



ecCLOUD Controller

User Manual

User Manual

ecCLOUD Controller

Cloud-Based Wired and Wireless Device Network Controller

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.

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

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 86](#)

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 80](#) and [Figure 76](#)
- Added visibility for network topology update time, see ["Locations and Maps" on page 97](#) and [Figure 98](#)
- Added Microsoft 365 Authentication support, see ["Microsoft 365 Authentication" on page 169](#) and [Figure 172](#)
- Updated System Settings for WiFi 6 Sites to include SNMP Trap Server, see ["SNMP" on page 198](#) 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 69](#)
- Added Aprecomm's Virtual Wireless Expert Add-on, see ["Using the Aprecomm Add-On" on page 82](#)
- Updated the LinqPath Tool to include Distance Steps and corresponding Expected MCS & Data Rate, see ["Using the LinqPath Tool" on page 250](#) 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 26](#)
- Updated [Figure 20](#), see ["Device Configuration Changes" on page 40](#)
- Modified Cloud Management Add-ons, see ["Add-Ons" on page 72](#)
- Modified Target Options in Firewall Settings, see WiFi-5 ["Firewall Settings" on page 137](#) and WiFi-6 ["Firewall Settings" on page 184](#)

- Added SSID Isolation Support, see ["Wireless SSID Configuration"](#) on page 159
- Added Dynamic PSK Keys Support, see ["Security Settings"](#) on page 161
- Added Mgmt Log and SysLog Level Capability, see ["System Settings"](#) on page 194
- Added SNMPv3 User Support for WiFi-6, see ["SNMPv3 User"](#) on page 203
- Added Site SD-WAN Settings, see ["Site SD-WAN Configuration"](#) on page 214
- Added 6 GHz Band Support, see ["WiFi 6 Device Configuration"](#) on page 226
- Added Device SD-WAN Settings, see ["SD-WAN Device Configuration"](#) on page 282

August 2023 Revision

This is the fifth revision of this guide. It includes the following changes:

- Added OpenRoaming, see ["Adding an SSID"](#) on page 160 and ["OpenRoaming"](#) on page 203
- Added RF Isolation, see ["Radio Settings"](#) on page 171
- Modified Broadcast Rate, see ["Radio Settings"](#) on page 171
- Added Site Grouping, see ["Site Grouping"](#) on page 61
- Added ["Always Follow Cloud Configuration"](#) on page 64

March 2023 Revision

This is the fourth revision of this guide. It includes the following changes:

- Added Airtime Fairness, see ["Global Settings"](#) on page 172
- Added 802.11v, see ["Adding an SSID"](#) on page 160
- Added BLE Tx Power, see ["iBeacon"](#) on page 202
- Added BLE Scan, see ["iBeacon"](#) on page 235
- Updated Channel Bandwidth, see ["Physical Radio Settings"](#) on page 172 and ["Physical Radio Settings"](#) on page 231
- Updated BSS Coloring, see ["Physical Radio Settings"](#) on page 172 and ["Physical Radio Settings"](#) on page 231
- Updated Minimum Allowed Signal, see ["Adding an SSID"](#) on page 118 and ["Adding an SSID"](#) on page 160

- Added Terragraph device configuration, see ["Terragraph Device Configuration" on page 253](#)
- Added Site Terragraph VLAN settings, see ["VLAN Settings" on page 212](#)

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 28](#) and ["Add Devices" on page 98](#)
- Updated Cloud menu, see ["Managing Your Devices" on page 53](#)
- Updated WiFi 5/WiFi 6 configuration, see ["WiFi Configuration" on page 101](#)
- Renamed chapter ["Site WiFi 5 Configuration" on page 116](#)
- Added Multicast/Broadcast Rate, see ["Adding an SSID" on page 118](#)
- Added OSEN, see ["Adding an SSID" on page 118](#)
- Added AuthPort External RADIUS, see ["Radio Settings" on page 126](#)
- Added Disabled W52 Channel, see ["Radio Settings" on page 126](#)
- Added IPv6 settings, see ["Internet Settings" on page 130](#)
- Added Uplink 802.1P, see ["VLAN Settings" on page 133](#)
- Added Enable RSTP, see ["Local Network Settings" on page 135](#)
- Added DNS Entries, see ["Local Network Settings" on page 135](#)
- Added ARP Inspection, see ["ARP Inspection" on page 139](#)
- Added DHCP Snooping, see ["DHCP Snooping" on page 140](#)
- Added AuthPort Remote Splash Page with External RADIUS, see ["Hotspot Settings" on page 140](#)
- Added DNS Entries and DNS Mapping, see ["Hotspot Settings" on page 140](#)
- Added Generate NAS ID, see ["RADIUS Server" on page 144](#)
- Added HTTPS Login, see ["Captive Portal" on page 145](#)
- Modified Cloud and Radio LEDs, see ["System Settings" on page 147](#)
- Added MSP Mode, see ["System Settings" on page 147](#)

- Added SNMP IPv6 Write Community and SNMP Location, see ["SNMP" on page 152](#)
- Added IGMP Snooping, see ["IGMP Snooping" on page 155](#)
- Added LLDP, see ["LLDP" on page 156](#)
- Added iBeacon, see ["iBeacon" on page 156](#)
- Added SNMPv3 User, see ["SNMPv3 User" on page 157](#)
- Added chapter ["Site WiFi 6 Configuration" on page 158](#)
- Added chapter ["Site Terragraph Configuration" on page 208](#)
- Renamed chapter ["WiFi 5 Device Configuration" on page 217](#)
- Added chapter ["WiFi 6 Device Configuration" on page 226](#)

May 2021 Revision

This is the second revision of this guide. It includes the following changes:

- Added support for EAP101 and EAP102.
- Added section ["QR Code Onboarding" on page 34](#).

December 2020 Revision

This is the first revision of this guide.

Contents

How to Use This Guide	3
Contents	8
Figures	15

Section I	Getting Started	24
	1 Introduction	25
	ecCLOUD Controller Login	26
	Creating Your First Cloud	28
	QR Code Onboarding	34
	Understanding Configuration Inheritance	36
	Understanding Device Registration	38
	Device Configuration Changes	40
	Configuration Errors and Failures	41
	Configuration Suspended Error	41
Section II	Cloud Configuration	43
	2 Cloud Management	44
	Managing Your Clouds	45
	Create a New Cloud (from an existing account)	45
	Editing Cloud Information	47
	Changing the Cloud Properties	48
	Deleting a Cloud	49
	Displaying the Cloud Dashboard	50
	Creating a Custom Cloud Dashboard	51
	Managing Your Devices	53
	Filtering the Device List	53

Configuring Inheritance Policy	54
Viewing Device Information	55
Adding Devices	55
Upgrading Device Firmware	55
Displaying System Activity	57
Manage Your Sites	58
User Management	59
Site Grouping	61
Always Follow Cloud Configuration	64
Managing Licenses and Billing	68
Report Management	69
Generate a Report	69
Add-Ons	72
Using the AuthPort Add-On	73
Service Plans	74
Accounts	76
AuthPort Certificate	78
Captive Portal	79
SSID Configuration	80
Using the Aprecomm Add-On	82
Supported Devices and Firmware Versions	82
Activating Freemium	83
Purchasing Licenses	83
Accessing the VWE Dashboard	85
Using the Smart NVR Add-On	86
Purchasing Licenses	86
Adding Smart NVR Devices	87
Manage Licenses and IP Camera Quotas	90
Add IP Cameras	91
Configure Notifications	92
3 General Site Configuration	93
Overview of Sites	94
Creating a Site	95
Site Configuration	97

Add Devices	98
Place Devices on a Google Map	100
Set Floor Maps	100
WiFi Configuration	101
Displaying the Site Dashboard	103
Creating a Custom Site Dashboard	104
Monitoring Wireless APs and Clients	107
Schedule Maintenance Tasks	111
Upgrade Firmware	111
Bulk Reboot	112
Site Notifications	112
4 Site WiFi 5 Configuration	116
Wireless SSID Configuration	117
Adding an SSID	118
Setting Wireless Schedules	125
Radio Settings	126
General Networking Settings	129
Internet Settings	130
Ethernet Settings	132
VLAN Settings	133
Local Network Settings	135
Firewall Settings	137
Port Forwarding	138
ARP Inspection	139
DHCP Snooping	140
Hotspot Settings	140
General Settings	140
Network Settings	142
DHCP Server	143
RADIUS Server	144
Captive Portal	145
Authentication Exceptions	147
System Settings	147
General Settings	147

SSH	149
Discovery Tool	149
Telnet	150
Web Server	150
Network Time	151
SNMP	152
Remote Syslog	153
Ping Watchdog	154
BLE Settings	154
Multicast DNS	155
IGMP Snooping	155
LLDP	156
iBeacon	156
SNMPv3 User	157
5 Site WiFi 6 Configuration	158
Wireless SSID Configuration	159
Adding an SSID	160
Setting Wireless Schedules	170
Radio Settings	171
General Networking Settings	175
Internet Settings	176
Ethernet Settings	179
VLAN Settings	180
Local Network Settings	182
Firewall Settings	184
Port Forwarding	185
ARP Inspection	186
DHCP Snooping	187
Hotspot Settings	187
General Settings	187
Network Settings	189
DHCP Server	190
RADIUS Server	190
Captive Portal	192

Authentication Exceptions	193
System Settings	194
General Settings	194
SSH	196
Discovery Tool	197
Network Time	197
SNMP	198
Telnet	199
Web Server	199
Remote Syslog	200
Multicast DNS	201
LLDP	201
iBeacon	202
SNMPv3 User	203
OpenRoaming	203
6 Site Terragraph Configuration	208
MetroLinq Terragraph Configuration	209
VLAN Settings	212
7 Site SD-WAN Configuration	214
VPN Group Configuration	215
VPN Group	215
8 WiFi 5 Device Configuration	217
Accessing Device-Level Configuration	218
Device Radio Settings	220
9 WiFi 6 Device Configuration	226
Accessing Device-Level Configuration	227
Device Radio Settings	228
System Settings	235
iBeacon	235
10 MetroLinq Device Configuration	237
MetroLinq Configuration	238
Wireless SSID	238

Radio Settings	239
Global Settings	239
Wireless 5 GHz	240
Wireless 2.4 GHz	242
Wireless 60 GHz	244
General Radio Settings	244
QoS Settings	248
Traffic Control	249
Using the LinqPath Tool	250
RSSI vs. Distance Graph	252
11 Terragraph Device Configuration	253
Terragraph Configuration	254
General Networking Settings	255
Radio Settings	257
System Settings	259
12 Switch Device Configuration	263
Switch Configuration	264
Port Configuration	265
Trunk Configuration	265
LACP Trunks	266
VLAN Configuration	267
Adding VLAN Port Members	267
Configuring Name Servers	269
Configuring Static IP Routes	269
Configuring Port Rate Limiting (QoS)	270
STP Configuration	271
Port Security Configuration	271
Configuring 802.1X Port Authentication	272
ACL Configuration	274
Binding Ports to an ACL	275
Configuring Switch Services	276
Configuring Port Mirroring	277
Configuring Local Logins	278
Configuring System Settings	278

Configuring Login Authentication	279
13 SD-WAN Device Configuration	282
Accessing SD-WAN Device-Level Configuration	283
WAN	284
LAN	289
Static Route	291
Dynamic Route	291
Access Control	292
Virtual Server	294
System Settings	295

Figures

Figure 1: ecCLOUD Controller Login	26
Figure 2: New User Registration	27
Figure 3: Creating a Cloud on First Login	28
Figure 4: Create Your First Cloud	28
Figure 5: Defining Your First Site	29
Figure 6: Saving the Site Configuration	30
Figure 7: Add Devices Prompt	30
Figure 8: Device Management View	30
Figure 9: Adding Devices	31
Figure 10: Adding Devices Warning Message	32
Figure 11: Adding Devices Successful Message	32
Figure 12: Firmware Upgrade Button	33
Figure 13: Filtering the Device View	33
Figure 14: Placing a Device on a Map	34
Figure 15: Scanning the AP QR Code	34
Figure 16: ecCLOUD Login Page	35
Figure 17: ecCLOUD Device Registration	36
Figure 18: Registering New Devices	38
Figure 19: Device Configuration Overrides	40
Figure 20: Reverting Device-Level Overrides	40
Figure 21: Cloud Menu	45
Figure 22: Displaying Cloud Membership	45
Figure 23: Adding Cloud Information	46
Figure 24: Showing Cloud Actions	47
Figure 25: Changing Cloud Properties	48
Figure 26: Delete Cloud Confirmation	49
Figure 27: The Cloud Dashboard	50
Figure 28: Adding a Custom Cloud Dashboard	51
Figure 29: Naming a Custom Cloud Dashboard	51

Figure 30: Adding a Widget to a Custom Cloud Dashboard	52
Figure 31: Selecting a Widget for a Custom Cloud Dashboard	52
Figure 32: Customized Widgets Added to a Custom Cloud Dashboard	52
Figure 33: Cloud Menu Devices	53
Figure 34: Manage Your Devices	53
Figure 35: Configuration Inheritance Policy Indication	54
Figure 36: Manage Your Devices Actions Menu	54
Figure 37: Accessing Device Details	55
Figure 38: Adding Devices to Your Cloud	55
Figure 39: Firmware Upgrade Indication	55
Figure 40: Device Firmware Upgrade	56
Figure 41: Showing All System Activity	57
Figure 42: Filtering by Activity Category	57
Figure 43: Site Management Page	58
Figure 44: Site Dashboard	58
Figure 45: Manage Users	59
Figure 46: Invite a New User	60
Figure 47: Accessing Site Grouping	61
Figure 48: Site Grouping Page	61
Figure 49: Creating a Site Group	62
Figure 50: Managing Site Groups	62
Figure 51: Viewing Site Group Information	63
Figure 52: Resetting Site Grouping	63
Figure 53: Enabling Always Follow Cloud Configuration During Device Registration	65
Figure 54: Enabling Always Follow Cloud Configuration on the Devices Page	65
Figure 55: Managing Follow Cloud Configuration	66
Figure 56: Using Force Configuration Push	66
Figure 57: Using Auto Follow Cloud Config	67
Figure 58: Managing Licenses and Billing	68
Figure 59: Report Information	69
Figure 60: Add Sites	69
Figure 61: Select Site Attributes	70
Figure 62: Schedule Report Export	70
Figure 63: Activity Section with Report	71

Figure 64: Report File	71
Figure 65: Add-ons Menu	72
Figure 66: AuthPort Add-On	73
Figure 67: The AuthPort Menu	74
Figure 68: Adding a Service Plan	74
Figure 69: Service Plans Overview	75
Figure 70: Creating a Single Account	76
Figure 71: Creating Accounts in a Batch	76
Figure 72: Account List	77
Figure 73: Account Details	77
Figure 74: AuthPort Certificate	78
Figure 75: AuthPort Captive Portal Themes	79
Figure 76: AuthPort Captive Portal Editor	80
Figure 77: AuthPort SSID Configuration	80
Figure 78: Aprecomm Add-On	82
Figure 79: Supported Devices and Firmware Versions	82
Figure 80: Add VWE Licenses	83
Figure 81: Apply VWE Licenses	84
Figure 82: VWE Licenses per Number of Days	84
Figure 83: Aprecomm QoE Score	85
Figure 84: Smart NVR Add-On	86
Figure 85: Adding Smart NVR Licenses	87
Figure 86: Adding a Smart NVR Device	87
Figure 87: Installing and Registering a Smart NVR	88
Figure 88: Smart NVR Dashboard	88
Figure 89: Applying Smart NVR Licenses	90
Figure 90: Available Quotas for IP Cameras per Smart NVR device	90
Figure 91: Add IP Cameras	91
Figure 92: IP Cameras Scan Details	91
Figure 93: Status and Details of IP Cameras	92
Figure 94: Enable Notifications for Unreachable IP Cameras	92
Figure 95: Default Site Dashboard	94
Figure 96: Creating a New Site	95
Figure 97: Entering Basic Site Properties	96
Figure 98: Topology Map with Timespamp	97

Figure 99: Setting the Regulatory Country	97
Figure 100: Setting Local Logins	98
Figure 101: Add Devices Prompt	98
Figure 102: Registering New Devices	99
Figure 103: Adding Devices Warning Message	99
Figure 104: Adding Devices Successful Message	100
Figure 105: Placing a Device on a Map	100
Figure 106: Adding a Floor Map	100
Figure 107: Configuring a Floor Map	101
Figure 108: Placing Devices on Floor Maps	101
Figure 109: WiFi5 Configuration	102
Figure 110: Site Dashboard	103
Figure 111: Adding a Custom Site Dashboard	104
Figure 112: Naming a Custom Site Dashboard	105
Figure 113: Adding a Widget to a Custom Site Dashboard	105
Figure 114: Selecting a Widget for a Custom Site Dashboard	105
Figure 115: Customizing a New Site Dashboard Widget	106
Figure 116: Customized Site Dashboard	106
Figure 117: Wireless Clients Page	107
Figure 118: Wireless AP Information	108
Figure 119: Wireless AP Live Status	109
Figure 120: Wireless AP Active Clients	109
Figure 121: Client Information Page	110
Figure 122: Renaming a Wireless Client	110
Figure 123: Maintenance Tasks Page	111
Figure 124: New Firmware Upgrade Task Page	111
Figure 125: Manage Bulk-Reboot Page	112
Figure 126: Site Notification Settings	113
Figure 127: Site WiFi5 Configuration	117
Figure 128: Radio Settings (New SSID)	118
Figure 129: Bridge to Internet	120
Figure 130: Route to Internet	120
Figure 131: Adding a Wireless Schedule	125
Figure 132: WiFi 5 Radio Settings	126

Figure 133: 5 GHz Radio Channels	127
Figure 134: 2.4 GHz Radio Channels	128
Figure 135: General Networking Settings	129
Figure 136: Internet Settings	130
Figure 137: Management VLAN Settings	131
Figure 138: IPv6 Settings	131
Figure 139: Ethernet Settings	132
Figure 140: VLAN Settings	134
Figure 141: Adding a VLAN	134
Figure 142: Local Network Settings	135
Figure 143: Firewall Settings	137
Figure 144: Port Forwarding	138
Figure 145: ARP Inspection	139
Figure 146: DHCP Snooping	140
Figure 147: Hotspot General Settings	141
Figure 148: Hotspot Network Settings	142
Figure 149: Hotspot DHCP Server Settings	143
Figure 150: Hotspot RADIUS Server Settings	144
Figure 151: Hotspot Captive Portal Settings	145
Figure 152: Hotspot Authentication Exceptions	147
Figure 153: General System Settings	148
Figure 154: SSH Server Settings	149
Figure 155: Discovery Tool Settings	149
Figure 156: Telnet Server Settings	150
Figure 157: Web Server Settings	151
Figure 158: NTP Settings	151
Figure 159: SNMP Settings	152
Figure 160: Remote Log Settings	153
Figure 161: Ping Watchdog Settings	154
Figure 162: BLE Settings	154
Figure 163: Multicast DNS Settings	155
Figure 164: IGMP Snooping Settings	155
Figure 165: LLDP Settings	156
Figure 166: iBeacon Settings	156
Figure 167: SNMPv3 User Settings	157

Figure 168: Site WiFi6 Configuration	159
Figure 169: Radio Settings (New SSID)	160
Figure 170: Bridge to Internet	167
Figure 171: Route to Internet	167
Figure 172: Enabling Microsoft 365 Authentication	169
Figure 173: Adding a Wireless Schedule	170
Figure 174: WiFi 6 Radio Settings	171
Figure 175: 5 GHz Radio Channels	173
Figure 176: 2.4 GHz Radio Channels	173
Figure 177: General Networking Settings	175
Figure 178: Internet Settings	176
Figure 179: Management VLAN Settings	177
Figure 180: DHCP Relay	178
Figure 181: IPv6 Settings	178
Figure 182: Ethernet Settings	179
Figure 183: VLAN Settings	180
Figure 184: Adding a VLAN	181
Figure 185: Local Network Settings	182
Figure 186: Firewall Settings	184
Figure 187: Port Forwarding	185
Figure 188: ARP Inspection	186
Figure 189: DHCP Snooping	187
Figure 190: Hotspot General Settings	188
Figure 191: Hotspot Network Settings	189
Figure 192: Hotspot DHCP Server Settings	190
Figure 193: Hotspot RADIUS Server Settings	190
Figure 194: Hotspot Captive Portal Settings	192
Figure 195: Hotspot Authentication Exceptions	193
Figure 196: General System Settings	194
Figure 197: SSH Server Settings	196
Figure 198: Discovery Tool Settings	197
Figure 199: NTP Settings	197
Figure 200: SNMP Settings	198
Figure 201: Telnet Server Settings	199

Figure 202: Web Server Settings	200
Figure 203: Remote Log Settings	200
Figure 204: Multicast DNS Settings	201
Figure 205: LLDP Settings	201
Figure 206: iBeacon Settings	202
Figure 207: SNMPv3 User Settings	203
Figure 208: OpenRoaming Profile	204
Figure 209: Site Terragraph Configuration	209
Figure 210: Add Terragraph Node	210
Figure 211: Delete Terragraph Node	210
Figure 212: Add Terragraph Link	211
Figure 213: Delete Terragraph Link	211
Figure 214: Site Terragraph VLAN Settings	212
Figure 215: Add New VPN Group	216
Figure 216: Accessing Device-Level Configuration	218
Figure 217: Device-Level Dashboard	219
Figure 218: Device Configuration	219
Figure 219: Device Global Radio Settings	220
Figure 220: Device General Radio Settings	220
Figure 221: Device Advanced Radio Settings	221
Figure 222: Device Physical Radio Settings	222
Figure 223: 5 GHz Radio Channels	223
Figure 224: 2.4 GHz Radio Channels	223
Figure 225: Accessing Device-Level Configuration	227
Figure 226: Device-Level Dashboard	227
Figure 227: Device Configuration	228
Figure 228: Device Global Radio Settings	228
Figure 229: Device Mesh Settings	229
Figure 230: Device General Radio Settings	230
Figure 231: Device Advanced Radio Settings	231
Figure 232: Device Physical Radio Settings	231
Figure 233: 5 GHz Radio Channels	232
Figure 234: 2.4 GHz Radio Channels	233
Figure 235: Device iBeacon Settings	235
Figure 236: MetroLinq Device Dashboard	238

Figure 237: MetroLinq Device Dashboard	239
Figure 238: MetroLinq Device 5 GHz Radio Settings	239
Figure 239: 5 GHz Radio Channels	241
Figure 240: MetroLinq Device 2.4 GHz Radio Settings	242
Figure 241: 2.4 GHz Radio Channels	243
Figure 242: MetroLinq Device 60 GHz Radio Settings	244
Figure 243: 60 GHz Radio Channels	246
Figure 244: MetroLinq Radio Beamwidth	247
Figure 245: MetroLinq QoS Settings	248
Figure 246: MetroLinq Traffic Control Settings	249
Figure 247: MetroLinq LinqPath Settings	250
Figure 248: MetroLinq LinqBudget Results	251
Figure 249: MetroLinq LinqPath Expected RSSI Graph	252
Figure 250: Terragraph Device Dashboard	254
Figure 251: Terragraph Device General Networking	255
Figure 252: Terragraph Device Radio Settings	257
Figure 253: Terragraph Device System Settings	259
Figure 254: Switch Device Dashboard	264
Figure 255: Switch Ports	265
Figure 256: Configuring a Trunk	266
Figure 257: Configuring Trunk Ports	266
Figure 258: Configuring LACP Trunks	267
Figure 259: Configuring VLANs	267
Figure 260: Configuring VLAN Port Members	268
Figure 261: Configuring VLAN Port Settings	269
Figure 262: Configuring Name Servers	269
Figure 263: Configuring IP Routes	270
Figure 264: Configuring Port Rate Limiting	270
Figure 265: Configuring STP	271
Figure 266: Configuring Port Security	272
Figure 267: Configuring Port Authentication	273
Figure 268: Configuring Port Authentication	273
Figure 269: Configuring ACLs	274
Figure 270: Adding a New ACL	275

Figure 271: Port ACL Bindings	275
Figure 272: Binding Ports to ACLs	275
Figure 273: Switch Services	277
Figure 274: Port Mirroring	277
Figure 275: Local Login Configuration	278
Figure 276: System Settings	279
Figure 277: Login Authentication	279
Figure 278: Adding Authentication Servers	280
Figure 279: Accessing Device-Level Configuration	283
Figure 280: Device-Level Dashboard	283
Figure 281: Device WAN Configuration	284
Figure 282: Create a New WAN VLAN Passthrough Rule	285
Figure 283: Select the Preferred WAN Interface for Internet Connectivity	285
Figure 284: SLA Configuration	286
Figure 285: Add Traffic Steering Filtering Rule	287
Figure 286: Configure Action to Filter-Matching Packets	288
Figure 287: Default LAN and DHCP Server Configuration	289
Figure 288: Static Route Configuration	291
Figure 289: Dynamic Settings Configuration	291
Figure 290: Add New Dynamic Route	292
Figure 291: Define the Default Filter Policy	292
Figure 292: Configuration of a New Access Control Rule	293
Figure 293: New Virtual Server Settings	294
Figure 294: SD-WAN Device System Settings	295

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:

- [“Introduction” on page 25](#)

1

Introduction

This chapter includes the following sections:

- “ecCLOUD Controller Login” on page 26
- “Creating Your First Cloud” on page 28
- “QR Code Onboarding” on page 34
- “Understanding Configuration Inheritance” on page 36
- “Understanding Device Registration” on page 38
- “Device Configuration Changes” on page 40
- “Configuration Errors and Failures” on page 41

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.

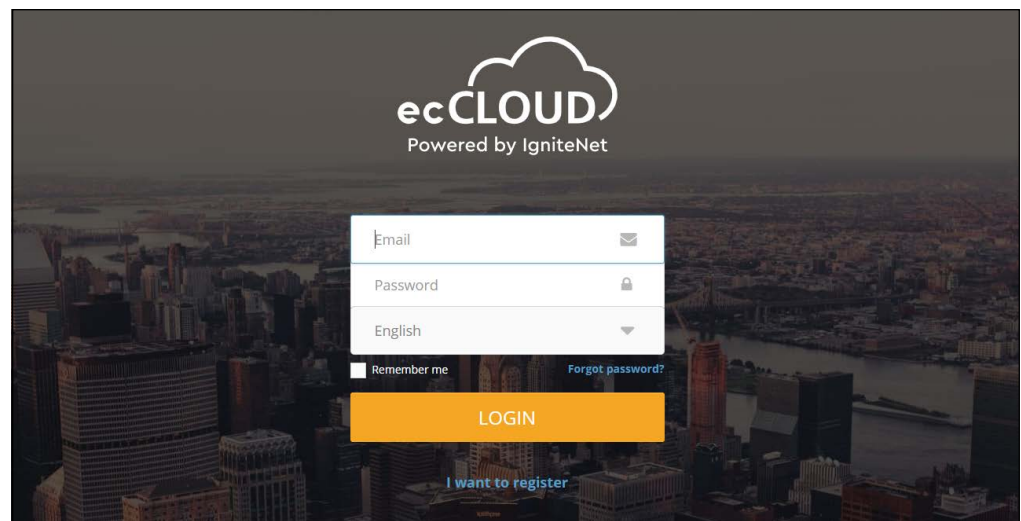
The following devices are supported by ecCLOUD:

- **Edgecore APs:** EAP101, EAP102, EAP104, EAP104 Lite, 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

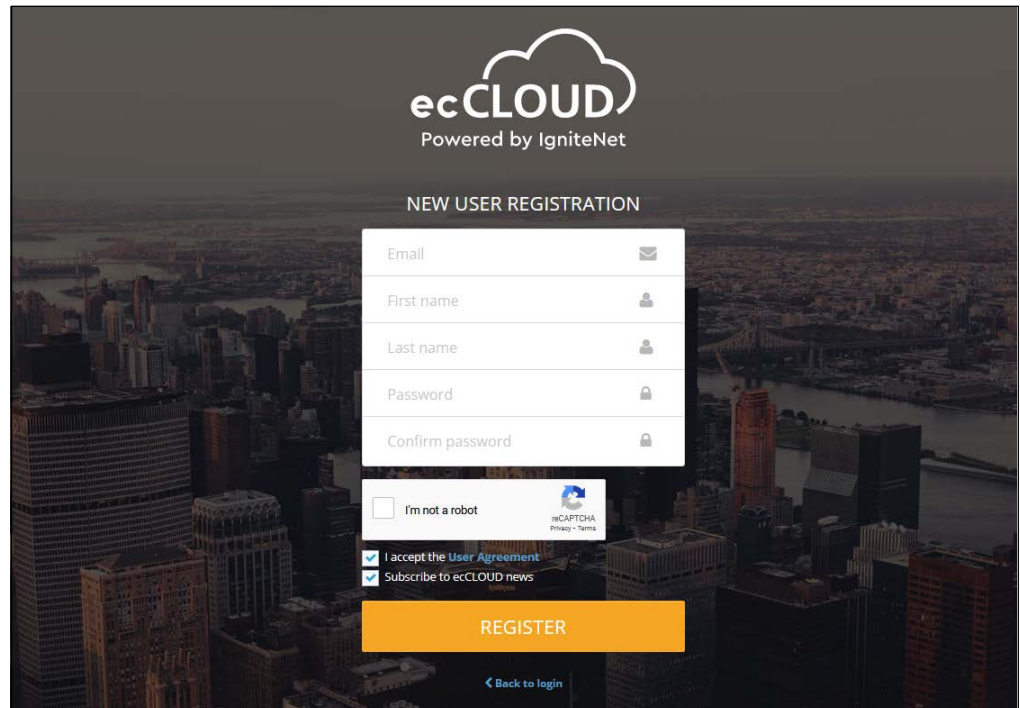
From a web browser, go to cloud.ignitenet.com to register an account and start creating your own cloud networks and sites.

Figure 1: ecCLOUD Controller Login



Click “I want to register” to create a new account.

Figure 2: New User Registration

The image shows a web registration form for ecCLOUD, powered by IgniteNet. The form is titled "NEW USER REGISTRATION" and is set against a background image of a city skyline. The form fields include: Email (with an envelope icon), First name (with a person icon), Last name (with a person icon), Password (with a lock icon), and Confirm password (with a lock icon). Below the fields is a reCAPTCHA section with the text "I'm not a robot" and a checkbox. There are also two checked checkboxes: "I accept the User Agreement" and "Subscribe to ecCLOUD news". At the bottom of the form is a large orange "REGISTER" button and a link that says "Back to login".

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.

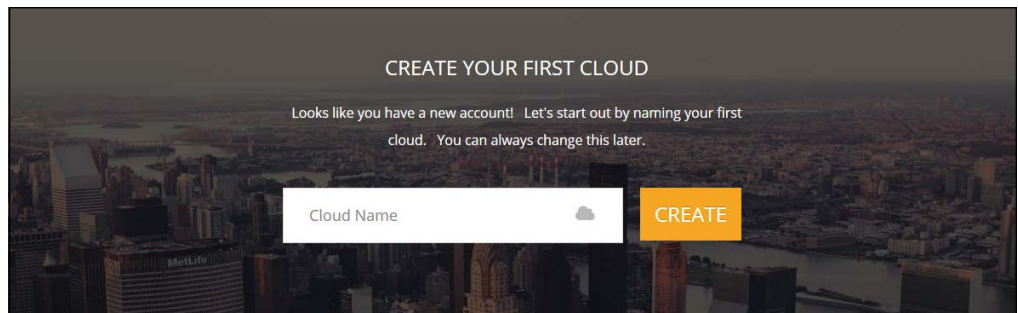
The ecCLOUD Controller sends a verification email to the account email address. When you receive the email, click on the provided link to activate your account.

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.

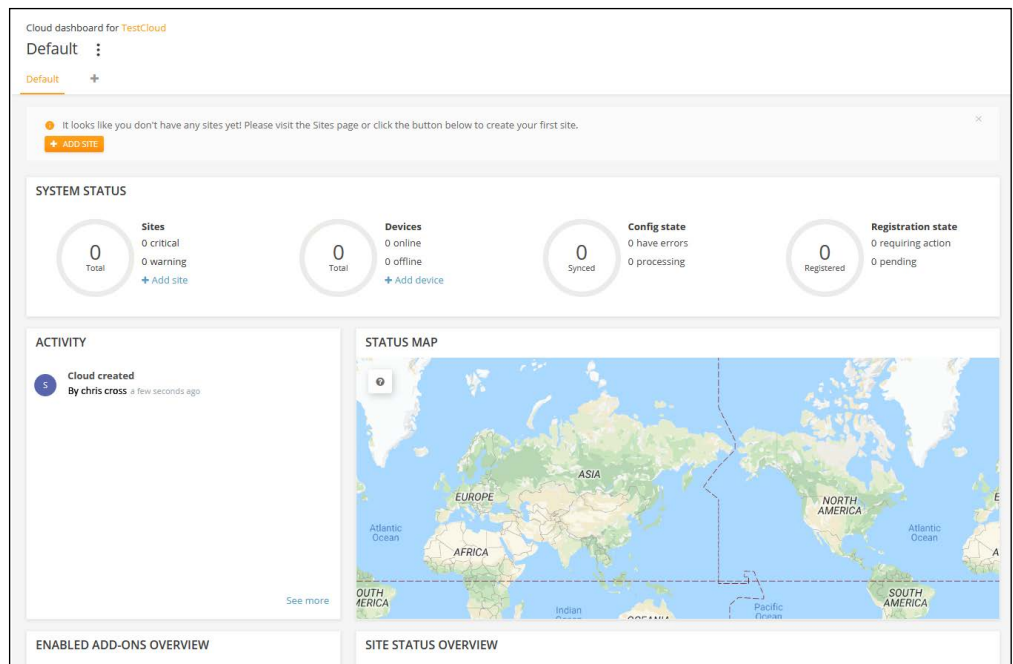
Once you are registered as a user on the ecCLOUD Controller, you are given the option to create a cloud when you first log in.

Figure 3: Creating a Cloud on First Login



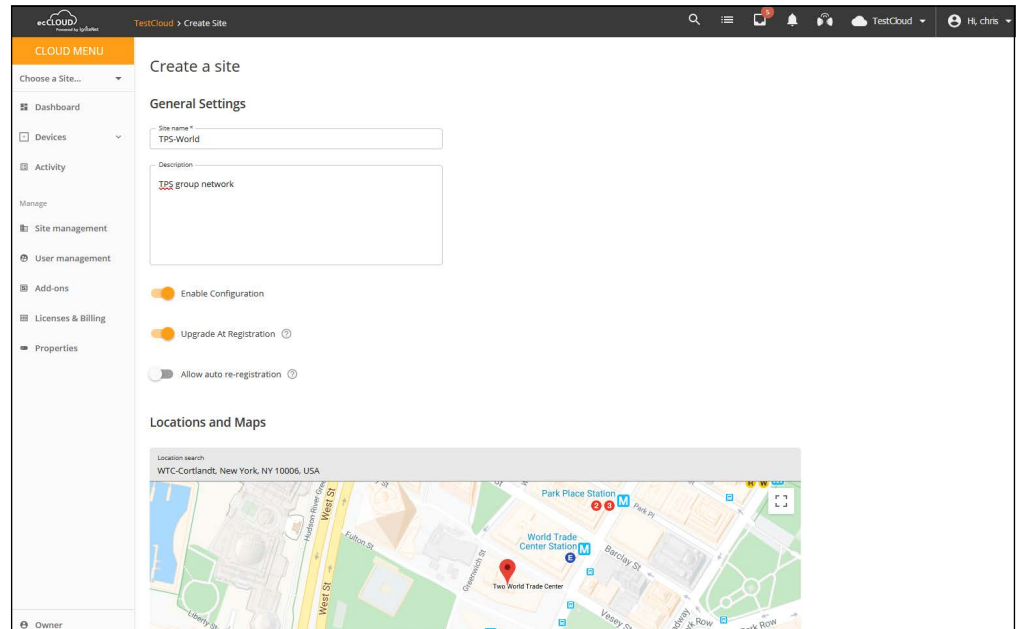
After entering a name for your first cloud, click CREATE to display the Cloud Dashboard.

Figure 4: Create Your First Cloud



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.

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.

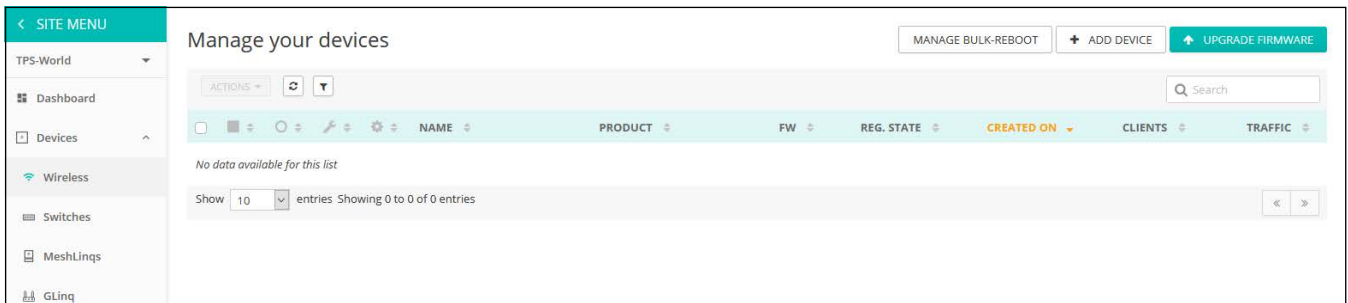
Figure 7: Add Devices Prompt



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” on page 34](#)), 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 64](#).

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 38](#).

Figure 9: Adding Devices

Register new devices

A new device can be added to a site by inputting (or scanning) the serial number and MAC address of the device. [Learn more](#)

You can find the serial number and MAC address on the product box or on the back of the product itself.

Add the following devices to the following site

Inherit site-level settings
Enable this if you want to manage the devices in this site like a single unit with a common configuration. [Learn more](#)

Enable barcode scanning mode ?

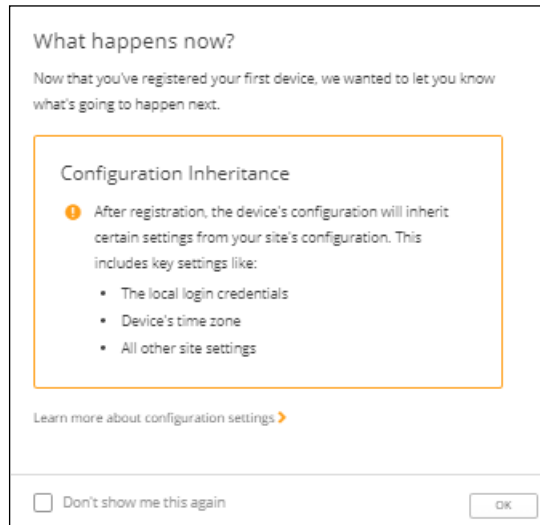
Always follow cloud configuration ?

Batch Upload File

You can register up to 48 devices.

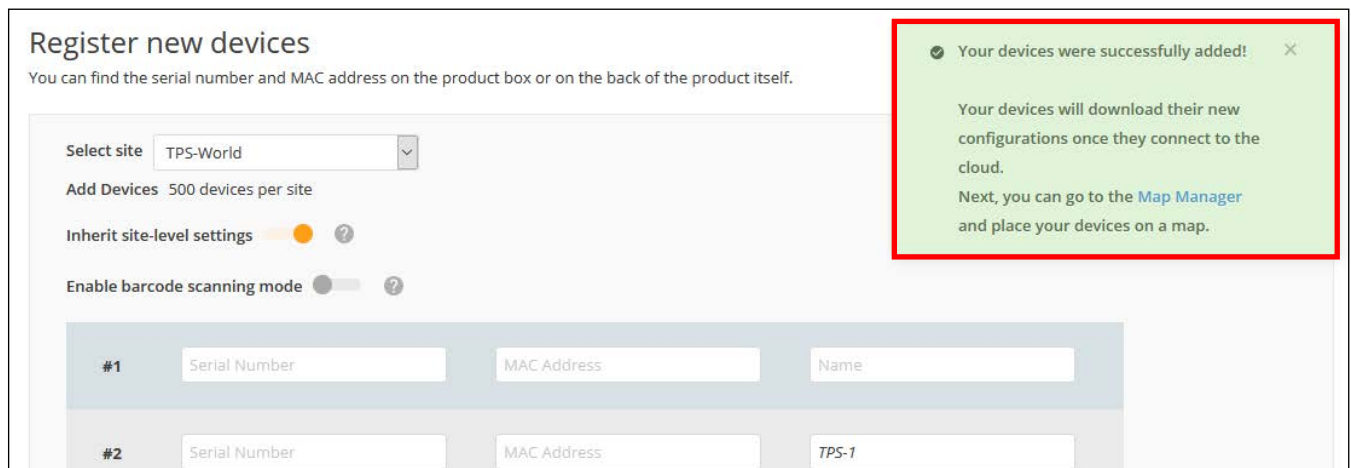
When the controller adds a device, the following pop-up window is displayed warning you that the device will inherit settings from the ecCLOUD controller site configuration. For more information on inheritance, see [“Understanding Configuration Inheritance”](#) on page 36.

Figure 10: Adding Devices Warning Message



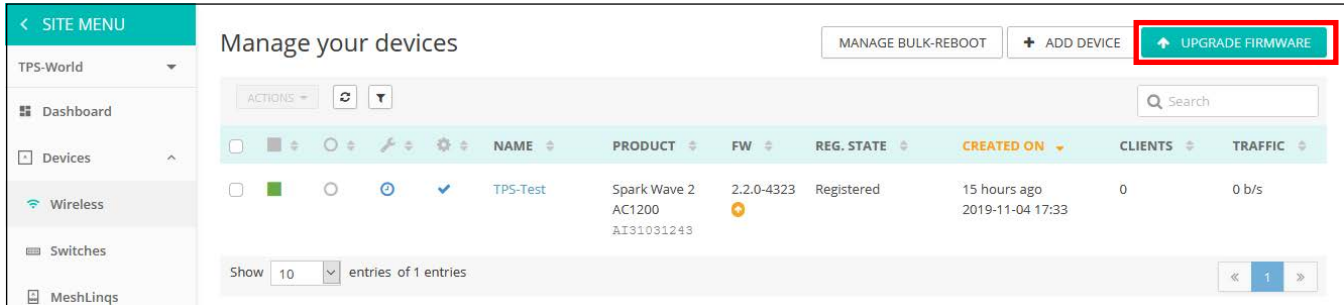
Further, at the top of the “Register new devices” page a message appears indicating that devices have been successfully added. Click on the blue link “Map Manager” in the message to place your device on a map. See [“Placing a Device on a Map”](#) on page 34.

Figure 11: Adding Devices Successful Message



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 111](#).

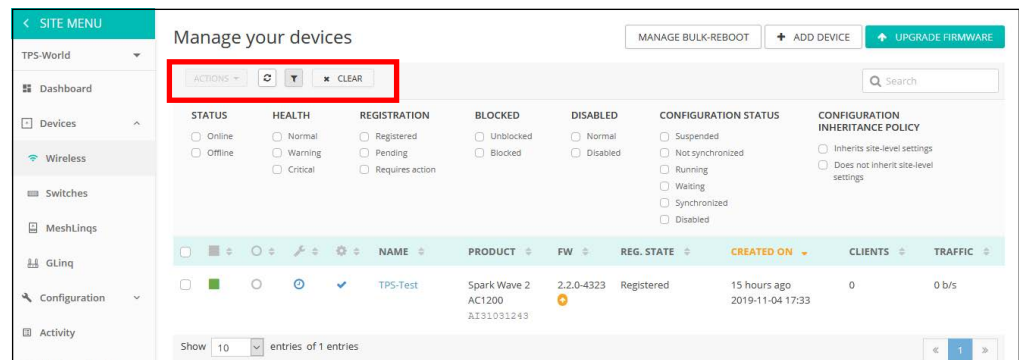
Figure 12: Firmware Upgrade Button



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.

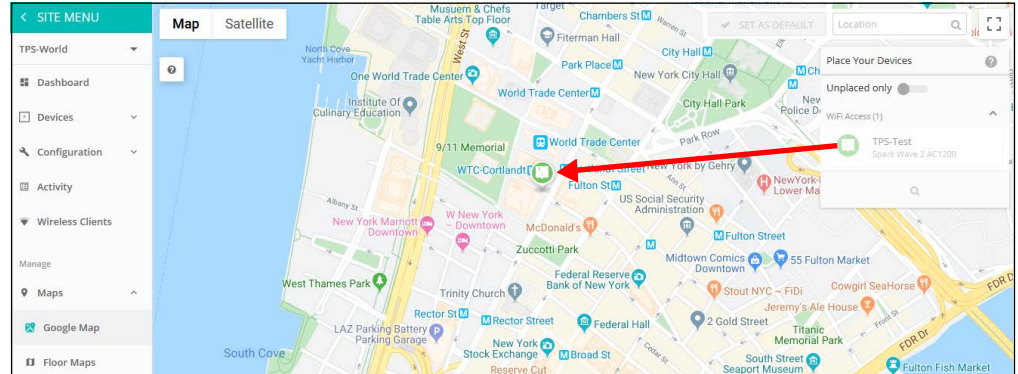
Figure 13: Filtering the Device View



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



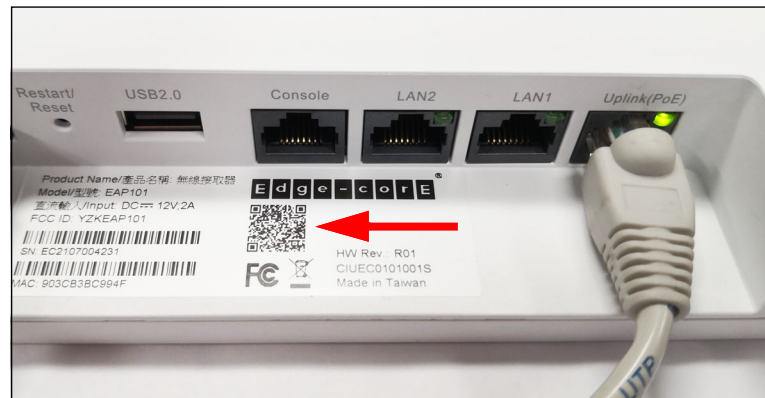
QR Code Onboarding

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



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.

i **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).

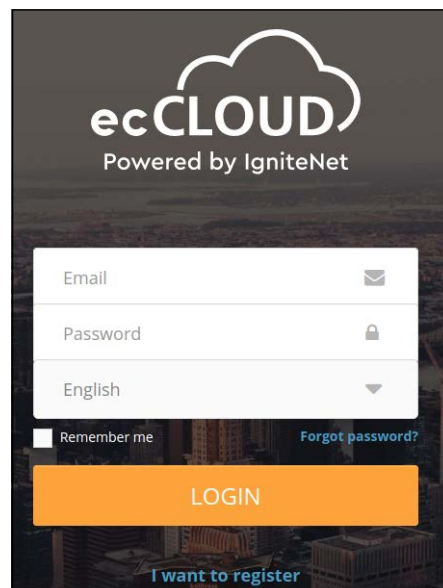
5. Select to manage the AP using the ecCLOUD controller, or to manage the AP in stand-alone mode.

- 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.

Figure 17: ecCLOUD Device Registration

The screenshot shows a 'Register Device' form. At the top, there is a 'Default Site' dropdown menu. Below it is a toggle switch for 'Inherit site-level settings' with a help icon. The form contains three text input fields: 'Serial Number *' with the value '000003', 'MAC*' with the value '00:00:00:00:00:03', and 'Device Name *' with the value 'Test Device'. At the bottom of the form is an orange 'SAVE' button.

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.

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 MetroLing 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.

i **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.

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

The screenshot shows a web form titled "Register new devices". At the top, there is a heading and a paragraph explaining that a new device can be added by inputting the serial number and MAC address, with a "Learn more" link. Below this, there is a section "Add the following devices to the following site" with a dropdown menu labeled "Choose a Site...". There are three toggle switches: "Inherit site-level settings" (checked), "Enable barcode scanning mode" (unchecked), and "Always follow cloud configuration" (unchecked). Below the toggles is a section "Batch Upload File" with a "+ UPLOAD" button. Underneath, there are three input fields: "Serial Number", "MAC Address", and "Name" (containing the number "0"). At the bottom, there is a note "You can register up to 48 devices." and two buttons: "RESET" and "SAVE".

i **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 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.

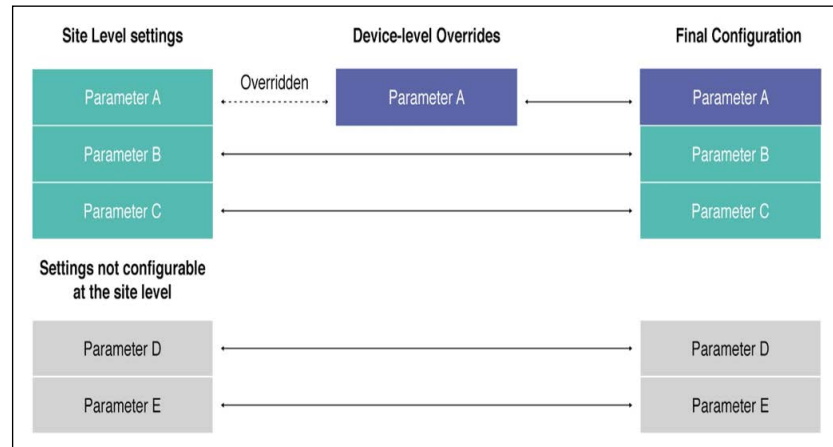
Device Configuration Changes

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:

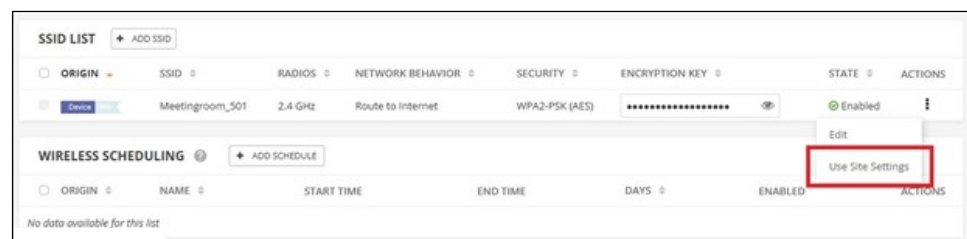
- The common Site-level configuration settings for that product type, and
- The device’s individual configuration, which includes settings not configurable at the site level, such as advanced radio settings, features unique to a single product, and more importantly, any Device-level configuration overrides.

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



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.

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.

i **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 unsuspending.

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:

- [“Cloud Management” on page 44](#)
- [“General Site Configuration” on page 93](#)
- [“Site WiFi 5 Configuration” on page 116](#)
- [“Site WiFi 6 Configuration” on page 158](#)
- [“Site Terragraph Configuration” on page 208](#)
- [“Site SD-WAN Configuration” on page 214](#)
- [“WiFi 5 Device Configuration” on page 217](#)
- [“WiFi 6 Device Configuration” on page 226](#)
- [“MetroLinq Device Configuration” on page 237](#)
- [“Terragraph Device Configuration” on page 253](#)
- [“Switch Device Configuration” on page 263](#)
- [“SD-WAN Device Configuration” on page 282](#)

2

Cloud Management

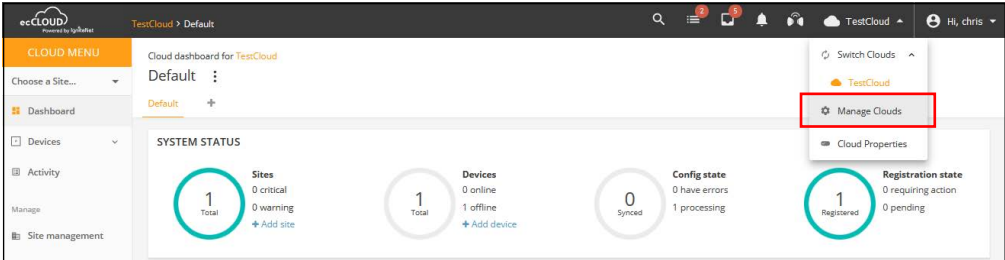
This chapter includes the following sections:

- [“Managing Your Clouds” on page 45](#)
- [“Displaying the Cloud Dashboard” on page 50](#)
- [“Creating a Custom Cloud Dashboard” on page 51](#)
- [“Managing Your Devices” on page 53](#)
- [“Manage Your Sites” on page 58](#)
- [“User Management” on page 59](#)
- [“Site Grouping” on page 61](#)
- [“Always Follow Cloud Configuration” on page 64](#)
- [“Managing Licenses and Billing” on page 68](#)
- [“Report Management” on page 69](#)
- [“Add-Ons” on page 72](#)
- [“Using the AuthPort Add-On” on page 73](#)
- [“Using the Aprecomm Add-On” on page 82](#)
- [“Using the Smart NVR Add-On” on page 86](#)

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

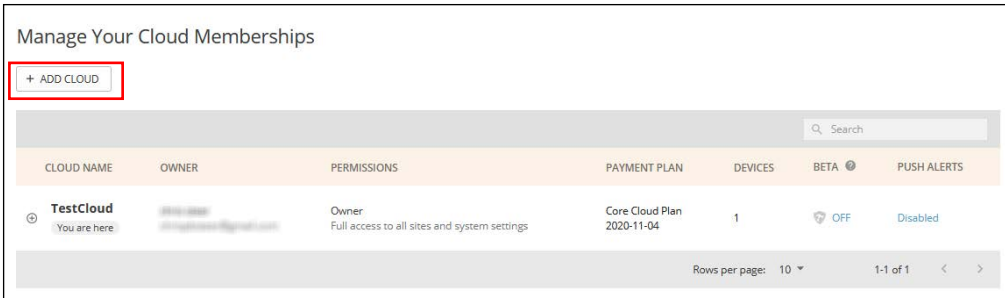


Create a New Cloud (from an existing account)

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

[← BACK TO ALL CLOUDS](#)

Cloud Properties

Cloud Information

Cloud name *

Description

Beta features [?](#)

Billing Information

Billing name

Email *

Company

Address 1

Address 2

City

State / Province / Region

ZIP

Country ▼

VAT ID

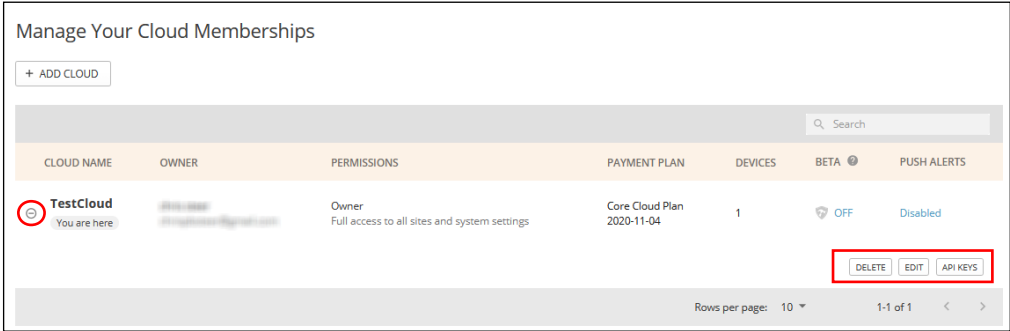
Invoice language ▼

[CANCEL](#) [✓ SAVE](#)

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.

Figure 25: Changing Cloud Properties

The screenshot displays a web form titled "Cloud Properties". At the top left, there is a button labeled "← BACK TO ALL CLOUDS". Below the title, the form is organized into two main sections: "Cloud Information" and "Billing Information".

Cloud Information

- Cloud name ***: A text input field containing "TestCloud".
- Description**: A large, empty text area.
- Beta features**: A toggle switch that is currently turned off, accompanied by a help icon.

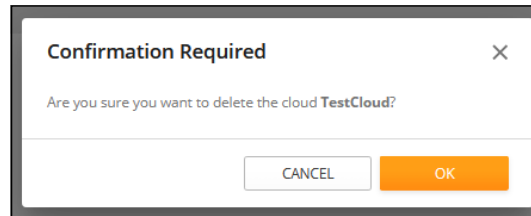
Billing Information

- Billing name**: A text input field.
- Email ***: A text input field.
- Company**: A text input field.
- Address 1**: A text input field.
- Address 2**: A text input field.
- City**: A text input field.
- State / Province / Region**: A text input field.
- ZIP**: A text input field.
- Country**: A dropdown menu.
- VAT ID**: A text input field.
- Invoice language**: A dropdown menu.

At the bottom of the form, there are two buttons: a "CANCEL" button and a "✓ SAVE" button.

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

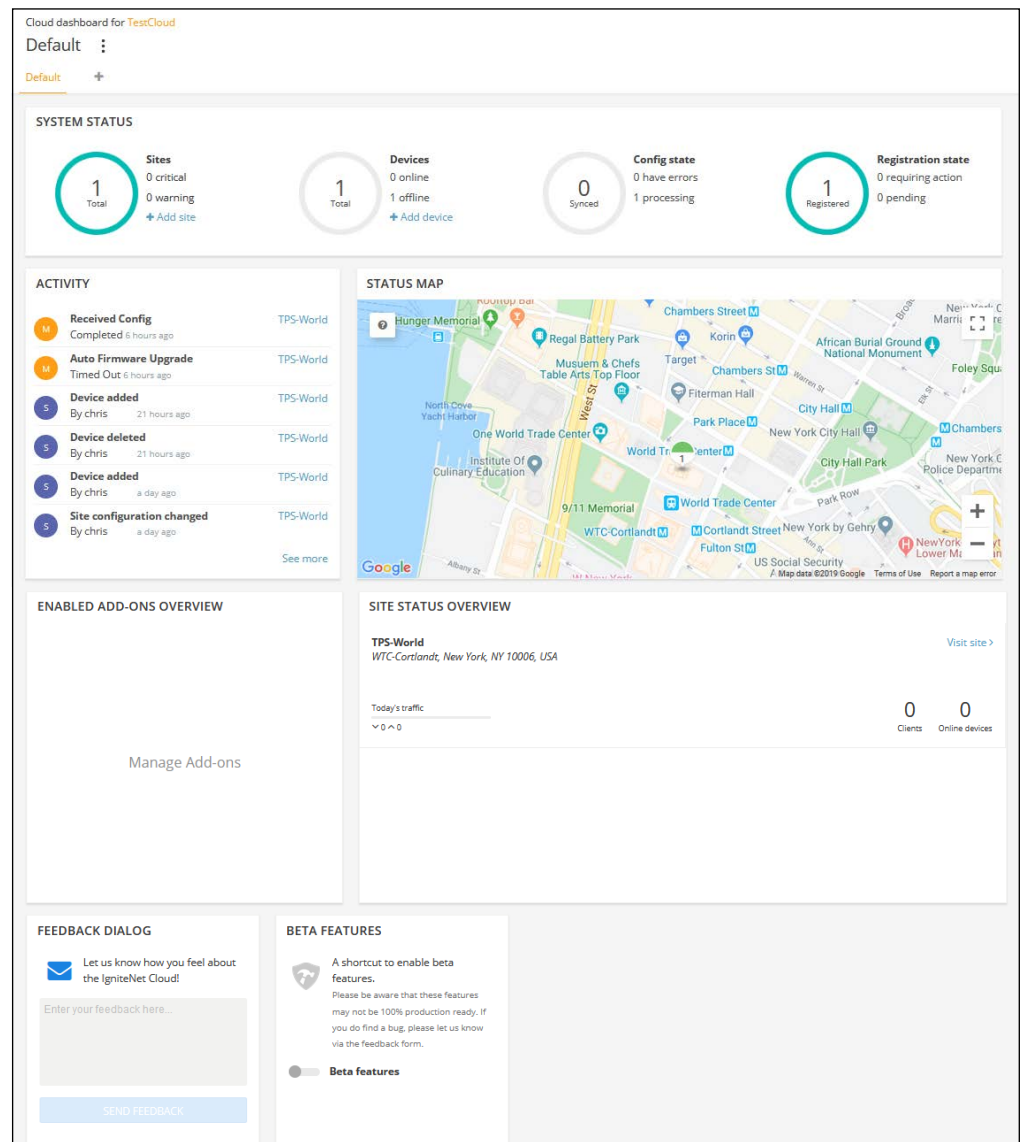


Caution: Deleting a cloud is a permanent action and will result in the deletion of all related records, such as APs, clients, sites, system activity logs, and device configurations stored for that cloud.

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.

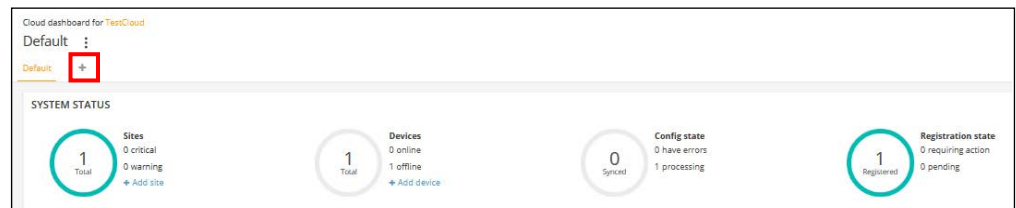
Note: Placing the mouse cursor over the four circles shows additional information.

- **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

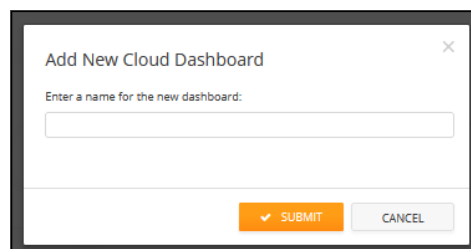
In the default cloud dashboard, click the plus sign next to the default tab at the top to create a custom dashboard suitable for your requirements.

Figure 28: Adding a Custom Cloud Dashboard



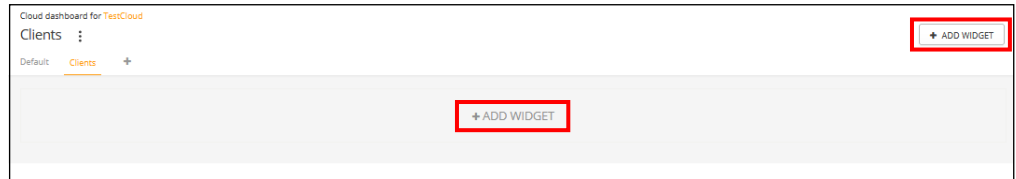
Enter a name for the new custom dashboard and click SUBMIT.

Figure 29: Naming a Custom Cloud Dashboard



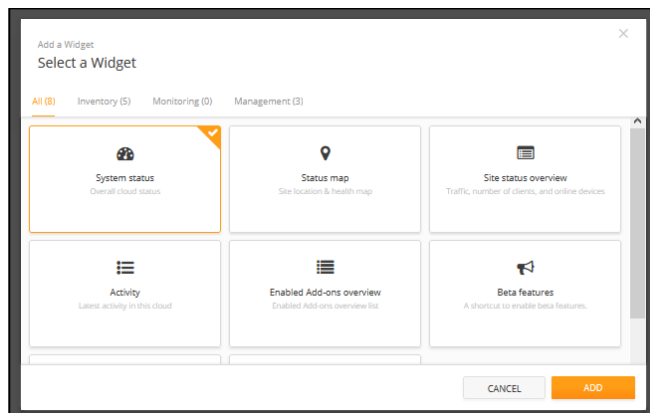
A new tab will appear next to the default dashboard tab with the custom dashboard's name. Click on one of the "+ Add Widget" buttons to add the desired item for the new dashboard.

Figure 30: Adding a Widget to a Custom Cloud Dashboard



Once a widget is selected click the "ADD" button.

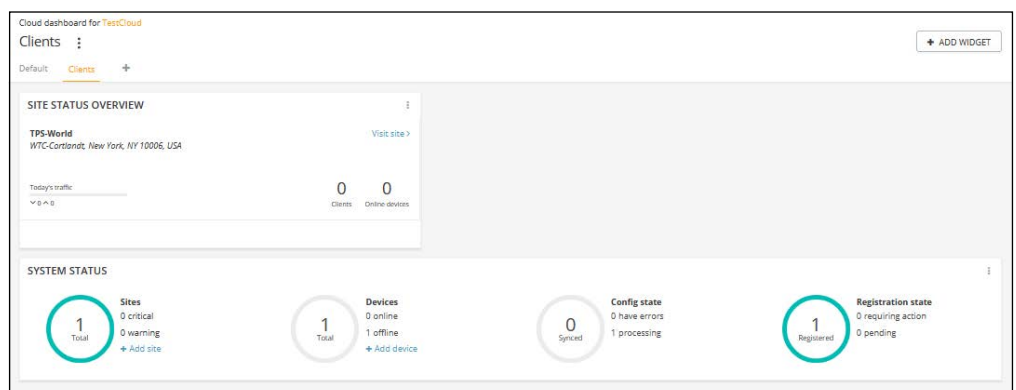
Figure 31: Selecting a Widget for a Custom Cloud Dashboard



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.

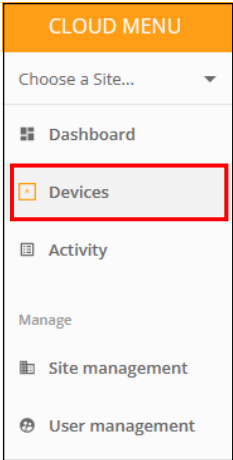
Figure 32: Customized Widgets Added to a Custom Cloud Dashboard



Managing Your Devices

Clicking the Devices section on the Cloud menu displays all the cloud devices for all sites.

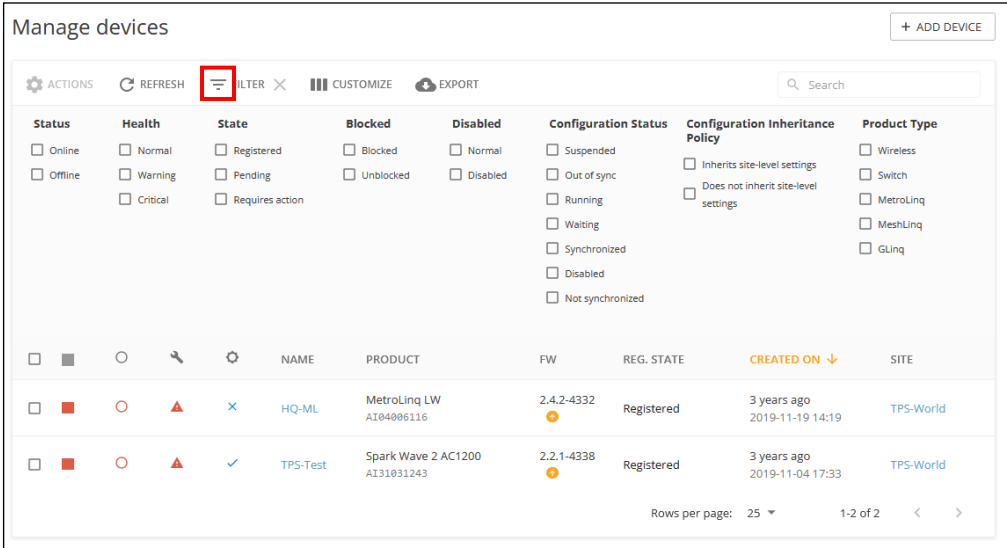
Figure 33: Cloud Menu Devices



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

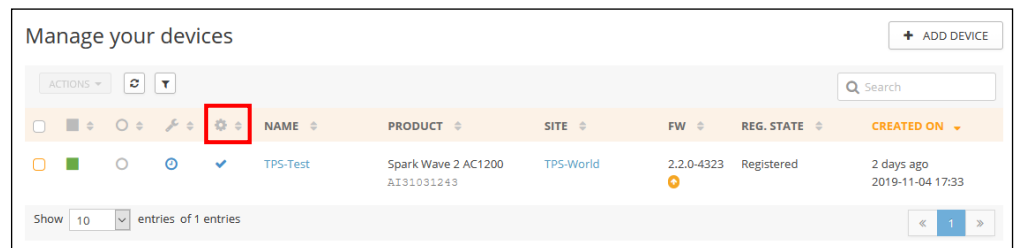


Configuring Inheritance Policy

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 36.

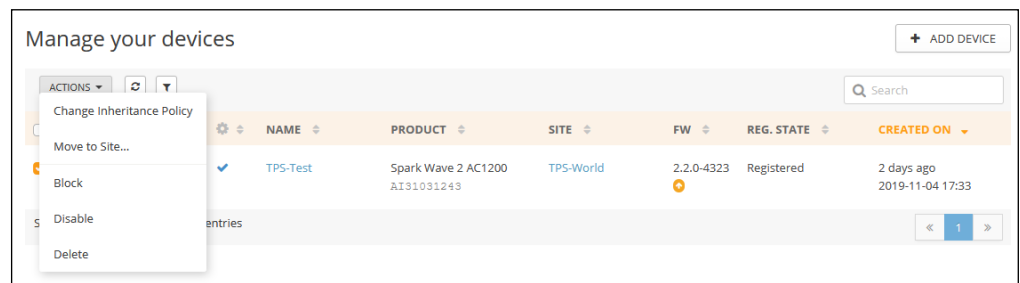
In the Cloud Devices list, the column with the gear icon indicates the devices that have the Configuration Inheritance Policy enabled. The Configuration Inheritance Policy field can be filtered and the policy for devices changed from the “Actions” list.

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

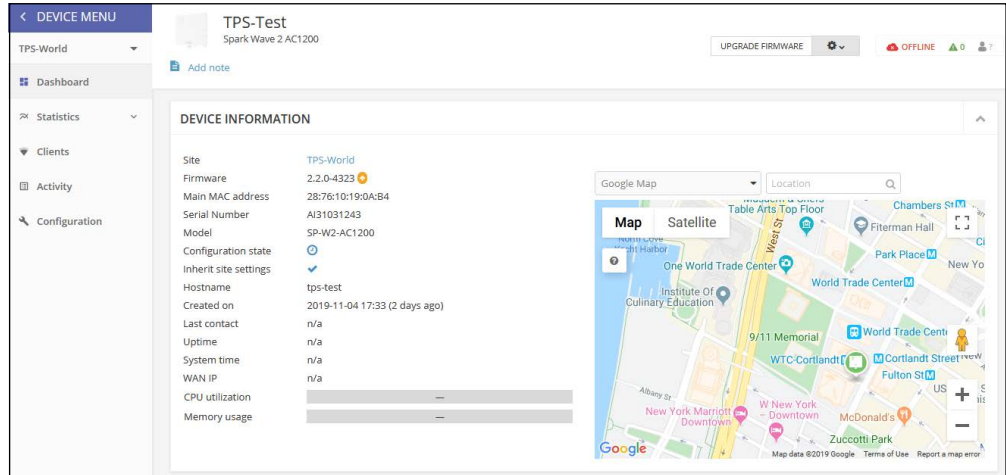


The following items are displayed on the Actions menu:

- **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.

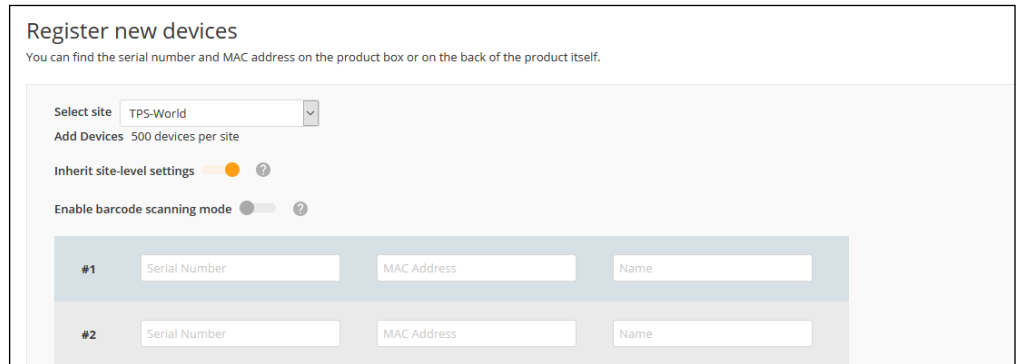
Viewing Device Information Click a device name link in the Name column to access the detailed device information.

Figure 37: Accessing Device Details



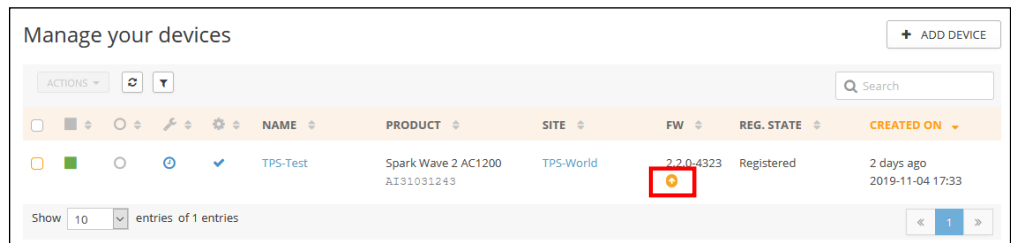
Adding Devices Click the Add Devices button to display the “Register new devices” page and add new devices to the cloud.

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

New Firmware Upgrade Task

Select Product Line:

Select Model:

Upgrade to version:

Give this task a name:

When do you want to start upgrade?
 Now
 Later 📅

How do you want the upgrade performed?
 All at the same time
 One at a time ⌚ 10 minutes

Which devices do you want to upgrade?
 All out-of-date compatible devices
 Let me choose
 Only **TPS-Test**

Reset to device defaults?

Number of selected devices: 1

Device Name	Product	Current FW	New FW	MAC
<input checked="" type="checkbox"/> TPS-Test	Spark Wave 2 AC1200	2.2.0-4323	2.2.1-4338	28:76:10:19:0A:B4

Show entries of 1 entries

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

Activity

All Alerts Maintenance System

DATE RANGE

From To

Navigate to a specific activity tab for additional filters.

DATE	TYPE	STATUS	AFFECTED	DETAILS
2 days ago 2019-11-04 10:30	Cloud created	Event	Global	User chris created this cloud
2 days ago 2019-11-04 10:50	Site created	Event	TPS-World	User chris created site TPS-World
2 days ago 2019-11-04 10:56	Site configuration changed	Event	TPS-World	User chris changed site configuration. Configuration Change Details: General: Locale Settings, Local Logins WiFi Access: Ethernet, Firewall, Hotspot, Internet, Mgmt VLAN, LAN, Advanced Radio Settings, Wireless 5 GHz, Wireless 2.4 GHz, System, ContentShield, Services, Wireless common.frequency_glinq/r24, System, Services, Internet, Coaxial, Wireless MetroLinq: Wireless 5 GHz, Wireless 2.4 GHz, Services, System

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

Activity

All Alerts Maintenance System

DATE STATUS TYPE AFFECTED DETAILS

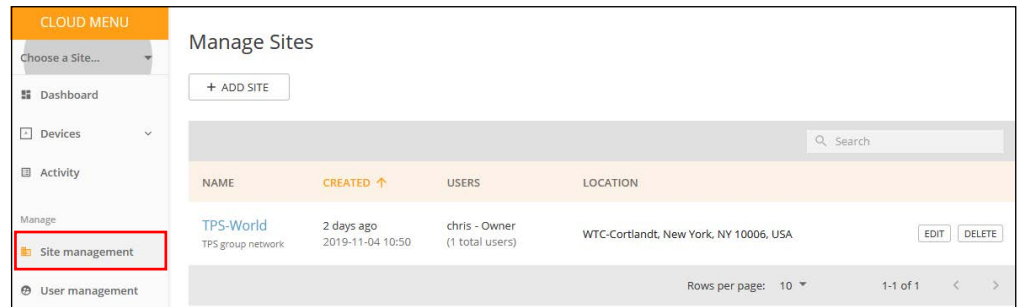
a day ago 2019-11-05 08:48	Completed 2019-11-05 08:49	Received Config (Device)	TPS-Test	Configuration was successfully updated on the cloud. Configurations received from device: Ignite, DHCP, Dropbear, Ethernet, Firewall, Hotspot, Language, mDNS, SNMP, Network, System, Telnet, UPnP, Users, Wifi Schedule, Wireless.
a day ago 2019-11-05 08:48	Timed Out 2019-11-05 08:18	Auto Firmware Upgrade	TPS-Test	Task timed out while running. Version 2.2.1-4338 Previous version 2.2.0-4323

Show 100 entries of 2 entries

Manage Your Sites

From a Cloud menu, click on the Site Management.

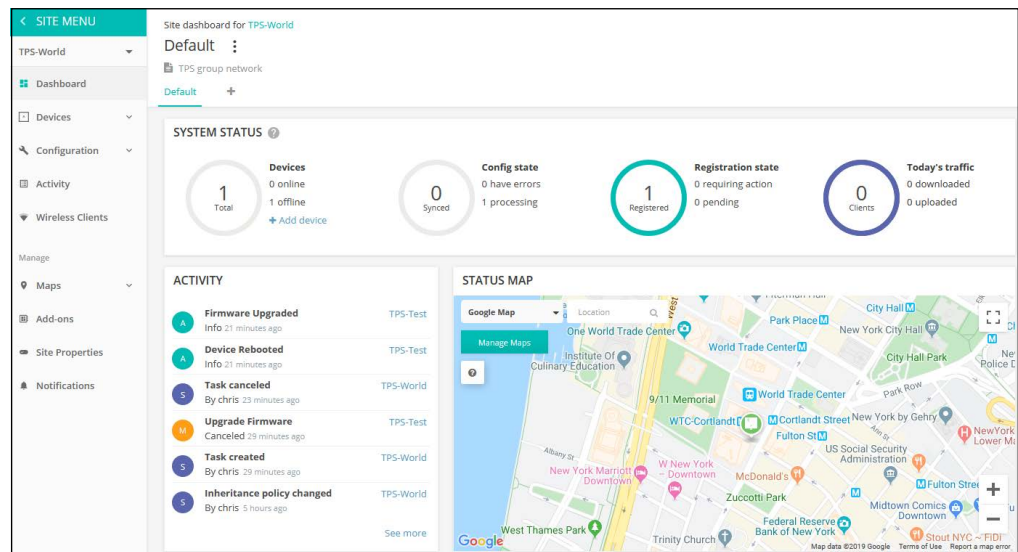
Figure 43: Site Management Page



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 93 for further detailed site management and configuration information.

User Management

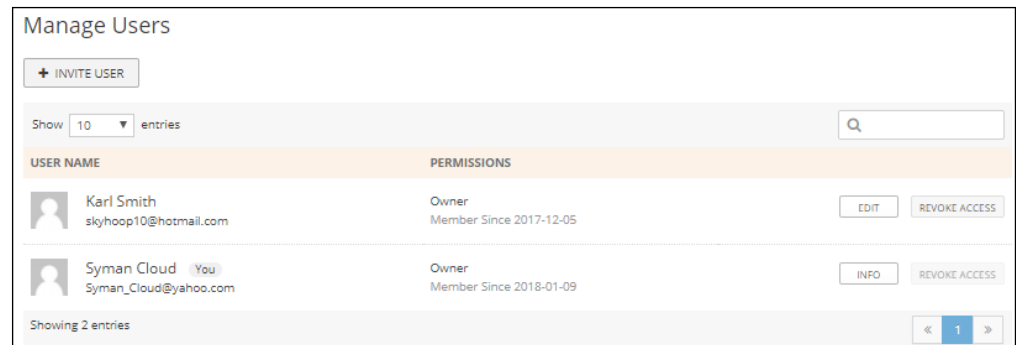
The user who originally creates a cloud is the cloud's owner. The owner can then invite any number of users to have Owner, Administrator, or Regular User access to the cloud and its sites.

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.

Figure 46: Invite a New User

← BACK TO ALL USERS

Invite a user

Email

Role

Owner
Cloud owners have complete control of all settings in their cloud.

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. You can grant additional permissions to administrators using the checkboxes below.

Additional permissions

Manage licenses and billing ⓘ

Manage VPC settings ⓘ

Regular User
Site-level users are bound to the sites that you specify below. They can further be classified as managers (with full write access), or guests (with only read-only access) within their specified sites.

Message

CANCEL INVITE

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.

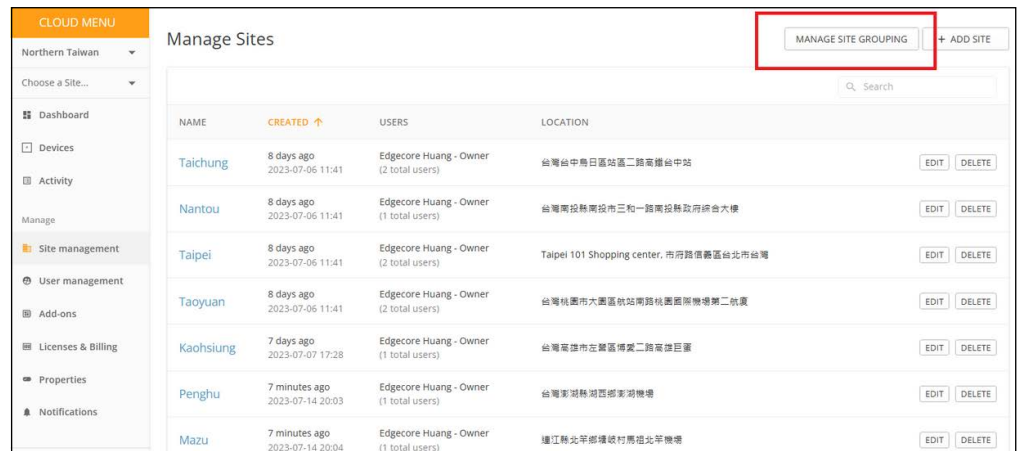
Site Grouping

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.

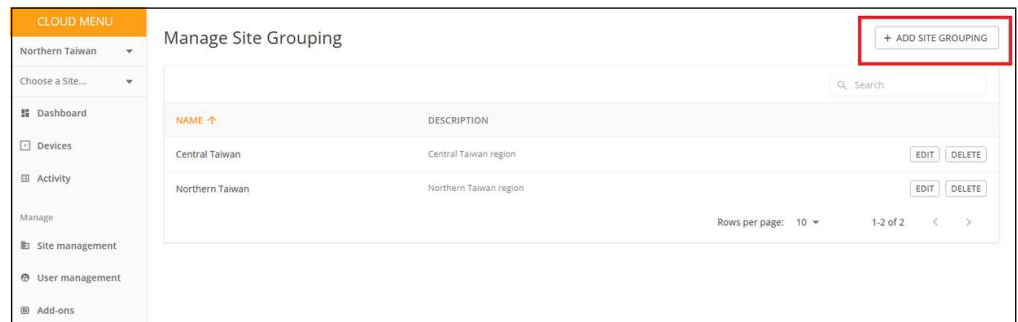
To create a site group, go to the Site Management page and click “Manage Site Grouping.”

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.

Figure 49: Creating a Site Group

Create a site grouping

A *site grouping is a logical grouping of sites.

Site Grouping Settings

Site grouping name*
Outlying islands

Description
Outlying islands

ADD SITE

Search

Site Name	Remove
Penghu	Remove

CANCEL SAVE

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

CLOUD MENU

Choose a Group... (highlighted)

Choose a Site...

Dashboard

Devices

Activity

Manage

Site management

User management

Add-ons

Licenses & Billing

Properties

Notifications

Manage Site Grouping

+ ADD SITE GROUPING

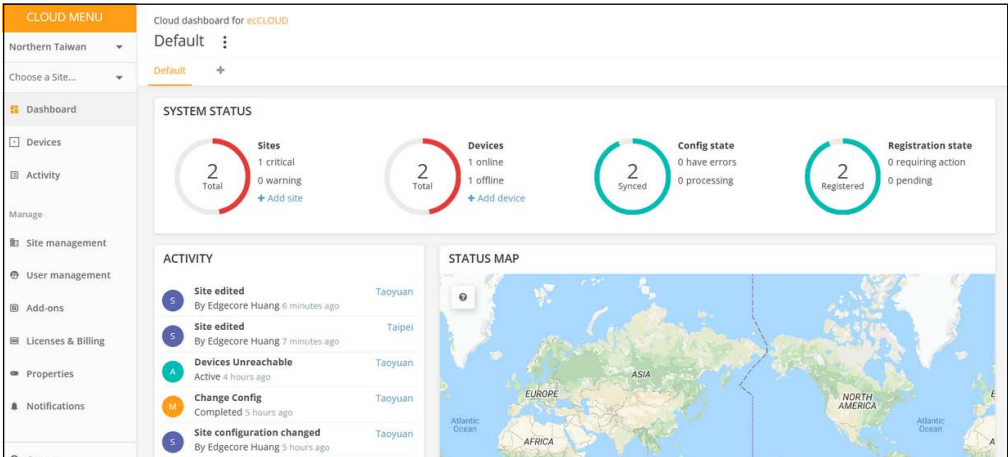
Search

NAME ↑	DESCRIPTION	
Central Taiwan	Central Taiwan region	EDIT DELETE
Northern Taiwan	Northern Taiwan region	EDIT DELETE
Outlying islands	Outlying islands	EDIT DELETE

Rows per page: 10 1-3 of 3 < >

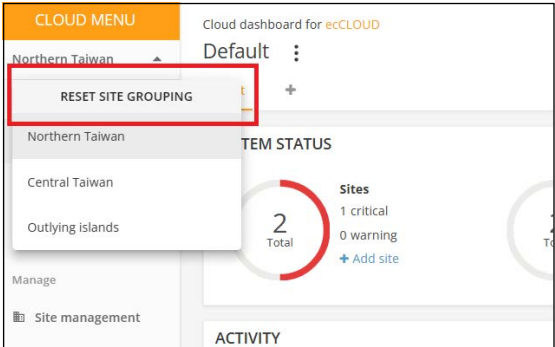
Selecting a Site Group refreshes the page and you can see aggregated information from sites in the group.

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.

i **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.

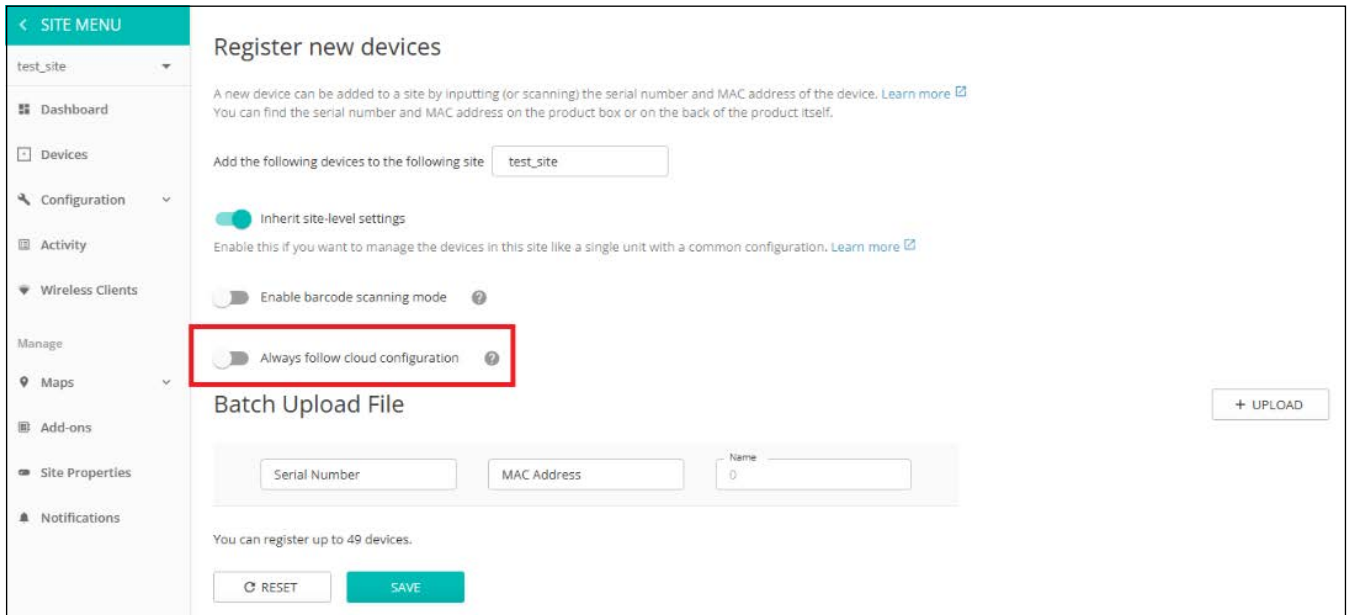
When there is a mismatched configuration between the cloud and the device, ecCLOUD notifies the cloud administrator with the message “The configuration between cloud and device is not matched” and the “Configuration status” is marked as “Configuration is not matched.”

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.”

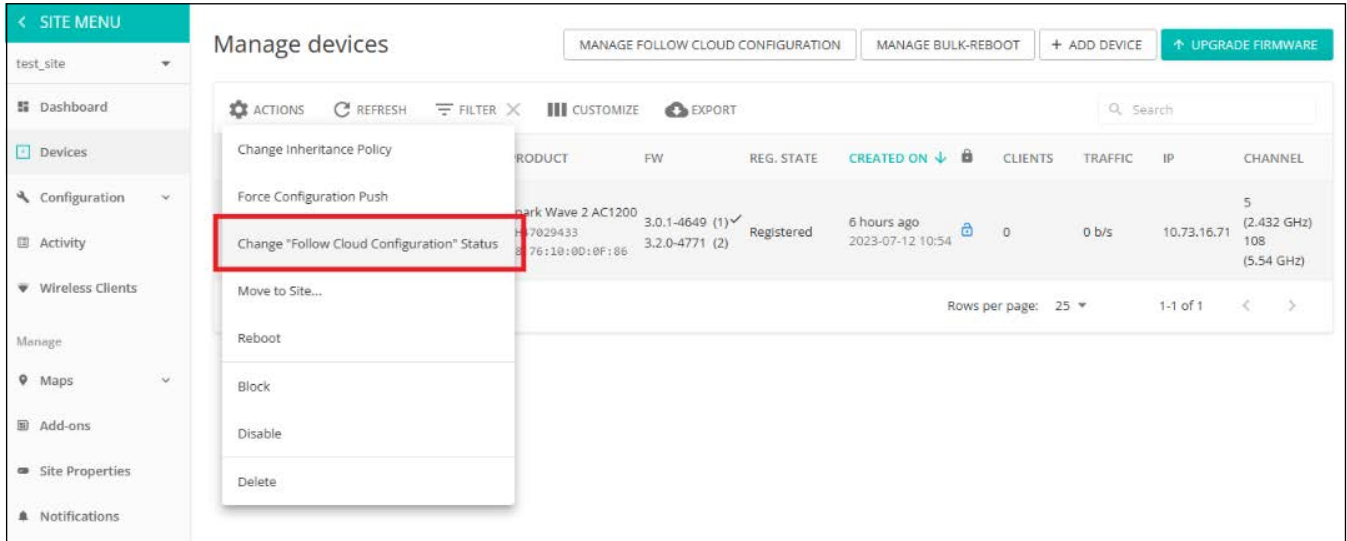
i **Note:** “Always follow cloud configuration” is automatically disabled when a device is added by QR code onboarding.

Figure 53: Enabling Always Follow Cloud Configuration During Device Registration



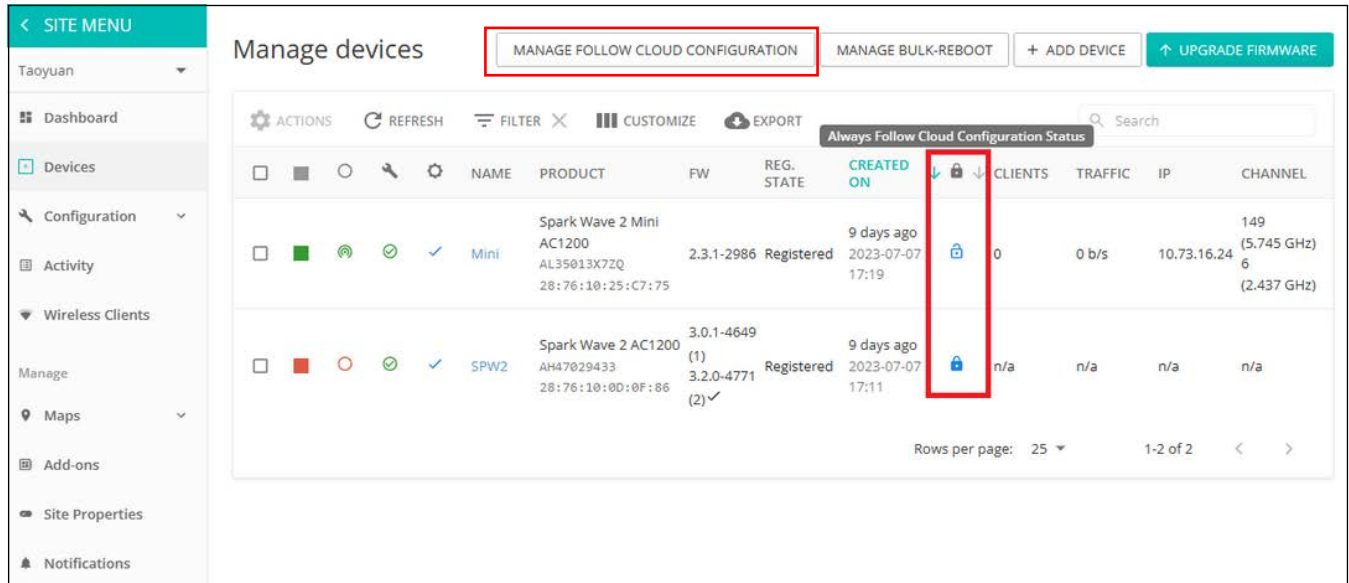
You can also enable or disable “Always follow cloud configuration” for multiple devices from the Site-level Devices page.

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.

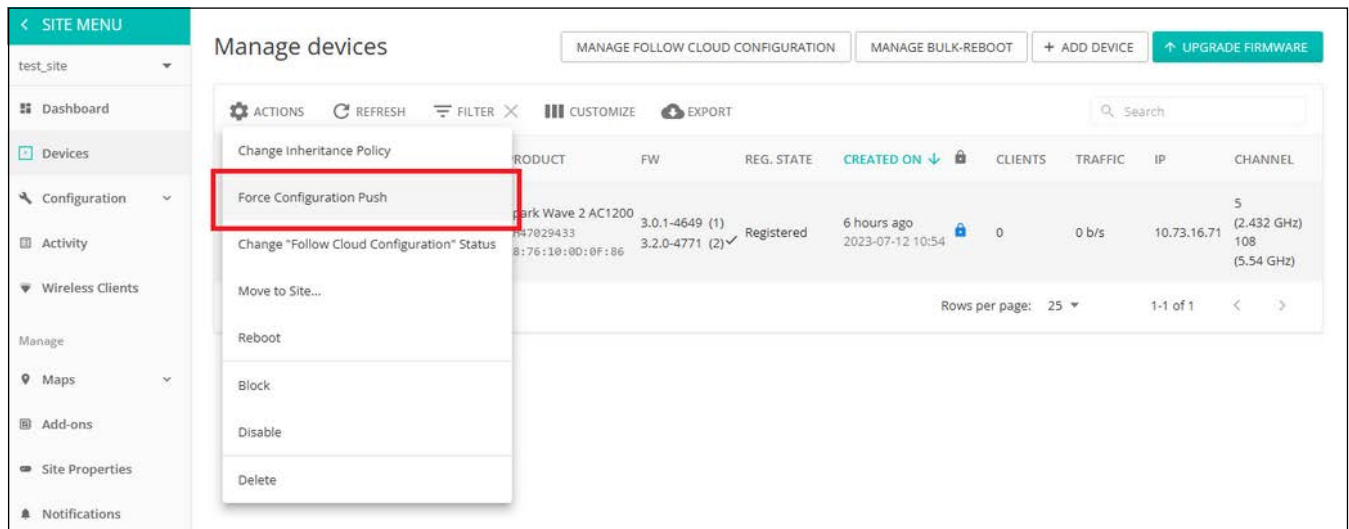
Figure 55: Managing Follow Cloud Configuration



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.”

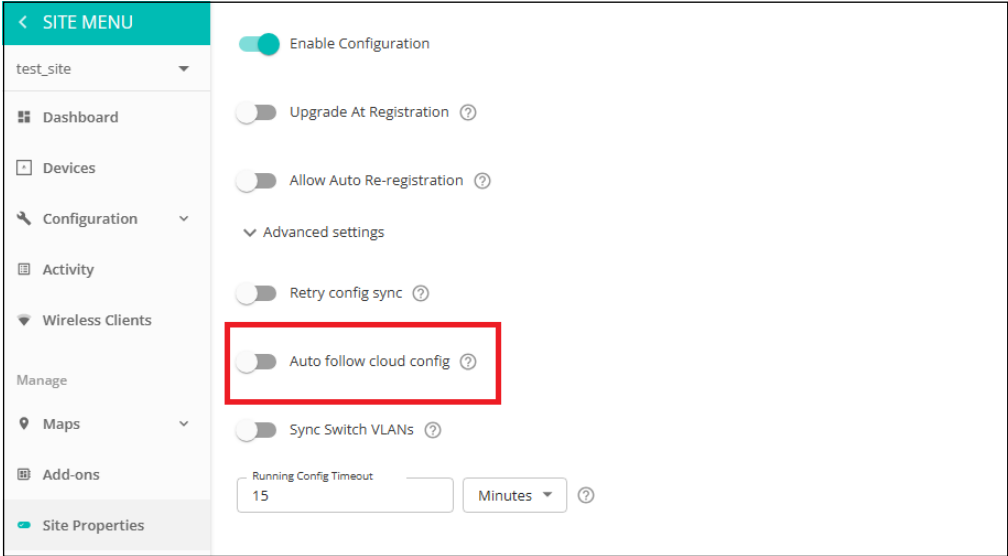
To synchronize cloud and device configurations, you can click “SYNC NOW” in the device-level configuration, or push the configuration from the Site-level Devices page.

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



i **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

The screenshot displays the 'Licenses & Billing' interface. It is divided into two main sections: 'CLOUD BALANCE' and 'CLOUD PLAN'.

CLOUD BALANCE (BILLED MONTHLY): Shows a balance of \$0.00. Below the balance, it states: 'You can apply any Cloud balance credits towards both your annual Cloud plan renewal and monthly Add-on invoices.' There is an 'APPLY VOUCHERS' button. To the right, the 'Invoice Date' is 2019-12-01 with the note 'You have nothing due at this time.' The 'Payment Method' is 'MANUAL PAY'. Below this, it says 'You haven't set your Billing Address' with an 'EDIT' button.

CLOUD PLAN (BILLED ANNUALLY): A table lists the current plan:

Your Cloud Plan	Available Licenses	Expires	Payment Method
Core Cloud Plan Change plan?	Unlimited	2020-11-04 RENEW	MANUAL PAY

Below the table, a note reads: 'Your current plan expires on 2020-11-04. Please pay the annual license fee before then to continue using your IgniteNet cloud. For a worry-free option, setup auto-pay below for automatic annual plan renewal.'

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.

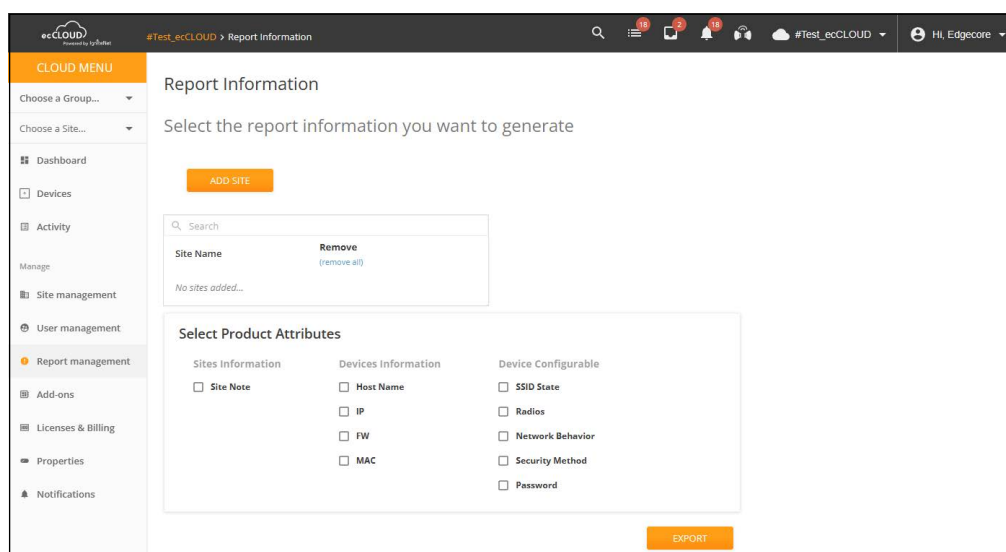
Report Management

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:

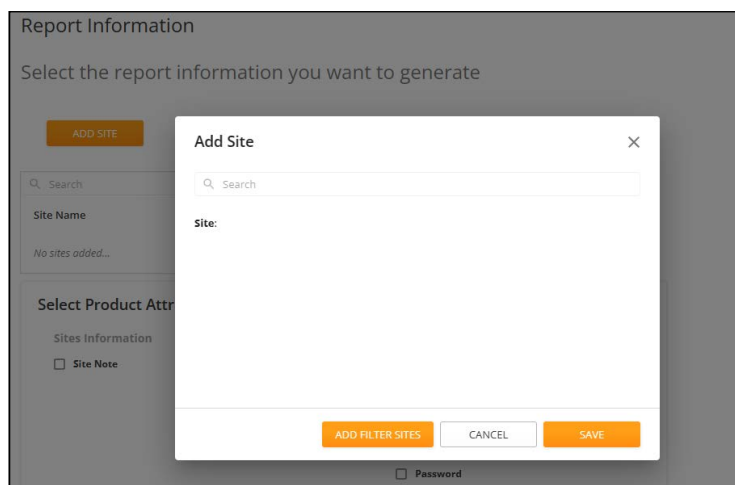
1. Navigate to 'Report Management' in the Cloud menu.

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

Sites Information	Devices Information	Device Configurable
<input checked="" type="checkbox"/> Site Note	<input checked="" type="checkbox"/> Host Name	<input checked="" type="checkbox"/> SSID State
	<input checked="" type="checkbox"/> IP	<input checked="" type="checkbox"/> Radios
	<input checked="" type="checkbox"/> FW	<input checked="" type="checkbox"/> Network Behavior
	<input checked="" type="checkbox"/> MAC	<input checked="" type="checkbox"/> Security Method
		<input checked="" type="checkbox"/> Password

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

Report Information

Select the report information you want to generate

ADD SITE

Search

Site Name	Remove
wif5	Remove
wif6	Remove

Select Product Attributes

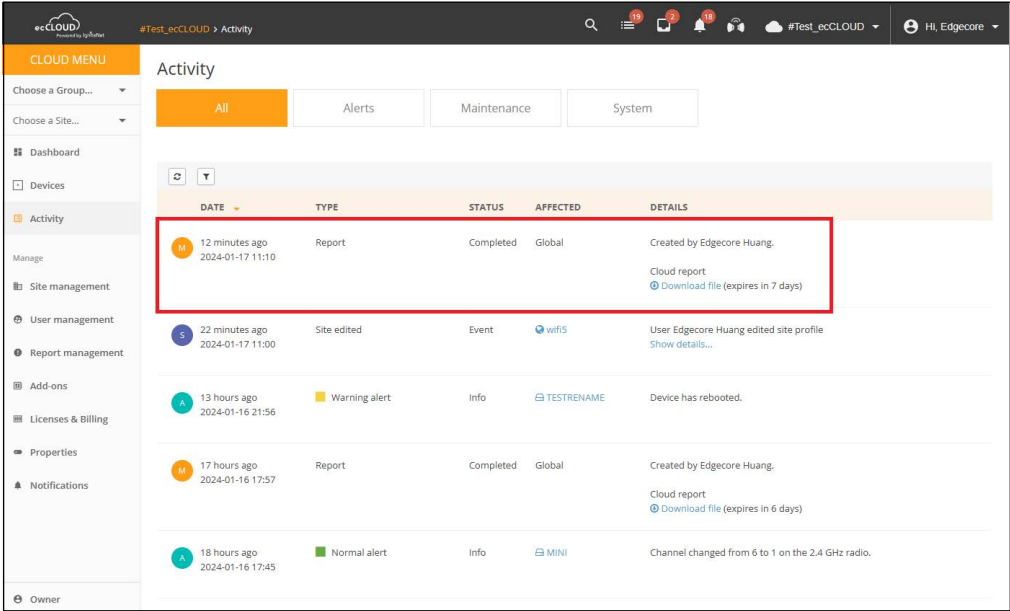
Sites Information	Devices Information	Device Configurable
<input checked="" type="checkbox"/> Site Note	<input checked="" type="checkbox"/> Host Name	<input checked="" type="checkbox"/> SSID State
	<input checked="" type="checkbox"/> IP	<input checked="" type="checkbox"/> Radios
	<input checked="" type="checkbox"/> FW	<input checked="" type="checkbox"/> Network Behavior
	<input checked="" type="checkbox"/> MAC	<input checked="" type="checkbox"/> Security Method
		<input checked="" type="checkbox"/> Password

EXPORT

Report was scheduled. You can monitor task status on the Maintenance tab of the Activity page. [GO TO MAINTENANCE:](#)

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



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

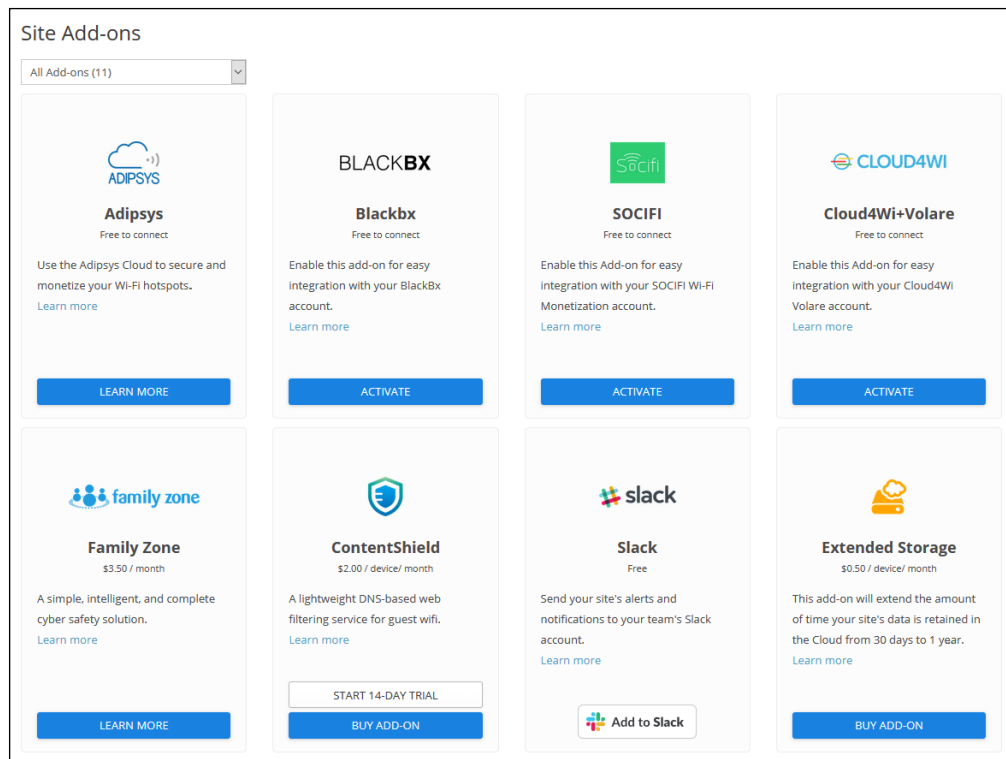
Using Add-ons

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



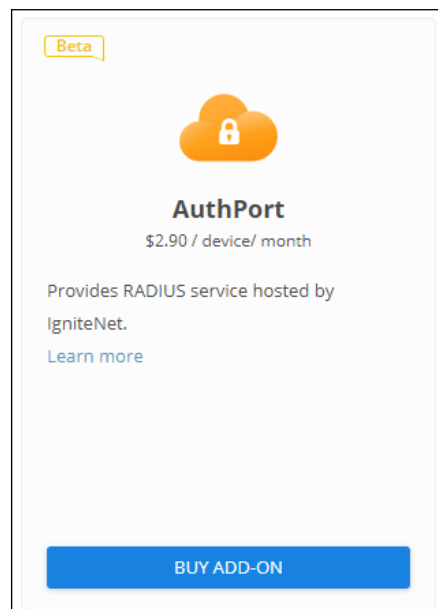
Using the AuthPort Add-On

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.

i **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.

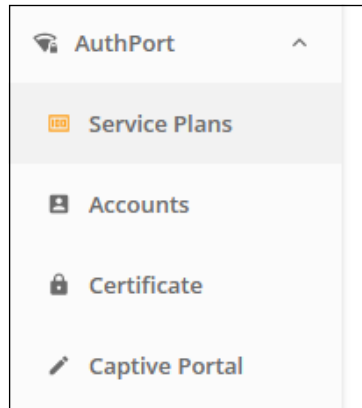
You can purchase this add-on by navigating to the “Add-ons” menu item from either the Cloud or Site-level menus, and pressing the “BUY ADD-ON” button on the AuthPort add-on.

Figure 66: AuthPort Add-On



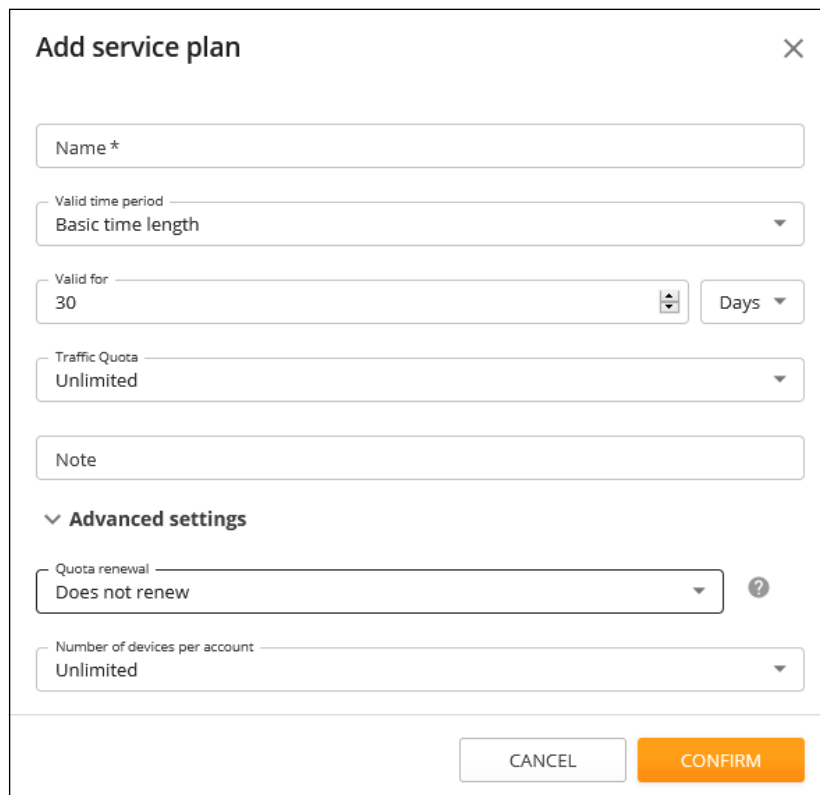
After enabling the AuthPort add-on, the AuthPort configuration menu will appear on the Cloud menu. You can configure a Service Plan, Accounts, Certificate, and Captive Portals respectively.

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

A screenshot of the 'Add service plan' form. The form has a title 'Add service plan' and a close button (X) in the top right corner. It contains several input fields and dropdown menus: 'Name *' (text input), 'Valid time period' (dropdown menu with 'Basic time length' selected), 'Valid for' (text input with '30' and a spinner icon, followed by a 'Days' dropdown), 'Traffic Quota' (dropdown menu with 'Unlimited' selected), 'Note' (text input), 'Advanced settings' (section header with a downward arrow), 'Quota renewal' (dropdown menu with 'Does not renew' selected and a help icon), and 'Number of devices per account' (dropdown menu with 'Unlimited' selected). At the bottom right, there are two buttons: 'CANCEL' and 'CONFIRM'.

The following list shows the configurable items for a service plan.

- **Name** — The name of the service plan.

- **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

NAME	PLAN DESCRIPTION	NOTE
10GB	Activation: Upon account creation Expiration: a month after account activation Number of devices: 10 Traffic quota: 10GB Traffic quota renewal: Weekly on Monday at 17:20	[EDIT] [DELETE]
3days	Activation: Before 2020-07-10 Expiration: 3 days after account activation Number of devices: 1 Traffic quota: Unlimited Traffic quota renewal: Does not renew	[EDIT] [DELETE]
1GB-6days	Activation: Before 2020-07-10 Expiration: 6 days after account activation Traffic quota: 1GB Traffic quota renewal: Daily at 13:30	[EDIT] [DELETE]
does not expires	Activation: Upon account creation Expiration: Does not expire Traffic quota: Unlimited Traffic quota renewal: Does not renew	[EDIT] [DELETE]

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

The 'Create an account' dialog box contains the following fields and options:

- Username *
- Password *
- Plan * (5 day plan)
- Activation: Upon account creation
- Quota renewal: Does not renew
- Number of devices: Unlimited
- Quota: Unlimited
- Expiration: 5 days after account activation
- Multiplier: 1
- Total** Expiration: 5 days after account activation
- Notes
- CANCEL and CONFIRM buttons

Figure 71: Creating Accounts in a Batch

The 'Generate accounts' dialog box contains the following fields and options:

- Plan * (5 day plan)
- Activation: Upon account creation
- Quota renewal: Does not renew
- Number of devices: Unlimited
- Quota: Unlimited
- Expiration: 5 days after account activation
- Multiplier: 1
- Total** Expiration: 5 days after account activation
- Number of accounts: 1
- Notes
- Export generated accounts to a file
- CANCEL and CONFIRM buttons

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

ACTIONS	USERNAME ↑	PLAN	TRAFFIC QUOTA	EXPIRATION TIME	NOTE
<input type="checkbox"/> <input type="checkbox"/> <input type="radio"/>	test1	2GB	26MB used total 2GB	Expires in 2 months 2020-09-13 10:48	<input type="button" value="EDIT"/> <input type="button" value="DELETE"/>
<input type="checkbox"/> <input type="checkbox"/> <input type="radio"/>	test2	3TB	516MB used total 3TB	Expires in 22 days 2020-08-07 02:08	<input type="button" value="EDIT"/> <input type="button" value="DELETE"/>
<input type="checkbox"/> <input type="checkbox"/> <input type="radio"/>	test3	Unlimit	Unlimited data 267MB used	Does not expire	<input type="button" value="EDIT"/> <input type="button" value="DELETE"/>
<input type="checkbox"/> <input type="checkbox"/> <input type="radio"/>	test4	30Day	Unlimited data 0B used	Expires in 22 days 2020-08-06 21:17	<input type="button" value="EDIT"/> <input type="button" value="DELETE"/>
<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="radio"/>	test5	300MB	741KB used total 300MB	Expires in 3 months 2020-10-13 13:45	<input type="button" value="EDIT"/> <input type="button" value="DELETE"/>
<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="radio"/>	test6	1Day	Unlimited data 50MB used	Expired 6 days ago 2020-07-09 13:40	<input type="button" value="EDIT"/> <input type="button" value="DELETE"/>

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.

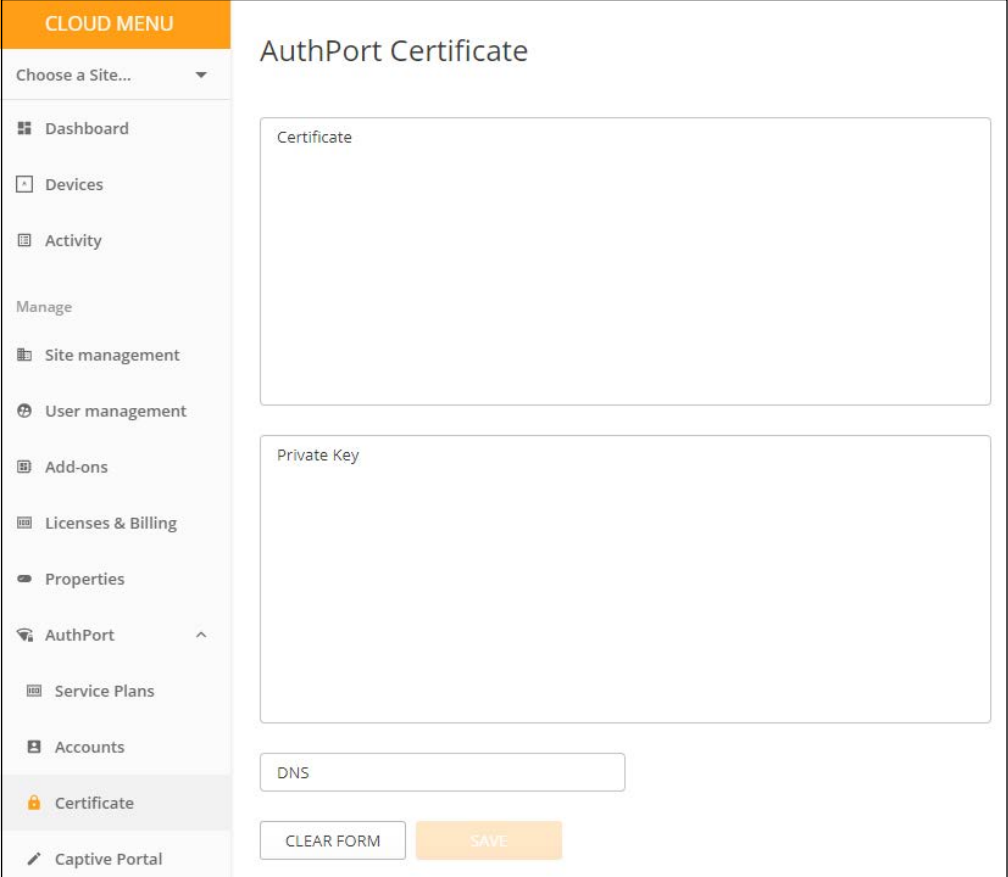
Figure 73: Account Details

<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="radio"/>	AAAA	333333	Unlimited data 117MB used	Expires in 10 days 2020-07-25 16:13	1234	<input type="button" value="EDIT"/> <input type="button" value="DELETE"/>			
MAC	SSID	Access Point	Site	IP Address	OS	Freq Band	RSI	Session Down/Up	Session Duration
48:fd:a3:f4:4d:ff	.authport1	ECW5211-L-31	authport site	192.168.2.113	Generic Android	5 (2432 MHz)	-53	42 kB / 26 kB	32 minutes

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.

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



The screenshot shows a web interface for configuring an AuthPort Certificate. On the left is a 'CLOUD MENU' sidebar with options: Choose a Site..., Dashboard, Devices, Activity, Manage, Site management, User management, Add-ons, Licenses & Billing, Properties, AuthPort, Service Plans, Accounts, Certificate (highlighted), and Captive Portal. The main content area is titled 'AuthPort Certificate' and contains two large text input fields: 'Certificate' and 'Private Key'. Below these fields is a 'DNS' input field, and at the bottom are 'CLEAR FORM' and 'SAVE' buttons.

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.

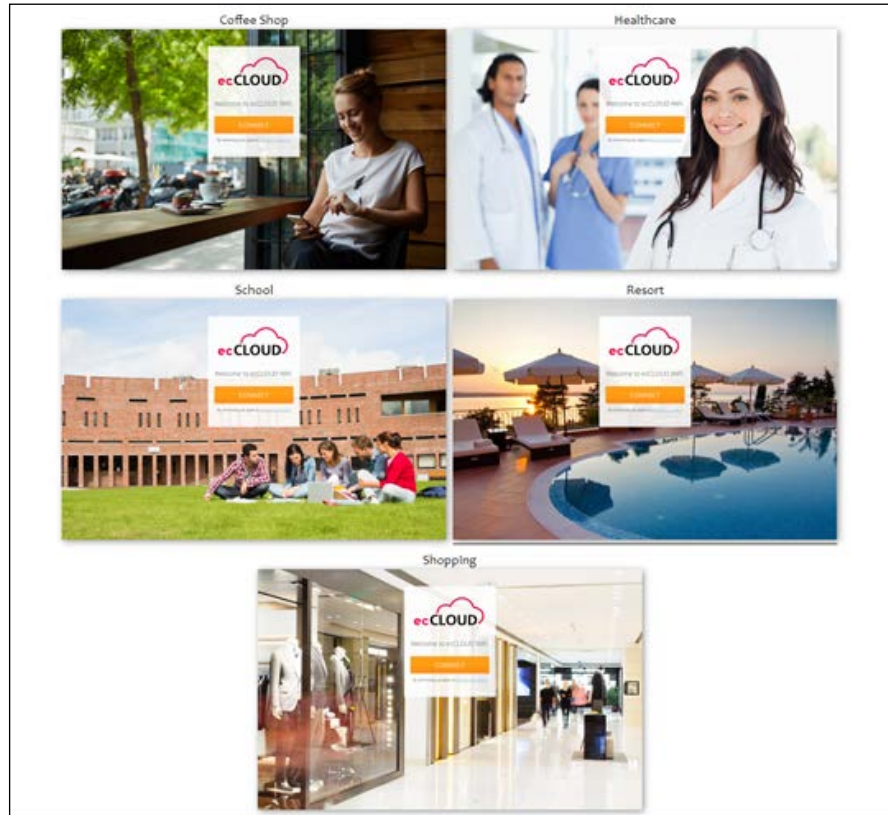
As for the DNS (domain name service), the administrator can configure a domain name that wireless clients will see for the captive portal page. If the DNS is not configured, clients will see the IP address of the AP in the URL of the captive portal page.

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.

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.

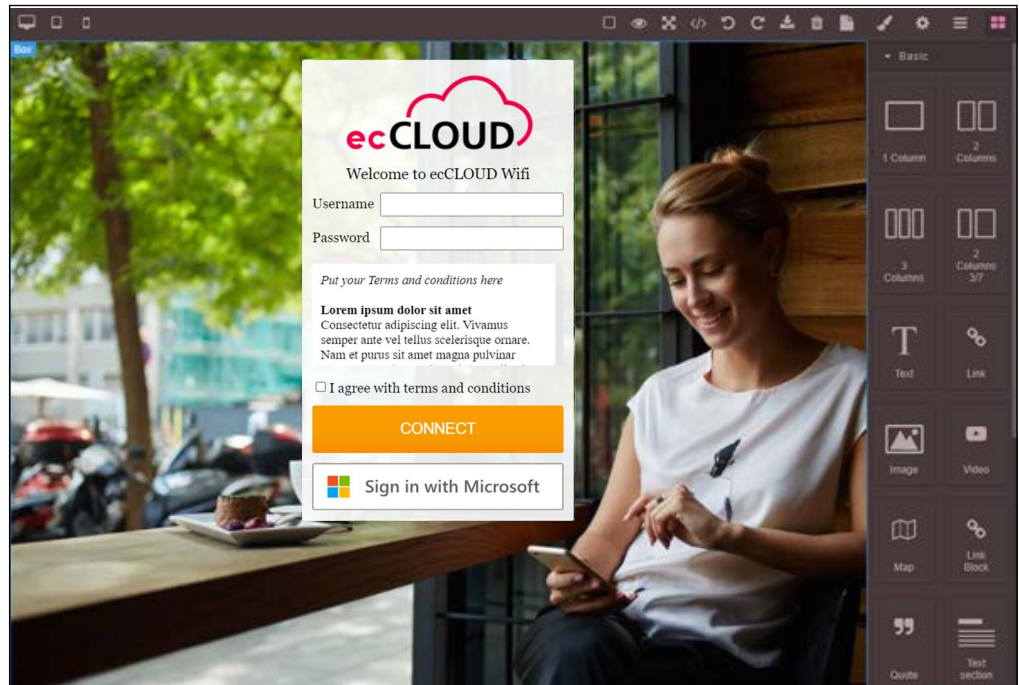
When you create a captive portal and access the editor for the first time, you will be asked to select a theme for your portal. You can select a theme that is appropriate for your service and start editing the page content.

Figure 75: AuthPort Captive Portal Themes



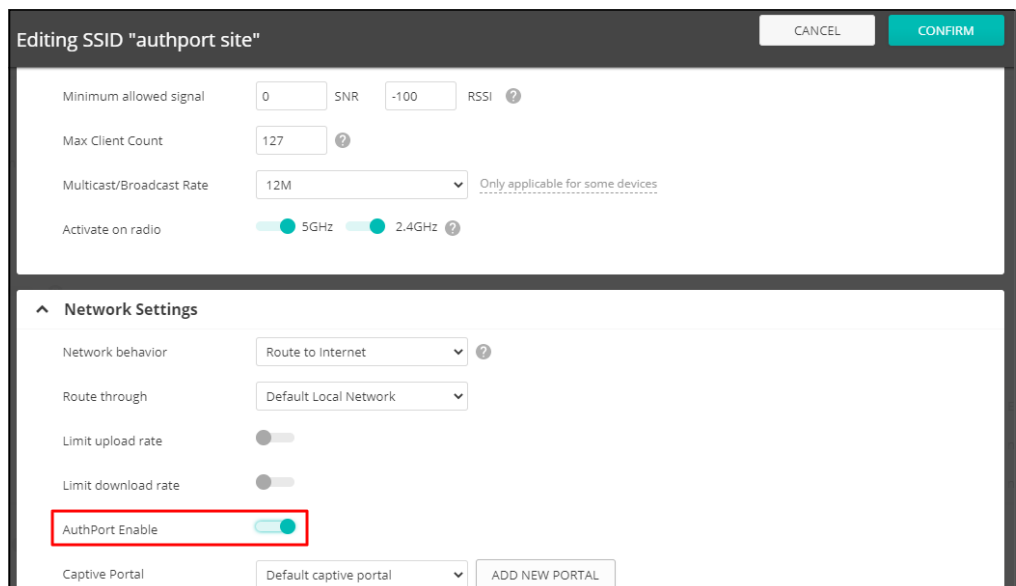
After selecting a template, you will enter the captive portal editor. The editor layout consists of three main parts; a tool bar, an options/attributes panel, and a preview frame. The tool bar is at the top of the editor. On the right-hand side is where the options or attributes can be configured. The preview frame allows you to drag-and-drop page objects and check your portal design in real-time.

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



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.

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

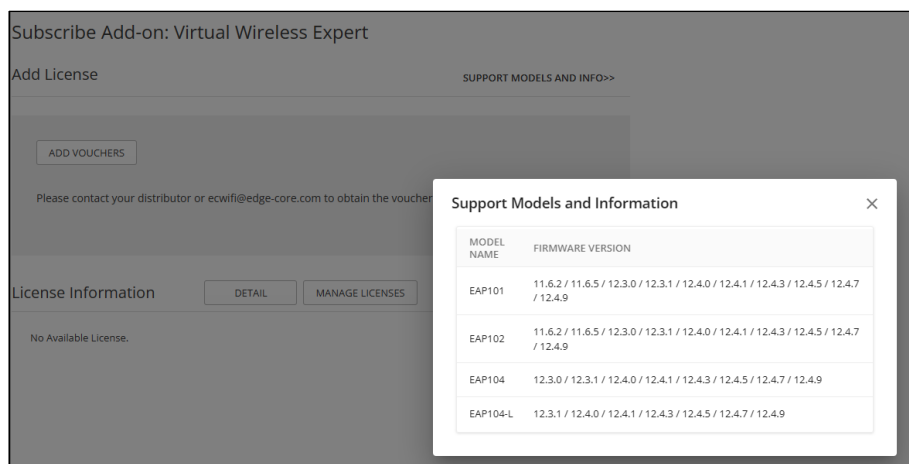


Supported Devices and Firmware Versions

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



Activating Freemium The freemium version can be activated globally at the cloud level or individually at the site level.

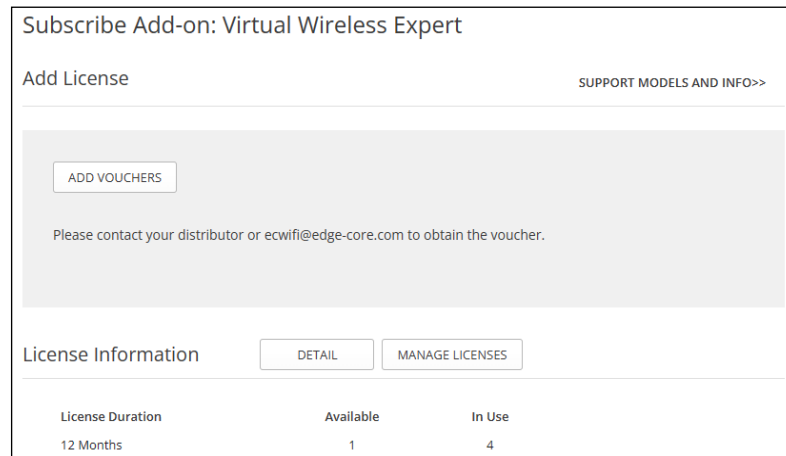
1. In the Cloud or Site menu, click 'Add-ons' and then 'Activate' under Aprecomm's Virtual Wireless Expert.
2. After confirming the activation, it automatically installs the Aprecomm package on devices running compatible firmware.

i **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'.

Figure 81: Apply VWE Licenses

Manage Licenses: Virtual Wireless Expert

ACTIONS REFRESH CUSTOMIZE EXPORT

	NAME	PRODUCT	FW	CREATED ON	SITE
<input type="checkbox"/>	5B-13	EAP101 EC21866002065	12.4.9-1293 (1) 12.4.9-1299 (2) ✓	2 years ago 2022-05-20 15:07	Taipei Office 2
<input type="checkbox"/>	5B-14	EAP101 EC21866002091	12.4.9-1293 (1) 12.4.9-1299 (2) ✓	2 years ago 2022-05-20 15:07	Taipei Office 2
<input type="checkbox"/>	5A-501	EAP101 EC21866001882	12.4.9-1293 (1) 12.4.9-1299 (2) ✓	2 years ago 2022-05-20 15:07	Taipei Office 2
<input type="checkbox"/>	5A-10	EAP101 EC21866001763	12.4.9-1293 (1) 12.4.9-1299 (2) ✓	a year ago 2022-10-06 17:03	Taipei Office 2
<input type="checkbox"/>	EAP102	EAP102 EC21266003799	11.2.0-796 ⚠	2 years ago 2022-06-30 12:03	Beaverworks
<input checked="" type="checkbox"/>	4F	EAP101 EC21870004186	12.4.9-1299 (1) ✓ 12.4.9-1293 (2)	6 months ago 2023-07-10 17:27	Taipei Office 2
<input type="checkbox"/>		EAP101	12.4.5-1118 (1)	3 months ago	

7. Filter the available licenses by the number of available days and apply as needed.

Figure 82: VWE Licenses per Number of Days

License Application

Selected Devices: 1

Devices with Applied License: 0

Apply License: Available > Days* 30 SUBMIT

There is 1 available license.

⚠ The licenses will be applied to those devices without licenses.
 ⚠ If the number of available licenses is less than the selected devices, you can apply the license first, and repeat this steps to choose other valid licenses for other devices

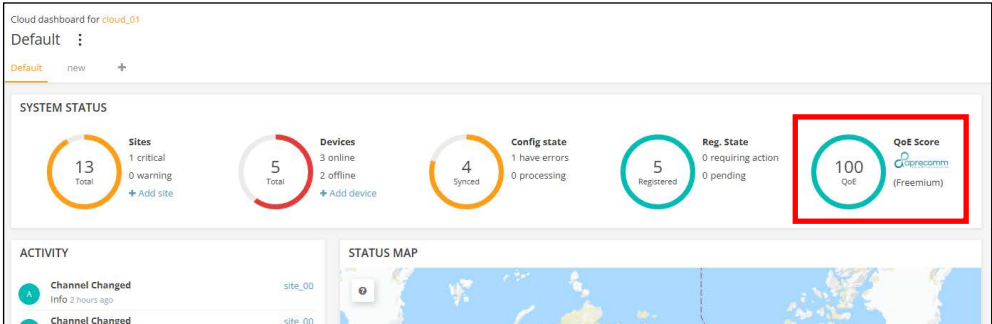
CANCEL APPLY

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.

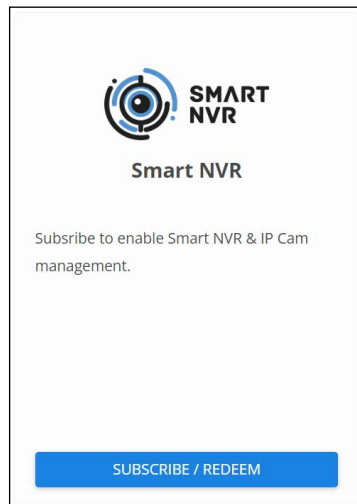
Figure 83: Aprecomm QoE Score



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.

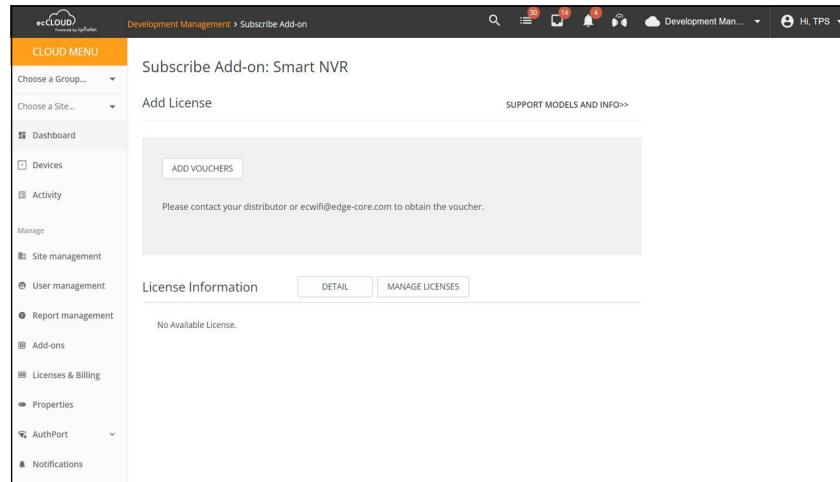
Figure 84: Smart NVR Add-On



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.

Figure 85: Adding Smart NVR Licenses

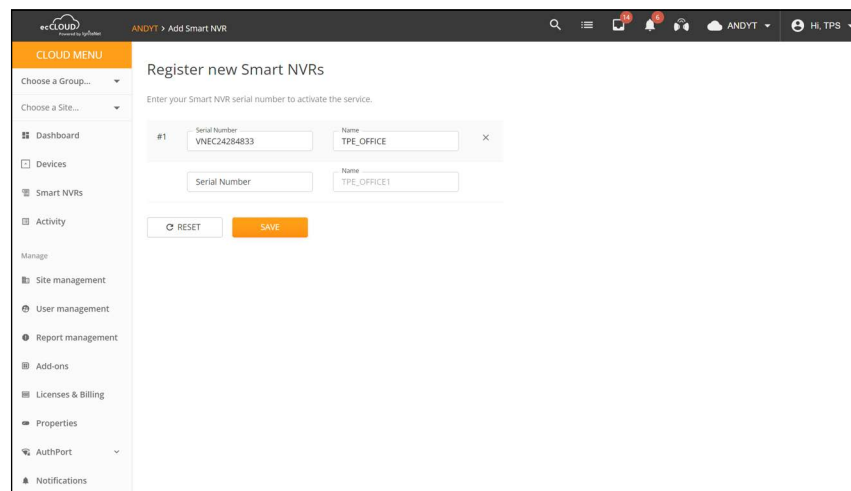


Once the voucher is successfully redeemed, the Smart NVR option will appear in the Cloud Menu.

Adding Smart NVR Devices

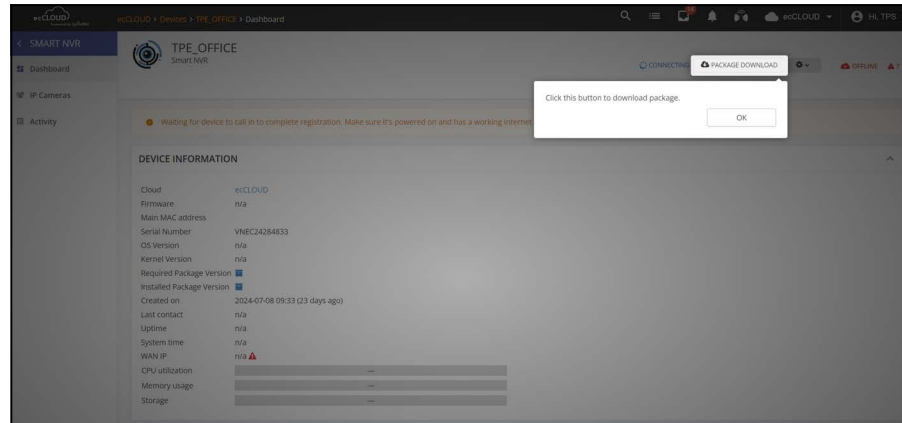
The currently supported Smart NVR device is a VM-based service. To add a new device, you will need the device's serial number. Please contact your distributor or Edgecore sales to obtain the serial number.

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.

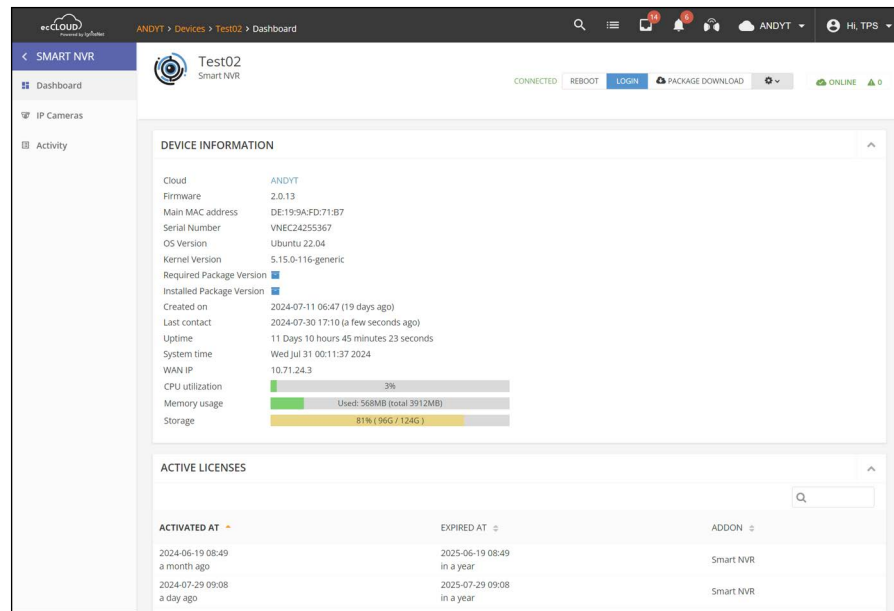
Figure 87: Installing and Registering a Smart NVR



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.

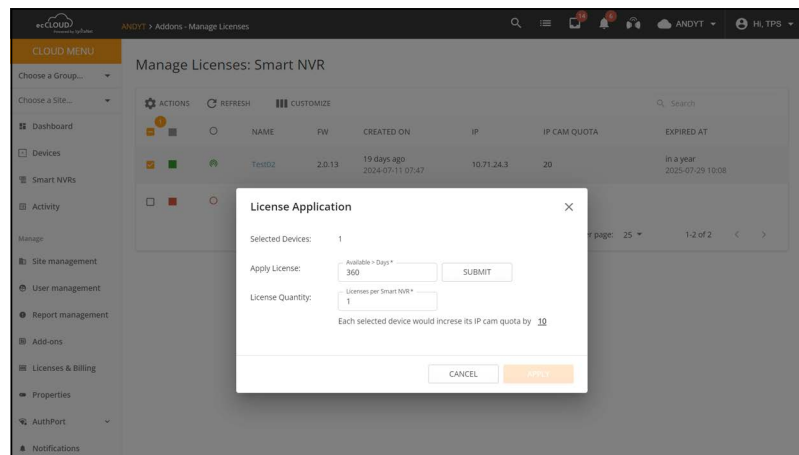
- Device Information Section:
 - **Cloud** — The name of the cloud managing the selected Smart NVR.
 - **Firmware** — The current firmware version installed on the Smart NVR.
 - **Main MAC Address** — The MAC address of the Smart NVR.
 - **Serial Number** — The Serial Number of the Smart NVR.
 - **OS 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.

- **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

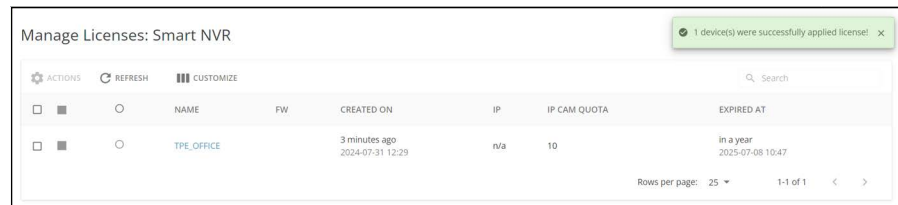
Once you have configured the Smart NVR device, you can add IP cameras. Each Smart NVR license has a quota of ten IP cameras.

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.

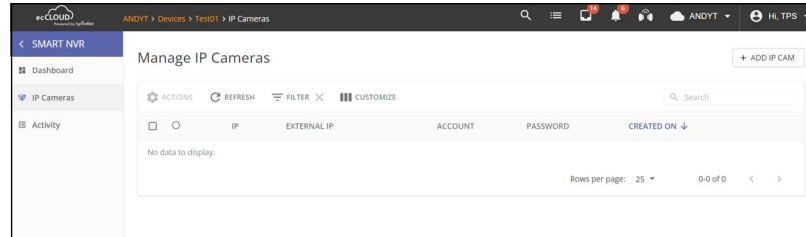
Figure 90: Available Quotas for IP Cameras per Smart NVR device



4. Confirm the available quota of IP cameras on each Smart NVR.

Add IP Cameras To add an IP camera to the Smart NVR, users can scan the IP camera through their Edgecore Access Point.

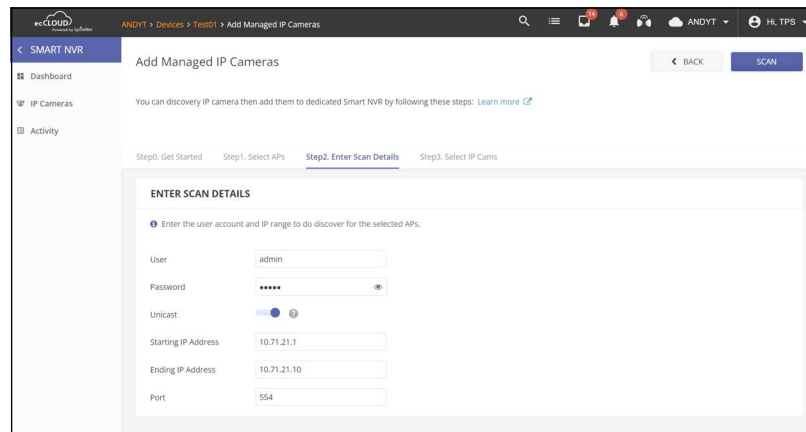
Figure 91: Add IP Cameras



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.

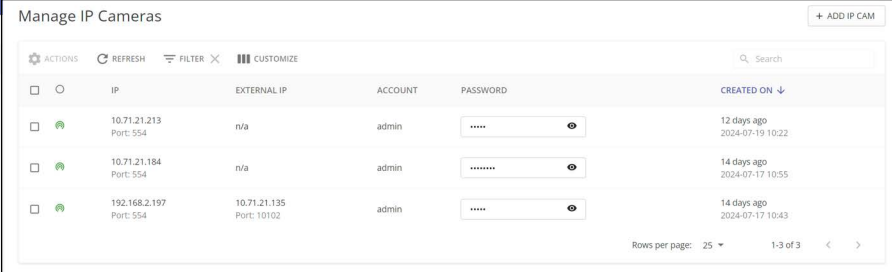
Figure 92: IP Cameras Scan Details



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.

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



The screenshot shows the 'Manage IP Cameras' interface. It includes a search bar, a table with columns for IP, External IP, Account, Password, and Created On, and a '+ ADD IP CAM' button. The table contains three rows of camera information.

IP	EXTERNAL IP	ACCOUNT	PASSWORD	CREATED ON
10.71.21.213 Port: 554	n/a	admin	12 days ago 2024-07-19 10:22
10.71.21.184 Port: 554	n/a	admin	14 days ago 2024-07-17 10:55
192.168.2.197 Port: 554	10.71.21.135 Port: 10102	admin	14 days ago 2024-07-17 10:43



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).

3

General Site Configuration

This chapter describes site configuration, including parameters that apply to all site devices or to the overall site.

- [“Overview of Sites” on page 94](#)
- [“Creating a Site” on page 95](#)
- [“Displaying the Site Dashboard” on page 103](#)
- [“Creating a Custom Site Dashboard” on page 104](#)
- [“Monitoring Wireless APs and Clients” on page 107](#)
- [“Schedule Maintenance Tasks” on page 111](#)
- [“Site Notifications” on page 112](#)

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.

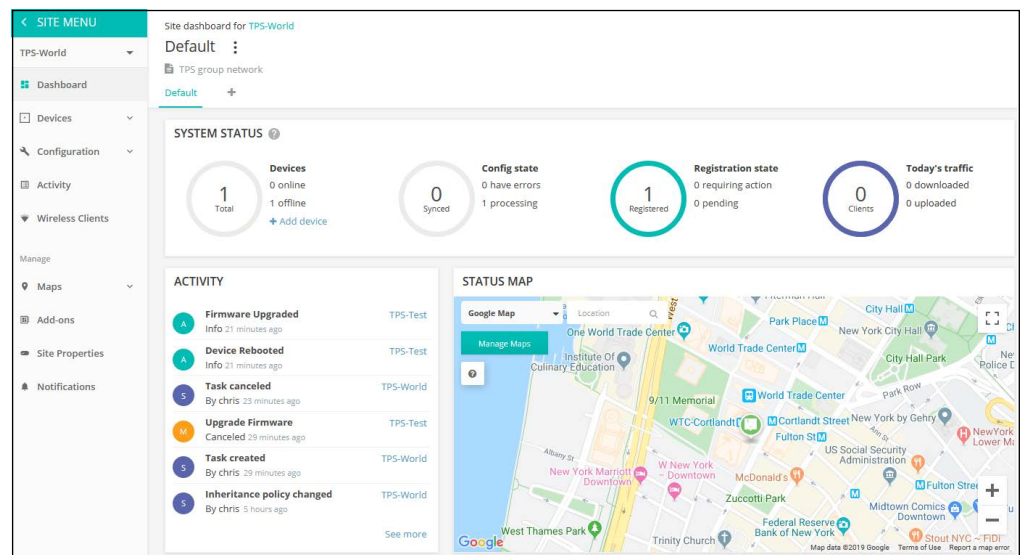
For example, if you are installing 50 APs for a hotel chain, each hotel location would be represented by a different site on the ecCLOUD controller. Each site can have a geographical location associated with it, a set of floor maps, and even preferred language and time zone settings.



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

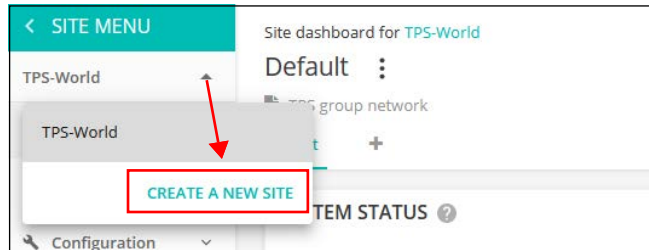


Creating a Site

When creating your first cloud, you are also prompted to create your first site and add devices. See [“Creating Your First Cloud” on page 28](#) 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

The screenshot shows a web form titled "Create a site". It is divided into two main sections: "General Settings" and "Locations and Maps".

General Settings

- Site name ***: A text input field.
- Description**: A larger text area for notes.
- Enable Configuration**: A toggle switch that is currently turned on (orange).
- Upgrade At Registration**: A toggle switch that is currently turned on (orange).
- Allow auto re-registration**: A toggle switch that is currently turned off (grey).

Locations and Maps

Location search

A map of Africa and surrounding regions is displayed. A red location pin is placed on the coast of West Africa, near the Gulf of Guinea. Below the map, there are input fields for "Latitude" and "Longitude", both currently showing "0".

At the bottom of the form, there are two buttons: "CANCEL" and "CREATE".

General Settings

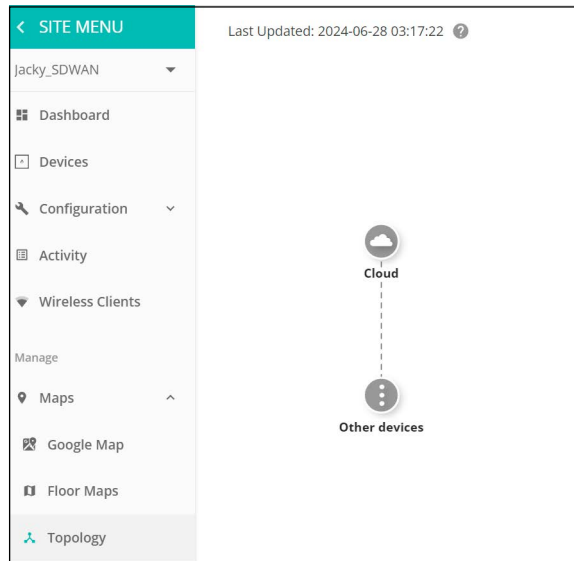
- **Site Name** – The name of your site. You should choose something short but meaningful. For example, use “ParkSide Atlanta” for a site that represents the Atlanta installment of a fictional ParkSide hotel chain.
- **Description** – Add any notes about your site here.
- **Enable Configuration**: This 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.

- 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.

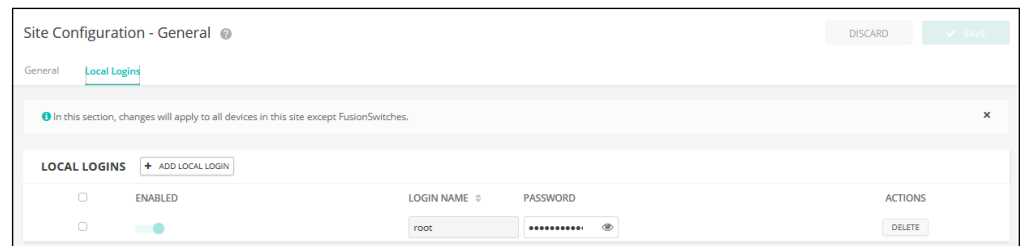
Figure 99: Setting the Regulatory Country



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

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

The screenshot shows a web interface titled "Register new devices". It includes a sub-header "Register new devices" and a paragraph explaining that a new device can be added by inputting or scanning the serial number and MAC address, with a "Learn more" link. Below this, there is a text input field for "Add the following devices to the following site" containing "TPS-World". There are two toggle switches: "Inherit site-level settings" (which is turned on) and "Enable barcode scanning mode" (which is turned off). A "Batch Upload File" section contains three input fields: "Serial Number", "MAC Address", and "Name" (with "0" entered). A "+ UPLOAD" button is located to the right of these fields. At the bottom, there are "RESET" and "SAVE" buttons. A note at the bottom left states "You can register up to 48 devices."

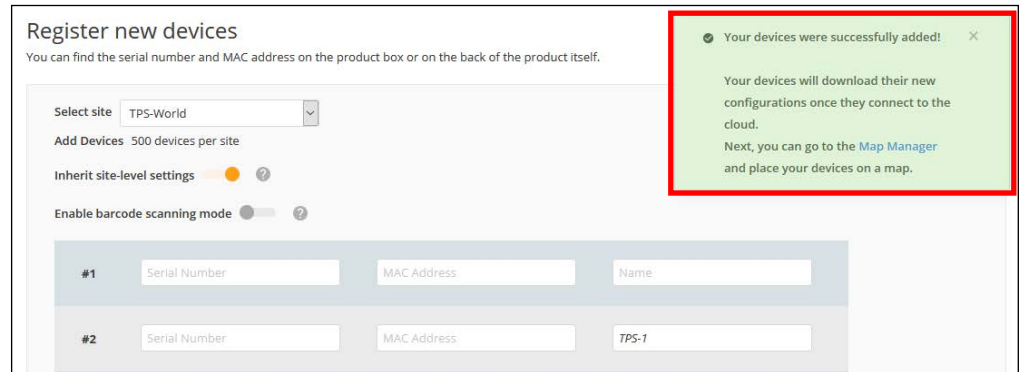
When the controller adds a device the following pop-up window is displayed warning you that the device will inherit settings from the ecCLOUD site configuration. Click OK.

Figure 103: Adding Devices Warning Message

The screenshot shows a warning message pop-up window titled "What happens now?". The text reads: "Now that you've registered your first device, we wanted to let you know what's going to happen next." Below this is a section titled "Configuration Inheritance" with an information icon. The text says: "After registration, the device's configuration will inherit certain settings from your site's configuration. This includes key settings like:" followed by a bulleted list: "The local login credentials", "Device's time zone", and "All other site settings". At the bottom left, there is a link "Learn more about configuration settings" with a right-pointing arrow. At the bottom right, there is a checkbox labeled "Don't show me this again" and an "OK" button.

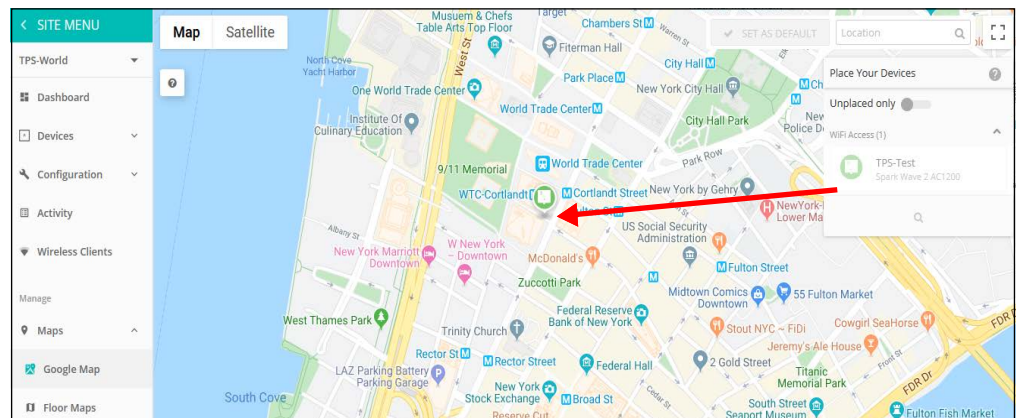
When devices have been successfully added, a message appears at the top of the "Register new devices" page. Click on the blue link "Map Manager" in the message to place your device on a map.

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.

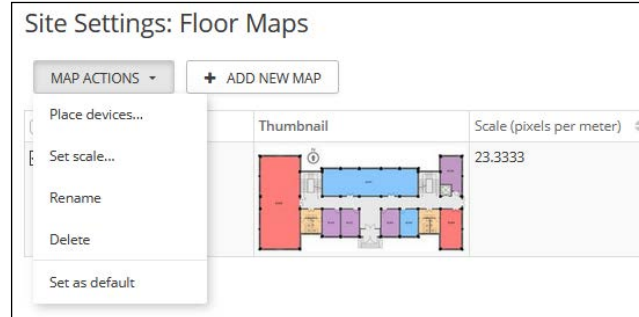
You can upload one or more custom images to create a background for the floor plan by clicking "Add New Map."

Figure 106: Adding a Floor Map



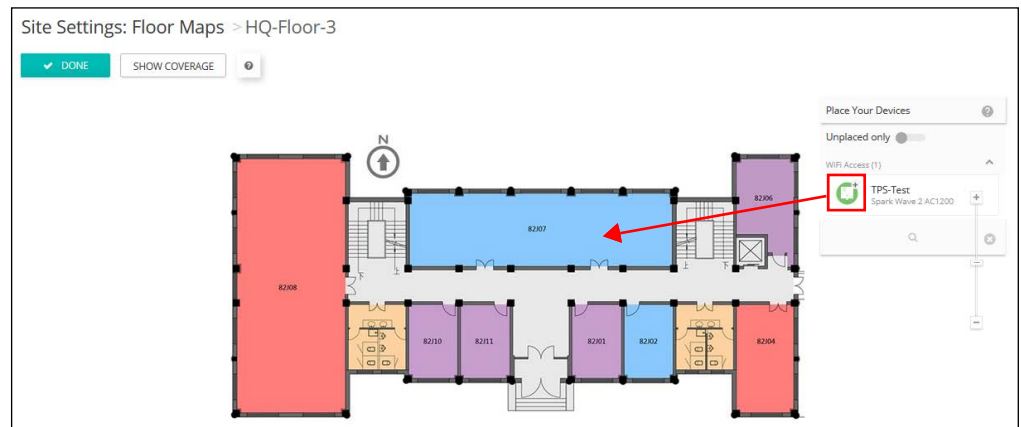
Use the “Place devices” feature from the Action icons or pull-down menu to set the location of wireless devices on the floor map image.

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

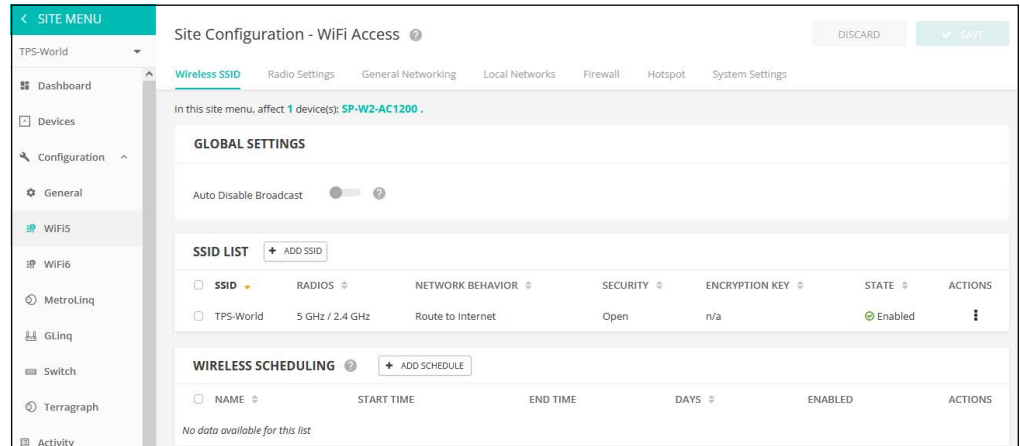


WiFi Configuration From the Site menu, select “Configuration” and then “WiFi5” or “WiFi6” to configure wireless settings that are inherited by all the site’s AP devices and any new devices that are added to the site.

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 116 for more detailed descriptions of wireless device configuration.

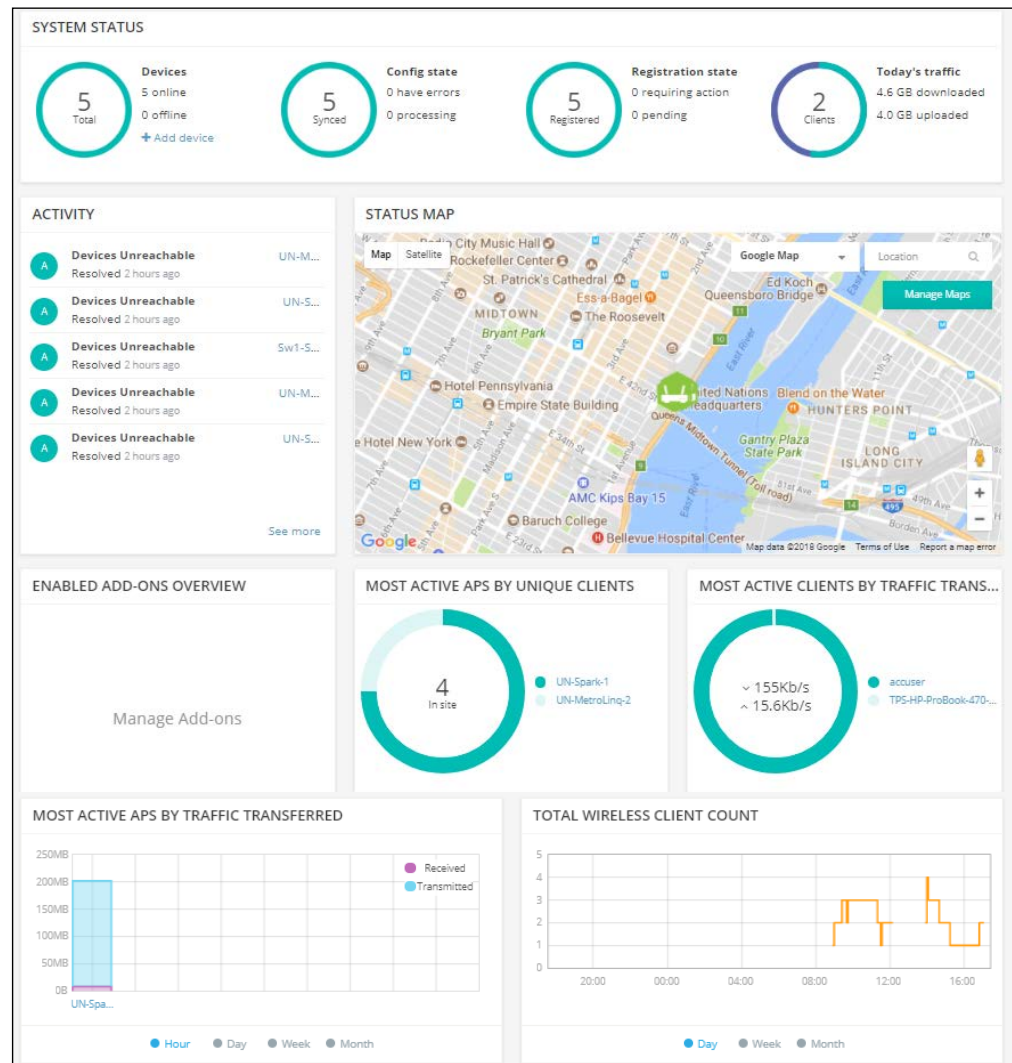
Figure 109: WiFi5 Configuration



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.

- **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

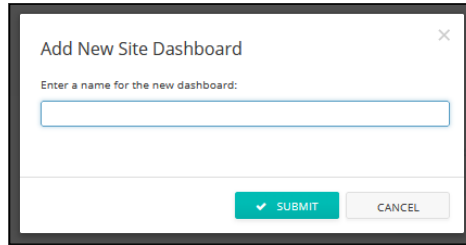
In the default site dashboard, click the plus sign next to the default tab at the top to create a custom dashboard suitable for your requirements.

Figure 111: Adding a Custom Site Dashboard



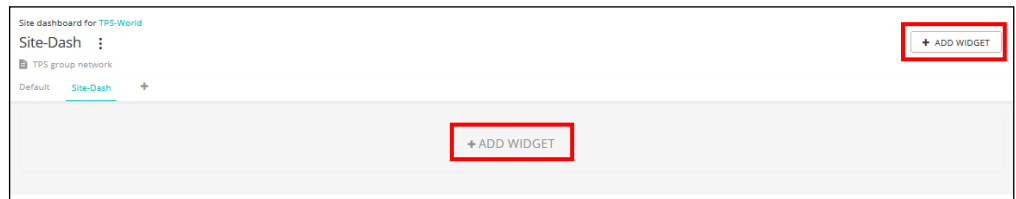
Enter a name for the new custom dashboard and click SUBMIT.

Figure 112: Naming a Custom Site Dashboard



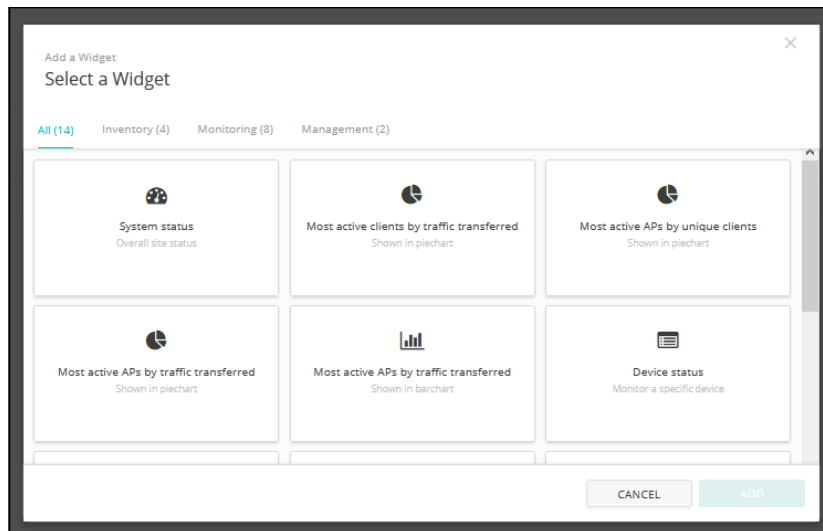
A new tab will appear next to the default dashboard tab with the custom dashboard's name. Click on one of the "+ Add Widget" buttons to add the desired item for the new dashboard.

Figure 113: Adding a Widget to a Custom Site Dashboard



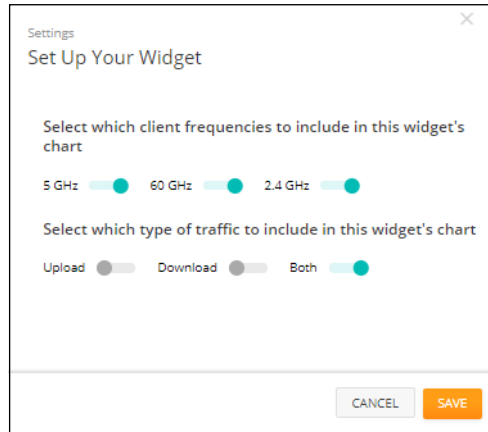
Once a widget is selected click the "ADD" button.

Figure 114: Selecting a Widget for a Custom Site Dashboard



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.

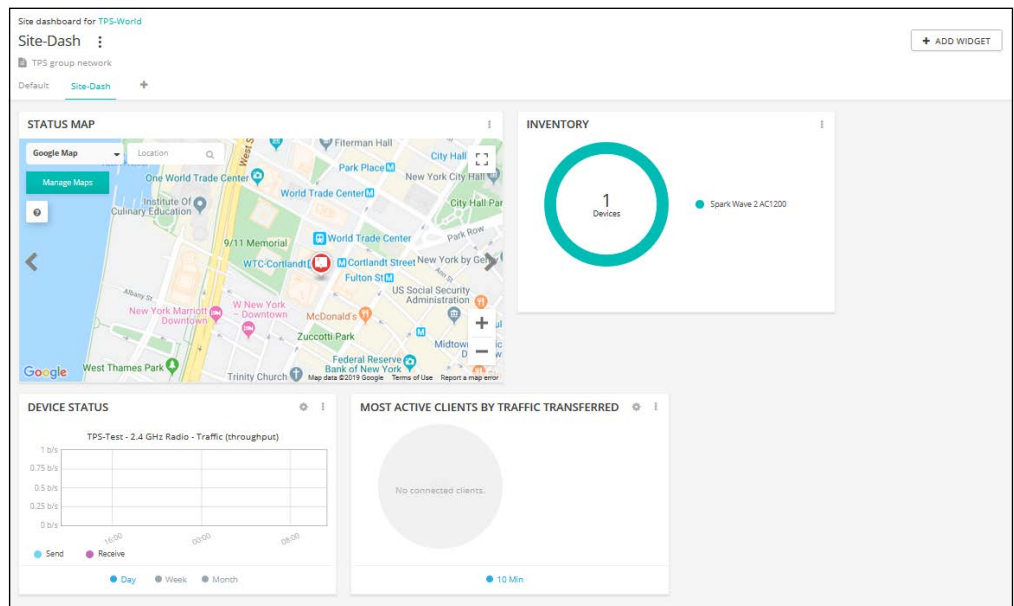
Figure 115: Customizing a New Site Dashboard Widget



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

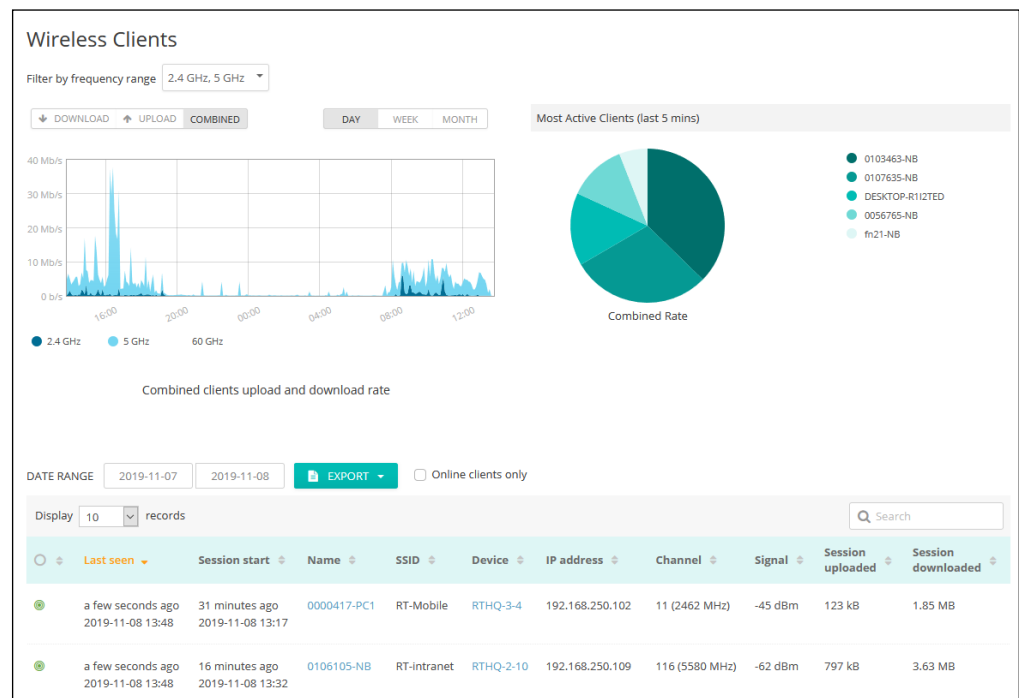


Monitoring Wireless APs and Clients

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.

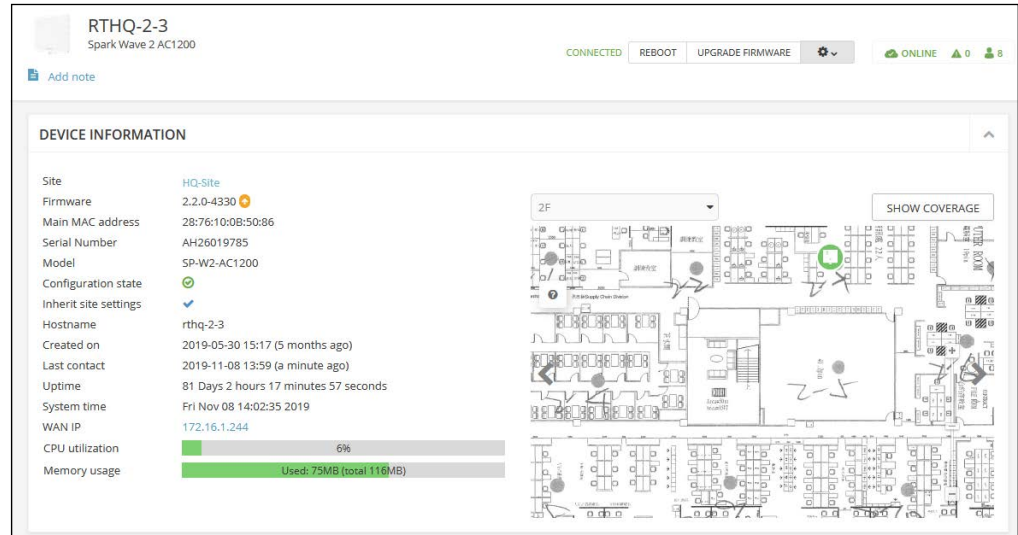
- **Export** — Exports the wireless client information to a CSV excel sheet available from the Activity menu under maintenance.
- **Online clients only** — Restricts the displayed session logs to wireless clients that are currently online.

Session Logs

To sort the session logs, click on the ascending or descending arrows for each column heading.

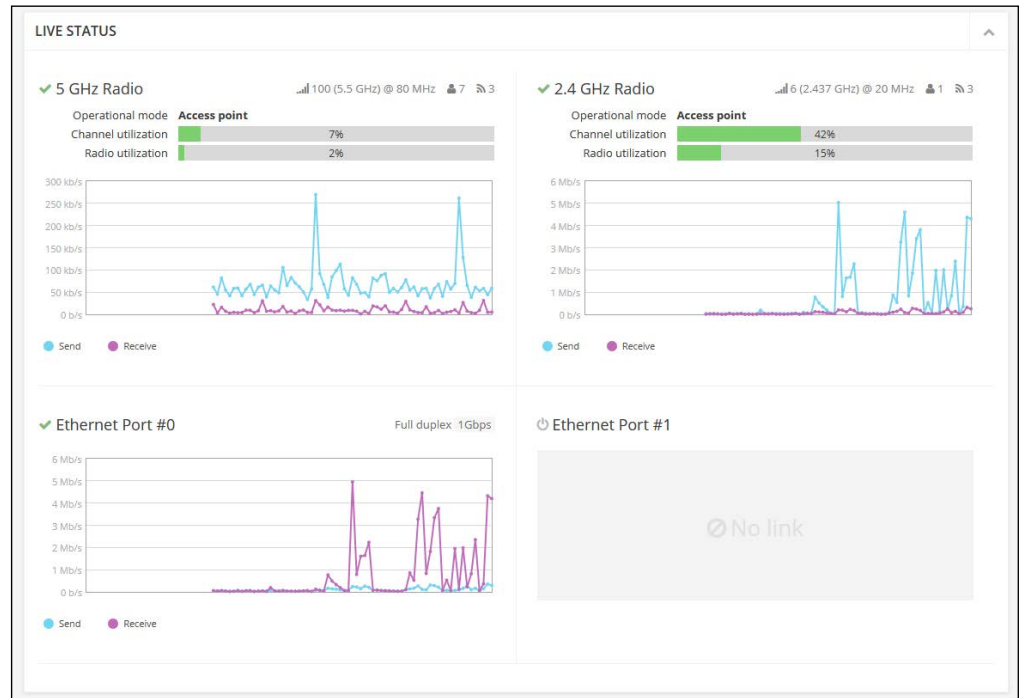
Click on any name in the Device column to open the Device information page for details on a specific AP. The first section of the Device information page includes details about the AP, including a location map.

Figure 118: Wireless AP Information



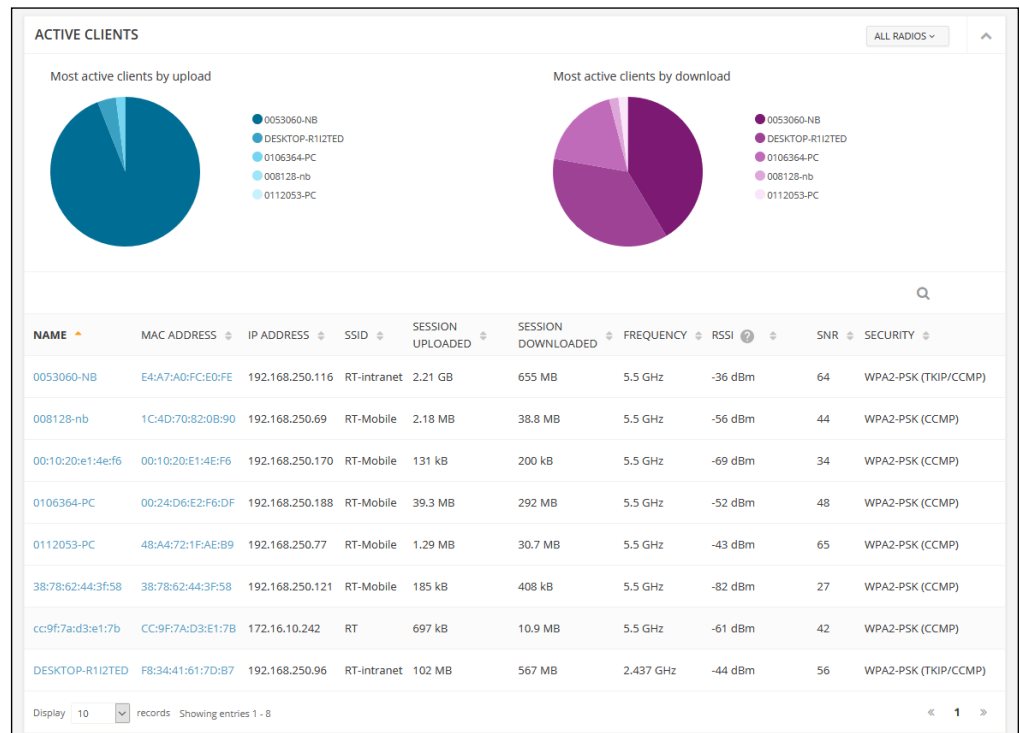
The second section of the Device information page shows throughput and utilization data for radio and Ethernet interfaces on the AP.

Figure 119: Wireless AP Live Status



The third section of the Device information page shows details on wireless clients associated to the AP.

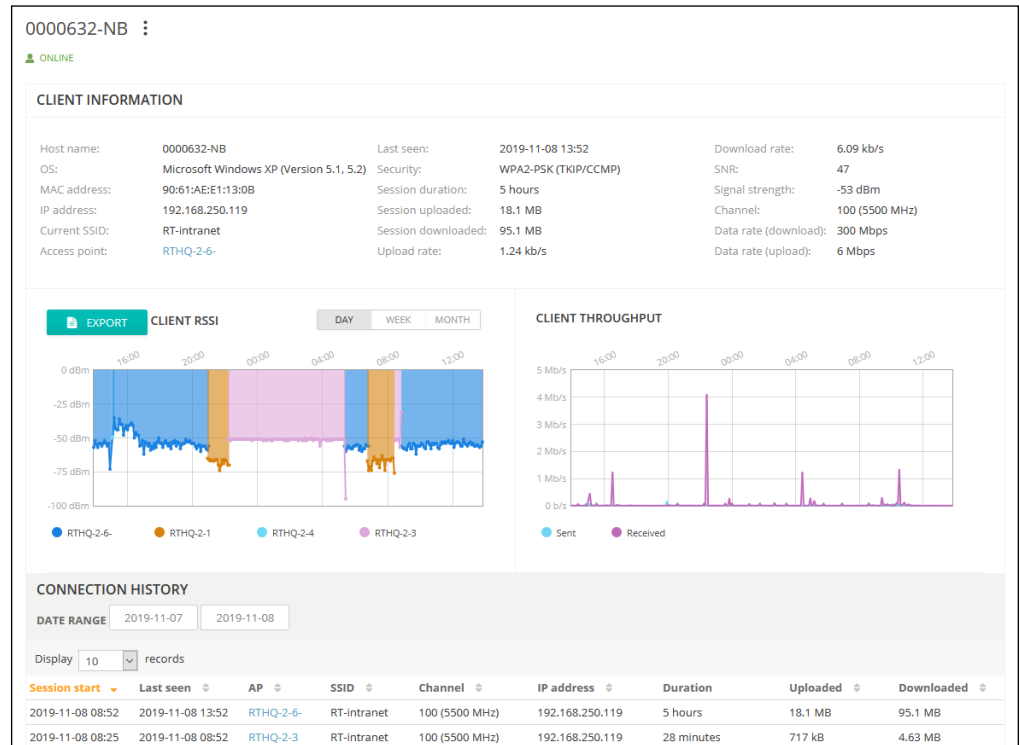
Figure 120: Wireless AP Active Clients



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.

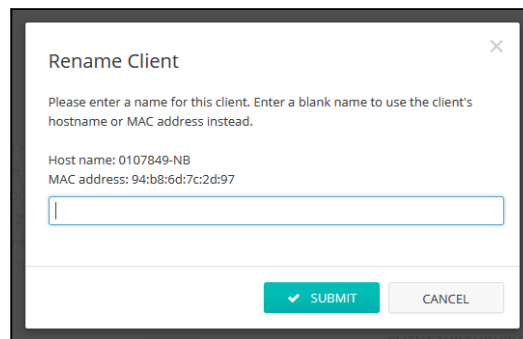
The client information page shows detailed information on the client, signal strength and throughput data, and a list of the client's connection history.

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.

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

Manage your devices											
MANAGE BULK-REBOOT + ADD DEVICE UPGRADE FIRMWARE											
ACTIONS 🔄 ⌵ 🔍 Search											
				NAME	PRODUCT	FW	REG. STATE	CREATED ON	CLIENTS	TRAFFIC	
<input type="checkbox"/>	🟢	🟢	🟢	✓	RTHQ3-5	SunSpot AC1200 AG33033936	1.4.1-3044	Registered	17 days ago 2019-10-22 20:10	3	31.1 kb/s
<input type="checkbox"/>	🟢	🟢	🟢	✓	RTHQ-3-10	SunSpot AC1200 AH12002512	1.4.1-3044	Registered	25 days ago 2019-10-14 12:20	3	57.7 kb/s

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

New Firmware Upgrade Task

Select Product Line:

Select Model:

Upgrade to version:

Give this task a name:

When do you want to start upgrade? Now Later 📅

How do you want the upgrade performed? All at the same time One at a time 60 minutes

Which devices do you want to upgrade? All out-of-date compatible devices Let me choose

Reset to device defaults?

Number of selected devices: 6

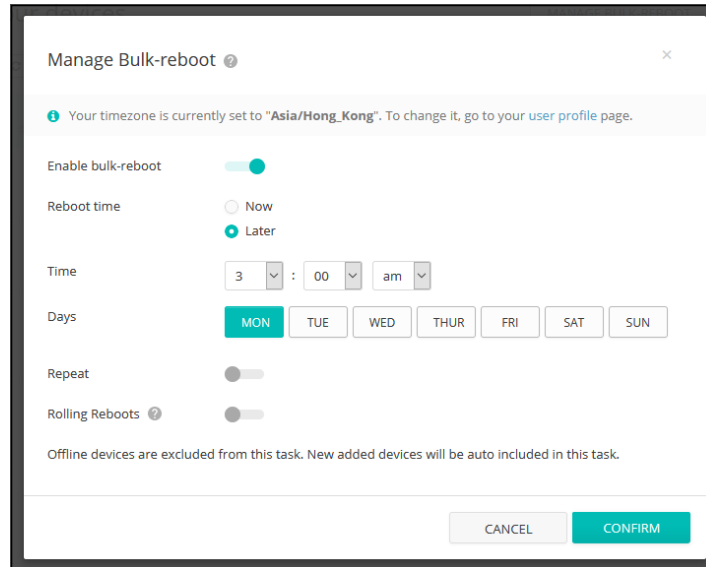
Device Name	Product	Current FW	New FW	MAC
<input checked="" type="checkbox"/> RTHQ-2-2	Spark Wave 2 AC1200	2.2.0-4330	2.2.1-4338	28:76:10:0C:24:FE
<input checked="" type="checkbox"/> RTHQ-2-3	Spark Wave 2 AC1200	2.2.0-4330	2.2.1-4338	28:76:10:0B:50:86
<input checked="" type="checkbox"/> RTHQ-2-5	Spark Wave 2 AC1200	2.2.0-4330	2.2.1-4338	28:76:10:0C:50:96
<input checked="" type="checkbox"/> RTHQ-2-9	Spark Wave 2 AC1200	2.2.0-4330	2.2.1-4338	28:76:10:0D:10:9E
<input checked="" type="checkbox"/> RTHQ-3-4	Spark Wave 2 AC1200	2.2.0-4330	2.2.1-4338	28:76:10:0C:55:8A
<input checked="" type="checkbox"/> RTHQ-3-6	SunSpot AC1200	1.4.0-3039	1.4.1-3044	28:76:10:07:0B:D8

Show entries of 21 entries « 1 2 3 »

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 72 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.

Figure 126: Site Notification Settings

Notification Settings

The settings on this page will be used for any email or Slack notifications sent for this site.

The Slack Add-on is not enabled for this site. You will not receive any notifications to your Slack account, even if you have the "Notify Slack" setting checked below, until the Add-on is enabled. You can enable the Slack Add-on by clicking [here](#) ✕

General

Note that if you leave the "Email contacts" blank, no email notifications will be sent regardless of the "Send email" settings below.

Language:

Email contacts:

Timezone:

Alerts

Receive email and/or Slack notifications whenever alerts are created. Note that you can disable creation of individual alerts using the toggle switches. No notifications will be sent for disabled alerts regardless of the "Send email" and "Notify Slack" settings.

Devices Unreachable
This alert is created when one or more of your devices cannot be reached.

Send email
 Notify Slack

Processing delay * minutes ?

Device Configuration Failed
This alert is created when an attempt to update configuration on one of your devices fails.

Send email
 Notify Slack

Device Requires Action
This alert is created when devices have registration issues that require your attention.

Send email
 Notify Slack

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.

- **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.

- **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.

4

Site WiFi 5 Configuration

This chapter describes configuration settings for WiFi 5 access point devices. It includes the following sections:

- [“Wireless SSID Configuration” on page 117](#)
- [“Radio Settings” on page 126](#)
- [“General Networking Settings” on page 129](#)
- [“Local Network Settings” on page 135](#)
- [“Firewall Settings” on page 137](#)
- [“Hotspot Settings” on page 140](#)
- [“System Settings” on page 147](#)

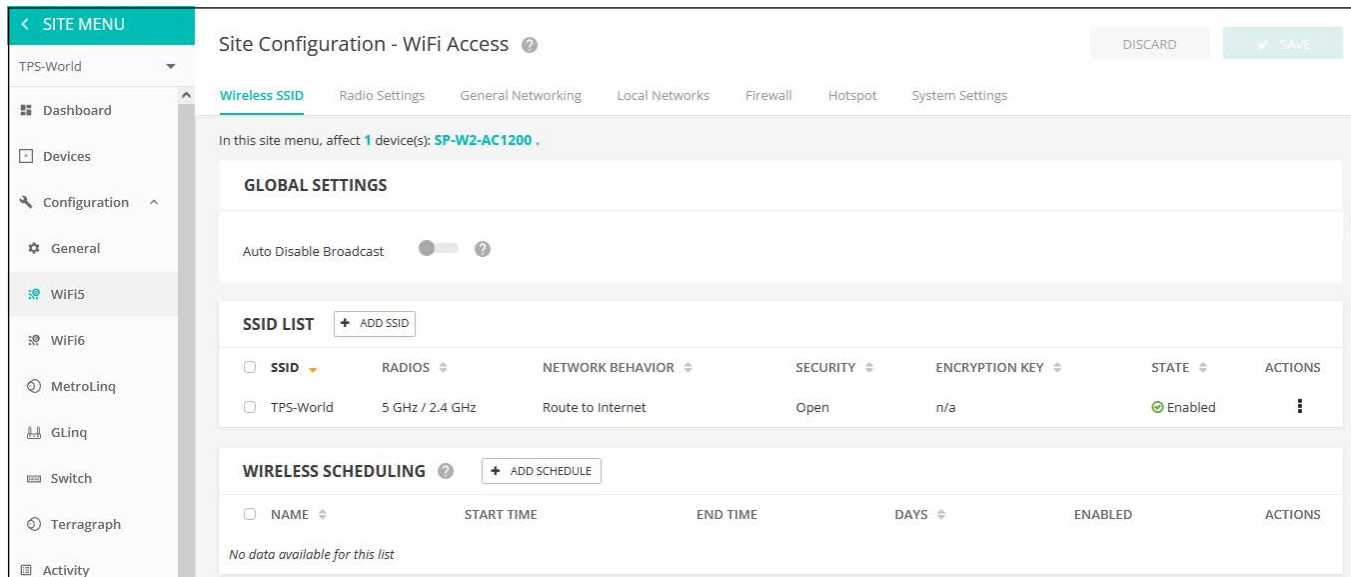
Wireless SSID Configuration

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

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 screenshot shows the 'Add SSID' configuration page with three main sections: General Settings, Network Settings, and Security Settings. The General Settings section includes options for enabling the SSID, setting the SSID name, broadcasting the SSID, client isolation, blocking multicast forwarding, minimum allowed signal (SNR and RSSI), maximum client count, multicast/broadcast rates for 5GHz and 2.4GHz, and activating the radio on both frequencies. The Network Settings section includes network behavior (Route to Internet), route through (Default Local Network), and limits on upload and download rates. The Security Settings section includes OSEN (disabled), security method (Open), RADIUS MAC Auth (disabled), and Access Control List (disabled).

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)
- **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)

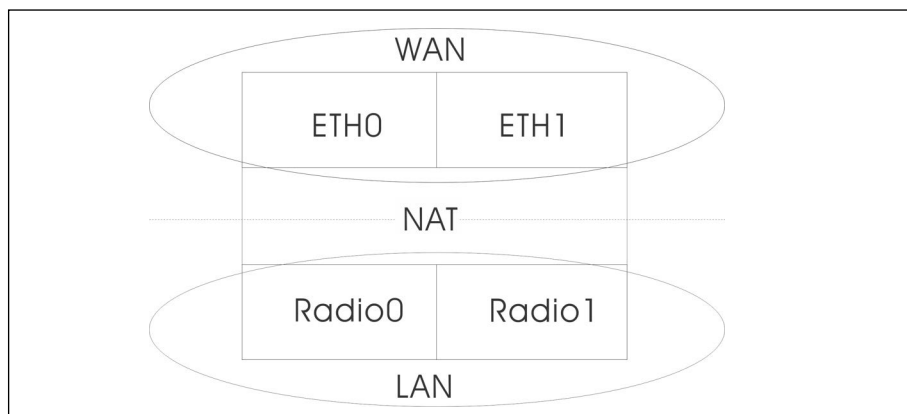
- **Max Client Count** — Sets the maximum number of wireless clients that can be connected to this SSID at the same time. (Default: 127; Range: 0 to 127)
- **Multicast/Broadcast Rate** — Allows a limit to be placed on the wireless bandwidth consumed by multicast and broadcast packets.
 - **Radio 5 Ghz** — 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)

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.

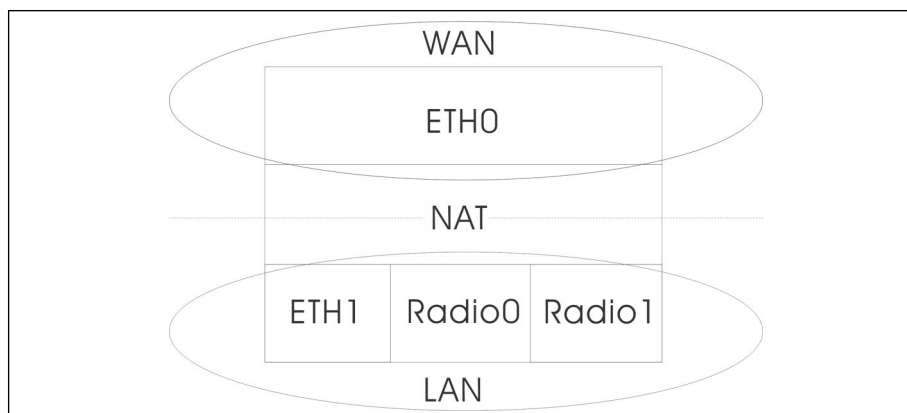
Figure 129: Bridge to Internet



- **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



- **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 133](#). 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

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

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.

- **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)

- **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 screenshot shows the 'Add schedule' configuration interface. At the top right are 'CANCEL' and 'CONFIRM' buttons. The main section is titled 'Schedule Settings' and contains a note about the site's timezone being set to UTC. Below the note, there is a toggle for 'Enabled' which is currently turned on. There is a text input field for 'Name'. The 'Start time' is set to 12:00 am, and the 'End time' is set to 06:00 am. At the bottom, there are radio buttons for 'Days' (Mon, Tue, Wed, Thur, Fri, Sat, Sun), with 'Mon' selected.

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

GLOBAL SETTINGS

Band Steering

External Radius Enabled

WIRELESS 5 GHZ

PHYSICAL RADIO SETTINGS

Channel Bandwidth: 80MHz

Channel: Auto (all channels)
[EDIT CHANNEL LIST](#)

Disabled W52 Channel

Max Tx Power: 28 dBm (530 mW)

Beacon Interval: 100

ADVANCED RADIO SETTINGS

Max Client Count: 0

Probe Req. Data Push

WIRELESS 2.4 GHZ

PHYSICAL RADIO SETTINGS

Channel Bandwidth: 40MHz

Channel: Auto (all channels)
[EDIT CHANNEL LIST](#)

Max Tx Power: 30 dBm (1000 mW)

Beacon Interval: 100

20/40MHz Coexist

ADVANCED RADIO SETTINGS

Max Client Count: 0

Probe Req. Data Push

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 73](#)). When using the AuthPort add-on, you can configure settings for an external RADIUS server.

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

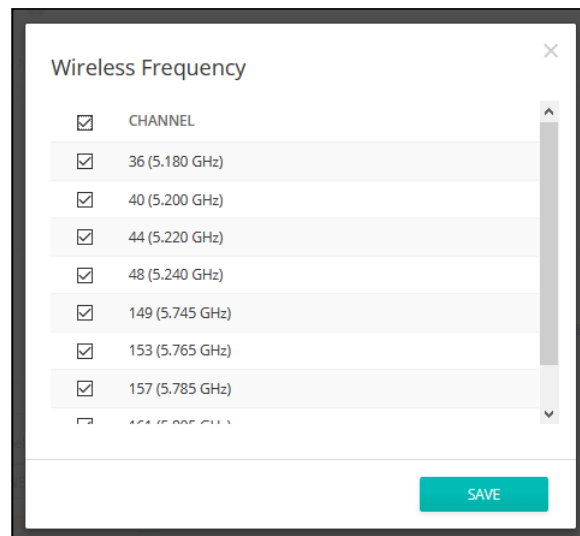
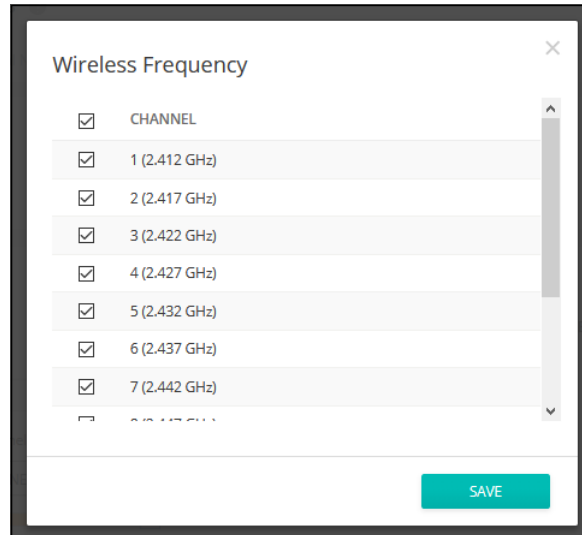


Figure 134: 2.4 GHz Radio Channels



- **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.

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

INTERNET

Only the Internet IP Address Mode and Mgmt VLAN settings can be changed here. The rest of these settings can only be overridden on a per-device basis at device-level config.

GENERAL SETTINGS

Internet Source: WAN Port

VLAN tag traffic:

IP Address Mode: DHCP

MTU Size: 1500

Fallback IP: 192.168.1.20

Fallback Netmask: 255.255.255.0

MGMT VLAN

Mgmt VLAN:

IPV6 SETTINGS

IP Address Mode: DHCP

Client ID:

ETHERNET

Some settings can only be overridden on a per-device basis at device-level config.

ETHERNET SETTINGS FOR WAN PORT

This port is the internet source for devices in this site

Auto negotiation:

ETHERNET SETTINGS FOR LAN PORT(S)

Network behavior: Bridge to Internet

Auto negotiation:

VLAN [+ ADD NEW VLAN](#)

VLAN ID	TAGGED PORTS	PPPOE PROFILE	UPLINK 802.1P	UNTAGGED INTERFACES	ACTIONS
33	WAN Port LAN Port(s)	Disabled	Video	Configure SSIDs	

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.

MGMT VLAN Settings

Figure 137: Management VLAN Settings

MGMT VLAN	
Mgmt VLAN	<input checked="" type="checkbox"/>
Mgmt VLAN ID	100
IP Address Mode	DHCP
Fallback IP	192.168.1.20
Fallback Netmask	255.255.255.0

- **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

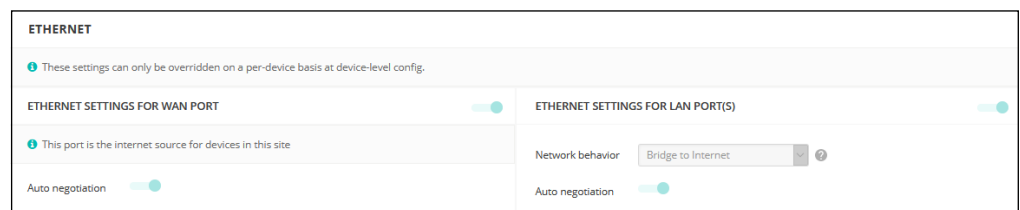
IPV6 SETTINGS	
IP Address Mode	DHCP
Client ID	

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 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.

- **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 118](#)).

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 140: VLAN Settings

VLAN ID	TAGGED PORTS	PPPOE PROFILE	UPLINK 802.1P	UNTAGGED INTERFACES	ACTIONS
33	WAN Port LAN Port(s)	Disabled	Video	Configure SSIDs	

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 118).
- **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

Add New VLAN [CANCEL] [CONFIRM]

General Settings

VLAN ID:

Ports: WAN Port LAN Port(s)

PPPoE Profile

Enable:

Uplink 802.1p

Uplink 802.1p:

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

LAN
+ ADD CUSTOM LAN

DEFAULT LOCAL NETWORK
BUILT-IN

<p>IP Address <input type="text" value="192.168.2.1"/></p> <p>Subnet Mask <input type="text" value="255.255.255.0"/></p> <p>MTU Size <input type="text" value="1500"/></p> <p>Enable STP <input type="checkbox"/></p> <p>Enable UPnP <input type="checkbox"/></p> <p>Enable RSTP <input type="checkbox"/></p> <p>Smart Isolation <input type="text" value="Disable (full access)"/></p> <p>Interface Members TPS-World (5 GHz), TPS-World (2.4 GHz)</p>	<p>DHCP Server <input checked="" type="checkbox"/></p> <p>DHCP Start <input type="text" value="100"/></p> <p>DHCP Limit <input type="text" value="150"/> ?</p> <p>Lease Time <input type="text" value="12hr"/></p> <p>DNS Servers (DHCP Option 6) <input type="text" value="Enter one IP address per line up to three addresses."/></p> <p>DNS Entries <input type="text"/> ?</p>
--	---

GUEST NETWORK
BUILT-IN

<p>IP Address <input type="text" value="192.168.3.1"/></p> <p>Subnet Mask <input type="text" value="255.255.255.0"/></p> <p>MTU Size <input type="text" value="1500"/></p> <p>Enable STP <input type="checkbox"/></p> <p>Enable UPnP <input type="checkbox"/></p> <p>Enable RSTP <input type="checkbox"/></p> <p>Smart Isolation <input type="text" value="Internet access only"/></p>	<p>DHCP Server <input checked="" type="checkbox"/></p> <p>DHCP Start <input type="text" value="100"/></p> <p>DHCP Limit <input type="text" value="150"/> ?</p> <p>Lease Time <input type="text" value="12hr"/></p> <p>DNS Servers (DHCP Option 6) <input type="text" value="Enter one IP address per line up to three addresses."/></p> <p>DNS Entries <input type="text"/> ?</p>
--	---

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.
 - **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)

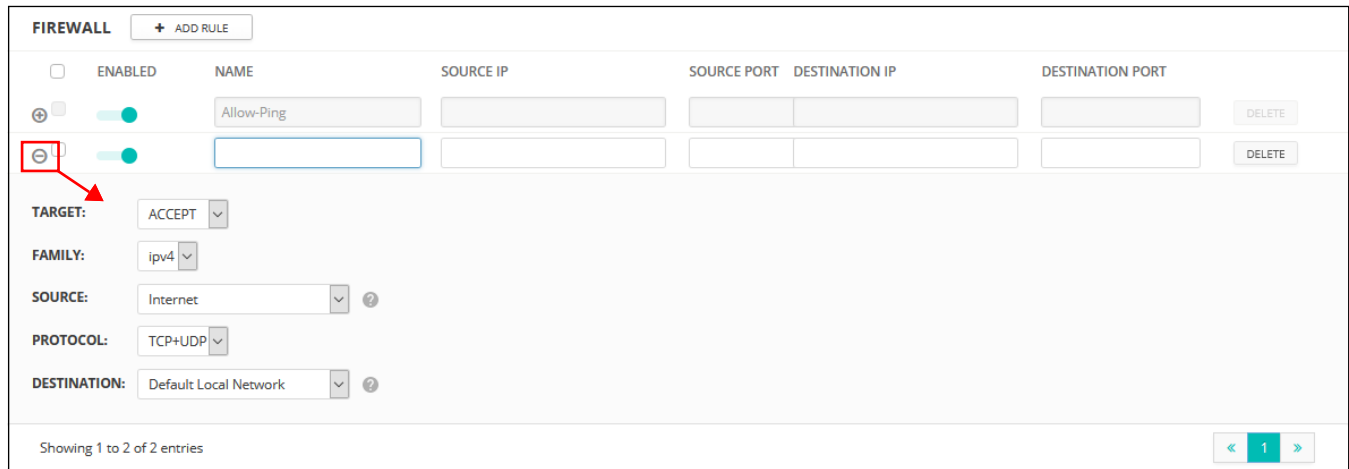
- **DHCP Limit** — Maximum number of addresses in the address pool. (Range: 1-254; Default: 150)
- **Lease Time** — The time period for which assigned IP addresses are valid.
- **DNS Servers** — List up to three DNS server IP addresses, one per line.
- **DNS Entries** — Only applicable for Spark AC Wave2 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)

- **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

PORT FORWARDING		+ ADD RULE				
ENABLED	NAME	PROTOCOL	EXTERNAL PORT	DESTINATION IP	DESTINATION PORT	DELETE
<input checked="" type="checkbox"/>		TCP+UDP				DELETE

Showing 1 to 1 of 1 entries

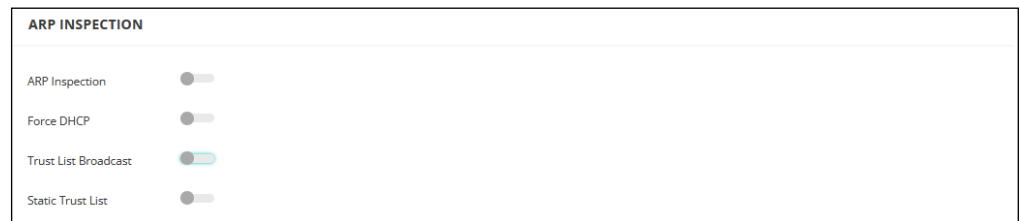
The following items are displayed on this page:

- **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)

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.

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 screenshot shows the DHCP Snooping configuration interface. At the top, there is a section titled 'DHCP SNOOPING'. Below this, there is a toggle switch labeled 'Enable' which is currently turned on (indicated by a green dot). Underneath the toggle is a '+ ADD' button. Below the button is a table with three columns: 'TRUST DHCP SERVER MAC', 'TRUST DHCP SERVER IP', and 'REMARK'. Each column has a corresponding input field. To the right of the 'REMARK' input field is a 'DELETE' button. Below the table, it says 'Showing 1 to 1 of 1 entries'. At the bottom right, there is a pagination control showing '1' between left and right arrows.

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.

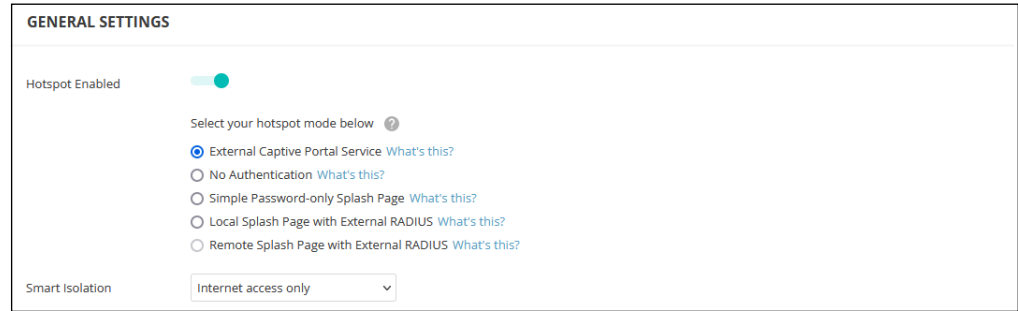
Hotspot Settings

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 117.](#))

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 73](#)). The hotspot will be redirected to an external splash page and authenticate with an external RADIUS server.

- **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

NETWORK SETTINGS			
IP Address	<input type="text" value="192.168.182.1"/>	DNS 1	<input type="text" value="192.168.182.1"/>
Netmask	<input type="text" value="255.255.255.0"/>	DNS 2	<input type="text"/>
DHCP Gateway	<input type="text"/>	DNS Domain Name	<input type="text"/>
DHCP Gateway Port	<input type="text"/>	DNS Entries	<input type="text"/> ?
		DNS Mapping	<div style="border: 1px solid #ccc; height: 80px;"></div>

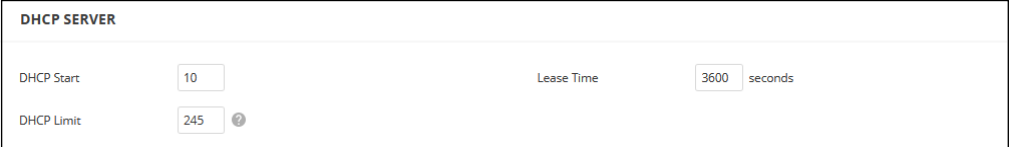
The following items are displayed on this page section:

- **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.
- **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 screenshot shows the 'DHCP SERVER' configuration page. It contains three input fields: 'DHCP Start' with the value '10', 'DHCP Limit' with the value '245' and a help icon, and 'Lease Time' with the value '3600' and the unit 'seconds'.

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)

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:

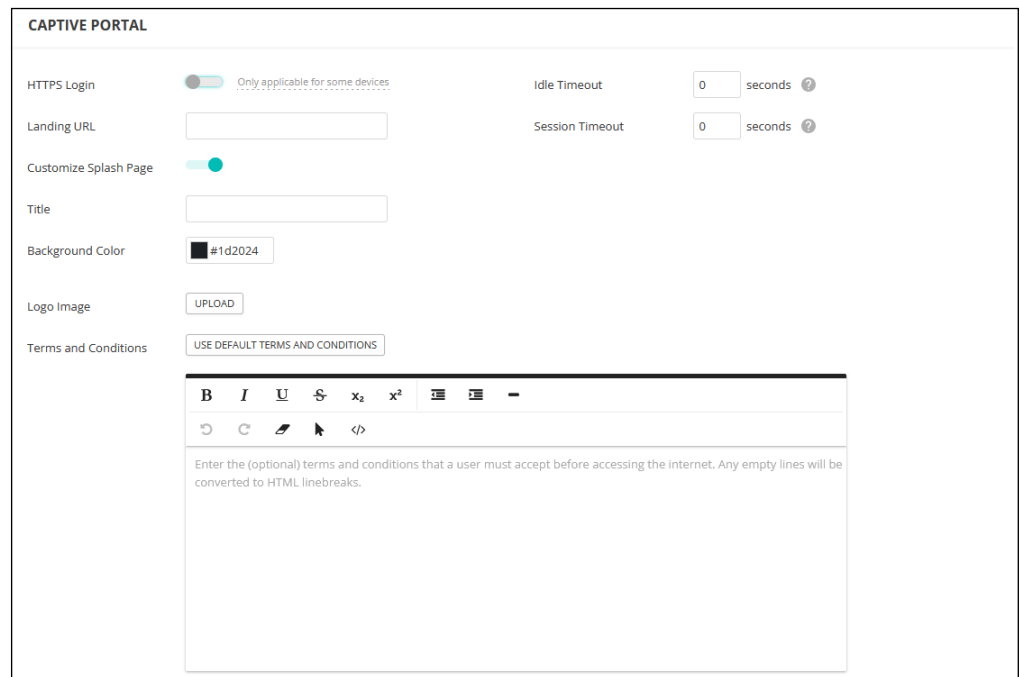
- **Enable RADIUS Auth** — Enables RADIUS authentication for clients attempting to access the captive portal.
- **RADIUS Server Address** — IP address or host name of the primary RADIUS server.
- **Backup RADIUS server address** — IP address or host name of the secondary RADIUS server.
- **RADIUS server 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)

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

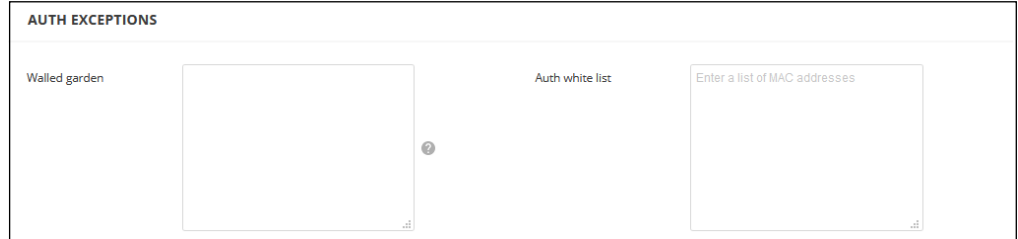
- **Captive portal URL** — Host name of Internet service portal for the hotspot.
- **Captive portal secret** — The password used for logging into the hotspot.
- **Swap Octets** — Swap the values of the reported “input octets” and “output octets.”

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 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.

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)

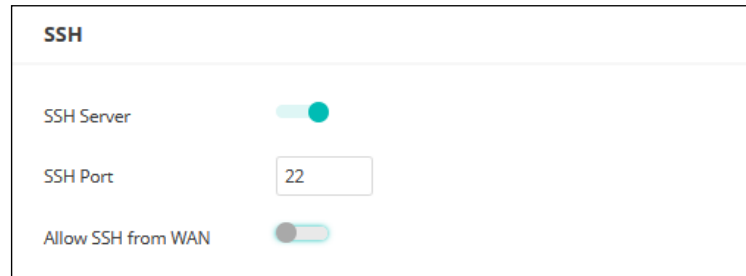
With MSP mode enabled, service providers have the option of making specific wireless SSID settings available for user configuration by enabling the “Local Configurable” setting.

i **Note:** Do not enable MSP Mode and “Always follow cloud configuration” (page 64) 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

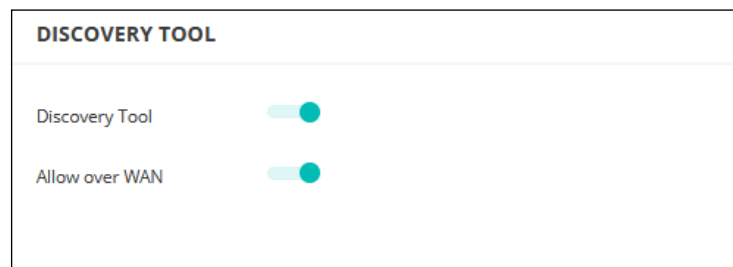


The following items are displayed on this page:

- **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

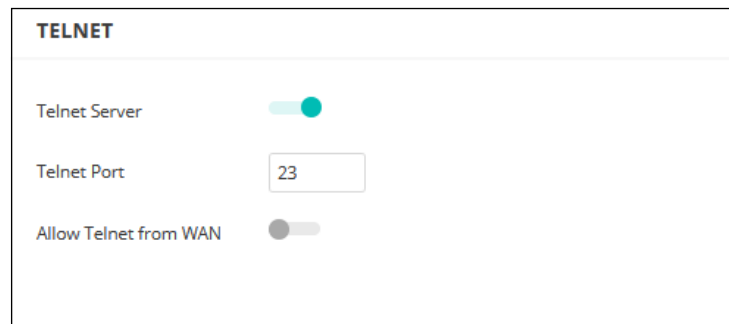


The following items are displayed on this page:

- **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.

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

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



SNMP	
SNMP Server	<input checked="" type="checkbox"/>
Contact	<input type="text" value="www.ignitenet.com"/>
Community String	<input type="text" value="public"/>
IPv6 Write Community	<input type="text" value="private6"/>
Location	<input type="text"/>
Allow SNMP over WAN	<input checked="" type="checkbox"/>

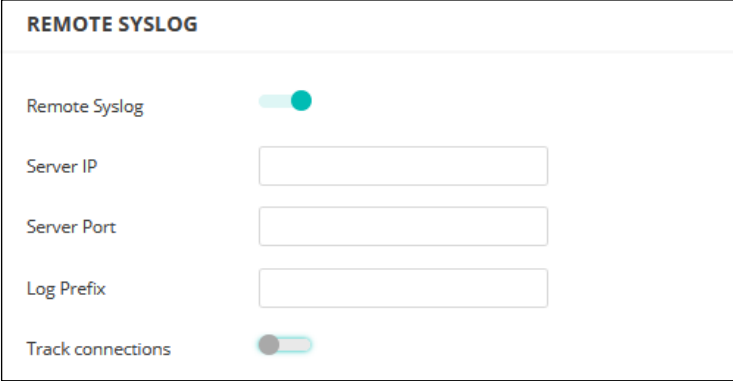
The following items are displayed on this page:

- **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)

- **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 screenshot shows a configuration page titled "REMOTE SYSLOG". It features five settings:

- Remote Syslog**: A toggle switch that is currently turned on (green).
- Server IP**: An empty text input field.
- Server Port**: An empty text input field.
- Log Prefix**: An empty text input field.
- Track connections**: A toggle switch that is currently turned off (grey).

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.

Ping Watchdog Use this feature to send ping probe packets to a defined IP address to confirm connectivity.

Figure 161: Ping Watchdog Settings

PING WATCHDOG	
Ping Watchdog	<input checked="" type="checkbox"/>
IP Address	<input type="text" value="192.168.2.1"/>
Failover IP Address	<input type="text" value="192.168.10.1"/> ?
Interval (min)	<input type="text" value="1"/> ?
Failure count	<input type="text" value="5"/> ?

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

BLE SETTINGS ?	
BLE Probe Req. Data Push	<input checked="" type="checkbox"/>
Push URL	<input type="text"/>

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)

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 screenshot shows the LLDP configuration page. At the top, the title "LLDP" is displayed. Below it, there are three settings: "Enable" with a toggle switch turned on (green), "Tx Interval (seconds)" with a text input field containing "30", and "Tx Hold (number of time(s))" with a text input field containing "4".

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



The screenshot shows the iBeacon configuration page. At the top, the title "IBEACON" is displayed. Below it, there are five settings: "Enable" with a toggle switch turned on (green), "UUID" with five text input fields containing "e2c56db5", "dffb", "48d2", "b060", and "d0f5a71096e0", "Major" with a text input field containing "21395", "Minor" with a text input field containing "100", and "Tx Power" with a slider set to 5 and a dropdown menu showing "5 dbm".

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

SNMP V3 USER							+ ADD
<input type="checkbox"/>	NAME	ACCESS AUTH	AUTH TYPE	AUTH PWD	ENCRYPTION TYPE	ENCRYPTION PWD	
<input type="checkbox"/>		Write	MD5		DES		DELETE

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.

5

Site WiFi 6 Configuration

This chapter describes configuration settings for WiFi 6 access point devices. It includes the following sections:

- [“Wireless SSID Configuration” on page 159](#)
- [“Radio Settings” on page 171](#)
- [“General Networking Settings” on page 175](#)
- [“Local Network Settings” on page 182](#)
- [“Firewall Settings” on page 184](#)
- [“Hotspot Settings” on page 187](#)
- [“System Settings” on page 194](#)
- [“OpenRoaming” on page 203](#)

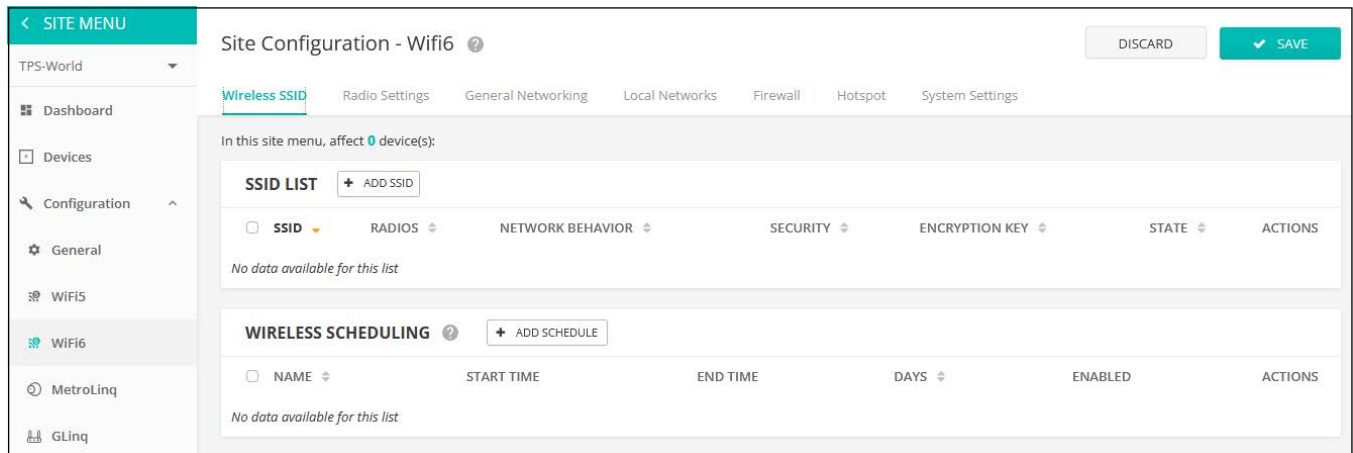
Wireless SSID Configuration

From the Site menu, open “Configuration” and then “WiFi6” 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.

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 screenshot shows the 'Add SSID' configuration page with three main sections: General Settings, Security Settings, and Network Settings. The General Settings section includes: Enable SSID (checked), SSID (text input), Broadcast SSID (checked), Client isolation (unchecked), Multicast-to-Unicast Conversion (checked), Max Client Count (127), Minimum allowed signal (-70 RSSI), and Activate on radio (5GHz and 2.4GHz checked). The Security Settings section includes: Method (Open), OWE (unchecked), RADIUS MAC Auth (unchecked), Access Control List (unchecked), 802.11k (unchecked), and 802.11v (unchecked). The Network Settings section includes: Network behavior (Route to Internet), Route through (Default Local Network), Limit upload rate (unchecked), Limit download rate (unchecked), OpenRoaming (checked), and Choose Profile (Select profile --). Buttons for CANCEL and CONFIRM are at the top right.

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)

- **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)

- **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.

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.

- **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.

- **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

communications between the AP and each client, but does not provide authentication of user identities.

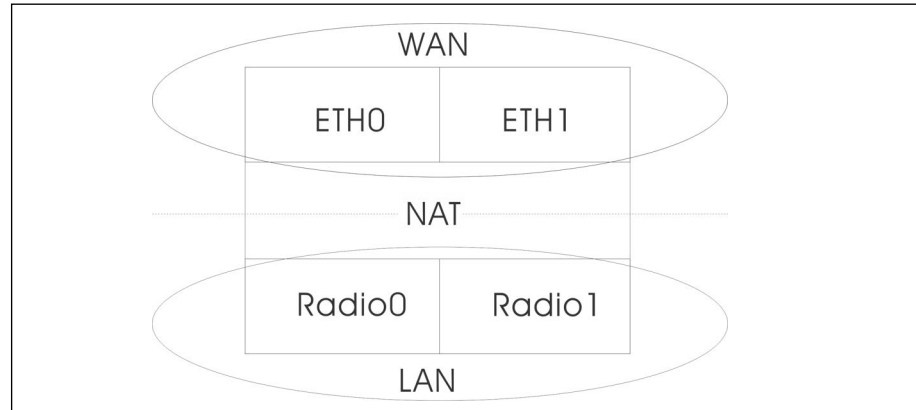
- **Access Control List** — Wireless clients can be authenticated for network access by checking their MAC address against the local database configured on the access point. (Default: OFF)
 - **Policy** — The MAC list can be configured to either allow or deny network access to specified clients. (Default: 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.

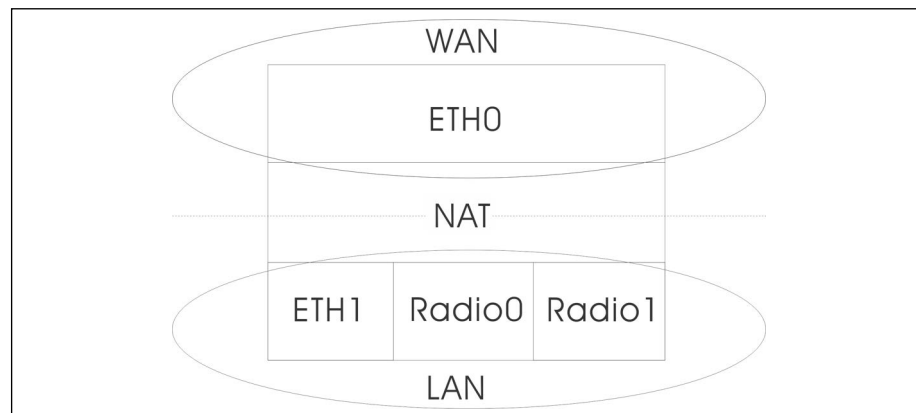
Figure 170: Bridge to Internet



- **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).

- **VLAN Tag Traffic** — Tags any packets passing from this SSID interface to the associated Ethernet port as configured under “[VLAN Settings](#)” on [page 180](#). 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. An 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 203](#) 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 73](#)).

Figure 172: Enabling Microsoft 365 Authentication

The screenshot shows the 'Add SSID' configuration interface. At the top right, there are 'CANCEL' and 'CONFIRM' buttons. The main section is titled 'Network Settings' and contains the following fields:

- Network behavior:** A dropdown menu set to 'VLAN tag traffic' with a help icon.
- VLAN ID:** A dropdown menu set to 'Please select VLAN' with a 'CONFIGURE VLANS' button.
- Limit upload rate:** A toggle switch that is turned off.
- Limit download rate:** A toggle switch that is turned off.
- AuthPort Enable:** A toggle switch that is turned on.
- Captive Portal:** A dropdown menu set to 'custom'.
- Microsoft 365 Authentication:** A toggle switch that is turned on.
- Microsoft 365 Default Plan:** A dropdown menu set to 'Test' with an 'ADD NEW PLAN' button.
- Microsoft 365 Authentication URL:** An empty text input field.
- Microsoft 365 Token:** An empty text input field.
- Microsoft 365 Client ID:** An empty text input field.
- Microsoft 365 Permission:** An empty text input field.
- Microsoft 365 Client Secret:** An empty text input field.
- Microsoft 365 Walled Garden:** A large empty text area.

- **Captive Portal** — Choose a captive portal that includes the Microsoft login button (see [“Captive Portal”](#) on page 79).
- **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.

- **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 screenshot shows the 'Add schedule' configuration page. At the top right are 'CANCEL' and 'CONFIRM' buttons. The main content area is titled 'Schedule Settings'. A message indicates the site's timezone is set to UTC. Below this, there is a toggle for 'Enabled' which is turned on. There is a text input field for 'Name'. The 'Start time' is set to 12:00 am, and the 'End time' is set to 06:00 am. The 'Days' section shows 'Mon' selected, with 'Tue', 'Wed', 'Thur', 'Fri', 'Sat', and 'Sun' unselected.

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 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

GLOBAL SETTINGS

Band Steering

Airtime Fairness ?

RF Isolation ?

WIRELESS 5 GHZ

<p>PHYSICAL RADIO SETTINGS</p> <p>802.11 Mode: 802.11ax</p> <p>Channel Bandwidth: 80MHz</p> <p>Channel: Auto (all channels) EDIT CHANNEL LIST</p> <p>Idle Timeout: 300</p> <p>Max Tx Power: <input type="range" value="20"/> 20 dBm (100 mW) ?</p> <p>Beacon Interval: 100 ?</p> <p>BSS Coloring: 64 ?</p> <p>Interference Detection: 0 ?</p> <p>Broadcast Rate: 6M</p> <p>Target Wake Time: <input type="checkbox"/></p> <p>OFDMA: <input checked="" type="checkbox"/></p>	<p>ADVANCED RADIO SETTINGS</p> <p>Probe Req. Data Push: <input type="checkbox"/> ?</p>
--	---

WIRELESS 2.4 GHZ

<p>PHYSICAL RADIO SETTINGS</p> <p>802.11 Mode: 802.11ax</p> <p>Channel Bandwidth: 40MHz</p> <p>Channel: Auto (all channels) EDIT CHANNEL LIST</p> <p>Idle Timeout: 300</p> <p>Max Tx Power: <input type="range" value="22"/> 22 dBm (158 mW) ?</p> <p>Beacon Interval: 100 ?</p> <p>BSS Coloring: 64 ?</p> <p>Interference Detection: 0 ?</p> <p>Broadcast Rate: 5.5M</p> <p>Target Wake Time: <input type="checkbox"/></p> <p>OFDMA: <input checked="" type="checkbox"/></p>	<p>ADVANCED RADIO SETTINGS</p> <p>Probe Req. Data Push: <input type="checkbox"/> ?</p>
--	---

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
 - **Radio 5 GHz** — Default: 11ax; Options: 11a, 11a+n, 11ac+a+n, 11ax
 - **Radio 2.4 GHz** — Default: 11ax; Options: 11ax
- **Channel Bandwidth** — The basic Wi-Fi channel bandwidth is 20 MHz, but by bonding channels together to create 40 MHz, 80 MHz, or 160 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 6 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 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
- **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

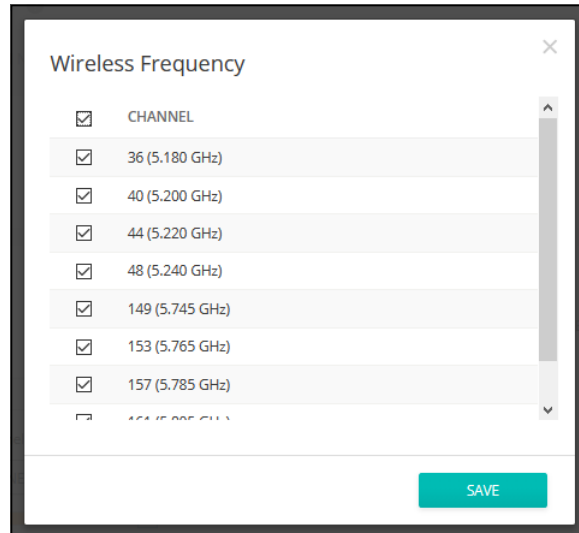
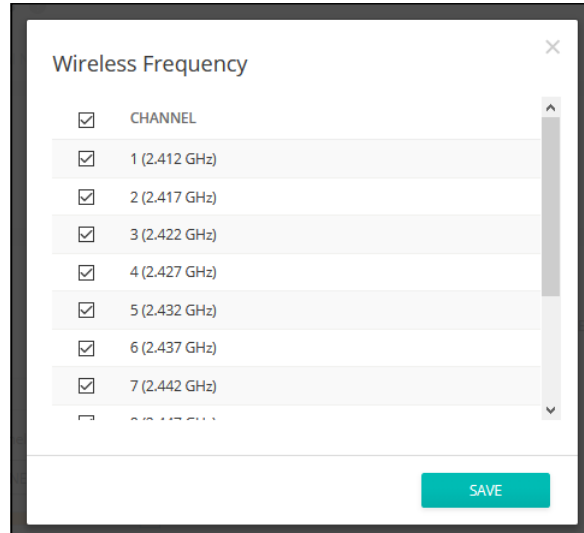


Figure 176: 2.4 GHz Radio Channels



- **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 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.

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

INTERNET

Only the Internet IP Address Mode and Mgmt VLAN settings can be changed here. The rest of these settings can only be overridden on a per-device basis at device-level config.

GENERAL SETTINGS	MGMT VLAN
Internet Source: WAN Port	Mgmt VLAN: <input checked="" type="checkbox"/> ?
VLAN tag traffic: <input type="checkbox"/>	
IP Address Mode: DHCP ?	
MTU Size: 1500	
Fallback IP: 192.168.1.20	
Fallback Netmask: 255.255.255.0	

DHCP RELAY

DHCP Relay:

DHCP Relay Server:

DHCP Relay Port: 67

Backup DHCP Relay:

Remote ID: Hostname

IPV6 SETTINGS

IP Address Mode: DHCP

Client ID:

ETHERNET

Some settings can only be overridden on a per-device basis at device-level config.

ETHERNET SETTINGS FOR WAN PORT	ETHERNET SETTINGS FOR LAN PORT(S)
This port is the internet source for this device.	Network behavior: Bridge to Internet ?

ADVANCED ETHERNET SETTINGS

PoE Out:

VLAN + ADD NEW VLAN

VLAN ID	TAGGED PORTS	UNTAGGED INTERFACES	ACTIONS
No data available for this list			

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

INTERNET

Only the Internet IP Address Mode and Mgmt VLAN settings can be changed here. The rest of these settings can only be overridden on a per-device basis at device-level config.

GENERAL SETTINGS	MGMT VLAN
Internet Source: WAN Port	Mgmt VLAN: <input checked="" type="checkbox"/>
VLAN tag traffic: <input type="checkbox"/>	
IP Address Mode: DHCP	
MTU Size: 1500	
Fallback IP: 192.168.1.20	
Fallback Netmask: 255.255.255.0	

DHCP RELAY

DHCP Relay:

DHCP Relay Server:

DHCP Relay Port: 67

Backup DHCP Relay:

Remote ID: Hostname

IPV6 SETTINGS

IP Address Mode: DHCP

Client ID:

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.

MGMT VLAN Settings

Figure 179: Management VLAN Settings

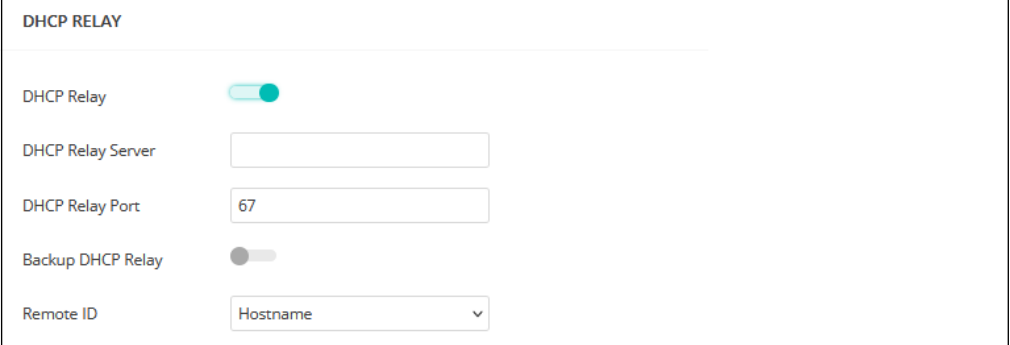
MGMT VLAN	
Mgmt VLAN	<input checked="" type="checkbox"/>
Mgmt VLAN ID	100
IP Address Mode	DHCP
Fallback IP	192.168.1.20
Fallback Netmask	255.255.255.0

- **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.

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 screenshot shows the DHCP Relay configuration page. It features a title 'DHCP RELAY' at the top. Below the title, there are five settings: 'DHCP Relay' is a toggle switch that is turned on (green); 'DHCP Relay Server' is an empty text input field; 'DHCP Relay Port' is a text input field containing the number '67'; 'Backup DHCP Relay' is a toggle switch that is turned off (grey); and 'Remote ID' is a dropdown menu currently set to 'Hostname'.

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 screenshot shows the IPv6 Settings configuration page. It features a title 'IPv6 SETTINGS' at the top. Below the title, there are two settings: 'IP Address Mode' is a dropdown menu currently set to 'DHCP'; and 'Client ID' is an empty text input field.

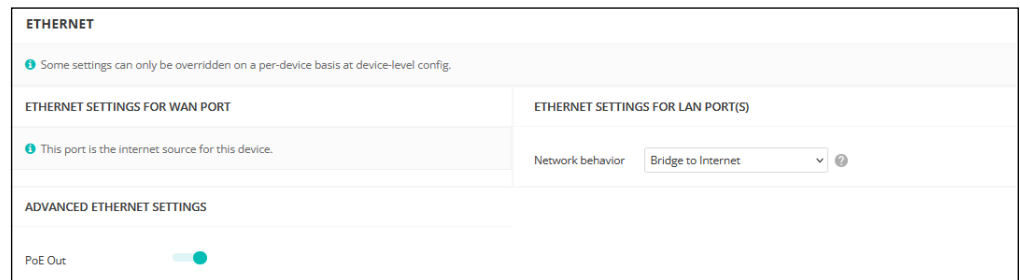
The following items are displayed on this section of the page:

- **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 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).

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 160).

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:

- **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 160).
- **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 screenshot shows a web interface for adding a new VLAN. At the top right, there are two buttons: 'CANCEL' and 'CONFIRM'. Below the title 'Add New VLAN', there is a section titled 'General Settings' with an expandable arrow. Under 'General Settings', there are two main fields: 'VLAN ID' and 'Ports'. The 'VLAN ID' field is a text input box. The 'Ports' section contains two radio button options: 'WAN Port' and 'LAN Port(s)', both of which are currently unselected.

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).

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 screenshot displays the 'Local Network Settings' interface. At the top, there is a 'LAN' tab and a '+ ADD CUSTOM LAN' button. Below this, the 'DEFAULT LOCAL NETWORK' section is active, indicated by a 'BUILT-IN' label and a green toggle switch. This section contains two columns of settings. The left column includes: IP Address (192.168.2.1), Subnet Mask (255.255.255.0), MTU Size (1500), Enable STP (disabled), Enable UPnP (disabled), and Smart Isolation (Disable (full access)). The right column includes: DHCP Server (enabled), DHCP Start (100), DHCP Limit (150), Lease Time (12hr), and DNS Servers (DHCP Option 6) with a text input field. Below this, the 'GUEST NETWORK' section is also active, with a 'BUILT-IN' label and a green toggle switch. It features identical settings to the Default Local Network, but with an IP Address of 192.168.3.1.

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)

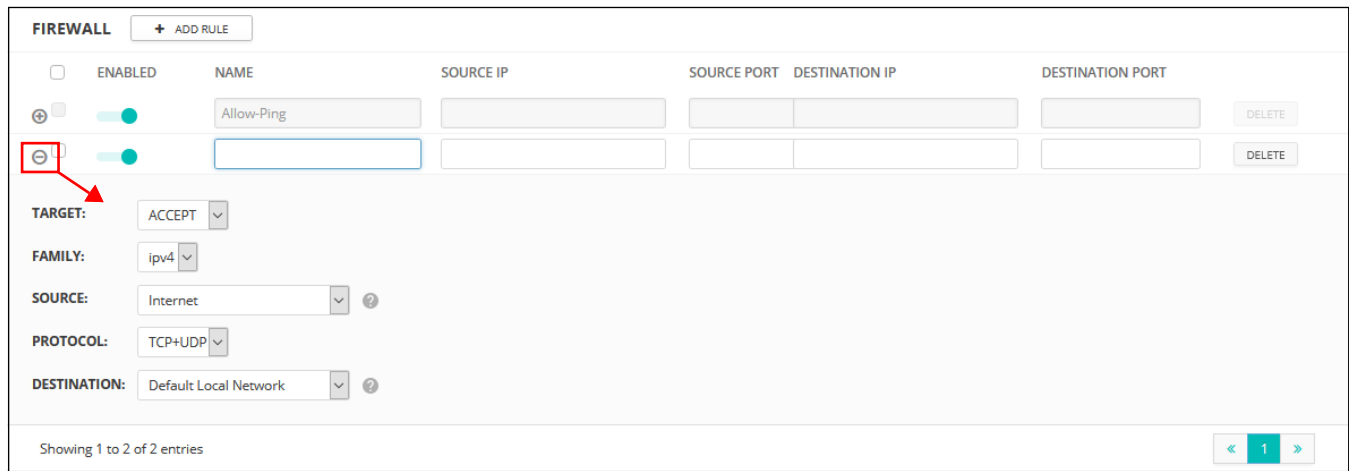
- **Enable UPnP** — Enables or disables Universal Plug-and-Play broadcast messages. (Default: Disabled)
- **Smart Isolation** — Enables network traffic to be restricted to the specified network:
 - **Disable (full access)** — There is no traffic isolation. Clients can access the Internet and other devices 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.

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)

- **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 screenshot displays the 'PORT FORWARDING' configuration page. At the top left, there is a header 'PORT FORWARDING' and a '+ ADD RULE' button. Below this, there is a section for 'ENABLED' with a checked checkbox. The main area contains a table with the following columns: NAME, PROTOCOL, EXTERNAL PORT, DESTINATION IP, and DESTINATION PORT. A single rule is listed with a protocol dropdown set to 'TCP+UDP' and a 'DELETE' button to its right. At the bottom left, it says 'Showing 1 to 1 of 1 entries'. At the bottom right, there is a pagination control showing '1' between left and right arrow buttons.

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)

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



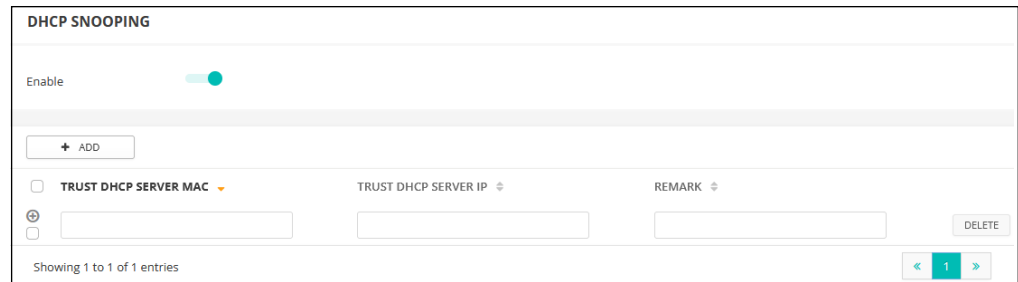
The following items are displayed on this page:

- **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.

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.

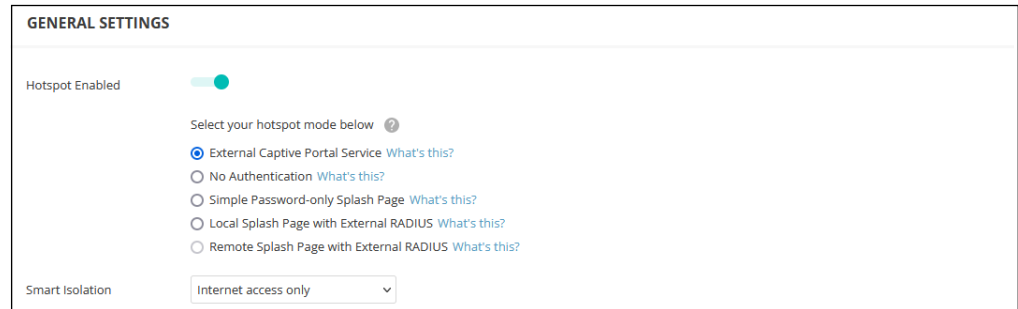
Hotspot Settings

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 159.)

General Settings The General Settings section on the Hotspot page configures the basic hotspot mode.

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 73](#)). The hotspot will be redirected to an external splash page and authenticate with an external RADIUS server.

- **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

NETWORK SETTINGS			
IP Address	192.168.182.1	DNS 1	192.168.182.1
Netmask	255.255.255.0	DNS 2	
DHCP Gateway		DNS Domain Name	
DHCP Gateway Port			

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.

- **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

DHCP SERVER			
DHCP Start	<input type="text" value="10"/>	Lease Time	<input type="text" value="3600"/> seconds
DHCP Limit	<input type="text" value="245"/> ⓘ		

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

RADIUS SERVER			
Enable RADIUS Auth	<input checked="" type="checkbox"/>	Enable RadSec	<input type="checkbox"/>
RADIUS Server Address	<input type="text" value="127.0.0.1"/>	Auth method	<input type="text" value="CHAP"/>
Backup RADIUS server address	<input type="text" value="Enter RADIUS server IP address"/>	Local ID	<input type="text" value="0"/>
RADIUS server shared secret	<input type="password" value="••••••"/> ⓘ	Local name	<input type="text"/>
RADIUS server auth port	<input type="text" value="1812"/>	Generate NAS ID	<input type="checkbox"/> ⓘ
RADIUS server acct port	<input type="text" value="1813"/>	NAS ID	<input type="text"/>

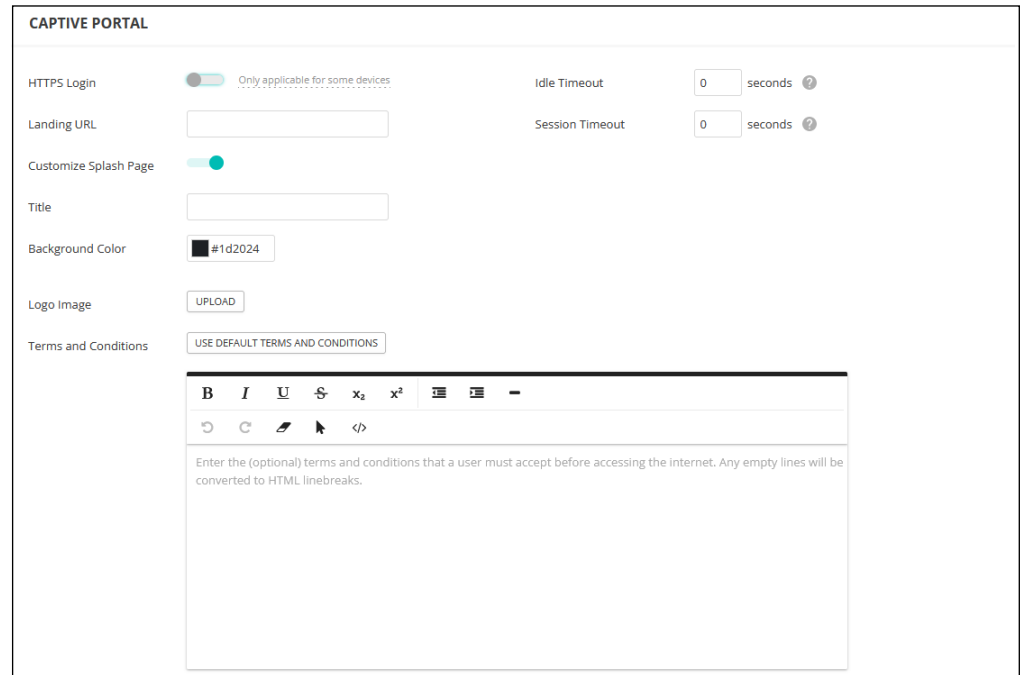
The following items are displayed on this page section:

- **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 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)

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

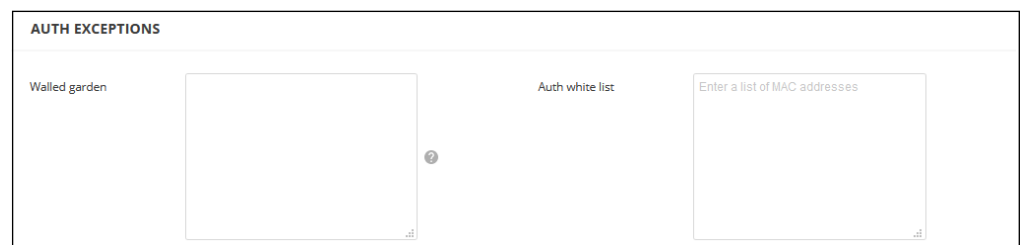
- **Captive portal URL** — Host name of Internet service portal for the hotspot.
- **Captive portal secret** — The password used for logging into the hotspot.
- **Swap Octets** — Swap the values of the reported “input octets” and “output octets.”

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



The following items are displayed on this page section:

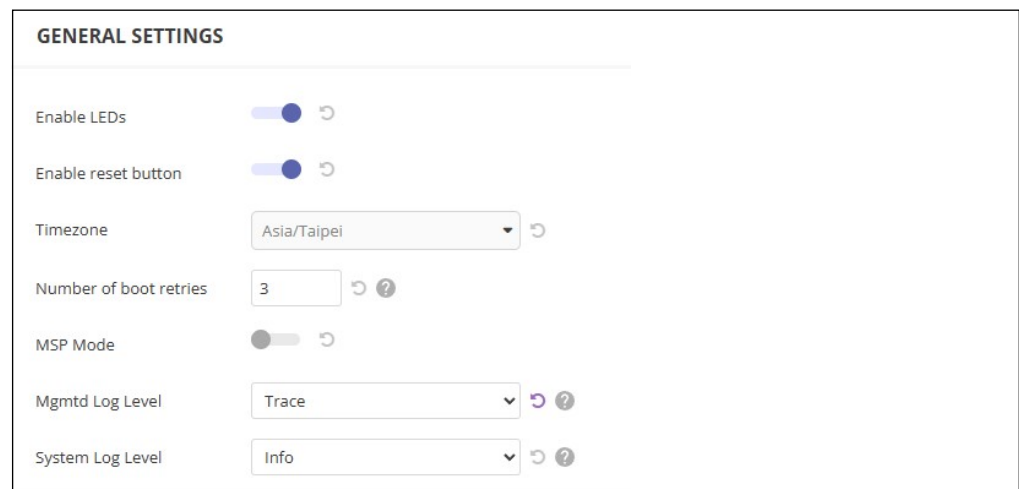
- **Walled garden** — Enter a list of domains or IP addresses in CIDR notation that hotspot users can access before being authenticated by the captive portal. Wildcard domains can be specified in the format of *domain.com* (allow domain and all sub-domains), or *.domain.com* (only allow sub-domains).
- **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.
- **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 64) at the same time. This will cause the device configuration not to be updated to ecCLOUD properly.

- **Mgmt 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:

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

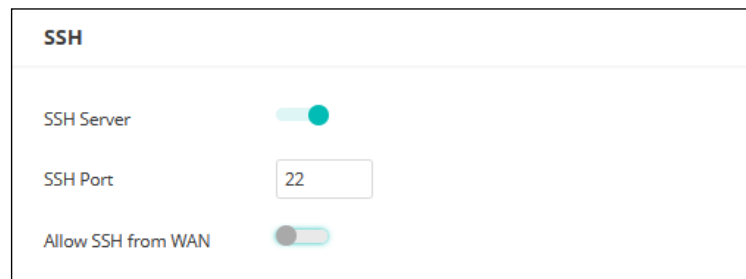
Table 2: System Logging Levels (Continued)

Level	Severity Name	Description
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.

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



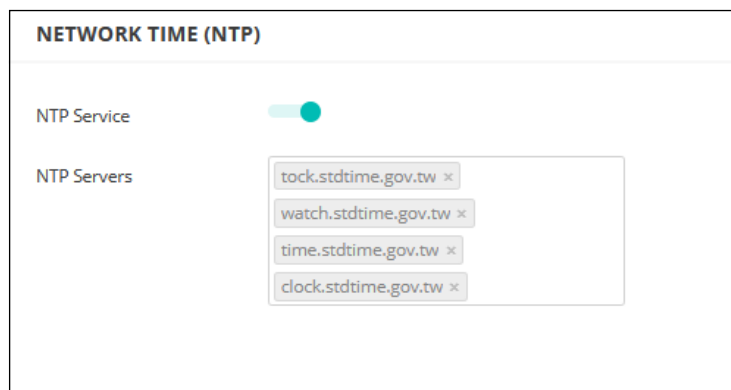
The following items are displayed on this page:

- **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

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

SNMP	
SNMP Server	<input checked="" type="checkbox"/>
Write Community	<input type="text" value="public"/>
IPv6 Write Community	<input type="text" value="private6"/>
Read Community	<input type="text" value="ecpublic"/>
IPv6 Read Community	<input type="text" value="public6"/>
Trap	<input checked="" type="checkbox"/>
Server IP	<input type="text"/>

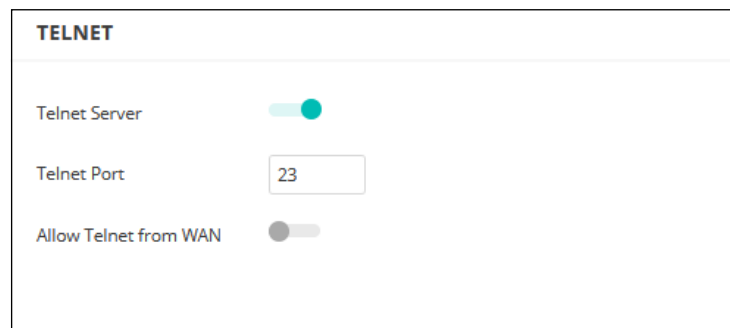
The following items are displayed on this page:

- **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)

- **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.

Figure 202: Web Server Settings

WEB SERVER	
HTTP Port	<input type="text" value="80"/>
Allow HTTP from WAN	<input checked="" type="checkbox"/>
HTTPS Port	<input type="text" value="443"/>
Allow HTTPS from WAN	<input checked="" type="checkbox"/>

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

REMOTE SYSLOG	
Remote Syslog	<input checked="" type="checkbox"/>
Server IP	<input type="text"/>
Server Port	<input type="text"/>
Log Prefix	<input type="text"/>
Track connections	<input type="checkbox"/>

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.

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)

- **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 screenshot shows the 'IBEACON' settings page. At the top, there is a title 'IBEACON' with a help icon. Below the title, there are five settings:

- Enable:** A toggle switch that is currently turned on (green).
- UUID:** A text input field containing the value 'e2c56db5 - dffb - 48d2 - b060 - d0f5a71096e0'.
- Major:** A text input field containing the value '21395'.
- Minor:** A text input field containing the value '100'.
- Tx Power:** A dropdown menu with '5 dbm' selected.

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)
- **Tx Power** — Sets the BLE radio transmit power (supported only on EAP101 and EAP104). (Range: 5 dBm to -20 dBm; Default: 5 dBm)

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

SNMP V3 USER	+	ADD					
<input type="checkbox"/>	NAME	ACCESS AUTH	AUTH TYPE	AUTH PWD	ENCRYPTION TYPE	ENCRYPTION PWD	
<input type="checkbox"/>		Write	MD5		DES		DELETE

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.

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 160](#)). Click “Add Custom Openroaming” to configure a profile.

Figure 208: OpenRoaming Profile

OPENROAMING ? + ADD CUSTOM OPENROAMING

TEST1

Internet Access

Access Network Type Private network: Home and Enterprise

HESSID ff:ff:ff:ff:ff:ff

Venue Group Unspecified

Venue Type Unspecified

Network Auth Type Acceptance of terms and conditions

IPv4 Address Type Address type not available

IPv6 Address Type Address type not available

Operating Class 5173

VENUE NAME INFORMATION + ADD RULE

NAI REALM LIST + ADD RULE

OPERATOR FRIENDLY NAME + ADD RULE

CELLULAR NETWORK INFORMATION LIST(PLMN) + ADD RULE

DOMAIN NAME LIST + ADD RULE

ROAMING CONSORTIUM LIST + ADD RULE

RENAME DELETE

The following items are displayed on this page:

- **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”)
- **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.
- **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.

6

Site Terragraph Configuration

This chapter describes configuration settings for MetroIQ Terragraph units at the Site level. It includes the following sections:

- [“MetroIQ Terragraph Configuration” on page 209](#)
- [“VLAN Settings” on page 212](#)

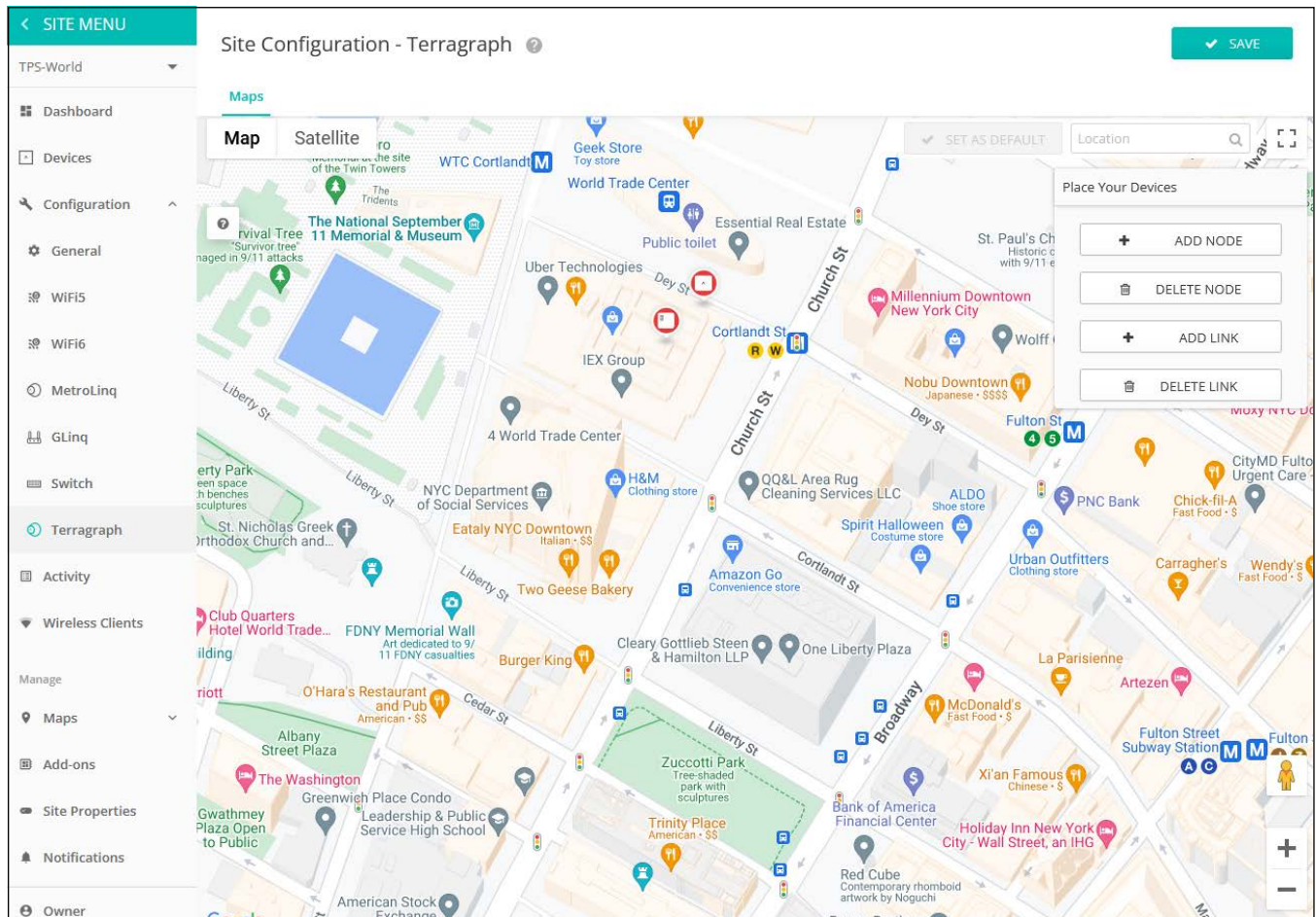
MetroInq Terragraph Configuration

The network connectivity and topology for MetroInq 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 MetroInq 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.

- **Add Link** — Select two nodes and corresponding radio MACs to establish a link.

Figure 212: Add Terragraph Link

The screenshot shows a configuration window titled "Add Link". At the top right are "CANCEL" and "CONFIRM" buttons. The main area is titled "Add Link" and contains the following fields:

- Node A:** A dropdown menu with a red border and a red error message below it: "Link can't be added."
- MAC A:** A dropdown menu.
- Node B:** A dropdown menu with a red border and a red error message below it: "Link can't be added."
- MAC B:** A dropdown menu.
- Channel:** A dropdown menu with the value "1" selected.

- **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

The screenshot shows a configuration window titled "Delete Link". At the top right are "CANCEL" and "CONFIRM" buttons. The main area is titled "Delete Link" and contains the following fields:

- Node A:** A dropdown menu with a red border and a red error message below it: "Link can't be deleted."
- MAC A:** A dropdown menu.
- Node B:** A dropdown menu.
- MAC B:** A dropdown menu.

- **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.

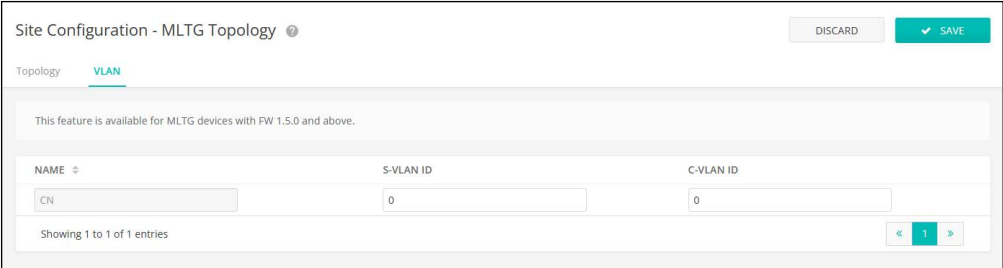
VLAN Settings

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



Site Configuration - MLTG Topology

DISCARD SAVE

Topology **VLAN**

This feature is available for MLTG devices with FW 1.5.0 and above.

NAME	S-VLAN ID	C-VLAN ID
CN	0	0

Showing 1 to 1 of 1 entries

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.

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 215](#)

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.

Figure 215: Add New VPN Group

The screenshot shows the 'Add VPN Group' configuration window. At the top right are 'CANCEL' and 'CONFIRM' buttons. The window is split into two sections. The top section, 'General Settings', contains: 'Name' (text input), 'Subnet IP' (text input), 'Subnet Mask' (dropdown menu showing '255.255.255.0 (/24)'), 'Protocol' (dropdown menu showing 'TCP'), 'Port' (text input showing '1194'), and 'Autonomous Data Tunnel' (toggle switch). The bottom section, 'VPN Group Devices', contains: 'VPN Device List' (empty table with '+' and '-' buttons), 'Group Devices' (dropdown menu showing 'Please select...'), 'SN' (text input), 'Role' (dropdown menu showing 'Hub'), 'WAN1 VPN Service Type' (dropdown menu showing 'Customized'), 'WAN1 VPN Service IP' (text input), 'WAN2 VPN Service Type' (dropdown menu showing 'Customized'), and 'WAN2 VPN Service IP' (text input).

■ 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.

8

WiFi 5 Device Configuration

This chapter describes configuration settings for access points at the Device level. It includes the following sections:

- [“Accessing Device-Level Configuration” on page 218](#)
- [“Device Radio Settings” on page 220](#)

Accessing Device-Level Configuration

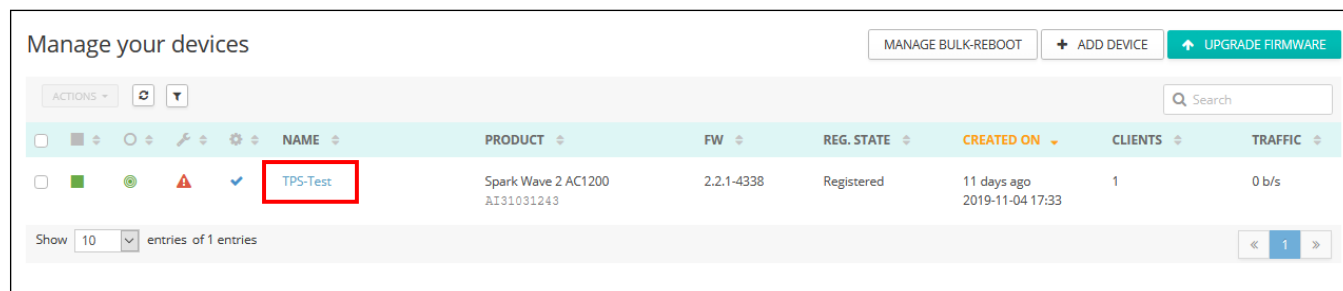
When a device’s “Inheritance Policy” is enabled, the device is configured from the Site level. However, a device can be individually configured at the Device level and the settings will override the Site-level configuration.

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

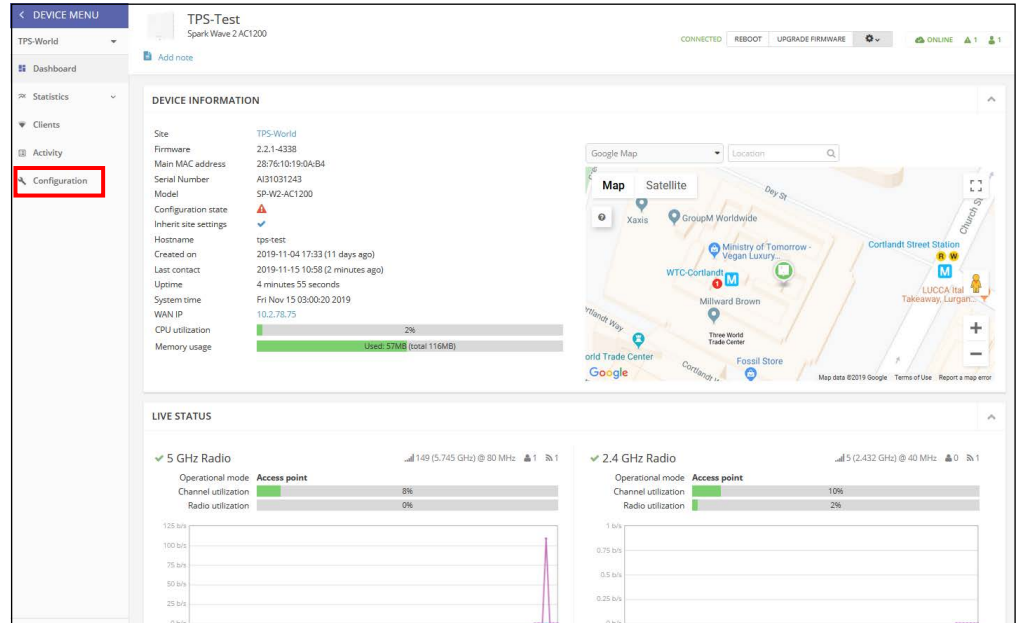


The screenshot shows a dashboard titled "Manage your devices" with several action buttons: "MANAGE BULK-REBOOT", "+ ADD DEVICE", and "UPGRADE FIRMWARE". Below the buttons is a search bar and a table of devices. The table has columns for NAME, PRODUCT, FW, REG. STATE, CREATED ON, CLIENTS, and TRAFFIC. The first row of data shows a device named "TPS-Test" with product "Spark Wave 2 AC1200", firmware "2.2.1-4338", and registration state "Registered". The device name "TPS-Test" is highlighted with a red box.

	NAME	PRODUCT	FW	REG. STATE	CREATED ON	CLIENTS	TRAFFIC
<input type="checkbox"/>	TPS-Test	Spark Wave 2 AC1200 AI31031243	2.2.1-4338	Registered	11 days ago 2019-11-04 17:33	1	0 b/s

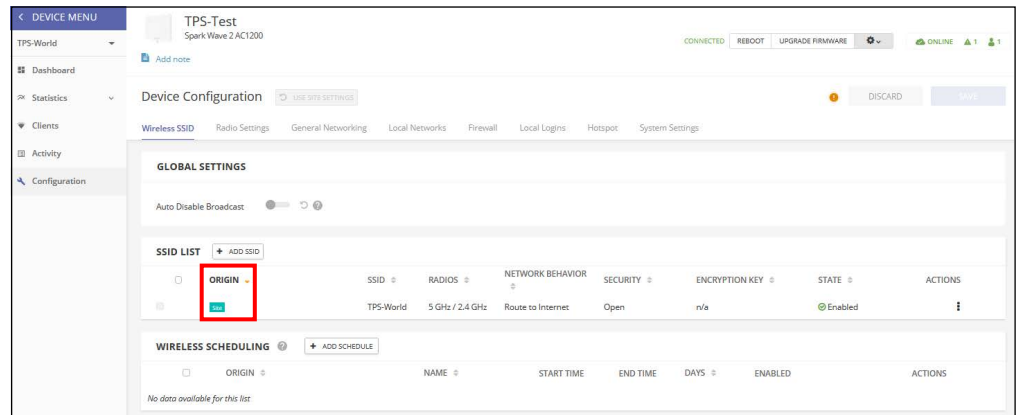
From the Device dashboard, click on “Configuration” on the Device menu to access a device’s configuration.

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 116.

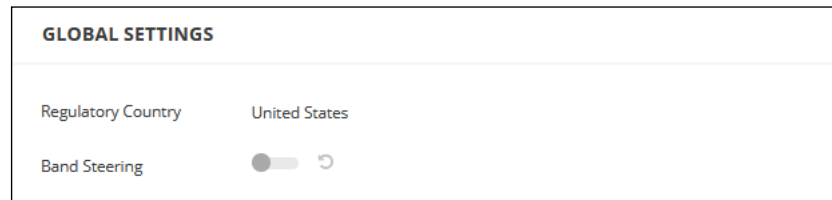
Device Radio Settings

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



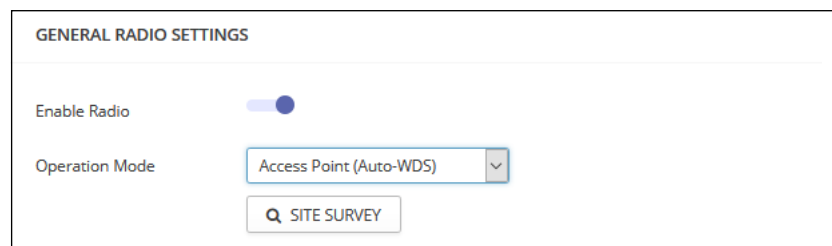
- **Regulatory Country** — The wireless device regulatory setting. This setting is displayed but not configurable at the Device level.

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



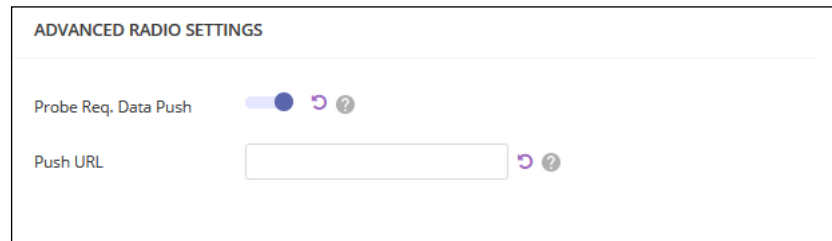
- **Enable Radio** — Enables or disables the wireless service on this interface.

- **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.

Physical Radio Settings

Figure 222: Device Physical Radio Settings

PHYSICAL RADIO SETTINGS

802.11 Mode	802.11ac+a+n	SGI	<input checked="" type="checkbox"/>
Channel Bandwidth	80MHz	STBC	<input type="checkbox"/>
Channel	Auto (all channels) EDIT CHANNEL LIST	DFS	<input checked="" type="checkbox"/>
Tx Power	22 dBm (158 mW)		
Fragmentation Thresh.	2346		
RTS Thresh.	2347		

- **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.

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

Figure 223: 5 GHz Radio Channels

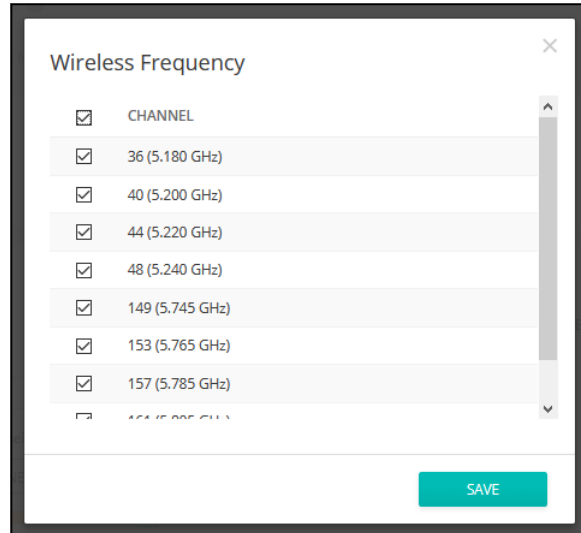
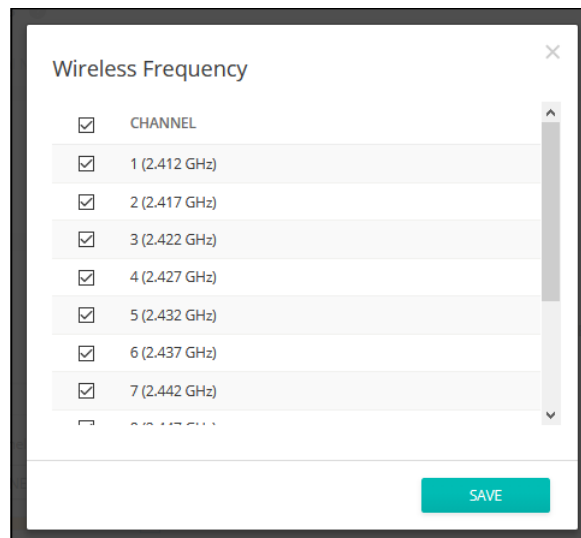


Figure 224: 2.4 GHz Radio Channels



- **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

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)

9

WiFi 6 Device Configuration

This chapter describes configuration settings for WiFi 6 access points at the Device level. It includes the following sections:

- [“Accessing Device-Level Configuration” on page 227](#)
- [“Device Radio Settings” on page 228](#)
- [“System Settings” on page 235](#)

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

	NAME	PRODUCT	FW	REG. STATE	CREATED ON	CLIENTS	TRAFFIC	IP	CHANNEL
	MA1F-AP4	AP101	11.6.3-1315 (1)	Registered	5 months ago	1	356 kb/s	120.105.6.75	149 (5.745 GHz)
		C2285002364	12.0.0-673 (2)		2022-05-05 14:25				6 (2.437 GHz)

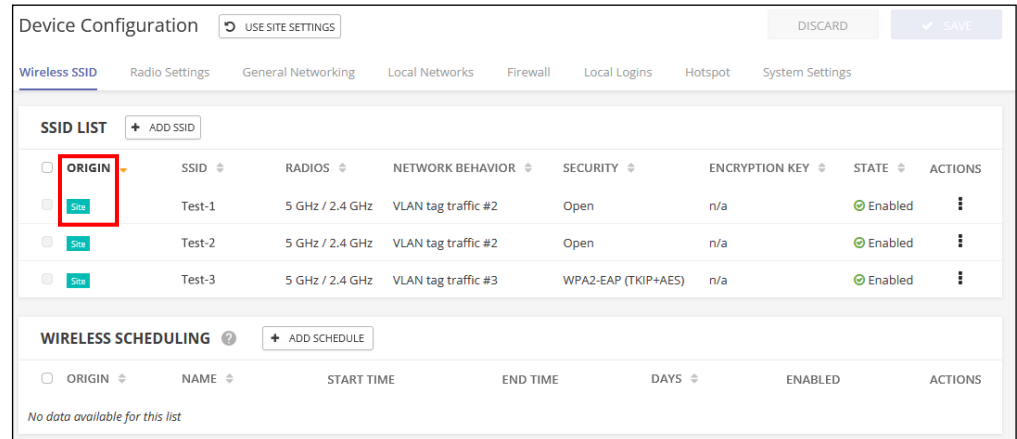
From the Device dashboard, click on “Configuration” on the Device menu to access a device’s configuration.

Figure 226: Device-Level Dashboard

DEVICE INFORMATION	
Site Sites	TPS-World
Firmware	12.0.0-673
Main MAC address	98:19:2C:F9:D5:30
Serial Number	EC2205002364
Model	EAP101
Configuration state	🟢
Inherit site settings	✓
Bootbank	2
Hostname	ma1fap4
Created on	2022-05-05 14:25 (5 months ago)
Last contact	2022-10-18 16:32 (2 minutes ago)
Uptime	32 Days 5 hours 30 minutes 54 seconds
System time	Tue Oct 18 16:34:11 2022
WAN IP	120.105.6.75
CPU utilization	4%
Memory usage	Used: 205MB (total 891MB)

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 158.

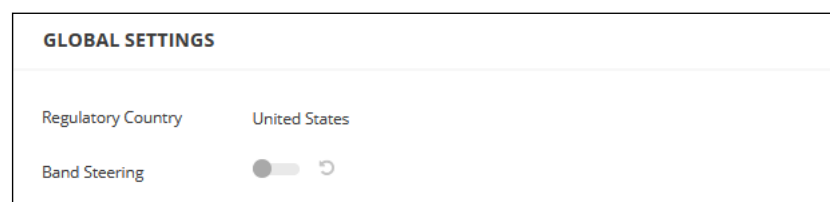
Device Radio Settings

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.

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

MESH SETTINGS	
Open Mesh	<input checked="" type="checkbox"/>
Mesh Id	<input type="text" value="openmesh"/>
Mesh Method	<input type="text" value="Open"/>
Network Behavior	<input type="text" value="Bridge to Internet"/>
Mesh Radio	<input type="text" value="5GHz"/>

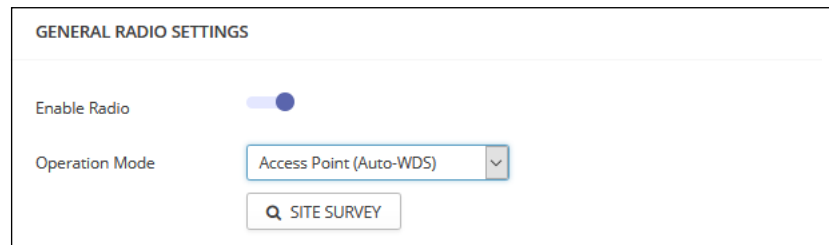
- **Open Mesh** — Enables Open Mesh support on the SSID interface.
- **Mesh ID** — Name of the mesh network.
- **Mesh Method** — Security applied on Open Mesh links.
 - **Open** — None.
 - **WPA3-Personal** — Uses WPA3 with Simultaneous Authentication of Equals (SAE) on mesh links to other APs.
- **Network 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 167.](#))
 - **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 171, “Route to Internet”](#), on page 167.)

- **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, or 6 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.

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.

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.
 - **6 GHz Radio** — Options: 802.11ax; Default: 802.11ax
 - **5 GHz Radio** — Options: 802.11a, 802.11a+n, 802.11ac+a+n, 802.11ax; Default: 802.11ax
 - **2.4 GHz Radio** — Options: 802.11ax; Default: 802.11ax

- **Channel Bandwidth** — The basic Wi-Fi channel bandwidth is 20 MHz, but by bonding channels together to create 40 MHz, 80 MHz, or 160 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 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 on EAP104 5 GHz radio, OAP101 5 GHz radio, and OAP101-6E 5 GHz and 6 GHz radios) For 802.11ac+a+n and 802.11ax
- **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

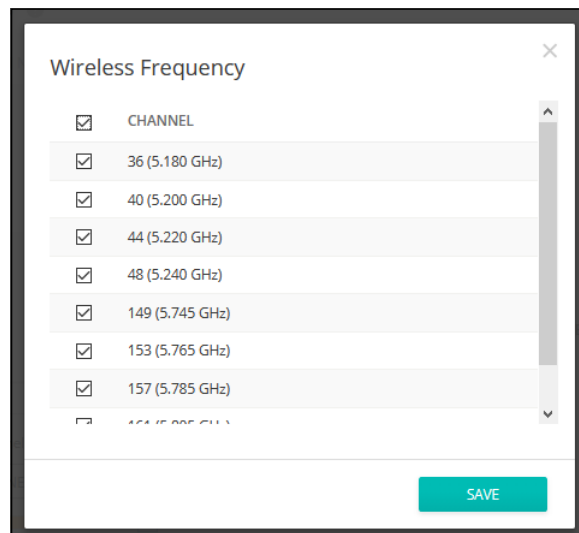
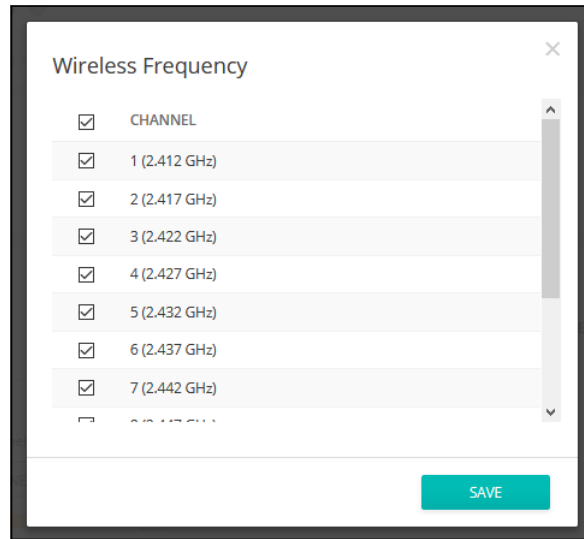


Figure 234: 2.4 GHz Radio Channels



- **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.

- **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.

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-UUID, 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)

- **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)

10

MetroLinq Device Configuration

This chapter describes configuration settings for MetroLinq units at the Device level. It includes the following sections:

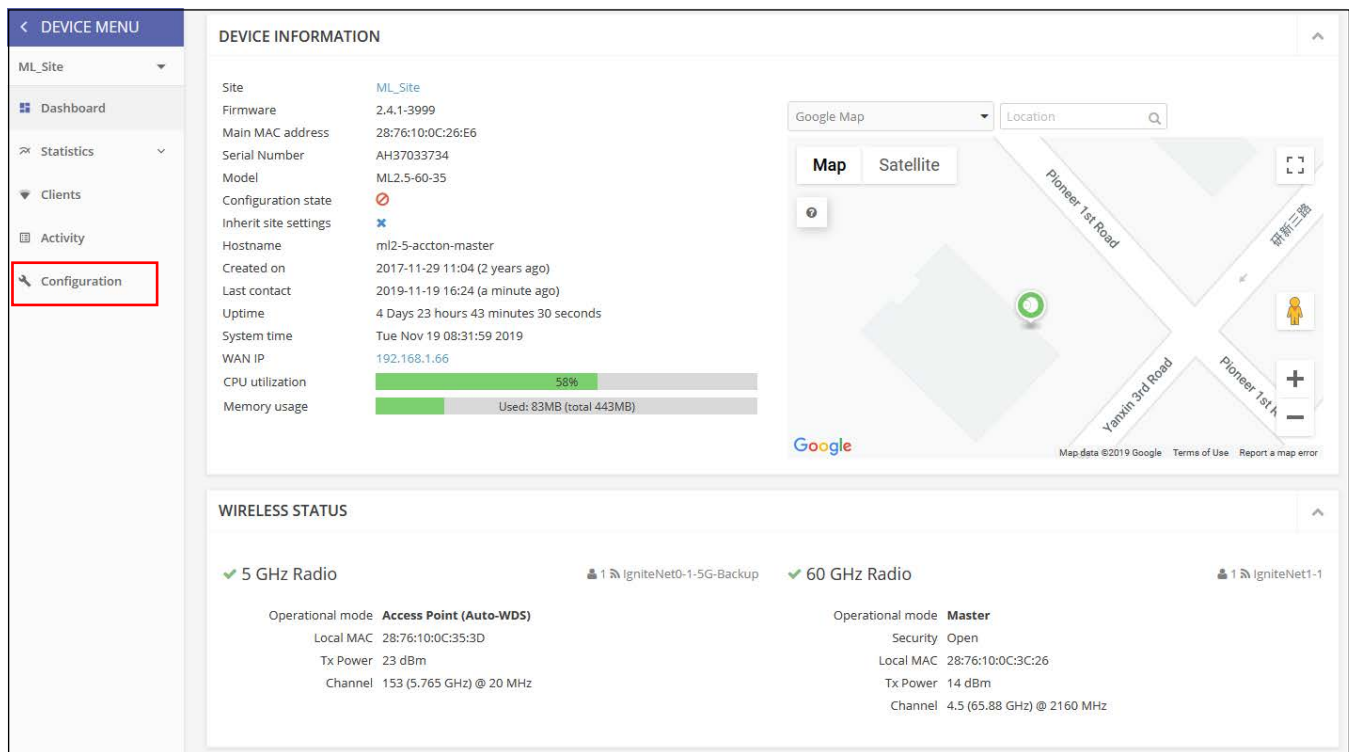
- [“MetroLinq Configuration” on page 238](#)
- [“Wireless SSID” on page 238](#)
- [“Radio Settings” on page 239](#)
- [“QoS Settings” on page 248](#)
- [“Traffic Control” on page 249](#)
- [“Using the LinqPath Tool” on page 250](#)

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 217.

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.

For details on configuring Wi-Fi access SSIDs, see [“Wireless SSID Configuration”](#) on page 117.

Figure 237: MetroLinq Device Dashboard

Attention The 5 GHz radio is in client mode. SSIDs on this radio will not be used.								
SSID LIST + ADD SSID								
<input type="checkbox"/>	ORIGIN	SSID	RADIOS	DATA VLAN	SECURITY	ENCRYPTION KEY	STATE	ACTIONS
<input type="checkbox"/>	Device	IgniteNet3-1 <small>60GHZ SSID</small>	60 GHz	n/a	Off	n/a	Enabled	
<input type="checkbox"/>	Device	IgniteNet-2.4G	2.4 GHz	Off	Off	n/a	Enabled	

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

Country: United States

WIRELESS 5 GHZ

GENERAL RADIO SETTINGS

Enable Radio:

Operation Mode: Access Point (Auto-WDS)

Q SITE SURVEY

PHYSICAL RADIO SETTINGS

Channel Bandwidth: 20MHz

Channel: Auto (all channels)

EDIT CHANNEL LIST

Tx Power: 20 dBm (100 mW)

Multicast Enhancement:

Global Settings The following items are displayed on this page section:

- **Country** — The MetroLinq device regulatory setting.

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.

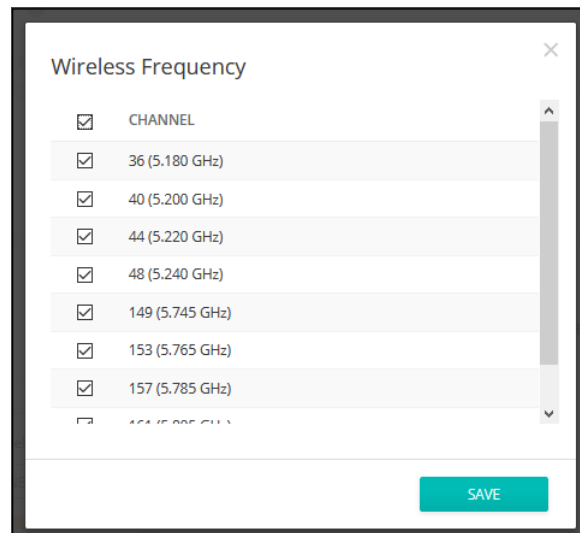
- **Key** — Sets the WPA2 pre-shared key to use for encryption.

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.)

Wireless 2.4 GHz Figure 240: MetroLinq Device 2.4 GHz Radio Settings

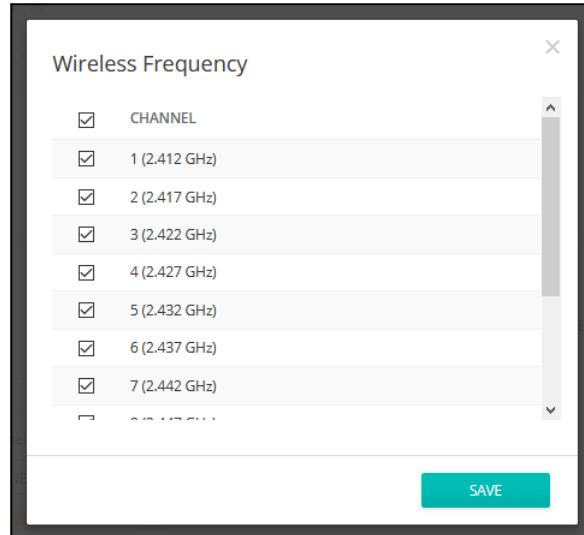
The screenshot shows the configuration page for the 2.4 GHz wireless interface. It includes sections for general settings (enabling the radio and performing a site survey) and physical settings (adjusting channel bandwidth, channel selection, transmit power, and multicast enhancement).

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.

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.

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

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)

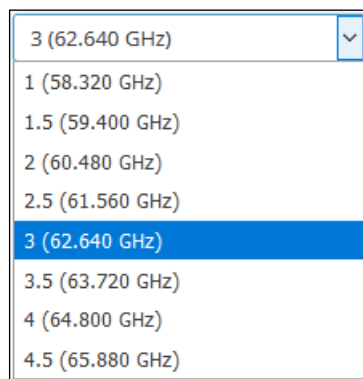
- **SSID** —Input a unique name for the service set identifier of the backup 5 GHz interface. MetroLinq units at each end of a point-to-point link must be set to the same 5 GHz backup SSID. (Range: 1—32 characters)
- **Broadcast SSID** — Enables or disables sending the configured SSID in beacon messages. (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.)

- **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

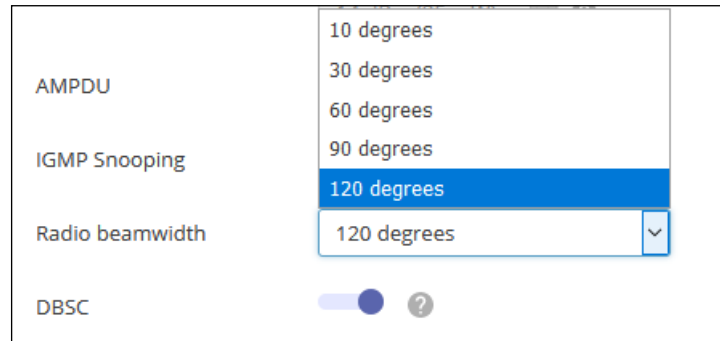


- **Tx Power** — Adjusts the maximum power of the radio signals transmitted on the 60 GHz interface. The higher the transmission power, the farther the transmission range and higher the data rate. (The range of power settings and defaults are dependent on the AP model and the Regulatory Country setting.)
- **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.

- **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)

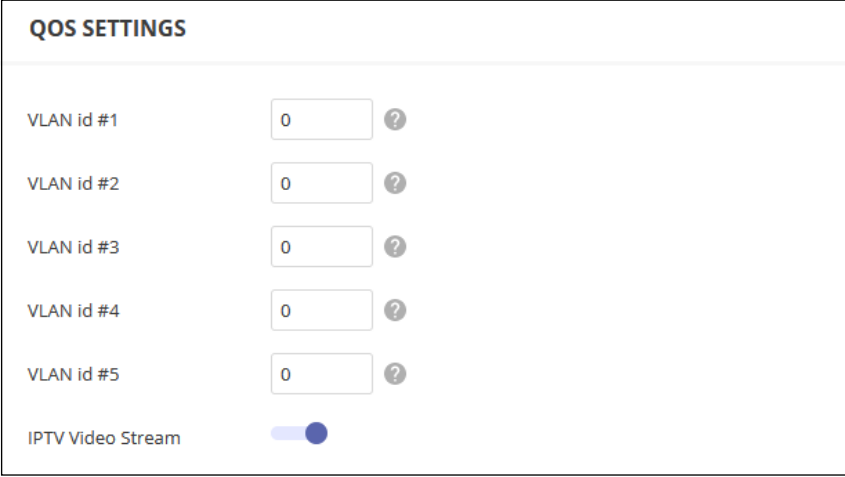
QoS Settings

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



QOS SETTINGS	
VLAN id #1	<input type="text" value="0"/> ?
VLAN id #2	<input type="text" value="0"/> ?
VLAN id #3	<input type="text" value="0"/> ?
VLAN id #4	<input type="text" value="0"/> ?
VLAN id #5	<input type="text" value="0"/> ?
IPTV Video Stream	<input checked="" type="checkbox"/>

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)

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 from the pull-down list.

Figure 246: MetroLinq Traffic Control Settings

GLOBAL SETTINGS

Traffic Control Enable

TRAFFIC PROFILE + ADD PROFILE

<input type="checkbox"/>	ORIGIN	PROFILE	DOWNLINK (MBPS)	UPLINK (MBPS)	ACTIONS
<input type="checkbox"/>	Device	Default	0	0	DELETE

Showing 1 to 1 of 1 entries « 1 »

TRAFFIC CONTROL + ADD CONTROL

<input type="checkbox"/>	ORIGIN	MAC	PROFILE	ACTIONS
No data available for this list				

Showing 0 to 0 of 0 entries « »

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)

- **Traffic Control** — Binds the Traffic Profiles to MAC addresses.
 - **MAC** — Device MAC address.
 - **Profile** — Configured profile name.

Using the LinqPath Tool

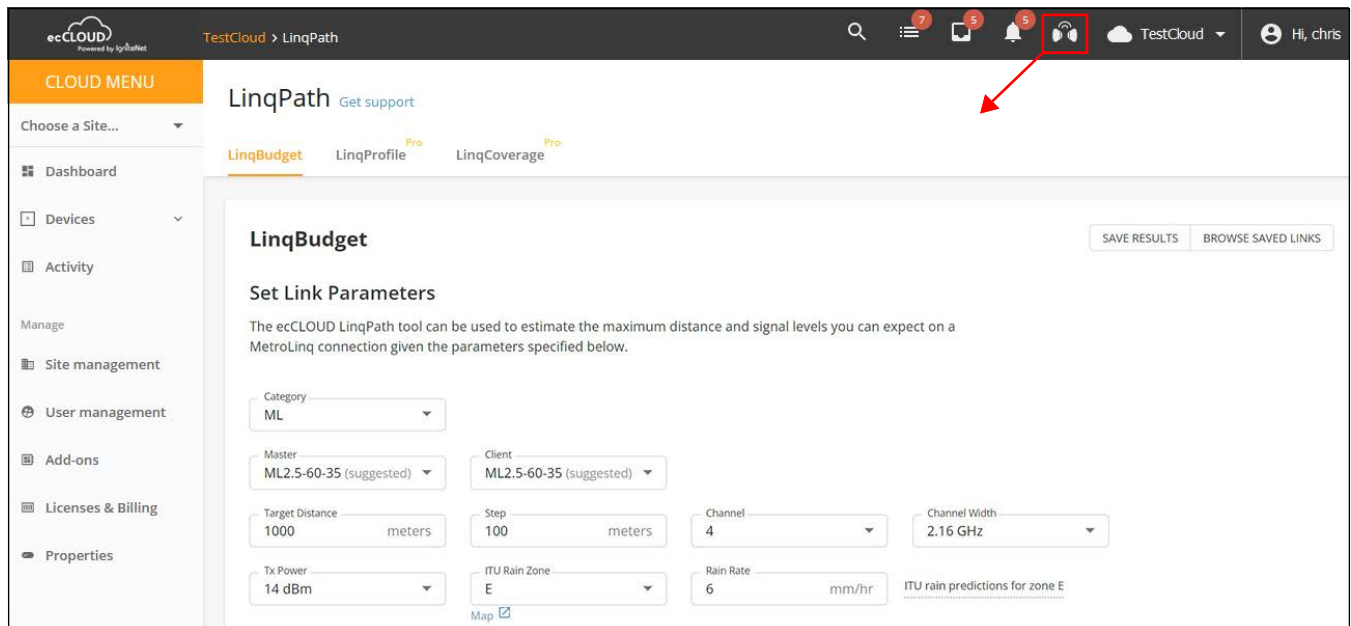
The Edgecore LinqPath™ tool can be used to estimate the maximum distance and signal levels you can expect on a MetroLinq connection given the specified parameters. Statistical rain fade calculations are included using the ITU rain model.

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

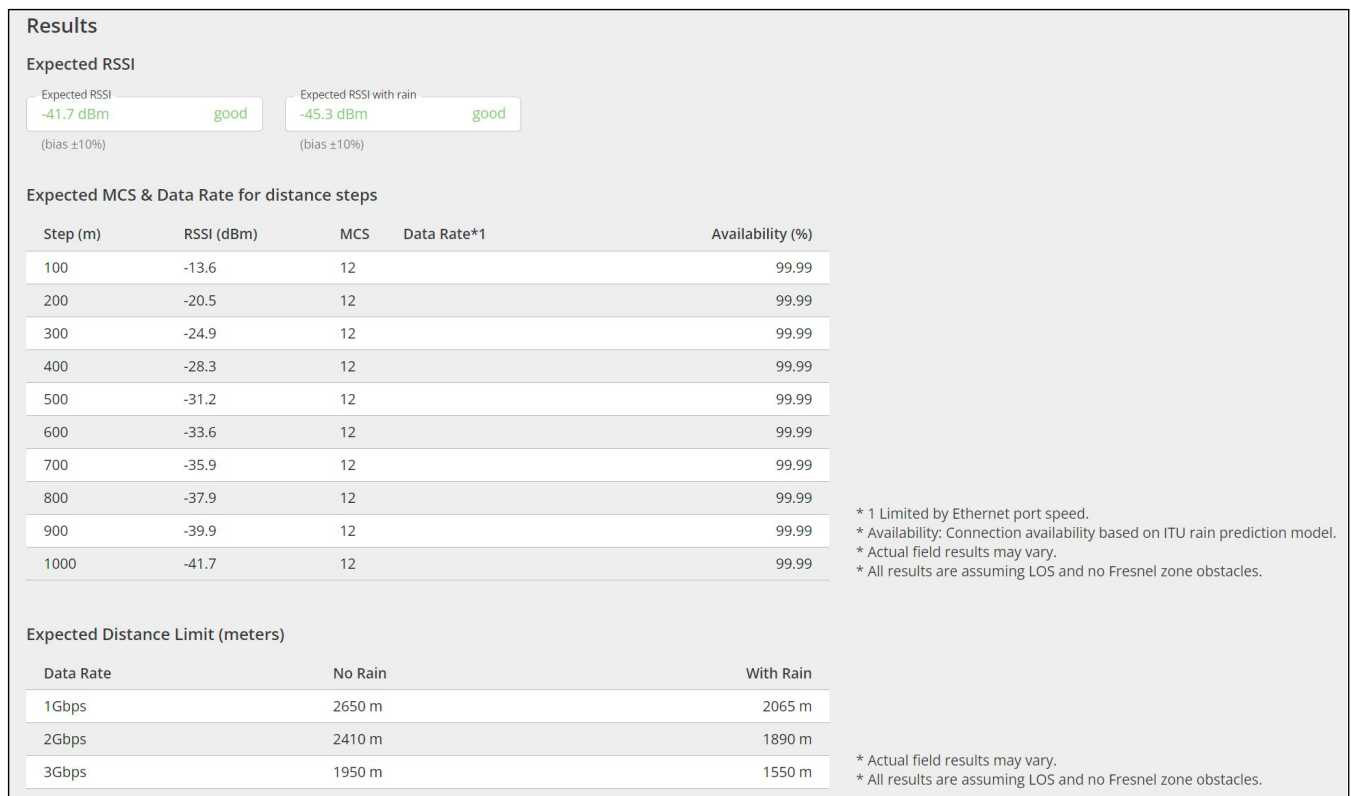


The following items are displayed on this page section:

- **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.

- **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



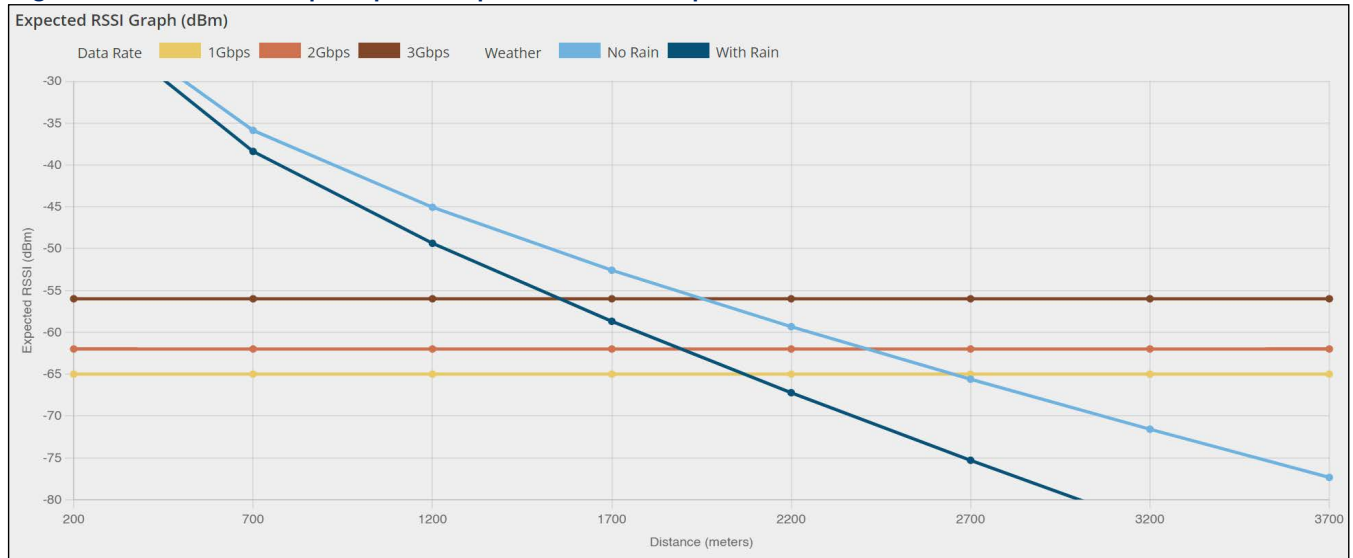
The following items are displayed on this page section:

- **Expected RSSI** — Shows the expected RSSI of the link based on the distance provided in the Target Distance input box.
- **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.

- **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



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” on page 254](#)
- [“General Networking Settings” on page 255](#)
- [“Radio Settings” on page 257](#)
- [“System Settings” on page 259](#)

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

The screenshot displays the Terragraph Device Dashboard for an LR-RTK device. The interface includes a left-hand navigation menu with options like Dashboard, Statistics, Activity, and Configuration (highlighted with a red box). The main content area is divided into several sections:

- DEVICE INFORMATION:** A table listing device details such as Site (ML_Site), Firmware (1.4.2-00266-4c6bd42), Main MAC address (14:44:8F:E5:7B:93), Serial Number (EC2223002535), Model (MLTG-CN_LR), Configuration state (with a warning icon), Inherit site settings (with an 'x' icon), Bootbank (0), Created on (2022-09-06 15:14), Last contact (2023-01-05 15:40), Uptime (n/a), LAN IP (192.168.1.121 with a warning icon), MANAGEMENT IP (n/a with a warning icon), CPU utilization, and Memory usage.
- Google Map:** A world map showing the device's location. A message states: "Your Google map is empty! Go to the Map Manager to place your devices."
- WIRELESS STATUS:** A section for 60 GHz Radio settings, including Operation Mode, Security, Local MAC, Remote MAC, Datarate, Tx Power, Channel, and Sector position, all of which are currently set to a dash (-).

General Networking Settings

Click the “General Networking” tab to configure management port and LAN port settings.

Figure 251: Terragraph Device General Networking

The screenshot shows the configuration interface for a Terragraph device. It is organized into three main sections:

- POE PORT:** Contains a dropdown menu for "POE Port Role" set to "Bridged with LAN Port".
- MANAGEMENT PORT SETTINGS:** Includes a dropdown for "IP Address Mode" (DHCP), a text input for "Fallback IP" (192.168.1.20), and a dropdown for "Fallback Netmask" (255.255.255.0).
- LAN PORT SETTINGS:** Includes a dropdown for "IP Address Mode" (Static IP), text inputs for "IP Address" (192.168.1.121), "Subnet Mask" (255.255.255.0), and "Default Gateway" (192.168.1.1). The "DNS Entries" field contains "8.8.8.8" and "2001:4860:4860::8888". At the bottom, there is a "Mgmt VLAN" toggle switch that is currently turned off.

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)

LAN Port Settings

- **IP Address Mode** — Configures the LAN interface to be in static IP mode or DHCP mode. In DHCP mode, a DHCP 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.

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.

- **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.

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 retries for switching bootbank** — The maximum number of bootup retries before switching to the next boot bank. (Range: 1-254; Default: 5)
- **Number of boot retries 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.

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.

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.

12

Switch Device Configuration

This chapter describes configuration settings for switches at the Device level. It includes the following sections:

- “Switch Configuration” on page 264
- “Port Configuration” on page 265
- “VLAN Configuration” on page 267
- “Configuring Name Servers” on page 269
- “Configuring Static IP Routes” on page 269
- “Configuring Port Rate Limiting (QoS)” on page 270
- “STP Configuration” on page 271
- “Port Security Configuration” on page 271
- “Configuring 802.1X Port Authentication” on page 272
- “ACL Configuration” on page 274
- “Configuring Switch Services” on page 276
- “Configuring Port Mirroring” on page 277
- “Configuring Local Logins” on page 278
- “Configuring System Settings” on page 278
- “Configuring Login Authentication” on page 279

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.

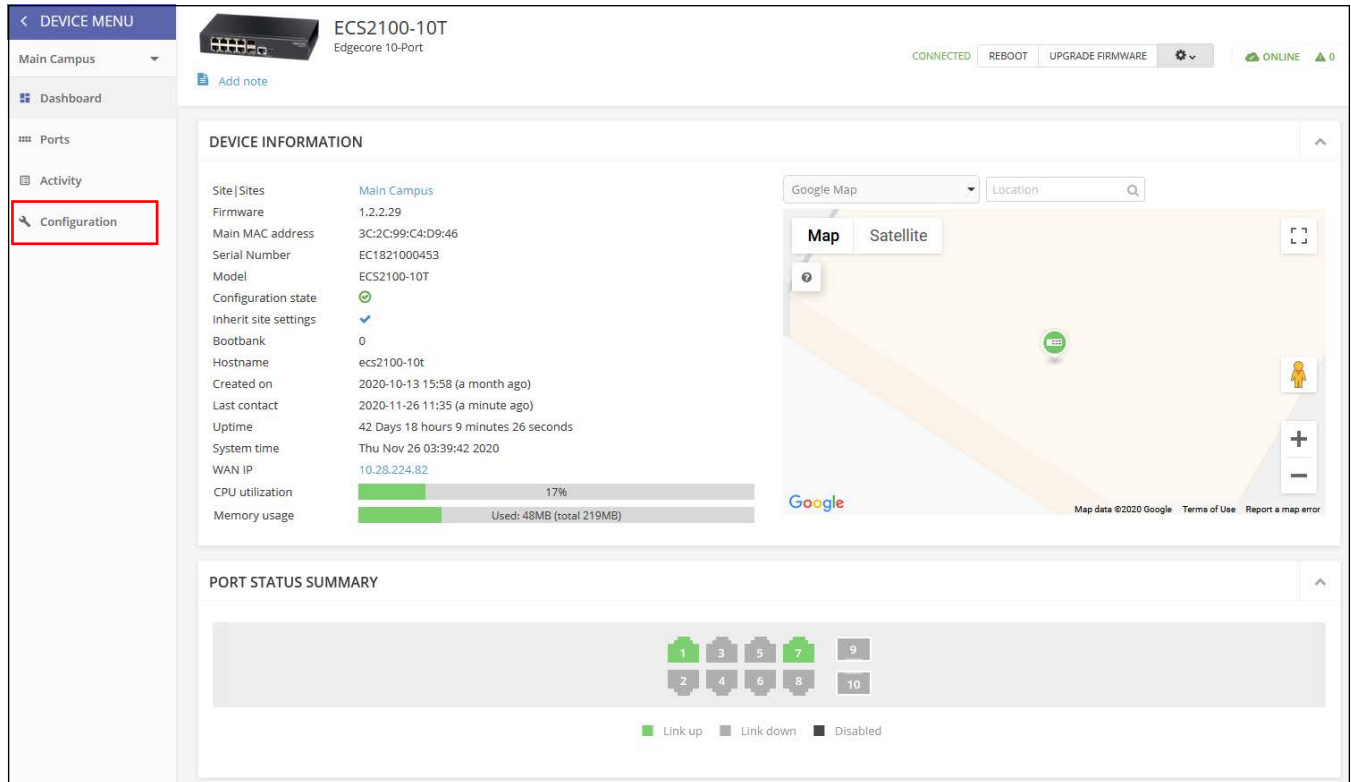
ECS2100-10P, ECS2100-10T, ECS2100-28P, ECS2100-28T, ECS2100-28PP, ECS2100-52T

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

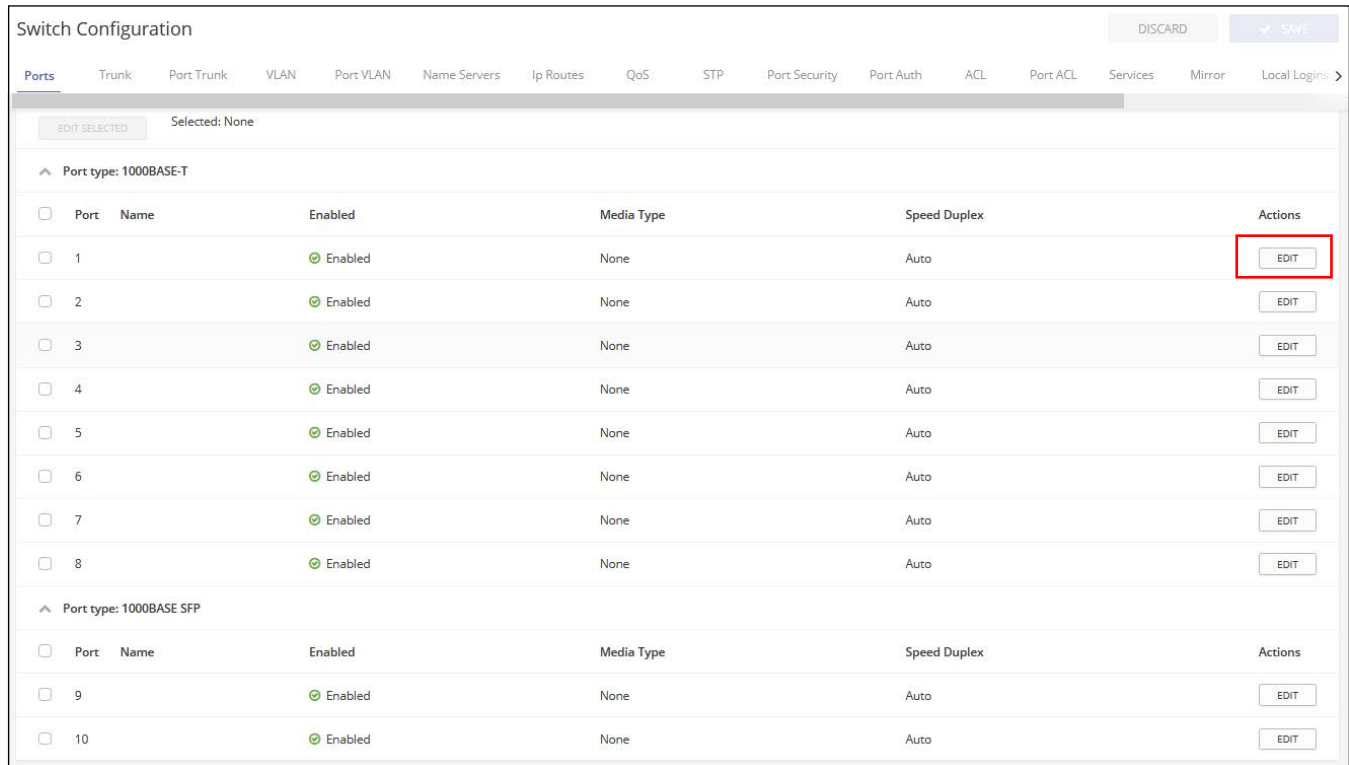


Port Configuration

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.

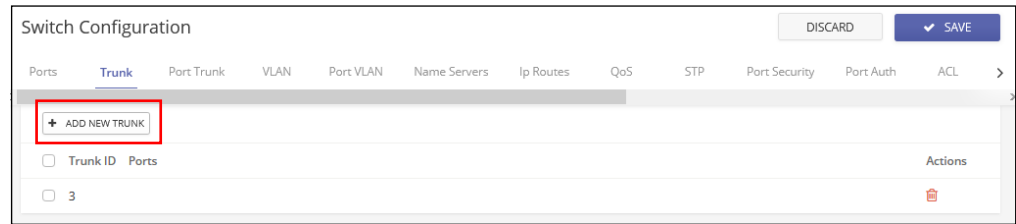
When setting up a static trunk between switches, take note of the following points:

- 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.

- 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.

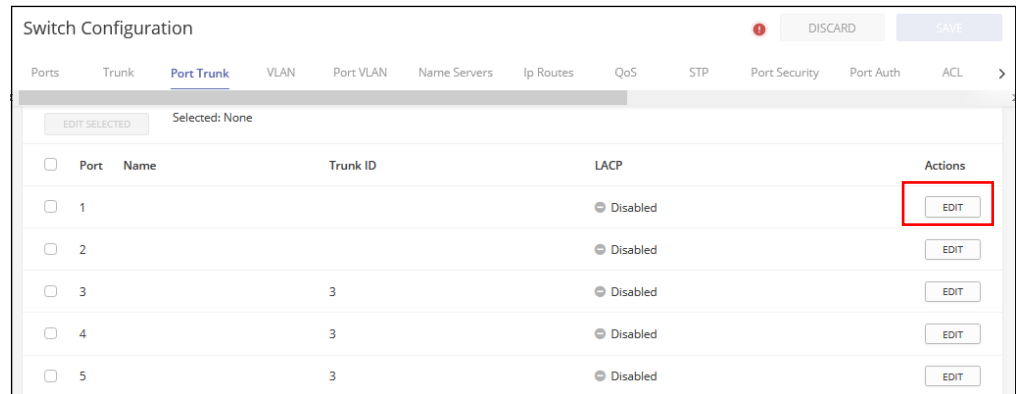
Click the Trunk tab and then the ADD NEW TRUNK button to create a trunk identifier.

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



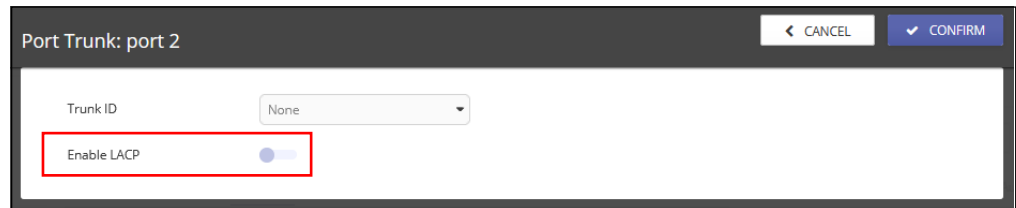
LACP Trunks The Link Aggregation Control Protocol (LACP) enables dynamic trunks to be created between two switches. LACP-configured ports automatically negotiate a trunked link with LACP-configured ports on another device. You can configure any number of ports on a switch as LACP, as long as they are 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.

- 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

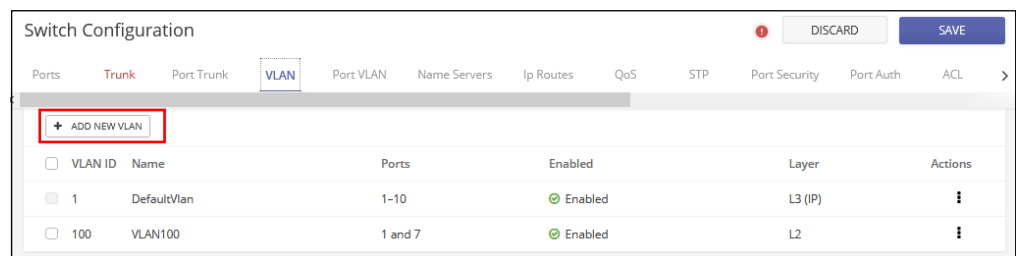


VLAN Configuration

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

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.

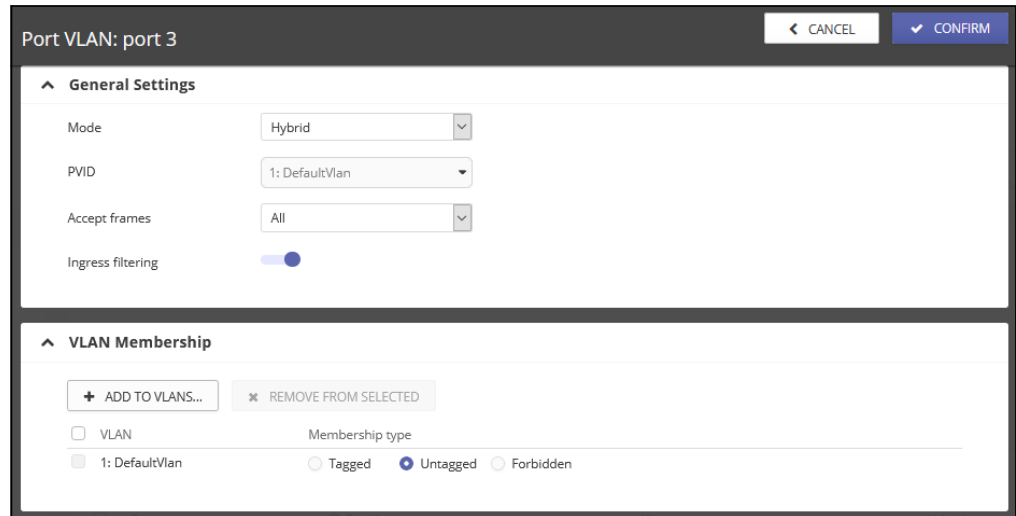
Click the Port VLAN tab to show port VLAN membership.

Figure 260: Configuring VLAN Port Members

Port	Name	Ingress filtering	Accept frames	Mode	VLANs	Actions
<input type="checkbox"/>	1	Enabled	All	Hybrid	1 and 100	EDIT
<input type="checkbox"/>	2	Enabled	All	Hybrid	1	EDIT
<input type="checkbox"/>	3	Enabled	All	Hybrid	1	EDIT
<input type="checkbox"/>	4	Enabled	All	Hybrid	1	EDIT

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.

Figure 261: Configuring VLAN Port Settings

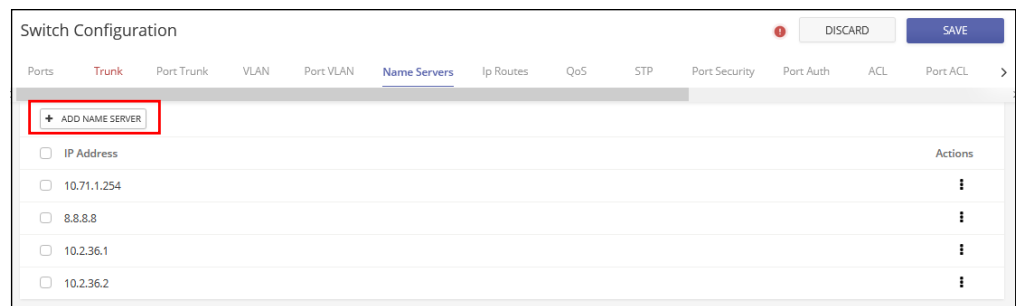


Configuring Name Servers

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

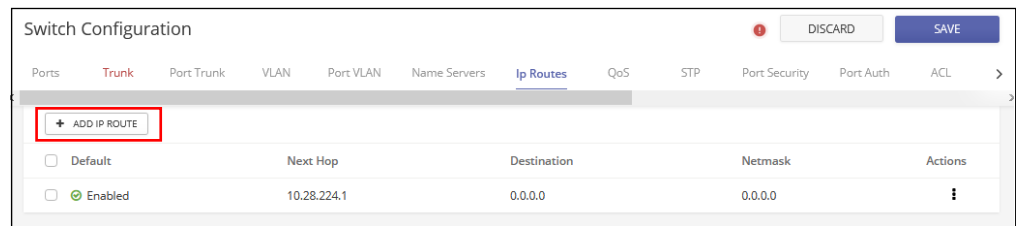
Edgecore switches support IP routing and routing path management via static routing definitions. When IP routing is functioning, a switch acts as a wire-speed router, passing traffic between VLANs with different IP interfaces, and routing traffic to external IP networks. However, when a switch is first booted, default routing can

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



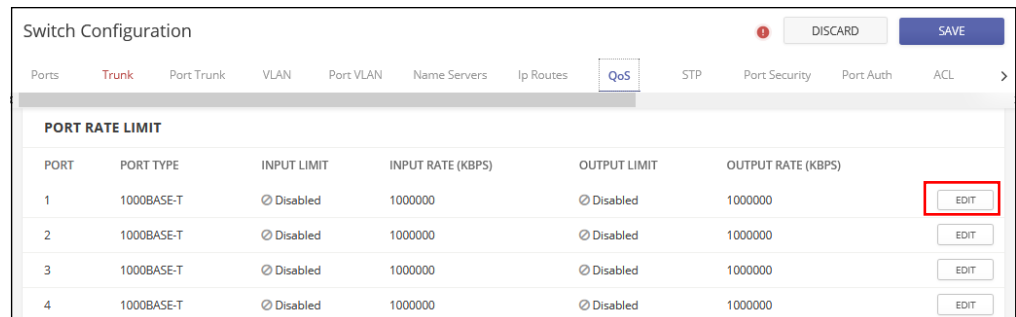
Configuring Port Rate Limiting (QoS)

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:

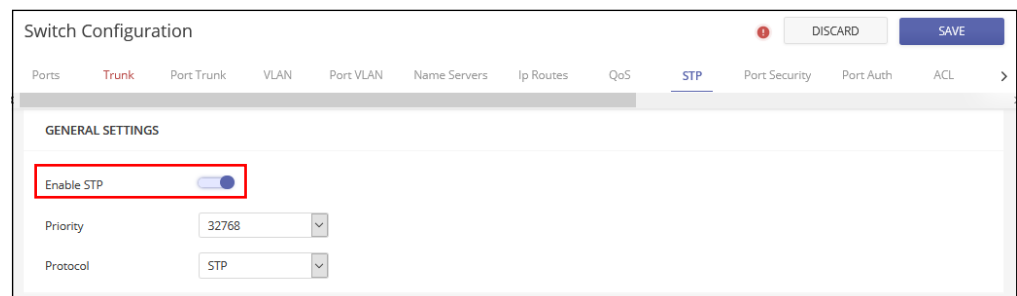
- **STP** — Spanning Tree Protocol (IEEE 802.1D). (When this option is selected, the switch will use RSTP set to STP forced-compatibility mode.)
- **RSTP** — Rapid Spanning Tree (IEEE 802.1w).
- **MSTP** — Multiple Spanning Tree (IEEE 802.1s).

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

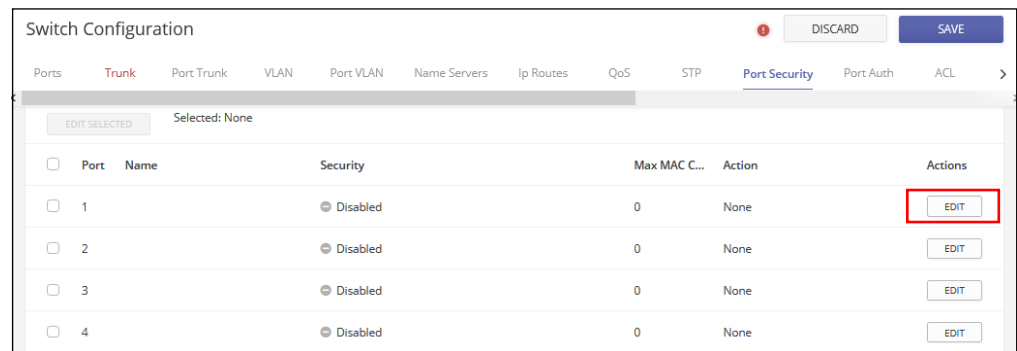
You can use Port Security to configure the maximum number of device MAC addresses that can be learned by a switch port, stored in the address table, and authorized to access the network.

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

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 279](#).

Click the EDIT button for a port to configure the port authentication details.

Figure 267: Configuring Port Authentication

Port	Name	Operation Mode	Control mode	Reauthentication	Actions
<input type="checkbox"/>	1	Single host	Force authorized	Disabled	EDIT
<input type="checkbox"/>	2	Single host	Force authorized	Disabled	EDIT
<input type="checkbox"/>	3	Single host	Force authorized	Disabled	EDIT
<input type="checkbox"/>	4	Single host	Force authorized	Disabled	EDIT

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

Port Auth: port 2

Control mode: Force authorized

Operation Mode: Single host

Max requests: 2

Quiet period: 60 seconds

Tx period: 30 seconds

Supplicant timeout: 30 seconds

Enable reauthentication:

Reauthentication period: 3600 seconds

Intrusion action: Block traffic



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.

ACL Configuration

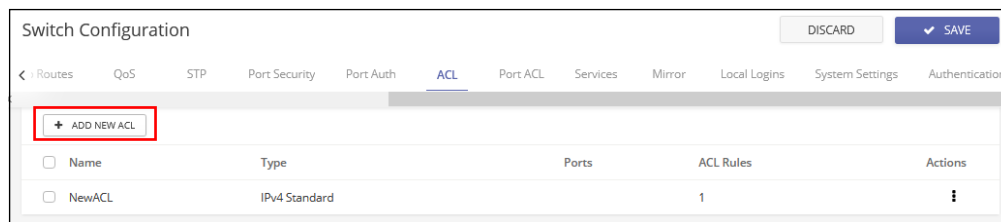
Access Control Lists (ACL) provide ingress packet filtering for IPv4/IPv6 frames (based on address, protocol, Layer 4 protocol port number or TCP control code), IPv6 frames (based on address, DSCP traffic class), or any frames (based on MAC address or Ethernet type). To filter incoming packets, first 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:

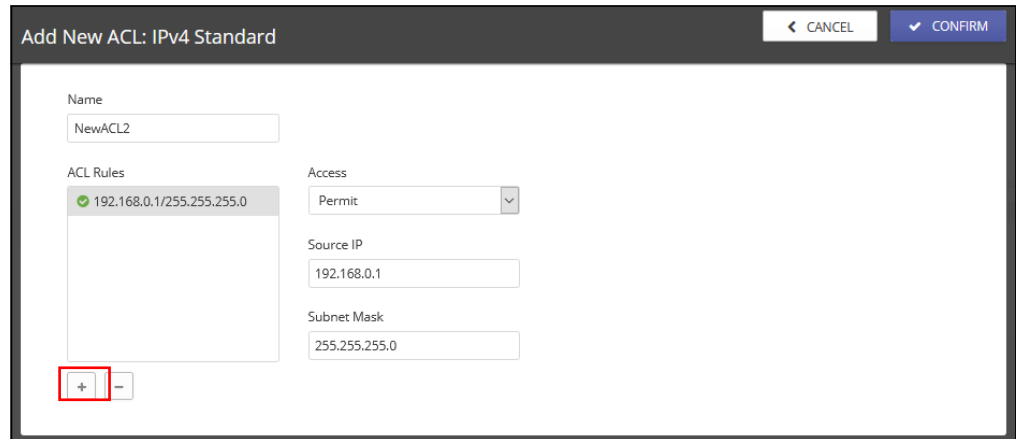
- **IPv4 Standard** — Configures an ACL based on source IPv4 addresses.
- **IPv4 Extended** — Configures an ACL based on source and destination IPv4 addresses, TCP/UDP port number, protocol type, and TCP control code.
- **IPv6 Standard** — Configures an ACL based on source IPv6 addresses.
- **IPv6 Extended** — 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.

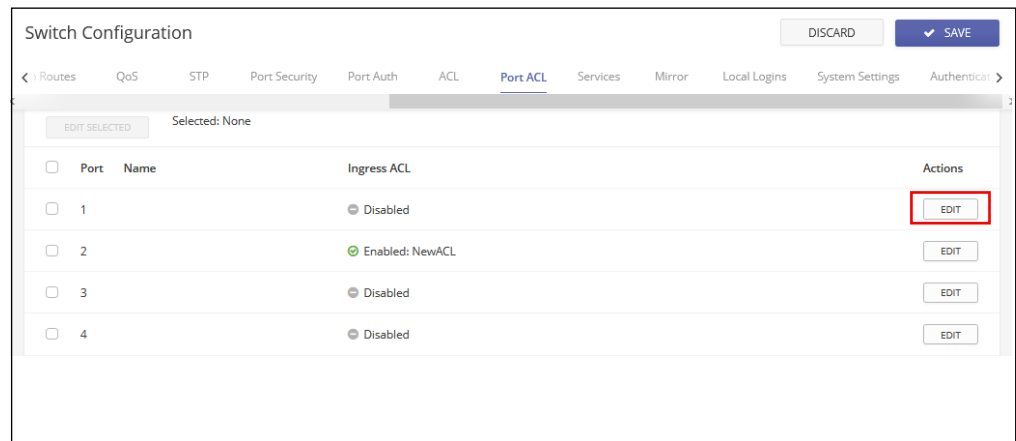
Figure 270: Adding a New ACL



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.

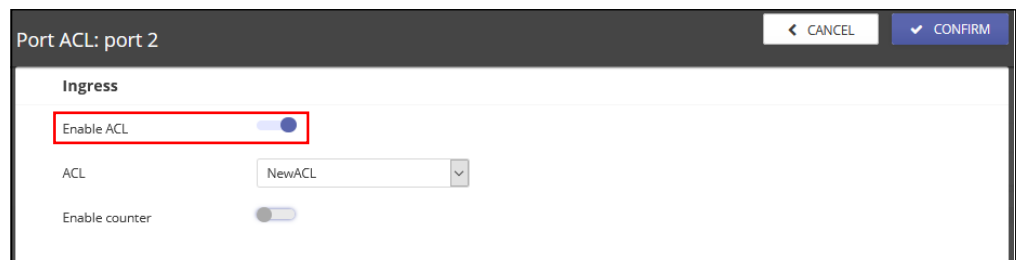
Click the EDIT button to configure an ACL for a port.

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





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.

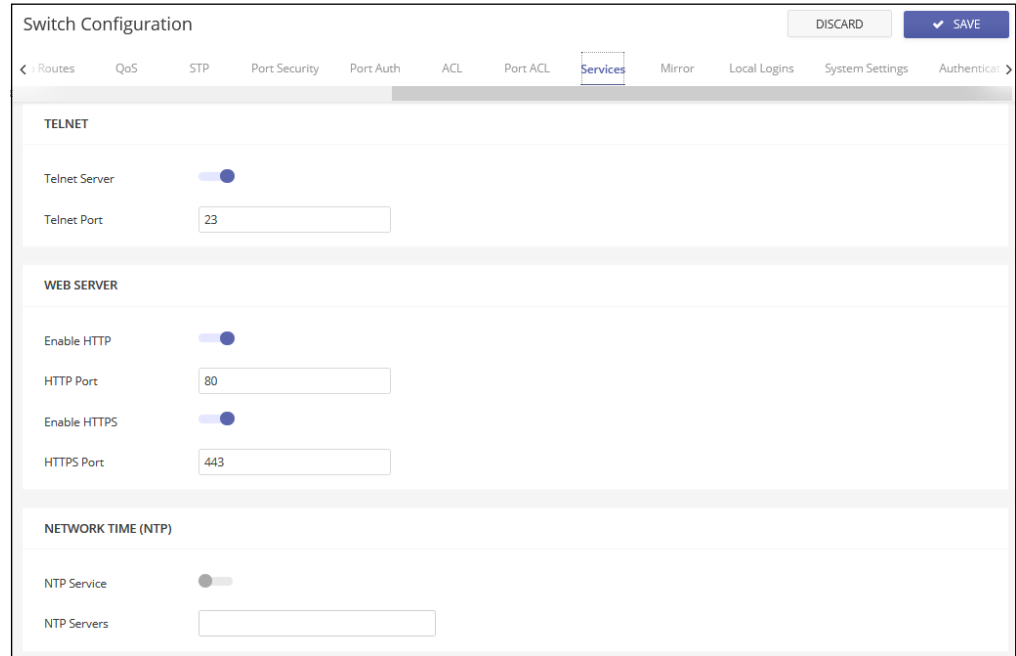
You can also enable HTTPS over the Secure Socket Layer (SSL), providing secure access (an encrypted connection) to the switch's web interface.

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.

Figure 273: Switch Services

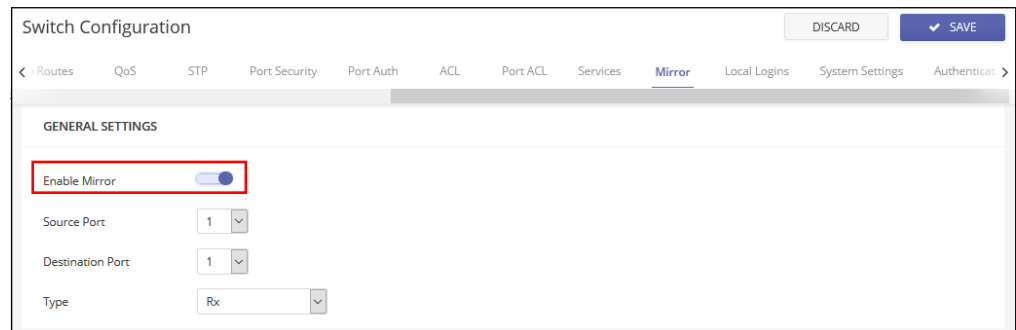


Configuring Port Mirroring

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



Configuring Local Logins

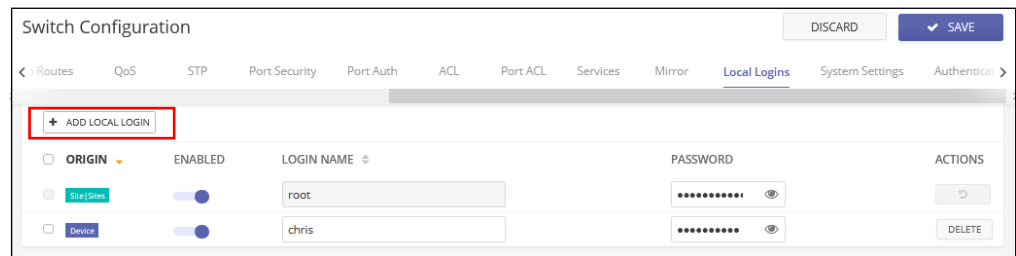
Use the Local Logins tab to control management access to the switch based on manually configured user names and passwords.

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



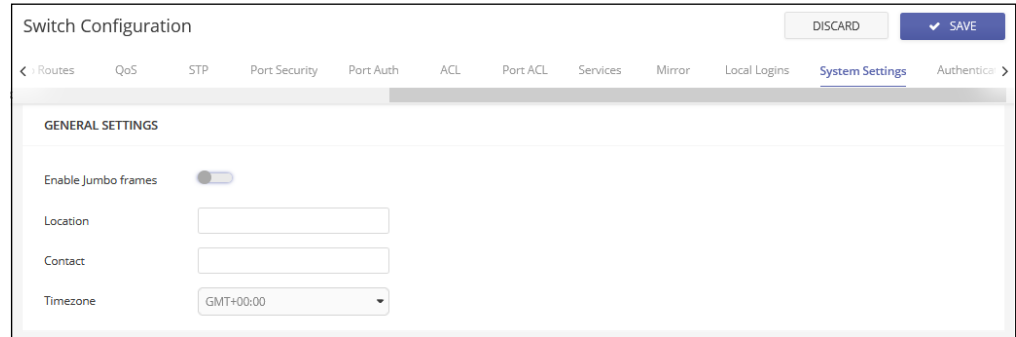
Configuring System Settings

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.

Figure 276: System Settings



Configuring Login Authentication

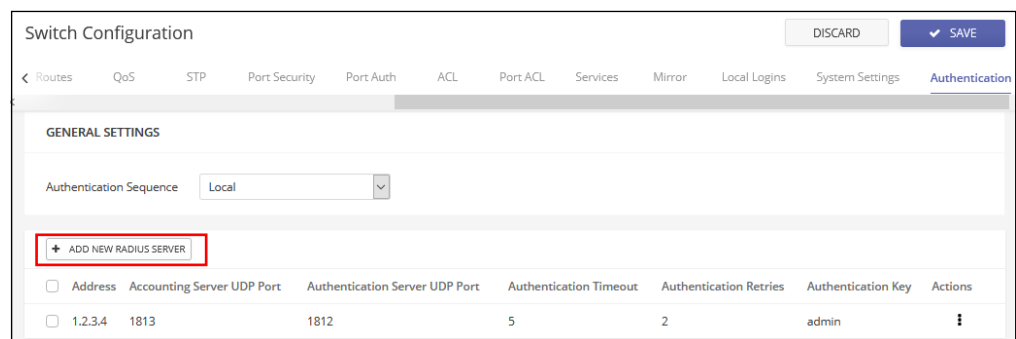
Use the Authentication tab to specify local or remote authentication. Local and remote login authentication control management access via the console port, web browser, or Telnet.

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.

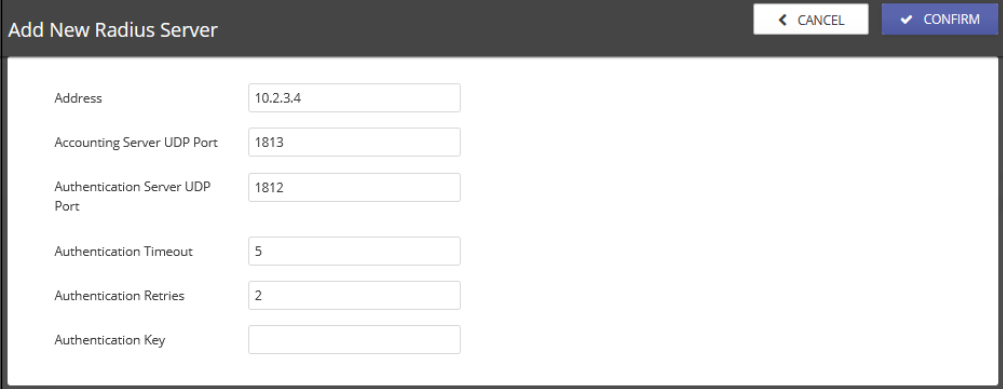
You can specify up to three authentication methods for any user to indicate the authentication sequence. For example, if you select (1) RADIUS, (2) TACACS and (3) Local, the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted using the TACACS+ server, and finally the local user name and password is checked.

Figure 277: Login Authentication



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



The screenshot shows a configuration dialog box titled "Add New Radius Server". It contains several input fields for configuring a RADIUS server. The fields and their values are as follows:

Field Name	Value
Address	10.2.3.4
Accounting Server UDP Port	1813
Authentication Server UDP Port	1812
Authentication Timeout	5
Authentication Retries	2
Authentication Key	

At the top right of the dialog, there are two buttons: "CANCEL" and "CONFIRM".

13

SD-WAN Device Configuration

This chapter describes configuration settings for SD-WAN at the Device level. It includes the following sections:

- [“SD-WAN Device Configuration” on page 282](#)
- [“WAN” on page 284](#)
- [“LAN” on page 289](#)
- [“Static Route” on page 291](#)
- [“Dynamic Route” on page 291](#)
- [“Access Control” on page 292](#)
- [“Virtual Server” on page 294](#)
- [“System Settings” on page 295](#)

Accessing SD-WAN Device-Level Configuration

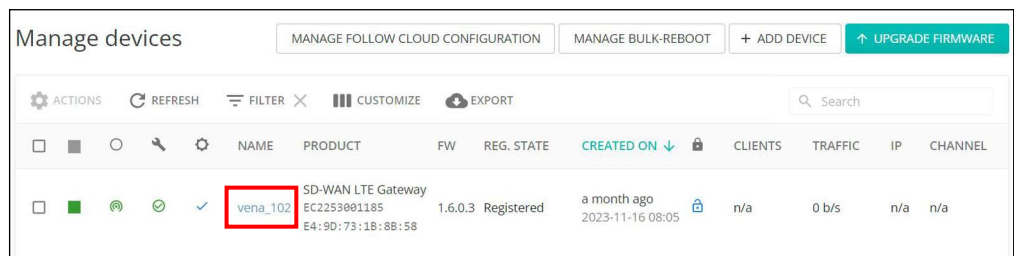
When a device’s “Inheritance Policy” is enabled, the device is configured from the Site level. However, a device can be individually configured at the Device level and the settings will override the Site-level configuration.

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.

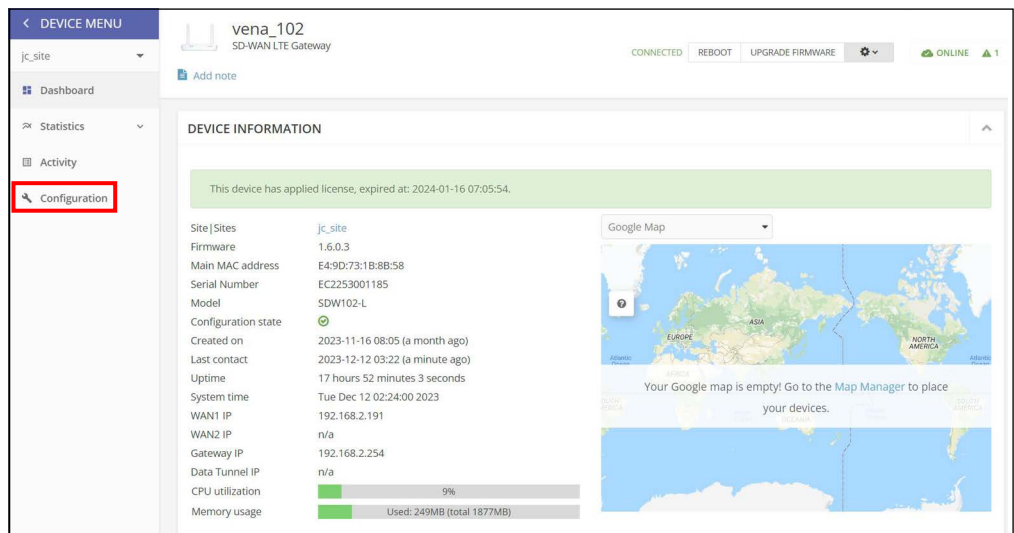
To access configuration for a device, click on the device name from the Site-level list of devices (also available from the Cloud-level list of devices).

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



This chapter only covers the device configuration that is different from the Site-level configuration, as documented in [“Site SD-WAN Configuration” on page 214](#).

WAN

Click the “WAN” tab to configure settings. The following items are displayed on the WAN tab.

WAN

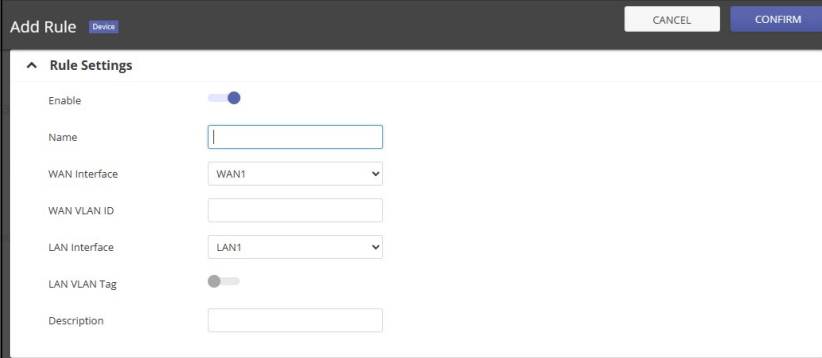
Figure 281: Device WAN Configuration

The screenshot shows the WAN configuration interface. At the top, there is a 'WAN' header. Below it is the 'WAN PROVISIONING' section, which includes an 'Enable' toggle switch that is turned on. The interface is divided into two columns: 'WAN1' and 'WAN2'. Under 'WAN1', there is an 'Enable' toggle switch (turned on), a 'Type' dropdown menu set to 'DHCP', and a 'NAT' toggle switch (turned on). Under 'WAN2', there is an 'Enable' toggle switch that is turned off.

- **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.

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.

SLA

Figure 284: SLA Configuration

The screenshot shows the SLA configuration interface with the following settings:

Field	Value	Unit
Enable	<input checked="" type="checkbox"/>	
Test IP	8.8.8.8	
Monitor Interval	5.0	seconds
Max Latency	700	milli seconds
Max Jitter	700000	micro seconds
WAN Load Balance	<input type="checkbox"/>	

- **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.

- **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

- 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

The screenshot shows a configuration form for a traffic steering rule. The fields are as follows:

Name	<input type="text"/>
Mode	Available <input type="button" value="info"/>
Multipath Default	<input type="checkbox"/>
Prefer Interface	WAN1 <input type="button" value="dropdown"/>
Prefer Gateway	<input type="text"/>
Backup Interface	<input type="button" value="dropdown"/>

- **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.

- **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

The screenshot displays the configuration page for the Default LAN. At the top left, there is a 'LAN' tab and an 'ADD LAN' button. Below this, the 'DEFAULT LAN' section contains several configuration options:

- IP Address:** A text input field containing '192.168.100.1'.
- Subnet Mask:** A dropdown menu showing '255.255.255.0 (/24)'.
- DPI:** A toggle switch currently turned off.
- DHCP Server:** A toggle switch currently turned on.
- DHCP Start:** A text input field containing '192.168.100.100'.
- DHCP Limit:** A text input field containing '192.168.100.200'.
- Lease Time:** A text input field containing '86400'.
- DNS 1:** A text input field containing '8.8.8.8'.
- DNS 2:** An empty text input field.

- **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.

- **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.

Static Route

Click the “Static Route” tab to configure the list of static routes.

Figure 288: Static Route Configuration

IP ADDRESS	NETMASK	GATEWAY	INTERFACE	METRIC
<input type="text"/>	255.255.255.0 (24)	<input type="text"/>	WAN1	0

Showing 1 to 1 of 1 entries

- **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

DYNAMIC SETTINGS

OSPF

OSPF Auto

BGP

BGP Auto

ASN

- **OSPF** — Enable or disable the OSPF protocol.

- **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	PROTOCOL	IP ADDRESS	NETMASK	AREA/ASN	
<input type="checkbox"/>	OSPF	Network	10.0.0.1	255.255.255.0 (/24)	1

- **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

NAME	APPLICATION MODE	ADDRESS	PROTOCOL	ACTION TYPE	DIRECTION	ACTIONS
No data available for this list						

- **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

The screenshot shows a configuration window titled "Add Rule" with a "Device" tab. At the top right are "CANCEL" and "CONFIRM" buttons. Below is a "Rule Settings" section with the following fields:

- Name: [Empty text input]
- Source IP: [Empty text input]
- Source Netmask: 255.255.255.255
- Destination IP: [Empty text input]
- Destination Netmask: 255.255.255.255
- Application Mode: Transport Protocol (dropdown)
- Application Name: - CUSTOMIZED - (dropdown)
- Protocol: None (dropdown)
- Action Type: Deny (dropdown)
- Direction: Any (dropdown)

- **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.

- **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

The screenshot shows a configuration window titled "Add Virtual Server" with a "Device" dropdown menu. The main content area is titled "Virtual Server Settings" and contains the following fields:

- Name: Text input field
- Classification: Dropdown menu with "Virtual Server" selected
- Private IP: Text input field
- Protocol: Dropdown menu with "UDP" selected
- Public Port: Text input field
- Private Port: Text input field
- Description: Text input field

At the top right of the window, there are "CANCEL" and "CONFIRM" buttons.

Click "Add Virtual Server" and configure the settings of a new virtual server:

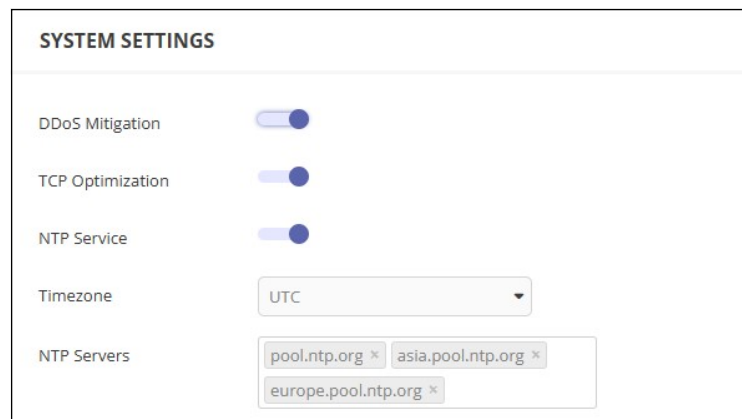
- **Name** — Enter a name for the virtual server entry.
- **Classification** — Choose the type of virtual server to deploy:

- **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.

- **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.

