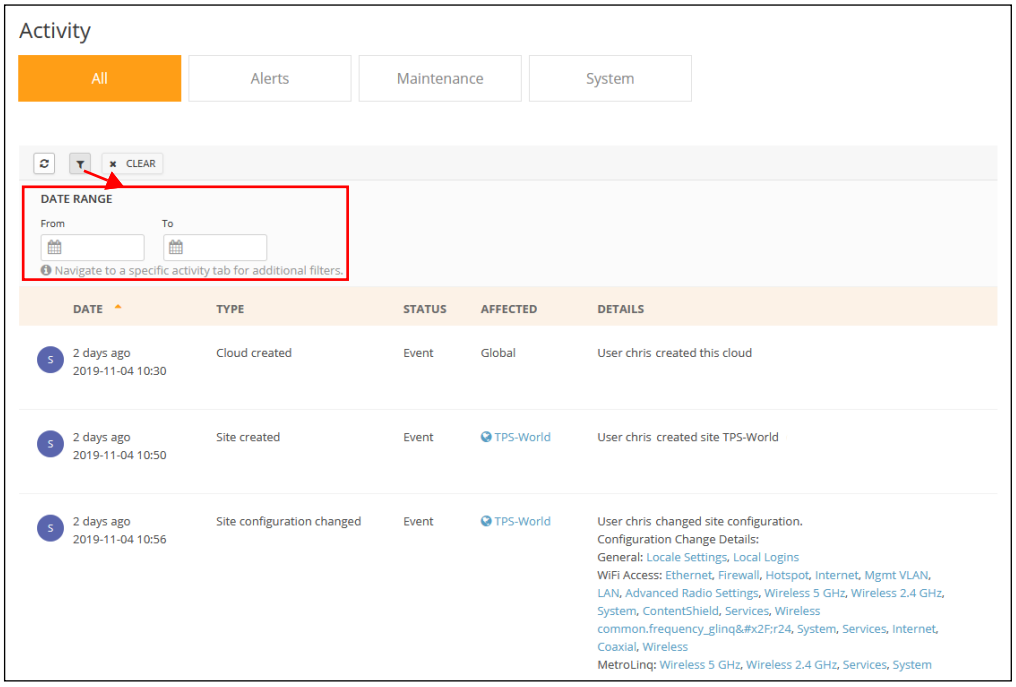
Figure 40: Device Firmware Upgrade



Displaying System Activity

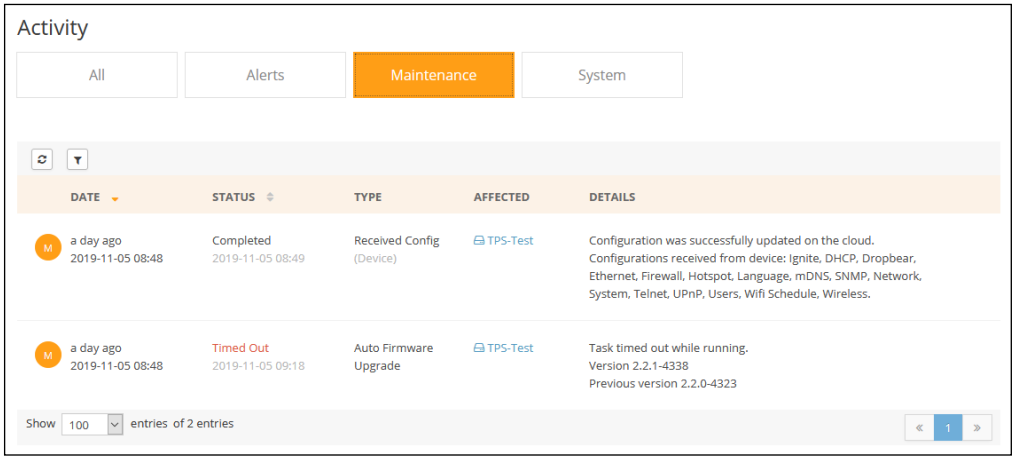
Click Activity on the Cloud menu to display all logged system alerts, maintenance tasks, and logged events. Click the filtering button on the left to specify a date range selection. The displayed messages can also be sorted by clicking on the ascending or descending arrows at the top of the Date column.

Figure 41: Showing All System Activity



Use the buttons at the top of the page to filter by the available categories: Alerts, Maintenance, or System logs.

Figure 42: Filtering by Activity Category

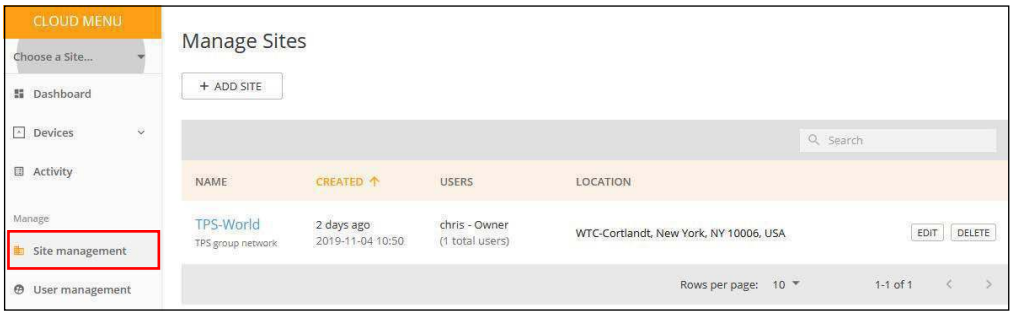


1Doc: Protocolo 1.943/2025 | Anexo Administrativo 08059386321866289 2025 Anistia EC_processo_disciplinar_029_2025_pdf (58/301) 1943/4726

Manage Your Sites

From a Cloud menu, click on the Site Management.

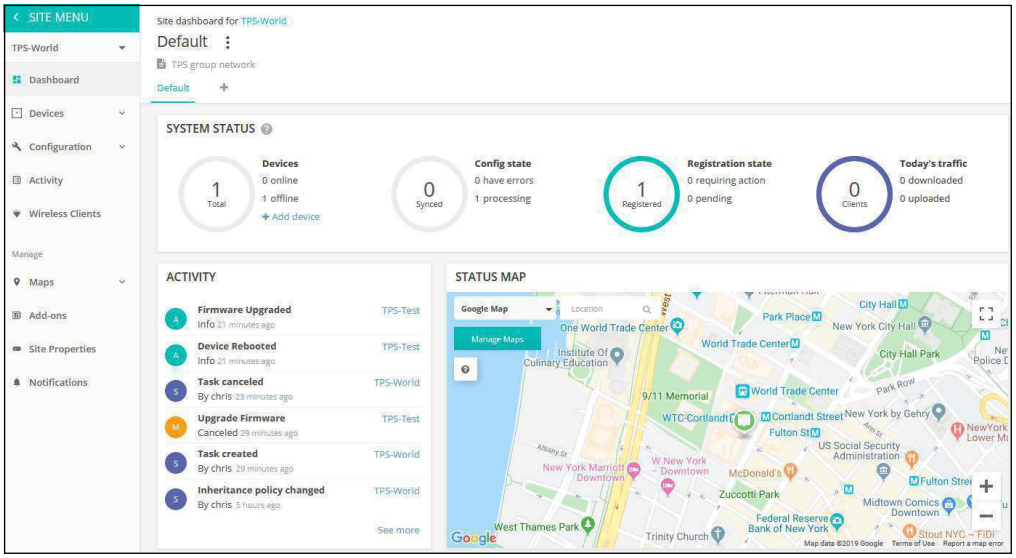
Figure 43: Site Management Page



In the Manage Sites window a list of all created sites is shown with each site name, creation date, user list, and location. Click the edit button to edit a site's properties, or the delete button to delete a site once all devices are removed from it. Click the Add Site button to open the site creation page.

Clicking on a site name opens the site's dashboard.

Figure 44: Site Dashboard



See "General Site Configuration" on page 95 for further detailed site management and configuration information.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3467088059838321866289 2025 Anistia EC_processo_digital_Manual_029_20252025027.pdf (59/301) 3792/4726

User Management

The user who originally creates a cloud is the cloud's owner. The owner can then invite any number of users to have Owner, Administrator, or Regular User access to the cloud and its sites.

Note the following access rights for users:

- **Owner** — Cloud Owners have full write permissions and access to all sites and devices within the clouds they administer.
- **Administrator** — Cloud Administrators have nearly full write permissions and access to all sites and devices within the clouds they administer. They, however, cannot manage billing and licensing settings by default only the cloud owner can do this. The cloud owner can grant this permission to an Administrator if required.
- **Regular User** — Site-level users that are bound to the sites that the owner specifies. They can further be classified as Managers (with full write access), or Guests (with read-only access) within their specified sites.

From the Cloud menu, click "User management."

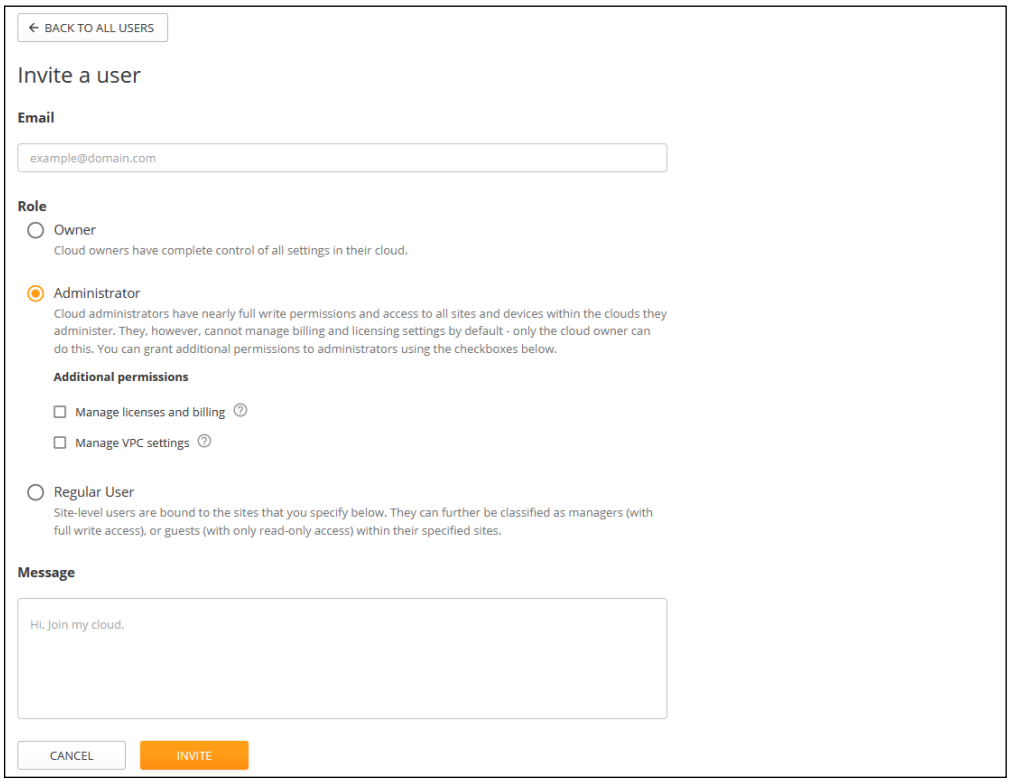
Figure 45: Manage Users

The Manage Users page allows you to invite new users, remove users, or edit a user's access permissions.

Click INVITE USER to open the invitation page. Fill in the user's email address and select the role for the user; Owner, Administrator, or a Regular User. For administrators, two additional permissions can be selected. Click INVITE to send an email message request to the new user to join the site.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo Processo Digital Nº 2025 | Anexo_Administrativo_Processo_Digital_Nº_2025_20250627.pdf (60/301) 3705/4726

Figure 46: Invite a New User



The "Additional permissions" field is optional and contains the following items:

- **Manage licenses and billing** — Provides full access to Licenses & Billing pages for the cloud.
- **Manage VPC settings** — Allows access to Virtual Private Cloud (VPC) settings used for custom clouds. Custom clouds remove the Edgecore branding from a cloud and allow all the pages to have a custom name, logo, etc.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 08059386121866289_29_2025_Administrativo_Acesso_Cloud_Usuario_029_20252025027.pdf (61/301) 3796/4726

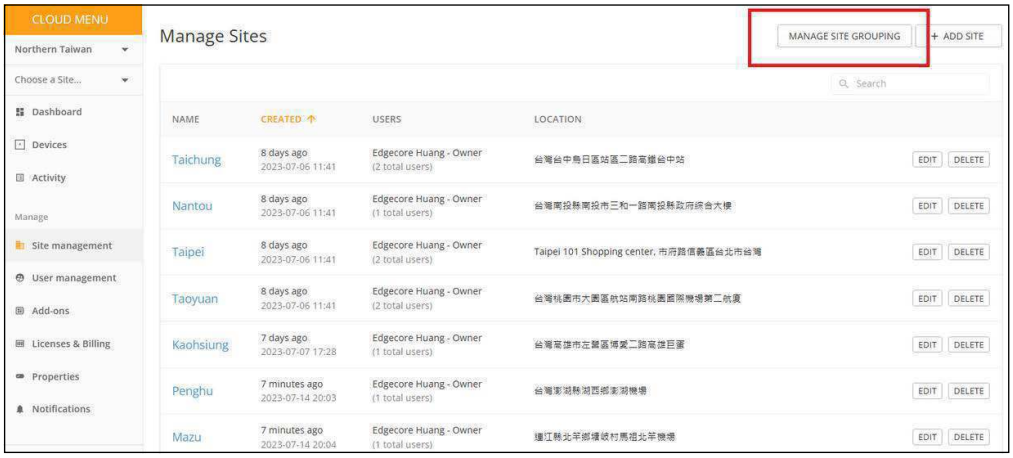
Site Grouping

When you need to manage multiple sites within the same cloud, you can use Site Grouping to aggregate information from various sites on one page, avoiding the need to constantly switch between sites.Site Grouping essentially enables you to create a logical collection of related sites.

Note that only Cloud Owners and Cloud Administrators have permission to use Site Grouping.

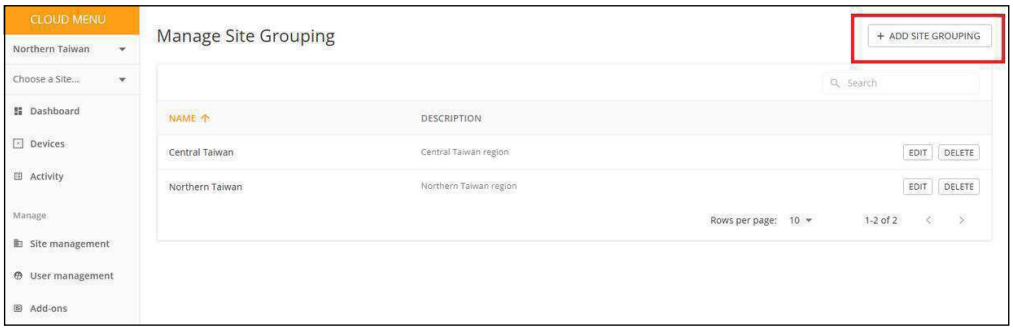
To create a site group, go to the Site Management page and click “Manage Site Grouping.”

Figure 47: Accessing Site Grouping



On the Site Grouping page, click “Add Site Grouping.”

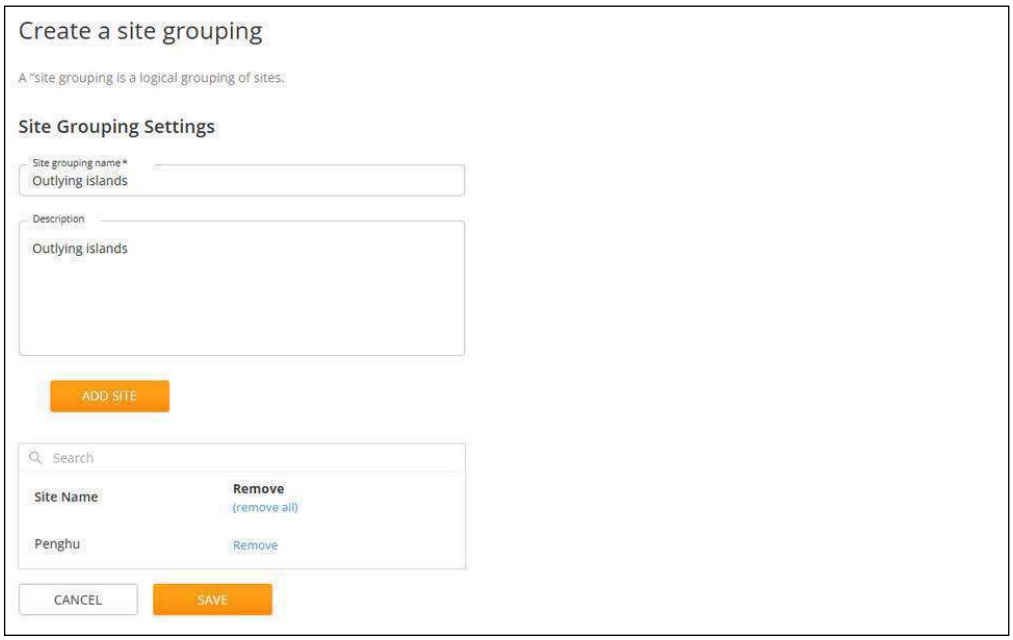
Figure 48: Site Grouping Page



Enter a name and description for the site group. Click “Add Site” to add available sites to the group from a list. Click Save to create the group.

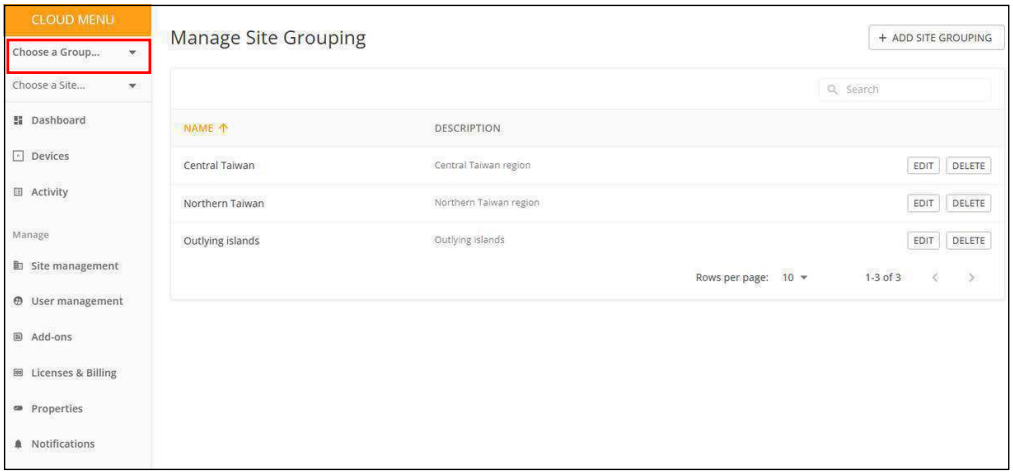
1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3467088059838632189329202 5 | Anistrator_proCesoDidatoMa_029_20252025627.pdf (62/301) 1705/4726

Figure 49: Creating a Site Group



From the Manage Site Grouping page you can edit or delete groups, and switch quickly between groups using the "Choose a Group" menu at the top-left of the page.

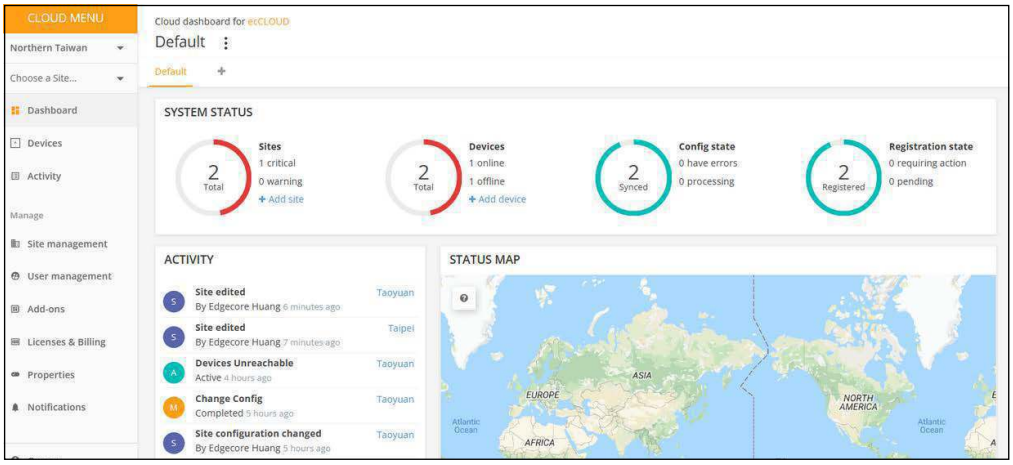
Figure 50: Managing Site Groups



Selecting a Site Group refreshes the page and you can see aggregated information from sites in the group.

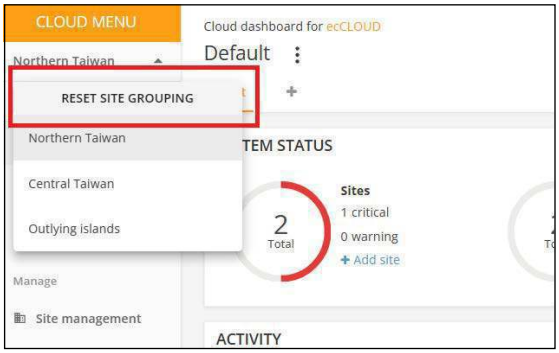
1Doc: Protocolo 1.943/2025 | Anexo Administrativo 08059386121866289 2025 Administrativo_proc_SEI_Diretoria_029_2025_0256227.pdf (63/301) 3706/4726

Figure 51: Viewing Site Group Information



To reset Site Grouping to the global view, click "Reset Site Grouping" on the Site Grouping drop down list.

Figure 52: Resetting Site Grouping



Always Follow Cloud Configuration

In addition to site inheritance and device-level changes, ecCLOUD supports two-way synchronization of cloud and device configuration. When a user modifies a device configuration locally through its web interface, the changes are pushed back to the ecCLOUD configuration.

To prevent the ecCLOUD configuration from being modified by local device changes, ecCLOUD provides an "Always follow cloud configuration" feature that ignores any local configuration changes received from a device. This feature is completely independent of the type of device or its firmware version.

Note: You cannot initiate a firmware upgrade on a device with "Always follow cloud configuration" enabled. First disable this feature before performing a firmware upgrade.

When there is a mismatched configuration between the cloud and the device, ecCLOUD notifies the cloud administrator with the message "The configuration between cloud and device is not matched" and the "Configuration status" is marked as "Configuration is not matched."

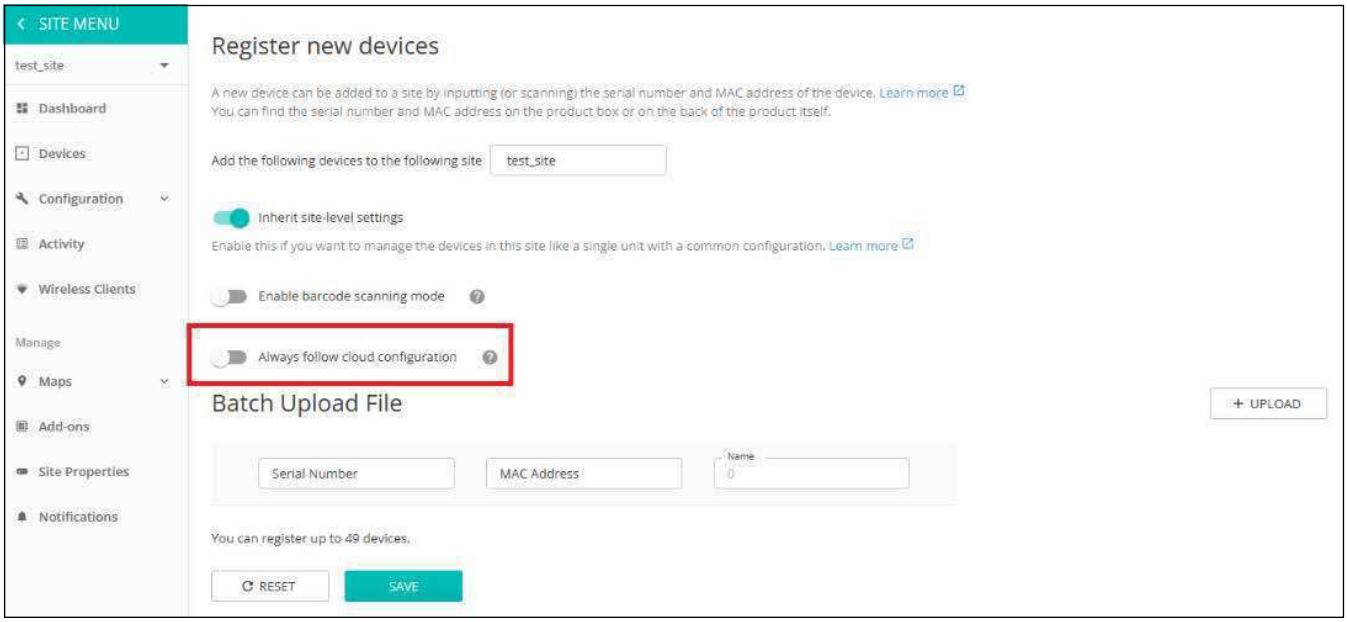
The cloud administrator then has the option to manually push the ecCLOUD configuration to the device, or to enable "Auto follow cloud config" to automatically resolve the mismatched configuration.

When registering new devices you can enable "Always follow cloud configuration."

Note: "Always follow cloud configuration" is automatically disabled when a device is added by QR code onboarding.

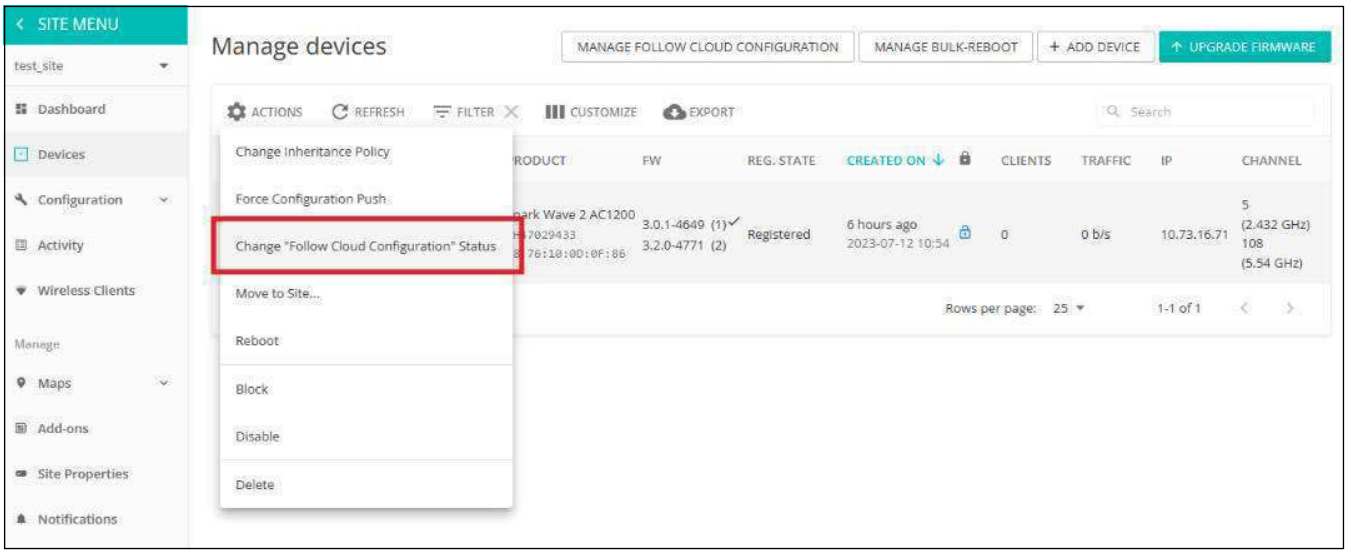
1Doc: Protocolo 1.943/2025 | Anexo Administrativo 34677088059838632168628970129202 5 | Anistrator_processoDigitalizado_029_20252026027.pdf (65/301) 1470/4726

Figure 53: Enabling Always Follow Cloud Configuration During Device Registration



You can also enable or disable "Always follow cloud configuration" for multiple devices from the Site-level Devices page.

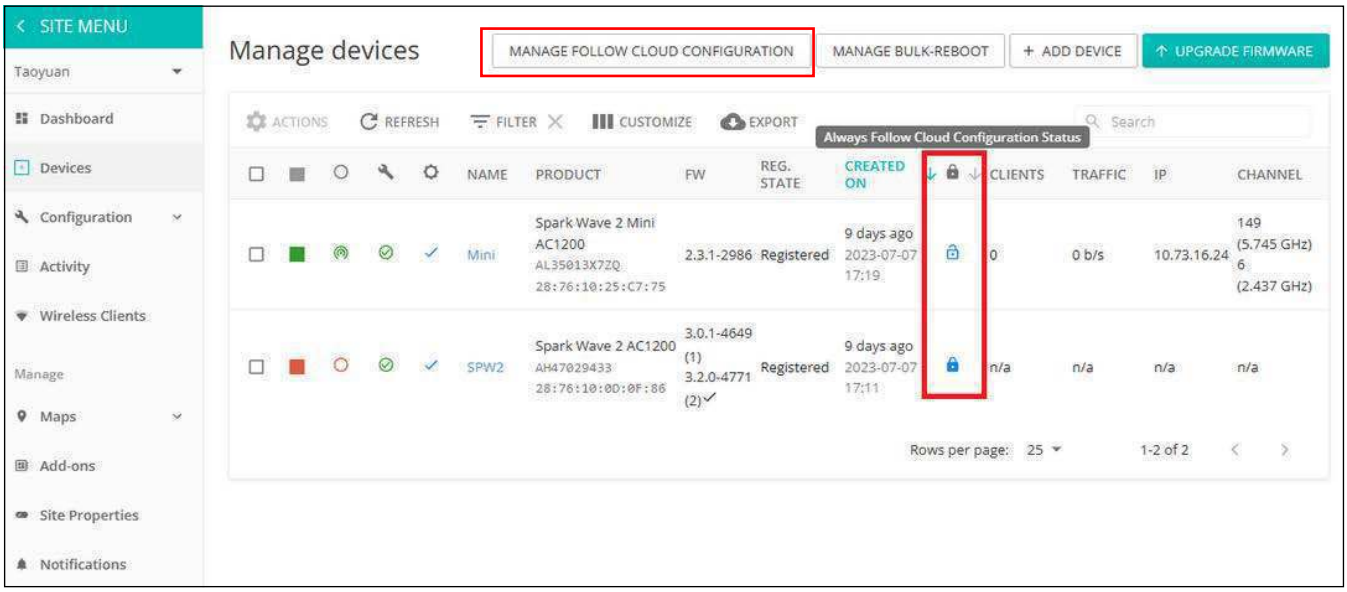
Figure 54: Enabling Always Follow Cloud Configuration on the Devices Page



You can check the status of "Always follow cloud configuration" for devices from the Site-level Devices page, as well as enable/disable the feature using the "MANAGE FOLLOW CLOUD CONFIGURATION" button.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3467088059838613866289 29/2025 Anistia EC_proc_SEI_Diretoria_029_2025_0256227.pdf (66/301) 379/4746

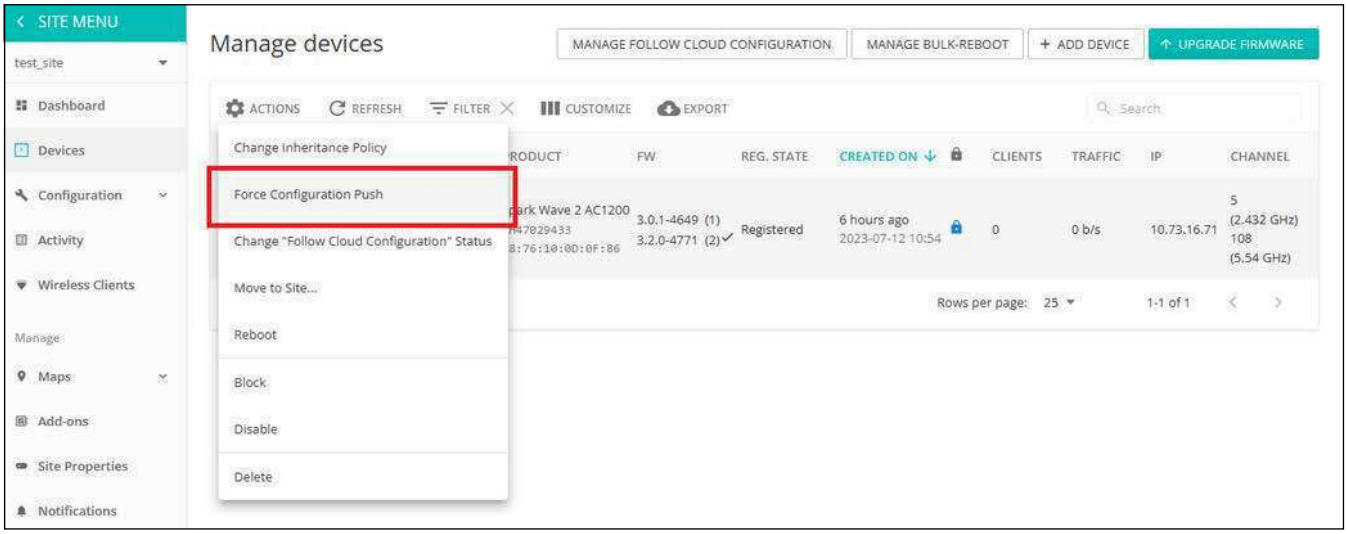
Figure 55: Managing Follow Cloud Configuration



Once "Always follow cloud configuration" is enabled, ecCLOUD will still receive configuration changes from devices, but it does not update the configuration in the cloud. In this situation, ecCLOUD marks the configuration state as "Configuration is not matched."

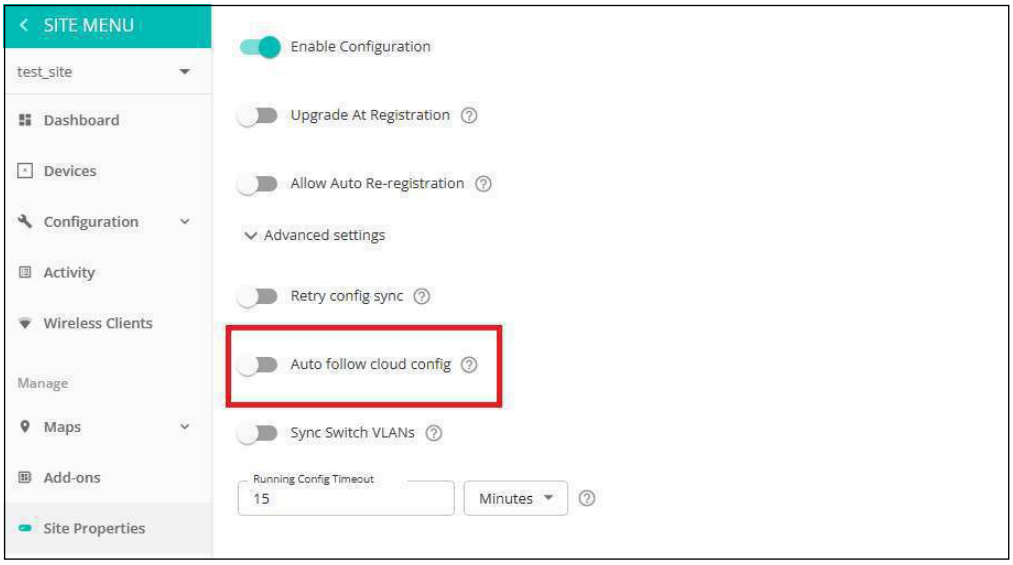
To synchronize cloud and device configurations, you can click "SYNC NOW" in the device-level configuration, or push the configuration from the Site-level Devices page.

Figure 56: Using Force Configuration Push



Alternatively, you can enable "Auto follow cloud config" on the Site Properties page to push a configuration to devices automatically.

Figure 57: Using Auto Follow Cloud Config

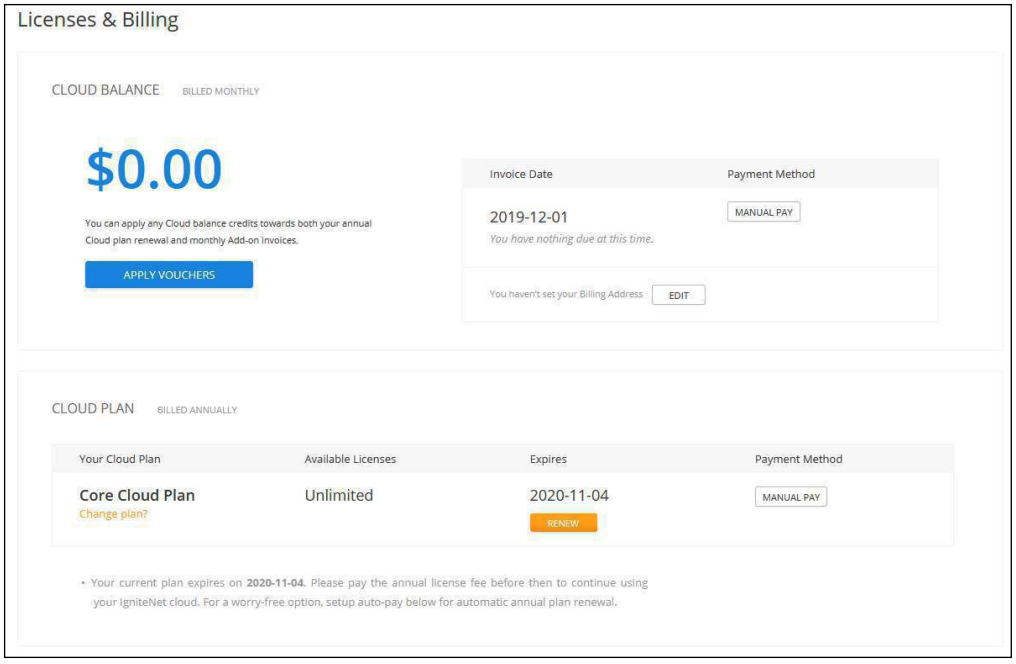


Note: Do not enable MSP Mode and "Always follow cloud configuration" at the same time. This will cause the device configuration not to be updated to ecCLOUD properly.

Managing Licenses and Billing

From the Cloud menu, click Licenses & Billing to manage your ecCLOUD payment plan.

Figure 58: Managing Licenses and Billing



From the Licensing and Billing page you can:

- Apply voucher codes to add credit to your existing cloud plan renewal and Add-on invoices.
- Upgrade the your cloud plan from a Trial Plan to a Core Cloud plan or a Virtual Private Cloud plan. Upgrades are enabled through credit card billing either a single manual payment or with automatic renewal payments. You can also apply Edgecore vouchers as payment for the upgrade.
- View Enabled Add-ons and Invoice History records.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3467D8B059B3E321B66283D2920E5 | Anistia EC_processoDigitalizado_029_20252025227.pdf (69/301) 3772/4726

Report Management

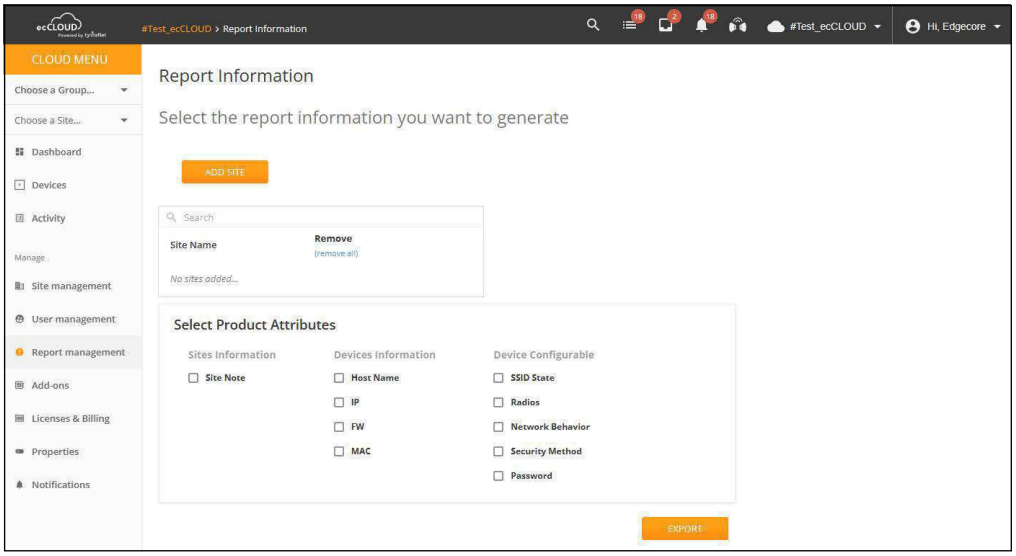
The Report Management feature in ecCLOUD provides a convenient way for Cloud Owners and Administrators to generate and download custom reports containing information of the sites within the network.

Generate a Report

To generate a custom report, follow these steps:

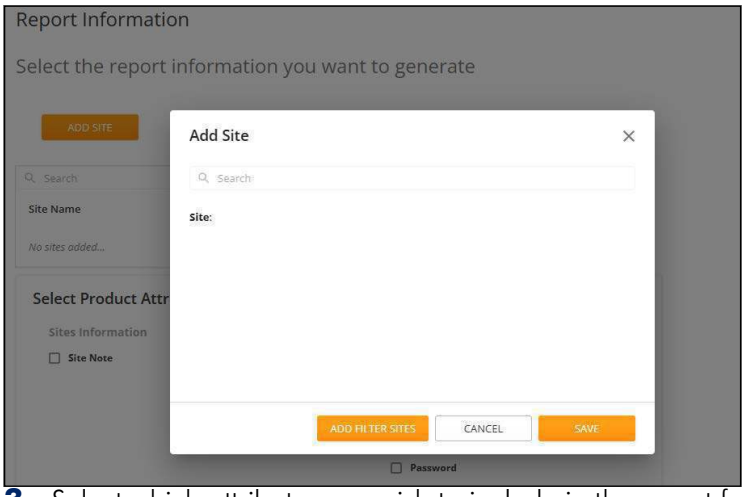
1. Navigate to 'Report Management' in the Cloud menu.

Figure 59: Report Information



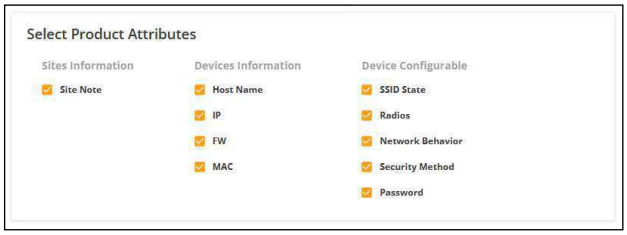
2. Click 'Add Site' to include sites in the report. Use the search bar to find specific sites or 'Add Filter Sites' to include all sites that meet certain criteria. Click 'Save' to confirm.

Figure 60: Add Sites



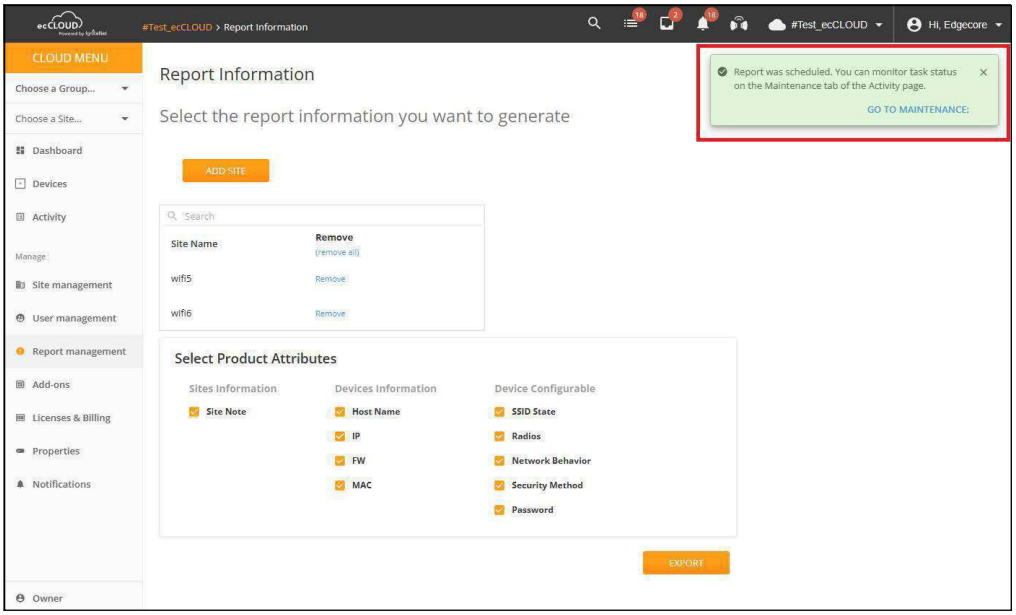
3. Select which attributes you wish to include in the report from the 'Select Product Attributes' section.

Figure 61: Select Site Attributes



4. Click 'Export' to generate the report. A green notification will appear in the top right corner as confirmation of the action.

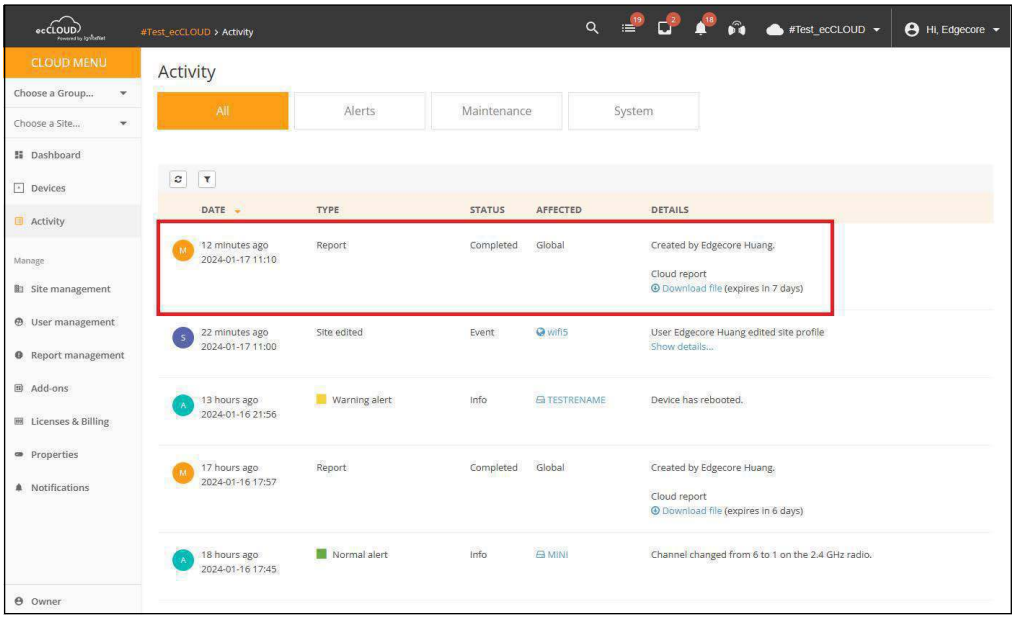
Figure 62: Schedule Report Export



1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - TR 029/2025 Anexo E - Especificações Técnicas (71/301) 1376/4746

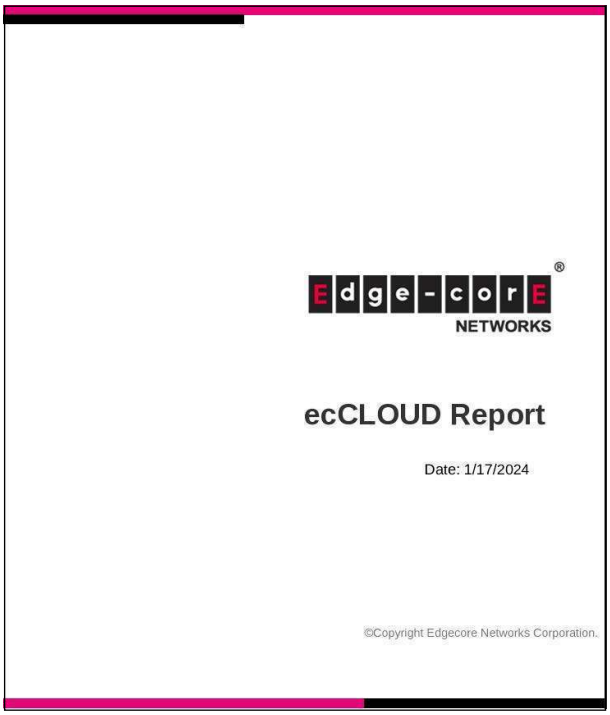
5. Monitor the status of the report creation in the 'Activity' section. A completed task will indicate the report is ready for download. Note that the file will expire after 7 days.

Figure 63: Activity Section with Report



6. Download the report by clicking on the 'Download file' link. The report will be saved locally to your device.

Figure 64: Report File



1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - 07/08/2025 | Anexo E - ecCloud Usuario - 29_05_2025_20250627.pdf (73/301) 1776/4746

Add-Ons

This chapter describes add-ons that can be used for the following categories:

- Enhanced Guest Wi-Fi & External Captive Portal Services
- Security and Family Services
- ecCLOUD Extensions
- Additional Hardware Support

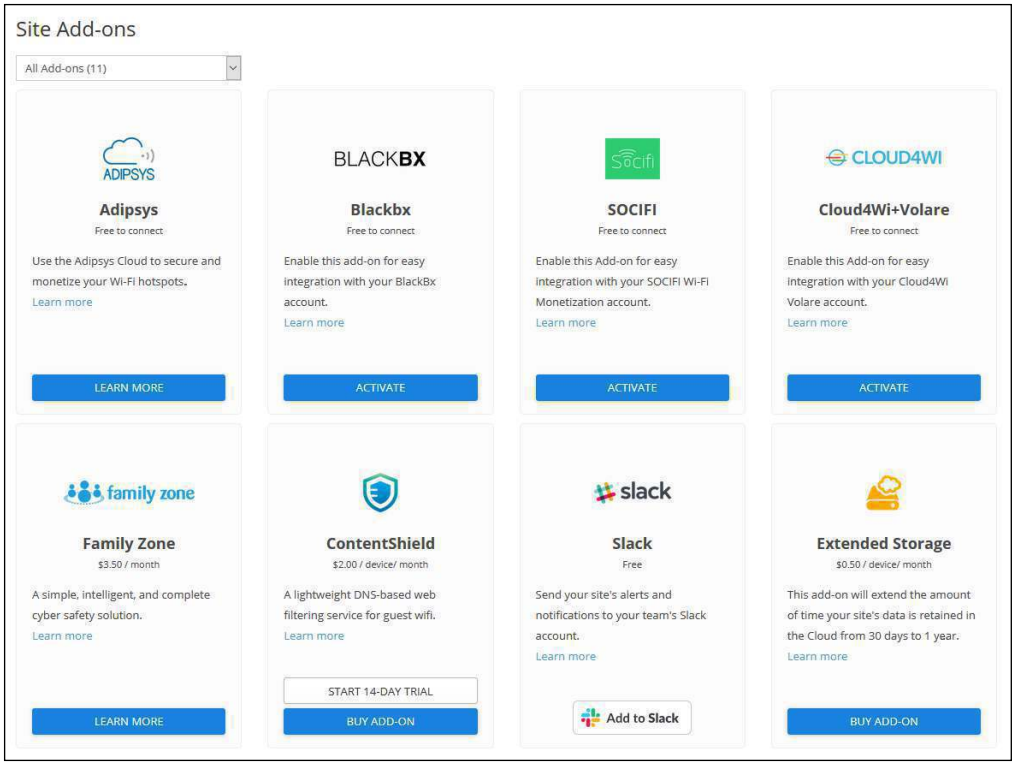
Using Add-ons

From the Add-ons Menu, available at both Cloud and Site levels, click on selection icon, click on "Learn More," and then click on the "Activate" button to use the selected service.

Certain add-ons are accessible exclusively at the Cloud level, as their features impact the entire cloud deployment. Examples include:

- Wedge Security Service
- Smart Indoor Location

Figure 65: Add-ons Menu



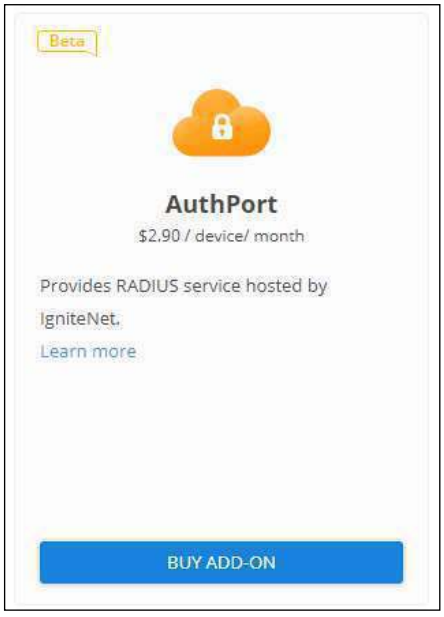
Using the AuthPort Add-On

The AuthPort Add-on enables the built-in authentication server of ecCLOUD, supporting authentication, authorization, and accounting (AAA) functions for wireless clients. With AuthPort enabled, you can create accounts based on different service plans, which defines the time and data quota for each account. When the wireless client associates to the network, the client can login with the created account to obtain Internet access.

Note: Currently, AuthPort is only supported on the following models: ECW5211-L, ECWO5211-L, OAP100, ECW5410-L, SP-W2-AC1200 (L), SS-W2-AC2600, EAP101, EAP102, EAP104.

You can purchase this add-on by navigating to the "Add-ons" menu item from either the Cloud or Site-level menus, and pressing the "BUY ADD-ON" button on the AuthPort add-on.

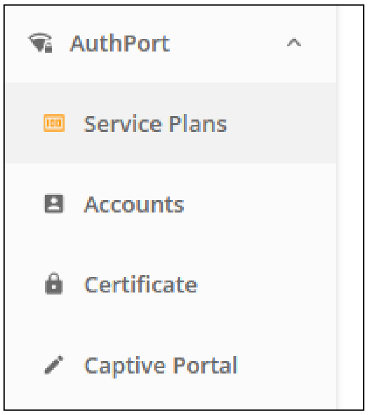
Figure 66: AuthPort Add-On



After enabling the AuthPort add-on, the AuthPort configuration menu will appear on the Cloud menu. You can configure a Service Plan, Accounts, Certificate, and Captive Portals respectively.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - Termo de Referência 29/2025 Administrativo_processo_licitatorio_029_2025_pdf_27.pdf (75/301) 1300/4726

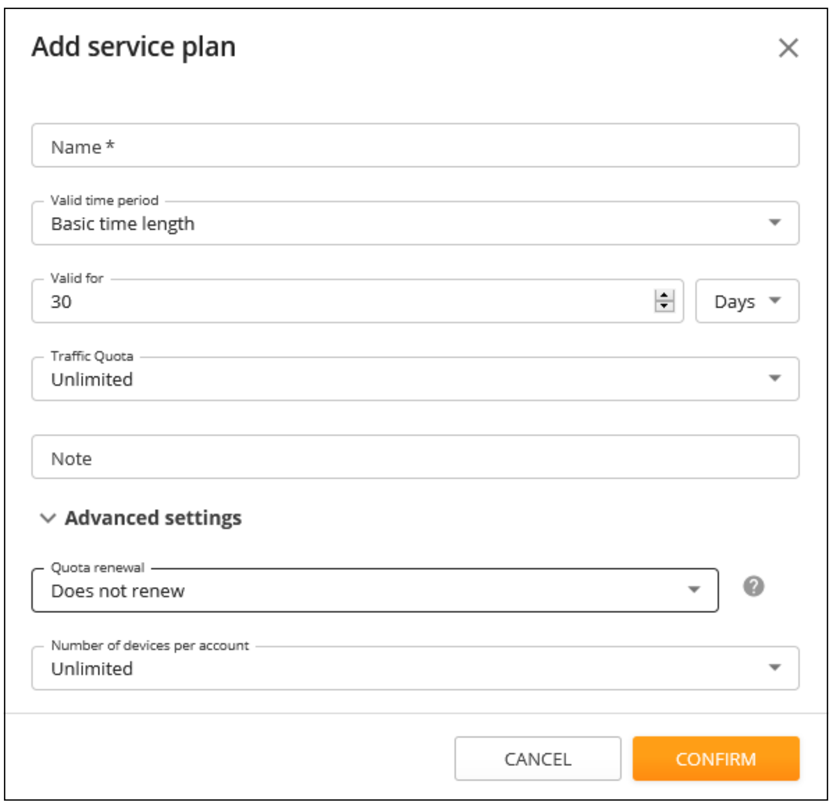
Figure 67: The AuthPort Menu



Service Plans

A service plan defines the usage limitations for an account. Before creating an account, you must define the service plan first.

Figure 68: Adding a Service Plan



The following list shows the configurable items for a service plan.

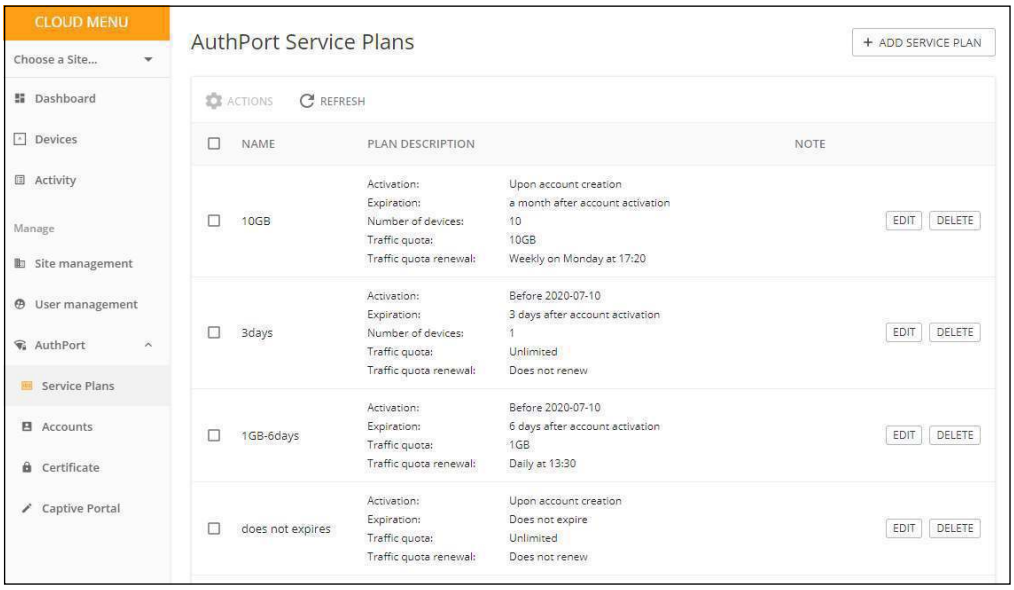
- **Name** — The name of the service plan.

1Doc: Protocolo 1.943/2025 ... .pdf (76/301)

- **Valid time period** — The account is available only in the defined valid time period. The time period is defined by the activation and expiration times.
- **Activation time** — The client must log in to the account before the activation time. If not, the account will expire and cannot be used.
- **Expiration time** — The account will expire and cannot be used after the expiration time.
- **Traffic quota** — The quota limitation for the account. If the client uses more traffic than the quota limitation, the account will be "out of quota" and cannot be used for login.
- **Note** — Any additional information for the plan.
- **Quota renewal** — Configure the time for the account to renew the traffic quota. The quota can be renewed daily, weekly, or monthly.
- **Number of devices per account** — The number of devices that can use the same account to login at the same time.

On the Service Plans page, you can see a list of overviews for all existing plans. You can also add new plans, edit existing plans, or delete plans from this page.

Figure 69: Service Plans Overview



1Doc: Protocolo 1.943/2025 | Anexo Administrativo Processo Digital Nº 029.2025.0256227.pdf (77/301) 1382/4726

Accounts

Accounts for wireless clients can be generated based on the service plans. Accounts can be created one by one or in a batch. When creating a single account, the username and the password of the account are configured manually. When creating accounts in a batch, the usernames and passwords are randomly generated.

Figure 70: Creating a Single Account

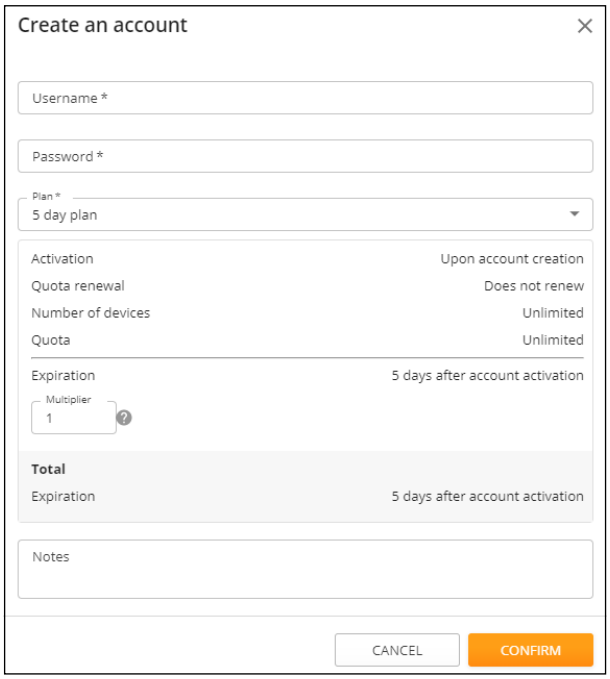
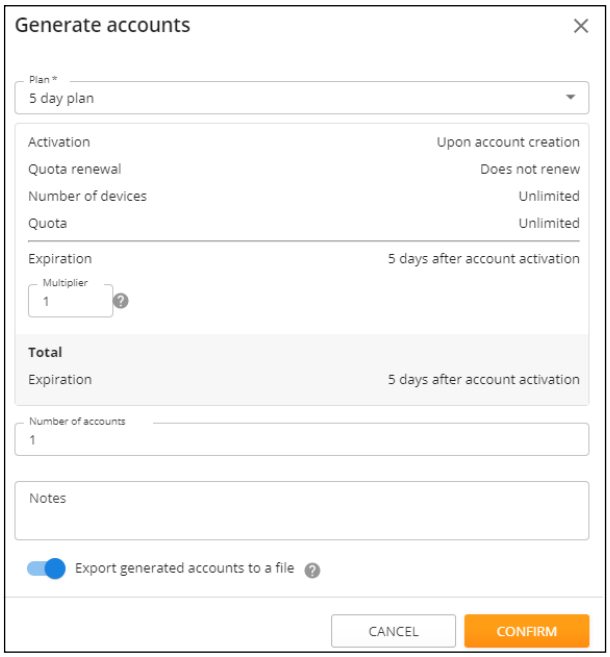


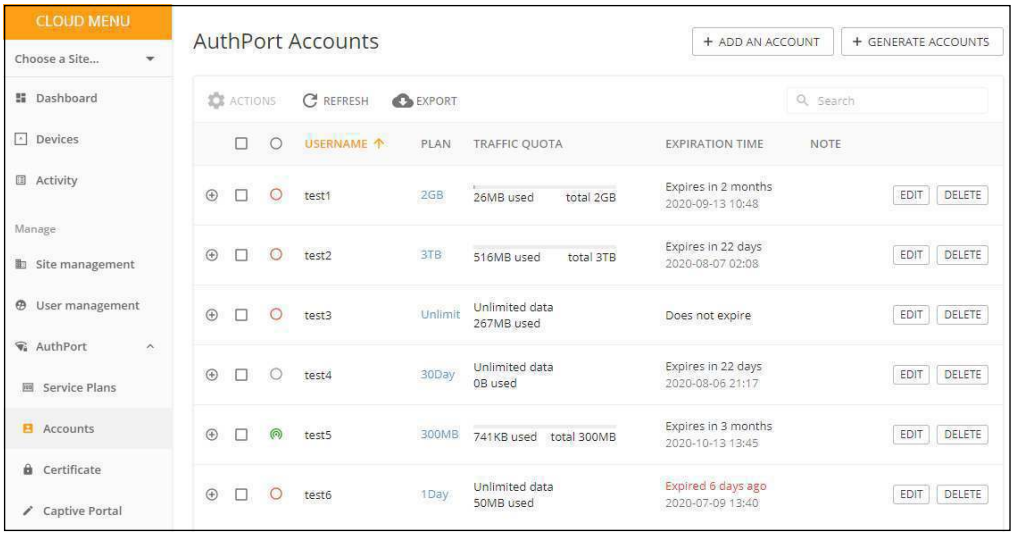
Figure 71: Creating Accounts in a Batch



1Doc: Protocolo 1.943/2025 | Anexo Administrativo 08059386321866289 2025 Anistia EC_processo_Diretoria_029_20252026227.pdf (78/301) 3783/4726

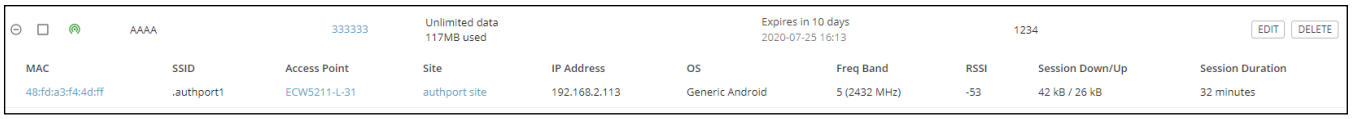
Both methods of creating accounts have a "multiplier" that can be configured to allow the account to include several units of the quota based on the service plan. For example, if an account is created based on a service plan with a 10 GB quota, you can set it to be three times the basic quota, making it have a 30 GB quota.

Figure 72: Account List



Once created, the accounts appear in the accounts list. In the accounts list, you can check the account status, corresponding plan, expiration time, and traffic quota information. Also, information of recent client device logins with the account can be examined here.

Figure 73: Account Details



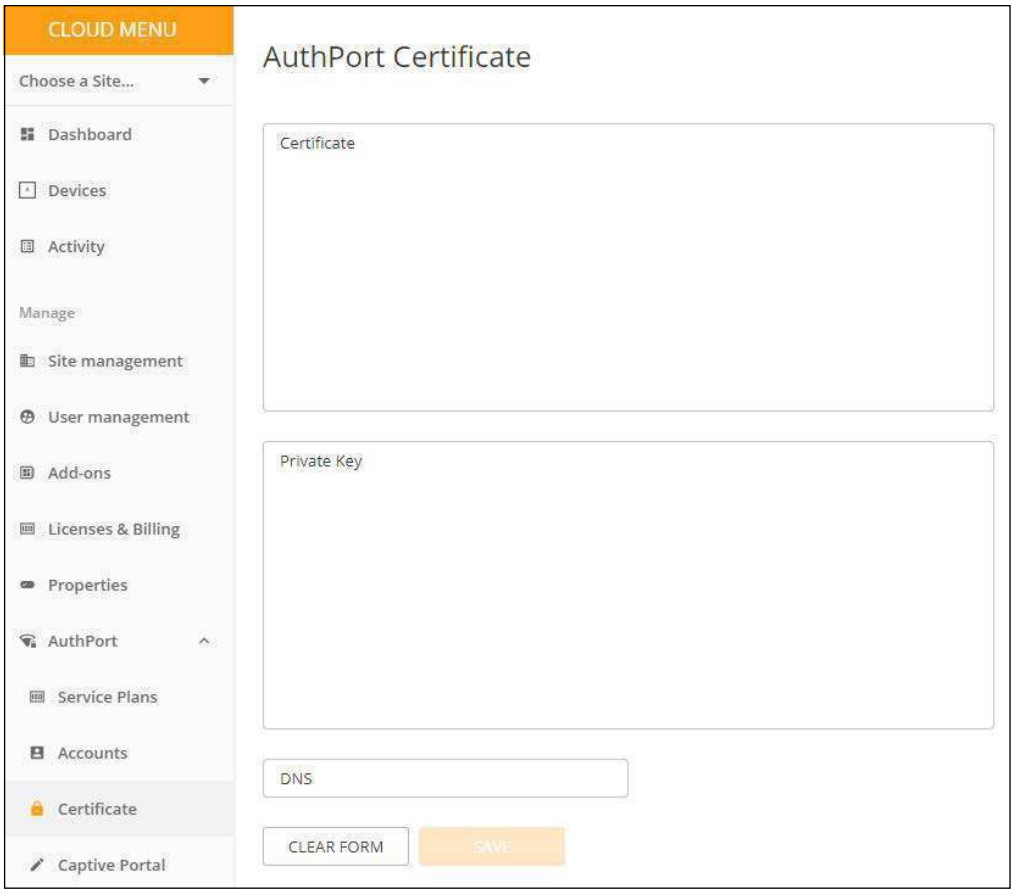
For each created account, the administrator can also edit its properties, including the password, corresponding service plan, and the multiplier for the total quota. In addition, the administrator can export selected accounts to a CSV format file and distribute the accounts to the wireless clients.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - Termo de Referência 29.2025 Administrativo_processo_licitatorio_029_2025_pdf (79/301) 3732/4726

AuthPort Certificate

When AuthPort authentication is enabled, clients will see a captive portal page after connecting to the SSID. The administrator can upload a security certificate and configure the domain name for the captive portal page.

Figure 74: AuthPort Certificate



If a certificate is not configured, wireless clients will be redirected to the captive portal with an unencrypted HTTP connection. For security concerns, it is strongly recommended to prepare a valid certificate and upload it so that the captive portal will be under HTTPS protection. Note that the certificate and private key should be in PEM format. Just copy and paste the content of the certificate file and the private key file to the corresponding fields.

As for the DNS (domain name service), the administrator can configure a domain name that wireless clients will see for the captive portal page. If the DNS is not configured, clients will see the IP address of the AP in the URL of the captive portal page.

To prevent a security warning in the web browser, make sure the certificate is signed by a trusted authority. Also, make sure the configured domain name is the same as the "common name" (CN) field defined in the certificate.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3467D8B059B3E321B66289D2/2025 | Anexo EC_proc_SEI_Diretoria_029_2025_pag_27.pdf (80/301) 1313/4746

Captive Portal

AuthPort provides an editor for captive portal page customization. You can define multiple captive portal templates and apply a different template to different AuthPort-enabled SSIDs.

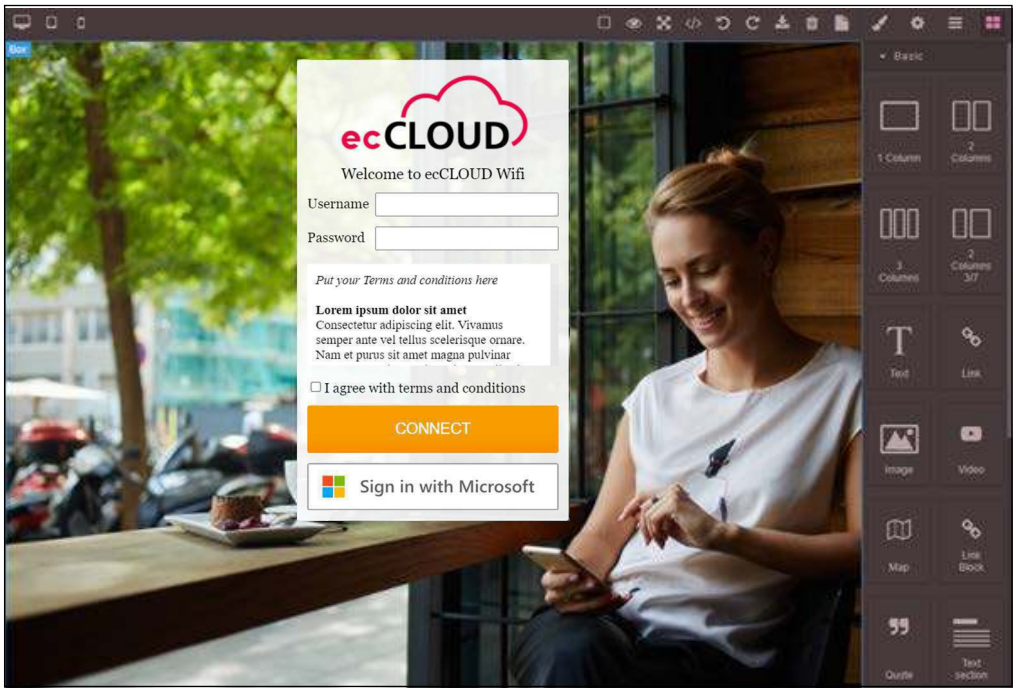
When you create a captive portal and access the editor for the first time, you will be asked to select a theme for your portal. You can select a theme that is appropriate for your service and start editing the page content.

Figure 75: AuthPort Captive Portal Themes

After selecting a template, you will enter the captive portal editor. The editor layout consists of three main parts; a tool bar, an options/attributes panel, and a preview frame. The tool bar is at the top of the editor. On the right-hand side is where the options or attributes can be configured. The preview frame allows you to drag-and-drop page objects and check your portal design in real-time.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 08059386121866289_2025 | Anistia EC_processo_digital_Manoela_2025_026227.pdf (81/301) 1736/4726

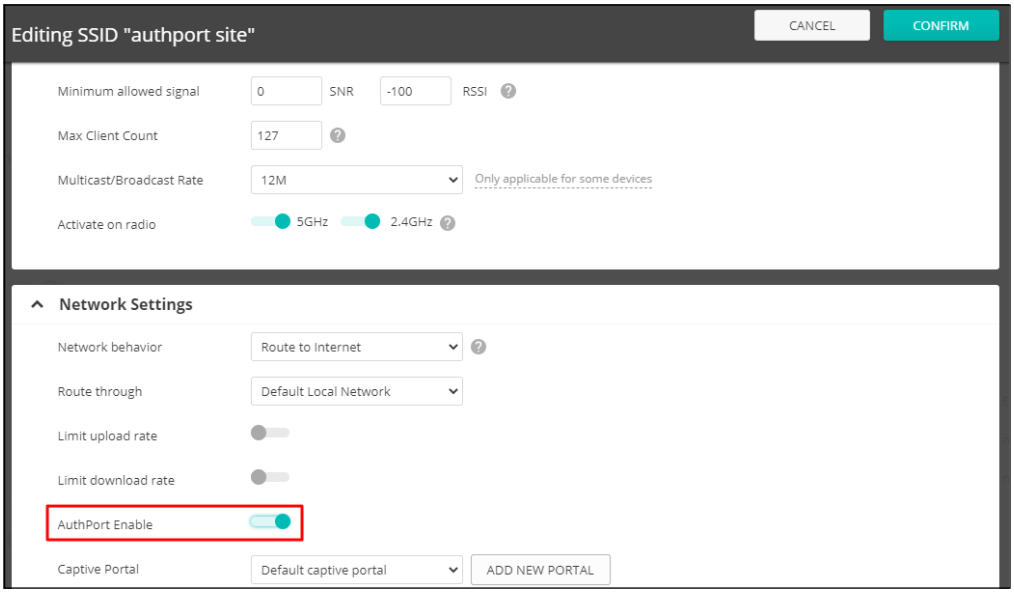
Figure 76: AuthPort Captive Portal Editor



SSID Configuration

AuthPort supports per-SSID configuration for enabling authentication. For example, if you have two SSIDs where one is for staff and the other is for customers, you can enable AuthPort authentication only on the customer SSID. When staff members associate to the staff SSID, they can immediately obtain Internet access. When customers associate to the customer SSID, they are brought to the captive portal page where login credentials are requested.

Figure 77: AuthPort SSID Configuration



1Doc: Protocolo 1.943/2025 | Anexo Administrativo 08059386121866289 - 29/2025 Administrativo_ecCloud_Usuario_029_20252026227.pdf (82/301) 1383/4746

AuthPort authentication not only works with a captive portal, but it also can be integrated with EAP authentication. When the security method is Open, WPA-PSK, or WPA2-PSK, and if AuthPort Enable is “on” for the SSID, wireless clients are redirected to the captive portal page after association. Clients can use the AuthPort-created account or use their Microsoft 365 credentials to login and obtain Internet access.

When the security method is WPA-EAP or WPA2-EAP, and if AuthPort Enable is “on” for the SSID, the cloud will become the RADIUS server for the EAP authentication. Wireless clients can use the AuthPort-created accounts as the credentials for wireless connection and complete the transparent login.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 08 (83/301) 1738/4746

Using the Aprecomm Add-On

The Aprecomm add-on service, through its Virtual Wireless Expert (VWE), equips ISPs with a unified tool for real-time network visibility and insights, simplifying troubleshooting and enhancing customer support. ecCLOUD users can activate a no-cost Freemium service or purchase a premium license for an extended feature set.

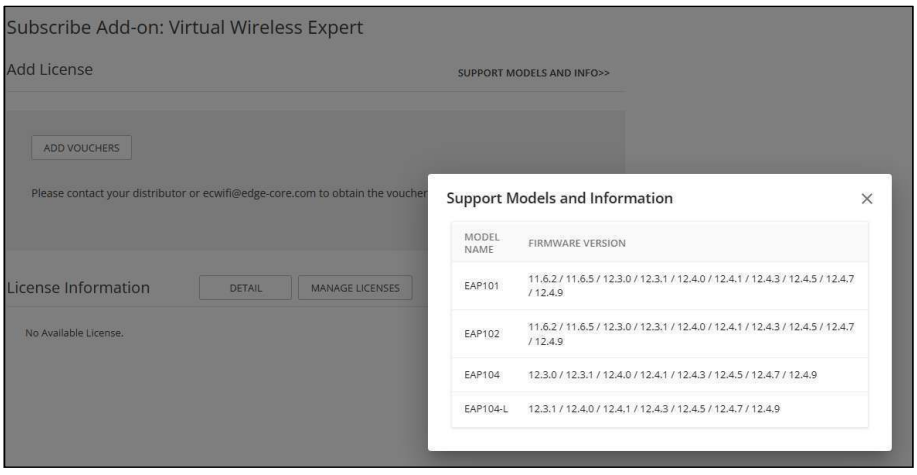
Figure 78: Aprecomm Add-On

Supported Devices and Firmware Versions

To view information on supported Edgecore Wi-Fi APs, follow these steps:

1. In the 'Add-ons' menu at the Cloud, Site or Device level, click 'Subscribe / Redeem'.
2. Select 'Support Models and Info' to view supported model names and firmware details.

Figure 79: Supported Devices and Firmware Versions



1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 de 2025 | Anexo EC_procesoDigitalizacion_029_2025_pag_27.pdf (84/301) 1789/4746

Activating Freemium

The freemium version can be activated globally at the cloud level or individually at the site level.

1. In the Cloud or Site menu, click 'Add-ons' and then 'Activate' under Aprecomm's Virtual Wireless Expert.
2. After confirming the activation, it automatically installs the Aprecomm package on devices running compatible firmware.

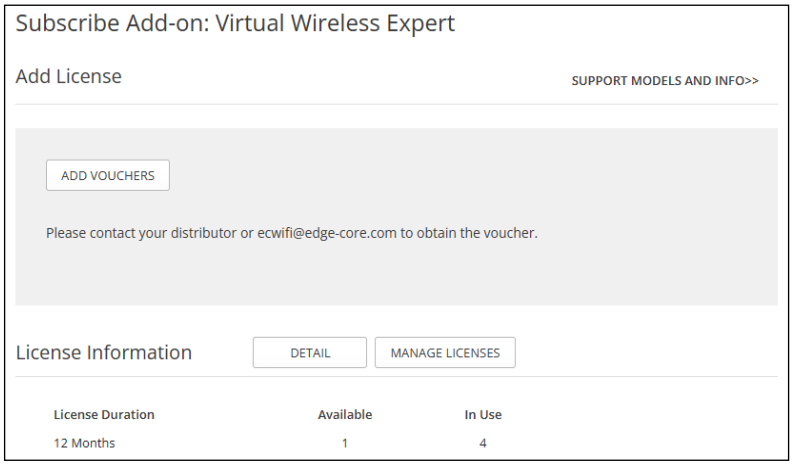
Note: The cloud agent on the device periodically queries ecCLOUD for new packages to install, including Aprecomm's package. A device reboot may expedite the process.

Purchasing Licenses

To enhance visibility and insights beyond the Freemium offer, follow these steps to purchase and apply Aprecomm VWE licenses:

1. Purchase voucher codes from your distributor or email ecwifi@edge-core.com.
2. Add licenses on ecCLOUD by selecting 'Subscribe / Redeem' under 'Add-ons' in the cloud menu. Click 'Add Vouchers' and enter the provided voucher code.

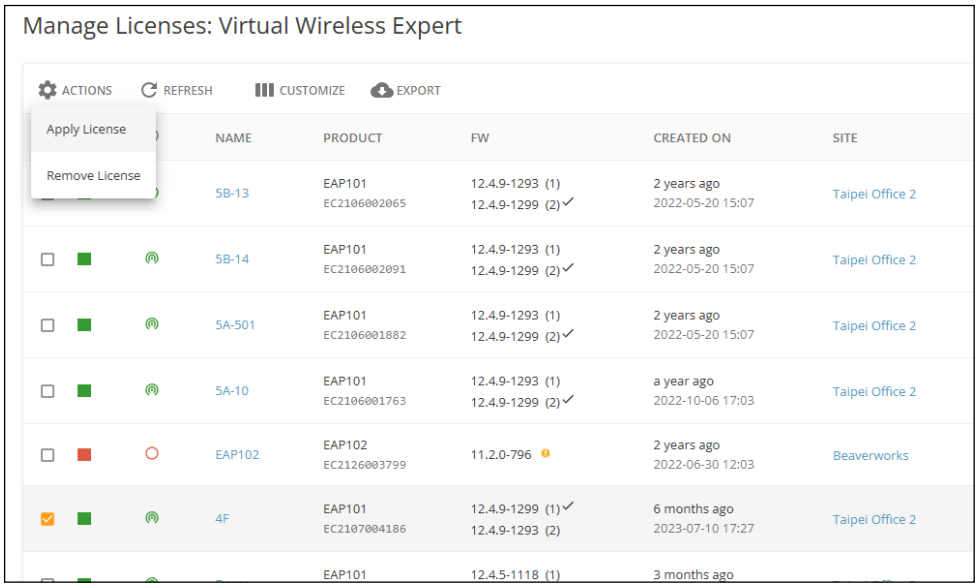
Figure 80: Add VWE Licenses



3. Activate the license in the cloud menu under 'Add-ons' by selecting 'Subscribe / Redeem'.
4. Click 'Manage Licenses' to list the supported devices.
5. Select the desired devices.
6. Click 'Actions' and 'Apply License'.

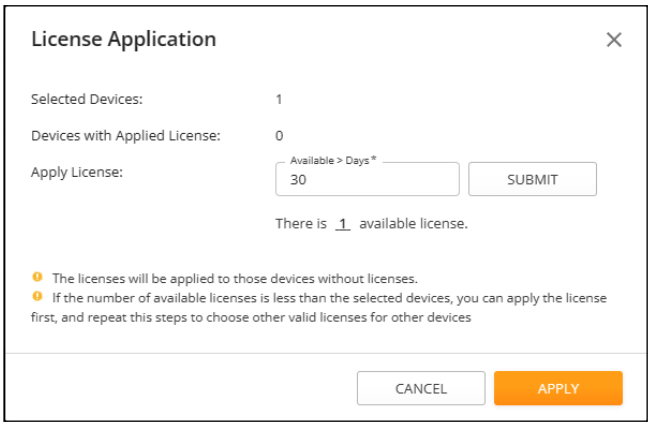
1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 de 2025 | Anexo Administrativo_procesado_Licitación_029_2025_page_27.pdf (85/301) 1798/4746

Figure 81: Apply VWE Licenses



7. Filter the available licenses by the number of available days and apply as needed.

Figure 82: VWE Licenses per Number of Days



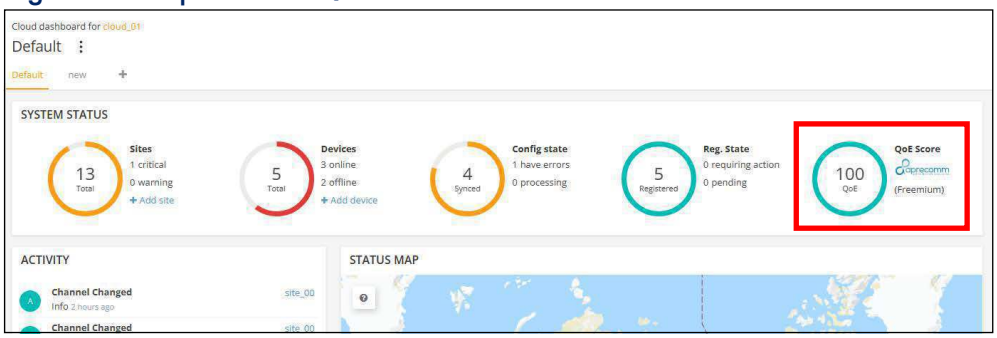
8. After applying the license, it automatically installs the Aprecomm package on the selected devices.

Note: The cloud agent on the device periodically queries ecCLOUD for new packages to install, including Aprecomm's and associated license. A device reboot may expedite the process.

Accessing the VWE Dashboard

In the Freemium plan, the QoE score by Aprecomm can be viewed in the dashboard at the Cloud, Site, or Device level.

Figure 83: Aprecomm QoE Score

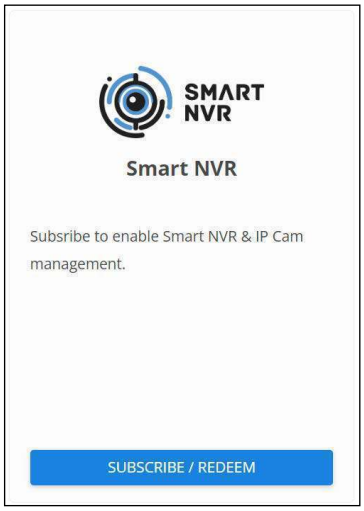


1Doc: Protocolo 1.943/2025 | Anexo Administrativo 08059386321866289_2025_Anexo_Administrativo_08059386321866289_2025.pdf (87/301) 1722/4726

Using the Smart NVR Add-On

The Smart NVR add-on integrates network video recording capabilities within the ecCLOUD platform, allowing users to manage IP cameras across multiple sites. This add-on supports the onboarding of Smart NVR devices and provides features for configuring, managing, and viewing live footage and recordings from IP cameras. ecCLOUD users benefit from automated IP camera scanning, cloud-based configuration, and real-time alerts for system status and camera connectivity.

Figure 84: Smart NVR Add-On



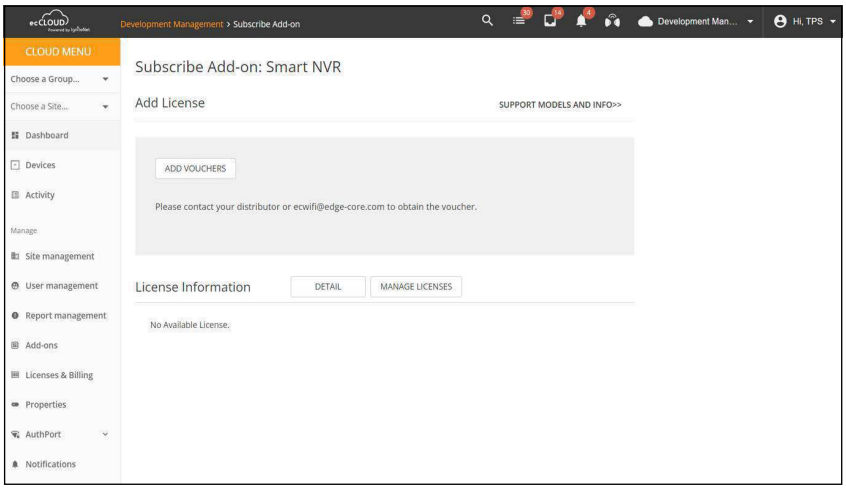
Purchasing Licenses

Follow these steps to purchase and apply Smart NVR licenses:

1. Purchase voucher codes from your distributor or contact ecwifi@edge-core.com.
2. Add licenses on ecCLOUD by selecting 'Subscribe / Redeem' under 'Add-ons' in the cloud menu. Click 'Add Vouchers' and enter the provided voucher code.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 (88/301) 3793/4746

Figure 85: Adding Smart NVR Licenses

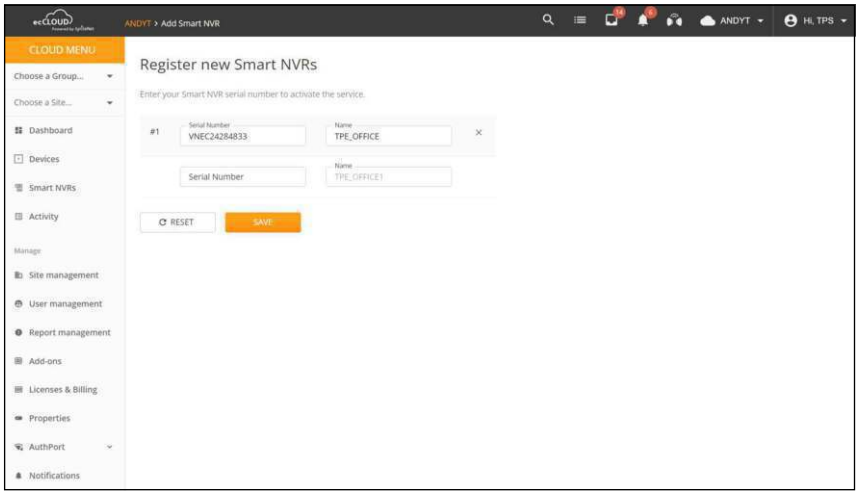


Once the voucher is successfully redeemed, the Smart NVR option will appear in the Cloud Menu.

Adding Smart NVR Devices

The currently supported Smart NVR device is a VM-based service. To add a new device, you will need the device's serial number. Please contact your distributor or Edgecore sales to obtain the serial number.

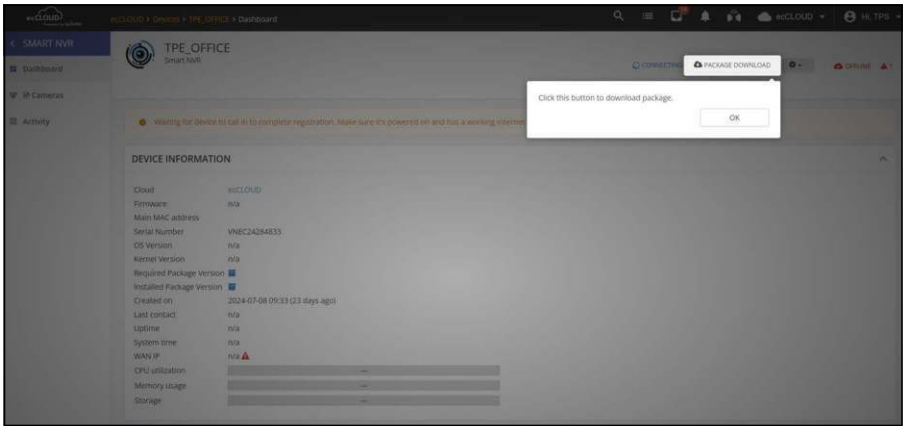
Figure 86: Adding a Smart NVR Device



1. Navigate to the Smart NVR management page and click 'Add Device'.
2. Enter the device's serial number and assign an easily identifiable name.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 de 3 | Anexo_Administrativo_3_de_3_Protocolo_1.943_2025.pdf (89/301) 1792/4746

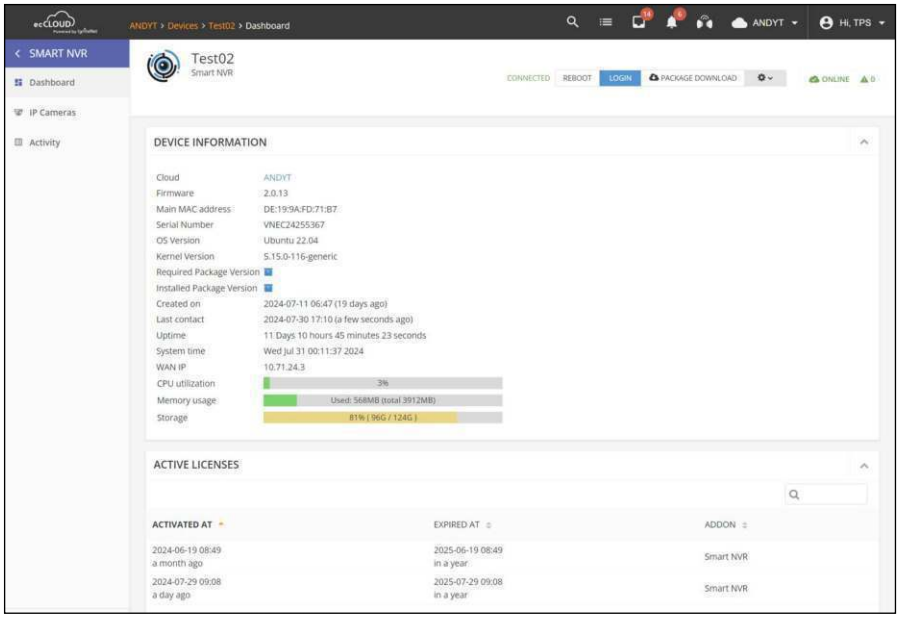
Figure 87: Installing and Registering a Smart NVR



After the device is added to the cloud account, users must download the required software package and install it on the Smart NVR device. To do this, follow these steps:

1. Access the Smart NVR's dashboard by clicking on the device name.
2. Click 'Package Download' to obtain and install the necessary software package, and register the device on the cloud account.

Figure 88: Smart NVR Dashboard



The Smart NVR dashboard provides a comprehensive overview of device status, system performance, and active licenses, offering users easy access to essential management features and real-time data.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 08059386121866289129_2025_Anexo_ECC_ecCloud_User_Manual_EN_20250627.pdf (90/301) 1795/4746

- Device Information Section:
  - **Cloud** — The name of the cloud managing the selected Smart NVR.
  - **Firmware** — The current firmware version installed on the Smart NVR.
  - **Main MAC Address** — The MAC address of the Smart NVR.
  - **Serial Number** — The Serial Number of the Smart NVR.
  - **OS Version** — The version of the operating system running on the Smart NVR.
  - **Kernel Version** — The kernel version of the Smart NVR's operating system.
  - **Required Package Version** — Hover over the icon to view the required package version for the Smart NVR.
  - **Installed Package Version** — Hover over this icon to see the currently installed package version on the Smart NVR.
  - **Created on** — The date and time when this device was added to the cloud.
  - **Last contact** — The most recent time the device reported its status to the cloud.
  - **Uptime** — The duration the Smart NVR has been running.
  - **System time** — The current system time set on the Smart NVR.
  - **WAN IP** — The WAN IP address assigned to the Smart NVR.
  - **CPU utilization** — The current CPU usage percentage of the Smart NVR.
  - **Memory usage** — The amount of memory currently being used by the Smart NVR.
  - **Storage** — The current status of the Smart NVR's storage, reflecting the operational capacity of the system.
- Active Licenses Section:
  - **Active Licenses** — Details of the licenses currently active on this Smart NVR.
- Live Action Section:
  - **Reboot** — Reboots the Smart NVR system.

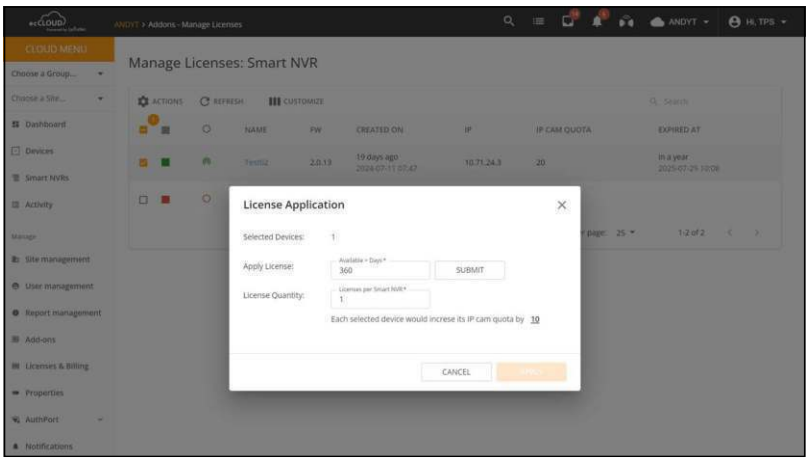
1Doc: Protocolo 1.943/2025 | Anexo Administrativo 08059386321866289 29/2025 Anistia EC processo Distorção 029 2025 26227.pdf (91/301) 1796/4746

- **Restart All Services** — Reboot all micro services running on the Smart NVR.
- **Login** — Allows the user to log in to the Smart NVR system for IP Camera live view and historical data access.
- **Package Download** — Download the Smart NVR package for installation or update.

Manage Licenses and IP Camera Quotas

Once you have configured the Smart NVR device, you can add IP cameras. Each Smart NVR license has a quota of ten IP cameras.

Figure 89: Applying Smart NVR Licenses



1. Navigate to 'Add-ons' and select the Smart NVR Add-on.
2. Click 'Manage Licenses', select one or more Smart NVR devices, and choose 'Apply license' from the Actions menu.
3. Specify the number of days and the quantity of licenses needed based on the number of IP cameras to connect.

Figure 90: Available Quotas for IP Cameras per Smart NVR device

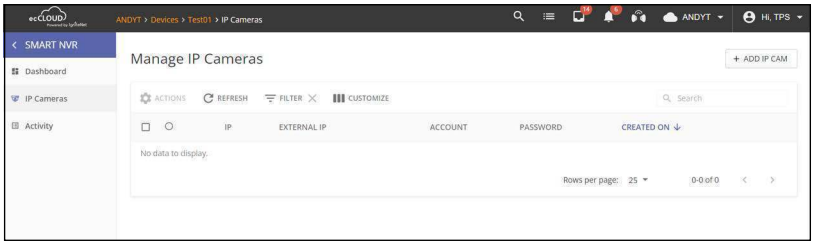
4. Confirm the available quota of IP cameras on each Smart NVR.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 08059386321 de 29/12/2025 | Anexo_EC_acCeso_Distancia_029_2025_pdf.pdf (92/301) 1795/4746

Add IP Cameras

To add an IP camera to the Smart NVR, users can scan the IP camera through their Edgecore Access Point.

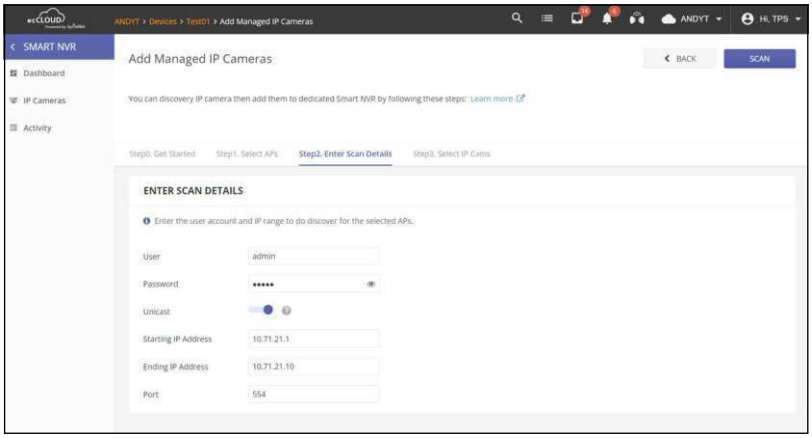
Figure 91: Add IP Cameras



Navigate to the Smart NVR device, click 'IP Cameras' and follow these steps:

1. Select the Access Point(s): Choose the APs for the scanning task. These devices will locate the IP cameras on the network.

Figure 92: IP Cameras Scan Details



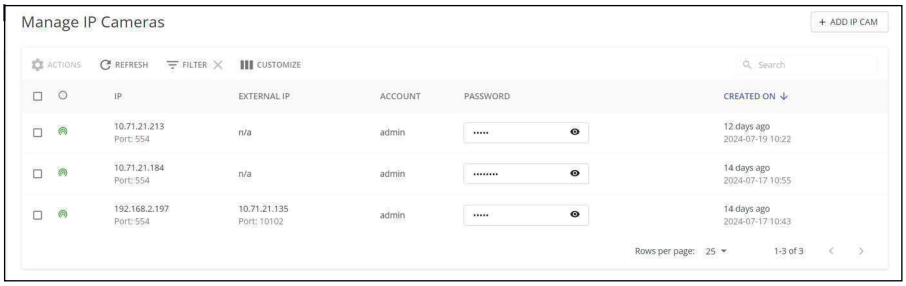
2. Configure the ONVIF scanning task:
   - Enter the login credentials of the IP cameras.
   - The AP automatically configures the Port Forwarding settings, allowing the Smart NVR to communicate with the IP cameras.
3. Multicast scan and additional Unicast scan:
   - Multicast Scan: By default, the scan uses Multicast to detect IP cameras connected to the AP's network.
   - Unicast Scan: Optionally, users can specify an IP range and port for Unicast scanning. This allows for locating IP cameras that may not be detected through Multicast.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 08059386121866289 29/2025 Administrativo_processo_Licitatorio_029_2025_26227.pdf (93/301) 1796/4746

4. Click 'Scan' to begin. Monitor the progress through the progress bar, indicating completed and in-progress APs. The scanning process may take some time.

5. Review and Select the cameras you wish to add to the Smart NVR. Click the 'Done' button to import the selected IP camera information into the Smart NVR.

Figure 93: Status and Details of IP Cameras



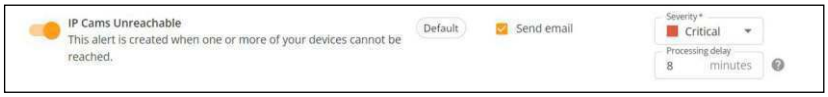
Note: ONVIF scanning results are stored in the cloud for 7 days. If an AP is deleted during an ONVIF scan task, the scan task for the deleted AP will be canceled. Deleting an AP will not remove IP cameras from the network, but these cameras may go offline if port forwarding rules were configured on the AP. If you add, edit, or delete profiles in an IP camera, you must re-scan and re-add the camera to the Smart NVR to update the profile information.

Configure Notifications

To receive email alerts for unreachable IP cameras:

1. Navigate to 'Notifications' in the cloud menu.

Figure 94: Enable Notifications for Unreachable IP Cameras



2. In the Alerts section, enable or disable email alerts for unreachable IP Cameras.

3. Users can define the severity and set the interval between health checks (minimum 5 minutes, default 8 minutes).

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 08059386121866289_29_2025_Anistratec_procesoDigitalMarco_2025_20250627.pdf (94/301) 1729/4746

3 General Site Configuration

This chapter describes site configuration, including parameters that apply to all site devices or to the overall site.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 (1) (95) | Anexo Administrativo 3 (1) (95).pdf (95/301) 1808/4746

Overview of Sites

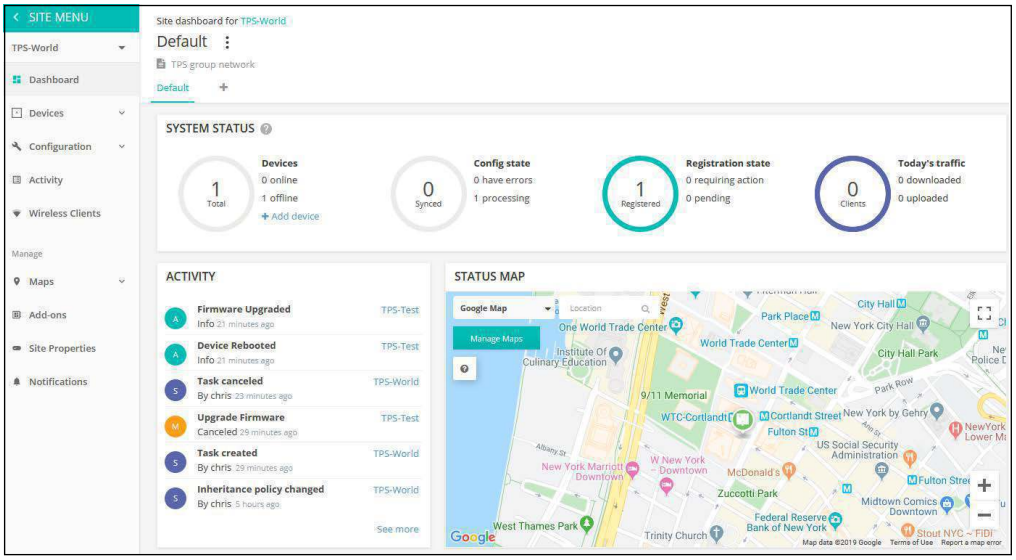
A site is a logical grouping of devices that may or may not share common configuration settings. It is customary to group devices located at the same site.

For example, if you are installing 50 APs for a hotel chain, each hotel location would be represented by a different site on the ecCLOUD controller. Each site can have a geographical location associated with it, a set of floor maps, and even preferred language and time zone settings.

Note: The number of devices in a site is limited to under 500.

The number of sites you can add to a cloud is dependent on your cloud plan; for a Core Cloud plan the limit is 500, for a Virtual Private Cloud plan the limit is 5000.

Figure 95: Default Site Dashboard



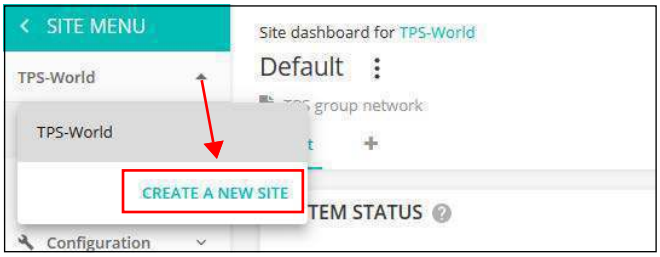
1Doc: Protocolo 1.943/2025 | Anexo Administrativo_pcCloudDistorta_029_20252025227.pdf (96/301) 1829/4726

Creating a Site

When creating your first cloud, you are also prompted to create your first site and add devices. See "Creating Your First Cloud" on page 29 for details.

To create additional sites from the Site menu, click on the pull-down list of sites at the top of the menu. At the bottom of the list, click "Create a New Site."

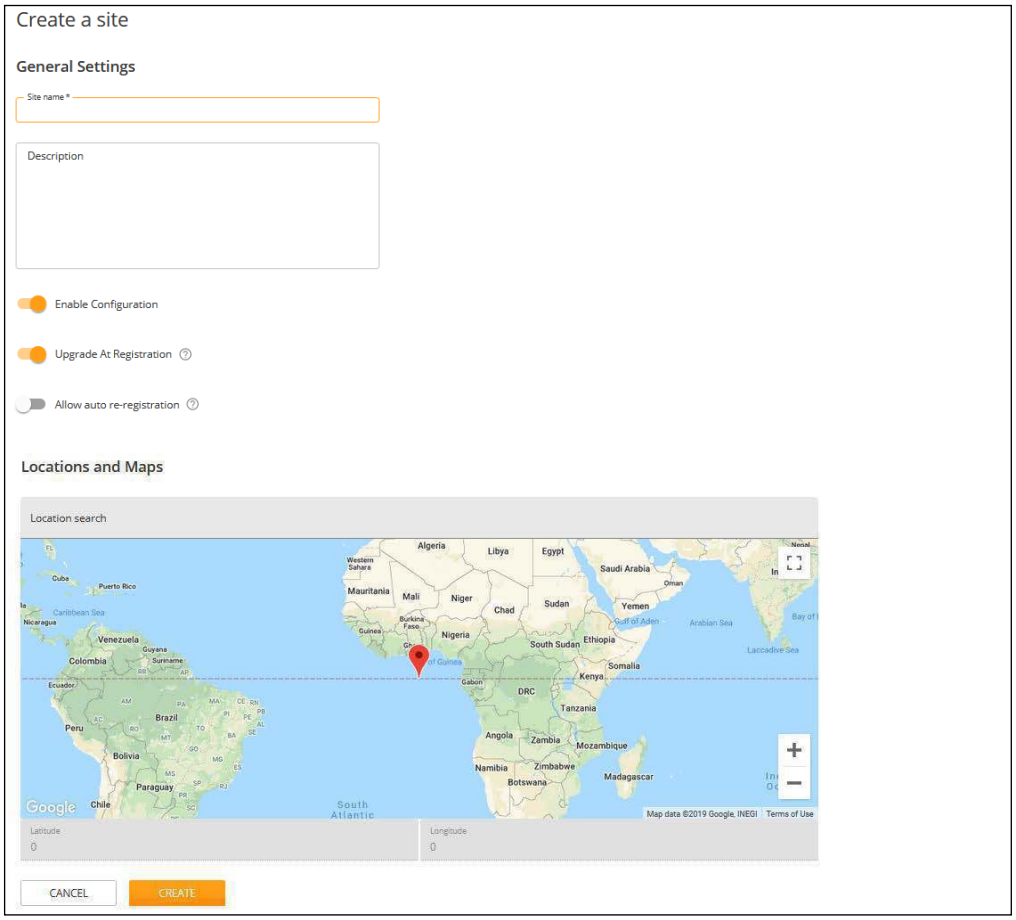
Figure 96: Creating a New Site



After opening the "Create a Site" page, fill in the properties for your new site and select the geographic location using the map.

Note: Items marked with an asterisk are mandatory.

Figure 97: Entering Basic Site Properties



General Settings

- **Site Name** – The name of your site. You should choose something short but meaningful. For example, use "ParkSide Atlanta" for a site that represents the Atlanta installment of a fictional ParkSide hotel chain.

- **Description** – Add any notes about your site here.

- **Enable Configuration**: This setting has the following options:

  - ON: Enables you to remotely configure your devices. (default)

  - OFF: Your devices need to be configured locally. However, you can still remotely monitor your devices and you will still receive alerts when a device goes offline.

- **Upgrade At Registration**: Enable this setting if you want your devices to be automatically upgraded to the latest firmware after registration. It is recommended that you keep this setting on.

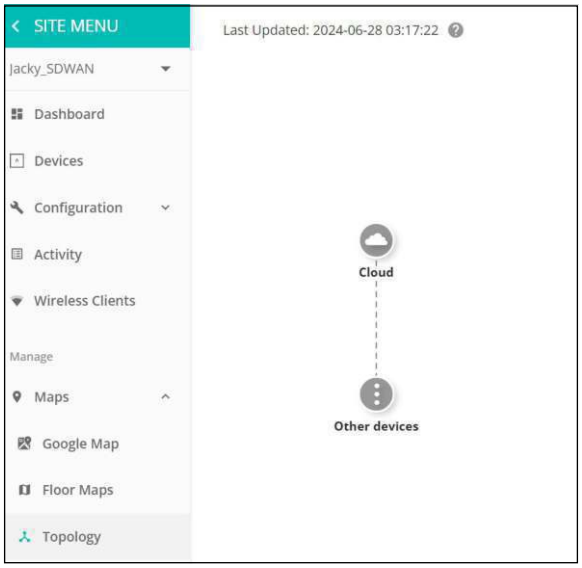
1Doc: Protocolo 1.943/2025 | Anexo Administrativo 08059386121866289129202 5 | Anistia EC_processo_disciplinar_029_2025_2025022 7.pdf (98/301) 1803/4746

- Allow auto re-registration: When this setting is enabled, your devices will automatically re-register when they are reset to defaults. If this setting is disabled, a user must log in to the cloud and manually chose the action to take when a device attempts to re-register.

Locations and Maps

Location – The location set here will determine which map is displayed on your site's dashboard by default, as well as which regulatory country will be used for wireless configuration purposes.

Figure 98: Topology Map with Timespamp



Topology Map – ecCLOUD automatically draws an interactive network topology based on network communication. The page displays the "Last Updated" timestamp, indicating the most recent update time. The minimum update interval is 1 hour.

Site Configuration

After configuring all the site information, click CREATE to create the site. You are then prompted to configure the new site's general settings, including the regulatory country and local logins.

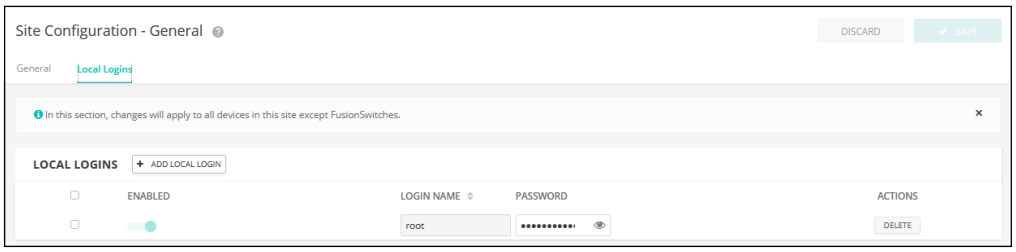
Figure 99: Setting the Regulatory Country

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 08059386321866289129202 5 | Anistia EC_proCesSo_Disciplinar_029_2025_2256227.pdf (99/301) 1802/4746

The Regulatory Country setting is typically pre-configured from the site's Location and Maps setting. The Local Logins also have one account configured by default using a randomly-generated password. You can modify the password and configure additional local accounts as needed.

Note: The Local Logins default account from the ecCLOUD Site-level configuration will overwrite the default account previously configured on the local user interface of a device. Once the Site-level configuration has been pushed to devices, you must use Local Login accounts configured in the ecCLOUD Site-level configuration.

Figure 100: Setting Local Logins



After setting the regulatory country and local logins, click "Save" to save your configuration.

Add Devices

When you first save the site configuration, you are prompted to add devices (wireless, switches, MeshLinqs, GLinqs) to your new site. Click "ADD DEVICES" to continue.

Figure 101: Add Devices Prompt

On the "Register new Devices" page, fill in the serial number, MAC address and name, and then click SAVE. Alternatively, you can use a barcode scanner by toggling the "Enable barcode scanning mode" to ON. You can then quickly enter the serial number and MAC addresses of your devices. Once entered, turn off the barcode scanning mode and enter the names of the devices manually. Click the SAVE button when you are ready to add your new devices to the site.

You also have the option of a batch upload. First, prepare a list of devices in a CSV (comma-separated values) file. A CSV file is a plain text file in which information is

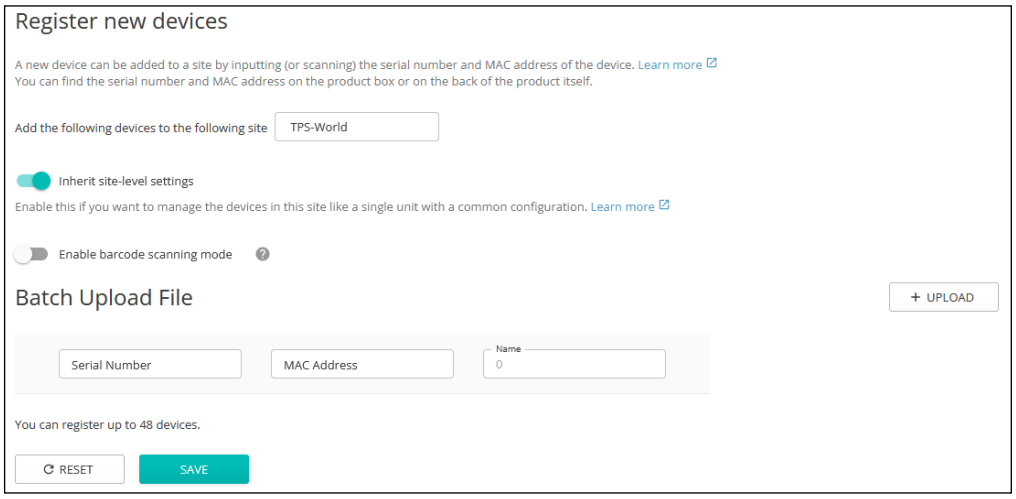
1Doc: Protocolo 1.943/2025 | Anexo Administrativo processo licitatório 029_2025_pregão 027.pdf (100/301) 1605/4726

separated by commas. For each device, the serial number, MAC address and name should be entered on one line, as in the following format.

```
<Serial Number 1>,<MAC 1>,<Device Name 1>
<Serial Number 2>,<MAC 2>,<Device Name 2>
```

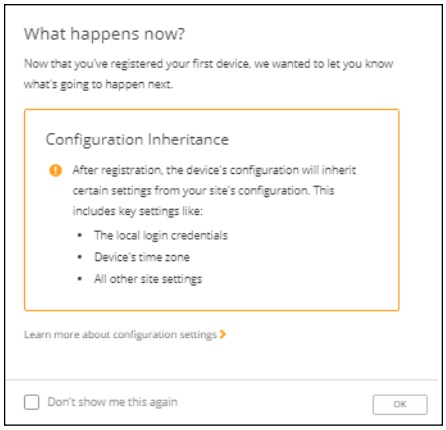
Click the UPLOAD button to upload your CSV file.

Figure 102: Registering New Devices



When the controller adds a device the following pop-up window is displayed warning you that the device will inherit settings from the ecCLOUD site configuration. Click OK.

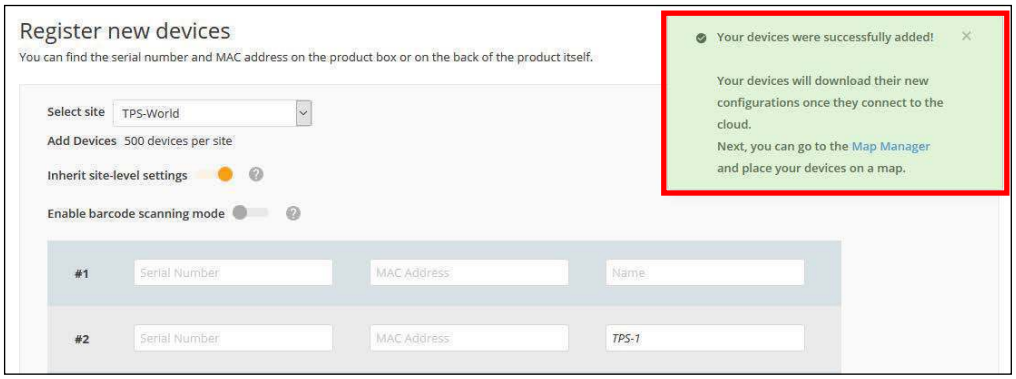
Figure 103: Adding Devices Warning Message



When devices have been successfully added, a message appears at the top of the "Register new devices" page. Click on the blue link "Map Manager" in the message to place your device on a map.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pag 1606/4726

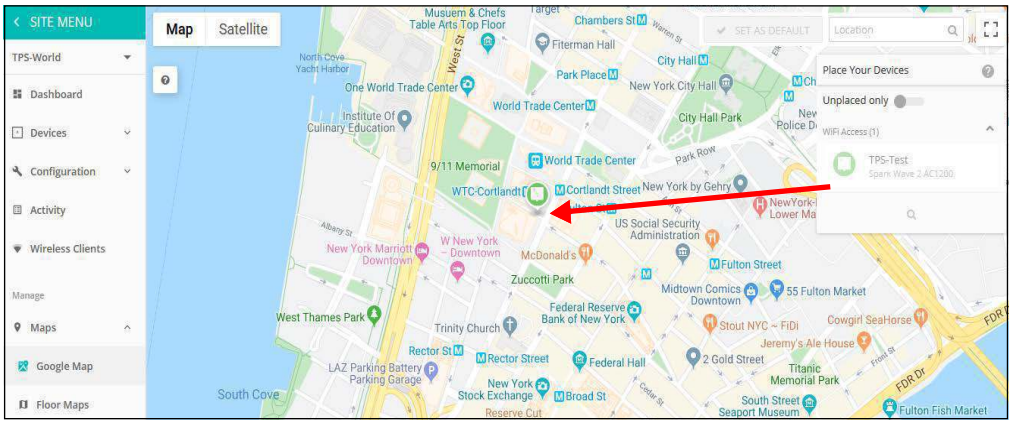
Figure 104: Adding Devices Successful Message



Place Devices on a Google Map

On the Google Map page, use the mouse to click-drag devices to installation locations on the map.

Figure 105: Placing a Device on a Map



Set Floor Maps

Floor maps provide a graphic view of your site, indicating the location and coverage area for each AP. Floor maps help you visualize where the APs and clients are in relationship to the building.

You can upload one or more custom images to create a background for the floor plan by clicking "Add New Map."

Figure 106: Adding a Floor Map

1Doc: Protocolo 1.943/2025 | Anexo Administrativo processo licitatório 029_2025_20250227.pdf (102/301) 1805/4726

Use the "Place devices" feature from the Action icons or pull-down menu to set the location of wireless devices on the floor map image.

Figure 107: Configuring a Floor Map

Place devices by dragging an AP from the list on the right side of the page, which contains unplaced devices, to its location on the image. Position the cursor over a device to display information about the device. Click "Show Coverage" to display the area covered by the placed devices.

Figure 108: Placing Devices on Floor Maps

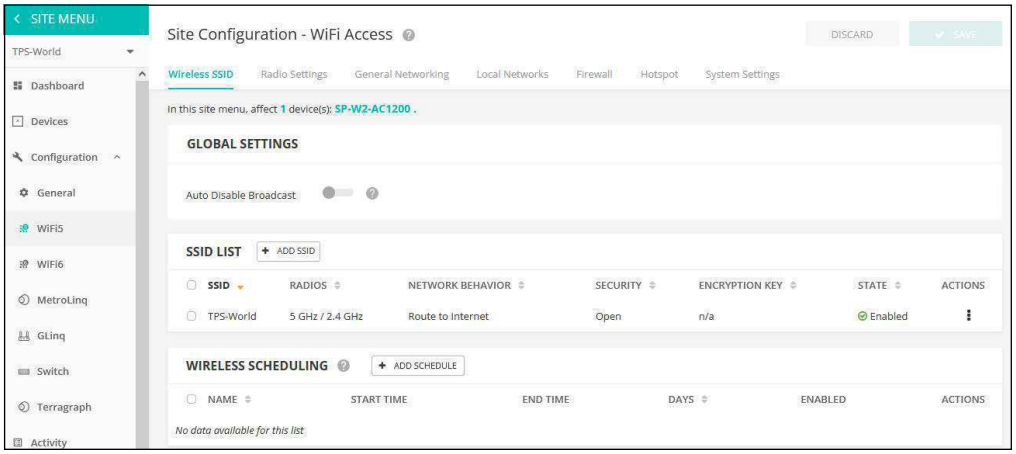
WiFi Configuration

From the Site menu, select "Configuration" and then "WiFi5" or "WiFi6" to configure wireless settings that are inherited by all the site's AP devices and any new devices that are added to the site.

Note: The WiFi5 or WiFi6 configuration does not apply to devices that have their inheritance policy set to "Do not inherit site-level configuration."

Refer to "Site WiFi 5 Configuration" on page 118 for more detailed descriptions of wireless device configuration.

Figure 109: WiFi5 Configuration

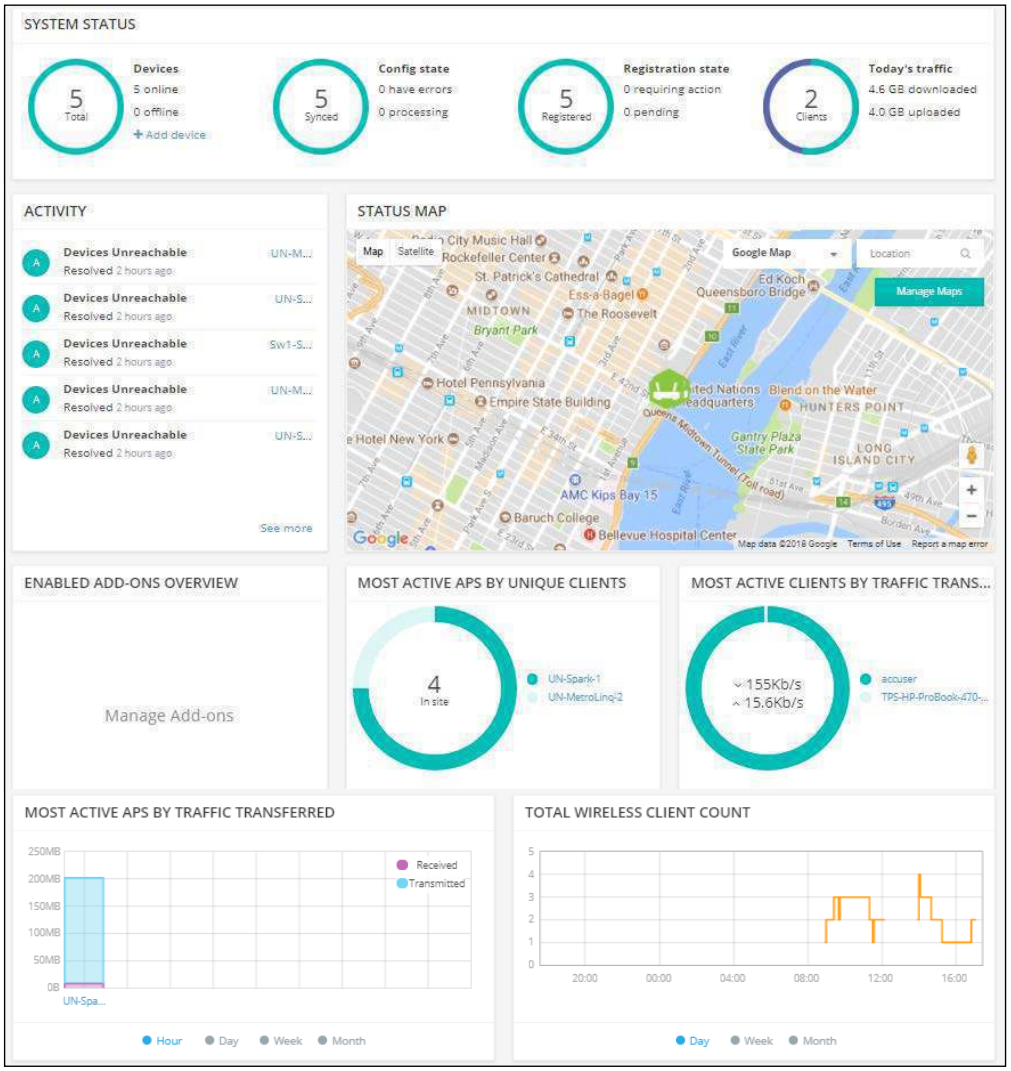


1Doc: Protocolo 1.943/2025 | Anexo Administrativo processo 029_2025_para 27.pdf (104/301) 3609/4746

Displaying the Site Dashboard

The site dashboard provides status information for configured devices, client activity, most active clients, most active clients and application, gateway interface, site maps, and site activity.

Figure 110: Site Dashboard



The following items are displayed on the site dashboard:

- **System Status** — The four circles represent (from left to right): the number of devices (with online/offline counts), the number of devices with synced configurations, and the number of devices registered, and the day's client traffic.

Note: Placing the mouse cursor over the four circles shows additional information.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (105/301) 1838/4726

- **Activity** — Provides a short summary of the most recent device, network and system alerts, and maintenance notifications such as the device being unreachable or rebooted. Clicking on each entry provides further details.
- **Status Map** — Displays the geographical location of this site and the site's devices. Placing the mouse cursor over a device displays a pop up with further device detail.
- **Enabled Add-Ons Overview** — A summary of the currently enabled Add-ons. Clicking in the box opens the Site Add-ons management view.
- **Most Active APs by Unique Clients** — This area shows the APs with single clients showing the most network activity i.e. download and upload traffic transferred. Click on one the APs to go to the APs detailed Dashboard view. Click on the buttons at the bottom to change the measurement window to either 10 minutes, 1 hour, 1 day, or 1 week.
- **Most Active Clients by Traffic Transferred** — This area shows the clients with the most network activity i.e. download and upload traffic transferred in the last 10 minutes. Click on one the clients to go to the clients detailed information view.
- **Most Active APs by Traffic Transferred** — This graph shows the APs with the most network activity i.e. download and upload traffic transferred. Click on the buttons at the bottom to change the measurement window to either 1 hour, 1 day, 1 week or 1 month.
- **Total Wireless Client Count**— This graph shows total clients attached to the cloud within the measurement window. Click on the buttons at the bottom to change the measurement window to either 1 day, 1 week or 1 month.

Creating a Custom Site Dashboard

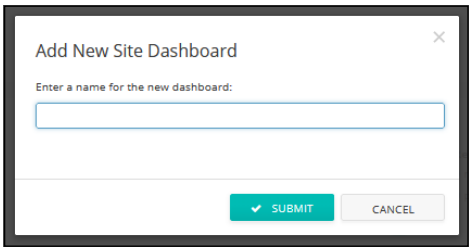
In the default site dashboard, click the plus sign next to the default tab at the top to create a custom dashboard suitable for your requirements.

Figure 111: Adding a Custom Site Dashboard

Enter a name for the new custom dashboard and click SUBMIT.

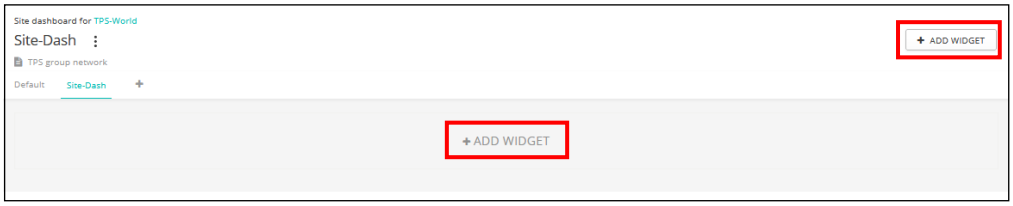
1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (106/301) 3819/4726

Figure 112: Naming a Custom Site Dashboard



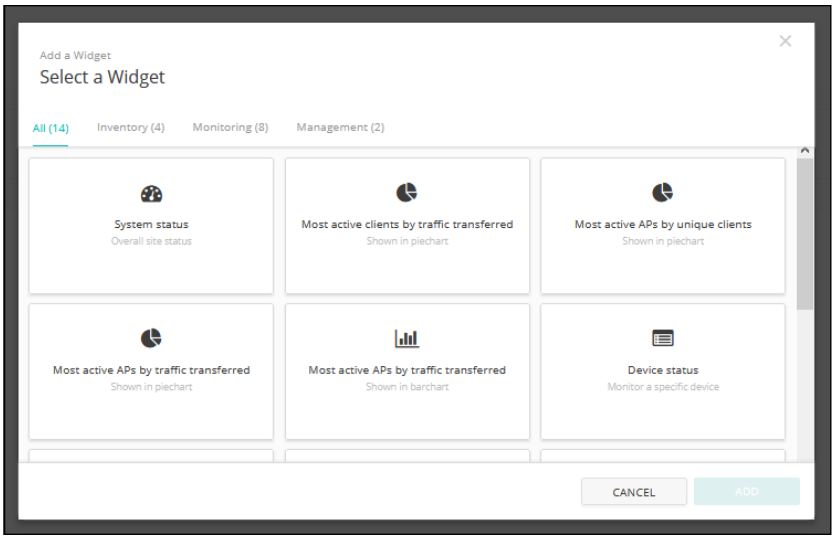
A new tab will appear next to the default dashboard tab with the custom dashboard's name. Click on one of the "+ Add Widget" buttons to add the desired item for the new dashboard.

Figure 113: Adding a Widget to a Custom Site Dashboard



Once a widget is selected click the "ADD" button.

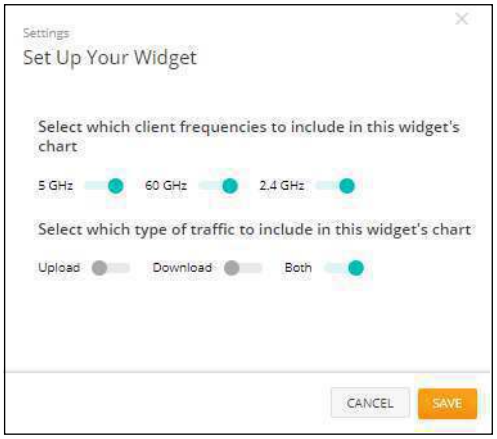
Figure 114: Selecting a Widget for a Custom Site Dashboard



1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (107/301) 3642/4726

For some widgets, custom setup controls are available and these are presented in a new window. Select the desired settings for the widget and then click the "Save" button.

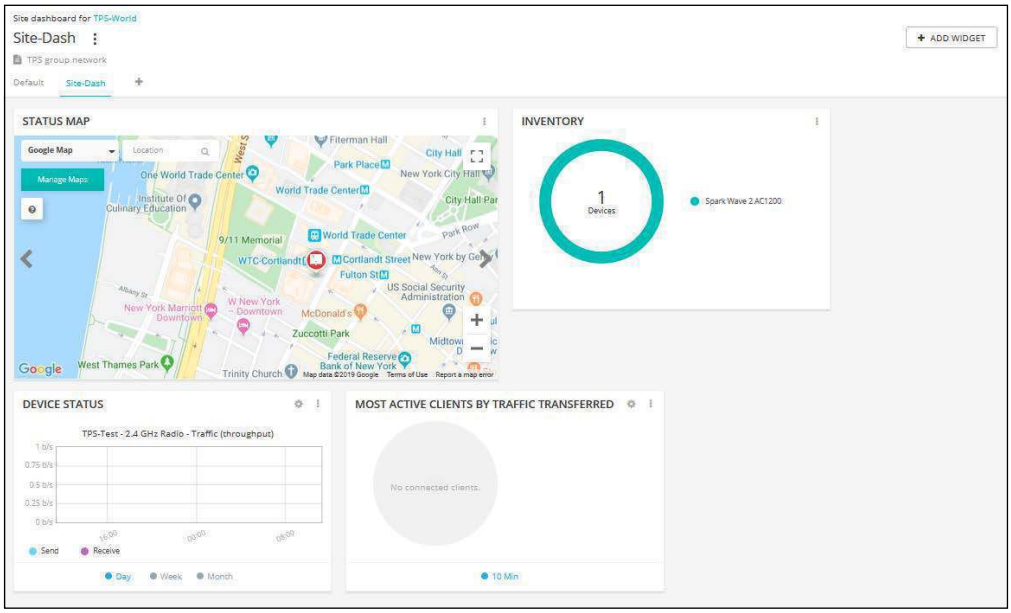
Figure 115: Customizing a New Site Dashboard Widget



Once selected and configured, the widget appears on the new custom dashboard. The widget size can be adjusted by dragging the edges of the widget box. Additionally, widgets can be renamed or removed by clicking the three dot icon in the upper right of the box and the widget settings can be adjusted by clicking the gear icon.

Click the "Add Widget" button again to add additional widgets to the custom dashboard.

Figure 116: Customized Site Dashboard



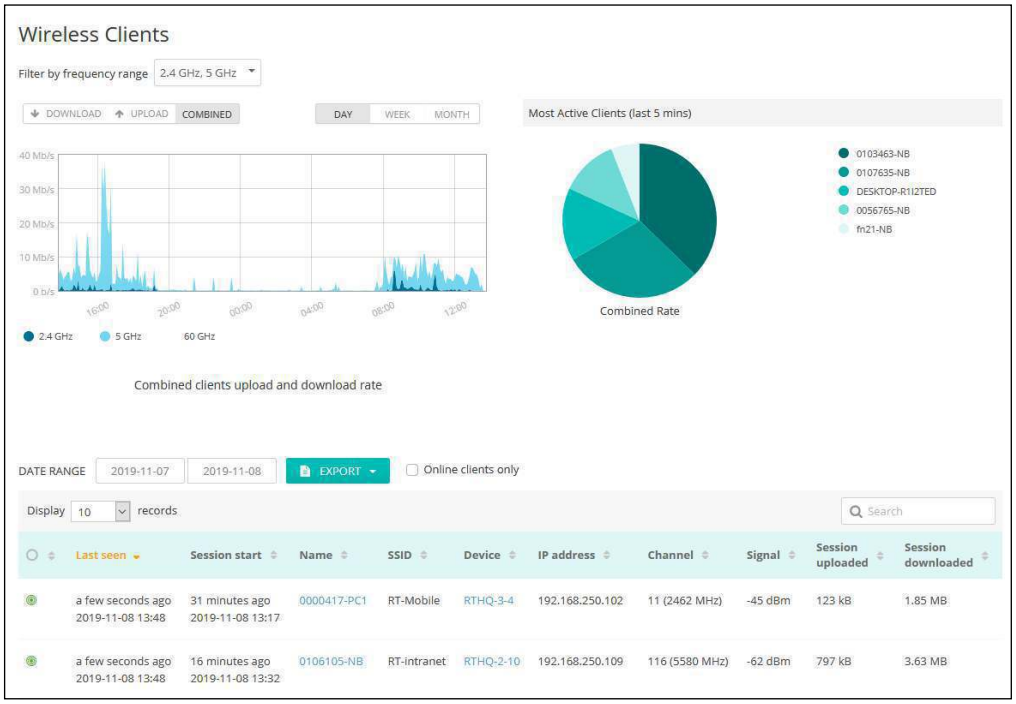
1Doc: Protocolo 1.943/2025 | Anexo Administrativo processo licitatório 029_2025_20250227.pdf (108/301) 3643/4726

Monitoring Wireless APs and Clients

The Wireless Clients page displays a list of wireless clients including their individual client information, associated AP, and network activity. Network activity is shown as combined throughput, most active clients, and sessions logs.

Wireless client data on the page can be filtered by band selection (2.4 GHz, 5 GHz, and 60 GHz) and the data traffic can be viewed based on traffic direction (download or upload) or time range (day, week, month, or by date).

Figure 117: Wireless Clients Page



The following items are displayed on the Wireless Clients page:

- **Filter by frequency range** — Shows or hides data on the page for the 2.4 GHz, 5 GHz, or 60 GHz frequency bands.
- **Download/Upload/Combined** — Selects the traffic throughput to display in the chart; downloaded, uploaded, or both (combined).
- **Day/Week/Month** — Selects the time range for the traffic throughput chart.
- **Most Active Clients** — Shows the most active clients (combined rate) over the last five minutes. To show more detailed information, click on a specific client in the pie chart to open the Client Information page.
- **Date Range** — Sets the date range to display for wireless client data in the session logs.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 6 processo licitatório 029_2025 (109/301) 3642/4726

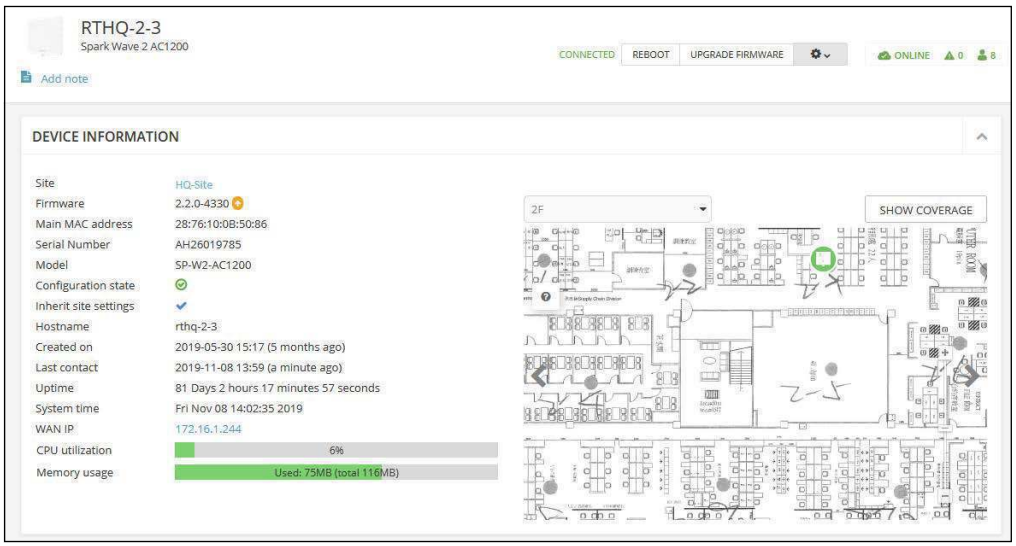
- **Export** — Exports the wireless client information to a CSV excel sheet available from the Activity menu under maintenance.
- **Online clients only** — Restricts the displayed session logs to wireless clients that are currently online.

Session Logs

To sort the session logs, click on the ascending or descending arrows for each column heading.

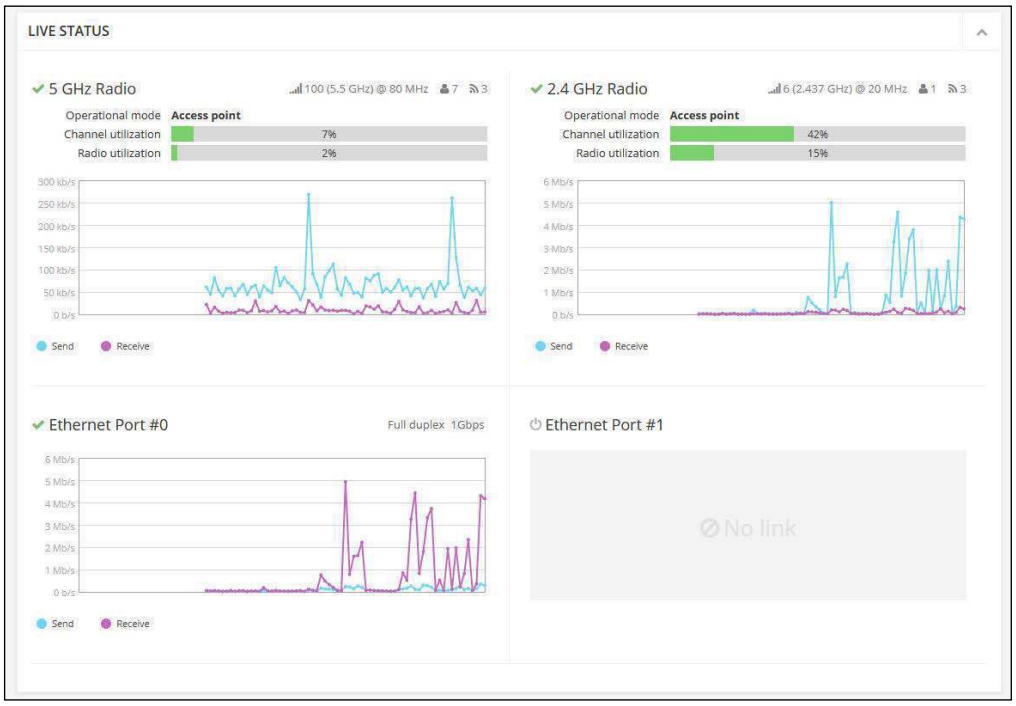
Click on any name in the Device column to open the Device information page for details on a specific AP. The first section of the Device information page includes details about the AP, including a location map.

Figure 118: Wireless AP Information



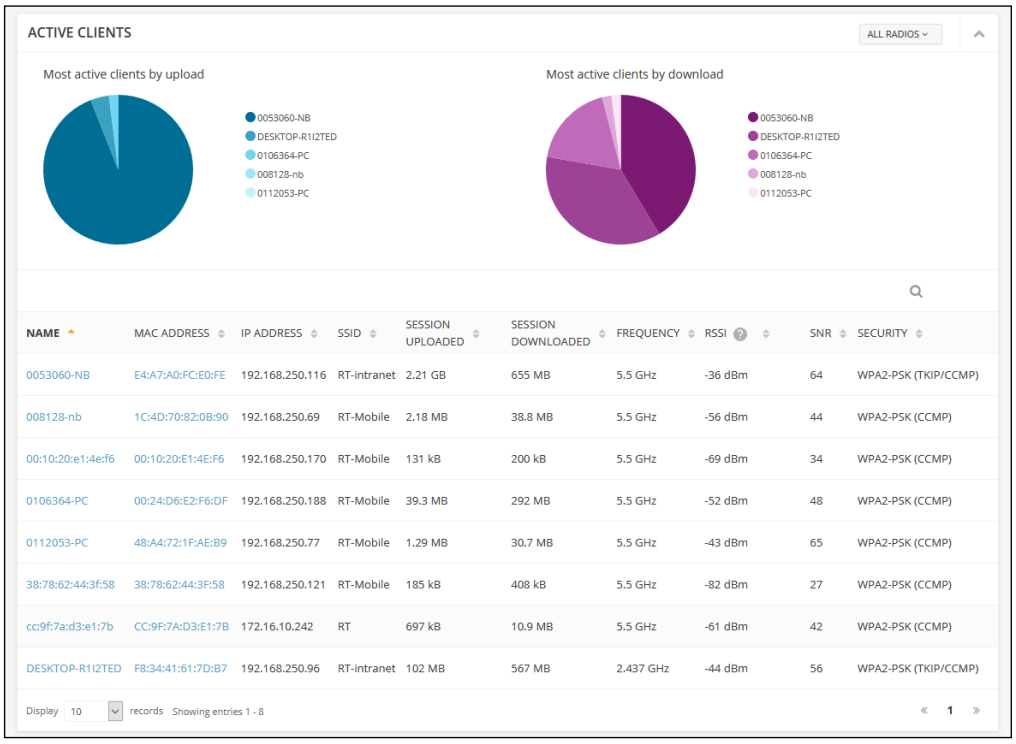
The second section of the Device information page shows throughput and utilization data for radio and Ethernet interfaces on the AP.

Figure 119: Wireless AP Live Status



The third section of the Device information page shows details on wireless clients associated to the AP.

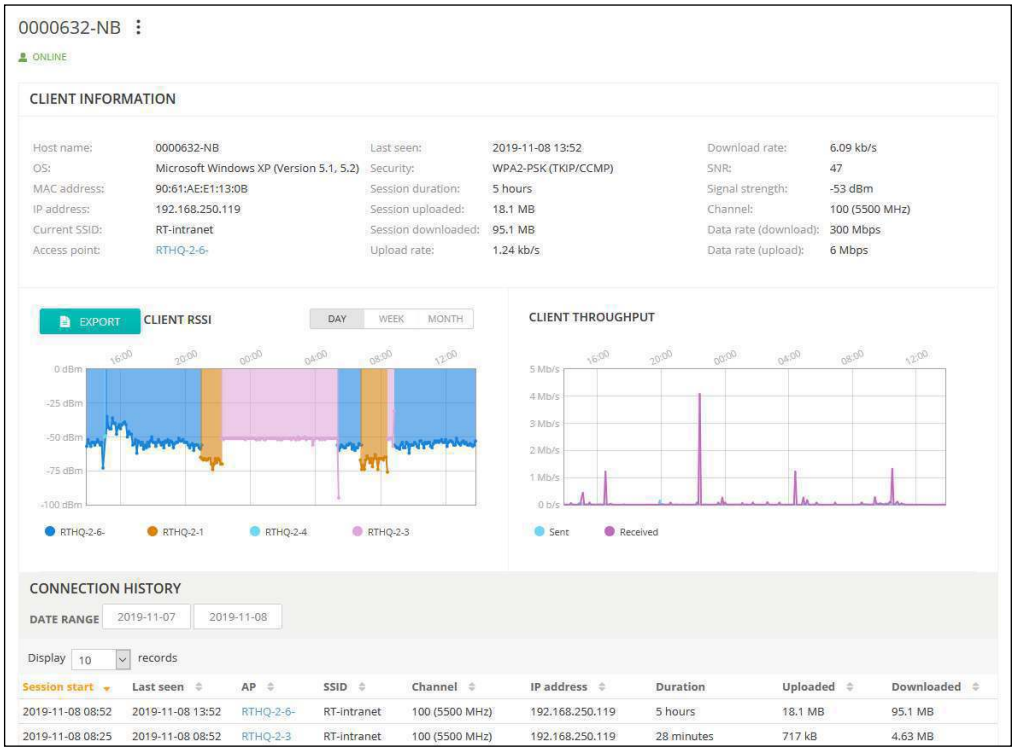
Figure 120: Wireless AP Active Clients



From the wireless client session logs or AP's active client list, click on any of the clients in the Name field to open the Client Information page for details on a specific client.

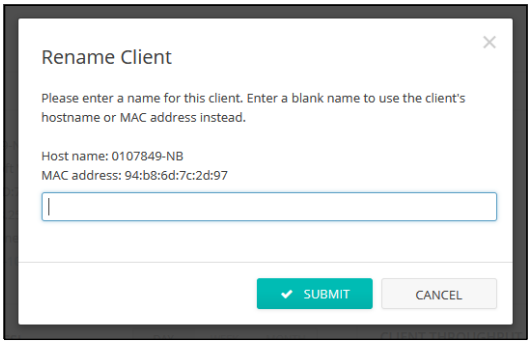
The client information page shows detailed information on the client, signal strength and throughput data, and a list of the client's connection history.

Figure 121: Client Information Page



To rename a client, on the client's information page click on the three-dot icon next to the client name at the top of the page.

Figure 122: Renaming a Wireless Client



To reset a client to its original name, enter a blank in the rename dialog box and click the Submit button.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 5 processo licitatório 029_2025_20250227.pdf (112/301) 3845/4746

Schedule Maintenance Tasks

From the Site menu, click on Devices and then Wireless (or other device type). The "Manage your devices" page will display. Use this page to manage a bulk reboot or upgrade firmware.

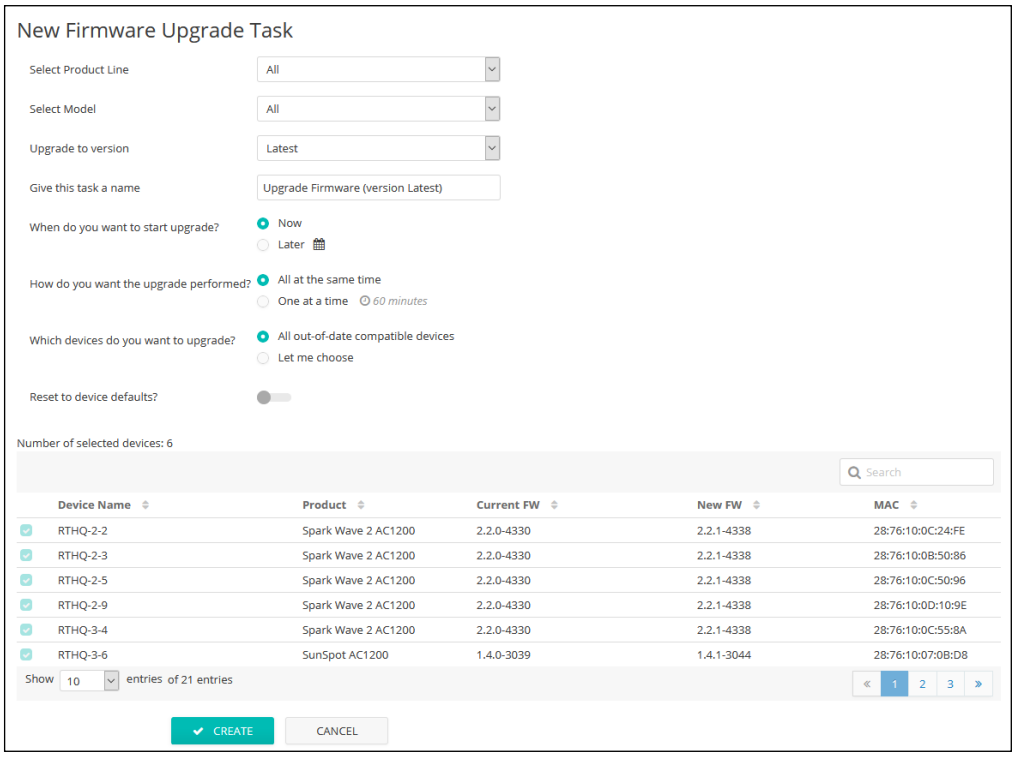
Figure 123: Maintenance Tasks Page

Upgrade Firmware

Click the Upgrade Firmware button to access New Firmware Upgrade Task page.

Select the product line, model number, or leave as "All" to upgrade all devices. You have the option to schedule when upgrades start and which devices will be upgraded. When configuration is complete, give the task a name and click Create.

Figure 124: New Firmware Upgrade Task Page



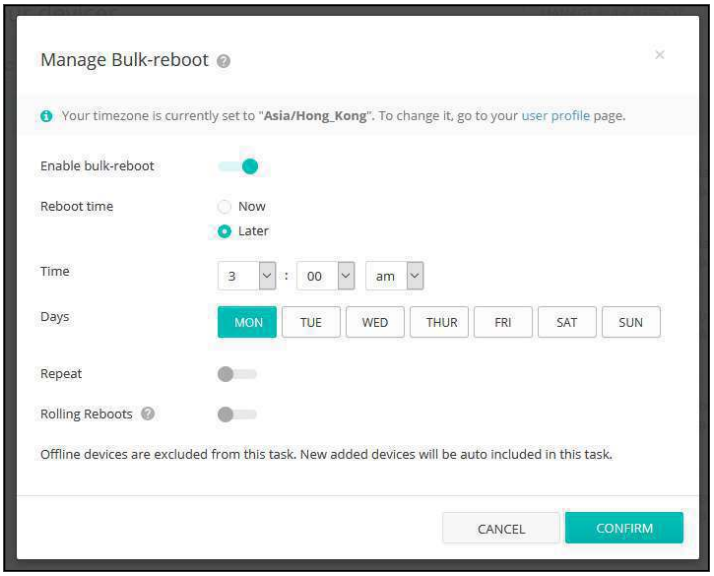
1Doc: Protocolo 1.943/2025 | Anexo Administrativo processo licitatório 029_2025_pdf (113/301) 3848/4726

Bulk Reboot

Click the Manage Bulk-Reboot button to access Bulk-Reboot page. This page enables you to reboot all devices at a site, either at the same time or in a rolling manner. You can also specify a bulk-reboot to repeat at certain times and dates.

The Rolling Reboots option means that devices are rebooted one after the other rather than all at the same time. In the case that a reboot times out for a device, all other reboots after will be canceled.

Figure 125: Manage Bulk-Reboot Page



Site Notifications

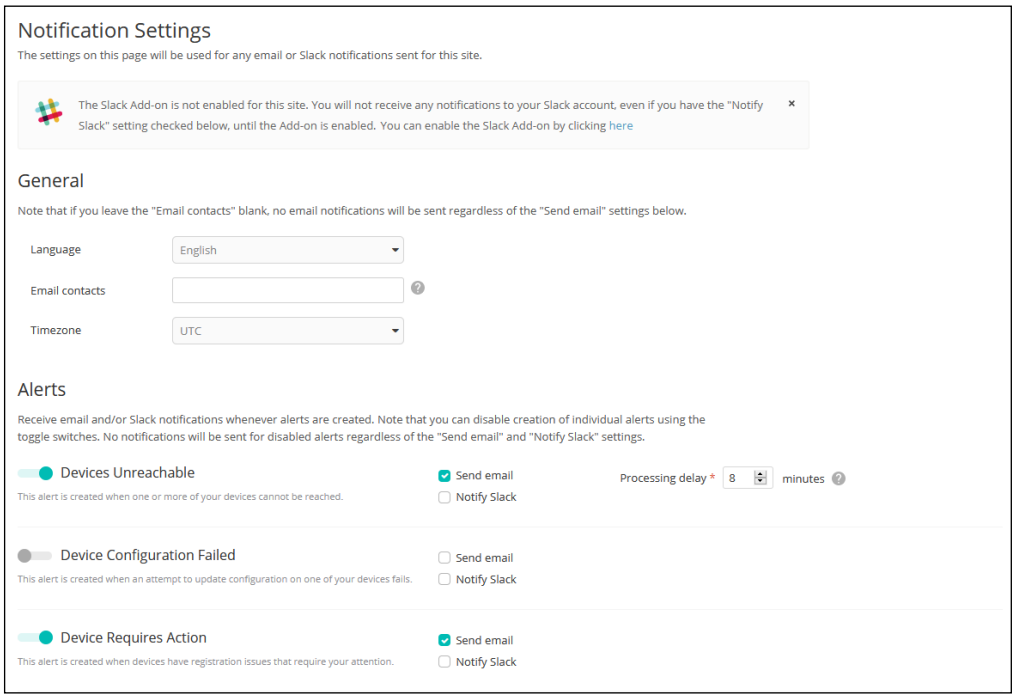
Click “Notifications” on the Site menu to access the notification settings for the selected site. The settings are used for any email or Slack notifications sent for this site.

Note: If the Slack Add-on is not enabled for a site, you will not receive any notifications to your Slack account, even if you have the “Notify Slack” setting enabled. Select ”Add-ons” from the Cloud or Site menu to install the Slack Add-on. See “Add-Ons” on page 74 for more information.

You can disable the creation of individual alerts using the toggle switches on the Notification Settings page. No notifications will be sent for disabled alerts regardless of the “Send email” and “Notify Slack” settings.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (114/301) 1649/4726

Figure 126: Site Notification Settings



The following items are displayed on the Notification Settings page:

- **Language** — The language used for the alert emails.
- **Email Contacts** — This is the list of email addresses that will receive alerts when your devices go offline or require action. Separate multiple email addresses with spaces.

  Note that if you leave the “Email contacts” blank, no email notifications will be sent regardless of the Alert “Send email” settings.
- **Timezone** — Sets the time zone that will be used when sending alert-related emails.

Alerts

- **Devices Unreachable** — This alert is created when one or more of your devices cannot be reached.
- **Processing delay** — An alert for unreachable (offline) devices is created when at least one of your site's devices does not contact the cloud in the given time period. For site-wide outages, this delay allows the system to create a single alert email for a group of offline/unreachable devices. (Default: 8 minutes)
- **Device Configuration Failed** — This alert is created when an attempt to update configuration on one of your devices fails.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (115/301) 38/47

- **Device Requires Action** — This alert is created when devices have registration issues that require your attention.
- **Device Re-registered** — This alert is created when devices automatically re-registers with cloud controller.
- **Device Rebooted** — This alert is created when one or more of your devices reboots.
- **MetroLinq 60 GHz Link is Down** — This alert is created when the 60 GHz link goes down on a MetroLinq (and the 5 GHz failover link is activated if enabled).
- **Time not in sync.** — This alert is created when the time on device not in sync with the cloud.
- **Channel Changed** — This alert is created when a radio on one of your devices switches to a different channel (as a result of a DFS event or otherwise).
- **Streaming Failure** — This alert is created when an attempt to start playing an audio stream on one of your devices fails.
- **Maintenance Task Failure** — This alert is created when a scheduled maintenance task fails on one of your devices.
- **File Sync Error** — This alert is created when an attempt to sync files (e.g. custom Hotspot terms and logo) on one of your devices fails.
- **Firmware Downgraded** — This indicates either manual firmware downgrade or bootbank failure.
- **Firmware Upgraded** — Notifies only about upgrades via device UI. Cloud upgrades are registered as tasks.

Maintenance Tasks

- **Change Config** — Receive notifications when the Cloud pushes configuration to one or more of your devices.
- **Received Config** — Receive notifications when a device pushes its config to the Cloud.
- **Upgrade Firmware** — Receive notifications when the Cloud upgrades firmware on one or more of your devices.
- **Auto Firmware Upgrade** — Receive notifications when the Cloud performs automatic firmware upgrades on your devices.
- **Rolling Firmware Upgrade** — Receive notifications when the Cloud performs rolling firmware upgrades on your devices.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo processo digital (116/301) 3829/4726

- **Troubleshooting** — Receive notifications when Troubleshooting files requested by the Cloud from your devices become available.
- **Packet Capture** — Receive notifications when packet capture files requested by the Cloud from your devices become available.
- **Report** — Receive notifications when reports requested by the Cloud from your devices become available.
- **Reboot** — Receive notifications when the Cloud reboots one or more of your devices.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo processo digital nº 37.808.059/0001-29_2025_Anexo_Administrativo_processo_digital_nº_37.808.059_0001_29_2025_page_27.pdf (117/301) 1850/4746

4 Site WiFi 5 Configuration

This chapter describes configuration settings for WiFi 5 access point devices. It includes the following sections:

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - Termo de Referência_processo_licitatorio_029_2025_pdf (118/301) 1853/4746

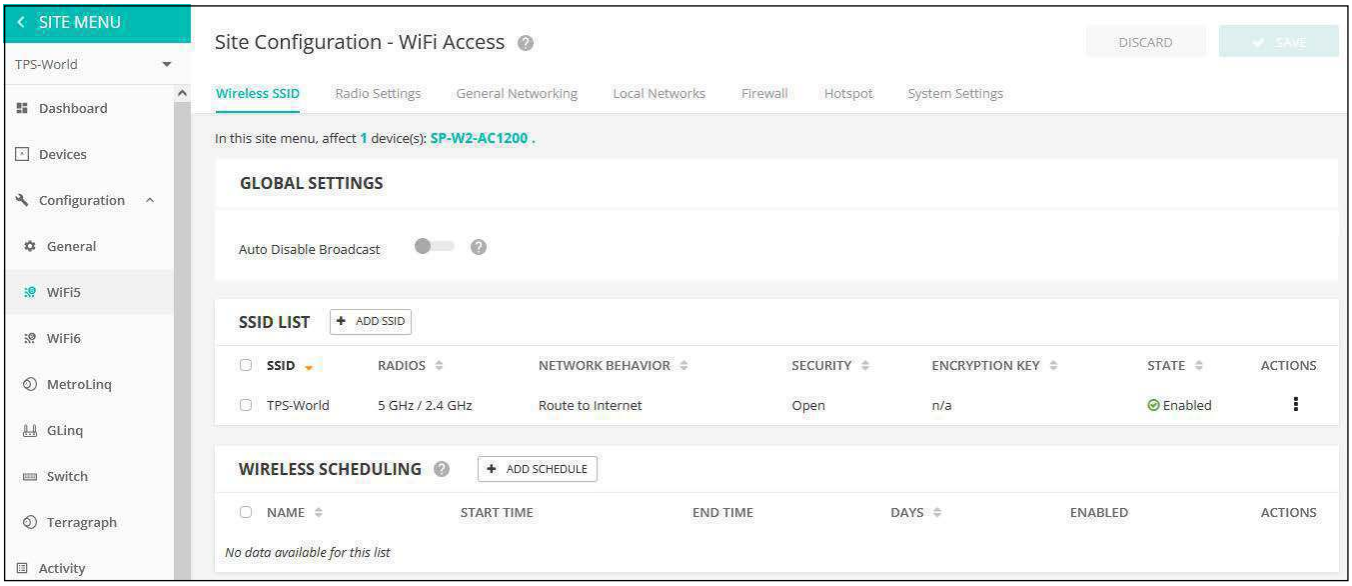
Wireless SSID Configuration

From the Site menu, open "Configuration" and then "WiFi5" to display the configuration options that apply to all Edgecore Wi-Fi 5 access points in the same site.

The Edgecore Wi-Fi 5 access points can operate in several radio modes, 802.11a/a+n/ac+a+n (5 GHz) or 802.11b+g/b+g+n (2.4 GHz). Supported modes depend on the access point model. Note that the dual-band access points can operate at 2.4 GHz and 5 GHz at the same time.

Each radio supports eight Service Set Identification (SSID) or virtual access point (VAP) interfaces. Each VAP functions as a separate access point, and can be configured with its own SSID and security settings. However, most radio signal parameters apply to all VAP interfaces. Traffic to specific VAPs can be segregated based on user groups or application traffic. Wireless clients associate with each VAP in the same way as they would with separate physical access points. Edgecore AP devices support up to a total of 128 wireless clients across all SSID interfaces per radio.

Figure 127: Site WiFi5 Configuration



The Wireless SSID tab on the WiFi5 configuration page includes these items:

- **Global Settings** — Configuration that applies to all SSID interfaces.
  - **Auto Disable Broadcast** — Automatically disables SSID broadcasts when a Wi-Fi device cannot connect to the cloud. (Default: Disabled)
- **SSID List** — The list of configured SSID interfaces for the Wi-Fi devices in this site. Note that each SSID applies to both the 2.4 GHz and 5 GHz radios unless

1Doc: Protocolo 1.943/2025 | Anexo Administrativo Processo Licitatório 029_2025_pdf (119/301) 1852/4726

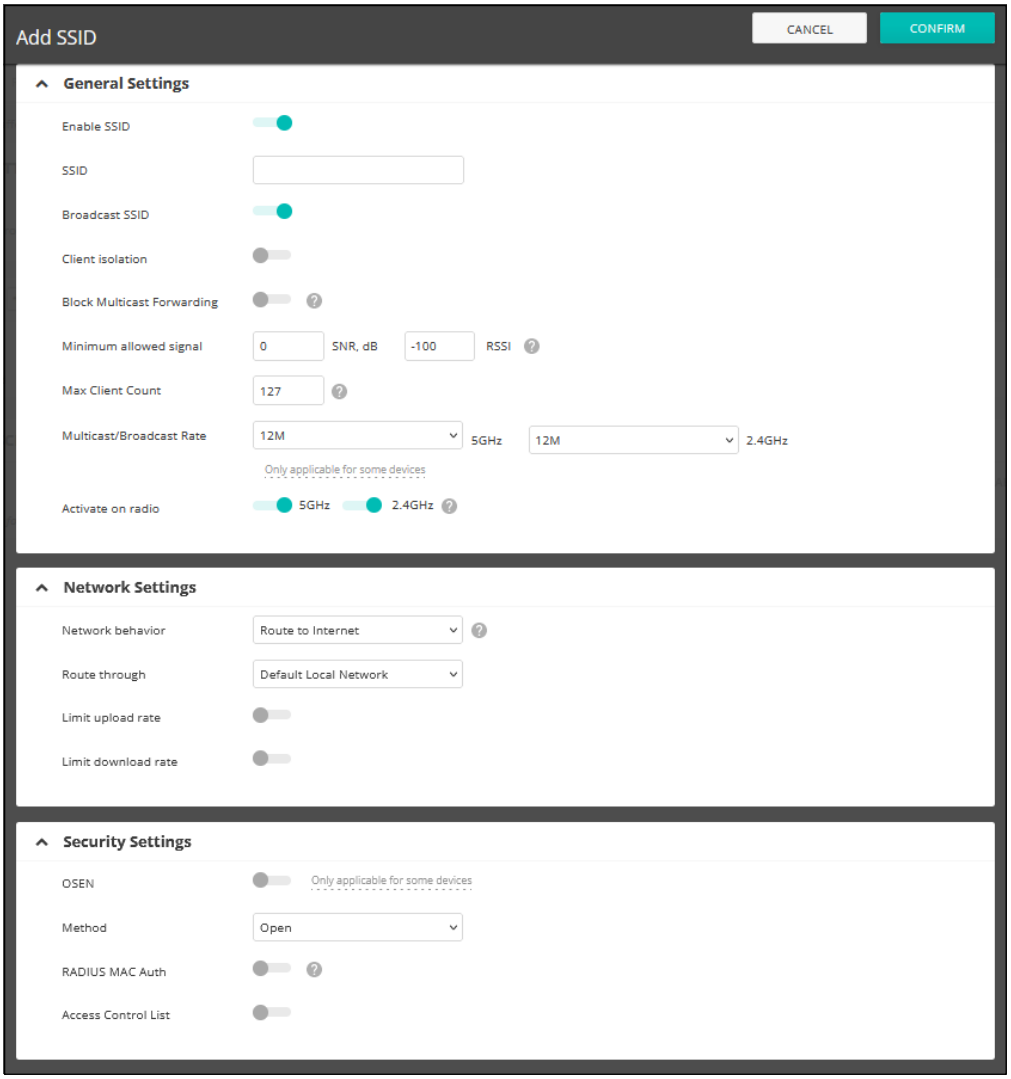
otherwise configured. You can configure a maximum of eight SSIDs. Click the "Add SSID" button to create an SSID interface.

- **Wireless Scheduling** — A list of configured schedules for turning AP radios on and off at specified times. The scheduling rules apply to all 2.4 GHz and 5 GHz interfaces on all site APs. Click the "Add Schedule" button to create a wireless schedule.

Adding an SSID

Click the Add SSID button on the WiFi Access configuration page and enter SSID, network, and security settings as displayed below.

Figure 128: Radio Settings (New SSID)



The following items are displayed on the Add SSID page:

General Settings

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (120/301) 1825/4746

- **Enable SSID** — Enables or disables the SSID interface.

- **SSID** — The name of the basic service set provided by the VAP interface. Clients that want to connect to the network through the access point must set their SSID to the same as that of the access point's VAP interface. (Range: 1-32 characters)

- **Broadcast SSID** — The SSID can be broadcast at regular intervals so that wireless stations searching for a network connection can discover it. This allows wireless clients to dynamically discover and roam between WLANs. This feature also makes it easier for hackers to break into your home network. Because SSIDs are not encrypted, it is easy to scan WLANs looking for SSID broadcast messages coming from an AP. (Default: On)

- **Client Isolation** — When enabled, wireless clients can talk to the LAN, and reach the Internet if such connection is available, but they cannot communicate with one another. (Default Off)

- **Block Multicast Forwarding** — Stops multicast traffic from being forwarded to wireless clients connected to the SSID. (Default Off)

- **Minimum allowed Signal** — Only allows clients to associate to this SSID if their signal strength (RSSI) is equal or greater than the specified value. Setting the value to -100 disables this feature. Clients already connected are checked periodically.

  This forces clients to associate with an AP that has a better signal strength (also called assisted roaming). Suggested value is -70 to -80 depending on access point density and coverage.

  Enter an RSSI (Received Signal Strength Indicator) in decibels from -1 to -100db. Note that the closer it is to zero, the stronger the signal. (Default: -70)

- **Max Client Count** — Sets the maximum number of wireless clients that can be connected to this SSID at the same time. (Default: 127; Range: 0 to 127)

- **Multicast/Broadcast Rate** — Allows a limit to be placed on the wireless bandwidth consumed by multicast and broadcast packets.

  - **Radio 5 Ghz** — Options: 6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M; Default: 6M

  - **Radio 2.4 Ghz** — Options: 5.5M, 6M, 9M, 11M, 12M, 18M, 24M, 36M, 48M, 54M; Default: 5.5M

- **Activate on radio** — Selects the radios on which this SSID should be created. If an SSID is activated on both radios for a device (meaning that the SSID will be mirrored), you can edit its record from either configuration tab, and the changes will be made on both the 2.4 GHz and 5 GHz SSID records. (Default: 5GHz and 2.4GHz enabled)

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (121/301) 1836/4746

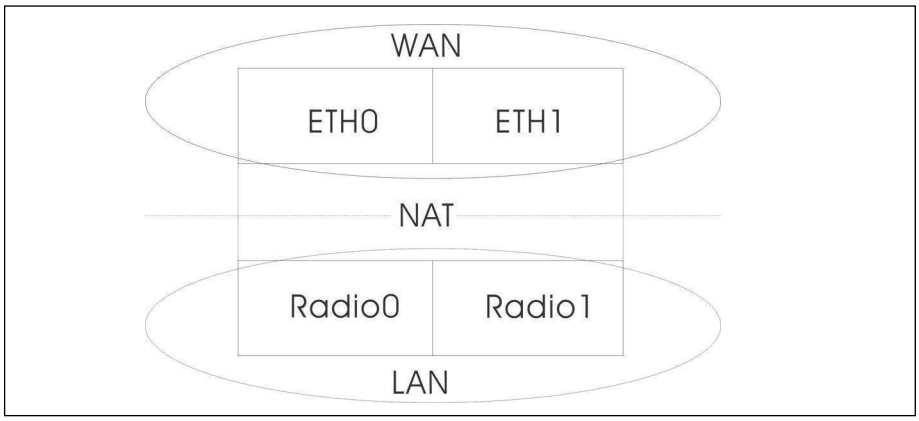
Network Settings

- **Network Behavior** — One of the following connection methods must be specified. (Default: Route to Internet)

  - **Bridge to Internet (AP Bridge Mode)** — Configures an interface as attached to the WAN (that is, the Internet).

    In the following figure, Ethernet port 0 and Ethernet port 1 are both attached to the WAN. Traffic from these interfaces is directly bridged into the Internet. Any of the Ethernet or radio interfaces can be configured this way.

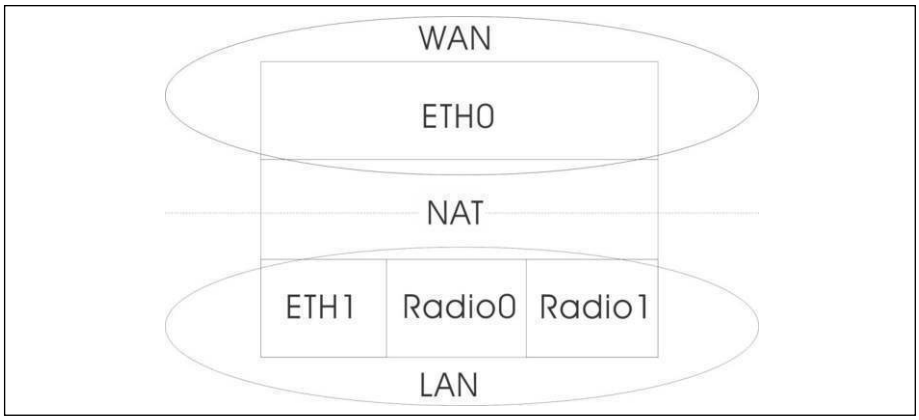
Figure 129: Bridge to Internet



  - **Route to Internet (AP Router Mode)** — Configures an interface as a member of the LAN.

    In the following figure, Ethernet port 1, Wireless LAN 0 (5 GHz radio), and Wireless LAN 1 (2.4 GHz radio) are all included in the LAN. Traffic from these interfaces is routed across the access point through Ethernet port 0 to the Internet.

Figure 130: Route to Internet



1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - Termo de Referência_procesSoDigitalizado_029_20250226227.pdf (122/301) 1837/4746

- **Route through** — The network to be routed. The default is "Default local network" as displayed under LAN Settings – Local Network.

- **Add to Guest Network** — This interface can only support the guest network.

- **Hotspot Controlled** — This interface can only support hotspot services.

  - **Walled garden** — Enter a list of domains and/or IP addresses in CIDR notation that the hotspot user can access before being authenticated by the captive portal. Wildcard domains can be specified in the format of *domain.com* (allow domain and all of its subdomains), or *.domain.com* (only allow subdomains).

- **VLAN Tag Traffic** — Tags any packets passing from this SSID interface to the associated Ethernet port as configured under "VLAN Settings" on page 135. When enabled, select a configured VLAN ID from the list.

Note: ecCLOUD supports VLAN synchronization between APs and switches. When VLAN tagging is enabled for an SSID, the configured VLAN ID is automatically "pushed" by ecCLOUD to the attached switch port. This enables the VLAN-tagged traffic from the AP to be accepted by the switch port and avoids any loss of connectivity.

- **Limit upload rate** — Enables rate limiting of traffic from the SSID interface as it is passed to the wired network. You can set a maximum rate in Kbytes per second. (Range: 256-10048576 Kbytes per second; Default: OFF)

- **Limit download rate** — Enables rate limiting of traffic from the wired network as it is passed to the SSID interface. You can set a maximum rate in Kbytes per second. (Range: 256-10048576 Kbytes per second; Default: OFF)

Security Settings

- **OSEN** — Enable this option for OSU Server-Only Authenticated L2 Encryption Network.

- **Method** — Sets the wireless security method for each SSID, including association mode, encryption, and authentication. (Default: Open)

  - **Open** — The SSID interface broadcasts a beacon signal including the configured SSID. Wireless clients with an SSID setting of "any" can read the SSID from the beacon and automatically set their SSID to allow immediate connection.

  - **WPA-PSK** — For enterprise deployment, WPA requires a RADIUS authentication server to be configured on the wired network. However, for small office networks that may not have the resources to configure and maintain a RADIUS server, WPA provides a simple operating mode that

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (123/301) 1838/4746

uses just a pre-shared password for network access. The Pre-Shared Key mode uses a common password for user authentication that is manually entered on the access point and all wireless clients. The PSK mode uses the same TKIP packet encryption and key management as WPA in the enterprise, providing a robust and manageable alternative for small networks.

- **Encryption** — Data encryption uses one of the following methods:
  - **AES** — AES-CCMP is used as the multicast encryption cipher. AES-CCMP is the standard encryption cipher required for WPA2. (This is the default setting.)
  - **TKIP + AES** — The encryption method used by the client is discovered by the access point.
- **Key** — WPA is used to encrypt data transmitted between wireless clients and the SSID interface. WPA uses static shared keys (fixed-length hexadecimal or alphanumeric strings) that are manually distributed to all clients that want to use the network.

  String length must be 8 to 63 ASCII characters (letters and numbers). No special characters are allowed.
- **Dynamic Keys** — Enables the use of dynamic PSK keys that are periodically generated and updated by a RADIUS authentication server. The RADIUS server IP address, UDP port, and secret text string must be specified.

  Dynamic keys are supported only for WPA2-PSK security.

- **WPA2-PSK** — Clients using WPA2 with a Pre-shared Key are accepted for authentication.

  WPA was introduced as an interim solution for the vulnerability of WEP pending the ratification of the IEEE 802.11i wireless security standard. In effect, the WPA security features are a subset of the 802.11i standard. WPA2 includes the now ratified 802.11i standard, but also offers backward compatibility with WPA. Therefore, WPA2 includes the same 802.1X and PSK modes of operation and support for TKIP encryption.

  Refer to WPA-PSK for a description of encryption methods and the key.

- **WPA-EAP** — WPA employs a combination of several technologies to provide an enhanced security solution for 802.11 wireless networks. A RADIUS server is used for authentication, and can also be used for accounting.

  Refer to WPA-PSK for a description of encryption methods.

  RADIUS Settings

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_procesoDistancia_2025_pdf (124/301) 1839/4746

A RADIUS server must be specified for the access point to implement IEEE 802.1X network access control and Wi-Fi Protected Access (WPA) wireless security.

In addition, you can configure a RADIUS Accounting server to receive user-session accounting information from the access point. RADIUS Accounting can be used to provide valuable information on user activity in the network.

Note: This guide assumes that you have already configured RADIUS servers) to support the access point. Configuration of RADIUS server software is beyond the scope of this guide, refer to the documentation provided with the RADIUS server software.

- **802.11r** — Enables 802.11r fast roaming on the SSID interface. This feature is only supported on AC Wave 2 devices (Sunspot Wave2, Spark Wave2) running 2.2.0+ firmware. (Default: Disabled)
- **Mobility Domain** — The ID number that identifies the 802.11r domain in which the AP operates. (Range: 1-65535)
- **Encryption Key** — The pre-shared key for fast roaming. This key must be exactly 16 characters long and only contain characters A-Z, a-z, 0-9, space, and ~!@$%^*()_+-=[]{}|:;<>?,./
- **Transition over the DS** — Enables support for fast transitions over a wireless distribution system (WDS) network.
- **MAC NASID list** — Enter one MAC address and NAS ID per line. Example: 00:12:34:56:78:9a a00123456789
- **Radius MAC Auth** — Use RADIUS authentication. When this setting is enabled, the AP will send the MAC address of the client device to the specified RADIUS server for authentication. The server verifies the MAC is a valid user, and then replies to the AP with the dynamic VLAN ID (if configured) and other resources for the client device.

  Note: On your RADIUS server, both the user ID and password will need to be set to the WiFi MAC of the client device and must be formatted without punctuation.

  This feature is supported with “Open Security” in v1.1.1 firmware, and all other security methods (besides WEP) in v1.1.2 firmware.
- **Use RADIUS Auth** — For WPA-EAP and WPA2-EAP security, a RADIUS server must be specified.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - Termo de Referência_processo_licitatorio_029_2025_pdf (125/301) 1650/4726

- **RADIUS Auth Server** — Specifies the IP address or host name of the RADIUS authentication server.
- **RADIUS Auth Port** — The UDP port number used by the RADIUS server for authentication messages. (Range: 1024-65535; Default: 1812)
- **RADIUS Auth Secret** — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS authentication server. Do not use blank spaces in the string. (Maximum length: 255 characters)
- **NAS ID** — The RADIUS NAS identifier for the SSID interface. A NAS ID can be used instead of an IP address to identify a client to a server.
- **Backup RADIUS Auth** — Configures a secondary RADIUS server to act as a backup should the primary server become unavailable.
- **Use RADIUS Accounting** — Use RADIUS accounting to enable accounting of requested services for billing or security purposes.
- **RADIUS Acct Server** — Specifies the IP address or host name of the RADIUS accounting server.
- **Radius Acct Port** — The UDP port number used by the RADIUS server for accounting messages. (Range: 1024-65535; Default: 1813)
- **RADIUS Acct Secret** — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS accounting server. Do not use blank spaces in the string. (Maximum length: 255 characters)

- **WPA2-EAP** — WPA was introduced as an interim solution for the vulnerability of WEP pending the ratification of the IEEE 802.11i wireless security standard. In effect, the WPA security features are a subset of the 802.11i standard. WPA2 includes the now ratified 802.11i standard, but also offers backward compatibility with WPA. Therefore, WPA2 includes the same 802.1X and PSK modes of operation and support for TKIP encryption.

  A RADIUS server is used for authentication, and can also be used to accounting.

  Refer to WPA-PSK for a description of encryption methods.

  Refer to WPA-EAP for information on configuring the RADIUS server.

- **Access Control List** — Wireless clients can be authenticated for network access by checking their MAC address against the local database configured on the access point. (Default: OFF)

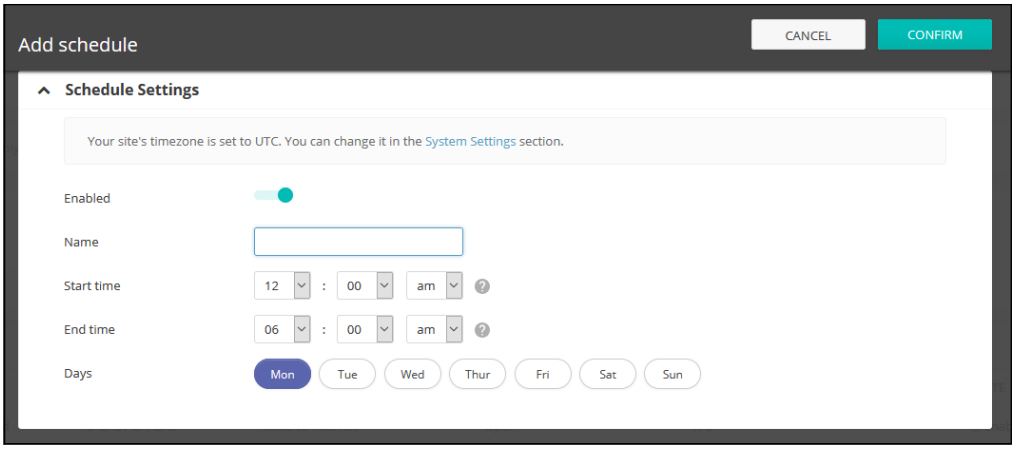
1Doc: Protocolo 1.943/2025 | Anexo Administrativo_procesoDistancia_2025_2026_27.pdf (126/301) 1659/4746

- **Dynamic Authorization** — The Dynamic Authorization Extensions (DAE) to RADIUS enable a server to disconnect or change the authorization of clients that are already connected to the network.
  - **DAE Port** — The UDP port number to use for DAE messages. (Default: 3799)
  - **DAE Client** — The IPv4 address of the RADIUS server.
  - **DAE Secret** — The shared text string used to encrypt DAE messages between the access point and the RADIUS server.

Setting Wireless Schedules

Configuring wireless schedules enables the AP radios to be turned on and off at specified times. The scheduling rules apply to all 2.4 GHz and 5 GHz interfaces on all site APs. Click the "Add Schedule" button to create a wireless schedule.

Figure 131: Adding a Wireless Schedule



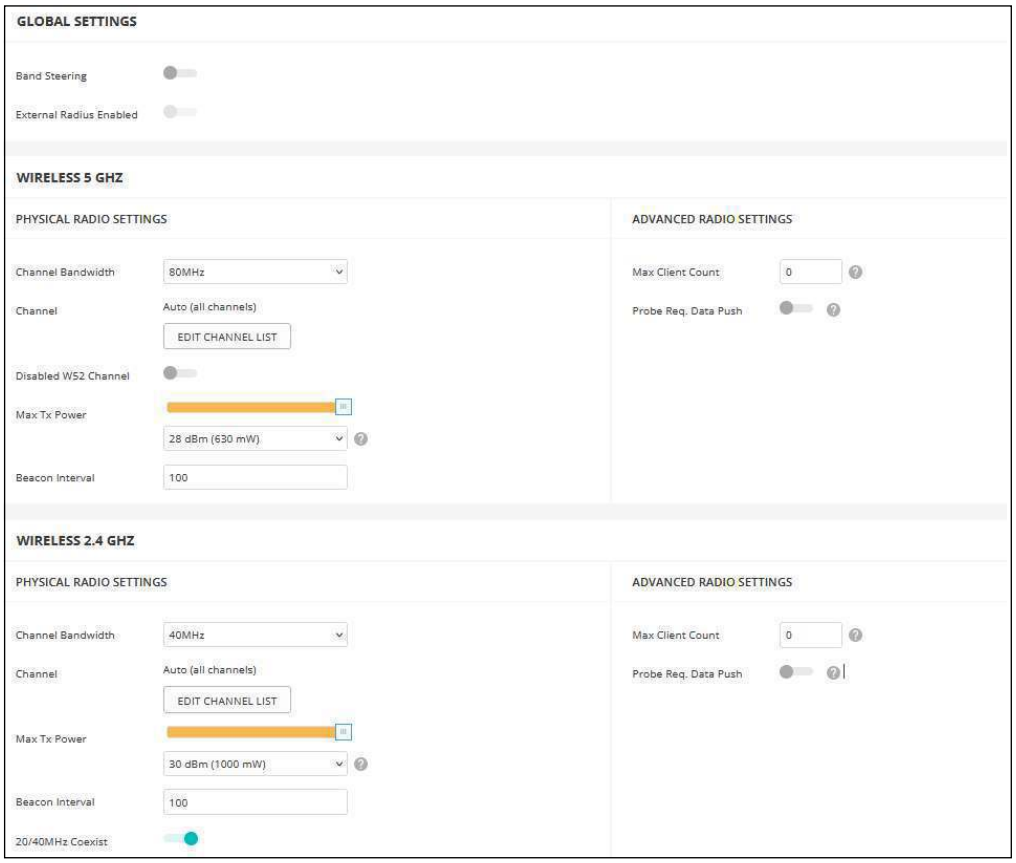
The following items are displayed on the Add schedule page:

- **Enabled** — Makes the defined schedule active. (Default: Enabled)
- **Name** — A text string to identify the schedule.
- **Start time** — The time that you want the radios to be turned on.
- **End Time** — The time that you want the radios to be turned off.
- **Days** — The selected days of the week on which to apply the schedule.

Radio Settings

On the "WiFi Access" page, click the "Radio Settings" tab to configure 5 GHz and 2.4 GHz radio settings. Note that settings apply to all configured SSID interfaces.

Figure 132: WiFi 5 Radio Settings



The following items are displayed on the Radio Settings tab. Note that configuration options apply to both the 5 GHz and 2.4 GHz radios unless otherwise indicated.

Global Settings

- **Band Steering** — When enabled, clients that support 2.4 GHz and 5 GHz are first connected to the 5 GHz radio. This feature helps balance the client load over the two radio bands. Note that both radios must have configured SSIDs that match for this feature to fully operate. (Default: Disabled)

- **External Radius Enabled** — This is an AuthPort add-on feature (see "Using the AuthPort Add-On" on page 75). When using the AuthPort add-on, you can configure settings for an external RADIUS server.

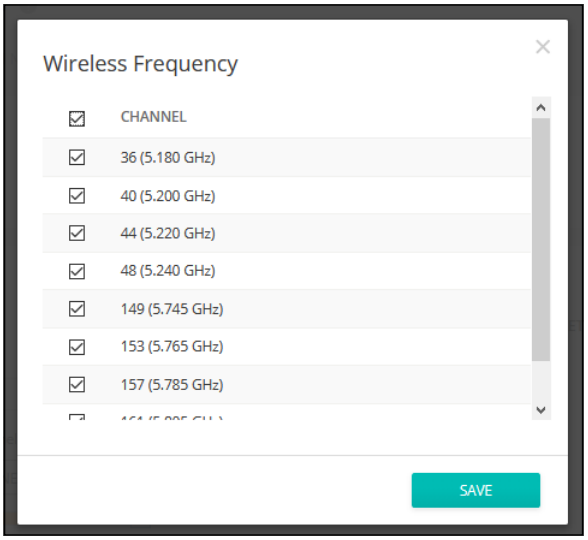
1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - Termo de Referência - Processo Licitatório 029_2025_Pregão 027.pdf (128/301) 1863/4746

Physical Radio Settings

- **Channel Bandwidth** — The basic Wi-Fi channel bandwidth is 20 MHz, but by bonding channels together to create 40 MHz or 80 MHz channels, higher data transmission rate can be achieved. However, selecting larger channel bandwidths reduces the number a radio channels available.
  - **5 GHz Radio** — Options include 20, 40, and 80 MHz. (Default: 80 MHz)
  - **2.4 GHz Radio** — Options include 20 and 40 MHz. (Default: 40 MHz)
- **Channel** — The radio channel that the access point uses to communicate with wireless clients. The available channels are dependent on the radio, Channel Bandwidth, and Regulatory Country settings. You can also click the "Edit Channel List" button to select specific available channels to use for each radio interface.

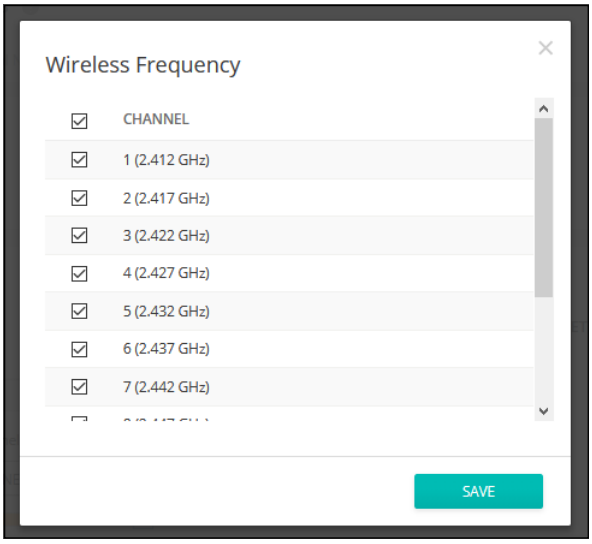
  Selecting Auto enables the access point to automatically select an unoccupied radio channel. (Default: Auto)

Figure 133: 5 GHz Radio Channels



1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pagina_227.pdf (129/301) 1662/4746

Figure 134: 2.4 GHz Radio Channels



- **Disabled W52 Channel** — Applies only to the 5 GHz radio. This feature is designed for Spark AC Wave2 Mini APs with software version v2.3.1 or newer. When enabled, this feature disables channels 36-48 automatically.

- **Max Tx Power** — Adjusts the maximum power of the radio signals transmitted from the access point. The higher the transmission power, the farther the transmission range. Power selection is not just a trade-off between coverage area and maximum supported clients. You also have to ensure that high-power signals do not interfere with the operation of other radio devices in the service area. (The range of power settings and defaults are dependent on the AP model and the Regulatory Country setting.)

- **Beacon Interval** — The rate at which beacon signals are transmitted from the access point. The beacon signals allow wireless clients to maintain contact with the access point. They also carry power-management and other information. (Range: 100-1024 TUs; Default: 100 TUs)

- **20/40MHz Coexist** — Applies only to the 2.4 GHz radio. This option allows 802.11n 20 MHz and 40 MHz channel bandwidths to operate together in the same network. (Default: On)

Advanced Radio Settings

- **Max Client Count** — Sets the max number of clients that are allowed to connect to this radio. To disable this feature, set the value to 0. (Range: 0-64; Default: 0)

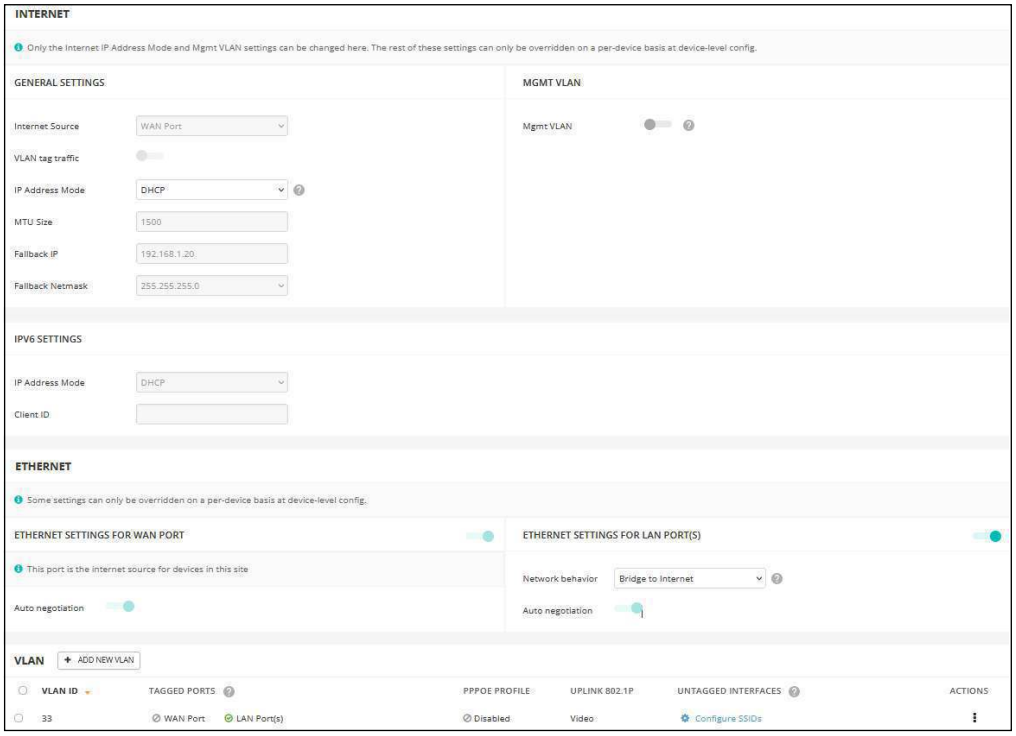
- **Probe Req. Data Push** — Enable Client Probe Request Data Push for this radio. When enabled, the radio will push client probe request data in JSON format to your specified URL.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (130/301) 1665/4726

General Networking Settings

On the "WiFi Access" page, click the "General Networking" tab to configure Internet, Ethernet ports, and VLAN settings for all devices in a site. Some items on this page only display the current setting, they cannot be configured. These settings can only be overridden at the device-level configuration.

Figure 135: General Networking Settings

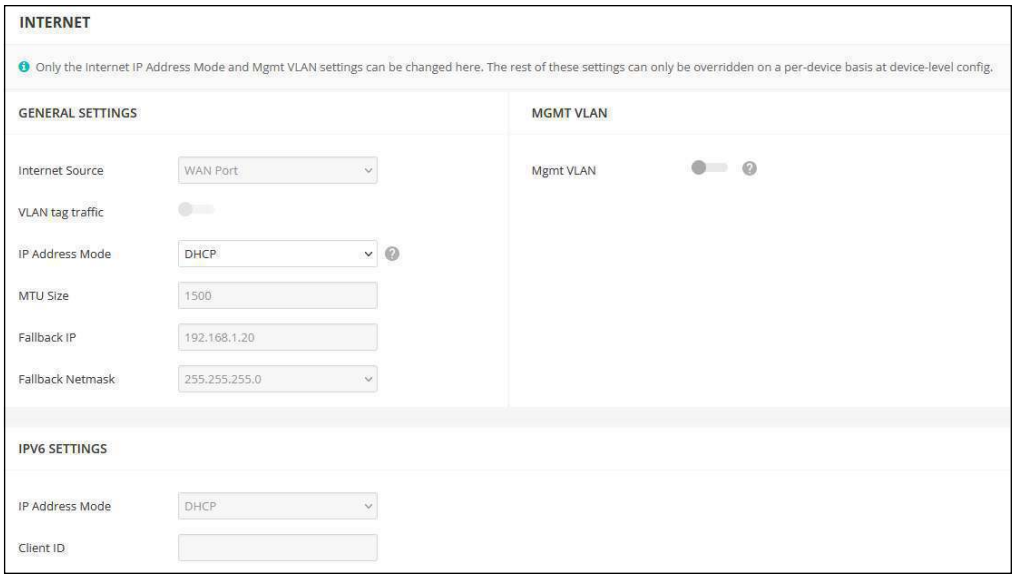


1Doc: Protocolo 1.943/2025 | Anexo Administrativo processo 029.2025 (131/301) 1866/4726

Internet Settings

Note that only the Internet IP Address Mode and Management VLAN settings can be changed on this page. These rest of these settings can only be overridden on a per-device basis at device-level configuration.

Figure 136: Internet Settings



The following items are displayed on this page section:

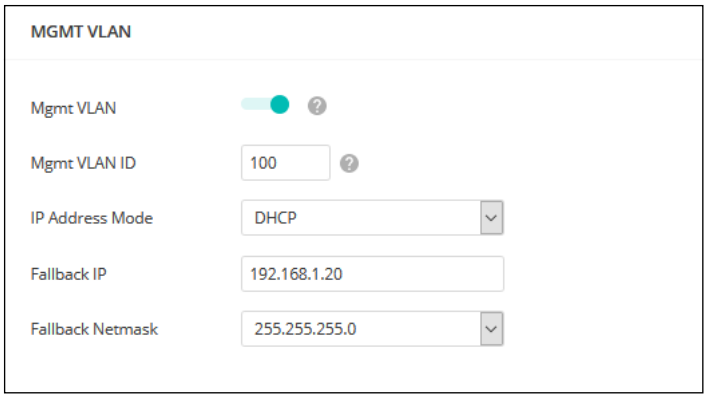
General Settings

- **Internet Source** — The interface on devices used to access the Internet.
- **VLAN tag traffic** — Enable to activate tagging on this interface and choose a tagging ID value between 2 and 4094, inclusive.
- **IP Address Mode** — The method used to provide an IP address for the Internet access port. (Options: DHCP, Use Device's Settings; Default: DHCP)
  - **DHCP** — Enables DHCP on the Internet Source interface.
  - **Use Device's Settings** — Select this option if you plan on assigning static IPs to your devices prior to registration. Also choose this option if you are mixing static IP and DHCP-based modes. By default, all devices will use DHCP unless configured otherwise.
- **MTU Size** — Sets the size of the maximum transmission unit (MTU) for packets sent on this network.
- **Fallback IP** — This IP address is used if you cannot connect to the device IP address.
- **Fallback Netmask** — The network mask associated with the fallback IP address.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (132/301) 1865/4746

MGMT VLAN Settings

Figure 137: Management VLAN Settings



- **Mgmt VLAN** — Select this option to enable a management VLAN on site devices. Once you enable this option, you will no longer be able to access devices on any of the built-in the local networks (like 192.168.2.1 for example). You will only be able to access devices from the specified VLAN network. If a device's IP mode is set to DHCP, it will also request a new IP address in the subnet range assigned to the VLAN network.
- **Mgmt VLAN ID**— Specifies the ID of the management VLAN.
- **IP Address Mode** — The method used to provide an IP address for a device over the Management VLAN. (Options: DHCP, Static IP; Default: DHCP)
  - **DHCP** — Enables DHCP on the management VLAN.
  - **Static IP** — Sets a static IP to access site devices over the management VLAN. Configure an IP address, subnet mask, and default gateway address.
- **Fallback IP** — The IP address to use to connect to a device over the management VLAN if the DHCP-assigned address cannot be reached.
- **Fallback Netmask** — The network mask associated with the fallback IP address.

IPV6 Settings

Figure 138: IPv6 Settings

The following items are displayed on this section of the page:

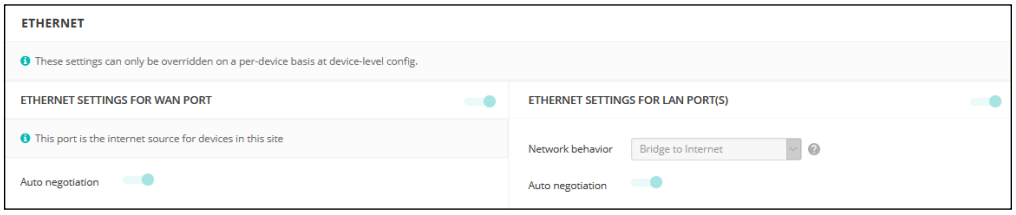
1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (133/301) 1666/4726

- **IP Address Mode** — The method used to provide an IPv6 address for the Internet access port. (Default: DHCP; Options: DHCP, Static IP)
  - **DHCP** — If you configure DHCP, the Client Id must be specified.
    - **Client Id** — Manually enter the client ID for the DHCP client.
  - **Static IP** — To configure a static IPv6 address for the Internet access port, the following items must be specified.
    - **IP Address** — Specifies an IPv6 address for the access point. An IPv6 address must be configured according to RFC 2373 using 8 colon separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
    - **Default Gateway** — The IPv6 address of the default gateway, which is used if the requested destination address is not on the local subnet.
    - **DNS** — The IPv6 address of Domain Name Servers on the network. A DNS maps numerical IPv6 addresses to domain names and can be used to identify network hosts by familiar names instead of the IPv6 addresses. If you have a DNS server located on the local network, type the IPv6 address in the text field provided.

Ethernet Settings

This page section shows basic Ethernet settings for site APs. These settings can only be overridden on a per-device basis at device-level configuration.

Figure 139: Ethernet Settings



The following items are displayed on this page section:

Ethernet Settings for WAN Port

By default, the WAN port interface is set as the Internet source and the following message is displayed: “This port is the Internet source for devices in this site.”

If more than one interface is connected to the Internet, only the last configured interface is used.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_procesoDiseño_029_2025_pdf (134/301) 1669/4746

- **Auto-negotiation** — Enables or disables auto-negotiation for the WAN port interface.

Ethernet Settings for LAN Port(s)

- **Network Behavior** — Shows the network connection method (that is, the manner in which the LAN ports are used).
- **Auto-negotiation** — Enables or disables auto-negotiation for a given port interface.

  1000BASE-T does not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T port.

  When auto-negotiation is enabled, the access point will negotiate the best settings for a link based on advertised capabilities.

VLAN Settings

The access point can employ VLAN tagging to control access to network resources and increase security. VLANs separate traffic passing between the access point, associated clients, and the wired network. You can create up to 12 VLAN tagged networks.

VLANs (virtual local area networks) are turned off by default. If turned on they will automatically tag any packets passed to Ethernet ports from the relevant VAP (virtual access point). Note also that specific VAPs can enable or disable VLAN tagging (see "Adding an SSID" on page 120).

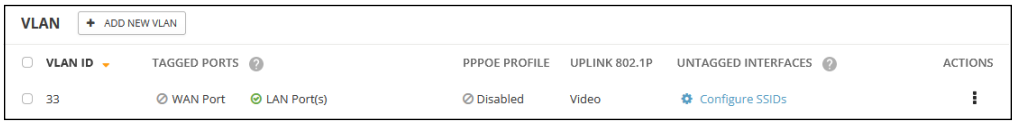
Note the following points about the access point's VLAN support:

- If an Ethernet LAN port on the access point is assigned a VLAN ID, any traffic entering that port must be also tagged with the same VLAN ID.
- Wireless clients associated to the access point can be assigned to a VLAN. Wireless clients are assigned to the VLAN for the VAP interface with which they are associated. The access point only allows traffic tagged with correct VLAN IDs to be forwarded to associated clients on each VAP interface.
- When VLAN support is enabled on the access point, traffic passed to the wired network is tagged with the appropriate VLAN ID. When an Ethernet port on the access point is configured as a VLAN member, traffic received from the wired network must also be tagged with the same VLAN ID. Received traffic that has an unknown VLAN ID or no VLAN tag is dropped.
- When VLAN support is disabled, the access point does not tag traffic passed to the wired network and ignores the VLAN tags on any received frames.

Note: Before enabling VLAN tagging on the access point, be sure to configure the attached network switch port to support tagged VLAN frames for the VLAN IDs configured on the access point. Otherwise, connectivity to the access point will be lost when you enable the VLAN feature.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (135/301) 1360/4726

Figure 140: VLAN Settings



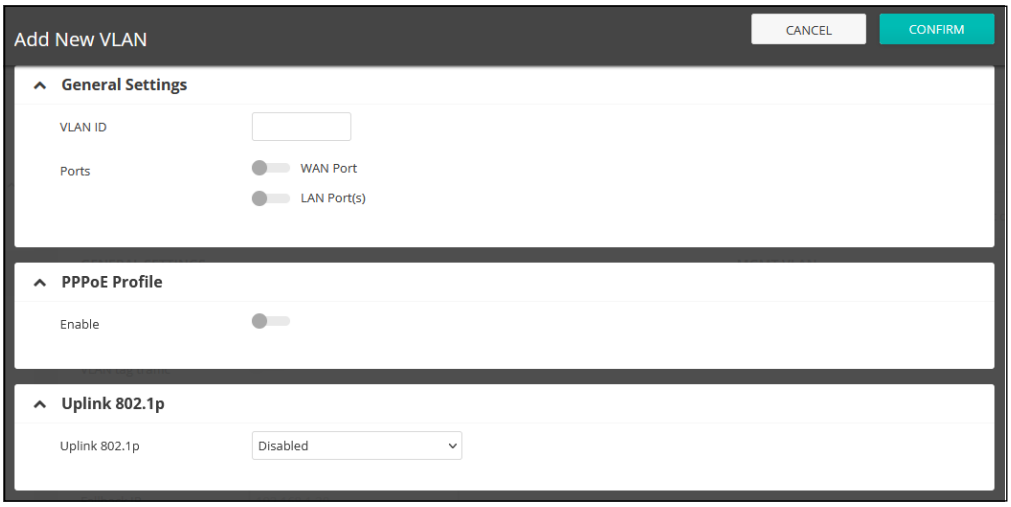
The following items are displayed on this page section:

- **VLAN ID** — The identifier assigned to the VLAN. (Range: 2-4094)
- **Tagged Ports** — The Ethernet ports assigned to the VLAN. Options include WAN port or LAN port(s).
- **PPPoE Profile** — Indicates if PPPoE is enabled or disabled for the VLAN.
- **Uplink 802.1P** — Indicates the IEEE 802.1p priority setting for traffic on this VLAN.
- **Untagged Interfaces** — Click the "Configure SSIDs" link to open the Wireless SSID tab. Then edit or create an SSID interface to be a member of the specified VLAN (see "Adding an SSID" on page 120).
- **Actions** — Click and select to edit or delete a configured VLAN.

Adding a VLAN

Click the "Add New VLAN" button to create a VLAN.

Figure 141: Adding a VLAN



The following items are displayed on this page section:

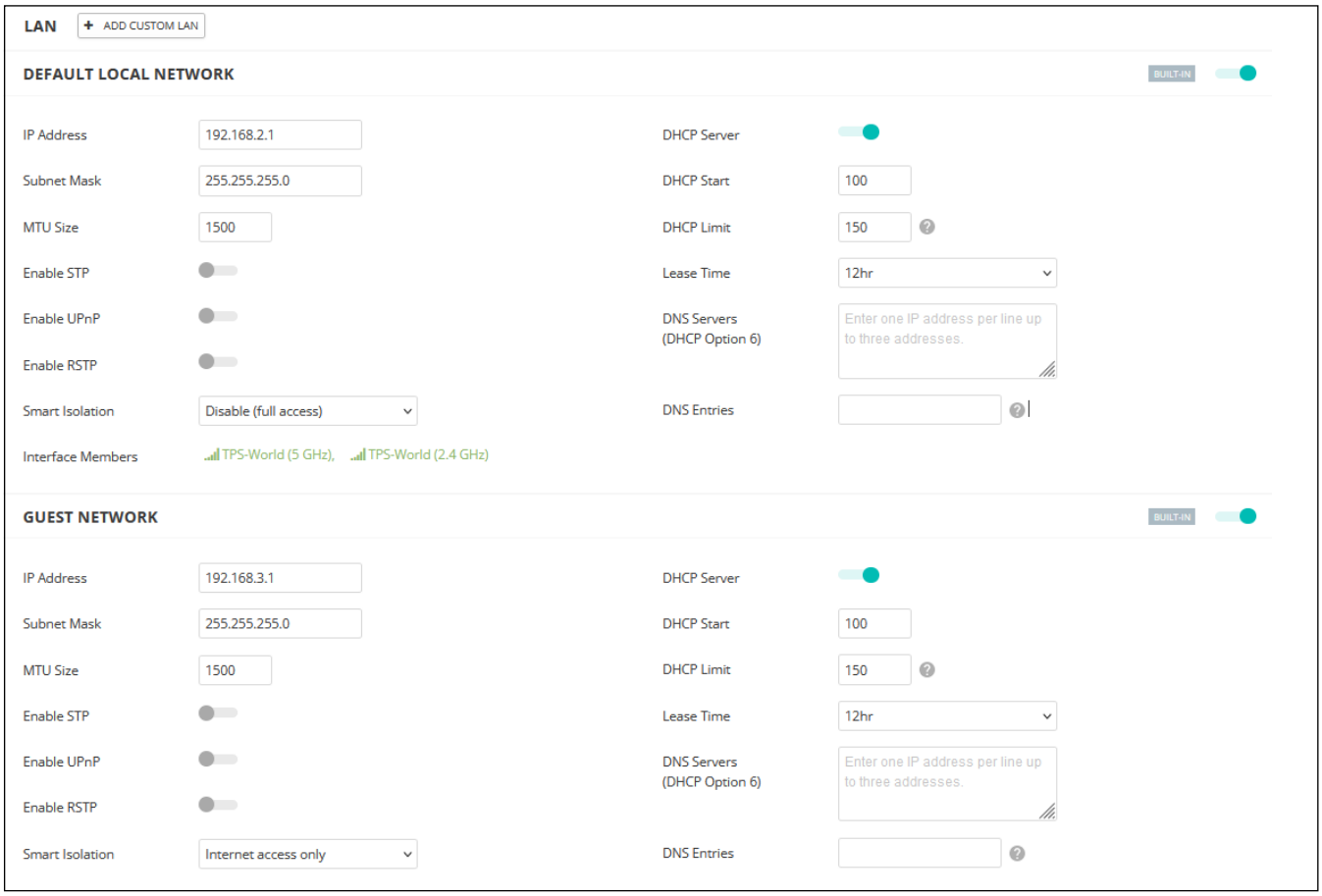
- **VLAN ID** — The VLAN identifier to be assigned. (Range: 2-4094)

- **Ports** — The Ethernet ports assigned to the VLAN. Options include WAN port or LAN port(s).
- **PPPoE Profile** — The Point-to-Point Protocol over Ethernet (PPPoE) is a common WAN protocol that provides a secure "tunnel" connection between a service provider and the local network.
  - **User Name** — The name to use for the service provider connection.
  - **Password** — The password to use for the service provider connection.
  - **IP Address** — The IP address to use for the service provider connection.
- **Uplink 802.1P** — Sets the IEEE 802.1p priority for traffic on this VLAN. Priorities range from "Best Effort" (lowest) to "Network Control" (highest).

Local Network Settings

The Local Network tab configures settings for the default LAN network, guest network, and other custom networks.

Figure 142: Local Network Settings



The following items are displayed on this page:

- **Add Custom LAN** — Click this button to create a additional networks with their own custom settings. You can create up to 10 custom LANs.
- **IP Address** — Specifies the IP address for the local network or guest network. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. (Default: 192.168.2.1)
- **Subnet Mask** — Indicates the local subnet mask. (Default: 255.255.255.0)
- **MTU Size** — Sets the size of the maximum transmission unit (MTU) for packets sent on this network. (Default: 1500)
- **Enable STP** — Enables or disables processing of Spanning Tree Protocol messages. (Default: Disabled)
- **Enable UPnP** — Enables or disables Universal Plug-and-Play broadcast messages. (Default: Disabled)
- **Enable RSTP** — Enables or disables processing of Rapid Spanning Tree Protocol messages. (Default: Disabled)
- **Smart Isolation** — Enables network traffic to be restricted to the specified network:
  - **Disable (full access)** — There is no traffic isolation. Clients can access the Internet and other devices on the local LAN. This is the option to choose if you trust the clients that will be connecting to your network.
  - I**nternet access only** — Traffic from this network can only be routed to and from the Internet. This is the option to choose for hotspot users or users connecting to a guest network.
  - **LAN access only** — Traffic from this network is restricted to local LAN devices only.
  - **Internet-only (strict)** — This is the same as "Internet access only," but with the additional restriction that users cannot access resources or devices on any private network (192.168.0.0, 172.16.0.0, 10.0.0.0, etc.). This is useful if an AP is “double NAT’ed” and the network upstream from your AP’s gateway is another private network.
- **Interface Members** — The interfaces attached to the local area network.
- **DHCP Server** — Enables/disables DHCP on this network. (Default: Enabled)
  - **DHCP Start** — First address in the address pool. (Range: 1-256; Default: x.x.x.100)

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (138/301) 1673/4726

- **DHCP Limit** — Maximum number of addresses in the address pool. (Range: 1-254; Default: 150)
- **Lease Time** — The time period for which assigned IP addresses are valid.
- **DNS Servers** — List up to three DNS server IP addresses, one per line.

- **DNS Entries** — Only applicable for Spark AC Wave2 Mini APs.Allows clients to access the web interface through the specified domain from a local network.

Firewall Settings

Firewall filtering restricts connection parameters to limit the risk of intrusion. The firewall settings allow you to define a sequential list of rules that filter traffic based on source and destination IP addresses and ports. Ingress packets are tested against the filter rules one by one. As soon as a packet matches a rule, the configured action is implemented.

One rule, "Allow-Ping," is pre-configured to allow Ping packets from the Internet. You can enable or disable this rule, but it cannot be modified or deleted. Click the "Add Rule" button to add a new firewall rule.

Figure 143: Firewall Settings

The following items are displayed on this page:

- **Enabled** — Enables the configured firewall rule.
- **Name** — User defined name for the filtering rule. (Range: 1-30 characters)
- **Source IP** — An IPv4 address in CIDR notation. Includes an IP address followed by a slash (/) and a decimal number to define the network mask.
- **Source Port** — The source protocol port. (Range: 1-65535)

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_procesoDistancia_029_2025_pag27.pdf (139/301) 3672/4726

- **Destination IP** — The destination IPv4 address.
- **Destination Port** — The destination protocol port. (Range: 1-65535)
- **Target** — The action to take when the configured rule matches a packet. (Options: Accept, Reject, Drop)
- **Family** — Specifies IPv4 or IPv6 traffic, or both. (Options: IPv4, IPv6, Any)
- **Source** — The source interface. (Options: Any, Default Local Network, Internet, Guest Network, Hotspot Network)
- **Protocol** — Defines the protocol type of packets. (Options: Any, TCP+UDP, TCP, UDP, ICMP)
- **Destination** — The destination interface. (Options: Any, Default Local Network, Internet, Guest Network, Hotspot Network)

Port Forwarding

Port Forwarding can be used to map an inbound protocol type (TCP/UDP) and port to an "internal" IP address and port. The internal (local) IP addresses are the IP addresses assigned to local devices at the edge of a network, and the external IP address is the IP address assigned to the AP interface. This allows remote users to access different servers on your local network using your single public IP address.

Remote users accessing services such as web or FTP at your local site through your public IP address, are redirected (mapped) to other local server IP addresses and TCP/UDP port numbers. For example, if you set Protocol/External Port to TCP/80 (HTTP or web) and the Destination IP/Destination Port to 192.168.3.9/80, then all HTTP requests from outside users are forwarded to 192.168.3.9 on port 80. Therefore, by just using your external IP address provided by your ISP, Internet users can access the services they need at the local addresses to which you redirect them.

The more common TCP service port numbers include: HTTP: 80, FTP: 21, Telnet: 23, and POP3: 110.

Figure 144: Port Forwarding

The following items are displayed on this page:

- **Enabled** — Enables port forwarding.
- **Name** — User-defined name. (Range: 1-30 characters)

1Doc: Protocolo 1.943/2025 | Proexadmin:3HG70B0B0B9B5321B6628972920250aa7Aniston_FC_proCelSD_UserMan_029_20250206227.pdf (140/301) 3675/4726

- **Protocol** — Set the protocol type to which port forwarding is applied. (Options: TCP, UDP, TCP+UDP)
- **External Port** — The Internet traffic TCP/UDP port number. (Range: 1-65535)
- **Destination IP** — The destination IP address on the local network.
- **Destination Port** — The destination protocol port. (Range: 1-65535)

ARP Inspection

ARP Inspection is a security feature that validates the MAC Address bindings for Address Resolution Protocol packets. It provides protection against ARP traffic with invalid MAC-to-IP address bindings, which forms the basis for certain "man-in-the middle" attacks. This is accomplished by intercepting all ARP requests and responses and verifying each of these packets before the local ARP cache is updated or the packet is forwarded to the appropriate destination. Invalid ARP packets are dropped.

Figure 145: ARP Inspection

The following items are displayed on this page:

- **ARP Inspection** — When enabled, ARP packets are validated against ARP spoofing.
- **Force DHCP** — Allows an AP to only learn MAC/IP pair information through DHCP packets. Since devices configured with static IP address do not send DHCP traffic, any clients with static IP addresses will be blocked by APs unless their MAC/IP pair is listed and enabled in the Static Trust List.
- **Trust List Broadcast** — Lets other APs learn the trusted MAC/IP pairs to issue ARP requests.
- **Static Trust List** — Adds the MAC or MAC/IP pairs of devices that are trusted to issue ARP requests. Other network nodes can still send their ARP requests, but if their IP appears in the static list with a different MAC, their ARP requests will be dropped.

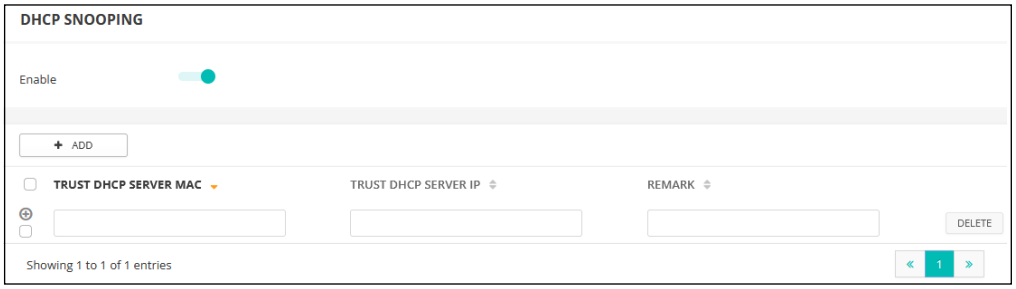
1Doc: Protocolo 1.943/2025 | Anexo Administrativo_procesoDistancia_029_2025_pdf (141/301) 1876/4726

DHCP Snooping

DHCP snooping is used to validate and filter DHCP messages received by APs. When DHCP snooping is enabled, DHCP messages received from a device not listed in the DHCP snooping table are dropped.

You can add known and trusted DHCP servers to the table by specifying their MAC and IP addresses.

Figure 146: DHCP Snooping



The following items are displayed on this page:

- **Enable** — Enables DHCP Snooping.
- **Trust DHCP Server MAC** — The MAC address of a known and trusted DHCP server.
- **Trust DHCP Server IP** — The IP address of a known and trusted DHCP server.
- **Remark** — A comment relating to the DHCP server configured.

Hotspot Settings

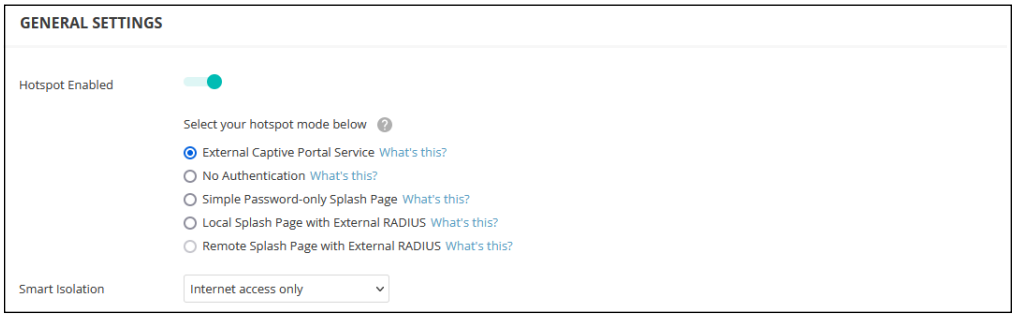
The Hotspot settings page can configure Internet access for the general public in places such as coffee shops, libraries, and hospitals. Specific access rights may also be defined through a RADIUS server.

When setting up a hotspot service, you must also navigate to the wireless SSID configuration page and select “Hotspot-Controlled” as the network behavior on an SSID interface. (See “Wireless SSID Configuration” on page 119.)

General Settings

The General Settings section on the Hotspot page configures the basic hotspot mode.

Figure 147: Hotspot General Settings



The following items are displayed on this page section:

- **Hotspot Enabled** — Enables or disables the hotspot service.

  Select the hotspot mode below. (Hotspot Mode will be statically set to "External Portal" for all firmware greater than 1.1.4. Please upgrade to firmware greater than 1.1.4 in order to take advantage of this setting.)

  - **External Captive Portal Service** — This option will show the hotspot guest an externally hosted captive portal splash page and may prompt them to login, depending on how you have configured your service settings. Choose this option if you have signed up with a third-party captive portal service provider, such as Cloud4Wi or HotSpotSystem.

  - **No Authentication** — This option shows the hotspot guest your customized, locally hosted captive portal splash page, and will not require the guest to login before accessing the Internet. If you fill out the (optional) terms of service text, the guest will be required to accept these before they can access the Internet.

  - **Simple Password-only Splash Page** — This option will show the hotspot guest your customized, locally hosted captive portal splash page, and will require them to enter a simple password to login and access the Internet. If you fill out the (optional) terms of service text, the guest will be required to accept these before they can access the Internet.

  - **Local Splash Page with External RADIUS** — This option shows the hotspot guest your customized, locally hosted captive portal splash page, and will require them to enter a valid RADIUS user name and password to login and access the Internet. If you fill out the (optional) terms of service text, the guest will be required to accept these before they can access the Internet.

  - **Remote Splash Page with External RADIUS** — This is an AuthPort add-on feature (see "Using the AuthPort Add-On" on page 75). The hotspot will be redirected to an external splash page and authenticate with an external RADIUS server.

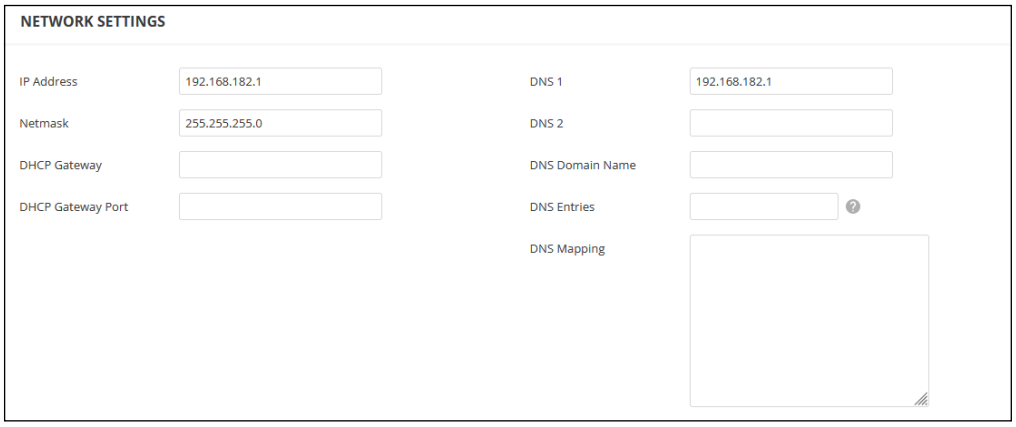
1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - Termo de Referência_processo_licitatorio_029_2025_pdf (143/301) 1678/4726

- **Smart Isolation** — Enables network traffic to be restricted to the specified network:
  - **Disable (full access)** — There is no traffic isolation. Clients can access the Internet and other devices on the local LAN. This is the option to choose if you trust the clients that will be connecting to your network.
  - **Internet access only** — Traffic from this network can only be routed to and from the Internet. This is the option to choose for hotspot users or users connecting to a guest network.
  - **LAN access only** — Traffic from this network is restricted to local LAN devices only.
  - **Internet-only (strict)** — This is the same as "Internet access only," but with the additional restriction that users cannot access resources or devices on any private network (192.168.0.0, 172.16.0.0, 10.0.0.0, etc.). This is useful if an AP is "double NAT'ed" and the network upstream from your AP's gateway is another private network.

Network Settings

The Network Settings section on the Hotspot page configures local network settings for the hotspot service.

Figure 148: Hotspot Network Settings



The following items are displayed on this page section:

- **IP Address** — Specifies the IP address for the hotspot. Valid IPv4 addresses consist of four decimal numbers, 0 to 255, separated by periods. (Default: 192.168.182.1)
- **Netmask** — Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- **DHCP Gateway** — The gateway used to access the DHCP server.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo processo licitatório 029_2025_pdf (144/301) 1879/4726

- **DHCP Gateway Port** — The UDP/TCP port used to access the DHCP server.
- **DNS 1** — The IP address of the primary Domain Name Server on the network. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses.
- **DNS 2** — The secondary DNS server available to DHCP clients.
- **DNS Domain Name** — The domain name used to resolve incomplete host names via the Domain Name System. (Range: 1-32 characters)
- **DNS Entries** — Only applicable for Spark AC Wave2 Mini APs.Allows clients to access the web interface through the specified domain from a local network.
- **DNS Mapping** — Configures DNS mapping for user-specified IP and domain name.

DHCP Server

The DHCP Server section on the Hotspot page configures DHCP address pool settings for the hotspot service.

Figure 149: Hotspot DHCP Server Settings

The following items are displayed on this page section:

- **Start** — Starting number of (last numeric field) in address pool. (Range: 1-254; Default: 10)
- **Limit** — Ending number of (last numeric field) in address pool. (Range: 1-245; Default: 245)
- **Lease Time** — The duration that an IP address is assigned to a DHCP client. (Range: 600-43200 seconds; Default: 3600 seconds)

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (145/301) 3870/4726

RADIUS Server

The RADIUS Server section on the Hotspot page configures RADIUS server settings for the hotspot service.

Figure 150: Hotspot RADIUS Server Settings

The following items are displayed on this page section:

- **Enable RADIUS Auth** — Enables RADIUS authentication for clients attempting to access the captive portal.
- **RADIUS Server Address** — IP address or host name of the primary RADIUS server.
- **Backup RADIUS server address** — IP address or host name of the secondary RADIUS server.
- **RADIUS server shared secret** — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS server. Do not use blank spaces in the string. (Range: 1-255 characters).
- **RADIUS server auth port** — RADIUS server UDP port used for authentication messages. (Range: 1-65535, Default: 1812)
- **RADIUS server acct port** — RADIUS server UDP port used for accounting messages. (Range: 1-65535, Default: 1813)
- **Enable RadSec** — An authentication and authorization protocol for transporting RADIUS datagrams over TCP and TLS. RadSec replaces UDP used in the initial RADIUS design, providing a reliable transport protocol and more extensive security for the packet payload.
- **Auth method** — Selects the encryption method to use for messages between the AP and the RADIUS server; CHAP, PAP, or MS-CHAPv2. The encryption method must match that used by the RADIUS server. (Default: CHAP)
- **Local ID** — Local RADIUS server identifier.

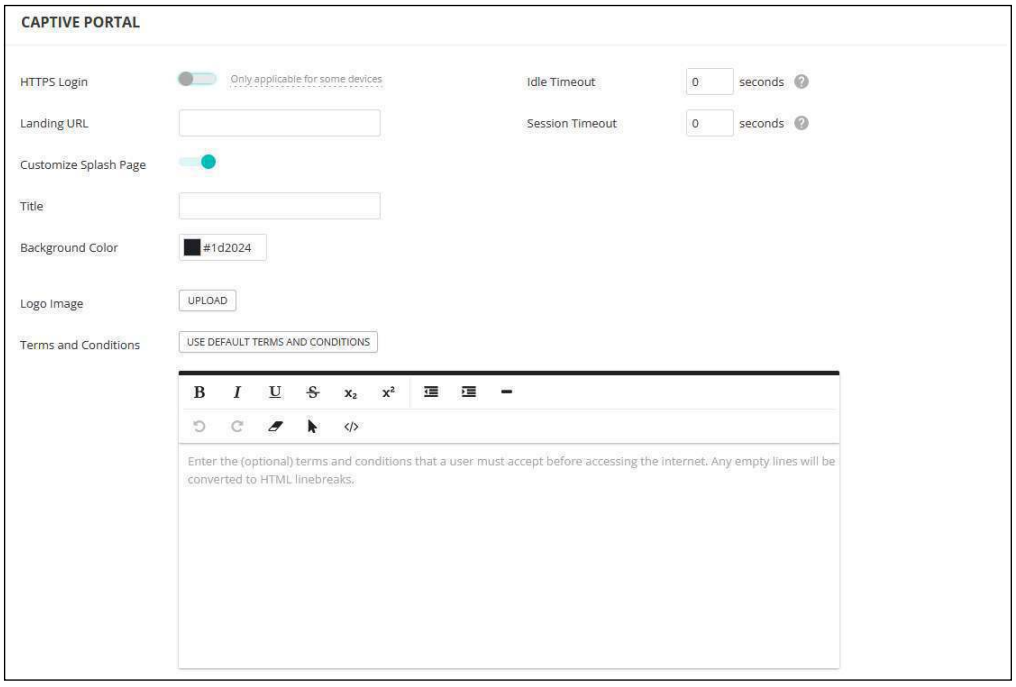
- **Local Name** — Local RADIUS server name
- **Generate NAS ID** — This option will generate a unique NAS ID for each device in this site.
- **NAS ID** — Local RADIUS server operation identifier.

Captive Portal

The Captive Portal section on the Hotspot page configures portal details for the hotspot service.

A captive portal forces a hotspot client to access a welcome web page before gaining further access to the Internet. The welcome page may require authentication and/or payment.

Figure 151: Hotspot Captive Portal Settings



Depending on the hotspot mode selected, the following items are displayed on this page section:

Common to all Modes

- **Landing URL** — Indicates the URL to which the user is directed after logging in to the captive portal.
- **Idle Timeout** — The maximum a connection can remain inactive before it is closed. (Range: 0-86400 seconds)
- **Session Timeout** — The maximum time a client can stay logged in to the hotspot. (Range: 0-86400 seconds)

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pregao_227.pdf (147/301) 1880/4726

Common to all Modes Except External Captive Portal Service and Remote Splash Page with External RADIUS

- **HTTPS Login** — Enables HTTPS for the captive portal.

Common to all Modes Except External Captive Portal Service

- **Customize Splash Page** — When enabled, fill in the information that is used to create the local captive portal welcome page.
  - **Title** — Enter the text you want to display as the title on the page.
  - **Background Color** — Click the button to select a color for the page background.
  - **Logo Image** — Click the "Upload" button to send an image file. Files are limited to a size of 1MB and the image must have a maximum height and width of 1000 pixels.
  - **Terms and Conditions** — Enter text in the window that define the captive portal terms and conditions, and then use the controls to format the text. Alternatively, click the "Use Default Terms and Conditions" button to import a generic text that you can then edit.

External Captive Portal Service Mode

- **Captive portal URL** — Host name of Internet service portal for the hotspot.
- **Captive portal secret** — The password used for logging into the hotspot.
- **Swap Octets** — Swap the values of the reported "input octets" and "output octets."

Simple Password-only Splash Page Mode

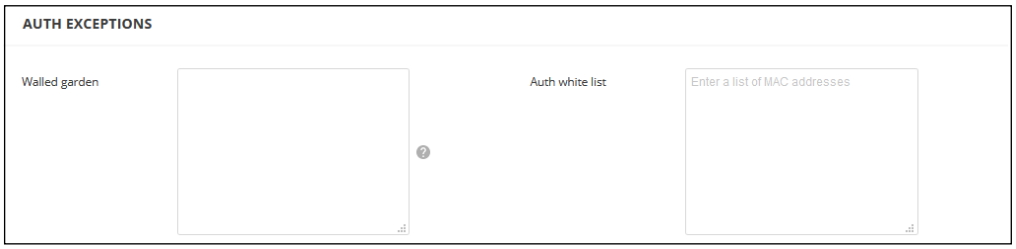
- **Splash Page Password** — The password required for users to log in and access the Internet.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (148/301) 1883/4726

Authentication Exceptions

The Auth Exceptions section on the Hotspot page configures a "walled garden" and white list for the hotspot service.

Figure 152: Hotspot Authentication Exceptions



The following items are displayed on this page section:

- **Walled garden** — Enter a list of domains or IP addresses in CIDR notation that hotspot users can access before being authenticated by the captive portal. Wildcard domains can be specified in the format of *domain.com* (allow domain and all sub-domains), or *.domain.com* (only allow sub-domains).
- **Auth white list** — A list of MAC addresses that are allowed to bypass the captive portal to access the Internet.

System Settings

The System Settings page allows you to control remote management access to APs and configure NTP time servers, Telnet, Web, and SNMP management interfaces are enabled and open to access from the Internet. To provide more security, specific services can be disabled and management access prevented from the Internet.

General Settings

The General Settings section on the System Settings page can be used to configure the cloud status LED, reset button, and time zone.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (149/301) 1852/4726

Figure 153: General System Settings

The following items are displayed on this page:

- **Enable cloud status LED** — For some devices (SkyFire, SunSpot, Spark, and Spark Wave 2 Mini), the LED is green when the AP is successfully connected to ecCLOUD and is operating normally.
- **Enable radio LEDs** — Only supported on ECW5211, ECWO5211, OAP100, and Spark Wave 2/SunSpot Wave 2 running 3.0.0+ firmware. The LEDs are on when a radio is enabled and operating normally.
- **Enable reset button** — Enables or disables the hardware reset button. Note that the reset button cannot be disabled at the site level.
- **Timezone** — To display a time corresponding to your local time, choose one of the predefined time zones from the pull-down list.
- **Number of boot retries** — The maximum number of bootup retries before switching to the next boot bank. (Range: 1-254; Default: 3)
- **Enable prelogin PPPoE form** — Turn this setting on in order to show a PPPoE username/password input form before the local web UI login form whenever the Internet does not appear to be accessible. This will allow end users to enter their PPPoE credentials without having to log in to the device UI.
- **MSP Mode** — Enables the Managed Service Provider (MSP) mode that prevents end-users from accessing and modifying most device settings from user-defined user accounts. Management access from "root" and "admin" accounts still provide full access to all device settings. (Default: Disabled)

  With MSP mode enabled, service providers have the option of making specific wireless SSID settings available for user configuration by enabling the "Local Configurable" setting.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - Termo de Referência_processo_licitatorio_029_2025_pdf (150/301) 1885/4726

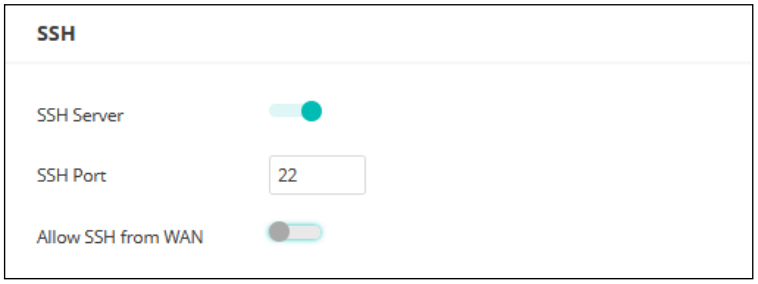
Note: Do not enable MSP Mode and "Always follow cloud configuration" (page 65) at the same time. This will cause the device configuration not to be updated to ecCLOUD properly.

SSH

The Secure Shell (SSH) acts as a secure replacement for Telnet. The SSH protocol uses generated public keys to encrypt all data transfers passing between the access point and SSH-enabled management station clients and ensures that data traveling over the network arrives unaltered. Clients can then securely use the local user name and password for access authentication.

Note that SSH client software needs to be installed on the management station to access the access point for management via the SSH protocol.

Figure 154: SSH Server Settings



The following items are displayed on this page:

- **SSH Server** — Enables or disables SSH access to the access point. (Default: Enabled)
- **SSH Port** — Sets the TCP port number for the SSH server on the access point. (Range: 1-65535; Default: 22)
- **Allow SSH from WAN** — Allows SSH management access from the WAN.

Discovery Tool

The Edgecore Discovery agent allows the AP to be discovered by other devices on the local network or over the Internet.

Figure 155: Discovery Tool Settings

1Doc: Protocolo 1.943/2025 | Proxeden Administrator EC_proceso_usuario_029_20252026227.pdf (151/301) 1886/4726

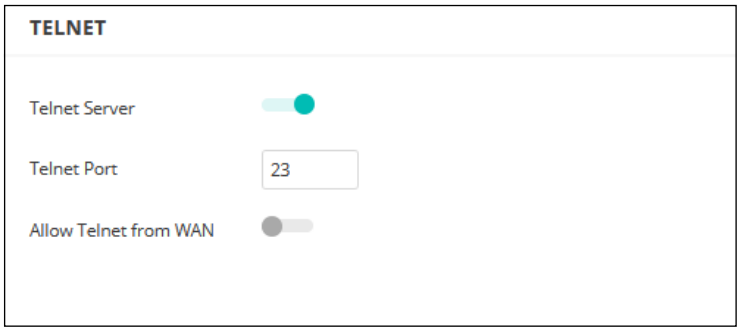
The following items are displayed on this page:

- **Discovery Tool** — Enables or disables the discovery tool. (Default: Enabled)
- **Allow over WAN** — Allows discovery tool access from the WAN.

Telnet

Telnet is a remote management tool that can be used to configure the access point from anywhere in the network. However, note that Telnet is not secure from hostile attacks. Telnet provides access to a Linux-based interface which is used for device analysis and debugging.

Figure 156: Telnet Server Settings



The following items are displayed on this page:

- **Telnet Server** — Enables or disables Telnet access to the access point. (Default: Enabled)
- **Telnet Port** — Sets the TCP port number for the Telnet server on the access point. (Range: 1-65535; Default: 23)
- **Allow Telnet from WAN** — Allows Telnet management access from the WAN.

Web Server

A Web browser provides the primary method of managing the access point. Both HTTP and HTTPS service can be accessed independently. If you enable HTTPS, you must indicate this in the URL: https://device:port_number]

When you start HTTPS, the connection is established in this way:

- The client authenticates the server using the server's digital certificate.
- The client and server negotiate a set of security protocols to use for the connection.
- The client and server generate session keys for encrypting and decrypting data.
- The client and server establish a secure encrypted connection.
- A padlock icon should appear in the status bar for most browsers.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (152/301) 3885/4746

Figure 157: Web Server Settings

The following items are displayed on this page:

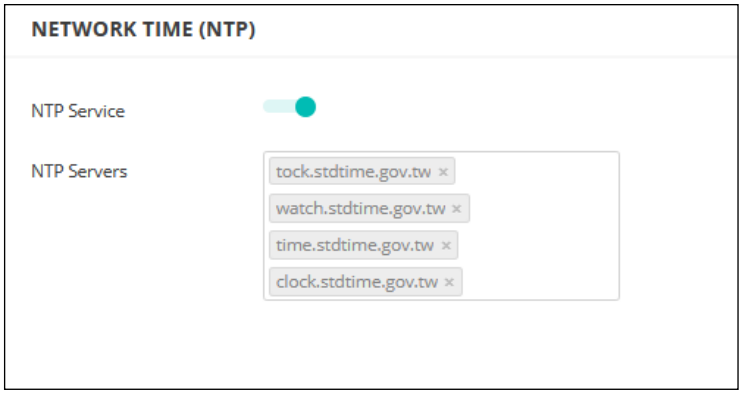
- **HTTP Port** — The TCP port to be used by the HTTP Web browser interface. (Range: 1-65535; Default: 80)
- **Allow HTTP from WAN** — Allows HTTP management access from the WAN.
- **HTTPS Port** — The TCP port to be used by the HTTPS Web browser interface. (Range: 1-65535; Default: 443)
- **Allow HTTPS from WAN** — Allows HTTPS management access from the WAN.

Network Time

Network Time Protocol (NTP) allows the access point to set its internal clock based on periodic updates from a time server (SNTP or NTP). Maintaining an accurate time on the access point enables the system log to record meaningful dates and times for event entries. If the clock is not set, the access point will only record the time from the factory default set at the last bootup.

The access point acts as an NTP client, periodically sending time synchronization requests to specified time servers. The access point will attempt to poll each server in the configured sequence to receive a time update.

Figure 158: NTP Settings



1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - Termo de Referência - Processo Licitatório 029_2025_Pregão 027.pdf (153/301) 1886/4746

The following items are displayed on this page:

- **NTP Service** — Enables or disables sending of requests for time updates. (Default: Enabled)
- **NTP Servers** — Sets the host names for time servers. The switch attempts to update the time from the first server, if this fails it attempts an update from the next server in the sequence. To configure additional servers, type in an entry in the blank field at the bottom of the list.

SNMP

Simple Network Management Protocol (SNMP) is a communication protocol designed specifically for managing devices on a network. It is typically used to configure these devices for proper operation in a network environment, as well as to monitor them to evaluate performance or detect potential problems.

Figure 159: SNMP Settings

The following items are displayed on this page:

- **SNMP Server** — Enables or disables SNMP on the access point. (Default: Enabled)
- **Contact** — Administrator responsible for the access point.
- **Community String** — A community string that acts like a password and permits access to the SNMP protocol. (Range: 1-32 characters, case sensitive; Default: public)

  The default string "public" provides read-only access to the access point's Management Information (MIB) database.
- **IPv6 Write Community** — A community string for IPv6 access to the access point's Management Information (MIB) database. (Range: 1-32 characters, case sensitive; Default: private6)

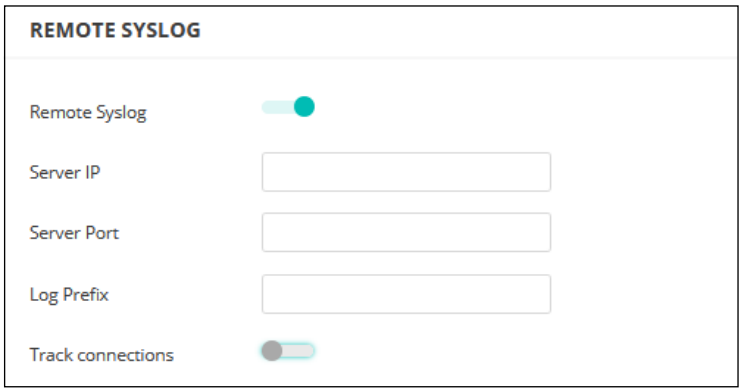
1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - Termo de Referência_processo_licitatorio_029_2025_pdf (154/301) 1889/4746

- **Location** — Sets the SNMP system location string. (Maximum length: 255 characters)
- **Allow SNMP from WAN** — Allows SNMP management access from the WAN.

Remote Syslog

Use this feature to send log messages to a Syslog server.

Figure 160: Remote Log Settings



The following items are displayed on this page:

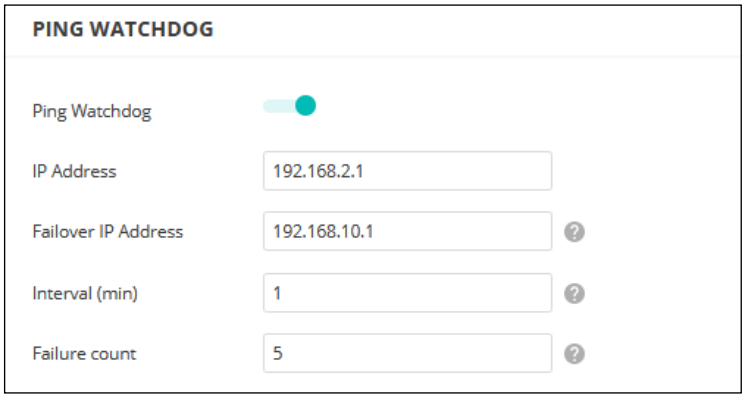
- **Remote Syslog** — Enables/disables the logging of debug or error messages to the remote logging process. (Default: Disabled)
- **Server IP** — Specifies the IP address of a remote server which will be sent syslog messages.
- **Server Port** — Specifies the UDP port number used by the remote server. (Range: 1-65535)
- **Log Prefix** — Sets the prefix for the log file sent to the specified server. The file suffix "log" is used.
- **Track connections** — Sends wireless client connection log messages to the Syslog server.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (155/301) 1868/4746

Ping Watchdog

Use this feature to send ping probe packets to a defined IP address to confirm connectivity.

Figure 161: Ping Watchdog Settings



The following items are displayed on this page:

- **Ping Watchdog** — Enable the sending of ping probe packets to a defined IP address to confirm connectivity. (Default: Disabled)
- **IP Address** — The primary IP address to ping.
- **Failover IP Address** — The (optional) failover IP address to ping if a ping probe to the primary IP fails. Note that if the failover IP can successfully be pinged, the fail counter will reset to zero again.
- **Interval (min)** — How often, in minutes, a ping check should be made.
- **Failure count** — The number of consecutive pings that must fail before the device is rebooted.

BLE Settings

Use this feature to enable devices to push records of Bluetooth Low Energy (BLE) probe requests to a specified URL.

BLE settings are available only on devices with BLE support.

Figure 162: BLE Settings

1Doc: Protocolo 1.943/2025 | Anexo Administrativo processo licitatório 029_2025_pdf (156/301) 156/4726

The following items are displayed on this page:

- **BLE Probe Req. Data Push** — Enable BLE Probe Request Data Push for site APs. When enabled, APs will push BLE probe request data in JSON format to the specified URL.
- **Push URL** — The URL to which to send data.

Multicast DNS

Use this feature to enable Multicast DNS support on APs. Multicast DNS can be used on small networks that do not have a DNS server to resolve host names to multicast IP addresses.

Multicast DNS settings are available only on devices with mDNS support.

Figure 163: Multicast DNS Settings

The following items are displayed on this page:

- **MDNS** — Enables or disables multicast DNS support. (Default: Enabled)

IGMP Snooping

APs can use IGMP (Internet Group Management Protocol) to check for any clients that want to receive a specific multicast service. APs can then propagate service requests up to any neighboring multicast switch/router to ensure that clients will continue to receive the multicast service.

Figure 164: IGMP Snooping Settings

The following items are displayed on this page:

- **Enable** — Enables the IGMP Snooping service. (Default: Disabled)

1Doc: Protocolo 1.943/2025 | Anexo Administrativo processo 029.00052.0000227.pdf (157/301) 1892/4746

LLDP

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices in a network. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device.

Figure 165: LLDP Settings

The following items are displayed on this page:

- **Enable** — Enables the sending of LLDP advertisements about the AP to neighboring devices in the network. (Default: Disabled)
- **Tx Interval (seconds)** — Sets the periodic transmit interval for LLDP advertisements. (Range: 5-32768 seconds; Default: 30 seconds)
- **Tx Hold (number of time(s))** — Configures a time-to-live (TTL) value sent in the LLDP advertisements as shown in the formula below. (Range: 2-10; Default: 4)

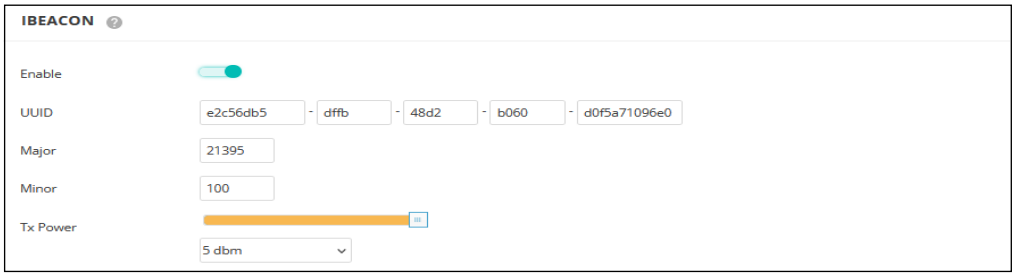
  The time-to-live tells the receiving LLDP agent how long to retain all information pertaining to the sending device if it does not transmit updates in a timely manner.

  The TTL in seconds is based on the following rule:
  minimum value ((Tx Interval * Tx Hold), or 65535)
  Therefore, the default TTL is 4*30 = 120 seconds.

iBeacon

The AP supports the iBeacon standard based on Bluetooth Low Energy (BLE). Devices with BLE Beacons can provide location-based services to BLE clients, such as phones, that can recognize the beacon advertisements, extract the provided information, and then take actions based on the content.

Figure 166: iBeacon Settings



1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (158/301) 1893/4746

The following items are displayed on this page:

- **Enable** — Enables iBeacon support on the AP. (Default: Enabled)
- **UUID** — The iBeacon Universally Unique Identifier that advertises the beacon service. The UUID contains 32 hexadecimal digits in five groups, separated by hyphens.
- **Major** — The iBeacon value that is used to identify a beacon group. (Range: 0-65535)
- **Minor** — The iBeacon value that is used to identify individual beacons within a group. (Range: 0-65535)

SNMPv3 User

SNMP protocol version 3 provides secure access by account authentication and data encryption. An SNMP v3 user can be defined by clicking the Add button.

Figure 167: SNMPv3 User Settings

The following items are displayed on this page:

- **Name** — The user name used to access the SNMP service.
- **Access Auth** — Select the access permission as “Read Only” or “Write.”
- **Auth Type** — Select the hash algorithm for authentication.
- **Auth Pwd** — Configure the password for authentication.
- **Encryption Type** — Select the encryption algorithm for data packets.
- **Encryption Pwd** — Configure the password for data encryption.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo processo licitatório 029_2025_pregão 027.pdf (159/301) 1892/4746

5 Site WiFi 6 Configuration

This chapter describes configuration settings for WiFi 6 access point devices. It includes the following sections:

1Doc: Protocolo 1.943/2025 | Anexo Administrativo processo digital (160/301) 1895/4726

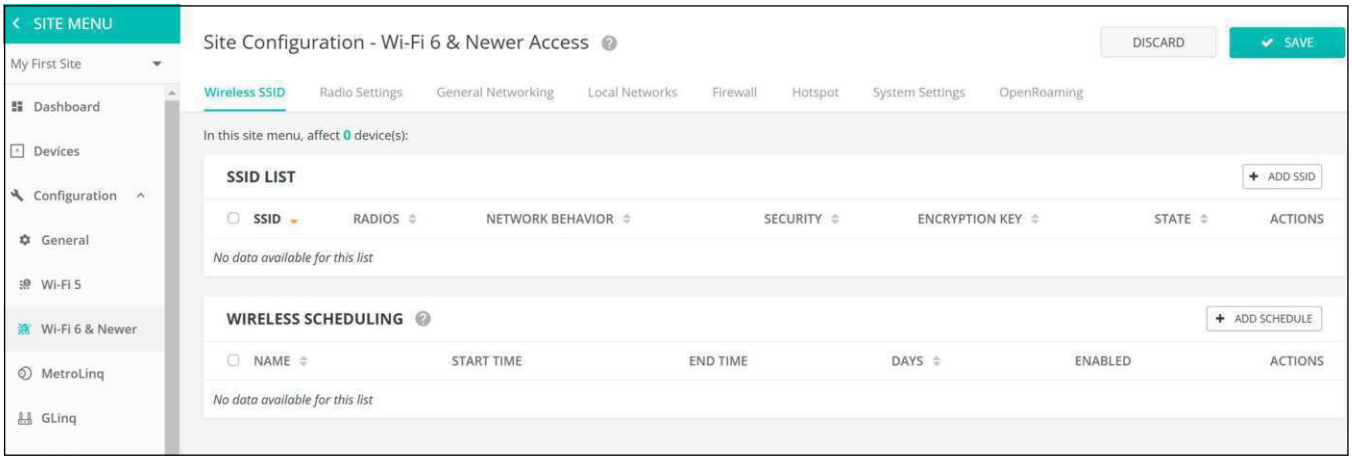
Wireless SSID Configuration

From the Site menu, open "Configuration" and then "WiFi6 & Newer" to display the configuration options that apply to all Edgecore Wi-Fi 6 access points in the same site.

The Edgecore Wi-Fi 6 access points can operate in several radio modes, 802.11a/a+n/ac+a+n/ax (5 GHz) or 802.11b+g+n/ax (2.4 GHz). Supported modes depend on the access point model. Note that the dual-band access points can operate at 2.4 GHz and 5 GHz at the same time.

Each radio supports eight Service Set Identification (SSID) or virtual access point (VAP) interfaces. Each VAP functions as a separate access point, and can be configured with its own SSID and security settings. However, most radio signal parameters apply to all VAP interfaces. Traffic to specific VAPs can be segregated based on user groups or application traffic. Wireless clients associate with each VAP in the same way as they would with separate physical access points. Edgecore AP devices support up to a total of 128 wireless clients across all SSID interfaces per radio.

Figure 168: Site WiFi6 Configuration



The Wireless SSID tab on the WiFi6 configuration page includes these items:

- **SSID List** — The list of configured SSID interfaces for the Wi-Fi devices in this site. Note that each SSID applies to both the 2.4 GHz, 5 GHz, and 6 GHz radios unless otherwise configured. You can configure a maximum of eight SSIDs. Click the "Add SSID" button to create an SSID interface.

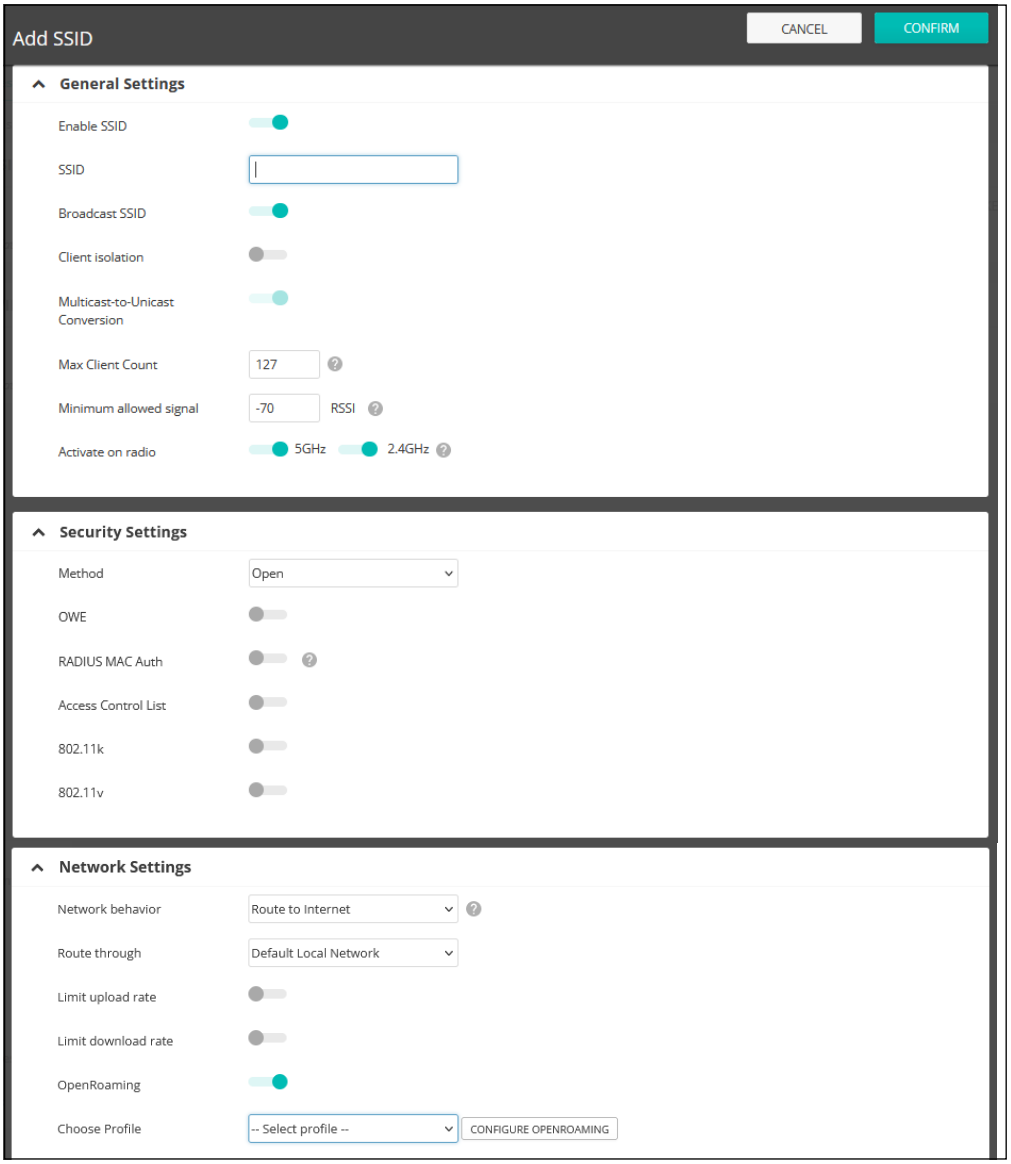
- **Wireless Scheduling** — A list of configured schedules for turning AP radios on and off at specified times. The scheduling rules apply to all 2.4 GHz, 5 GHz and 6 GHz interfaces on all site APs. Click the "Add Schedule" button to create a wireless schedule.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo Processo Licitatório 029_2025_pdf (161/301) 1896/4746

Adding an SSID

Click the Add SSID button on the WiFi6 Access configuration page and enter SSID, network, and security settings as displayed below.

Figure 169: Radio Settings (New SSID)



The following items are displayed on the Add SSID page:

General Settings

- **Enable SSID** — Enables or disables the SSID interface.
- **SSID** — The name of the basic service set provided by the VAP interface. Clients that want to connect to the network through the access point must set their SSID to the same as that of the access point's VAP interface. (Range: 1-32 characters)

1Doc: Protocolo 1.943/2025 | Anexo Administrativo ... (162/301) 3895/4746

- **Broadcast SSID** — The SSID can be broadcast at regular intervals so that wireless stations searching for a network connection can discover it. This allows wireless clients to dynamically discover and roam between WLANs. This feature also makes it easier for hackers to break into your home network. Because SSIDs are not encrypted, it is easy to scan WLANs looking for SSID broadcast messages coming from an AP. (Default: On)

- **SSID Isolation** — When enabled, wireless clients connected to different SSIDs on the same radio cards are isolated from each other. (Default Off)

- **Client Isolation** — When enabled, wireless clients can talk to the LAN, and reach the Internet if such connection is available, but they cannot communicate with one another. (Default Off)

- **Multicast-to-Unicast Conversion** — When enabled, the AP forwards multicast traffic only to those clients that request multicast traffic, instead of broadcasting traffic to all clients. This feature is automatically enabled when client isolation is disabled, and disabled when client isolation is enabled. The feature cannot be configured manually. (Default On)

- **Max Client Count** — Sets the maximum number of wireless clients that can be connected to this SSID at the same time. (Default: 127; Range: 0 to 127)

- **Minimum allowed Signal** — Only allows clients to associate to this SSID if their signal strength (RSSI) is equal or greater than the specified value. Setting the value to -100 disables this feature. Clients already connected are checked periodically.

  This forces clients to associate with an AP that has a better signal strength (also called assisted roaming). Suggested value is -70 to -80 depending on access point density and coverage.

  Enter an RSSI (Received Signal Strength Indicator) in decibels from -1 to -100db. Note that the closer it is to zero, the stronger the signal. (Default: -70)

- **Activate on radio** — Selects the radios on which this SSID should be created. If an SSID is activated on both radios for a device (meaning that the SSID will be mirrored), you can edit its record from either configuration tab, and the changes will be made on both the 2.4 GHz and 5 GHz SSID records. (Default: 6GHz, 5GHz, and 2.4GHz enabled)

Security Settings

Method — Sets the wireless security method for each SSID, including association mode, encryption, and authentication. (Default: Open)

Note: The OAP101-6E 6GHz radio supports only WPA3 Personal, WPA3 Enterprise, WPA3 Enterprise 192-bit, and OWE. (Default: WPA3 Personal)

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (163/301) 3696/4726

- **Open** — The SSID interface broadcasts a beacon signal including the configured SSID. Wireless clients with an SSID setting of "any" can read the SSID from the beacon and automatically set their SSID to allow immediate connection.

- **WPA-PSK** — For enterprise deployment, WPA requires a RADIUS authentication server to be configured on the wired network. However, for small office networks that may not have the resources to configure and maintain a RADIUS server, WPA provides a simple operating mode that uses just a pre-shared password for network access. The Pre-Shared Key mode uses a common password for user authentication that is manually entered on the access point and all wireless clients. The PSK mode uses the same TKIP packet encryption and key management as WPA in the enterprise, providing a robust and manageable alternative for small networks.

  - **Encryption** — Data encryption uses one of the following methods:

    - **AES** — AES-CCMP is used as the multicast encryption cipher. AES-CCMP is the standard encryption cipher required for WPA2. (This is the default setting.)

    - **TKIP + AES** — The encryption method used by the client is discovered by the access point.

  - **Key** — WPA is used to encrypt data transmitted between wireless clients and the SSID interface. WPA uses static shared keys (fixed-length hexadecimal or alphanumeric strings) that are manually distributed to all clients that want to use the network.

    String length must be 8 to 63 ASCII characters (letters and numbers). No special characters are allowed.

  - **Dynamic Keys** — Enables the use of dynamic PSK keys that are periodically generated and updated by a RADIUS authentication server. The RADIUS server IP address, UDP port, and secret text string must be specified.

    Dynamic keys are supported only for WPA2-PSK security.

  - **Multiple Keys** — Enables the entry of multiple keys, one per line. Entering a key with a specific MAC address limits the key for use by a single client. Entering a key without a MAC address enables the key to be used by all clients.

    Multiple keys are supported for WPA-PSK, WPA2-PSK, and WPA3 Personal Transition security.

- **WPA2-PSK** — Clients using WPA2 with a Pre-shared Key are accepted for authentication.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - Termo de Referência_processo_licitatorio_029_2025_pdf (164/301) 3697/4746

WPA was introduced as an interim solution for the vulnerability of WEP pending the ratification of the IEEE 802.11i wireless security standard. In effect, the WPA security features are a subset of the 802.11i standard. WPA2 includes the now ratified 802.11i standard, but also offers backward compatibility with WPA. Therefore, WPA2 includes the same 802.1X and PSK modes of operation and support for TKIP encryption.

Refer to WPA-PSK for a description of encryption methods and the key.

- **WPA-EAP** — WPA employs a combination of several technologies to provide an enhanced security solution for 802.11 wireless networks. A RADIUS server is used for authentication, and can also be used for accounting.

  Refer to WPA-PSK for a description of encryption methods.

  RADIUS Settings

  A RADIUS server must be specified for the access point to implement IEEE 802.1X network access control and Wi-Fi Protected Access (WPA) wireless security.

  In addition, you can configure a RADIUS Accounting server to receive user-session accounting information from the access point. RADIUS Accounting can be used to provide valuable information on user activity in the network.

Note: This guide assumes that you have already configured RADIUS servers) to support the access point. Configuration of RADIUS server software is beyond the scope of this guide, refer to the documentation provided with the RADIUS server software.

- **Radius MAC Auth** — Use RADIUS authentication. When this setting is enabled, the AP will send the MAC address of the client device to the specified RADIUS server for authentication. The server verifies the MAC is a valid user, and then replies to the AP with the dynamic VLAN ID (if configured) and other resources for the client device.

  Note: On your RADIUS server, both the user ID and password will need to be set to the WiFi MAC of the client device and must be formatted without punctuation.

  This feature is supported with “Open Security” in v1.1.1 firmware, and all other security methods (besides WEP) in v1.1.2 firmware.

- **Use RADIUS Auth** — For WPA-EAP and WPA2-EAP security, a RADIUS server must be specified.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (165/301) 1870/4726

- **RADIUS Auth Server** — Specifies the IP address or host name of the RADIUS authentication server.
- **RADIUS Auth Port** — The UDP port number used by the RADIUS server for authentication messages. (Range: 1024-65535; Default: 1812)
- **RADIUS Auth Secret** — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS authentication server. Do not use blank spaces in the string. (Maximum length: 255 characters)
- **Backup RADIUS Auth** — Configures a secondary RADIUS server to act as a backup should the primary server become unavailable.
- **Use RADIUS Accounting** — Use RADIUS accounting to enable accounting of requested services for billing or security purposes.
- **RADIUS Acct Server** — Specifies the IP address or host name of the RADIUS accounting server.
- **Radius Acct Port** — The UDP port number used by the RADIUS server for accounting messages. (Range: 1024-65535; Default: 1813)
- **RADIUS Acct Secret** — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS accounting server. Do not use blank spaces in the string. (Maximum length: 255 characters)

- **WPA2-EAP** — WPA was introduced as an interim solution for the vulnerability of WEP pending the ratification of the IEEE 802.11i wireless security standard. In effect, the WPA security features are a subset of the 802.11i standard. WPA2 includes the now ratified 802.11i standard, but also offers backward compatibility with WPA. Therefore, WPA2 includes the same 802.1X and PSK modes of operation and support for TKIP encryption.

  A RADIUS server is used for authentication, and can also be used to accounting.

  Refer to WPA-PSK for a description of encryption methods.

  Refer to WPA-EAP for information on configuring the RADIUS server.

- **WPA3 Personal** — Clients using WPA3 with Simultaneous Authentication of Equals (SAE) are accepted for authentication.

  WPA3 provides more robust password-based authentication called Simultaneous Authentication of Equals (SAE), which replaces Pre-Share Key (PSK) in WPA2-Personal. This technology prevents offline dictionary attacks so that data traffic can be transmitted securely.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf_3f4c7d8b9e2a1f6d8b9e2a1f6d8b9e2a_Anexo_EC_processo_licitatorio_029_2025_page_27.pdf (166/301) 1879/4746

- **WPA3 Personal Transition** — Clients using WPA3 with SAE or clients using WPA2 with PSK are accepted for authentication. The AP negotiates the supported authentication and encryption with each client before allowing access to the network.

- **WPA3 Enterprise** — An enhanced version of WPA2-EAP security that uses more robust encryption. Clients must support one of the stronger WPA3 encryption options and use Protected Management Frames (PMF) to be able to access the network. The use of IEEE 802.1X network access control and a RADIUS server is required.

  Refer to RADIUS Settings above for information on RADIUS configuration.

- **WPA3 Enterprise Transition** — Allows WPA3 and WPA2 clients to access the network. Encryption options and the use of Protected Management Frames (PMF) are negotiated with each client before allowing access to the network.

  Refer to RADIUS Settings above for information on RADIUS configuration.

- **WPA3 Enterprise 192-bit** — WPA3 Enterprise security uses a standard 128-bit encryption. For a network handling more sensitive data, there is an option to use 192-bit encryption for additional protection.

  Refer to RADIUS Settings above for information on RADIUS configuration.

- **PMF** — Protected Management Frames (PMF) provide WPA2/WPA3 security for unicast and multicast management frames between the AP and clients. The "Optional" setting allows clients that do not support PMF to access the network. The "Mandatory" setting allows only clients that support PMF to access the network. (Default: Optional)

- **802.11k** — Provides clients with information on neighbor APs when roaming. As a client is about to roam from an AP, it sends a request for a "Neighbor Report" that includes a list of available APs and associated information. The client can then quickly identify the best AP to which it can roam without having to scan all channels. (Default: Disabled)

- **802.11v** — Provides information to associated clients that facilitates the overall improvement of the wireless network. Also helps clients to improve battery life by setting the idle period. (Default: Disabled)

- **802.11r** — Provides a method for fast transition roaming between APs. Before clients roam to a new AP, the initial handshake and encryption calculations are performed in advance, which results in a fast hand off without the need for re-authentication. (Default: Disabled)

- **OWE** — Opportunistic Wireless Encryption (OWE) is the WPA3 open network security that allows users of public Wi-Fi networks to gain secure access without using a password. OWE provides individual encryption of data

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 27/08/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (167/301) 167/301

communications between the AP and each client, but does not provide authentication of user identities.

- **Access Control List** — Wireless clients can be authenticated for network access by checking their MAC address against the local database configured on the access point. (Default: OFF)
  - **Policy** — The MAC list can be configured to either allow or deny network access to specified clients. (Default: Allow all MACs on list)
  - **Filtered MACs** — List of client MAC addresses.
- **Dynamic Authorization** — The Dynamic Authorization Extensions (DAE) to RADIUS enable a server to disconnect or change the authorization of clients that are already connected to the network.
  - **DAE Port** — The UDP port number to use for DAE messages. (Default: 3799)
  - **DAE Client** — The IPv4 address of the RADIUS server.
  - **DAE Secret** — The shared text string used to encrypt DAE messages between the access point and the RADIUS server.

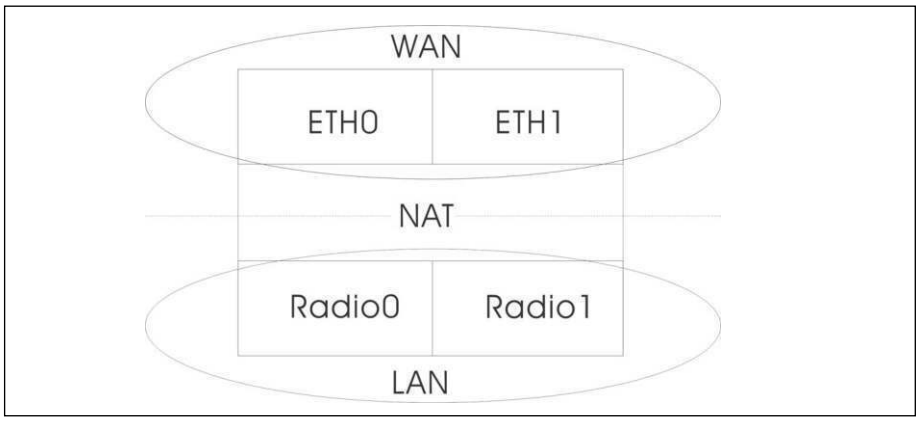
Network Settings

- **Network Behavior** — One of the following connection methods must be specified. (Default: Route to Internet)
  - **Bridge to Internet (AP Bridge Mode)** — Configures an interface as attached to the WAN (that is, the Internet).

    In the following figure, Ethernet port 0 and Ethernet port 1 are both attached to the WAN. Traffic from these interfaces is directly bridged into the Internet. Any of the Ethernet or radio interfaces can be configured this way.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo processo licitatório 029_2025_pdf (168/301) 1673/4726

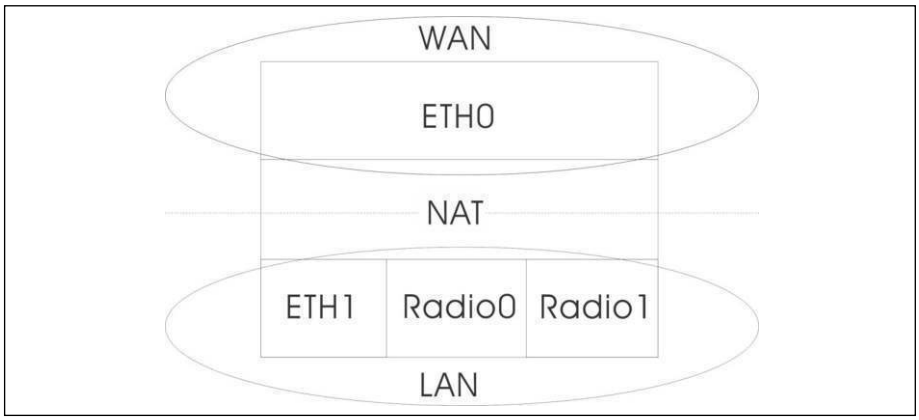
Figure 170: Bridge to Internet



- **Route to Internet (AP Router Mode)** — Configures an interface as a member of the LAN.

  In the following figure, Ethernet port 1, Wireless LAN 0 (5 GHz radio), and Wireless LAN 1 (2.4 GHz radio) are all included in the LAN. Traffic from these interfaces is routed across the access point through Ethernet port 0 to the Internet.

Figure 171: Route to Internet



  - **Route through** — The network to be routed. The default is "Default local network" as displayed under LAN Settings – Local Network.

- **Add to Guest Network** — This interface can only support the guest network.

- **Hotspot Controlled** — This interface can only support hotspot services.

  - **Walled garden** — Enter a list of domains and/or IP addresses in CIDR notation that the hotspot user can access before being authenticated by the captive portal. Wildcard domains can be specified in the format of *domain.com* (allow domain and all of its subdomains), or *.domain.com* (only allow subdomains).

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 (27/28) - Processo Licitatório 029_2025_Pregão 027.pdf (169/301) 169/4726

- **VLAN Tag Traffic** — Tags any packets passing from this SSID interface to the associated Ethernet port as configured under "VLAN Settings" on page 182. When enabled, select a configured VLAN ID from the list.

- **Dynamic VLAN** — The RADIUS server provides the access point with the user VLAN information. The access point assigns the associated user to the related VLAN.

Note: ecCLOUD supports VLAN synchronization between APs and switches. When VLAN tagging is enabled for an SSID, the configured VLAN ID is automatically "pushed" by ecCLOUD to the attached switch port. This enables the VLAN-tagged traffic from the AP to be accepted by the switch port and avoids any loss of connectivity.

- **Limit upload rate** — Enables rate limiting of traffic from the SSID interface as it is passed to the wired network. You can set a maximum rate in Kbytes per second. (Range: 256-10048576 Kbytes per second; Default: OFF)

- **Limit download rate** — Enables rate limiting of traffic from the wired network as it is passed to the SSID interface. You can set a maximum rate in Kbytes per second. (Range: 256-10048576 Kbytes per second; Default: OFF)

- **OpenRoaming** — Available when WPA2-EAP security is selected, OpenRoaming (Hotspot 2.0) provides a standard for public-access Wi-Fi networks to support seamless roaming between wireless networks. A OpenRoaming AP advertises its public Wi-Fi capabilities and services so that clients can decide if they want to connect to the network. (Default: Disabled)

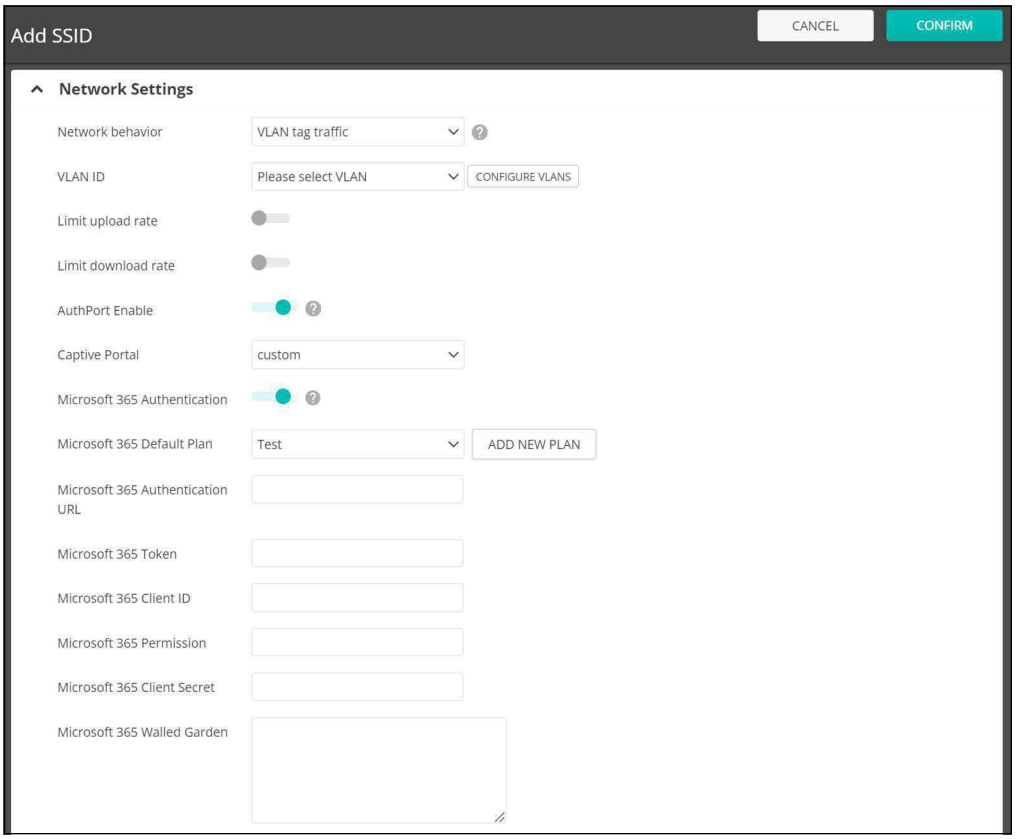
  - **Choose Profile** — Selects a configured profile to apply to the wireless network.

  - **Configure OpenRoaming** — Click to access the OpenRoaming profile settings page. See "OpenRoaming" on page 206 for profile configuration.

- **AuthPort Enable** — When this option is enabled, Wi-Fi users are asked to authenticate against a configurable ecCLOUD hosted account database before they are granted Internet access. The AuthPort add-on must be enabled for this option to be activated (see "Using the AuthPort Add-On" on page 75).

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (170/301) 3675/4726

Figure 172: Enabling Microsoft 365 Authentication



- **Captive Portal** — Choose a captive portal that includes the Microsoft login button (see "Captive Portal" on page 81).
- **Microsoft 365 Authentication** — Administrators can enable Microsoft 365 Authentication.
- **Microsoft 365 Default Plan** — Associates the billing plan consumed when the client is associated and authenticated. Choose an existing plan from the list or add a new plan.
- **Microsoft 365 Authentication URL** — Sets the endpoint for the Microsoft 365 authentication server.
- **Microsoft 365 Token** — Sets token for Microsoft 365 authorization.
- **Microsoft 365 Client ID** — The Application (client) ID assigned to your app by the Microsoft Entra admin center – App registrations experience.
- **Microsoft 365 Permission** — Specifies reading and writing permissions to the Microsoft 365 authorization server.
- **Microsoft 365 Client Secret** — Sets the client secret for Microsoft 365 authorization.

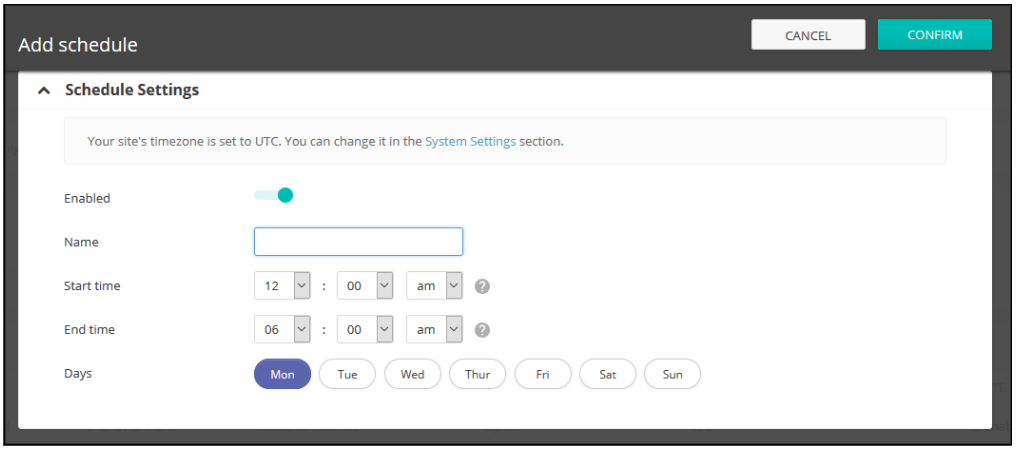
1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - Termo de Referência_029_2025_Aquisição de Access Point_assinado (171/301) 1676/4726

- **Microsoft 365 Walled Garden** — Specifies the walled garden during the Microsoft 365 login flow.
- **Proxy ARP** — When Proxy ARP is enabled, the AP maintains its own ARP lookup table and replies to ARP requests on behalf of downstream stations, avoiding network inefficiencies. This feature is automatically enabled when client isolation is disabled, and disabled when client isolation is enabled. The feature cannot be configured manually. Proxy ARP is supported when the network behavior is “Bridge to Internet” or “VLAN Tag Traffic.”

Setting Wireless Schedules

Configuring wireless schedules enables the AP radios to be turned on and off at specified times. The scheduling rules apply to all 2.4 GHz, 5 GHz, and 6 GHz interfaces on all site APs. Click the “Add Schedule” button to create a wireless schedule.

Figure 173: Adding a Wireless Schedule



The following items are displayed on the Add schedule page:

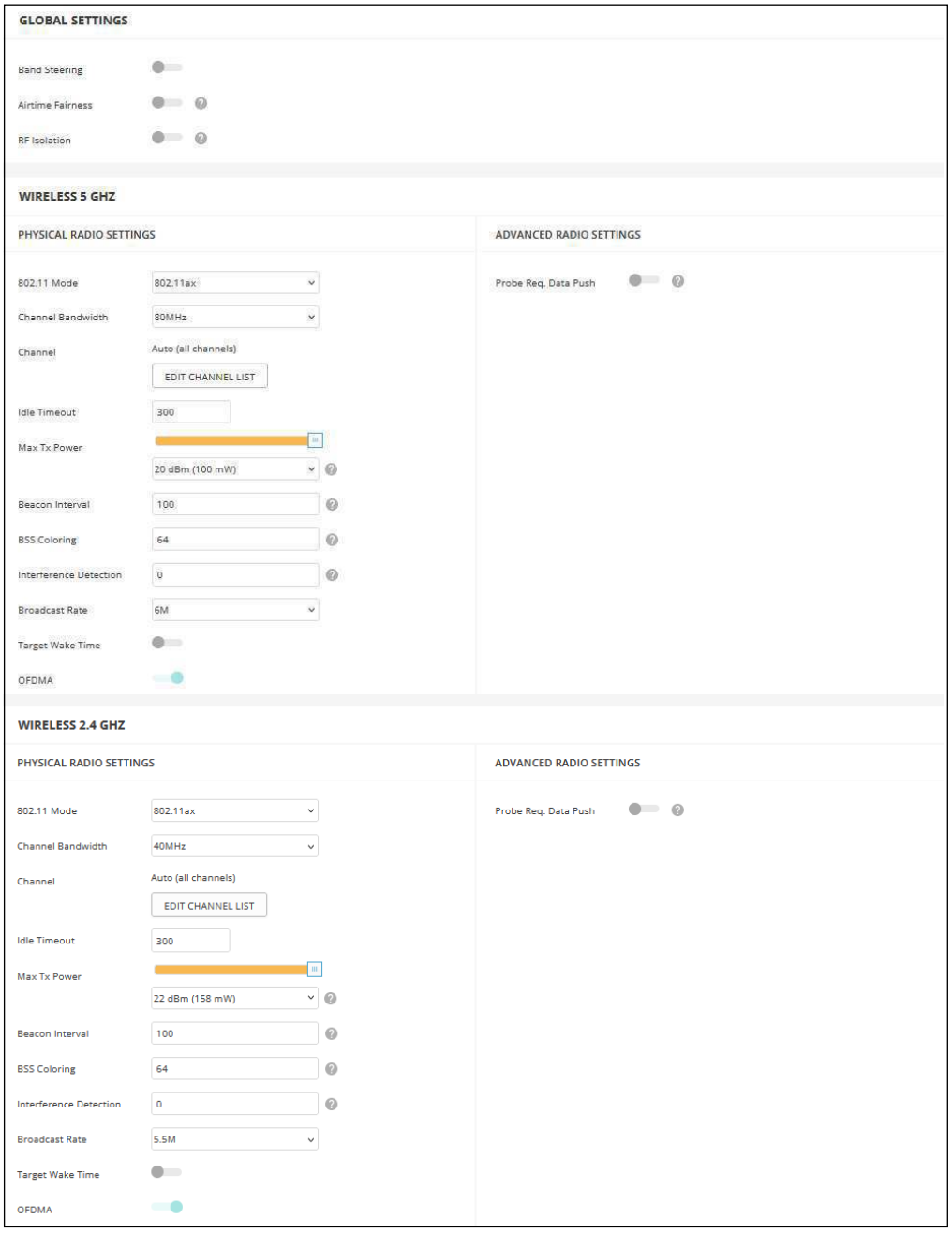
- **Enabled** — Makes the defined schedule active. (Default: Enabled)
- **Name** — A text string to identify the schedule.
- **Start time** — The time that you want the radios to be turned on.
- **End Time** — The time that you want the radios to be turned off.
- **Days** — The selected days of the week on which to apply the schedule.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo processo licitatório 029_2025_pdf (172/301) 3675/4746

Radio Settings

On the "WiFi Access" page, click the "Radio Settings" tab to configure 6 GHz, 5 GHz, and 2.4 GHz radio settings. Note that settings apply to all configured SSID interfaces.

Figure 174: WiFi 6 Radio Settings



1Doc: Protocolo 1.943/2025 | Anexo Administrativo_procesoDiscovery_2025_0236227.pdf (173/301) 1676/4746

The following items are displayed on the Radio Settings tab. Note that configuration options apply to both the 5 GHz and 2.4 GHz radios unless otherwise indicated.

Global Settings

- **Band Steering** — When enabled, clients that support 2.4 GHz, 5 GHz, and 6 GHz are first connected to the 6 GHz radio. This feature helps balance the client load over the two radio bands. Note that both radios must have configured SSIDs that match for this feature to fully operate. (Default: Disabled)

- **Airtime Fairness** — Enabling this feature improves the overall performance of the wireless network. (Default: Disabled)

- **RF Isolation** — When enabled, clients are isolated between different radio cards.

Physical Radio Settings

- **802.11 Mode** — Defines the radio operation mode.

  - **Radio 6 GHz** — Default: 11ax; Options: 11ax, 11be

  - **Radio 5 GHz** — Default: 11ax; Options: 11a, 11a+n, 11ac+a+n, 11ax, 11be

  - **Radio 2.4 GHz** — Default: 11ax; Options: 11ax, 11be

- **Channel Bandwidth** — The basic Wi-Fi channel bandwidth is 20 MHz, but by bonding channels together to create 40 MHz, 80 MHz, 160 MHz, and 320 MHz channels, higher data transmission rate can be achieved. However, selecting larger channel bandwidths reduces the number a radio channels available. The available channel bandwidth is dependent on the 802.11 Mode.
  (Default: 20 MHz on 2.4 GHz Radio, 80 MHz on 5 GHz and 6 GHz Radio; Options: 20 MHz, 40 MHz, 80 MHz, 160 MHz, and 320 MHz)

  - **20MHz** — For 802.11b+g+n and 802.11ax

  - **40MHz** — For 802.11b+g+n, 802.11a, 802.11a+n, 802.11ac+a+n and 802.11ax

  - **80MHz** — For 802.11ac+a+n and 802.11ax

  - **160MHz** — (Supported on EAP104 5 GHz radio, OAP101 5 GHz radio, and OAP101-6E 5 GHz and 6GHz radios) For 802.11ac+a+n and 802.11ax

  - **320MHz** — (Supported on EAP105) For 802.11be

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_procesoDistancia_2025_pdf (174/301) 1679/4726

- **Channel** — The radio channel that the access point uses to communicate with wireless clients. The available channels are dependent on the radio, Channel Bandwidth, and Regulatory Country settings. You can also click the "Edit Channel List" button to select specific available channels to use for each radio interface.

  Selecting Auto enables the access point to automatically select an unoccupied radio channel. (Default: Auto)

Figure 175: 5 GHz Radio Channels

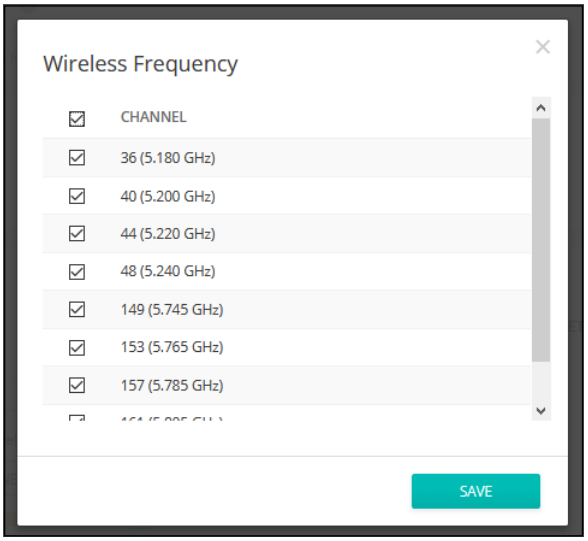
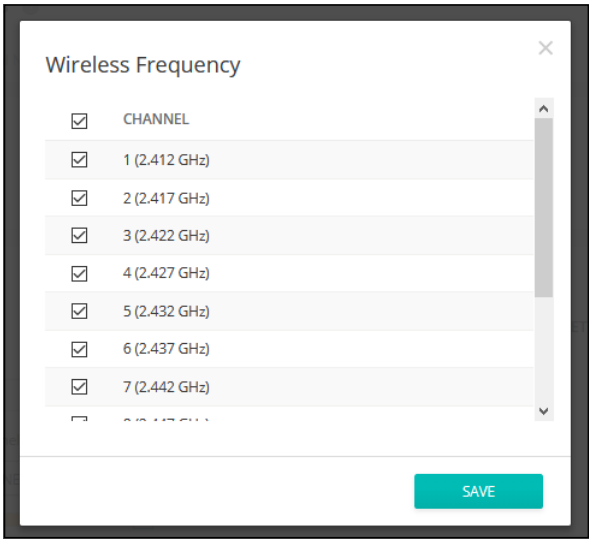


Figure 176: 2.4 GHz Radio Channels



- **Idle Timeout** — The maximum a connection can remain inactive before it is closed. (Default: 300 seconds)

- **Max Tx Power** — Adjusts the maximum power of the radio signals transmitted from the access point. The higher the transmission power, the farther the

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_procesoDisciplinario_2025_0236227.pdf (175/301) 3600/4726

transmission range. Power selection is not just a trade-off between coverage area and maximum supported clients. You also have to ensure that high-power signals do not interfere with the operation of other radio devices in the service area. (The range of power settings and defaults are dependent on the AP model and the Regulatory Country setting.)

- **Beacon Interval** — The rate at which beacon signals are transmitted from the access point. The beacon signals allow wireless clients to maintain contact with the access point. They also carry power-management and other information. (Range: 100-1024 TUs; Default: 100 TUs)

- **BSS coloring** — In 802.11ax (Wi-Fi 6) mode, BSS coloring allows nearby APs operating at the same frequency to identify traffic belonging to their own Basic Service Set (BSS). The BSS coloring enables Wi-Fi 6 networks to operate more efficiently in high-density environments where neighboring AP and client transmissions overlap. Assign a color value (a number from 1 to 63) to identify the radio BSS, or enter value 64 to allow the AP to randomly select a color value. (Range: 1-63, 64 random, Default: 64)

- **Broadcast Rate** — Allows a limit to be placed on the wireless bandwidth consumed by broadcast packets.

  - **Radio 6 GHz** — Options: 6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M; Default: 6M

  - **Radio 5 GHz** — Options: 6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M; Default: 6M

  - **Radio 2.4 GHz** — Options: 5.5M, 6M, 9M, 11M, 12M, 18M, 24M, 36M, 48M, 54M; Default: 5.5M

- **Target Wake Time** — In 802.11ax (Wi-Fi 6) mode, the AP can allow clients to request a specific Target-Wakeup Time (TWT) to transmit or receive frames, rather than rely on periodic beacons. This feature enables client devices to have much longer sleep states and results in significant power savings. In addition, the AP can control and schedule client TWTs to both manage contention in the network and accommodate delay-sensitive traffic. (Default: Disabled)

- **OFDMA** — The 802.11ax (Wi-Fi 6) mode supports Orthogonal Frequency Division Multiple Access (OFDMA) and this cannot be disabled.

Advanced Radio Settings

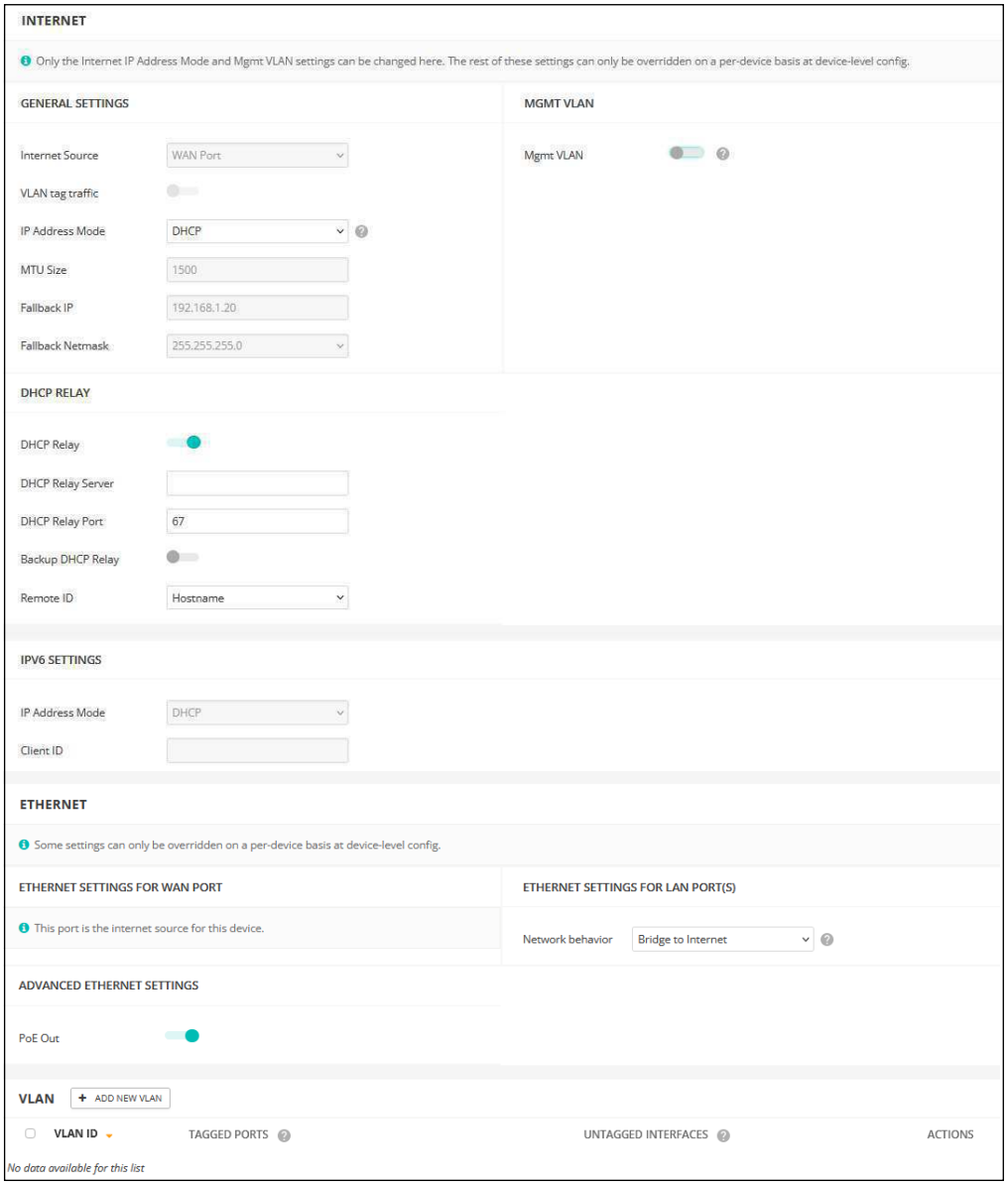
- **Probe Req. Data Push** — Enable Client Probe Request Data Push for this radio. When enabled, the radio will push client probe request data in JSON format to your specified URL.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - Termo de Referência_processo_licitatorio_029_2025_pdf (176/301) 3689/4726

General Networking Settings

On the "WiFi Access" page, click the "General Networking" tab to configure Internet, Ethernet ports, and VLAN settings for all devices in a site. Some items on this page only display the current setting, they cannot be configured. These settings can only be overridden at the device-level configuration.

Figure 177: General Networking Settings

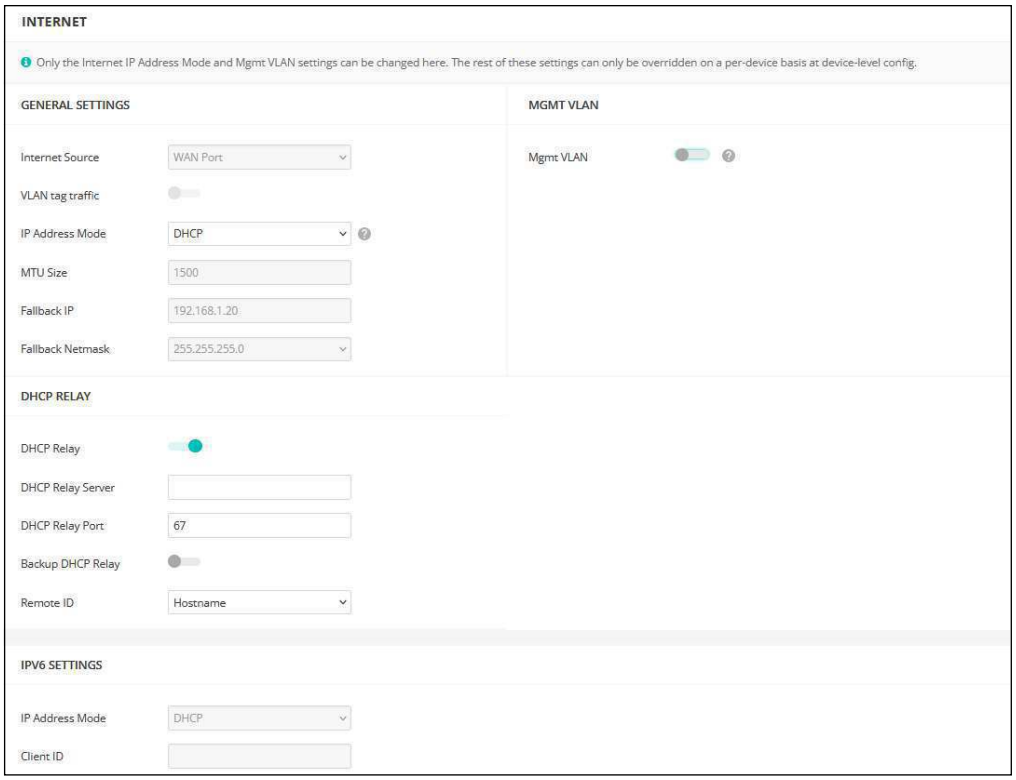


1Doc: Protocolo 1.943/2025 | Anexo Administrativo processo licitatório 029_2025_pdf (177/301) 3680/4746

Internet Settings

Note that only the Internet IP Address Mode and Management VLAN settings can be changed on this page. These rest of these settings can only be overridden on a per-device basis at device-level configuration.

Figure 178: Internet Settings



The following items are displayed on this page section:

General Settings

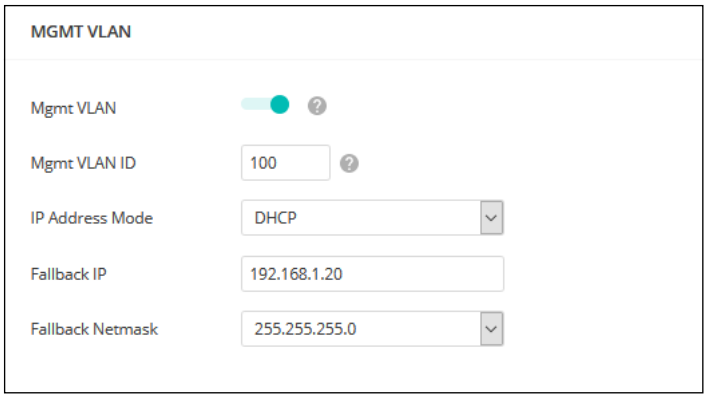
- **Internet Source** — The interface on devices used to access the Internet.
- **VLAN tag traffic** — Enable to activate tagging on this interface and choose a tagging ID value between 2 and 4094, inclusive.
- **IP Address Mode** — The method used to provide an IP address for the Internet access port. (Options: DHCP, Use Device's Settings; Default: DHCP)
  - **DHCP** — Enables DHCP on the Internet Source interface.
  - **Use Device's Settings** — Select this option if you plan on assigning static IPs to your devices prior to registration. Also choose this option if you are mixing static IP and DHCP-based modes. By default, all devices will use DHCP unless configured otherwise.
- **MTU Size** — Sets the size of the maximum transmission unit (MTU) for packets sent on this network.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo Técnico | Processo Licitatório 029_2025_Pregão 027.pdf (178/301) 3683/4746

- **Fallback IP** — This IP address is used if you cannot connect to the device IP address.
- **Fallback Netmask** — The network mask associated with the fallback IP address.

MGMT VLAN Settings

Figure 179: Management VLAN Settings



- **Mgmt VLAN** — Select this option to enable a management VLAN on site devices. Once you enable this option, you will no longer be able to access devices on any of the built-in the local networks (like 192.168.2.1 for example). You will only be able to access devices from the specified VLAN network. If a device's IP mode is set to DHCP, it will also request a new IP address in the subnet range assigned to the VLAN network.
- **Mgmt VLAN ID**— Specifies the ID of the management VLAN.
- **IP Address Mode** — The method used to provide an IP address for a device over the Management VLAN. (Options: DHCP, Static IP; Default: DHCP)
  - **DHCP** — Enables DHCP on the management VLAN.
  - **Static IP** — Sets a static IP to access site devices over the management VLAN. Configure an IP address, subnet mask, and default gateway address.
- **Fallback IP** — The IP address to use to connect to a device over the management VLAN if the DHCP-assigned address cannot be reached.
- **Fallback Netmask** — The network mask associated with the fallback IP address.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (179/301) 3682/4726

DHCP Relay Settings

When DHCP relay is enabled, APs act as an agent for all clients and sends all broadcast DHCP requests directly to a specified DHCP server. The DHCP server IP address and port must be configured, and optionally a backup server.

Figure 180: DHCP Relay

The following items are displayed on this page:

- **DHCP Relay** — Enables the DHCP relay feature on the AP.
- **DHCP Relay Server** — Specifies the IP address of the DHCP server.
- **DHCP Relay Port** — Specifies the port of the DHCP server.
- **Backup DHCP Relay** — Optionally specifies a backup DHCP server IP address and port to use if there is no response from the primary server.
- **Remote ID** — Use the hostname as the remote ID, or manually configure a text string as the remote ID.

IPV6 Settings

Figure 181: IPv6 Settings

The following items are displayed on this section of the page:

- **IP Address Mode** — The method used to provide an IPv6 address for the Internet access port. (Default: DHCP; Options: DHCP, Static IP)
  - **DHCP** — If you configure DHCP, the Client ID must be specified.
    - **Client ID** — Manually enter the client ID for the DHCP client.

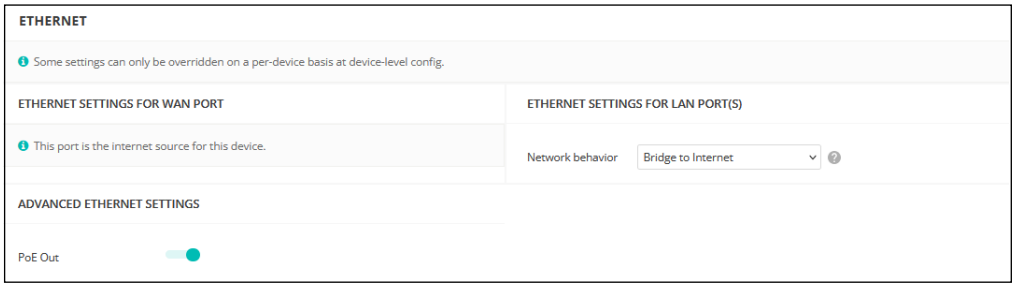
1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (180/301) 3685/4746

- **Static IP** — To configure a static IPv6 address for the Internet access port, the following items must be specified.
  - **IP Address** — Specifies an IPv6 address for the access point. An IPv6 address must be configured according to RFC 2373 using 8 colon separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
  - **Default Gateway** — The IPv6 address of the default gateway, which is used if the requested destination address is not on the local subnet.
  - **DNS** — The IPv6 address of Domain Name Servers on the network. A DNS maps numerical IPv6 addresses to domain names and can be used to identify network hosts by familiar names instead of the IPv6 addresses. If you have a DNS server located on the local network, type the IPv6 address in the text field provided.

Ethernet Settings

This page section shows basic Ethernet settings for site APs. These settings can only be overridden on a per-device basis at device-level configuration.

Figure 182: Ethernet Settings



The following items are displayed on this page section:

Ethernet Settings for WAN Port

By default, the WAN port interface is set as the Internet source and the following message is displayed: “This port is the Internet source for devices in this site.”

If more than one interface is connected to the Internet, only the last configured interface is used.

Ethernet Settings for LAN Port(s)

- **Network Behavior** — Shows the network connection method (that is, the manner in which the LAN ports are used).

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pregao_027.pdf (181/301) 3686/4746

Advanced Ethernet Settings

- **PoE Out** — Enables the PoE Out feature when the PoE source is detected as 802.3at, otherwise the PoE Out feature is disabled. When set to "Off," PoE Out is always disabled.

VLAN Settings

The access point can employ VLAN tagging to control access to network resources and increase security. VLANs separate traffic passing between the access point, associated clients, and the wired network. You can create up to 12 VLAN tagged networks.

VLANs (virtual local area networks) are turned off by default. If turned on they will automatically tag any packets passed to Ethernet ports from the relevant VAP (virtual access point). Note also that specific VAPs can enable or disable VLAN tagging (see "Adding an SSID" on page 162).

Note the following points about the access point's VLAN support:

- If an Ethernet LAN port on the access point is assigned a VLAN ID, any traffic entering that port must be also tagged with the same VLAN ID.
- Wireless clients associated to the access point can be assigned to a VLAN. Wireless clients are assigned to the VLAN for the VAP interface with which they are associated. The access point only allows traffic tagged with correct VLAN IDs to be forwarded to associated clients on each VAP interface.
- When VLAN support is enabled on the access point, traffic passed to the wired network is tagged with the appropriate VLAN ID. When an Ethernet port on the access point is configured as a VLAN member, traffic received from the wired network must also be tagged with the same VLAN ID. Received traffic that has an unknown VLAN ID or no VLAN tag is dropped.
- When VLAN support is disabled, the access point does not tag traffic passed to the wired network and ignores the VLAN tags on any received frames.

Note: Before enabling VLAN tagging on the access point, be sure to configure the attached network switch port to support tagged VLAN frames for the VLAN IDs configured on the access point. Otherwise, connectivity to the access point will be lost when you enable the VLAN feature.

Figure 183: VLAN Settings

The following items are displayed on this page section:

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_procesoDigitalizacion_029_20252026227.pdf (182/301) 3685/4746

- **VLAN ID** — The identifier assigned to the VLAN. (Range: 2-4094)
- **Tagged Ports** — The Ethernet ports assigned to the VLAN. Options include WAN port or LAN port(s).
- **Untagged Interfaces** — Click the "Configure SSIDs" link to open the Wireless SSID tab. Then edit or create an SSID interface to be a member of the specified VLAN (see "Adding an SSID" on page 162).
- **Actions** — Click and select to edit or delete a configured VLAN.

Adding a VLAN

Click the "Add New VLAN" button to create a VLAN.

Figure 184: Adding a VLAN

The following items are displayed on this page section:

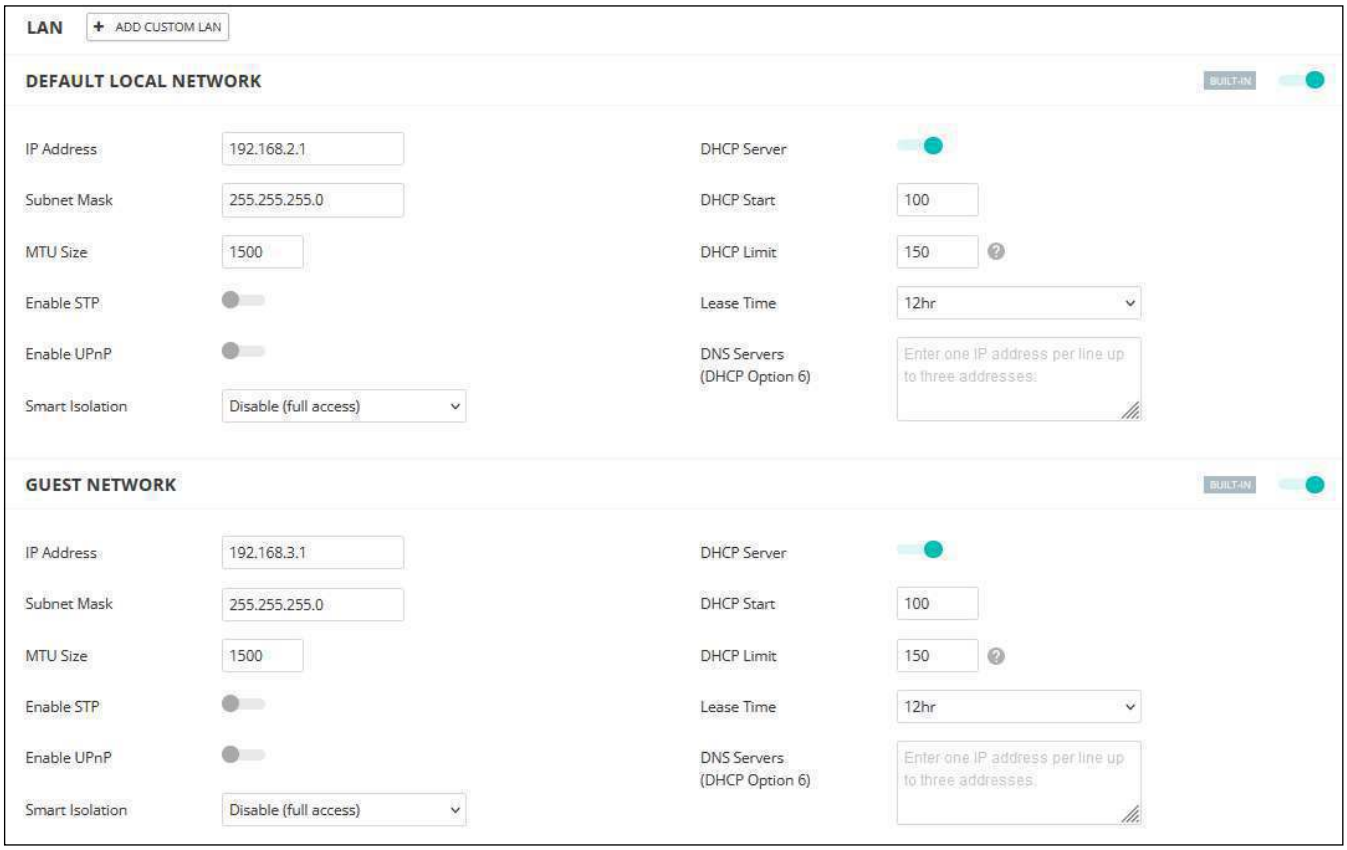
- **VLAN ID** — The VLAN identifier to be assigned. (Range: 2-4094)
- **Ports** — The Ethernet ports assigned to the VLAN. Options include WAN port or LAN port(s).

1Doc: Protocolo 1.943/2025 | Proexad... 3688/4726

Local Network Settings

The Local Network tab configures settings for the default LAN network, guest network, and other custom networks.

Figure 185: Local Network Settings



The following items are displayed on this page:

- **Add Custom LAN** — Click this button to create a additional networks with their own custom settings. You can create up to 10 custom LANs.
- **IP Address** — Specifies the IP address for the local network or guest network. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. (Default: 192.168.2.1)
- **Subnet Mask** — Indicates the local subnet mask. (Default: 255.255.255.0)
- **MTU Size** — Sets the size of the maximum transmission unit (MTU) for packets sent on this network. (Default: 1500)
- **Enable STP** — Enables or disables processing of Spanning Tree Protocol messages. (Default: Disabled)

1Doc: Protocolo 1.943/2025 | Anexo Administrativo | Processo Licitatório 029_2025_Page 27.pdf (184/301) 3689/4726

- **Enable UPnP** — Enables or disables Universal Plug-and-Play broadcast messages. (Default: Disabled)
- **Smart Isolation** — Enables network traffic to be restricted to the specified network:
  - **Disable (full access)** — There is no traffic isolation. Clients can access the Internet and other devices on the local LAN. This is the option to choose if you trust the clients that will be connecting to your network.
  - **Internet access only** — Traffic from this network can only be routed to and from the Internet. This is the option to choose for hotspot users or users connecting to a guest network.
  - **LAN access only** — Traffic from this network is restricted to local LAN devices only.
  - **Internet-only (strict)** — This is the same as "Internet access only," but with the additional restriction that users cannot access resources or devices on any private network (192.168.0.0, 172.16.0.0, 10.0.0.0, etc.). This is useful if an AP is “double NAT’ed” and the network upstream from your AP’s gateway is another private network.
- **Interface Members** — The interfaces attached to the local area network.
- **DHCP Server** — Enables/disables DHCP on this network. (Default: Enabled)
  - **DHCP Start** — First address in the address pool. (Range: 1-256; Default: x.x.x.100)
  - **DHCP Limit** — Maximum number of addresses in the address pool. (Range: 1-254; Default: 150)
  - **Lease Time** — The time period for which assigned IP addresses are valid.
  - **DNS Servers** — List up to three DNS server IP addresses, one per line.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo | Processo Licitatório 029_2025_Pregão 027.pdf (185/301) 3690/4726

Firewall Settings

Firewall filtering restricts connection parameters to limit the risk of intrusion. The firewall settings allow you to define a sequential list of rules that filter traffic based on source and destination IP addresses and ports. Ingress packets are tested against the filter rules one by one. As soon as a packet matches a rule, the configured action is implemented.

One rule, "Allow-Ping," is pre-configured to allow Ping packets from the Internet. You can enable or disable this rule, but it cannot be modified or deleted. Click the "Add Rule" button to add a new firewall rule.

Figure 186: Firewall Settings

The following items are displayed on this page:

- **Enabled** — Enables the configured firewall rule.
- **Name** — User defined name for the filtering rule. (Range: 1-30 characters)
- **Source IP** — An IPv4 address in CIDR notation. Includes an IP address followed by a slash (/) and a decimal number to define the network mask.
- **Source Port** — The source protocol port. (Range: 1-65535)
- **Destination IP** — The destination IPv4 address.
- **Destination Port** — The destination protocol port. (Range: 1-65535)
- **Target** — The action to take when the configured rule matches a packet. (Options: Accept, Reject, Drop)
- **Family** — Specifies IPv4 or IPv6 traffic, or both. (Options: IPv4, IPv6, Any)

1Doc: Protocolo 1.943/2025 | Anexo Administrativo | Processo Licitatório 029_2025_Pregão 027.pdf (186/301) 3699/4726

- **Source** — The source interface. (Options: Any, Default Local Network, Internet, Guest Network, Hotspot Network)
- **Protocol** — Defines the protocol type of packets. (Options: Any, TCP+UDP, TCP, UDP, ICMP)
- **Destination** — The destination interface. (Options: Any, Default Local Network, Internet, Guest Network, Hotspot Network)

Port Forwarding

Port Forwarding can be used to map an inbound protocol type (TCP/UDP) and port to an "internal" IP address and port. The internal (local) IP addresses are the IP addresses assigned to local devices at the edge of a network, and the external IP address is the IP address assigned to the AP interface. This allows remote users to access different servers on your local network using your single public IP address.

Remote users accessing services such as web or FTP at your local site through your public IP address, are redirected (mapped) to other local server IP addresses and TCP/UDP port numbers. For example, if you set Protocol/External Port to TCP/80 (HTTP or web) and the Destination IP/Destination Port to 192.168.3.9/80, then all HTTP requests from outside users are forwarded to 192.168.3.9 on port 80. Therefore, by just using your external IP address provided by your ISP, Internet users can access the services they need at the local addresses to which you redirect them.

The more common TCP service port numbers include: HTTP: 80, FTP: 21, Telnet: 23, and POP3: 110.

Figure 187: Port Forwarding

The following items are displayed on this page:

- **Enabled** — Enables port forwarding.
- **Name** — User-defined name. (Range: 1-30 characters)
- **Protocol** — Set the protocol type to which port forwarding is applied. (Options: TCP, UDP, TCP+UDP)
- **External Port** — The Internet traffic TCP/UDP port number. (Range: 1-65535)
- **Destination IP** — The destination IP address on the local network.
- **Destination Port** — The destination protocol port. (Range: 1-65535)

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - Termo de Referência_pregão_Licitação_029_2025_pdf (187/301) 3690/4746

ARP Inspection

ARP Inspection is a security feature that validates the MAC Address bindings for Address Resolution Protocol packets. It provides protection against ARP traffic with invalid MAC-to-IP address bindings, which forms the basis for certain "man-in-the middle" attacks. This is accomplished by intercepting all ARP requests and responses and verifying each of these packets before the local ARP cache is updated or the packet is forwarded to the appropriate destination. Invalid ARP packets are dropped.

Figure 188: ARP Inspection

The following items are displayed on this page:

- **ARP Inspection** — When enabled, ARP packets are validated against ARP spoofing.
- **Force DHCP** — Allows an AP to only learn MAC/IP pair information through DHCP packets. Since devices configured with static IP address do not send DHCP traffic, any clients with static IP addresses will be blocked by APs unless their MAC/IP pair is listed and enabled in the Static Trust List.
- **Trust List Broadcast** — Lets other APs learn the trusted MAC/IP pairs to issue ARP requests.
- **Static Trust List** — Adds the MAC or MAC/IP pairs of devices that are trusted to issue ARP requests. Other network nodes can still send their ARP requests, but if their IP appears in the static list with a different MAC, their ARP requests will be dropped.

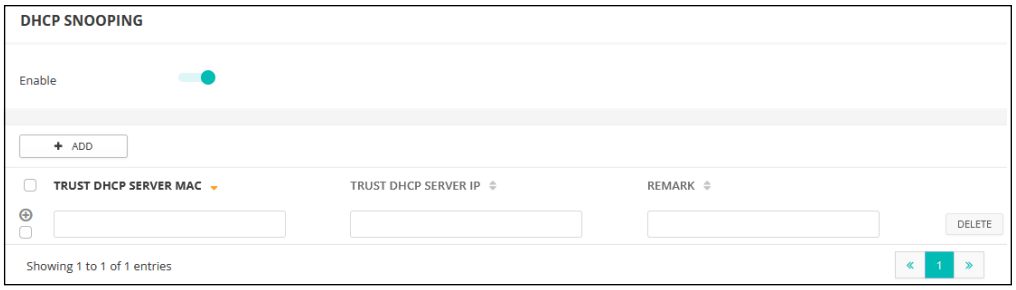
1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - Termo de Referência_processo_licitatorio_029_2025_pdf (188/301) 1693/4746

DHCP Snooping

DHCP snooping is used to validate and filter DHCP messages received by APs. When DHCP snooping is enabled, DHCP messages received from a device not listed in the DHCP snooping table are dropped.

You can add known and trusted DHCP servers to the table by specifying their MAC and IP addresses.

Figure 189: DHCP Snooping



The following items are displayed on this page:

- **Enable** — Enables DHCP Snooping.
- **Trust DHCP Server MAC** — The MAC address of a known and trusted DHCP server.
- **Trust DHCP Server IP** — The IP address of a known and trusted DHCP server.
- **Remark** — A comment relating to the DHCP server configured.

Hotspot Settings

The Hotspot settings page can configure Internet access for the general public in places such as coffee shops, libraries, and hospitals. Specific access rights may also be defined through a RADIUS server.

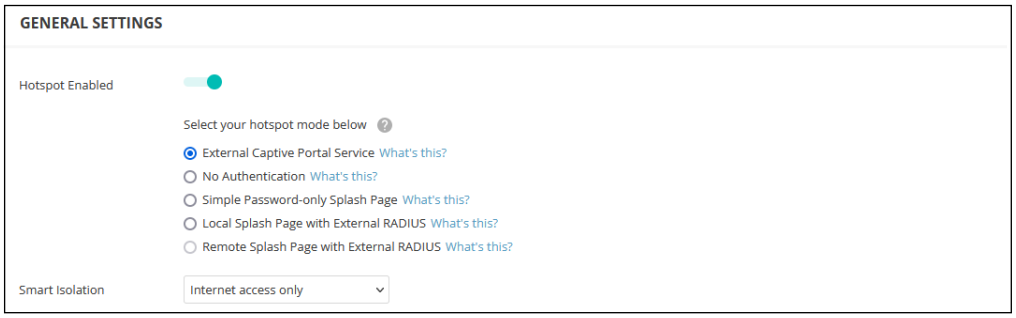
When setting up a hotspot service, you must also navigate to the wireless SSID configuration page and select “Hotspot-Controlled” as the network behavior on an SSID interface. (See “Wireless SSID Configuration” on page 161.)

General Settings

The General Settings section on the Hotspot page configures the basic hotspot mode.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo Técnico Digital Nº 029_2025_pdf (189/301) 3692/4746

Figure 190: Hotspot General Settings



The following items are displayed on this page section:

- **Hotspot Enabled** — Enables or disables the hotspot service.

  Select the hotspot mode below. (Hotspot Mode will be statically set to "External Portal" for all firmware greater than 1.1.4. Please upgrade to firmware greater than 1.1.4 in order to take advantage of this setting.)

  - **External Captive Portal Service** — This option will show the hotspot guest an externally hosted captive portal splash page and may prompt them to login, depending on how you have configured your service settings. Choose this option if you have signed up with a third-party captive portal service provider, such as Cloud4Wi or HotSpotSystem.

  - **No Authentication** — This option shows the hotspot guest your customized, locally hosted captive portal splash page, and will not require the guest to login before accessing the Internet. If you fill out the (optional) terms of service text, the guest will be required to accept these before they can access the Internet.

  - **Simple Password-only Splash Page** — This option will show the hotspot guest your customized, locally hosted captive portal splash page, and will require them to enter a simple password to login and access the Internet. If you fill out the (optional) terms of service text, the guest will be required to accept these before they can access the Internet.

  - **Local Splash Page with External RADIUS** — This option shows the hotspot guest your customized, locally hosted captive portal splash page, and will require them to enter a valid RADIUS user name and password to login and access the Internet. If you fill out the (optional) terms of service text, the guest will be required to accept these before they can access the Internet.

  - **Remote Splash Page with External RADIUS** — This is an AuthPort add-on feature (see "Using the AuthPort Add-On" on page 75). The hotspot will be redirected to an external splash page and authenticate with an external RADIUS server.

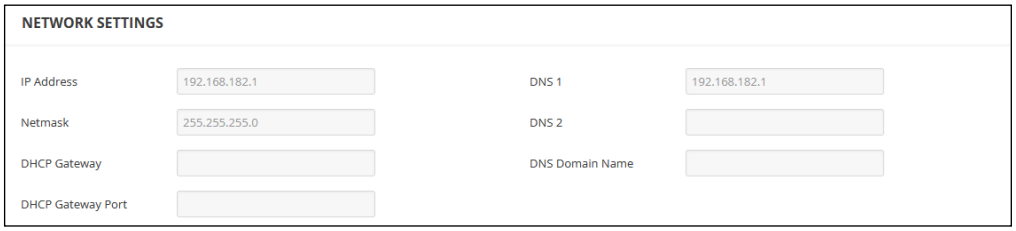
1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - Termo de Referência_processo_licitatorio_029_2025_pdf (190/301) 1695/4746

- **Smart Isolation** — Enables network traffic to be restricted to the specified network:
  - **Disable (full access)** — There is no traffic isolation. Clients can access the Internet and other devices on the local LAN. This is the option to choose if you trust the clients that will be connecting to your network.
  - **Internet access only** — Traffic from this network can only be routed to and from the Internet. This is the option to choose for hotspot users or users connecting to a guest network.
  - **LAN access only** — Traffic from this network is restricted to local LAN devices only.
  - **Internet-only (strict)** — This is the same as "Internet access only," but with the additional restriction that users cannot access resources or devices on any private network (192.168.0.0, 172.16.0.0, 10.0.0.0, etc.). This is useful if an AP is "double NAT'ed" and the network upstream from your AP's gateway is another private network.

Network Settings

The Network Settings section on the Hotspot page configures local network settings for the hotspot service.

Figure 191: Hotspot Network Settings



The following items are displayed on this page section:

- **IP Address** — Specifies the IP address for the hotspot. Valid IPv4 addresses consist of four decimal numbers, 0 to 255, separated by periods. (Default: 192.168.182.1)
- **Netmask** — Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- **DHCP Gateway** — The gateway used to access the DHCP server.
- **DHCP Gateway Port** — The UDP/TCP port used to access the DHCP server.
- **DNS 1** — The IP address of the primary Domain Name Server on the network. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_procesoDistancia_029_2025_20250227.pdf (191/301) 1696/4746

- **DNS 2** — The secondary DNS server available to DHCP clients.
- **DNS Domain Name** — The domain name used to resolve incomplete host names via the Domain Name System. (Range: 1-32 characters)

DHCP Server

The DHCP Server section on the Hotspot page configures DHCP address pool settings for the hotspot service.

Figure 192: Hotspot DHCP Server Settings

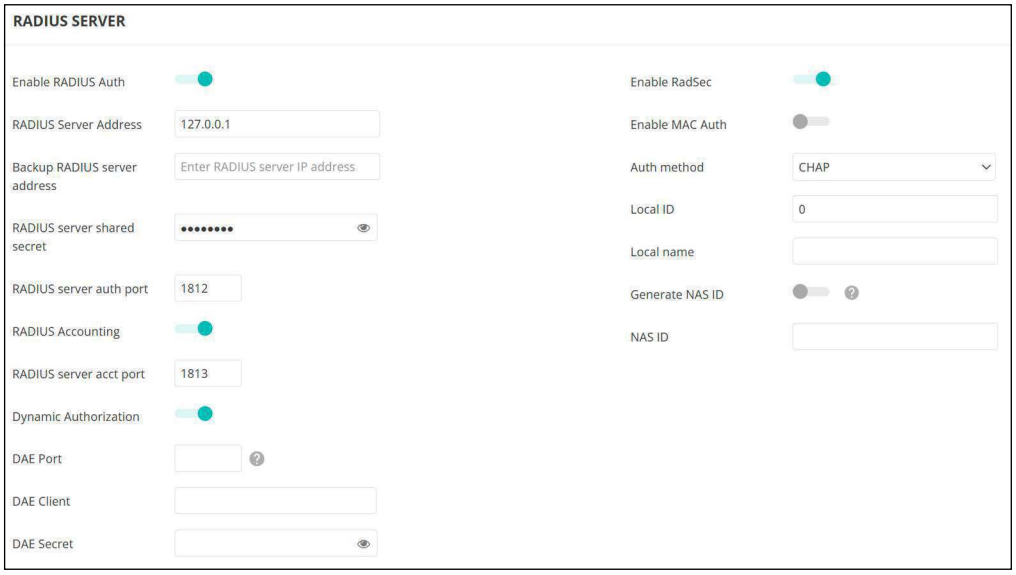
The following items are displayed on this page section:

- **DHCP Start** — Starting number of (last numeric field) in address pool. (Range: 1-254; Default: 10)
- **DHCP Limit** — Ending number of (last numeric field) in address pool. (Range: 1-245; Default: 245)
- **Lease Time** — The duration that an IP address is assigned to a DHCP client. (Range: 600-43200 seconds; Default: 3600 seconds)

RADIUS Server

The RADIUS Server section on the Hotspot page configures RADIUS server settings for the hotspot service.

Figure 193: Hotspot RADIUS Server Settings



1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (192/301) 1695/4746

The following items are displayed on this page section:

- **Enable RADIUS Auth** — Enables RADIUS authentication for clients attempting to access the captive portal.
- **RADIUS Server Address** — IP address or host name of the primary RADIUS server.
- **Backup RADIUS server address** — IP address or host name of the secondary RADIUS server.
- **RADIUS server shared secret** — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS server. Do not use blank spaces in the string. (Range: 1-255 characters).
- **RADIUS server auth port** — RADIUS server UDP port used for authentication messages. (Range: 1-65535, Default: 1812)
- **RADIUS server acct port** — RADIUS server UDP port used for accounting messages. (Range: 1-65535, Default: 1813)
- **Dynamic Authorization** — Enables Radius Dynamic Authorization Extensions, allowing administrators to dynamically disconnect online users or change authorization levels.
  - **DAE Port** — UDP port used for Dynamic Authorization requests between the RADIUS server and the access point.
  - **DAE Client** — IP address of the AP that is authorized to send Disconnect and Change of Authorization requests to the RADIUS server.
  - **DAE Secret** — Shared secret used for secure communication between the RADIUS server and the access point.
- **Enable RadSec** — An authentication and authorization protocol for transporting RADIUS datagrams over TCP and TLS. RadSec replaces UDP used in the initial RADIUS design, providing a reliable transport protocol and more extensive security for the packet payload.
- **Auth method** — Selects the encryption method to use for messages between the AP and the RADIUS server; CHAP, PAP, or MS-CHAPv2. The encryption method must match that used by the RADIUS server. (Default: CHAP)
- **Local ID** — Local RADIUS server identifier.
- **Local Name** — Local RADIUS server name
- **Generate NAS ID** — This option will generate a unique NAS ID for each device in this site.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (193/301) 1696/4746

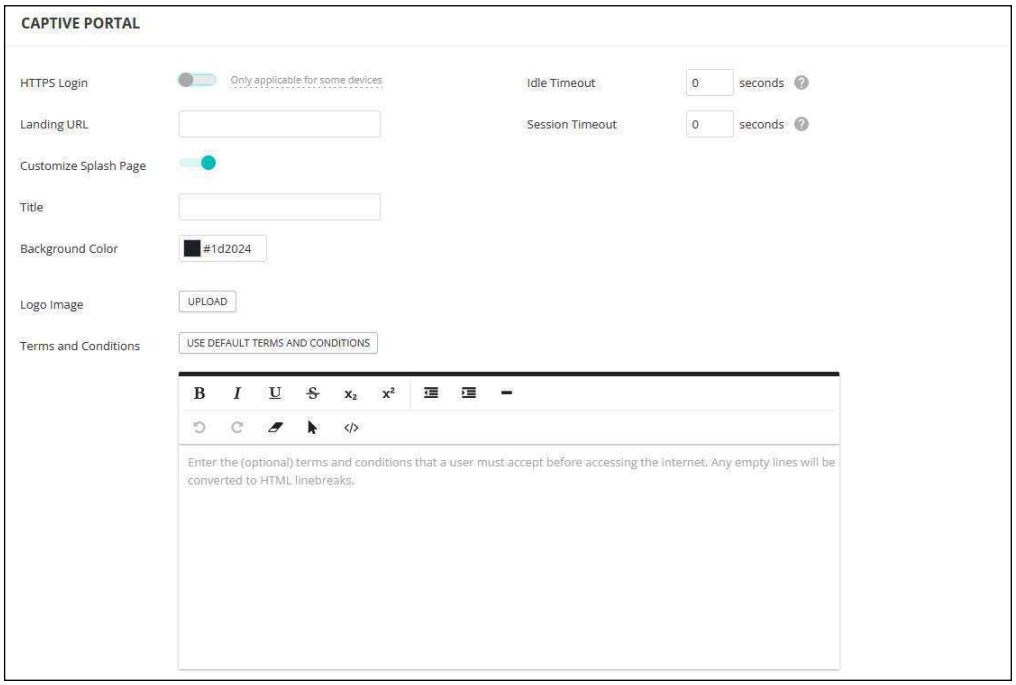
- **NAS ID** — Local RADIUS server operation identifier.

Captive Portal

The Captive Portal section on the Hotspot page configures portal details for the hotspot service.

A captive portal forces a hotspot client to access a welcome web page before gaining further access to the Internet. The welcome page may require authentication and/or payment.

Figure 194: Hotspot Captive Portal Settings



Depending on the hotspot mode selected, the following items are displayed on this page section:

Common to all Modes

- **Landing URL** — Indicates the URL to which the user is directed after logging in to the captive portal.
- **Idle Timeout** — The maximum a connection can remain inactive before it is closed. (Range: 0-86400 seconds)
- **Session Timeout** — The maximum time a client can stay logged in to the hotspot. (Range: 0-86400 seconds)

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (194/301) 3629/4726

Common to all Modes Except External Captive Portal Service and Remote Splash Page with External RADIUS

- **HTTPS Login** — Enables HTTPS for the captive portal.

Common to all Modes Except External Captive Portal Service

- **Customize Splash Page** — When enabled, fill in the information that is used to create the local captive portal welcome page.
  - **Title** — Enter the text you want to display as the title on the page.
  - **Background Color** — Click the button to select a color for the page background.
  - **Logo Image** — Click the "Upload" button to send an image file. Files are limited to a size of 1MB and the image must have a maximum height and width of 1000 pixels.
  - **Terms and Conditions** — Enter text in the window that define the captive portal terms and conditions, and then use the controls to format the text. Alternatively, click the "Use Default Terms and Conditions" button to import a generic text that you can then edit.

External Captive Portal Service Mode

- **Captive portal URL** — Host name of Internet service portal for the hotspot.
- **Captive portal secret** — The password used for logging into the hotspot.
- **Swap Octets** — Swap the values of the reported "input octets" and "output octets."

Simple Password-only Splash Page Mode

- **Splash Page Password** — The password required for users to log in and access the Internet.

Authentication Exceptions

The Auth Exceptions section on the Hotspot page configures a "walled garden" and white list for the hotspot service.

Figure 195: Hotspot Authentication Exceptions

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pag (195/301) 1020/4726

The following items are displayed on this page section:

- **Walled garden** — Enter a list of domains or IP addresses in CIDR notation that hotspot users can access before being authenticated by the captive portal. Wildcard domains can be specified in the format of *domain.com* (allow domain and all sub-domains), or *.domain.com* (only allow sub-domains).
- **Auth white list** — A list of MAC addresses that are allowed to bypass the captive portal to access the Internet.

System Settings

The System Settings page allows you to control remote management access to APs and configure NTP time servers, Telnet, Web, and SNMP management interfaces are enabled and open to access from the Internet. To provide more security, specific services can be disabled and management access prevented from the Internet.

General Settings

The General Settings section on the System Settings page can be used to configure the cloud status LED, reset button, and time zone.

Figure 196: General System Settings

The following items are displayed on this page:

- **Enable LEDs** — Only supported on ECW5211, ECWO5211, OAP100, and Spark Wave 2/SunSpot Wave 2 running 3.0.0+ firmware. The LEDs are on when a radio is enabled and operating normally.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo EC_processo_licitatorio_029_2025_pregao_027.pdf (196/301) 1029/4726

- **Enable reset button** — Enables or disables the hardware reset button. Note that the reset button cannot be disabled at the site level.

- **Timezone** — To display a time corresponding to your local time, choose one of the predefined time zones from the pull-down list.

- **Number of boot retries** — The maximum number of bootup retries before switching to the next boot bank. (Range: 1-254; Default: 3)

- **MSP Mode** — Enables the Managed Service Provider (MSP) mode that prevents end-users from accessing and modifying most device settings from user-defined user accounts. Management access from “root” and “admin” accounts still provide full access to all device settings. (Default: Disabled)

  With MSP mode enabled, service providers have the option of making specific wireless SSID settings available for user configuration by enabling the “Local Configurable” setting.

Note: Do not enable MSP Mode and “Always follow cloud configuration” (page 65) at the same time. This will cause the device configuration not to be updated to ecCLOUD properly.

- **Mgmtd Log Level** — Use the menu to select the severity of the system log level for the ecCLOUD daemon (mgmtd). Logs with the severity level you select and all logs of greater severity print. For example, if you select Debug, the logged messages include Debug, Informational, Warning, and Error. The default severity level is Informational(2). The severity can be one of the following levels:

Table 1: Management Daemon Logging Levels

Level	Severity Name	Description
4	Trace	Granular details about the system's interactions, state changes, and network communications
3	Debug	Debugging messages
2	Info	Informational messages only
1	Warn	Warning conditions (e.g., return false, unexpected return)
0	Error	Error conditions (e.g., invalid input, default used)

- **Syslog Level** — Use the menu to select the severity of the logs to print to the console. The default severity level is Informational(6). The severity can be one of the following levels:

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - Termo de Referência_processo_licitatorio_029_2025_pdf (197/301) 3000/4746

Table 2: System Logging Levels

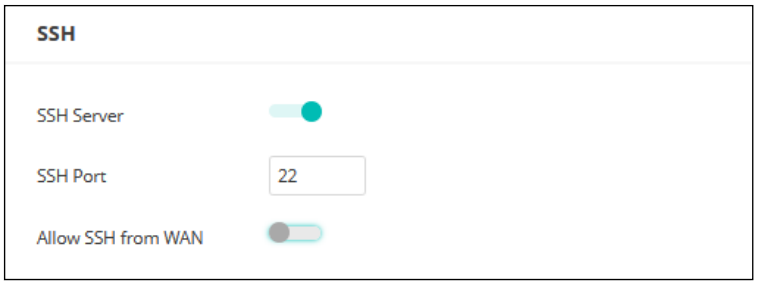
Level	Severity Name	Description
7	Debug	Debugging messages
6	Info	Informational messages only
5	Notice	Normal but significant condition, such as cold start
4	Warn	Warning conditions (e.g., return false, unexpected return)
3	Error	Error conditions (e.g., invalid input, default used)
2	Critical	Critical conditions (e.g., memory allocation, or free memory error - resource exhausted)
1	Alert	Immediate action needed
0	Emergency	System unusable

SSH

The Secure Shell (SSH) acts as a secure replacement for Telnet. The SSH protocol uses generated public keys to encrypt all data transfers passing between the access point and SSH-enabled management station clients and ensures that data traveling over the network arrives unaltered. Clients can then securely use the local user name and password for access authentication.

Note that SSH client software needs to be installed on the management station to access the access point for management via the SSH protocol.

Figure 197: SSH Server Settings



The following items are displayed on this page:

- **SSH Server** — Enables or disables SSH access to the access point. (Default: Enabled)
- **SSH Port** — Sets the TCP port number for the SSH server on the access point. (Range: 1-65535; Default: 22)
- **Allow SSH from WAN** — Allows SSH management access from the WAN.

1Doc: Protocolo 1.943/2025 | Proexad... pdf (198/301) 1003/4726

Discovery Tool

The Edgecore Discovery agent allows the AP to be discovered by other devices on the local network or over the Internet.

Figure 198: Discovery Tool Settings

The following items are displayed on this page:

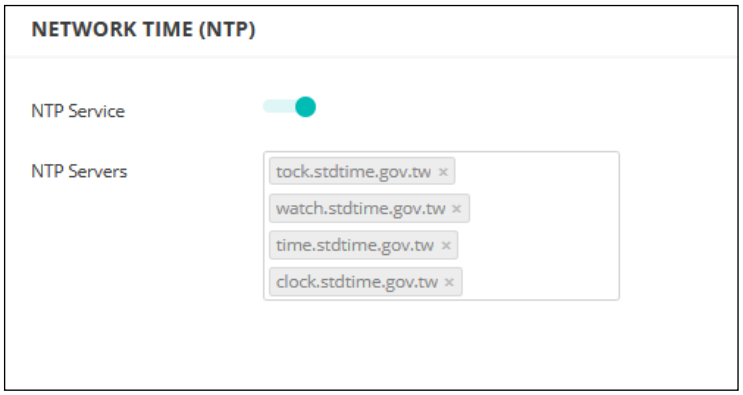
- **Discovery Tool** — Enables or disables the discovery tool. (Default: Enabled)
- **Allow over WAN** — Allows discovery tool access from the WAN.

Network Time

Network Time Protocol (NTP) allows the access point to set its internal clock based on periodic updates from a time server (SNTP or NTP). Maintaining an accurate time on the access point enables the system log to record meaningful dates and times for event entries. If the clock is not set, the access point will only record the time from the factory default set at the last bootup.

The access point acts as an NTP client, periodically sending time synchronization requests to specified time servers. The access point will attempt to poll each server in the configured sequence to receive a time update.

Figure 199: NTP Settings



The following items are displayed on this page:

- **NTP Service** — Enables or disables sending of requests for time updates. (Default: Enabled)
- **NTP Servers** — Sets the host names for time servers. The switch attempts to update the time from the first server, if this fails it attempts an update from the

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (199/301) 1002/4726

next server in the sequence. To configure additional servers, type in an entry in the blank field at the bottom of the list.

SNMP

Simple Network Management Protocol (SNMP) is a communication protocol designed specifically for managing devices on a network. It is typically used to configure these devices for proper operation in a network environment, as well as to monitor them to evaluate performance or detect potential problems.

Figure 200: SNMP Settings

The following items are displayed on this page:

- **SNMP Server** — Enables or disables SNMP on the access points. (Default: Enabled)
- **Write Community** — A community string that acts like a password and permits access to the SNMP protocol. (Range: 1-32 characters, case sensitive; Default: public)

  The default string "public" provides read-only access to the access point's Management Information (MIB) database.
- **IPv6 Write Community** — A community string for IPv6 access to the access point's Management Information (MIB) database. (Range: 1-32 characters, case sensitive; Default: private6)
- **Read Community** — A community string for read-only access to the access point's Management Information (MIB) database. (Range: 1-32 characters, case sensitive; Default: public)
- **IPv6 Read Community** — A community string for IPv6 read-only access to the access point's Management Information (MIB) database. (Range: 1-32 characters, case sensitive; Default: public6)

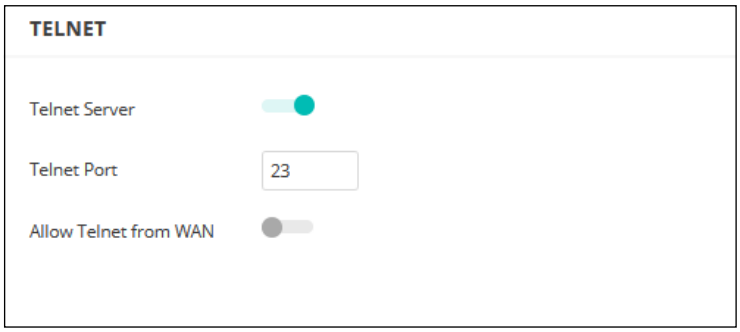
1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - Termo de Referência_processo_licitatorio_029_2025_pdf (200/301) 1005/4746

- **Trap** — Enables the sending of SNMP trap messages to a specified server. The access point sends the following trap messages: cold start, warm start, link up, and link down. (Default: Disabled)
  - **Server IP** — The IP address of the SNMP trap server that will receive the trap messages.

Telnet

Telnet is a remote management tool that can be used to configure the access point from anywhere in the network. However, note that Telnet is not secure from hostile attacks. Telnet provides access to a Linux-based interface which is used for device analysis and debugging.

Figure 201: Telnet Server Settings



The following items are displayed on this page:

- **Telnet Server** — Enables or disables Telnet access to the access point. (Default: Enabled)
- **Telnet Port** — Sets the TCP port number for the Telnet server on the access point. (Range: 1-65535; Default: 23)
- **Allow Telnet from WAN** — Allows Telnet management access from the WAN.

Web Server

A Web browser provides the primary method of managing the access point. Both HTTP and HTTPS service can be accessed independently. If you enable HTTPS, you must indicate this in the URL: https://device:port_number]

When you start HTTPS, the connection is established in this way:

- The client authenticates the server using the server's digital certificate.
- The client and server negotiate a set of security protocols to use for the connection.
- The client and server generate session keys for encrypting and decrypting data.
- The client and server establish a secure encrypted connection.
- A padlock icon should appear in the status bar for most browsers.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (201/301) 1006/4726

Figure 202: Web Server Settings

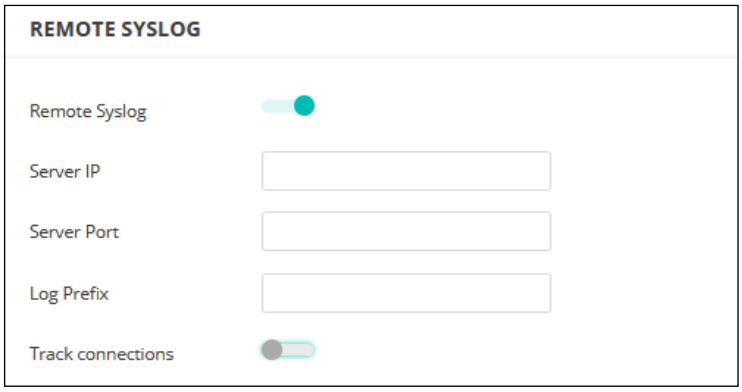
The following items are displayed on this page:

- **HTTP Port** — The TCP port to be used by the HTTP Web browser interface. (Range: 1-65535; Default: 80)
- **Allow HTTP from WAN** — Allows HTTP management access from the WAN.
- **HTTPS Port** — The TCP port to be used by the HTTPS Web browser interface. (Range: 1-65535; Default: 443)
- **Allow HTTPS from WAN** — Allows HTTPS management access from the WAN.

Remote Syslog

Use this feature to send log messages to a Syslog server.

Figure 203: Remote Log Settings



The following items are displayed on this page:

- **Remote Syslog** — Enables/disables the logging of debug or error messages to the remote logging process. (Default: Disabled)
- **Server IP** — Specifies the IP address of a remote server which will be sent syslog messages.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_procesoDistancia_029_2025_pag27.pdf (202/301) 1005/4746

- **Server Port** — Specifies the UDP port number used by the remote server. (Range: 1-65535)
- **Log Prefix** — Sets the prefix for the log file sent to the specified server. The file suffix "log" is used.
- **Track connections** — Sends wireless client connection log messages to the Syslog server.

Multicast DNS

Use this feature to enable Multicast DNS support on APs. Multicast DNS can be used on small networks that do not have a DNS server to resolve host names to multicast IP addresses.

Multicast DNS settings are available only on devices with mDNS support.

Figure 204: Multicast DNS Settings

The following items are displayed on this page:

- **MDNS** — Enables or disables multicast DNS support. (Default: Enabled)

LLDP

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices in a network. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device.

Figure 205: LLDP Settings

The following items are displayed on this page:

- **Enable** — Enables the sending of LLDP advertisements about the AP to neighboring devices in the network. (Default: Disabled)
- **Tx Interval (seconds)** — Sets the periodic transmit interval for LLDP advertisements. (Range: 5-32768 seconds; Default: 30 seconds)

1Doc: Protocolo 1.943/2025 | Anexo Administrativo processo 029_2025_pregão 027.pdf (203/301) 1006/4746

- **Tx Hold (number of time(s))** — Configures a time-to-live (TTL) value sent in the LLDP advertisements as shown in the formula below. (Range: 2-10; Default: 4)

  The time-to-live tells the receiving LLDP agent how long to retain all information pertaining to the sending device if it does not transmit updates in a timely manner.

  The TTL in seconds is based on the following rule:
  minimum value ((Tx Interval * Tx Hold), or 65535)
  Therefore, the default TTL is 4*30 = 120 seconds.

iBeacon

The AP supports the iBeacon standard based on Bluetooth Low Energy (BLE). Devices with BLE Beacons can provide location-based services to BLE clients, such as phones, that can recognize the beacon advertisements, extract the provided information, and then take actions based on the content.

Figure 206: iBeacon Settings

The following items are displayed on this page:

- **Enable** — Enables iBeacon support on the AP. (Default: Enabled)

- **UUID** — The iBeacon Universally Unique Identifier that advertises the beacon service. The UUID contains 32 hexadecimal digits in five groups, separated by hyphens.

- **Major** — The iBeacon value that is used to identify a beacon group. (Range: 0-65535)

1Doc: Protocolo 1.943/2025 | Anexo Administrativo processo licitatório 029_2025_pdf (204/301) 1009/4746

- **Minor** — The iBeacon value that is used to identify individual beacons within a group. (Range: 0-65535)
- **Tx Power** — Sets the BLE radio transmit power (supported only on EAP101 and EAP104). (Range: 5 dBm to -20 dBm; Default: 5 dBm)
- **BLE Probe Request Data Push** — Enables BLE probe request detection and sends collected data to the cloud.
- **Publish MQTT** — Sends iBeacon data to a Message Queuing Telemetry Transport broker for integration with external systems.
  - **Topic** — The MQTT topic where iBeacon data is published.
  - **Host** — The IP address or hostname of the MQTT broker. (Default: 127.0.0.1)
  - **Port** — The TCP port used for MQTT communication. (Default: 1883)
  - **Client ID** — The identifier for this AP when connecting to the MQTT broker.
  - **User Name / Password** — Optional authentication credentials for the MQTT broker.

SNMPv3 User

SNMP protocol version 3 provides secure access by account authentication and data encryption. An SNMP v3 user can be defined by clicking the Add button.

Figure 207: SNMPv3 User Settings

The following items are displayed on this page:

- **Name** — The user name used to access the SNMP service.
- **Access Auth** — Select the access permission as “Read Only” or “Write.”
- **Auth Type** — Select the hash algorithm for authentication.
- **Auth Pwd** — Configure the password for authentication.
- **Encryption Type** — Select the encryption algorithm for data packets.
- **Encryption Pwd** — Configure the password for data encryption.

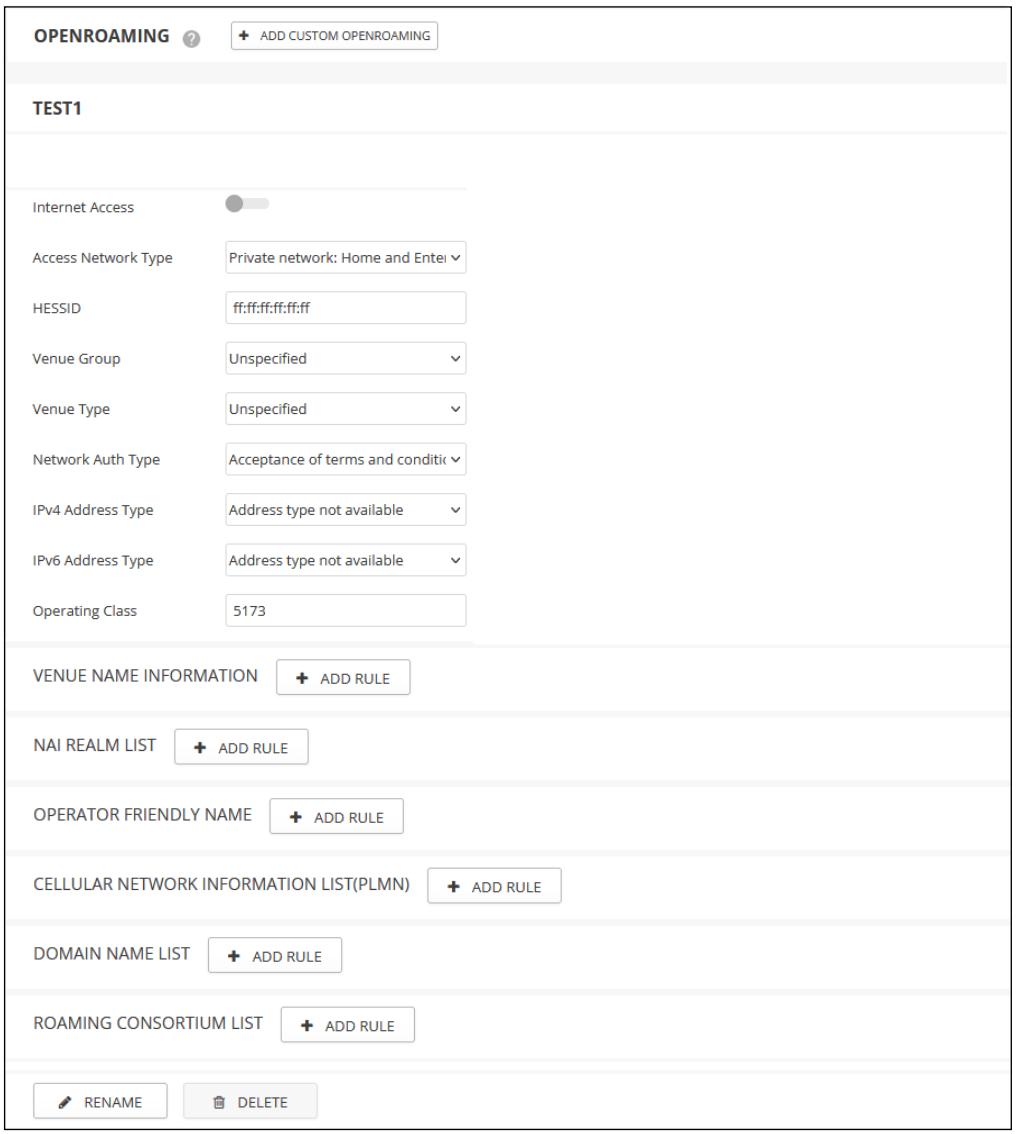
1Doc: Protocolo 1.943/2025 | Anexo Administrativo EC_processo_licitatorio_029_2025_pdf (205/301) 1638/4746

OpenRoaming

OpenRoaming provides a standard for public-access Wi-Fi networks to support seamless roaming between wireless networks. An OpenRoaming network advertises its public Wi-Fi capabilities and services so that clients can decide if they want to connect to the network.

Up to 32 OpenRoaming profiles can be configured and applied to specific wireless networks (see "OpenRoaming" under "Adding an SSID" on page 162). Click "Add Custom Openroaming" to configure a profile.

Figure 208: OpenRoaming Profile



The following items are displayed on this page:

- **Internet Access** — Enable if this network provides access to the Internet.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (206/301) 1639/4746

- **Access Network Type** — Select one from the predefined list.
  - **Private network** — Home and enterprise networks that unauthorized users cannot access.
  - **Private network with guest access** — A private network that provides for guest access. A typical example would be an enterprise network that offers guest access.
  - **Chargeable public network** — A network that is available to all users, but requires a fee.
  - **Free Public Network** — A network that is available to all users without any fees.
  - **Personal device network** — A network for peripheral connectivity in an ad-hoc mode. For example, a camera that connects to a printer.
  - **Emergency services only network** — A network that is dedicated for access to emergency services only.
  - **Test or experimental** — A network for tests or experimental work.
  - **Wildcard** — When selected, the AP will reply to clients regardless of the network type requested by the client query.
- **HESSID** — The Homogenous Extended Service Set Identifier (HESSID) for the OpenRoaming network. When configured, the HESSID (a MAC address) uniquely identifies all APs belonging to the same network.
- **Venue Group** — Identifies the general class of the venue. Select from the predefined list.
- **Venue Type** — Identifies the specific type of venue within each group.
- **Network Auth Type** — Specifies the authentication required for the network. Select an option from the predefined list. (Default: "Acceptance of terms and conditions")
- **IPv4 Address Type** — Specifies the IPv4 address type available from the network.
- **IPv6 Address Type** — Specifies the IPv6 address type available from the network
- **Operating Class** — A standard index (based on IEEE Std 802.11-2012 Annex E) that specifies the AP supported operating channels.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (207/301) 3040/4746

- **Venue Name Information** — Configures a list of up to 10 venue names.
  - **Language** — Select a language from the list. (Default: English)
  - **Name** — The name of the network venue. Multiple names can be added to the list.
  - **URL** — Specifies a URL that provides additional venue information to users.
- **NAI Realm List** — (Optional) The network access identifier (NAI) realm list identifies those service provider or other networks that are accessible through the AP. By discovering which authentication realms are supported by a network, a mobile device can selectively authenticate to its preferred network. Up to 10 identifiers can be configured.
- **Operator Friendly Name** — The name of the network operator and the specified language. Up to 10 names can be configured.
- **Cellular Network Information List (PLMN)** — (Optional) Identifies the 3GPP cellular networks available through the AP. Specifically, this field identifies the Public Land Mobile Network (PLMN) ID, comprised of the Mobile Country Code (MCC) and Mobile Network Code (MNC) of the mobile operator. Up to 10 PLMN IDs can be configured. Input the pair of MCC, MNC.
  For example: 400, 00
  MCC: Three decimal digits (000-999)
  MNC: Two (00-99) or three decimal digits (000-999)
- **Domain Name List** — Lists one or up to 10 domain names for the entity operating the AP. This is critical for OpenRoaming network selection policy, as it identifies the operator of the network. It indicates to the mobile device whether they are at a home hotspot or a visited hotspot.
- **Roaming Consortium List** — (Optional) A roaming consortium is a group of service providers (SP) with which a user's credentials can be used for authentication. Each roaming consortium is identified by an organization identifier (OI) that is assigned by the IEEE. An OI is often 24 bits in length, but can also be 36 bits. Up to 10 identifiers can be configured.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (208/301) 1943/4726

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - Termo de Referência - Processo Digital nº 029.00052026-27.pdf (209/301) 1042/4726

6 Site Terragraph Configuration

This chapter describes configuration settings for Metrolinq Terragraph units at the Site level. It includes the following sections:

1Doc: Protocolo 1.943/2025 | Anexo Administrativo processo licitatório 029_2025_pdf (210/301) 1045/4726

Metrolinq Terragraph Configuration

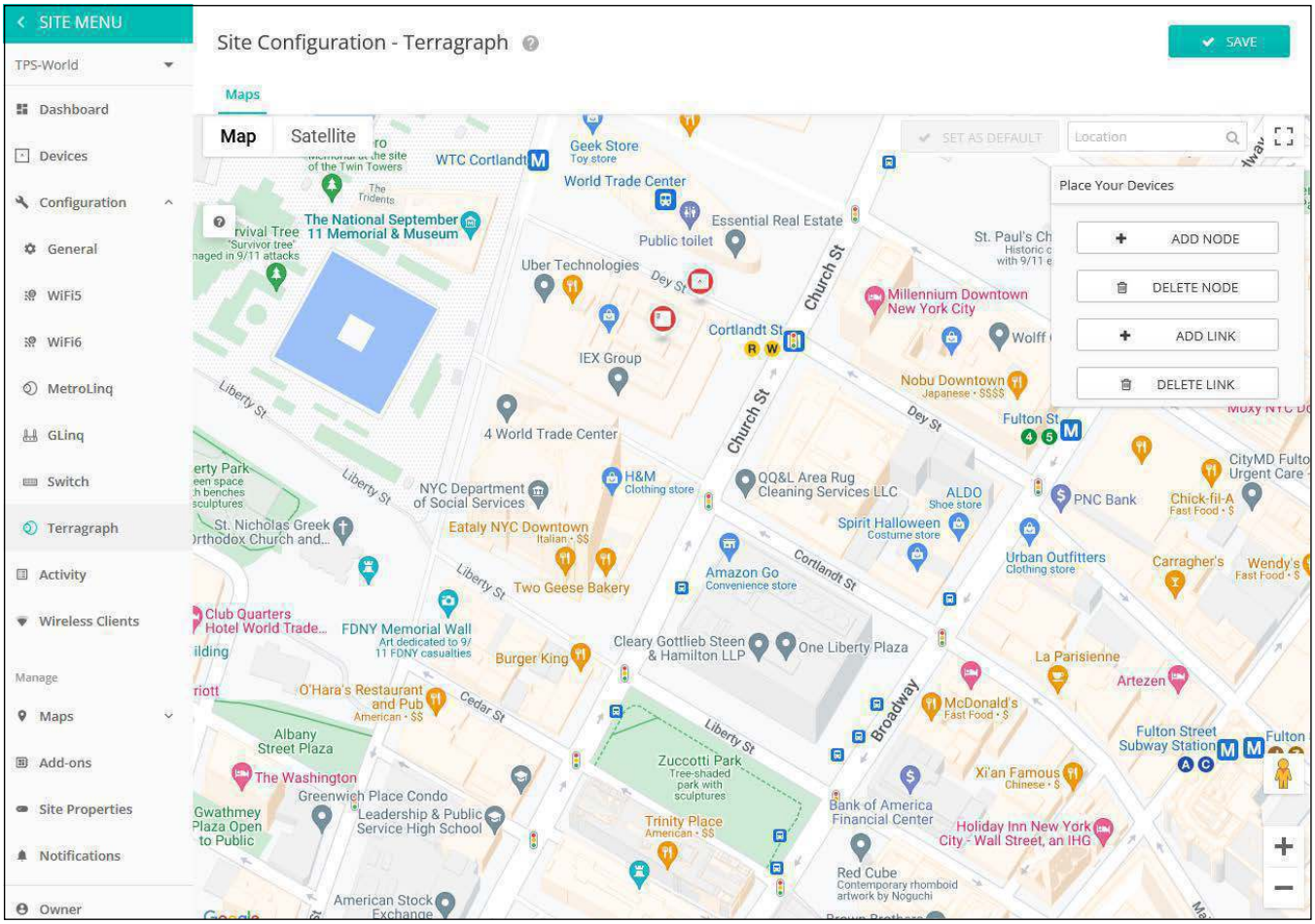
The network connectivity and topology for Metrolinq Terragraph units can be defined on the PoP node when the local controller is enabled. After defining the topology, the PoP will find the nodes and set up links automatically.

Note: When configuring Metrolinq Terragraph units, be sure to follow these points:

1. After resetting a PoP node to defaults, you should delete all nodes and links, and then re-add them to the Site Configuration page.

2. Be sure to delete all related links and nodes before you delete or move a device to another site.

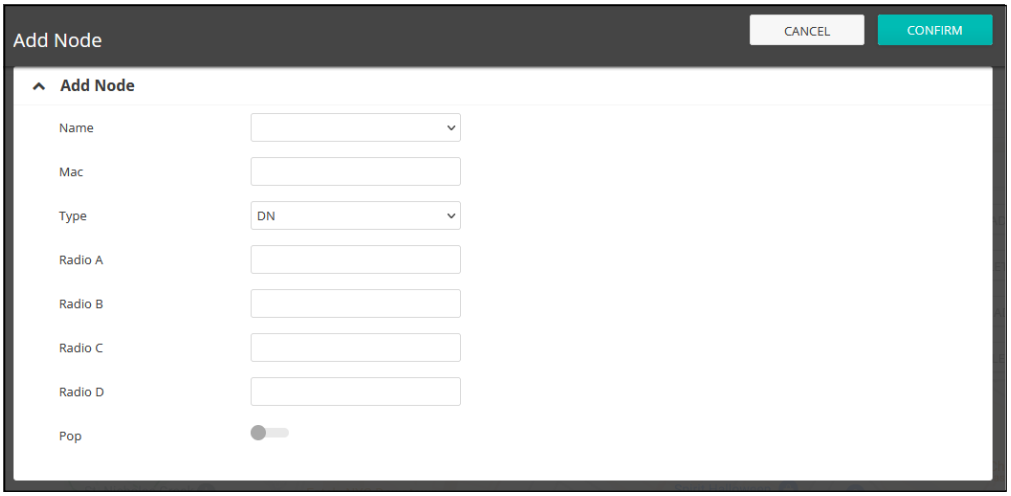
Figure 209: Site Terragraph Configuration



The Terragraph site configuration page includes these items:

- **Add Node** — Fill in correspond type and Radio MAC to add Node.

Figure 210: Add Terragraph Node

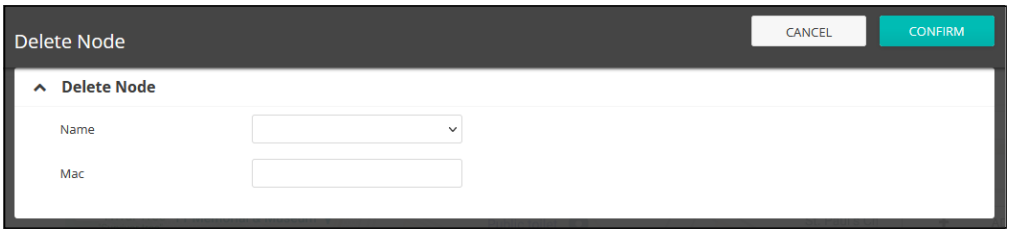


- **Name** — The name of the node. It is defined automatically based on the node type, but can be modified afterward.
- **MAC** — The system MAC address of the node. For a DN, the system MAC address can be found on the device's label or on the Dashboard tab. For a CN, use the radio MAC as the node MAC.
- **Type** — Set the node as Distribution Node (DN) or Client Node (CN).
- **Radio A/B/C/D** — The MAC addresses of the radios.
- **Pop** — Only one of the MLTG-360 devices can be the PoP node in a topology.

  Note that POP DN can only be named as "POP."

- **Delete Node** — Delete the node from the topology. You need to delete all related links before deleting a node.

Figure 211: Delete Terragraph Node

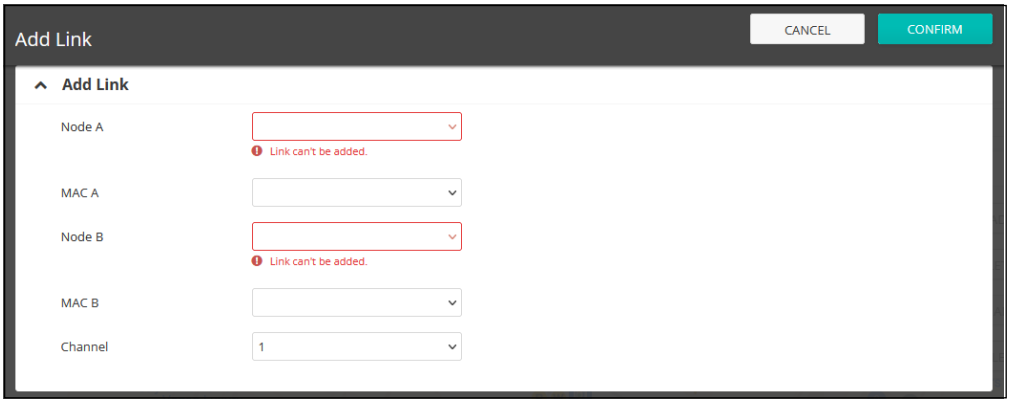


- **Name** — The name of the node.
- **MAC** — The system MAC address of the node.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_procesoDiseño_029_2025_pag (212/301) 3045/4726

- **Add Link** — Select two nodes and corresponding radio MACs to establish a link.

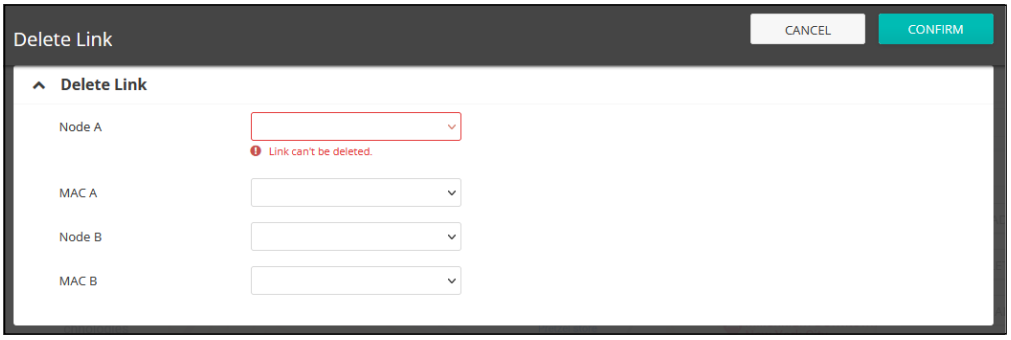
Figure 212: Add Terragraph Link



  - **Node A** — Selects the node A name.
  - **MAC A** — Selects the node A radio MAC address.
  - **Node B** — Selects the node B name.
  - **MAC B** — Selects the node B radio MAC address.
  - **Channel** — Select the working channel. Channels 1 to 4 are available.

- **Delete Link** — Select a specific node pair to delete a link.

Figure 213: Delete Terragraph Link



  - **Node A** — Selects the node A name.
  - **MAC A** — Selects the node A radio MAC address.
  - **Node B** — Selects the node B name.
  - **MAC B** — Selects the node B radio MAC address.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_procesoDeLicitacion_029_2025_pag227.pdf (213/301) 1048/4726

VLAN Settings

QinQ tagging adds a second VLAN tag to the Ethernet frame, which then contains the original VLAN tag and additional information, such as the service provider VLAN. This allows network operators to extend VLANs across multiple switches and service provider networks, creating a more scalable and flexible network architecture.

After configuring the VLANs, data traffic from the LAN side of a CN device will be encapsulated with configured S-VLAN and C-VLAN headers, and then be forwarded to the uplink of the POP node.

This feature is available for MLTG devices with firmware 1.5.0 and above.

Figure 214: Site Terragraph VLAN Settings

The following items are displayed on this page:

- **Name** — A name that identifies the VLAN configuration.
- **S-VLAN ID** — The Service VLAN, which is a VLAN that is used to differentiate traffic from different customers or services in a service provider network.
- **C-VLAN ID** — The Customer VLAN, which is a VLAN that is used to differentiate traffic from different customers in a service provider network.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo processo licitatório 029_2025_pregão 027.pdf (214/301) 3049/4746

1Doc: Protocolo 1.943/2025 | Procedimiento Administrativo Electrónico | Anexo 3 - 27292025 | Anexo 3 - 27292025.pdf (215/301) 1048/4746

7 Site SD-WAN Configuration

This chapter describes the configuration settings for SD-WAN devices at the site level. It includes the following section:

- "VPN Group Configuration" on page 217

1Doc: Protocolo 1.943/2025 | Anexo Administrativo Processo Digital 029_2025_Anexo_Administrativo_029_2025_page_27.pdf (216/301) 1029/4726

VPN Group Configuration

From the Site menu, open “Configuration” and then “SDWAN” to display the configuration options that apply to all SD-WAN devices in the same site.

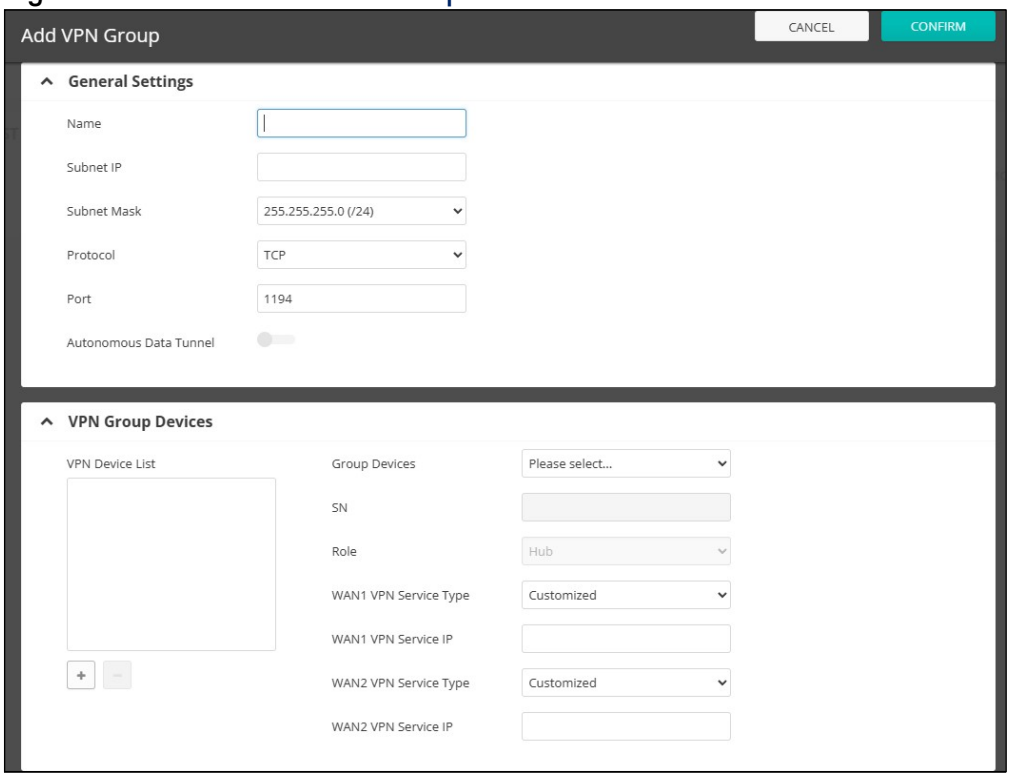
VPN Group

The VPN Group tab on the SD-WAN configuration page includes these items:

- **General Settings**
  - **Name** — Define a name for the new VPN group.
  - **Subnet IP** — Specify the virtual IP address for the VPN tunnel. It does not overlap with WAN IPs or LAN subnets of devices within the group.
  - **Subnet Mask** — Select the subnet mask of the virtual tunnel IP.
  - **Protocol** — Select TCP (default and recommended) or UDP for the VPN tunnel.
  - **Port** — The port used by Hub devices in the VPN group. Ensure no conflicts with ports in use on the Hub device.
  - **Autonomous Data Tunnel** — Enable or disable autonomous tunneling to allow independent data tunnel creation without manual intervention.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - Termo de Referência - Processo Licitatório 029_2025_page 27.pdf (217/301) 1030/4746

Figure 215: Add New VPN Group



- **VPN Group Devices**
  - **Group Devices** — Add devices to the VPN Device List by selecting from the available list.
  - **SN** — Serial Number of this site device.
  - **Role** — Devices in the VPN Group are assigned one of the following roles:
    - **Hub** — The central node that acts as a VPN server. For Hubs behind NAT, set a WAN VPN Service Type as 'Customized' with the WAN IP of the NAT router. Only one Hub is permitted per VPN Group.
    - **Spoke** — Device acting as VPN client, where Internet access is local to the site device.
    - **To Server** — Device acting as a VPN client, where Internet traffic is routed to the Hub through the VPN tunnel.
  - **WAN1/WAN2 VPN Configuration** — For Hub devices, specify service type between Customized and Domain Name., domain name, and public IP for WAN1 and WAN2. If 'Customized' is selected, manually input the service IP for the corresponding WAN. If 'Domain Name' is selected, manually input the service domain.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (218/301) 1093/4746

8 WiFi 5 Device Configuration

This chapter describes configuration settings for access points at the Device level. It includes the following sections:

1Doc: Protocolo 1.943/2025 | Anexo Administrativo processo digital 029.2025.pdf (219/301) 1032/4746

Accessing Device-Level Configuration

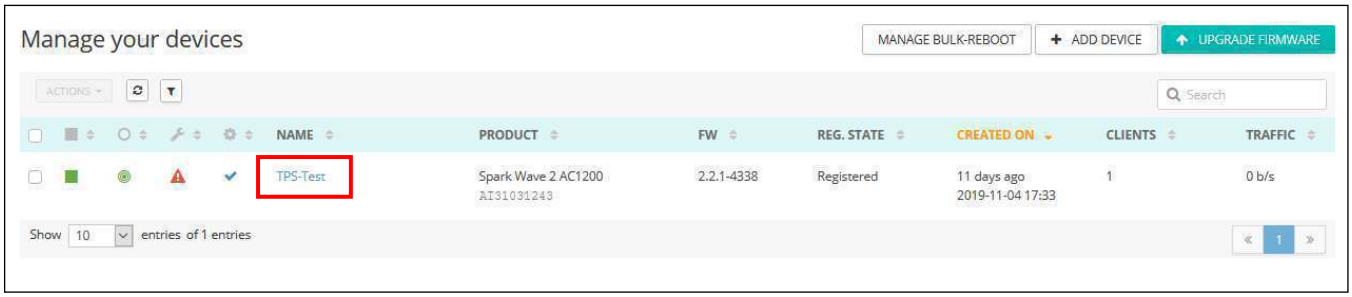
When a device's "Inheritance Policy" is enabled, the device is configured from the Site level. However, a device can be individually configured at the Device level and the settings will override the Site-level configuration.

Note: Individual device overrides can be reset to the Site-level configuration by clicking the "Use Site Settings" button on the page where a setting has been changed.

In addition, wireless devices include settings not configurable at the Site level, such as advanced radio settings and features unique to a specific product. These settings can only be configured at the Device level.

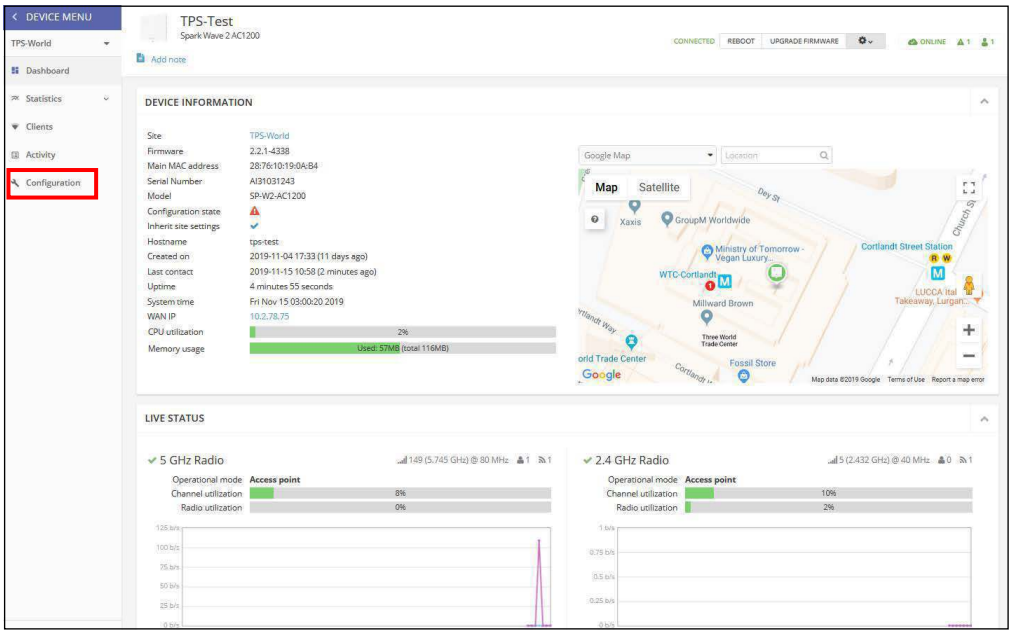
To access configuration for a device, click on the device name from the Site-level list of devices (also available from the Cloud-level list of devices).

Figure 216: Accessing Device-Level Configuration



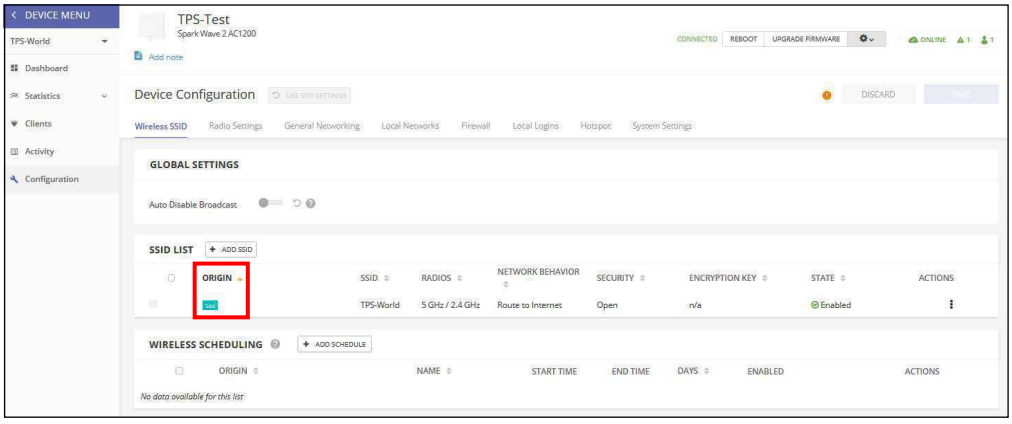
From the Device dashboard, click on "Configuration" on the Device menu to access a device's configuration.

Figure 217: Device-Level Dashboard



The Device Configuration page includes tabbed sections similar to the Site Configuration page.

Figure 218: Device Configuration



Device-level configuration for SSIDs are indicated in the “Origin” column of the SSID list; either “Site” or “Device” is displayed. Most other configuration items at the Device level are identical to those at the Site level.

This chapter only covers the device configuration that is different from the Site-level configuration, as documented in “Site WiFi 5 Configuration” on page 118.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_procesoDigitalizado_029_20250227.pdf (221/301) 1026/4746

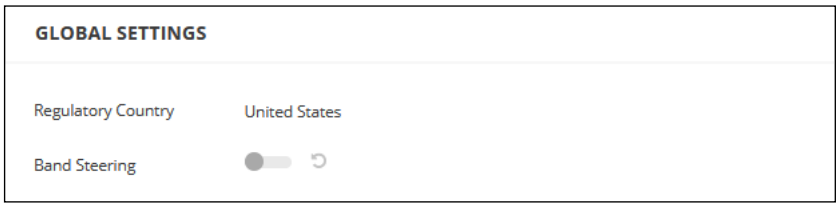
Device Radio Settings

Click the "Radio Settings" tab to configure 5 GHz and 2.4 GHz radio settings. Note that settings apply to all configured SSID interfaces.

The following items are displayed on the Radio Settings tab. Configuration options apply to both the 5 GHz and 2.4 GHz radios unless otherwise indicated.

Global Settings

Figure 219: Device Global Radio Settings



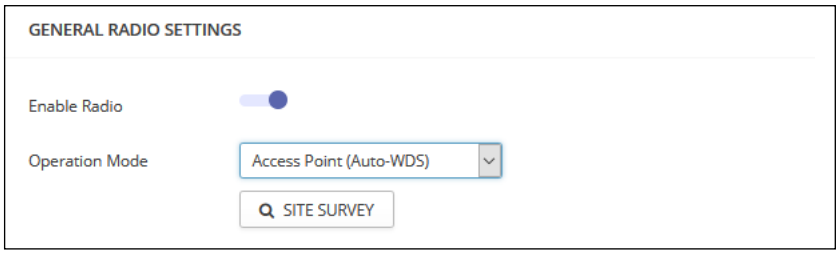
- **Regulatory Country** — The wireless device regulatory setting. This setting is displayed but not configurable at the Device level.

  The AP's country code must be correctly set to be sure that the radios operate according to permitted local regulations. That is, setting the country code restricts operation of the AP to the radio channels and transmit power levels permitted for wireless networks in the specified country.

- **Band Steering** — When enabled, clients that support 2.4 GHz and 5 GHz are first connected to the 5 GHz radio. This feature helps balance the client load over the two radio bands. Note that both radios must have configured SSIDs that match for this feature to fully operate. (Default: Disabled)

General Radio Settings

Figure 220: Device General Radio Settings



- **Enable Radio** — Enables or disables the wireless service on this interface.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 08059826321866289 2025 | Anexo Administrativo_procesado_1_029_20252026227.pdf (222/301) 1037/4746

- **Operation Mode** — Selects the mode in which the AP radio will function.
  - **Access Point (Auto-WDS)** — The AP operates as an access point in WDS mode, which accepts connections from APs in Client WDS mode. (This is the default setting.)

    In this mode, the AP provides services to clients as a normal access point. WDS is used to automatically search for and connect to other AP nodes using the same SSID and security settings.
  - **Client** — The AP can provide a wireless connection to another AP. In this mode, it can pass information from or to locally wired hosts, but does not provide services to any wireless clients.
  - **Client WDS** — The AP operates as a client station in WDS mode, which can connect to other access points in Auto-WDS mode. Connection to another AP can be made automatically by other access points operating in Auto-WDS mode.
- **Site Survey** — Click the button to scan for other Wi-Fi devices in the device location.

Advanced Radio Settings

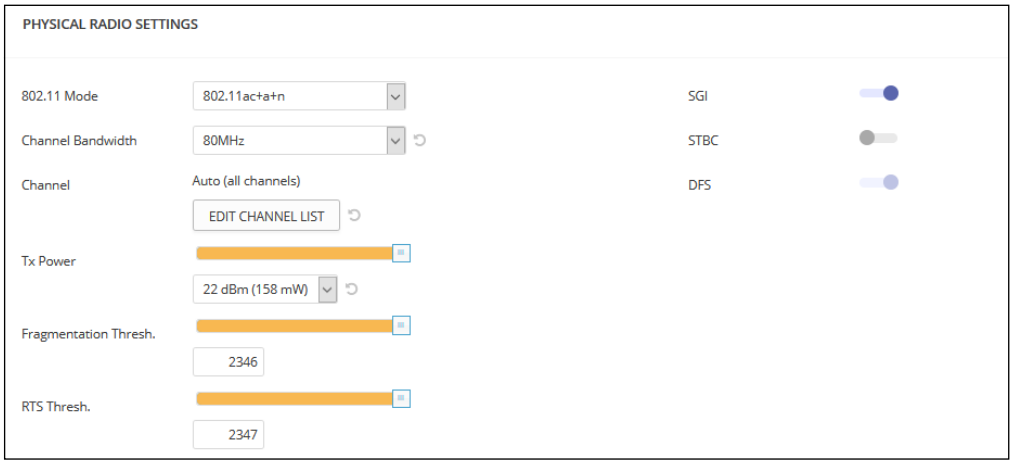
Figure 221: Device Advanced Radio Settings

- **Probe Req. Data Push** — Enable Client Probe Request Data Push for this radio. When enabled, the radio will push client probe request data in JSON format to your specified URL.
- **Push URL** — The web address where probe request data from this radio will be pushed.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (223/301) 1038/4746

Physical Radio Settings

Figure 222: Device Physical Radio Settings



- **802.11 Mode** — Defines the radio operation mode.
  - **5 GHz Radio** — Options: 802.11a, 802.11a+n, 11ac+a+n; Default: 802.11ac+a+n
  - **2.4 GHz Radio** — Fixed: 802.11b+g+n
- **Channel Bandwidth** — The basic Wi-Fi channel bandwidth is 20 MHz, but by bonding channels together to create 40 MHz or 80 MHz channels, higher data transmission rate can be achieved. However, selecting larger channel bandwidths reduces the number a radio channels available.
  - **5 GHz Radio** — Options include 20, 40, and 80 MHz. (Default: 80 MHz)
  - **2.4 GHz Radio** — Options include 20 and 40 MHz. (Default: 40 MHz)
- **Channel** — The radio channel that the access point uses to communicate with wireless clients. The available channels are dependent on the radio, Channel Bandwidth, and Regulatory Country settings. You can also click the "Edit Channel List" button to select specific available channels to use for each radio interface.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_page227.pdf (224/301) 1029/4746

Selecting Auto enables the access point to automatically select an unoccupied radio channel. (Default: Auto)

Figure 223: 5 GHz Radio Channels

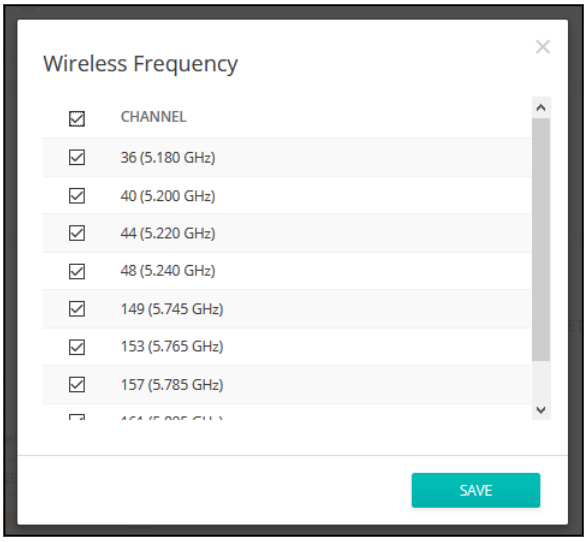
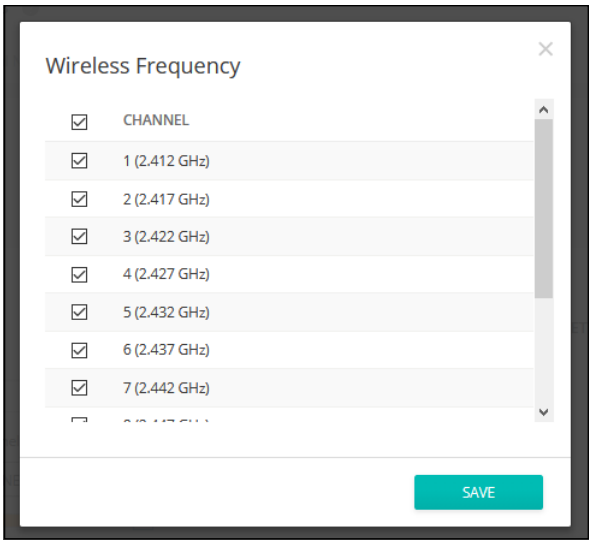


Figure 224: 2.4 GHz Radio Channels



- **Tx Power** — Adjusts the maximum power of the radio signals transmitted from the access point. The higher the transmission power, the farther the transmission range. Power selection is not just a trade off between coverage area and maximum supported clients. You also have to ensure that high-power signals do not interfere with the operation of other radio devices in the service area. (The range of power settings and defaults are dependent on the AP model and the Regulatory Country setting.)

- **Fragmentation Thresh.** — Sets the maximum frame size above which packets are fragmented. This reduces the time required to transmit the frame, and

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - Termo de Referência_processo_licitatorio_029_2025_pdf (225/301) 1050/4726

therefore reduces the probability that it will be corrupted (at the cost of more data overhead). (Range: 256-2346 bytes; Default: 2346 bytes)

- **RTS Thresh.** — Sets the packet size threshold at which a Request to Send (RTS) frame must be sent to a receiving station prior to the sending station starting communications. The access point sends CTS frames to a receiving station to negotiate the sending of a data frame. After receiving an RTS frame, the access point sends a CTS (clear to send) frame to notify the sending station that it can start sending data.

  If the RTS threshold is set to 1, the access point always sends RTS signals. If set to 2347, the access point never sends RTS signals. If set to any other value, and the packet size equals or exceeds the RTS threshold, the RTS/CTS (Request to Send / Clear to Send) mechanism will be enabled.

  The access points contending for the medium may not be aware of each other. The RTS/CTS mechanism can solve this "Hidden Node Problem." (Range: 1-2347 bytes: Default: 2347 bytes)

- **SGI** — The 802.11n draft specifies two guard intervals: 400ns (short) and 800ns (long). Support of the 400ns Short Guard Interval is optional for transmit and receive. The purpose of a guard interval is to introduce immunity to propagation delays, echoes, and reflections to which digital data is normally very sensitive. Enabling the SGI sets it to 400ns. (Default: Enabled)

- **STBC** — Space-time Block Coding sends multiple copies of the same data over a number of antennas, using the various received versions to improve the reliability of data transfer. The transmitted signal may traverse a difficult environment with scattering, reflection, and refraction which may then be further corrupted by thermal noise in the receiver, so some of the received copies will be better than others. This redundancy results in a higher chance of being able to use one or more of the received copies to correctly decode the received signal. (Default: Disabled)

- **DFS** — This field is available only if the selected radio mode operates in the 5 GHz frequency.

  For radios in the 5 GHz band, When DFS support is on and the regulatory domain requires radar detection on the channel, the Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) features of 802.11h are activated. The default is Off.

  DFS is a mechanism that requires wireless devices to share spectrum and avoid cochannel operation with radar systems in the 5 GHz band. DFS requirements vary based on the regulatory domain, which is determined by the country code setting of the AP. (Default: Enabled)

- **20/40MHz Coexist** — Applies only to the 2.4 GHz radio. This option allows 802.11n 20 MHz and 40 MHz channel bandwidths to operate together in the same network. (Default: On)

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - Termo de Referência_procesSoDigitalizado_029_20252026227.pdf (226/301) 1659/4746

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 pdf (227/301) 1060/4746

9 WiFi 6 and Newer Device Configuration

This chapter describes configuration settings for WiFi 6 access points at the Device level. It includes the following sections:

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_procesoDigital_1943_2025_20250227.pdf (228/301) 1963/4746

Accessing Device-Level Configuration

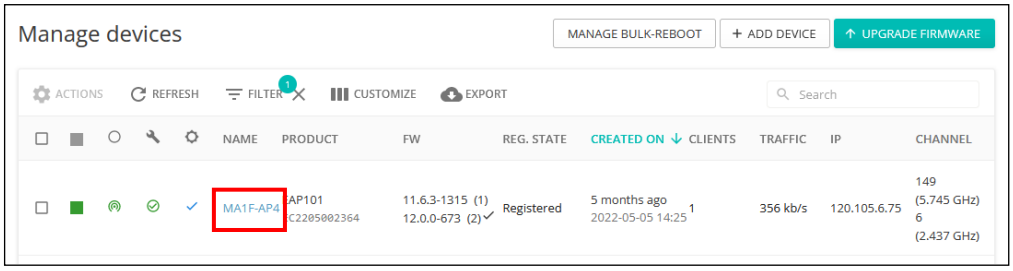
When a device's "Inheritance Policy" is enabled, the device is configured from the Site level. However, a device can be individually configured at the Device level and the settings will override the Site-level configuration.

Note: Individual device overrides can be reset to the Site-level configuration by clicking the "Use Site Settings" button on the page where a setting has been changed.

In addition, wireless devices include settings not configurable at the Site level, such as advanced radio settings and features unique to a specific product. These settings can only be configured at the Device level.

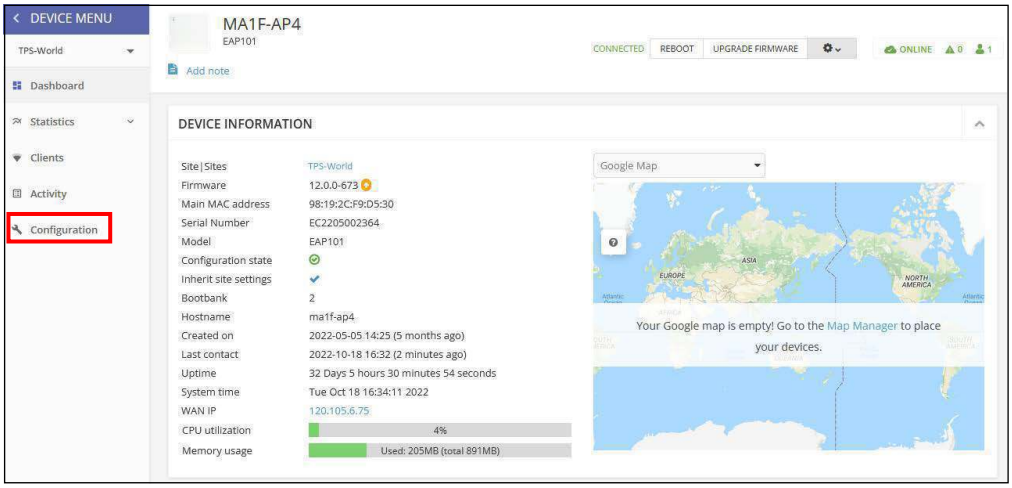
To access configuration for a device, click on the device name from the Site-level list of devices (also available from the Cloud-level list of devices).

Figure 225: Accessing Device-Level Configuration



From the Device dashboard, click on "Configuration" on the Device menu to access a device's configuration.

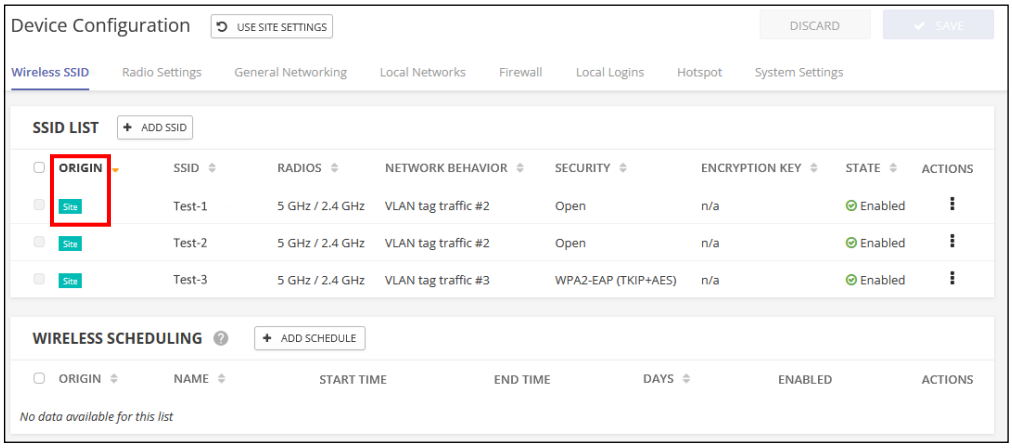
Figure 226: Device-Level Dashboard



1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - Termo de Referência_procedimento_029_2025_pdf (229/301) 1662/4746

The Device Configuration page includes tabbed sections similar to the Site Configuration page.

Figure 227: Device Configuration



Device-level configuration for SSIDs are indicated in the "Origin" column of the SSID list; either "Site" or "Device" is displayed. Most other configuration items at the Device level are identical to those at the Site level.

This chapter only covers the device configuration that is different from the Site-level configuration, as documented in "Site WiFi 6 Configuration" on page 160.

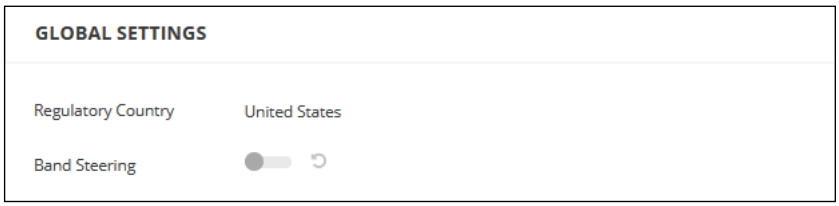
Device Radio Settings

Click the "Radio Settings" tab to configure 6 GHz, 5 GHz, and 2.4 GHz radio settings. Note that settings apply to all configured SSID interfaces.

The following items are displayed on the Radio Settings tab. Configuration options apply to the 6 GHz, 5 GHz, and 2.4 GHz radios unless otherwise indicated.

Global Settings

Figure 228: Device Global Radio Settings



- **Regulatory Country** — The wireless device regulatory setting. This setting is displayed but not configurable at the Device level.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (230/301) 1665/4746

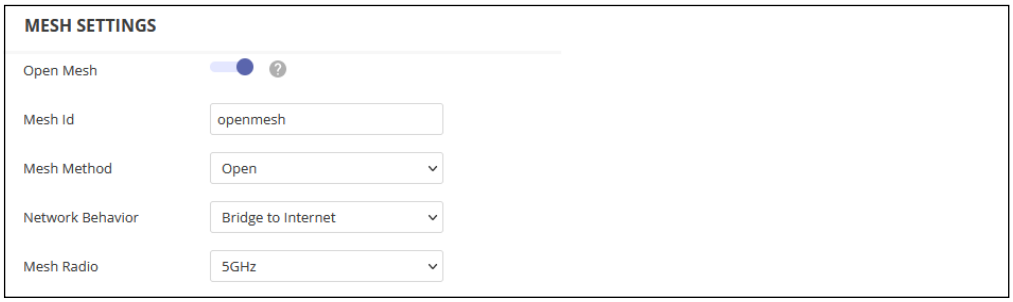
The AP's country code must be correctly set to be sure that the radios operate according to permitted local regulations. That is, setting the country code restricts operation of the AP to the radio channels and transmit power levels permitted for wireless networks in the specified country.

- **Band Steering** — When enabled, clients that support 2.4 GHz, 5 GHz and 6 GHz are first connected to the 6 GHz radio. This feature helps balance the client load over the two radio bands. Note that both radios must have configured SSIDs that match for this feature to fully operate. (Default: Disabled)

Mesh Settings

Open Mesh is a network of interconnected node APs, of which only one has a wired connection to the network (and the Internet). The other AP nodes provide wireless links to each other and some support connections to wireless clients. The mesh network not only extends wireless connectivity over a greater distance, but also provides backup links should one node in the network fail.

Figure 229: Device Mesh Settings



- **Open Mesh** — Enables Open Mesh support on the SSID interface.
- **Mesh ID** — Name of the mesh network.
- **Mesh Method** — Security applied on Open Mesh links.
  - **Open** — None.
  - **WPA3-Personal** — Uses WPA3 with Simultaneous Authentication of Equals (SAE) on mesh links to other APs.
- **Network Behavior** — One of the following connection methods must be specified. (Default: Route to Internet)
  - **Bridge to Internet** — Configures an interface as attached to the WAN. Traffic from this interface is directly bridged into the Internet. (See Figure 170, "Bridge to Internet", on page 169.)
  - **Route to Internet** — Configures an interface as a member of the LAN. Traffic from this interface is routed across the access point and out through

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (231/301) 1066/4726

an interface which is bridged to the Internet. (See Figure 171, "Route to Internet", on page 169.)

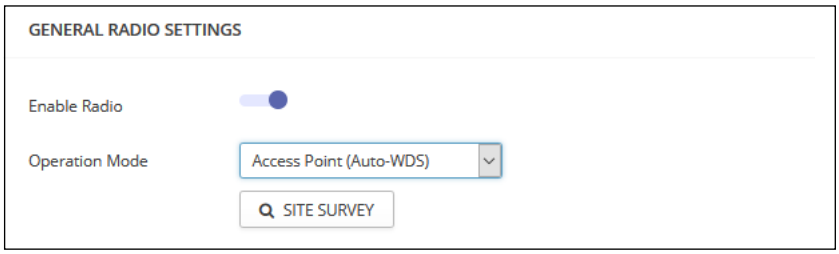
- **Network Name** — The network to be routed. The default is "Default local network" as displayed under LAN Settings – Local Network.

- **Mesh Radio** — When setting up an AP to be a node in a mesh network, select one radio interface: 2.4 GHz, 5 GHz, 6 GHz, or HaLow (sub-1 GHz). Configure it to operate on a specific channel (do not select Auto). Set up other AP nodes to operate on the same radio interface, channel, and with the same SSID.

Note: HaLow Open Mesh Mode is available on EAP112 with firmware version 12.5.0 or later.

General Radio Settings

Figure 230: Device General Radio Settings



- **Enable Radio** — Enables or disables the wireless service on this interface.

- **Operation Mode** — Selects the mode in which the AP radio will function.

  - **Access Point (Auto-WDS)** — The AP operates as an access point in WDS mode, which accepts connections from APs in Client WDS mode. (This is the default setting.)

    In this mode, the AP provides services to clients as a normal access point. WDS is used to automatically search for and connect to other AP nodes using the same SSID and security settings.

  - **Client** — The AP can provide a wireless connection to another AP. In this mode, it can pass information from or to locally wired hosts, but does not provide services to any wireless clients.

- **Site Survey** — Click the button to scan for other Wi-Fi devices in the device location.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo ... (232/301) 1065/4746

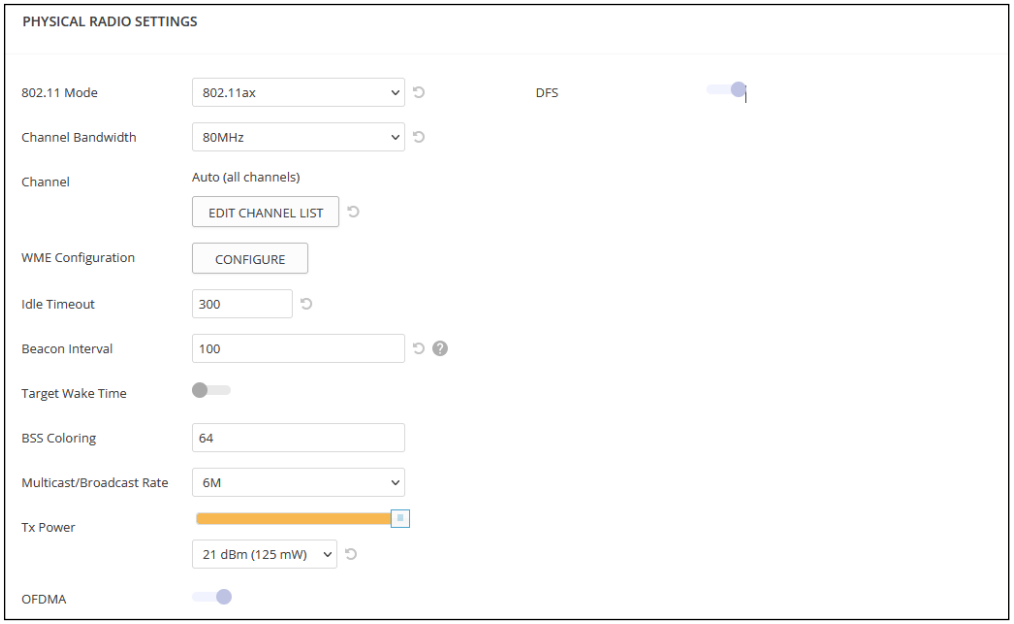
Advanced Radio Settings

Figure 231: Device Advanced Radio Settings

- **Probe Req. Data Push** — Enable Client Probe Request Data Push for this radio. When enabled, the radio will push client probe request data in JSON format to your specified URL.
- **Push URL** — The web address where probe request data from this radio will be pushed.

Physical Radio Settings

Figure 232: Device Physical Radio Settings



- **802.11 Mode** — Defines the radio operation mode.
  - **Radio 6 GHz** — Default: 11ax; Options: 11ax, 11be
  - **Radio 5 GHz** — Default: 11ax; Options: 11a, 11a+n, 11ac+a+n, 11ax, 11be
  - **Radio 2.4 GHz** — Default: 11ax; Options: 11ax, 11be

1Doc: Protocolo 1.943/2025 | Anexo Administrativo Técnico Digital nº 029_2025_20250227.pdf (233/301) 1066/4726

- **Channel Bandwidth** — The basic Wi-Fi channel bandwidth is 20 MHz, but by bonding channels together to create 40 MHz, 80 MHz, 160 MHz, and 320 MHz channels, higher data transmission rate can be achieved. However, selecting larger channel bandwidths reduces the number a radio channels available. The available channel bandwidth is dependent on the 802.11 Mode.
  (Default: 20 MHz on 2.4 GHz Radio, 80 MHz on 5 GHz and 6 GHz Radio; Options: 20 MHz, 40 MHz, 80 MHz, 160 MHz, and 320 MHz)
  - **20MHz** — For 802.11b+g+n and 802.11ax
  - **40MHz** — For 802.11b+g+n, 802.11a, 802.11a+n, 802.11ac+a+n and 802.11ax
  - **80MHz** — For 802.11ac+a+n and 802.11ax
  - **160MHz** — (Supported on EAP104 5 GHz radio, OAP101 5 GHz radio, and OAP101-6E 5 GHz and 6GHz radios) For 802.11ac+a+n and 802.11ax
  - **320MHz** — (Supported on EAP105) For 802.11be
- **Channel** — The radio channel that the access point uses to communicate with wireless clients. The available channels are dependent on the radio, Channel Bandwidth, and Regulatory Country settings. You can also click the "Edit Channel List" button to select specific available channels to use for each radio interface.

  Selecting Auto enables the access point to automatically select an unoccupied radio channel. (Default: Auto)

Figure 233: 5 GHz Radio Channels

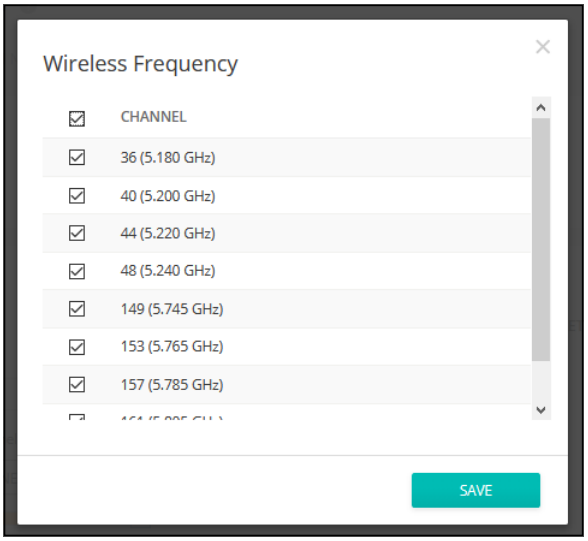
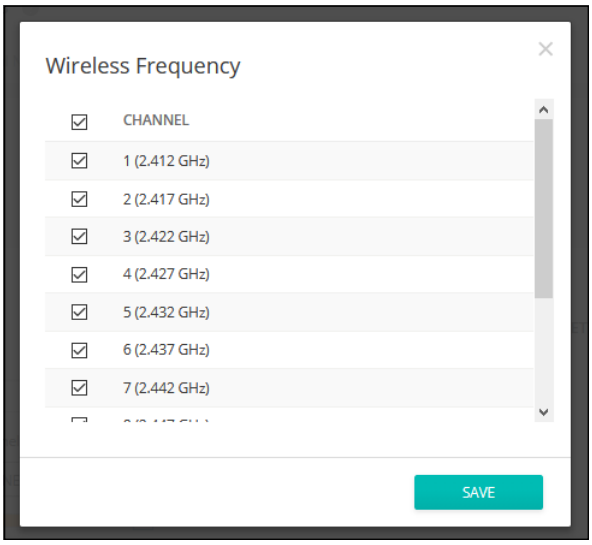


Figure 234: 2.4 GHz Radio Channels



- **WME Configuration** — Wireless Multimedia Extensions (WME), also known as Wi-Fi Multimedia (WMM), is a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. It provides basic Quality of service (QoS) features for IEEE 802.11 networks. Access priority can be configured for four "Access Category"(AC) types using the following parameters:

  - **CW Min (Minimum Contention Window)** – The initial upper limit of the random backoff wait time before wireless medium access can be attempted. The initial wait time is a random value between zero and the CWMin value. Specify the CWMin value in the range 0-15 microseconds. Note that the CWMin value must be equal or less than the CWMax value.

  - **CW Max (Maximum Contention Window)** – The maximum upper limit of the random backoff wait time before wireless medium access can be attempted. The contention window is doubled after each detected collision up to the CWMax value. Specify the CWMax value in the range 0-15 microseconds. Note that the CWMax value must be greater or equal to the CWMin value.

  - **AIFS (Arbitration Inter-Frame Space)** – The minimum amount of wait time before the next data transmission attempt. Specify the AIFS value in the range 0-15 microseconds.

  - **TXOP Limit (Transmit Opportunity Limit)** – The maximum time an AC transmit queue has access to the wireless medium. When an AC queue is granted a transmit opportunity, it can transmit data for a time up to the TXOP Limit. This data bursting greatly improves the efficiency for high data-rate traffic. Specify a value in the range 0-8192 microseconds.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_procesoDistancia_029_2025_pdf (235/301) 1968/4726

- **Idle Timeout (sec)** — The AP disconnects a client when there is no activity for the configured amount of time. (Default: 300 seconds; Range: 60-60000 seconds)
- **Beacon Interval** — The rate at which beacon signals are transmitted from the access point. The beacon signals allow wireless clients to maintain contact with the access point. They also carry power-management and other information. (Range: 100-1024 TUs; Default: 100 TUs)
- **Target Wake Time** — In 802.11ax (Wi-Fi 6) mode, the AP can allow clients to request a specific Target-Wakeup Time (TWT) to transmit or receive frames, rather than rely on periodic beacons. This feature enables client devices to have much longer sleep states and results in significant power savings. In addition, the AP can control and schedule client TWTs to both manage contention in the network and accommodate delay-sensitive traffic. (Default: Disabled)
- **BSS coloring** — In 802.11ax (Wi-Fi 6) mode, BSS coloring allows nearby APs operating at the same frequency to identify traffic belonging to their own Basic Service Set (BSS). The BSS coloring enables Wi-Fi 6 networks to operate more efficiently in high-density environments where neighboring AP and client transmissions overlap. Assign a color value (a number from 1 to 63) to identify the radio BSS, or enter value 64 to allow the AP to randomly select a color value. (Range: 1-63, 64 random, Default: 64)
- **Multicast/Broadcast Rate** — Allows a limit to be placed on the wireless bandwidth consumed by multicast and broadcast packets.
  - **Radio 6 GHz** — Options: 6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M; Default: 6M
  - **Radio 5 GHz** — Options: 6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M; Default: 6M
  - **Radio 2.4 GHz** — Options: 5.5M, 6M, 9M, 11M, 12M, 18M, 24M, 36M, 48M, 54M; Default: 5.5M
- **Tx Power** — Adjusts the maximum power of the radio signals transmitted from the access point. The higher the transmission power, the farther the transmission range. Power selection is not just a trade off between coverage area and maximum supported clients. You also have to ensure that high-power signals do not interfere with the operation of other radio devices in the service area. (The range of power settings and defaults are dependent on the AP model and the Regulatory Country setting.)
- **OFDMA** — The 802.11ax (Wi-Fi 6) mode supports Orthogonal Frequency Division Multiple Access (OFDMA) and this cannot be disabled.
- **DFS** — This field is available only if the selected radio mode operates in the 5 GHz frequency.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - Termo de Referência_processo_licitatorio_029_2025_pdf.pdf (236/301) 1969/4726

For radios in the 5 GHz band, When DFS support is on and the regulatory domain requires radar detection on the channel, the Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) features of 802.11h are activated. The default is Off.

DFS is a mechanism that requires wireless devices to share spectrum and avoid cochannel operation with radar systems in the 5 GHz band. DFS requirements vary based on the regulatory domain, which is determined by the country code setting of the AP. (Default: Enabled)

System Settings

Click the "System Settings" tab to configure Device-level features.

iBeacon

The AP supports the iBeacon standard based on Bluetooth Low Energy (BLE). Devices with BLE Beacons can provide location-based services to BLE clients, such as phones, that can recognize the beacon advertisements, extract the provided information, and then take actions based on the content.

Figure 235: Device iBeacon Settings

The following items are displayed on this page:

- **Enable** — Enables iBeacon support on the AP. (Default: Enabled)
- **BLE Scan** — (EAP101 and EAP104 only) Scans for all BLE devices, including these four types: EddyStone-UID, EddyStone-URL, EddyStone-TLM, and ibeacon.
- **UUID** — The iBeacon Universally Unique Identifier that advertises the beacon service. The UUID contains 32 hexadecimal digits in five groups, separated by hyphens.
- **Major** — The iBeacon value that is used to identify a beacon group. (Range: 0-65535)

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (237/301) 1670/4746

- **Minor** — The iBeacon value that is used to identify individual beacons within a group. (Range: 0-65535)
- **Tx Power** — Sets the BLE radio transmit power (supported only on EAP101 and EAP104). (Range: 5 dBm to -20 dBm; Default: 5 dBm)

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (238/301) 1073/4746

10 MetroLinq Device Configuration

This chapter describes configuration settings for MetroLinq units at the Device level. It includes the following sections:

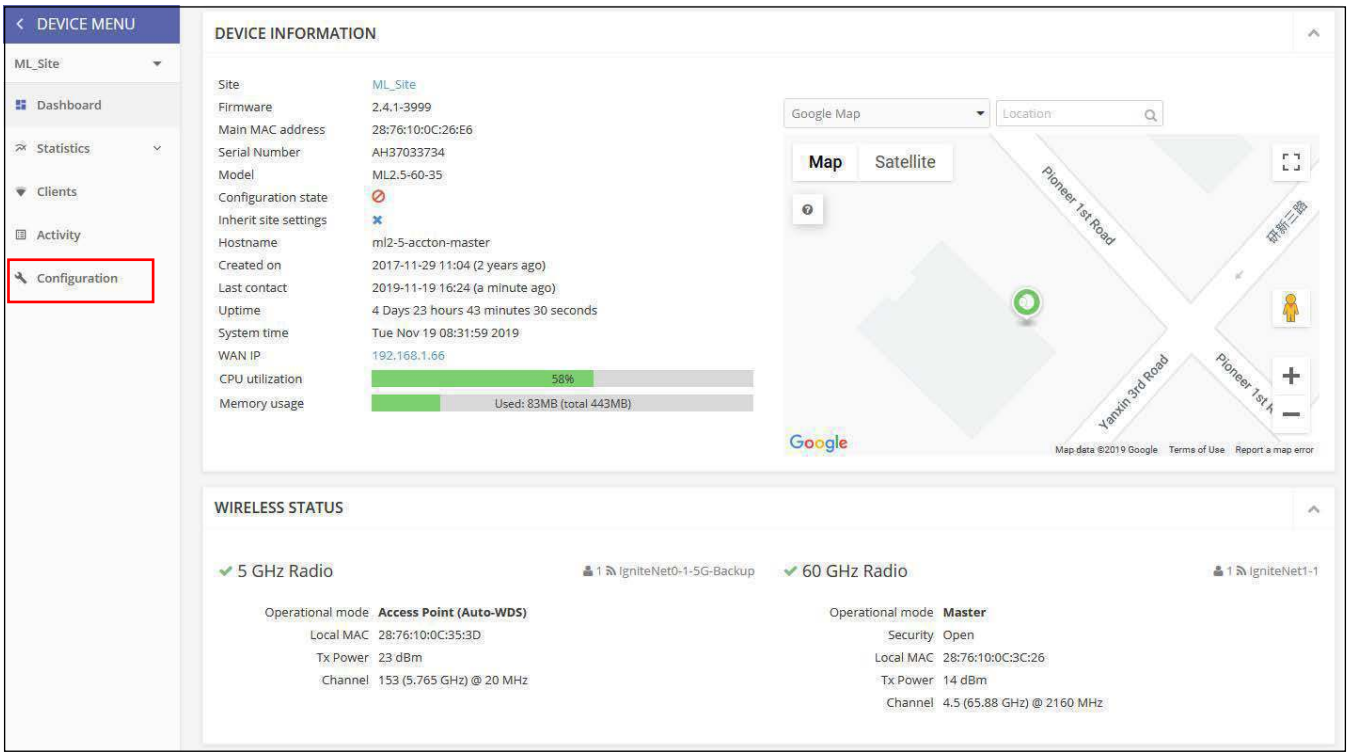
1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pregao_27.pdf (239/301) 1072/4746

MetroLinq Configuration

MetroLinq devices that support 2.4 GHz and 5 GHz bands can inherit configuration settings from the Site level for these radio interfaces. The 60 GHz radio settings cannot be inherited from the Site level and must be configured at the Device level.

This section covers Device-level configuration for MetroLinq devices, including specific settings not available at the Site level. For general Device-level settings, see "WiFi 5 Device Configuration" on page 219.

Figure 236: MetroLinq Device Dashboard



Wireless SSID

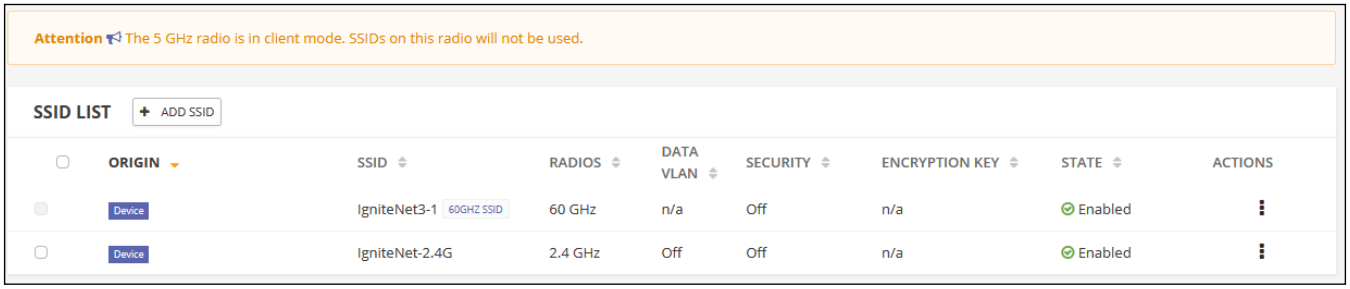
The MetroLinq devices support a 60 GHz radio, and often include 5 GHz and 2.4 GHz radios. SSIDs can only be configured for the 5 GHz and 2.4 GHz radios from the Wireless SSID page. The 60 GHz radio supports only one SSID and it must be configured on the Radio Settings page.

In cases where the 5 GHz radio is configured as a backup to the 60 GHz radio, the SSID must also be configured on the Radio Settings page.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo Processo Licitatório 029_2025_20250227.pdf (240/301) 1075/4746

For details on configuring Wi-Fi access SSIDs, see "Wireless SSID Configuration" on page 119.

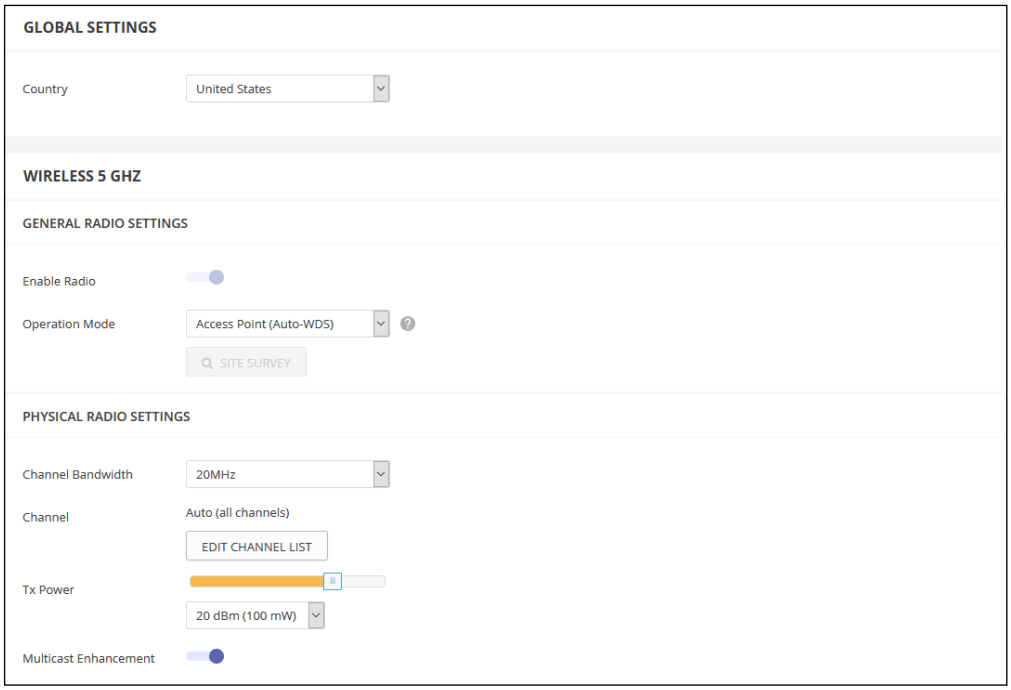
Figure 237: MetroLinq Device Dashboard



Radio Settings

Click the "Radio Settings" tab to configure 60 GHz, 5 GHz, and 2.4 GHz radio settings.

Figure 238: MetroLinq Device 5 GHz Radio Settings



Global Settings

The following items are displayed on this page section:

- **Country** — The MetroLinq device regulatory setting.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo processo licitatório 029_2025_pregão 027.pdf (241/301) 1076/4726

The MetroLinq's country code must be correctly set to be sure that the radios operate according to permitted local regulations. That is, setting the country code restricts operation of the MetroLinq to the radio channels and transmit power levels permitted for wireless networks in the specified country.

Wireless 5 GHz General Radio Settings

- **Enable Radio** — Enables or disables the wireless service on the 5 GHz interface. Note that the 5 GHz radio can be configured to operate as a backup link for the 60 GHz radio.

- **Operation Mode** — Selects the mode in which the 5 GHz radio will function.

  - **Access Point (Auto-WDS)** — The 5 GHz radio operates as an access point in WDS mode, which accepts connections from APs in Client WDS mode. (This is the default setting.)

    In this mode, the 5 GHz radio provides services to clients as a normal access point. WDS is used to automatically search for and connect to other AP nodes using the same SSID and security settings.

  - **Client WDS** — Sets the 5 GHz radio to only operate as the backup wireless bridge client in a point-to-point wireless link between two MetroLinq units.

- **Site Survey** — Click the button to scan for other Wi-Fi devices at the device location.

Client Mode Settings (when Client WDS mode selected)

- **SSID** —Input a unique name for the service set identifier of the 5 GHz interface. MetroLinq units at each end of a point-to-point backup link must be set to the same SSID. (Range: 1—32 characters)

- **Lock to BSSID** — Enter the MAC address of the Master unit in the link to lock the Client radio to only that unit.

- **Encryption** — Sets the wireless security method for the 5 GHz interface. When disabled, there is no security on the wireless link. When enabled, MetroLinq units in the point-to-point backup link use WPA2 security with a pre-shared key for authentication and encryption. (Default: Disabled)

  - **Encryption Cipher** — Sets the encryption cipher to use for the WPA2 pre-shared key.

    - **CCMP (AES)** — AES-CCMP is the standard encryption cipher required for WPA2. (This is the default setting.)

    - **Auto: TKIP + CCMP (AES)** — The encryption method used is discovered during association with the link partner.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - Termo de Referência_processo_licitatorio_029_2025_pdf (242/301) 1675/4726

- **Key** — Sets the WPA2 pre-shared key to use for encryption.

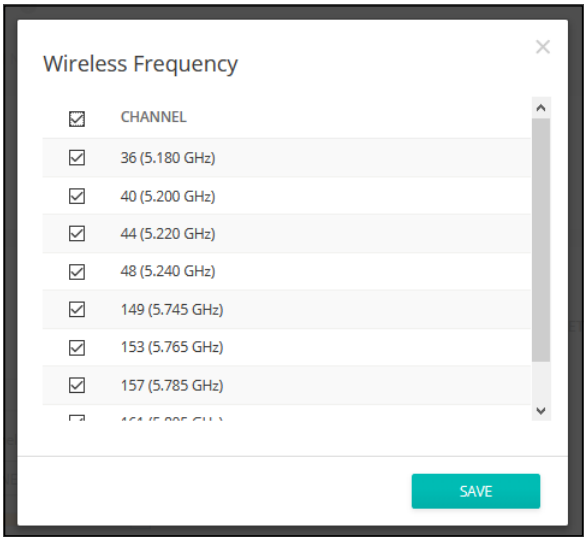
Physical Radio Settings

- **Channel Bandwidth** — The basic Wi-Fi channel bandwidth is 20 MHz, but by bonding channels together to create 40 MHz or 80 MHz channels, higher data transmission rate can be achieved. However, selecting larger channel bandwidths reduces the number a radio channels available. (Options: 20, 40, and 80 MHz; Default: 80 MHz)

- **Channel** — The radio channel that the access point uses to communicate with wireless clients. The available channels are dependent on the radio, Channel Bandwidth, and Regulatory Country settings. You can also click the "Edit Channel List" button to select specific available channels to use.

  Selecting Auto enables the access point to automatically select an unoccupied radio channel. (Default: Auto)

Figure 239: 5 GHz Radio Channels



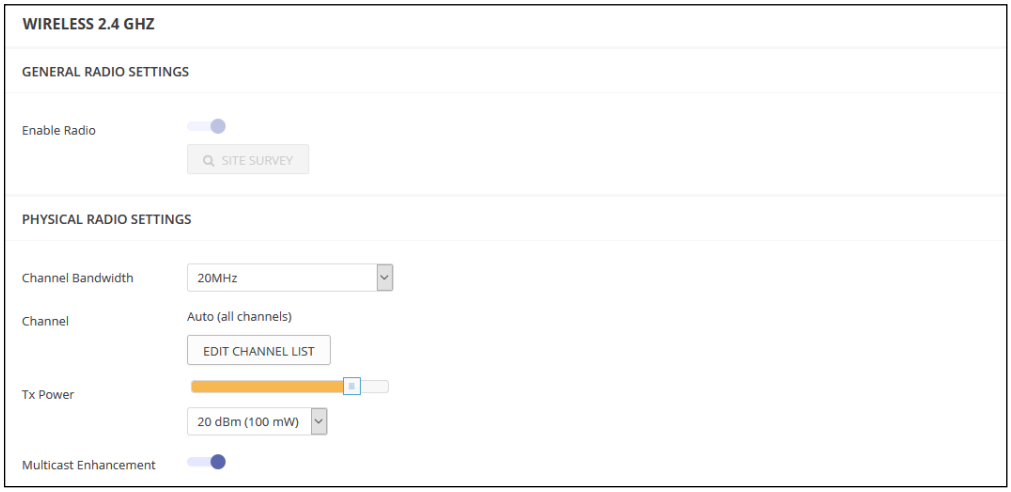
- **Tx Power** — Adjusts the maximum power of the radio signals transmitted from the access point. The higher the transmission power, the farther the transmission range. Power selection is not just a trade off between coverage area and maximum supported clients. You also have to ensure that high-power signals do not interfere with the operation of other radio devices in the service area. (The range of power settings and defaults are dependent on the AP model and the Regulatory Country setting.)

- **Multicast Enhancement** — This feature translates multicast packets to unicast packets before forwarding to clients, which results in more stable and faster transmissions. If poor multicast streaming is experienced by wireless clients, enable this feature to improve performance. (Not available when the 5 GHz radio is set to Client WDS mode.)

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (243/301) 1078/4746

Wireless 2.4 GHz

Figure 240: MetroLinq Device 2.4 GHz Radio Settings



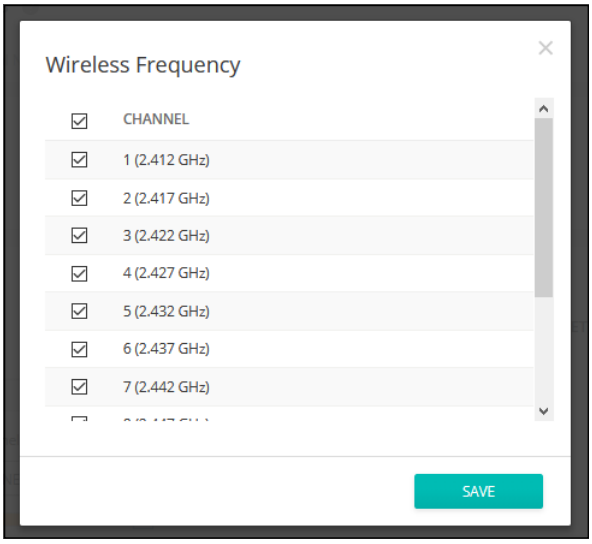
The following items are displayed on this page section:

- **Enable Radio** — Enables or disables the wireless service on the 2.4 GHz interface.
- **Site Survey** — Click the button to scan for other Wi-Fi devices at the device location.
- **Channel Bandwidth** — The basic Wi-Fi channel bandwidth is 20 MHz, but by bonding channels together to create 40 MHz or 80 MHz channels, higher data transmission rate can be achieved. However, selecting larger channel bandwidths reduces the number a radio channels available. (Options: 20 and 40 MHz; Default: 20 MHz)
- **Channel** — The radio channel that the access point uses to communicate with wireless clients. The available channels are dependent on the radio, Channel Bandwidth, and Regulatory Country settings. You can also click the "Edit Channel List" button to select specific available channels to use.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (244/301) 1679/4726

Selecting Auto enables the access point to automatically select an unoccupied radio channel. (Default: Auto)

Figure 241: 2.4 GHz Radio Channels



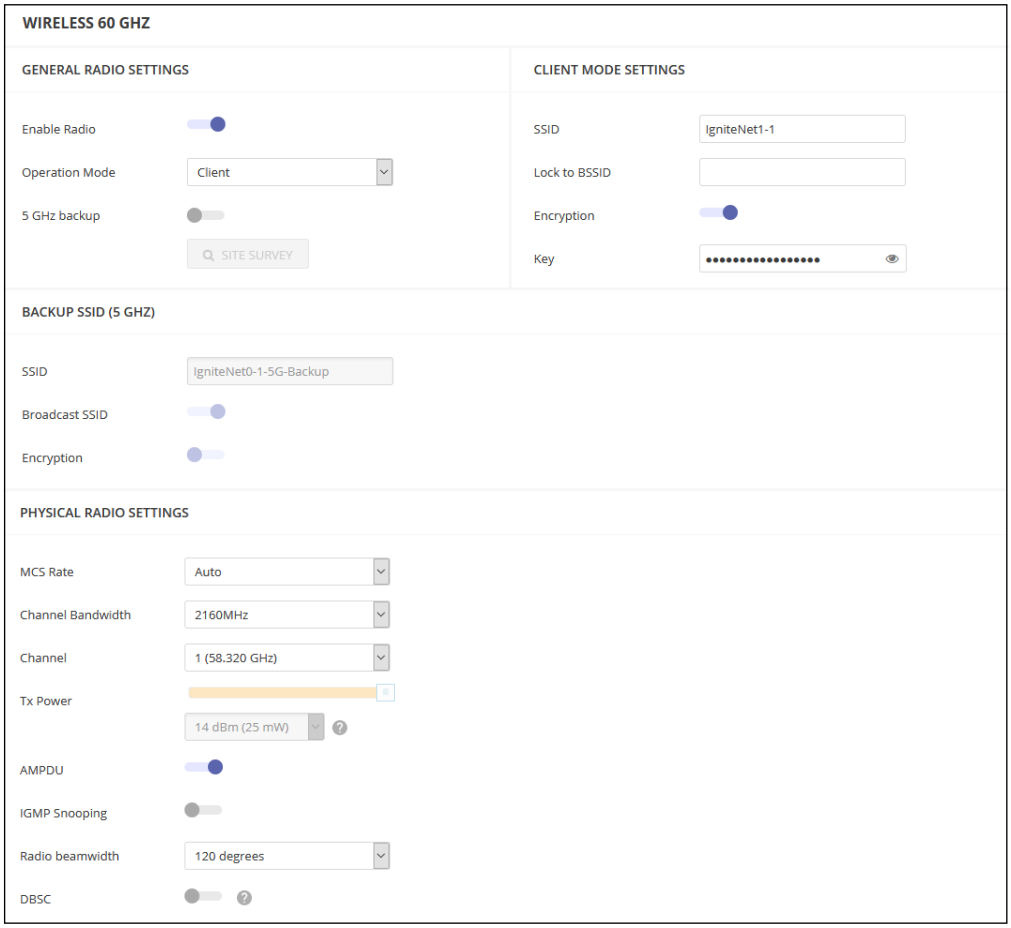
- **Tx Power** — Adjusts the maximum power of the radio signals transmitted from the access point. The higher the transmission power, the farther the transmission range. Power selection is not just a trade off between coverage area and maximum supported clients. You also have to ensure that high-power signals do not interfere with the operation of other radio devices in the service area. (The range of power settings and defaults are dependent on the AP model and the Regulatory Country setting.)

- **Multicast Enhancement** — This feature translates multicast packets to unicast packets before forwarding to clients, which results in more stable and faster transmissions. If poor multicast streaming is experienced by wireless clients, enable this feature to improve performance.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pagina_227.pdf (245/301) 1678/4746

Wireless 60 GHz

Figure 242: MetroLinq Device 60 GHz Radio Settings



General Radio Settings

The following items are displayed on this page section:

- **Enable Radio** — Enables the wireless service on the 60 GHz interface.
- **Operation Mode** — Selects the mode in which the 60 GHz interface will function.
  - **Master** — Sets the 60 GHz interface as the Master in a point-to-point or point-to-multi-point wireless link between two or more MetroLinq units. MetroLinq wireless links require one unit set as Master and the other(s) set to Client. Links to non-Edgecore devices are not supported.
  - **Client** — Sets the 60 GHz interface as a client in a point-to-point wireless link between two MetroLinq units.
- **5 GHz backup** — Configures the 5 GHz interface to function as a backup to the 60 GHz radio link. Should the 60 GHz link fail, the 5 GHz link is enabled

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (246/301) 1679/4726

to maintain connectivity. The 5 GHz backup can only be configured when the 60 GHz interface is set to Master mode. (Default: Disabled)

Wireless Networks (60 GHz radio set to Master mode)

- **SSID** —Input a unique name for the service set identifier of the 60 GHz interface. MetroLinq units at each end of a point-to-point link must be set to the same SSID. (Range: 1—32 characters)

- **Encryption** — Sets the wireless security method for the 60 GHz interface. When disabled, there is no security on the wireless link. When enabled, MetroLinq units in the point-to-point link use WPA2 security with a pre-shared key for authentication and encryption. (Default: Disabled)

    - **Key** — Sets the WPA2 pre-shared key to use for encryption.

Client Mode Settings (60 GHz radio set to Client mode)

- **SSID** —Input a unique name for the service set identifier of the 60 GHz interface. MetroLinq units at each end of a point-to-point link must be set to the same SSID. (Range: 1—32 characters)

- **Lock to BSSID** — Enter the MAC address of the Master unit in the link to lock the Client radio to only that unit.

- **Encryption** — Sets the wireless security method for the 60 GHz interface. When disabled, there is no security on the wireless link. When enabled, MetroLinq units in the point-to-point link use WPA2 security with a pre-shared key for authentication and encryption. (Default: Disabled)

    - **Key** — Sets the WPA2 pre-shared key to use for encryption.

Backup SSID (5 GHz)

- **SSID** —Input a unique name for the service set identifier of the backup 5 GHz interface. MetroLinq units at each end of a point-to-point link must be set to the same 5 GHz backup SSID. (Range: 1—32 characters)

- **Broadcast SSID** — Enables or disables sending the configured SSID in beacon messages. (Default: Enabled)

- **Encryption** — Sets the wireless security method for the 60 GHz interface. When disabled, there is no security on the wireless link. When enabled, MetroLinq units in the point-to-point link use WPA2 security with a pre-shared key for authentication and encryption. (Default: Disabled)

    - **Encryption Cipher** — Sets the encryption cipher to use for the WPA2 pre-shared key.

        - **CCMP (AES)** — AES-CCMP is the standard encryption cipher required for WPA2. (This is the default setting.)

1Doc: Protocolo 1.943/2025 | Anexo Administrativo processo licitatório 029_2025_pdf (247/301) 1050/4746

- **Auto: TKIP + CCMP (AES)** — The encryption method used is discovered during association with the link partner.

- **Key** — Sets the WPA2 pre-shared key to use for encryption.

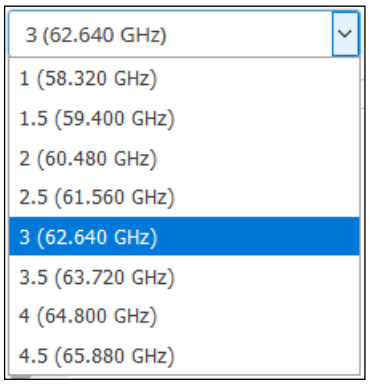
Physical Radio Settings

- **MCS Rate** — The modulation and coding scheme used to set the data rate at which the MetroLinq transmits packets on the 60 GHz interface. A setting of "Auto" sets the rate depending on the signal strength.

- **Channel Bandwidth** — For the 60 GHz radio, a channel bandwidth of 2160 MHz or 1080 MHz can be selected. (Default: 2160 MHz)

- **Channel** — The radio channel that the MetroLinq uses to communicate on the 60 GHz interface. The available channels are dependent on the radio, Channel Bandwidth, and Regulatory Country settings.

Figure 243: 60 GHz Radio Channels



- **Tx Power** — Adjusts the maximum power of the radio signals transmitted on the 60 GHz interface. The higher the transmission power, the farther the transmission range and higher the data rate. (The range of power settings and defaults are dependent on the AP model and the Regulatory Country setting.)

- **AMPDU** — Enables or disables the use of Aggregated MAC Protocol Data Units. Physical layer (PHY) data rate improvements do not increase real throughput beyond a point because of 802.11 protocol overheads. The main media access control feature that provides a performance improvement is aggregation. Aggregation of MAC protocol data units (MPDUs) is referred to as MPDU aggregation or (A-MPDU). (Default: Enabled)

- **Client Isolation** — When enabled, wireless clients can talk to the LAN, and reach the Internet if such connection is available, but they cannot communicate with one another. (Default Off)

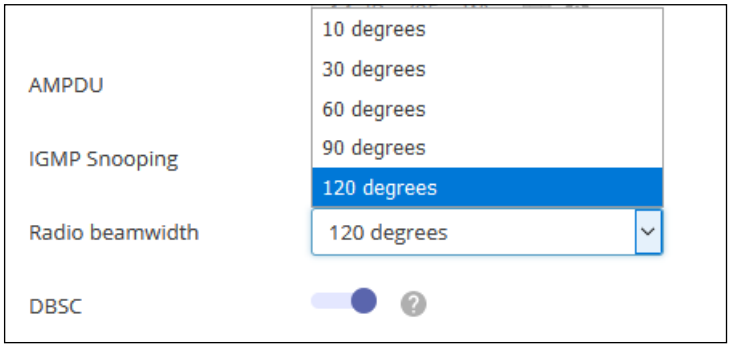
- **IGMP Snooping** — Enables IGMP snooping to manage and filter multicast streams over the 60 GHz interface.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - Termo de Referência_processo_licitatorio_029_2025_pdf (248/301) 1953/4726

- **RSSI based failover** —When enabled and the Received Signal Strength Indicator (RSSI) of the 60 GHz link falls below the "RSSI failover limit," the link will failover to the 5 GHz backup link. (Default:-65, Range: -95 to -25)

Settings for MetroLinq 60 LW, 2.5-60-18-BF, 10G Tri-Band Omni

Figure 244: MetroLinq Radio Beamwidth



- **Radio beamwidth** — Sets the sector antenna beamwidth for the MetroLinq 60 LW, 2.5-60-18-BF, and 10G Tri-Band Omni. The narrower the beamwidth, the more directional the signal, and higher the antenna gain. (Options: 10, 30, 60, 90, 120 degrees; Default: 120 degrees)

- **DBSC** — Enable Directional Beam Scan and Connect (DBSC) to address the limitation where phased array antennas only use a quasi-omni single directional beam to perform a wide area scanning. The lower gain of a quasi-omni beam limits the maximum distance at which connections can be established and traffic maintained. Enabling DBSC resolves the lower gain issue by using directed beams when scanning. (Default: Disabled)

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pag 249/301 (249/301) 1052/4726

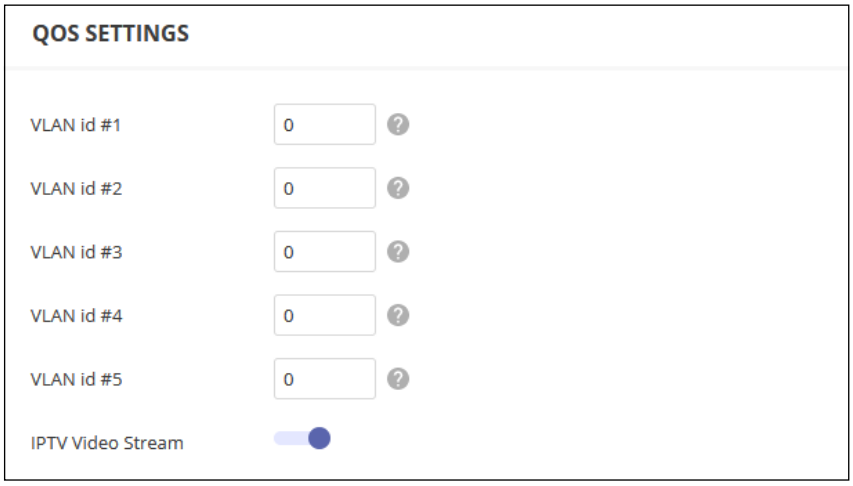
QoS Settings

The QoS (Quality of Service) Settings tab enables specific VLANs to be assigned as high priority traffic, where the data packets are tagged as high priority and are transmitted before other packets.

The MetroLinq interfaces have three priority queues; one for control messages, one for high priority traffic, and one for all other traffic. Packets tagged with an IEEE 802.1p priority of 4 to 7, or IP/TOS priority of 4 to 7, are classified as high priority and placed into the high priority queue by default.

On the QoS Settings page, you can also configure up to five VLANs as high priority traffic. That is, any data frame with one of the VLAN IDs will be classified as high priority and put in the high priority queue.

Figure 245: MetroLinq QoS Settings



The following items are displayed on this page:

- **VLAN id #1-#5** — Configures a VLAN ID as high priority traffic. All five VLANs have the same equal priority. (Range: 1-4094, 0 means disabled)
- **IPTV Video Stream** — When enabled, causes all multicast frames to be classified as high priority, improving performance for IPTV streams. (Default: Disabled)

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (250/301) 1665/4746

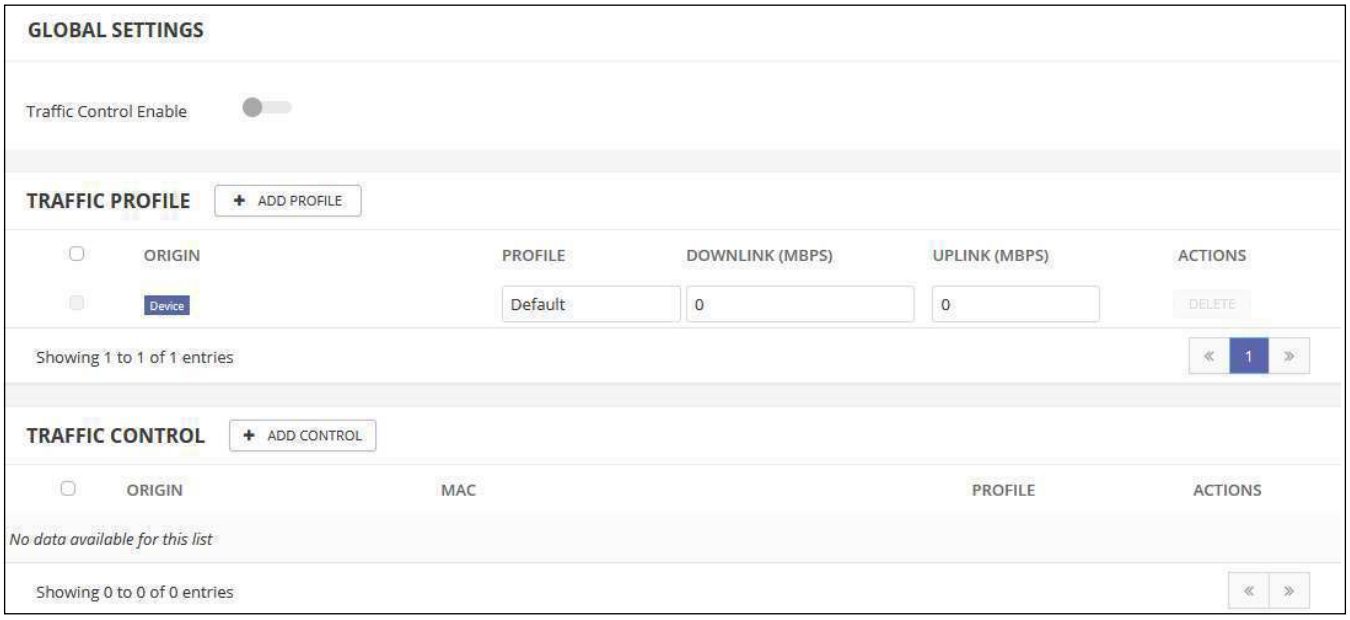
Traffic Control

Use the Traffic Control settings to limit the uplink and downlink bandwidth for specified devices. First create Traffic Profiles that specify the uplink and downlink bandwidth limits, and then bind the profiles to specific device MAC addresses.

Click the "Add Profile" button to add a new profile. Give the profile a name and specify the bandwidth limits.

To bind a profile to a MAC address, click the "Add Control" button, enter a device MAC address, and then select the profile name form the pull-down list.

Figure 246: MetroLinq Traffic Control Settings



The following items are displayed on this page:

- **Traffic Control Enable** — Enables the configured traffic control settings. (Default: Disabled)
- **Traffic Profile** — Configure the required profiles.
  - **Profile** — Specify a name that describes the profile.
  - **Download (Mbps)** — Sets the maximum downlink rate to a value between 0 and 1000 Mbps. (Default: 0)
  - **Upload (Mbps)** — Sets the maximum uplink rate to a value between 0 and 1000 Mbps. (Default: 0)

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 5 - Processo Licitatório 029_2025_pdf (251/301) 1056/4746

- **Traffic Control** — Binds the Traffic Profiles to MAC addresses.
  - **MAC** — Device MAC address.
  - **Profile** — Configured profile name.

Using the LinqPath Tool

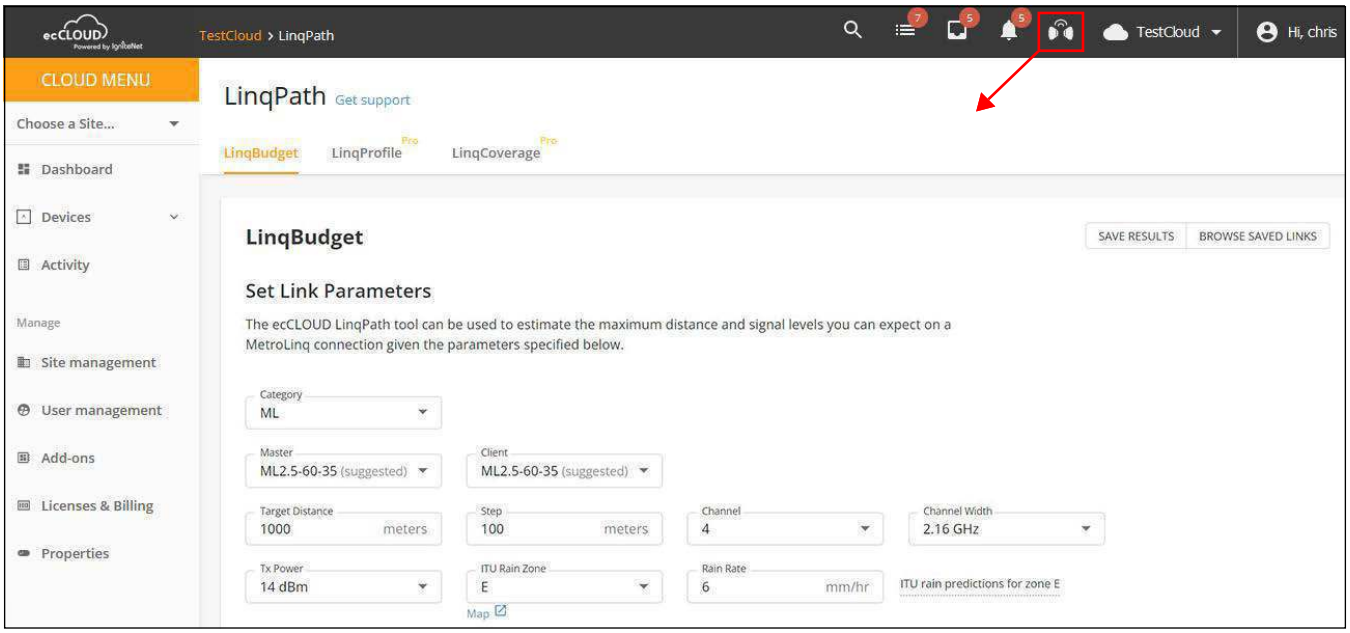
The Edgecore LinqPath™ tool can be used to estimate the maximum distance and signal levels you can expect on a MetroLinq connection given the specified parameters. Statistical rain fade calculations are included using the ITU rain model.

The LinqPath™ tool is available with a free ecCLOUD account. You can access LinqPath by clicking the icon in the top navigation menu.

Specify the planned link details in the LinqBudget section, and then view the results and RSSI graph to be sure it meets your required link performance.

You can save your LinqPath calculations using the “Save Results” button. Up to 10 link results can be saved in your LinqPath history.

Figure 247: MetroLinq LinqPath Settings



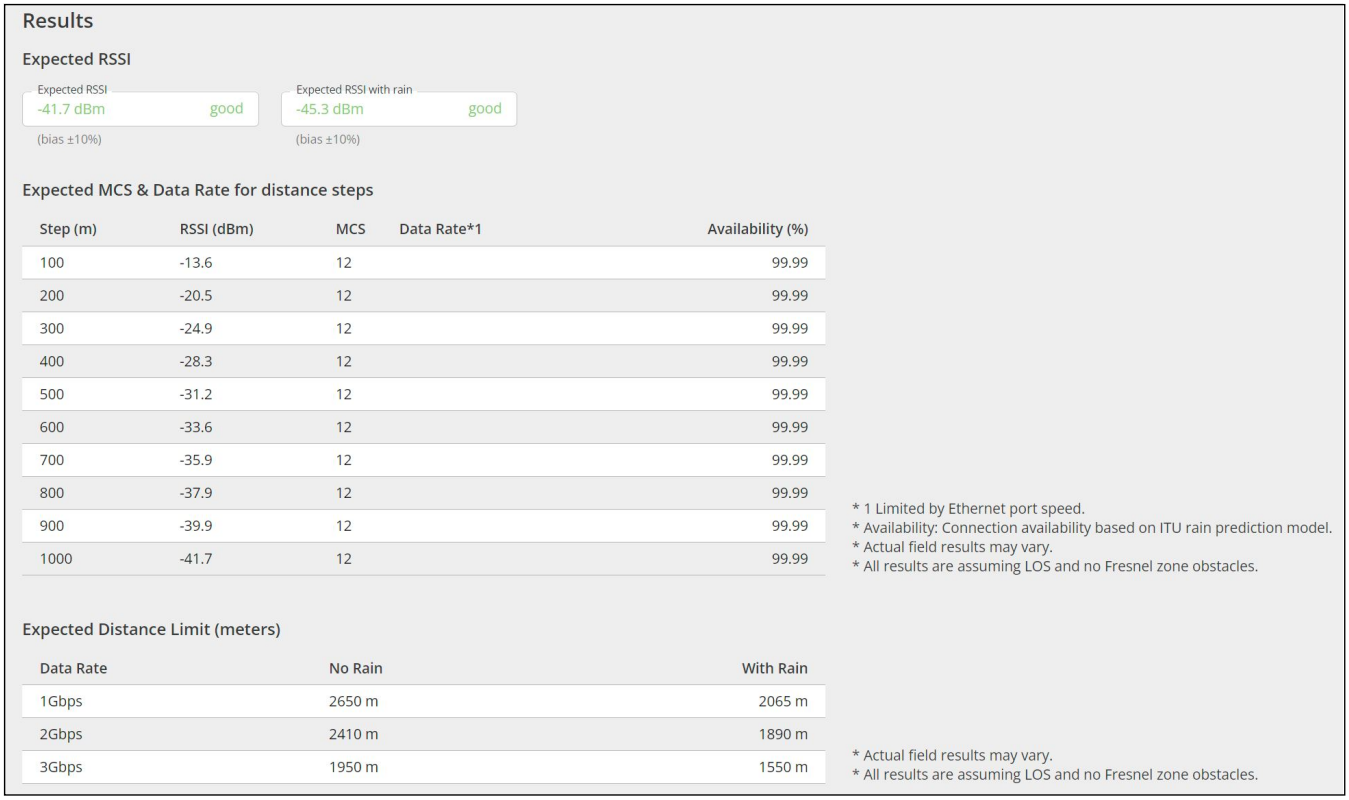
The following items are displayed on this page section:

- **Master** — The MetroLinq model that will be used as the PTP or PTMP master.
- **Client** — The MetroLinq model that will be used as the PTP or PTMP client.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo Técnico Nº 29/2025 | Anexo Técnico Nº 29/2025 (252/301) 1065/4746

- **Target Distance** — The intended distance of the link.
- **Step** — Distance intervals for assessing expected link performance at various distances up to the target distance. (Default: 10% of Target Distance)
- **Channel** — The radio channel that the link will operate on.
- **Channel Width** — The configured radio channel width.
- **Tx Power** — The transmit power that will be configured for the MetroLinq 60 GHz radio.
- **ITU Rain Zone** — The ITU rain zone in which the link will operate. A map highlighting the various rain regions are provided by the LinqPath tool.
- **Rain Rate** — The predicted ITU rain rate (mm per hour) for the specified zone.

Figure 248: MetroLinq LinqBudget Results



The following items are displayed on this page section:

- **Expected RSSI** — Shows the expected RSSI of the link based on the distance provided in the Target Distance input box. Links with RSSI below -70 dBm are classified as “No link.”

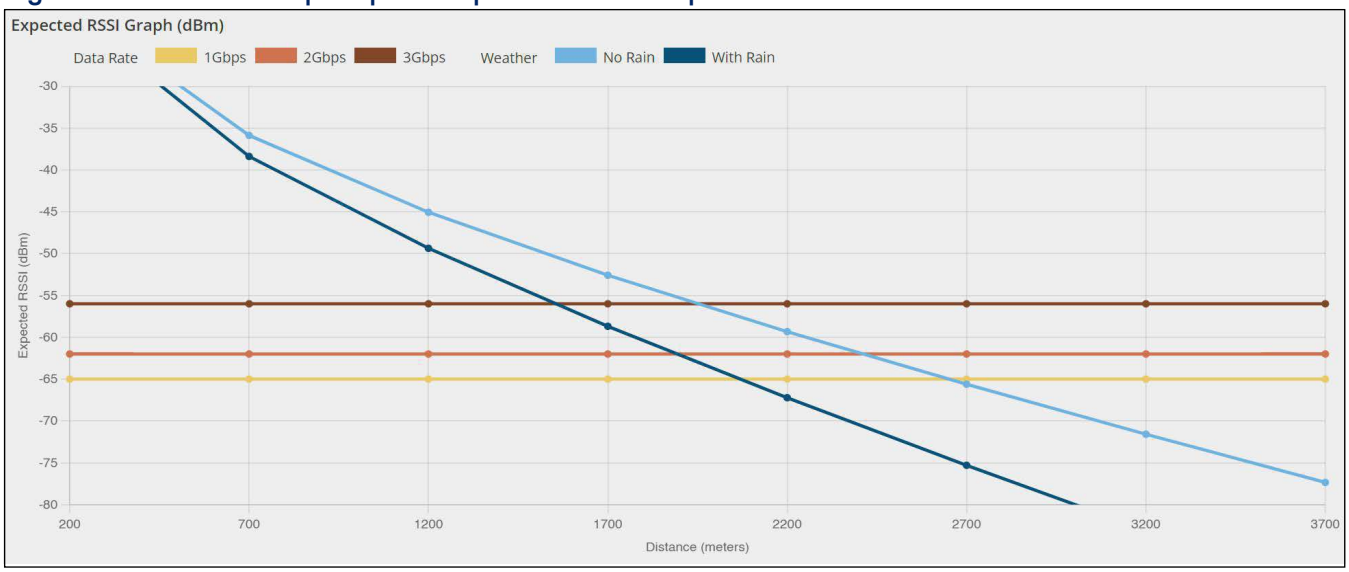
1Doc: Protocolo 1.943/2025 | Anexo Administrativo processo licitatório 029_2025_pregão 027.pdf (253/301) 1088/4746

- **Expected RSSI with rain** — Shows the expected RSSI of the link when it is raining based on the distance provided in the Target Distance input box. Links with RSSI below -70 dBm are classified as "No link."
- **Expected MCS & Data Rate for distance steps** (Only supports MLTG products) — Shows the expected RSSI, MCS values and corresponding Data Rates at each step interval up to the set target distance.
  - **Data Rate** — Expected data rate, limited by Ethernet port speed.
  - **Availability** — Connection availability based on the ITU rain prediction model.
- **Expected Distance Limit** — Shows the expected maximum distance at which a link with the selected MetroLinq models can achieve 3 Gbps, 2 Gbps, and 1 Gbps throughput. The "With Rain" values include the statistical rain fade considerations calculated using the ITU Rain Zone and Rain Rate settings.

RSSI vs. Distance Graph

LinqPath also produces a graph of the Expected RSSI versus distance. The purple "No Rain" line indicates the expected RSSI without rain. The blue "With Rain" line indicates the expected RSSI that should be exceeded by the percentage of time selected in the "60 GHz Rain Reliability" drop-down menu. The 1 Gbps, 2 Gbps, and 3 Gbps lines show the RSSI levels at which each data rate can be achieved.

Figure 249: MetroLinq LinqPath Expected RSSI Graph



1Doc: Protocolo 1.943/2025 | Anexo Administrativo 5 - Processo Licitatório 029_2025_20250227.pdf (255/301) 1068/4746

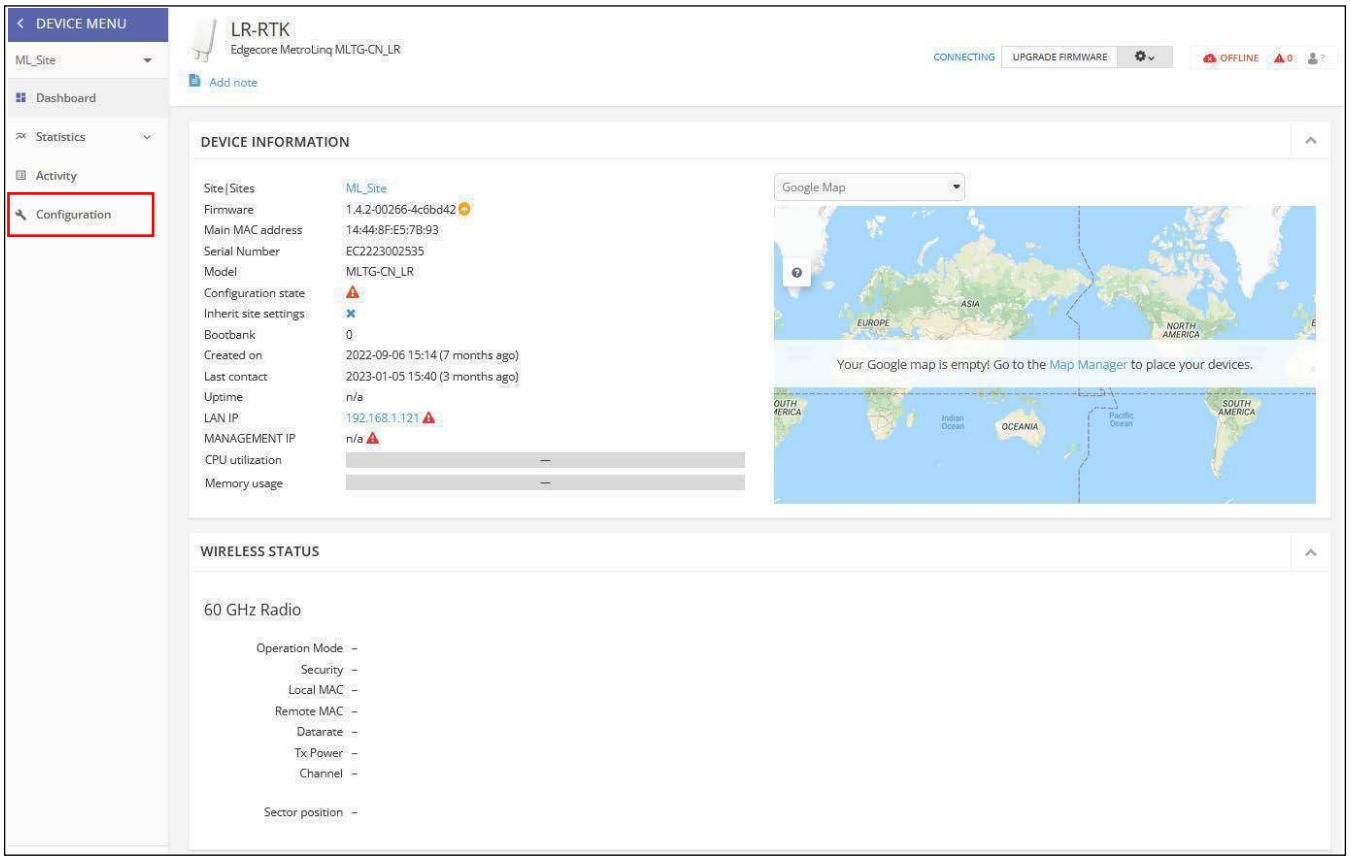
11 Terragraph Device Configuration

This chapter describes configuration settings for Terragraph MLTG-CN units at the Device level. It includes the following sections:

Terragraph Configuration

This section covers Device-level configuration for Terragraph MLTG-CN devices, including specific settings not available at the Site level.

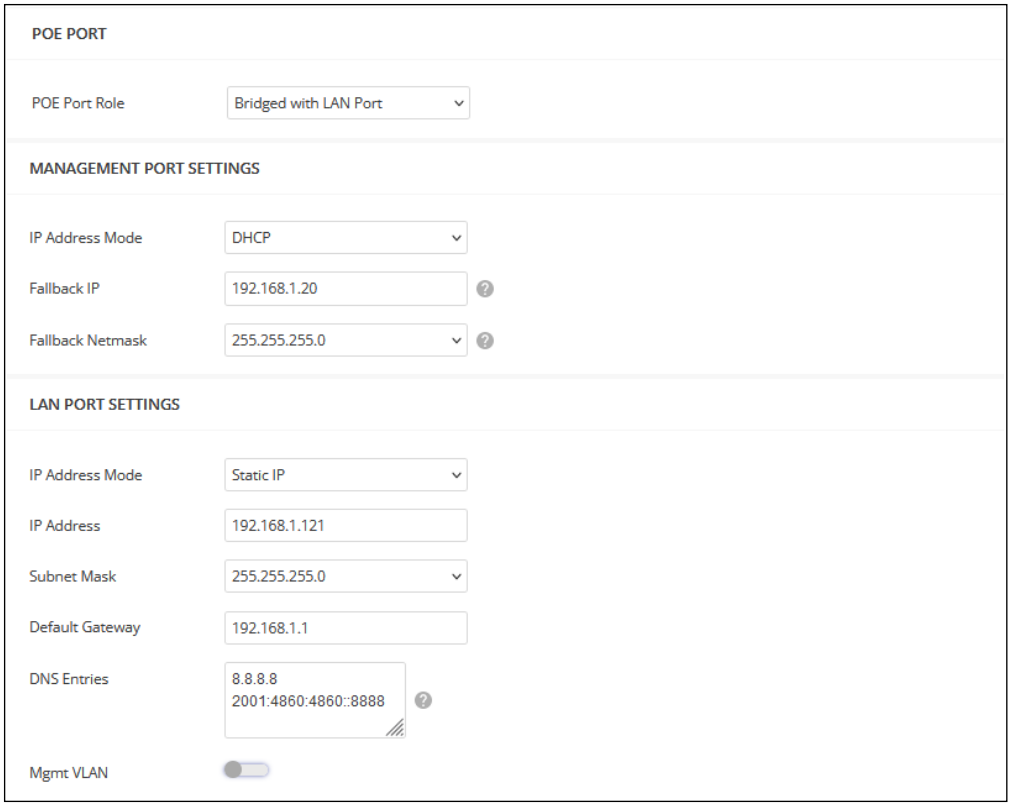
Figure 250: Terragraph Device Dashboard



General Networking Settings

Click the "General Networking" tab to configure management port and LAN port settings.

Figure 251: Terragraph Device General Networking



The following items are displayed on this page:

PoE Port

- **POE Port Role** — Selects the function of the Uplink Port (PoE port). This port functions as a dedicated management port by default. The role can be changed to "Bridged with LAN port" so that the port functions as a LAN port.

Management Port Settings

- **IP Address Mode** — Sets the method used to provide an IP address for the Internet access port. (Default: DHCP; Options: DHCP, static IP)
- **Fallback IP** — The IPv4 address used when a DHCP server is unavailable. (Default: 192.168.1.20)
- **Fallback Netmask** — The subnet mask used for the Fallback IP address. (Default: 255.255.255.0)

1Doc: Protocolo 1.943/2025 | Proexadmi 3HG70080059826321B662899129202 5ad Aristeu EC_proCesSoDi_tseMa_029_2025_0256227.pdf (259/301) 1092/4726

LAN Port Settings

- **IP Address Mode** — Configures the LAN interface to be in static IP mode or DHCP mode. In DHCP mode, a DCHP request is broadcast to the Layer 2 network when the network behavior is set to Layer 2 Bridge. When the network behavior is set to VXLAN, a DHCP request is sent to the core network via the VXLAN tunnel.

- **IP Address** — The static IP address when the IP Address Mode is "Static IP."

- **Subnet Mask** — The subnet mask when the IP Address Mode is "Static IP."

- **Default Gateway** — The IPv4 address of the default gateway, which is used if the requested destination address is not on the local subnet.

- **DNS Entries** — Allows clients to access the web interface through the specified domain from a local network.

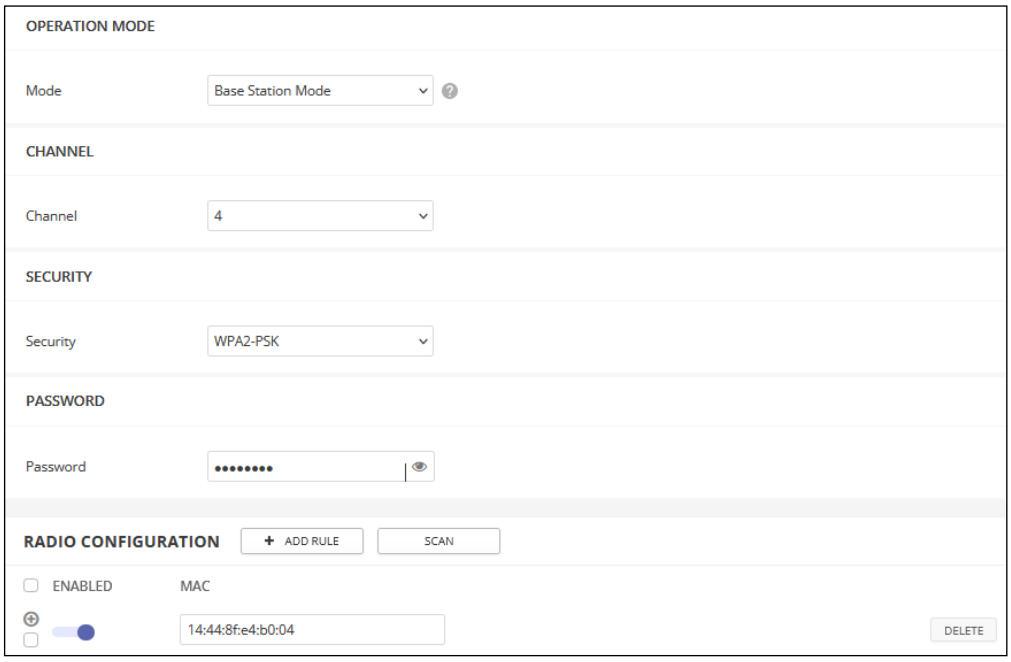
- **Mgmt VLAN** — Select this option to enable a management VLAN on site devices. Once you enable this option, you will no longer be able to access devices on any of the built-in the local networks (for example, 192.168.2.1). You will only be able to access devices from the specified VLAN network. If a device's IP mode is set to DHCP, it will also request a new IP address in the subnet range assigned to the VLAN network.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - Termo de Referência_processo_licitatorio_029_2025_pdf (260/301) 1005/4726

Radio Settings

Click the "Radio Settings" tab to configure the operation mode and security.

Figure 252: Terragraph Device Radio Settings



The following items are displayed on this page:

Operation Mode

- **Mode** — For firmware versions before 1.4.2:
  - **Client Mode (Terragraph Mode)** — Allows a connection to a Terragraph DN device. In this mode, the client passively waits for a DN device to connect.
  - **Client Mode (Point-to-point Mode)** — Allows a connection to a Base Station Mode CN device. In this mode, the client passively waits for a Base Station Mode CN to connect.
  - **Base Station Mode** — Allows links to be created to client mode (Point-to-point Mode) CN devices. For MLTG-CN units, up to 15 links can be created. For MLTG-CN LR units, only one link can be created.
- **Mode** — For firmware versions after 1.5.0:
  - **Client Mode** — Allows connections to DN or Base Station Mode CN devices. In this mode, the client passively waits for a connection.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - Termo de Referência 029_2025_pdf (261/301) 1006/4746

- **Base Station Mode** — Allows links to be created to client mode (Point-to-point Mode) CN devices. For MLTG-CN units, up to 15 links can be created. For MLTG-CN LR units, only one link can be created.

Channel

- **Channel** — In Base Station Mode, you can select the working channel (1 to 4) for a link.

Security

- **Security** — The security method used for the link. In the current version, only WPA2-PSK is supported.

Password

- **Password** — Configures the password for WPA2-PSK.

Radio Configuration

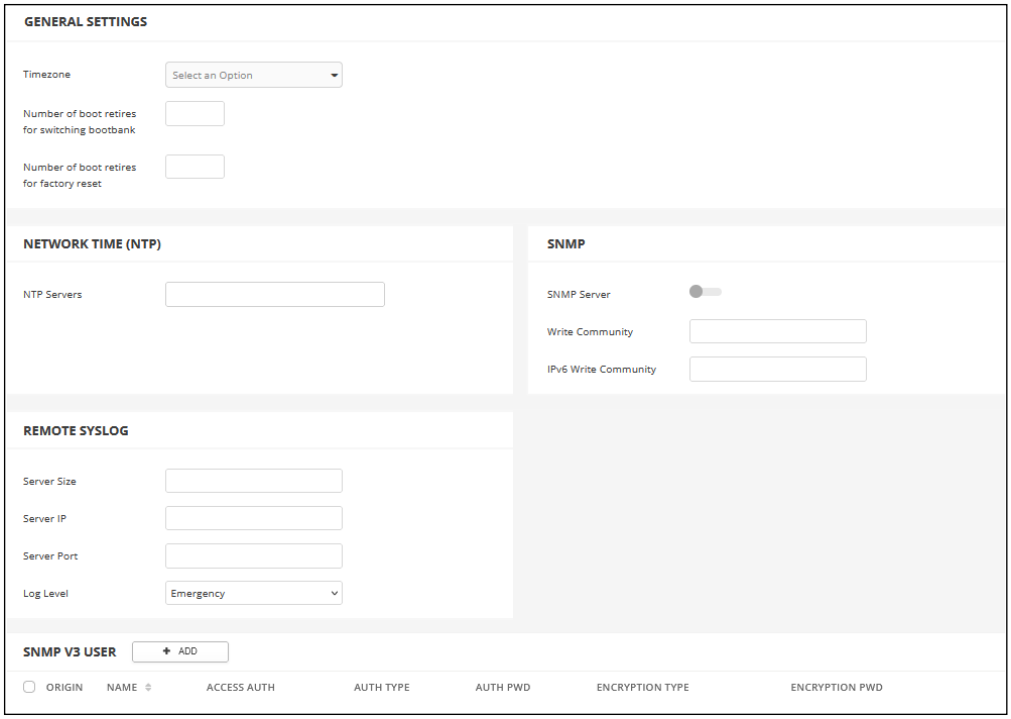
In Base Station Mode, click "ADD RULE" and enter the 60GHz radio MAC address of the another MLTG-CN device. Alternatively, click "SCAN" to find and select MAC addresses of other MLTG-CN devices.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (262/301) 1007/4746

System Settings

Click the "System Settings" tab to configure general settings, NTP, SNMP, and syslog.

Figure 253: Terragraph Device System Settings



The following items are displayed on this page:

General Settings

- **Timezone** — To display a time corresponding to your local time, choose one of the predefined time zones from the pull-down list.
- **Number of boot retires for switching bootbank** — The maximum number of bootup retries before switching to the next boot bank. (Range: 1-254; Default: 5)
- **Number of boot retires for factory reset** — The maximum number of bootup retries before reset device to default. (Range: 1-254; Default: 3)

Network Time (NTP)

Network Time Protocol (NTP) allows the device to set its internal clock based on periodic updates from a time server. The device acts as an NTP client, periodically sending time synchronization requests to specified time servers. The device will attempt to poll each server in the configured sequence to receive a time update.

- **NTP Servers** — Enter IP addresses of NTP servers.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - Termo de Referência_procesSEI_00029_010520_26227.pdf (263/301) 1006/4726

SNMP

The Simple Network Management Protocol (SNMP) is designed specifically for managing devices on a network. It is typically used to configure devices for proper operation in a network environment, as well as to monitor them to evaluate performance or detect potential problems.

- **SNMP Server** — Enables or disables SNMP.
- **Write Community** — A text string that acts like a password and permits access through SNMP protocol version 2. This community string verifies the access of IPv4 users.
- **IPv6 Write Community** — A text string that acts like a password and permits access through SNMP protocol version 2. This community string verifies the access of IPv6 users.

Remote Syslog

The device allows you to control the logging of error messages, including the type of events that are recorded and configure logging to a remote System Log (syslog) server or other management stations.

- **Server Size** — Specifies the available memory used for logging of error messages. (Default: 64 KiB)
- **Server IP** — Specifies the IPv4 or IPv6 address of a remote server which will be sent syslog messages.
- **Server Port** — Specifies the UDP port number used by the remote server. (Range: 1-65535; Default: 514)
- **Log Level** — Use the menu to select the severity of the logs to print to the console. Logs with the severity level you select and all logs of greater severity print. For example, if you select Error, the logged messages include Error, Critical, Alert, and Emergency. The default severity level is Debug(7). The severity can be one of the following levels:

Table 3: Logging Levels

Level	Severity Name	Description
7	Debug	Debugging messages
6	Informational	Informational messages only
5	Notice	Normal but significant condition, such as cold start
4	Warning	Warning conditions (e.g., return false, unexpected return)
3	Error	Error conditions (e.g., invalid input, default used)

* There are only Level 2, 5 and 6 error messages for the current firmware release.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - Termo de Referência_processo_licitatorio_029_2025_pdf (264/301) 1007/4746

Table 3: Logging Levels (Continued)

Level	Severity Name	Description
2	Critical	Critical conditions (e.g., memory allocation, or free memory error - resource exhausted)
1	Alert	Immediate action needed
0	Emergency	System unusable

* There are only Level 2, 5 and 6 error messages for the current firmware release.

SNMP V3 User

SNMP protocol version 3 provides secure access by account authentication and data encryption. The SNMP v3 user list can be defined with the following items.

- **Name** — The user name used to access the SNMP service.
- **Access Auth.** — Select the access permission as "Read Only" or "Write."
- **Auth. Type** — Select the hash algorithm for authentication.
- **Auth. Pwd.** — Configure the password for authentication.
- **Encryption Type** — Select the encryption algorithm for data packets.
- **Encryption Pwd** — Configure the password for data encryption.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_procesos_licitatorios_029_2025_pag 1070/4746

12 Switch Device Configuration

This chapter describes configuration settings for switches at the Device level. It includes the following sections:

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - 07208059825321866289 - 2025 | Anexo Administrativo_processo_licitatorio_029_2025_pag_227.pdf (267/301) 1770/4746

Switch Configuration

Edgecore switch devices can only inherit Site Port Security settings from the Site level. Other settings must be configured at the Device level.

This section covers Device-level configuration for switch devices. ecCLOUD supports switch management for the following Edgecore models.

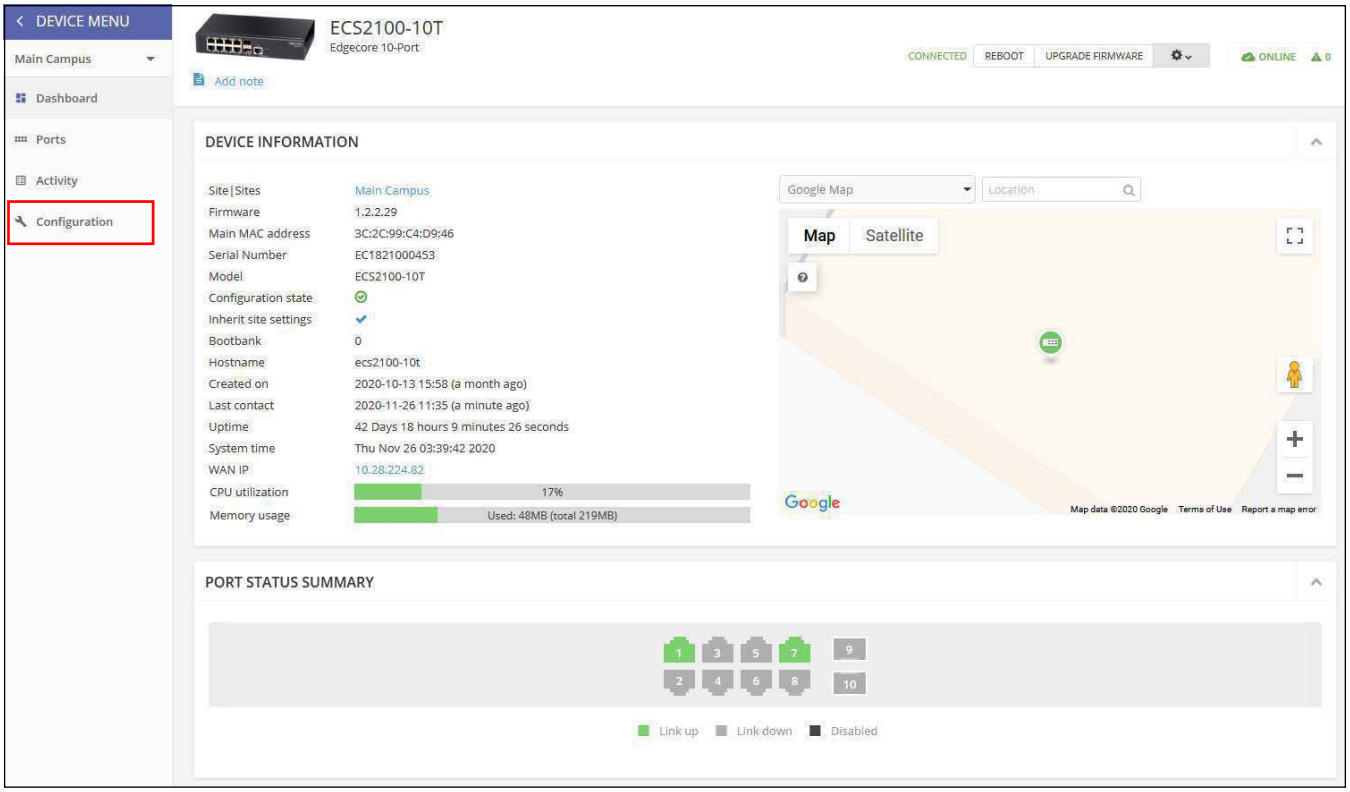
ECS2100-10P, ECS2100-10T, ECS2100-28P, ECS2100-28T, ECS2100-28PP, ECS2100-52T

ECS4100-12T, ECS4100-12PH, ECS4100-28P, ECS4100-28T, ECS4100-52P

ECS4120-28Fv2, ECS4120-28Fv2-I, ECS4120-28T, ECS4120-52T

Note: This chapter provides an example of switch configuration available from ecCLOUD. For complete feature support and configuration, refer to the *Web Management Guide* and *CLI Reference Guide* for the specific switch model, which can be obtained from **www.edgecore.com**.

Figure 254: Switch Device Dashboard

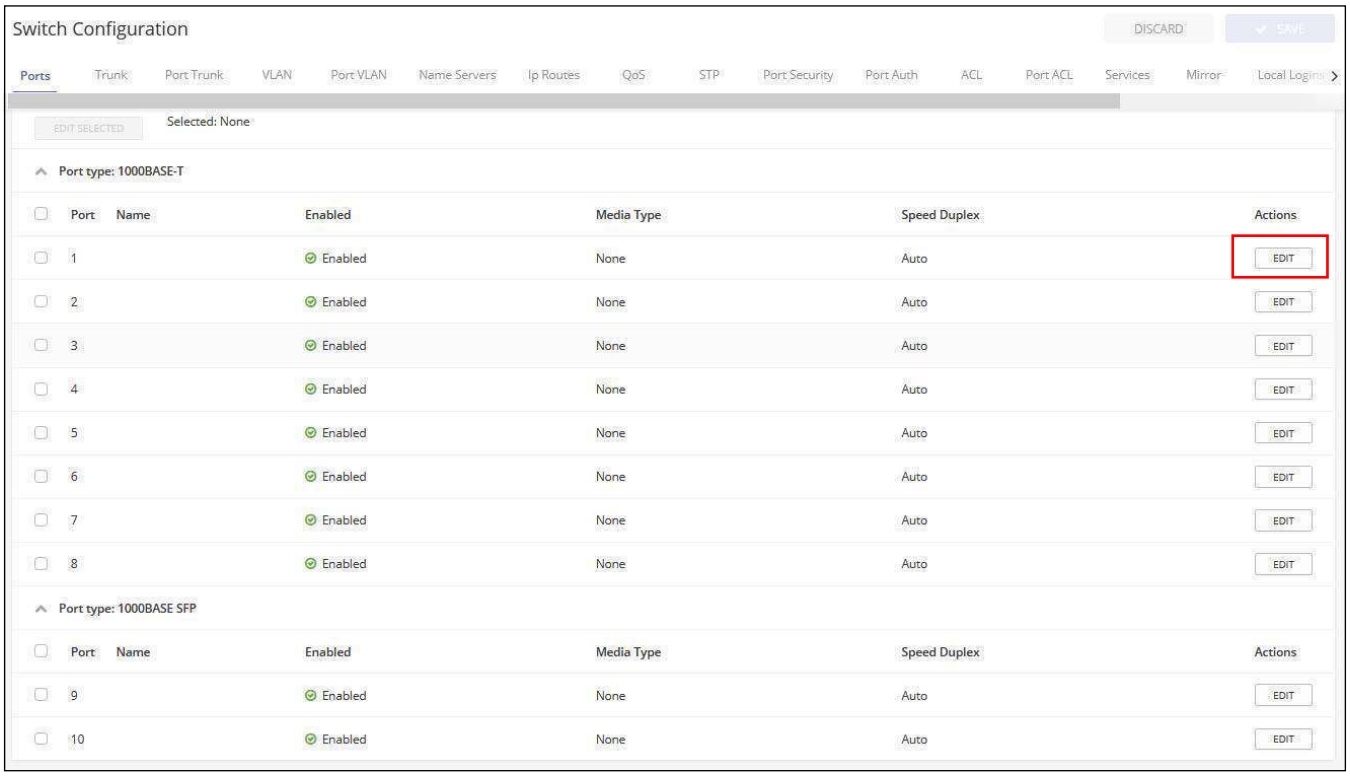


Port Configuration

The switch configuration Ports tab provides access to basic port settings.

Click the EDIT button to enable/disable a port interface, set auto-negotiation and the interface capabilities to advertise, or manually fix the speed, duplex mode, and flow control.

Figure 255: Switch Ports



Trunk Configuration

Trunks are multiple links between devices that work as one virtual, aggregate link. A port trunk offers a dramatic increase in bandwidth for network segments where bottlenecks exist, as well as providing a fault-tolerant link between two devices.

When setting up a static trunk between switches, take note of the following points:

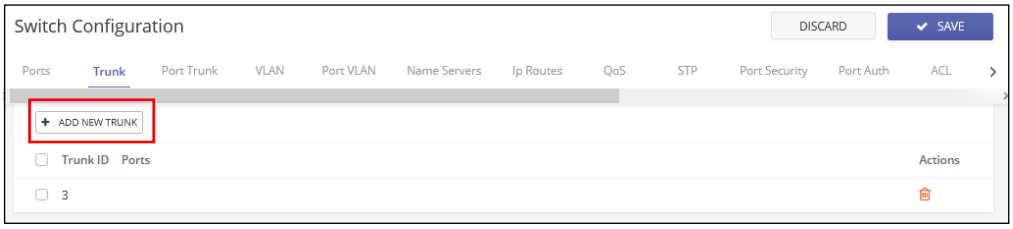
- Finish configuring trunks before you connect the corresponding network cables between switches to avoid creating a loop.
- The ports at both ends of a connection must be configured as trunk ports.
- When configuring static trunks on switches of different types, they must be compatible with the Cisco EtherChannel standard.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (269/301) 1972/4746

- The ports at both ends of a trunk must be configured in an identical manner, including speed, duplex mode, flow control, VLAN assignments, and CoS settings.

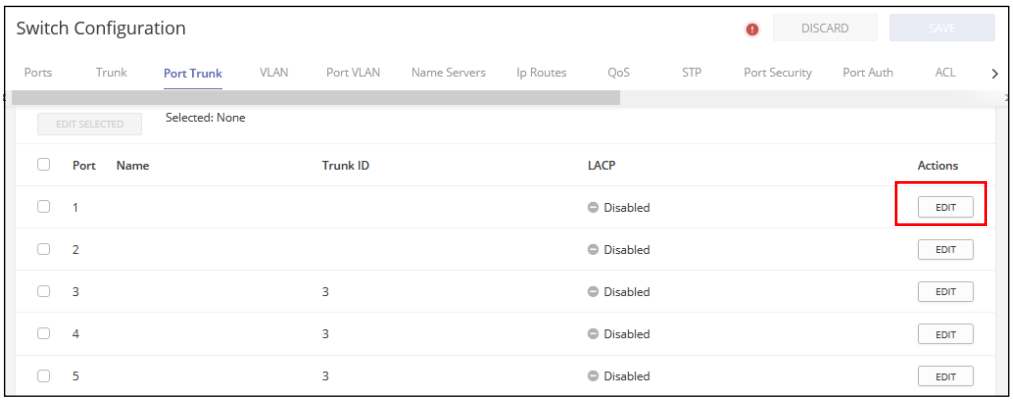
Click the Trunk tab and then the ADD NEW TRUNK button to create a trunk identifier.

Figure 256: Configuring a Trunk



Click the Port Trunk tab to add member ports to a static trunk. Click the EDIT button to assign a trunk ID to a port.

Figure 257: Configuring Trunk Ports



LACP Trunks

The Link Aggregation Control Protocol (LACP) enables dynamic trunks to be created between two switches. LACP-configured ports automatically negotiate a trunked link with LACP-configured ports on another device. You can configure any number of ports on a switch as LACP, as long as they are not already configured as part of a static trunk. If ports on another device are also configured as LACP, the switch and the other device will negotiate a trunk link between them.

When setting up LACP trunks, take note of the following points:

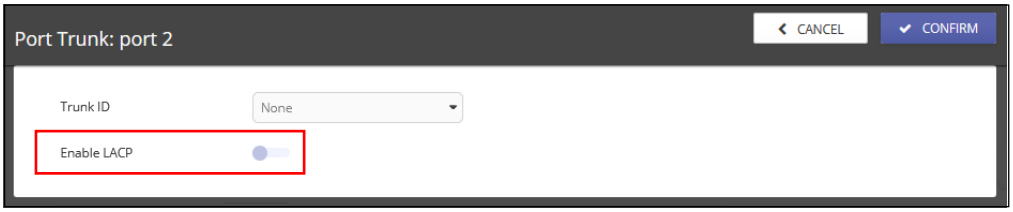
- To avoid creating a loop in the network, be sure you enable LACP before connecting the ports, and also disconnect the ports before disabling LACP.

- If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (270/301) 1975/4746

- A trunk formed with another switch using LACP will automatically be assigned the next available trunk ID.
- If more than the maximum number of ports attached to the same target switch have LACP enabled, the additional ports are placed in standby mode, and will only be enabled if one of the active links fails.
- All ports on both ends of an LACP trunk must be configured for full duplex, and auto-negotiation.

Figure 258: Configuring LACP Trunks

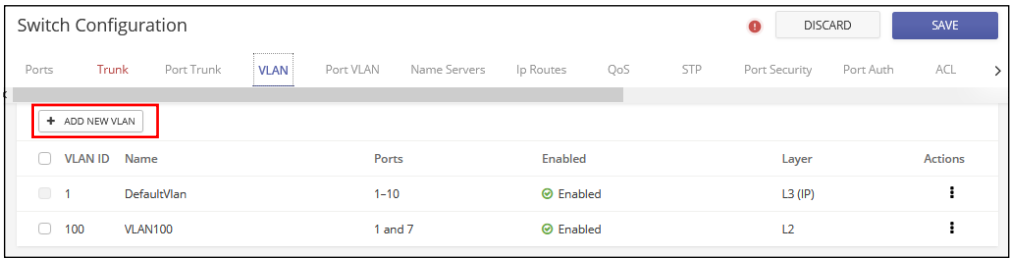


VLAN Configuration

Click the VLAN tab to create or remove VLAN groups, or set the administrative status. To propagate information about VLAN groups used on this switch to external network devices, you must specify a VLAN ID for each of these groups.

Click the ADD NEW VLAN button to create a new VLAN ID. You can also define a VLAN as an Layer 3 interface, which must be configured before you can assign an IP address to a VLAN.

Figure 259: Configuring VLANs



Adding VLAN Port Members

When creating and enabling VLANs for a switch, you must assign each port to the VLAN group(s) in which it will participate. By default, all ports are assigned to VLAN 1 as untagged ports. Add a port as a tagged port if you want it to carry traffic for one or more VLANs, and any intermediate network devices or the host at the other end of the connection supports VLANs. Then assign ports on the other VLAN-aware network devices along the path that will carry this traffic to the same VLAN(s). However, if you want a port on this switch to participate in one or more VLANs, but

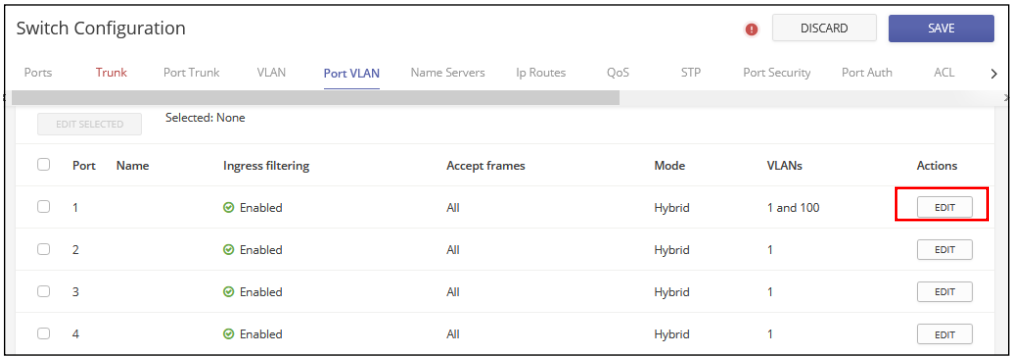
1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (271/301) 1976/4746

none of the intermediate network devices nor the host at the other end of the connection supports VLANs, then you should add this port to the VLAN as an untagged port.

Note: ecCLOUD supports VLAN synchronization between APs and switches. When VLAN tagging is enabled for an SSID, the configured VLAN ID is automatically "pushed" by ecCLOUD to the attached switch port. This enables the VLAN-tagged traffic from the AP to be accepted by the switch port and avoids any loss of connectivity.

Click the Port VLAN tab to show port VLAN membership.

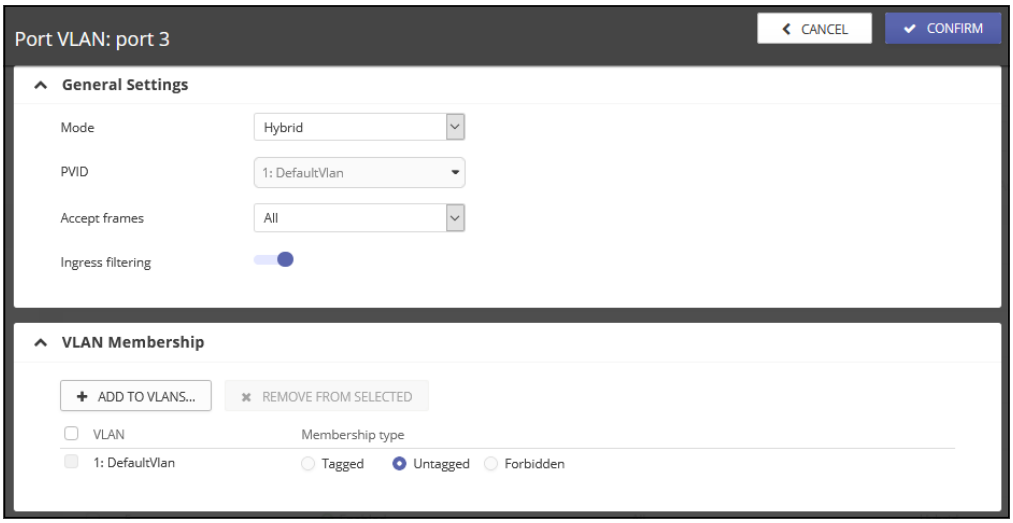
Figure 260: Configuring VLAN Port Members



Click the EDIT button to configure the VLAN behavior for a specific port, including the mode of operation (Hybrid or 1Q Trunk), the default VLAN identifier (PVID), accepted frame types, and ingress filtering. Assign ports as tagged if they are connected to 802.1Q VLAN compliant devices, or untagged they are not connected to any VLAN-aware devices. Or, configure a port as forbidden to prevent the switch from adding it to a VLAN.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_procesos_licitatorios_2025_parte27.pdf (272/301) 1975/4746

Figure 261: Configuring VLAN Port Settings

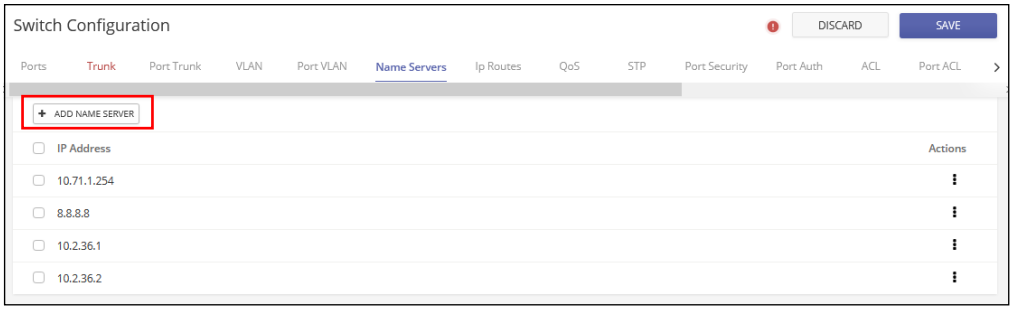


Configuring Name Servers

Click the Name Servers tab to configure a list of name servers to be used for dynamic DNS lookup. When more than one name server is specified, the servers are queried in the specified sequence until a response is received, or the end of the list is reached with no response.

Click the ADD NAME SERVER button and specify the IPv4 or IPv6 address of a domain name server to use for name-to-address resolution.

Figure 262: Configuring Name Servers



Configuring Static IP Routes

Edgecore switches support IP routing and routing path management via static routing definitions. When IP routing is functioning, a switch acts as a wire-speed router, passing traffic between VLANs with different IP interfaces, and routing traffic to external IP networks. However, when a switch is first booted, default routing can

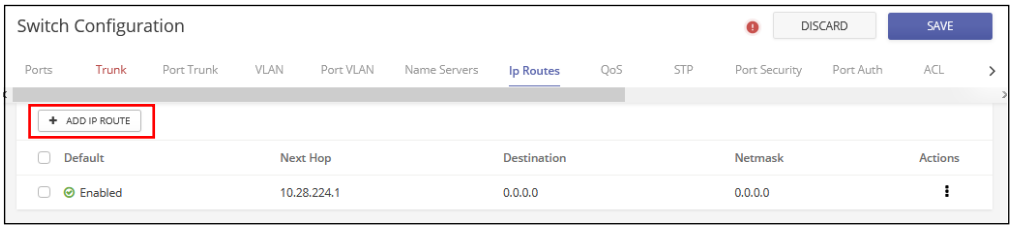
1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (273/301) 1976/4746

only forward traffic between local IP interfaces. As with all traditional routers, static routing needs to be manually configured.

Static routes may be required to force the use of a specific route to a subnet. Static routes do not automatically change in response to changes in network topology, so you should only configure a small number of stable routes to ensure network accessibility.

To enter static routes in the routing table, click the IP Routes tab and then the ADD IP ROUTE button. Specify the destination IP Address and net mask, and the IP address of the next router hop used for the route.

Figure 263: Configuring IP Routes



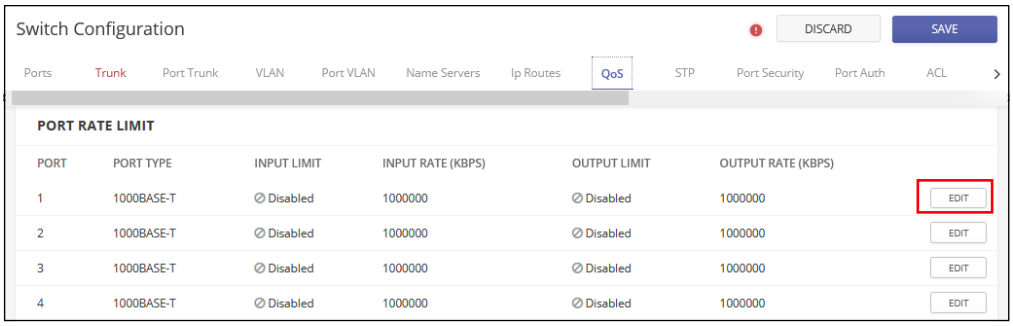
Configuring Port Rate Limiting (QoS)

Click the QoS tab to apply rate limiting to ingress or egress ports. This function allows a network manager to control the maximum rate for traffic received or transmitted on a port interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network.

Rate limiting can be applied to individual ports or trunks. When an interface is configured with this feature, the traffic rate will be monitored by the switch hardware to verify conformity. Non-conforming traffic is dropped, conforming traffic is forwarded without any changes.

Click the EDIT button for a port interface to enable input or output rate limiting and set the required rate limit.

Figure 264: Configuring Port Rate Limiting



STP Configuration

The Spanning Tree Protocol (STP) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STP-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

Edgecore switches support three types of spanning tree protocol:

- **STP** — Spanning Tree Protocol (IEEE 802.1D). (When this option is selected, the switch will use RSTP set to STP forced-compatibility mode.)
- **RSTP** — Rapid Spanning Tree (IEEE 802.1w).
- **MSTP** — Multiple Spanning Tree (IEEE 802.1s).

Click the STP tab and enable STP. Select the protocol and configure the bridge priority, which is used in selecting the spanning tree root device (the network device with the highest priority becomes the STP root device).

Note: For more information on STP configuration, refer to the *Web Management Guide* and *CLI Reference Guide* for the specific switch model, which can be obtained from **www.edgecore.com**.

Figure 265: Configuring STP

Port Security Configuration

You can use Port Security to configure the maximum number of device MAC addresses that can be learned by a switch port, stored in the address table, and authorized to access the network.

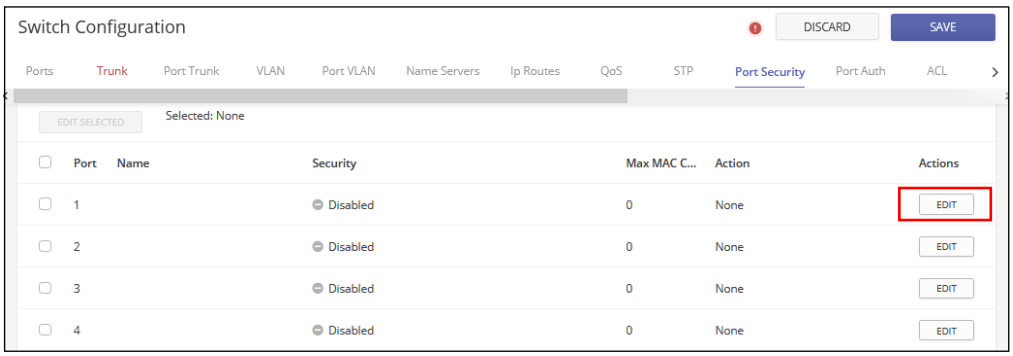
When port security is enabled on a port, the switch stops learning new MAC addresses on the specified port when it has reached a configured maximum

1Doc: Protocolo 1.943/2025 | Procedimiento Administrativo Común - Ley 39/2015 - Tramitación electrónica - Consulta documentos - 2025-0236227.pdf (275/301) 1700/4746

number. Only incoming traffic with source addresses already stored in the address table will be authorized to access the network through that port. If a device with an unauthorized MAC address attempts to use the switch port, the intrusion will be detected and the switch can automatically take action by disabling the port and sending a trap message.

Click the Port Security tab and then the EDIT button for ports you want to configure. Enable security for the port, set the action to take when an invalid address is detected on a port, and set the maximum number of MAC addresses allowed on the port.

Figure 266: Configuring Port Security



Configuring 802.1X Port Authentication

The IEEE 802.1X (802.1X or dot1X) standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. Access to all switch ports in a network can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

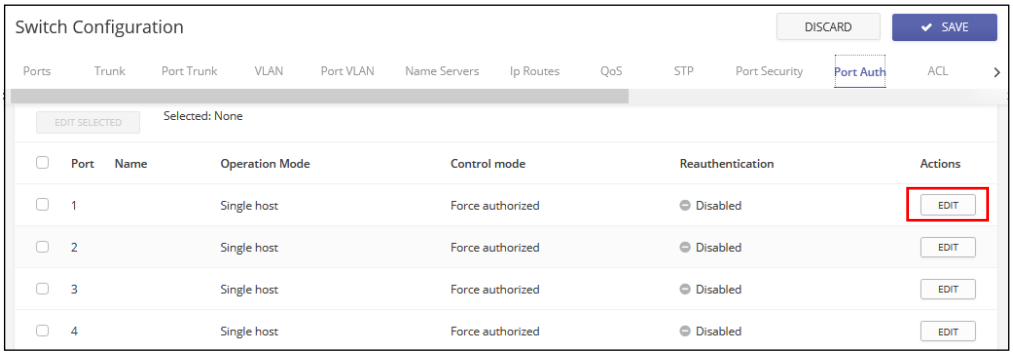
Click the Port Auth tab to configure 802.1X port settings for the switch as the local authenticator. When 802.1X is enabled, you need to configure the parameters for the authentication process that runs between the client and the switch (that is, the authenticator), as well as the client identity lookup process that runs between the switch and authentication server.

For information on authentication server configuration, see "Configuring Login Authentication" on page 283.

Click the EDIT button for a port to configure the port authentication details.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pagina 276 (276/301) 1969/4726

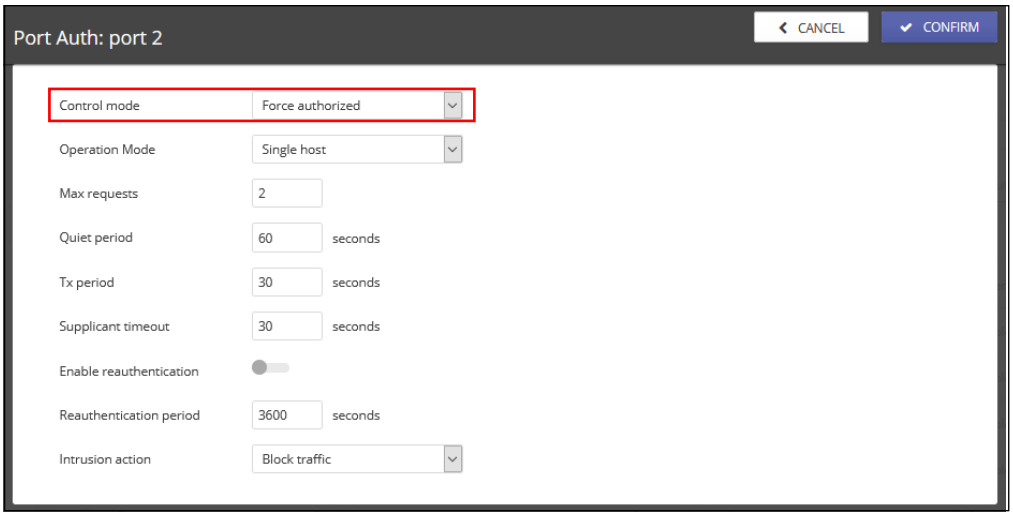
Figure 267: Configuring Port Authentication



When the switch functions as a local authenticator between supplicant devices attached to a switch port and the authentication server, you need to configure the parameters for the exchange of EAP messages between the authenticator and clients on the Authenticator configuration page.

On the port authentication details page, set the port Control Mode to "Auto" to enable authentication.

Figure 268: Configuring Port Authentication



Note: For more information on port authentication configuration, refer to the *Web Management Guide* and *CLI Reference Guide* for the specific switch model, which can be obtained from **www.edgecore.com**.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_procesoDigital_029_20252026227.pdf (277/301) 378/476

ACL Configuration

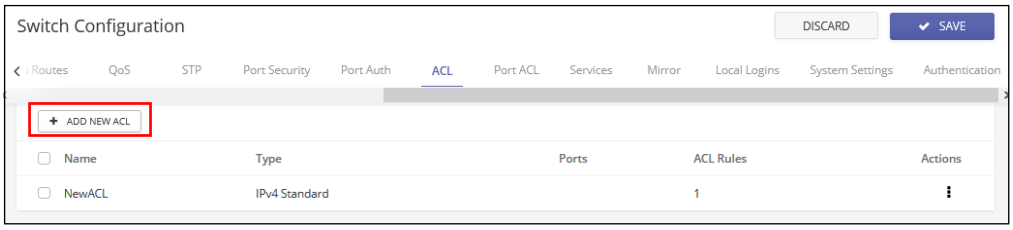
Access Control Lists (ACL) provide ingress packet filtering for IPv4/IPv6 frames (based on address, protocol, Layer 4 protocol port number or TCP control code), IPv6 frames (based on address, DSCP traffic class), or any frames (based on MAC address or Ethernet type). To filter incoming packets, first create an access list, add the required rules, and then bind the list to a specific port.

An ACL is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. The switch tests ingress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match, the packet is accepted.

To configure an ACL, click the ACL tab and then the ADD NEW ACL button. Select the type of ACL you want to configure:

- **IPv4 Standard** — Configures an ACL based on source IPv4 addresses.
- **IPv4 Extended** — Configures an ACL based on source and destination IPv4 addresses, TCP/UDP port number, protocol type, and TCP control code.
- **IPv6 Standard** — Configures an ACL based on source IPv6 addresses.
- **IPv6 Extended** — Configures an ACL based on source and destination IPv6 addresses, DSCP traffic class, or next header type.
- **MAC** — Configures an ACL based on hardware addresses, packet format, and Ethernet type.
- **ARP** — Configures an ACL based on ARP messages addresses.

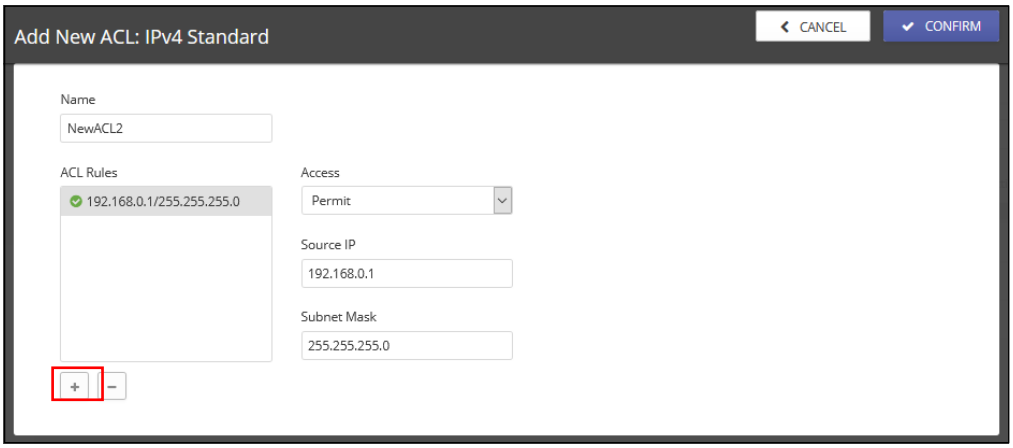
Figure 269: Configuring ACLs



On the Add New ACL page, give the ACL a name and then click the "+" button to configure rules to add to the ACL.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 3 - Termo de Referência_procesSoDigitalNo_029_2025_pdf (278/301) 3783/4746

Figure 270: Adding a New ACL

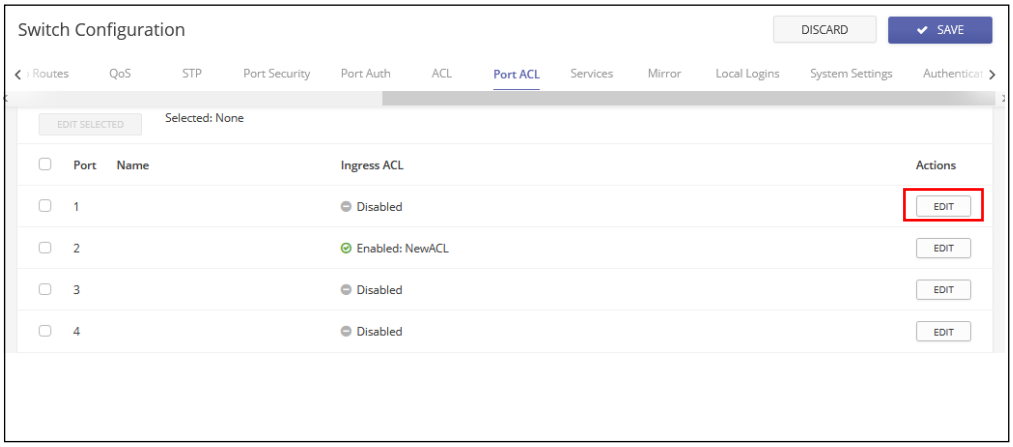


Binding Ports to an ACL

After configuring ACLs, click the Port ACL tab to bind the ports that need to filter ingress traffic to the appropriate ACLs.

Click the EDIT button to configure an ACL for a port.

Figure 271: Port ACL Bindings



On the Port ACL edit page, select the configured ACL name, enable the ACL, and optionally enable counters to collect ACL statistics.

Figure 272: Binding Ports to ACLs

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 6 processo 02912.000227.pdf (279/301) 3782/4746

Note: For more information on ACL configuration, refer to the *Web Management Guide* and *CLI Reference Guide* for the specific switch model, which can be obtained from **www.edgecore.com**.

Configuring Switch Services

Click the Services tab to configure Telnet and web server access to the switch, and to configure network time.

Enable the Telnet server for accessing the switch CLI over a Telnet connection.

Enable the HTTP web server for access to switch management using a web browser interface.

You can also enable HTTPS over the Secure Socket Layer (SSL), providing secure access (an encrypted connection) to the switch's web interface.

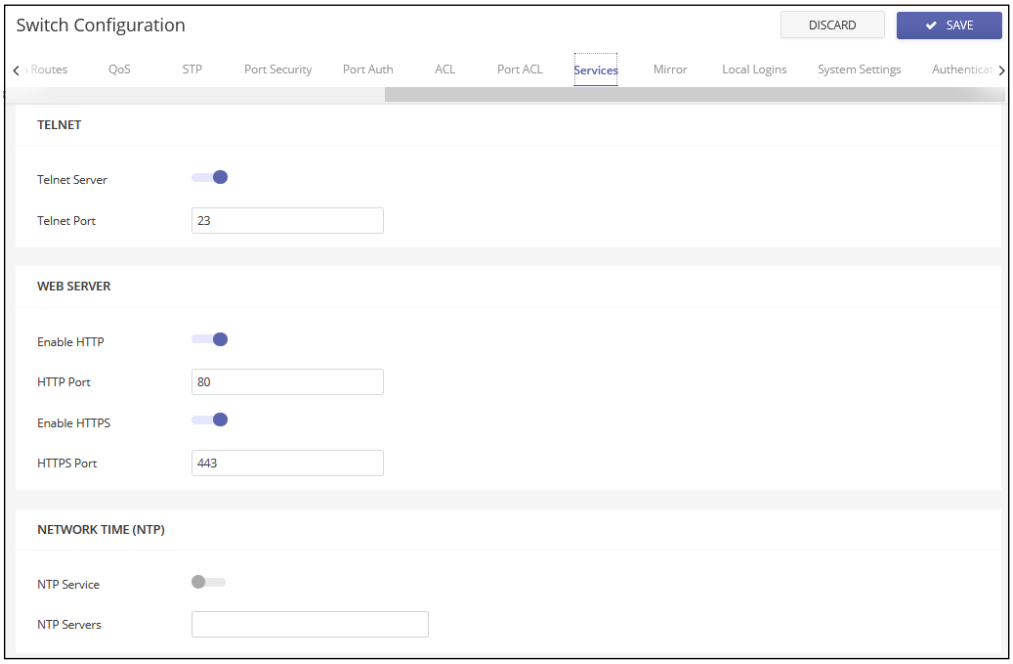
Both the HTTP and HTTPS service can be enabled independently on the switch. However, you cannot configure both services to use the same TCP port.

The Network Time Protocol (NTP) allows a switch to set its internal clock based on periodic updates from a time server. Maintaining an accurate time on a switch enables the system log to record meaningful dates and times for event entries.

To configure NTP, enter the IPv4 address for up to three time servers and then enable the NTP service. The switch will poll all the time servers configured, the responses received are filtered and compared to determine the most reliable and accurate time update for the switch.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo processo licitatório 029_2025_pregão 027.pdf (280/301) 1783/4726

Figure 273: Switch Services

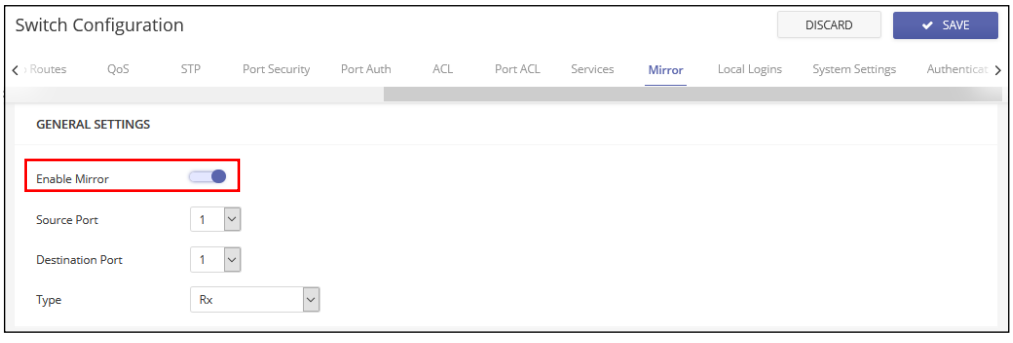


Configuring Port Mirroring

Use the Mirror tab to mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.

Enable mirroring, select the source and destination ports, and the type of traffic to mirror; received, transmitted, or both.

Figure 274: Port Mirroring



1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pregao_27.pdf (281/301) 3736/4726

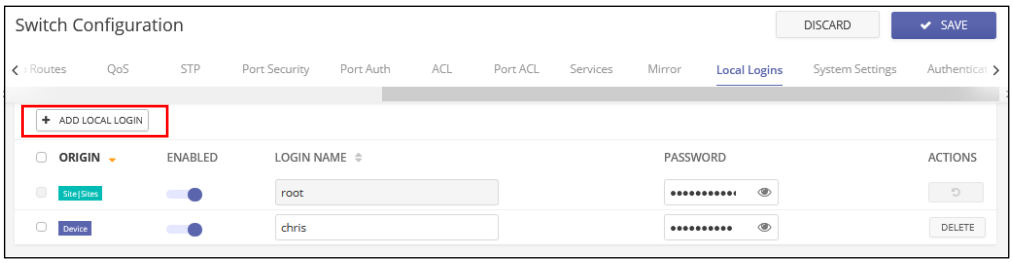
Configuring Local Logins

Use the Local Logins tab to control management access to the switch based on manually configured user names and passwords.

The Local Logins have one account configured by default using a randomly-generated password. You can modify the password and configure additional local accounts as needed.

Note: The Local Logins default account is from the ecCLOUD Site-level configuration and it will overwrite the default account previously configured on the local user interface of a device. Once the Site-level configuration has been pushed to devices, you must use Local Login accounts configured at the ecCLOUD Device-level configuration.

Figure 275: Local Login Configuration



Configuring System Settings

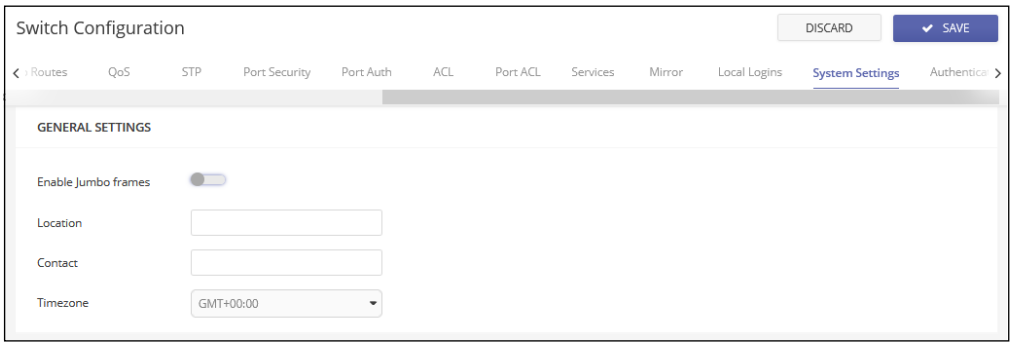
Use the System Settings tab to identify the system by displaying information such as the device location and contact information. You can also enable jumbo frames and configure the local timezone.

Edgecore switches include support for layer 2 jumbo frames. A switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames up to 10240 bytes for Gigabit Ethernet and 10 Gigabit Ethernet ports or trunks. Compared to standard Ethernet frames that run only up to 1.5 KB, using jumbo frames significantly reduces the per-packet overhead required to process protocol encapsulation fields.

You should also set the time zone of your switch location. NTP uses Coordinated Universal Time (or UTC, formerly Greenwich Mean Time, or GMT) based on the time at the Earth's prime meridian, zero degrees longitude, which passes through Greenwich, England. To display a time corresponding to your local time, you must indicate the number of hours and minutes your time zone is east (before) or west (after) of UTC. You can choose one of the predefined time zone definitions.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_procesoDigital_029_20252026227.pdf (282/301) 1985/4746

Figure 276: System Settings



Configuring Login Authentication

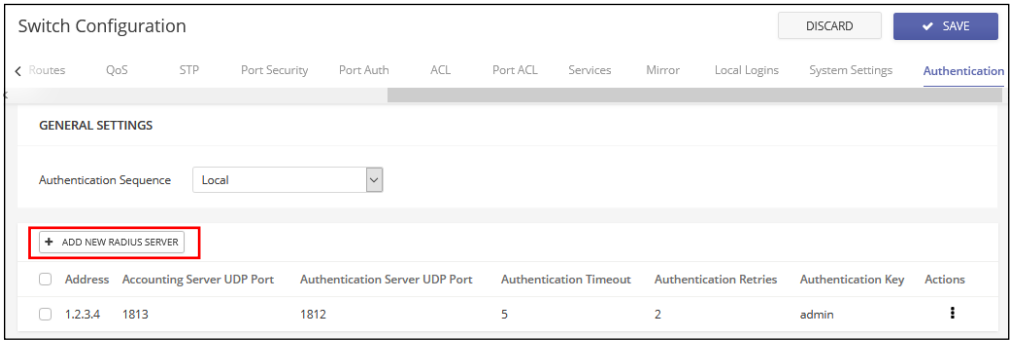
Use the Authentication tab to specify local or remote authentication. Local and remote login authentication control management access via the console port, web browser, or Telnet.

Local authentication restricts management access based on user names and passwords. Remote authentication uses a remote access authentication server based on RADIUS or TACACS+ protocols to verify management access.

By default, management access is always checked against the local authentication database. If a remote authentication server is used, you must specify the authentication sequence. Then specify the corresponding parameters for the remote authentication servers.

You can specify up to three authentication methods for any user to indicate the authentication sequence. For example, if you select (1) RADIUS, (2) TACACS and (3) Local, the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted using the TACACS+ server, and finally the local user name and password is checked.

Figure 277: Login Authentication



1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pag27.pdf (283/301) 3738/4746

To add authentication servers, click the ADD NEW RADIUS SERVER button and configure the IP address and other server details.

Figure 278: Adding Authentication Servers

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (285/301) 1798/4746

13 SD-WAN Device Configuration

This chapter describes configuration settings for SD-WAN at the Device level. It includes the following sections:

Accessing SD-WAN Device-Level Configuration

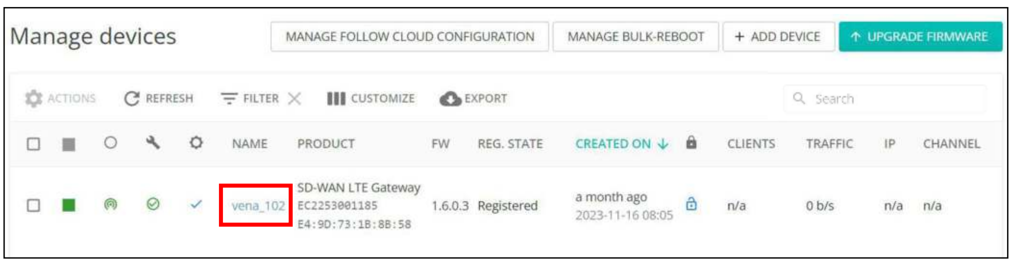
When a device's "Inheritance Policy" is enabled, the device is configured from the Site level. However, a device can be individually configured at the Device level and the settings will override the Site-level configuration.

Note: Individual device overrides can be reset to the Site-level configuration by clicking the "Use Site Settings" button on the page where a setting has been changed.

In addition, SD-WAN Devices include settings not configurable at the Site level, such as advanced settings and features unique to a specific product. These settings can only be configured at the Device level.

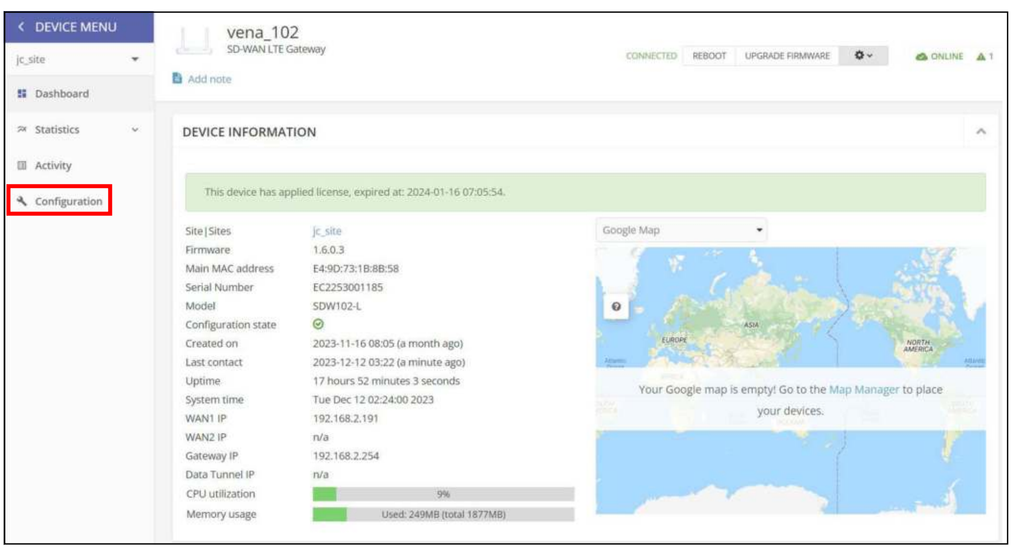
To access configuration for a device, click on the device name from the Site-level list of devices (also available from the Cloud-level list of devices).

Figure 279: Accessing Device-Level Configuration



From the Device dashboard, click on "Configuration" on the Device menu to access a device's configuration.

Figure 280: Device-Level Dashboard



1Doc: Protocolo 1.943/2025 ... .pdf (287/301)

This chapter only covers the device configuration that is different from the Site-level configuration, as documented in "Site SD-WAN Configuration" on page 216.

WAN

Click the "WAN" tab to configure settings. The following items are displayed on the WAN tab.

WAN

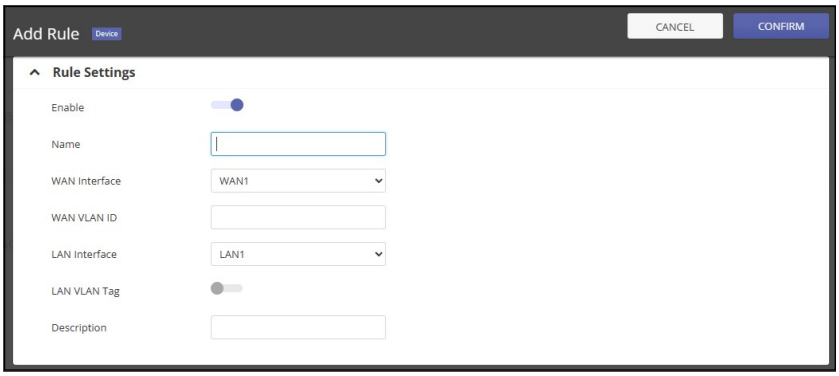
Figure 281: Device WAN Configuration

- **WAN Provisioning** — Configure the settings of WAN1 and WAN2. Each interface can be configured independently.
- **Type** — The method used to provide an IP address for the WAN Interface. (Default: DHCP. Other options: Static IP, PPPOE)
- **IP Address** — Enter the IP address here.
- **Netmask** — Specify the subnet mask associated with the WAN1 IP address.
- **Gateway** — Define the gateway IP address for WAN1 to route traffic outside the local network.
- **DNS 1** — Enter the primary DNS server IP address.
- **DNS 2** — Enter the secondary DNS server IP address.
- **NAT** — Enable or disable the NAT function.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (288/301) 1793/4746

WAN VLAN Passthrough

Figure 282: Create a New WAN VLAN Passthrough Rule



Add rules to allow traffic to traverse from the WAN to specified LAN interfaces. In the WAN VLAN Passthrough table, each entry can be enabled or disabled and comprises:

- **Name** — Define a name for the passthrough rule.
- **WAN Interface** — Designated WAN interface for the rule.
- **WAN VLAN ID** — VLAN ID tagged for the WAN, specifying which VLAN's traffic is to pass through.
- **LAN Interface** — Target LAN interface for the VLAN traffic.
- **LAN VLAN Tag** — VLAN ID assigned to the LAN interface, when VLAN tagging is enabled.
- **Description** — A brief note describing the rule.

WAN Internet Prefer

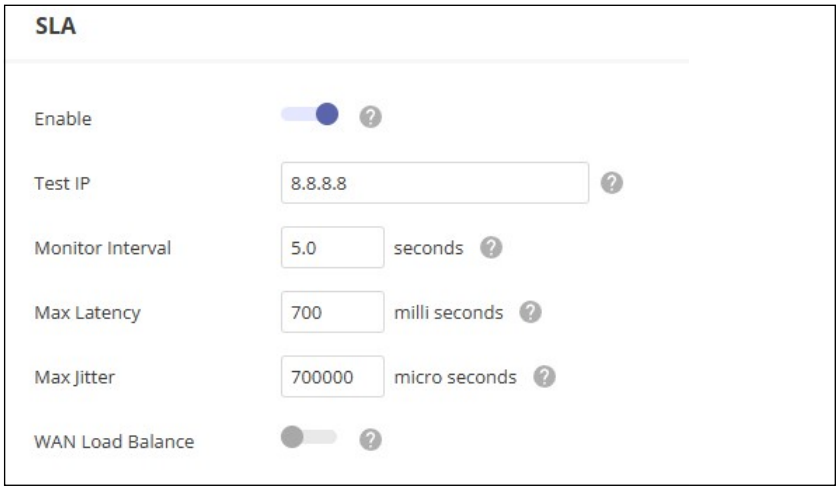
Figure 283: Select the Preferred WAN Interface for Internet Connectivity

- **Prefer WAN** — Select the WAN interface (WAN1 or WAN2) to be given priority for Internet traffic. If 'Disable' is selected, no preference is given, and the device will manage WAN selection based on availability or other load balancing setting.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo processo 029_2025_pdf (289/301) 1792/4746

SLA

Figure 284: SLA Configuration



- **Test IP** — Enter the IP address used to test the link quality.
- **Monitor Interval** — Set the time interval, in seconds, for how frequently the link quality is assessed.
- **Max Latency** — Maximum acceptable latency of qualified service level in milliseconds. The device changes the default route if this threshold is exceeded.
- **Max Jitter** — Maximum acceptable jitter of qualified service level in microseconds. The device changes the default route if this threshold is exceeded.
- **WAN Load Balance** — Enable or disable load balancing across WAN interfaces for Internet access.

Traffic Steering

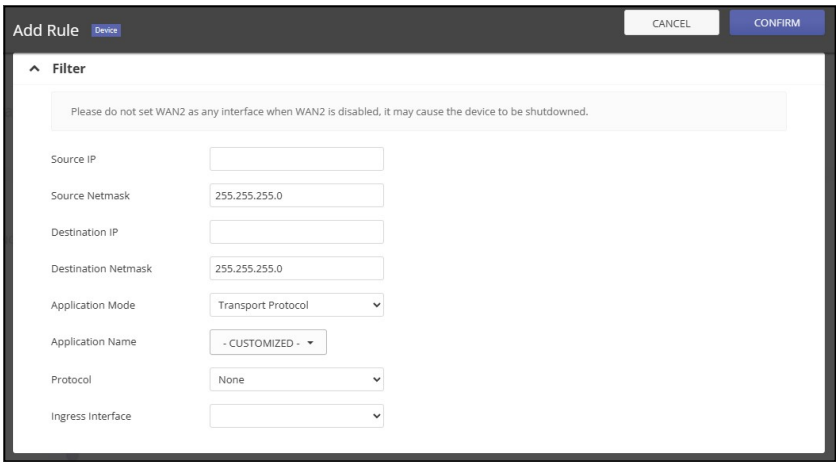
Allows for the management of network traffic direction based on specific rules.

- **Name** — Enter a name for the rule.
- **Mode** — Defines the steering behavior (Available, Mandatory, Load Balance).
- **IP Address (Source > Destination)** — Source and destination IP addresses of targeted packets.
- **Application/Protocol (Source > Destination)** — Choose a predefined application or set custom parameters for traffic matching or select customize and specify the protocol to use.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (290/301) 1725/4746

- **Interface Preferred/Backup** — The link (interface) which rule-matching target packets are forward to and when the preferred interface is unavailable.
- **Actions** — Edit or delete this traffic steering rule configuration.

Figure 285: Add Traffic Steering Filtering Rule



Add a new steering rule to control how traffic is directed through the network:

- **Source IP** — Enter the source IP or network IP.
- **Source Netmask** — Define the network netmask for the source IP.
- **Destination IP** — Specify the destination IP or network IP.
- **Destination Netmask** — Define the network mask for the destination IP.
- **Application** — Automatically set IP Protocol number, default destination IP port of filter rule for common application.
  - Customized applications require manually specify the source and destination ports, and the IP protocol rule number.
  - GRE protocol, IP protocol number: 47
  - ESP protocol, IP protocol number: 50
  - IGMP protocol IGMP protocol, IP protocol number: 2
  - SNMP protocol, UDP destination port: 21
  - SSH protocol, TCP destination port: 22
  - Telnet protocol, TCP destination port: 23
  - Web HTTP protocol, TCP destination port: 80

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_procesoDistancia_029_2025_page27.pdf (291/301) 1726/4746

- Web HTTPS protocol, TCP destination port: 443
- Email POP3 protocol, TCP destination port: 110
- Email SMTP protocol, TCP destination port: 25
- Email IMAP protocol, TCP destination port: 143
- Video RTP protocol, UDP destination port: 5004, 5005
- Video RTSP protocol, TCP/UDP destination port: 554
- Video RSVP protocol, TCP/UDP destination port: 3455
- VPN L2TP protocol, UDP destination port: 1701
- VPN PPTP protocol, TCP destination port: 1723
- VPN ISAKMP protocol, UDP destination port: 500
- VPN IPSec protocol, UDP destination port: 4500
- VoIP H.323 protocol, TCP destination port: 1720
- VoIP SIP protocol, TCP destination port: 5060

- **Ingress Interface** — Choose the ingress interface from options such as WAN1, WAN2, TUN, LAN, or specific VPN tunnels.

Figure 286: Configure Action to Filter-Matching Packets

- **Actions** — Edit or delete this traffic steering rule configurations.
  - **Name** — Name the filtering rule.
  - **Mode** — Set the Traffic Steering behavior:
    - **Available** — Traffic defaults to the preferred interface and falls back to the backup interface if needed.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo 03 - TR 2025 | Anexo Administrativo EC processo Licitatorio 029_2025 pdf (292/301) 1995/4746

- **Mandatory** — Traffic is strictly sent through the preferred interface or dropped if unavailable.
- **Load Balance** — Distributes traffic between the preferred and backup interfaces based on current load and availability.

- **Multipath Default** — Enable or Disable traffic multipath capability. (Default is Disabled)
- **Prefer Interface** — Select the primary interface to forward packets matching the rule.
- **Prefer Gateway** — Define the IP Address of the primary gateway.
- **Backup Interface** — Select an alternative interface to forward packets matching the rule if the preferred interface is unavailable.
- **Backup Gateway** — (Optional) Define an alternative gateway for use if the preferred gateway is unavailable.

LAN

Click the "LAN" tab to configure the Default LAN settings, DHCP Server settings, and define additional LAN subnets.

Default LAN

Figure 287: Default LAN and DHCP Server Configuration

- **IP Address** — Enter the IP address for the default LAN interface.
- **Subnet Mask** — Select the netmask for the default LAN.
- **DHCP Server** — Toggle this to enable or disable the DHCP (Dynamic Host Configuration Protocol) server.
- **DHCP Start and End** — Define the range of IP addresses in the DHCP pool, starting with the lowest assignable address and ending with the highest.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo processo 029_2025_00227.pdf (293/301) 1998/4746

- **Lease Time** — The duration, in seconds, that an IP address is assigned to a DHCP client.
- **DNS1** — The IP address of the primary Domain Name Server for network name resolution.
- **DNS2** — The IP address of a secondary Domain Name Server for network name resolution.

Additional LAN Subnet

Click "Add LAN" and configure additional LAN Subnets:

- **Name** — Define a name for the new subnet.
- **IP Address** — Set the LAN IP address for the subnet.
- **Subnet Mask** — Select the netmask of LAN IP address.
- **Port** — Select the local physical network interface for the subnet.
- **VLAN Tag** — Enable or disable VLAN Tagging for traffic segmentation.
  - **VLAN ID** — Set the VLAN ID within the range of 1 to 3999.
- **Remote Accessible** — The subnet can be other edge for VPN Group or P2P tunnel port to access.
- **DHCP Server** — Toggle this to enable or disable the DHCP (Dynamic Host Configuration Protocol) server.
- **DHCP Start and End** — Define the range of IP addresses in the DHCP pool, starting with the lowest assignable address and ending with the highest.
- **Lease Time** — The duration, in seconds, that an IP address is assigned to a DHCP client.
- **DNS1** — The IP address of the primary Domain Name Server for network name resolution.
- **DNS2** — The IP address of a secondary Domain Name Server for network name resolution.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo processo licitatório 029_2025_pdf (294/301) 1999/4746

Static Route

Click the “Static Route” tab to configure the list of static routes.

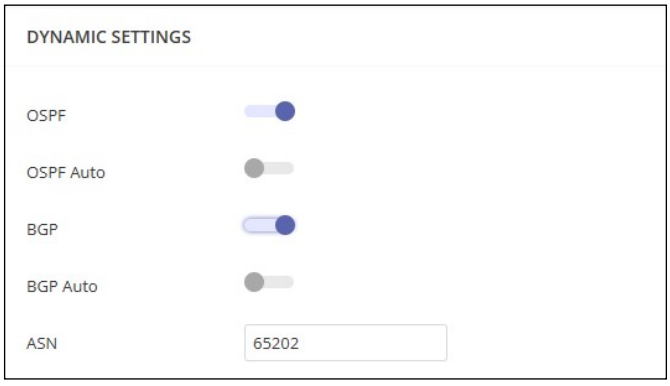
Figure 288: Static Route Configuration

- **Destination IP** — Enter the destination IP address. Valid IP addresses consist of four decimal numbers, ranging from 0 to 255, separated by periods.
- **Netmask** — Select the netmask that corresponds to the destination IP address. (Default: 255.255.255.0)
- **Gateway** — The IP address of the gateway router, which will be used to route traffic to destinations not on the local network.
- **Interface** — The point of interconnection between a device and a private or public network. Options include physical interfaces such as WANs or LANs, and virtual interfaces like multi-subnets.
- **Metric** — Assign a metric value to the route, which is used to determine its precedence within the routing table. A lower metric value gives the route a higher priority.

Dynamic Route

Click the “Dynamic Route” tab to manage the OSPF (Open Shortest Path First) and BGP (Border Gateway Protocol) protocols, as well as to configure dynamic routes.

Figure 289: Dynamic Settings Configuration



- **OSPF** — Enable or disable the OSPF protocol.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (295/301) 2708/4746

- **OSPF Auto** — When enabled, OSPF configuration is automated to include the default LAN, multi-subnets marked as 'Remote Accessible', VPN group subnets, and P2P tunnel IP subnets.
- **BGP** — Enable or disable the BGP protocol.
- **BGP Auto** — Automatically configures BGP settings, including default LAN, multi-subnets marked as 'Remote Accessible,' VPN group subnets, P2P tunnel IP subnets, and BGP Neighbors.
- **BGP ASN** — Enter the BGP Autonomous System Number (ASN) to identify the device in BGP routing networks.

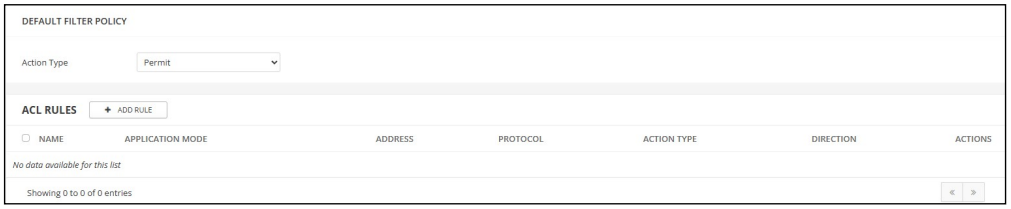
Figure 290: Add New Dynamic Route

- **Classification** — Select the protocol classification for the new route, whether OSPF or BGP.
- **Protocol** — Choose the type of protocol item to configure, such as BGP Network, OSPF Network, or BGP Neighbor.
- **IP Address** — Specify the network IP for BGP or OSPF Networks, or the neighbor IP for BGP Neighbor configurations.
- **Netmask** — Select the netmask for the BGP or OSPF Network, or for the BGP Neighbor.
- **Area/ASN** — Enter the OSPF Area number or the BGP ASN, as applicable to the chosen protocol.

Access Control

Navigate to the "Access Control" tab to configure endpoint security settings.

Figure 291: Define the Default Filter Policy

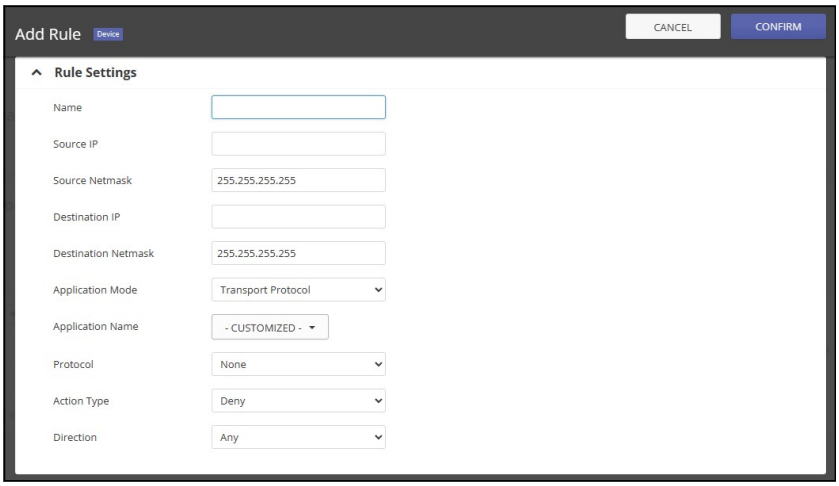


- **Default Filter Policy** — Set the default Access Control to either deny or permit network traffic.

ACL Rules

- **Name** — Define a name for the rule.
- **Application Mode** — Choose between the protocol "Transport Protocol" (dependent on the protocol mode) and Application Layer Protocol (based on the application-to-layer protocol) to define the rule's active mode.
- **Address (Source > Destination)** — Define the source and destination IPs of traffic to match the rule.
- **Protocol/Port (Source > Destination)** — Define the source and destination ports of traffic to match the rule.
- **Action Type** — Select if the rule should deny or permit the traffic.
- **Direction** — Select between 'Outbound' (only outbound traffic) and 'ANY' (both inbound and outbound traffic) as the protection direction.
- **Actions** — Modify or delete the selected ACL rule.

Figure 292: Configuration of a New Access Control Rule



- **Name** — Define a name for the rule name.
- **Source IP** — Specify the original source IP value.
- **Source Netmask** — Set the source IP subnet mask.
- **Destination IP** — Set the destination IP value.
- **Destination Netmask** — Set the destination IP subnet mask.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (297/301) 297/476

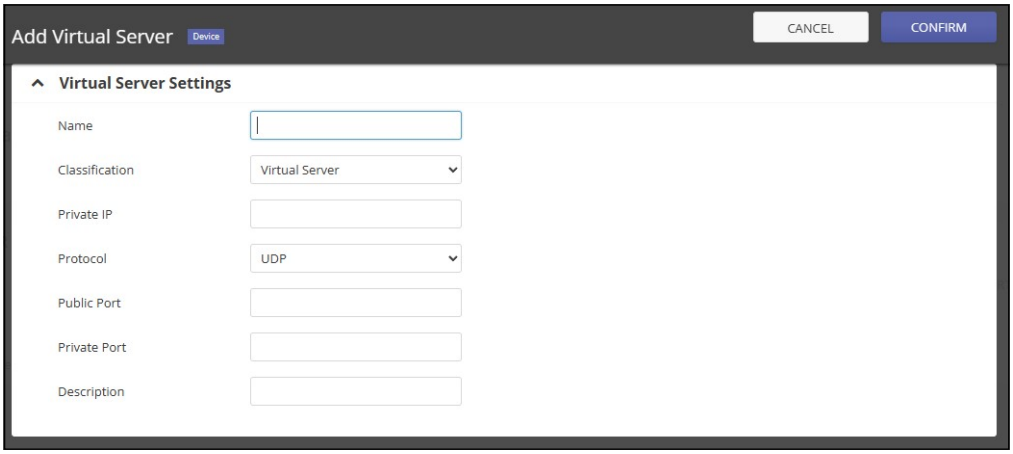
- **Application Mode** — Select the dependent the protocol mode (Transport Protocol) or the application mode (Application-to Layer Protocol) to set the active mode.
- **Application Name** — Set public application protocol the system will use relating and it can use multi applications.
- **Protocol** — Selecting UDP, TCP, or UDP/TCP and enter valid port numbers ranging from 1 to 65535 for both the source and destination ports. If IP Protocol is chosen, only the IP address is required.
- **Action Type** — Select whether the rule should deny or permit traffic..
- **Direction** — Select the protection direction as either 'Outbound' (only outbound) or 'ANY' (both inbound and outbound). When using the 'Application Layer Protocol', Direction is set to ANY.

Virtual Server

A Virtual Server allows remote computers to connect to specific computers or services within a private Local Area Network (LAN). It can do so using two primary mechanisms: Virtual Server (also known as Port-Forwarding) and 1-to-1 NAT (Network Address Translation) mapping.

The Virtual Server Section lists all configured virtual servers.

Figure 293: New Virtual Server Settings



Click "Add Virtual Server" and configure the settings of a new virtual server:

- **Name** — Enter a name for the virtual server entry.
- **Classification** — Choose the type of virtual server to deploy:

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (298/301) 2703/4746

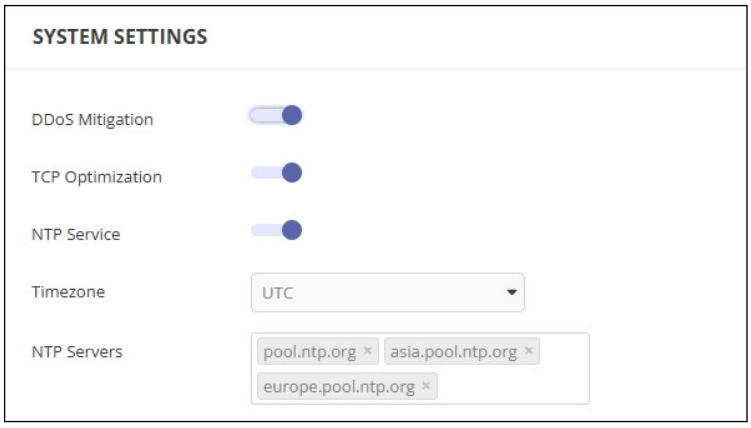
- **Virtual Server** — Redirects communication requests from one address and port number to another while traversing a network gateway. Useful for accessing services on a host within a protected network by remapping the destination address and port number to an internal host via a WAN interface.
- **1to1 NAT** — Maps one external IP address (typically public) to one internal IP address within LAN subnets. Overrides the Outbound NAT configuration for traffic from the private IP address to the Internet and vice versa.

- **Public IP Alias Inbound Interface** — Select the outbound WAN interface (WAN1 or WAN2) associated with the public IP alias.
- **Public IP Alias** — Specify the external (public) IP address for mapping.
- **Private IP** — Define the internal IP address to forward the packets.
- **Protocol** — Select the protocols for the virtual server (UDP or TCP).
- **Public Port** — Set the original destination port for packets via the WAN interface.
- **Private Port** — Define the internal port to redirected packets.
- **Description** — Add a brief comment to identify this virtual server setup.

System Settings

Access the "System Settings" tab to manage SD-WAN features at the device level.

Figure 294: SD-WAN Device System Settings



The following items are displayed on this page:

- **DDoS Mitigation** — Enable the Distributed Denial of Service (DDoS) mitigation mechanism within the Routing/System Control domain.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (299/301) 2704/4746

- **TCP Optimization** — Activate TCP Optimization to enhance the performance of TCP (Transmission Control Protocol) traffic across the network.
- **NTP Service** — Enable the Network Time Protocol (NTP) service to send time updates request to maintain accurate system time.
- **Time Zone** — Select the appropriate time zone from the dropdown list to ensure the device displays the local time accurately.
- **NTP Servers** — Configure the hostnames for NTP servers. The Bsta server initially attempts to synchronize the time with the first server. If unsuccessful, it sequentially attempts to synchronize with the next server in the list.

1Doc: Protocolo 1.943/2025 | Anexo Administrativo_processo_licitatorio_029_2025_pdf (300/301) 2705/4746