Wi-Fi 6 AX1800 Daul-Radio In-Wall AP

MI13

User Guide v1.2

Copyright

Notice

BROWAN reserves the right to change specifications without prior notice.

While the information in this document has been compiled with great care, it may not be deemed an assurance of product characteristics. BROWAN shall be liable only to the degree specified in the terms of sale and delivery.

The reproduction and distribution of the documentation and software supplied with this product and the use of its contents is subject to written authorization from BROWAN.

Trademarks

The product described in this book is a licensed product of BROWAN.

Microsoft, Windows 95, Windows 98, Windows Millennium, Windows NT, Windows 2000, Windows XP, Windows 7, Windows 10, Windows 11, and MS-DOS are registered trademarks of the Microsoft Corporation.

MacOS is a registered trademark of Apple Computer, Inc.

Wi-Fi is a registered trademark of Wi-Fi Alliance.

All other brand and product names are trademarks or registered trademarks of their respective holders.

Contents

About this Guide

Purpose

This document provides information of web configuration of the MI13 Wi-Fi 6 AX1800 Dual-Radio In-Wall AP.

Prerequisite Skills and Knowledge

To use this document effectively, you should have a working knowledge of Local Area Networking (LAN) concepts and wireless Internet access infrastructures. In addition, you should be familiar with the following:

- Hardware installers should have a working knowledge of basic electronics and mechanical assembly, and should understand related local building codes.
- Device administrators should have a solid understanding of device management, network operations and troubleshooting knowledge.
-

Conventions Used in this Document

The following typographic conventions and symbols are used throughout this document:

!!!	Very important information. Failure to observe this may result in damage.
!	Important information that should be observed.
i	Additional information that may be helpful but which is not required.
bold	Menu commands, buttons and input fields are displayed in bold
`code`	File names, directory names, form names, and system-generated output such as error messages are displayed in constant-width type
`<value>`	Placeholder for certain values, e.g. user inputs
[value]	Input field format, limitations, and/or restrictions.

Chapter 1 – Introduction

Thank you for choosing the MI13 Wi-Fi 6 AX1800 Dual-Radio In-Wall MI13 In-Wall AP product.

The MI13 In-Wall AP product features 2.4GHz and 5GHz 2x2 dual-radio MIMO with four (4) Gigabit Ethernet ports, one of which delivers PoE to power and connect an 802.3af device to the network.

By utilizing AX1800 data rate, MI13 In-Wall AP product ensures superior performance for concurrent real-time applications such as multimedia streaming, online gaming and audio/video chats in indoor environment.

Configuration

Access and configure the MI13 In-Wall AP by executing web browser and enter IP address. The default IP address is:

```
IP 192.168.19.1  subnet 255.255.255.0
```
on WAN port

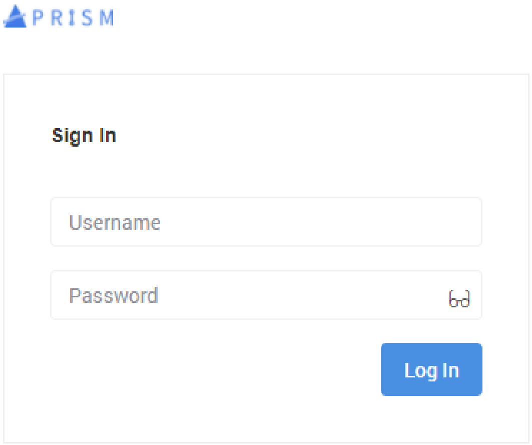
Step 1 Configure your PC with Static IP address and connect to WAN ports on the MI13 In-Wall AP into your PC’s RJ45 Ethernet port. Open the Web browser and type the default IP address 192.168.19.1.

ℹ	1. Please refer to quick installation guide for hardware installation and physical Ethernet port connection on each model. 2. You can set any static IP address from 192.168.19.2 to 192.168.19.250 for the PC to connect with MI13.

Step 2 Enter the administrator login details to access the Web management.

ℹ	The default administrator settings for web interfaces are: Username: **prism** Password: **prism**

Click Log In to proceed:



Chapter 2 – Web Management Menu

This chapter describes the web management menu of the MI13 MI13 In-Wall AP which works in Router mode and MI13 In-Wall AP (AP) mode.

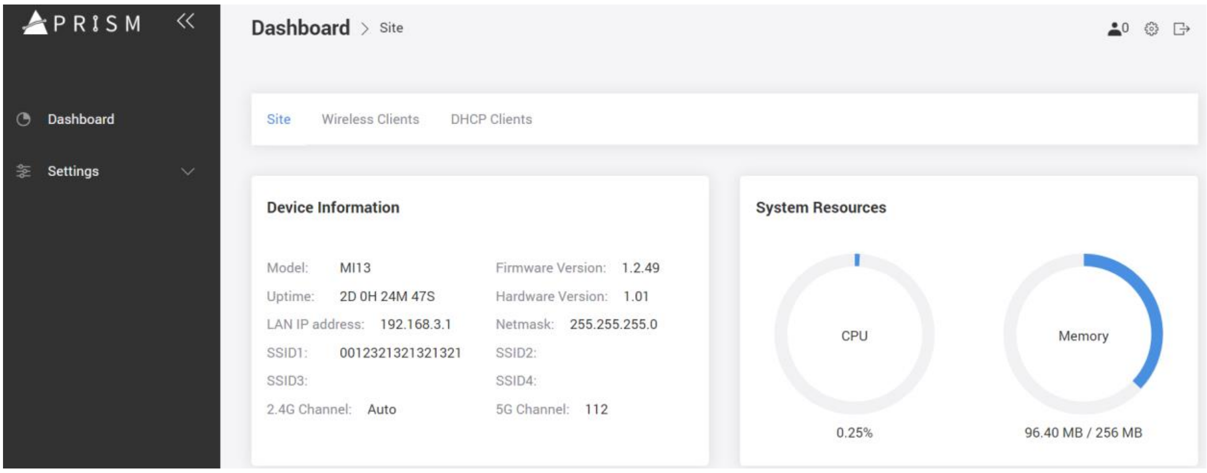
!	The default configuration is AP mode.

The **main menu** consists of the following sub menus:

- **Dashboard** – to show current status.
- **Settings** – to configure the MI13 In-Wall AP.

Web Management

The web management page is displayed after successfully logging into the system. From the menu all essential configuration pages are accessible.



Model: MI13
Uptime: 2D 0H 24M 47S
LAN IP address: 192.168.3.1
SSID1: 0012321321321321
SSID3:
2.4G Channel: Auto
Firmware Version: 1.2.49
Hardware Version: 1.01
Netmask: 255.255.255.0
SSID2:
SSID4:
5G Channel: 112

The **web management** has the following structure:

Dashboard

Site – show the status related with the whole device.

Wireless Clients – show the status of wireless client (users) information.

DHCP Clients – show the status of DHCP clients information.

Settings

Network – specify the network parameters.

Wireless – define the settings of Wi-Fi radios.

Services – set management’s interfaces.

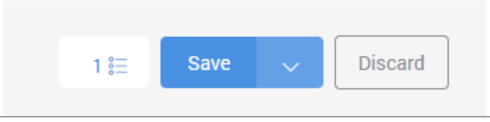
System – configure basic information.

Users – manage the login credentials.

Tools - built-in tools that help to debug the connection.

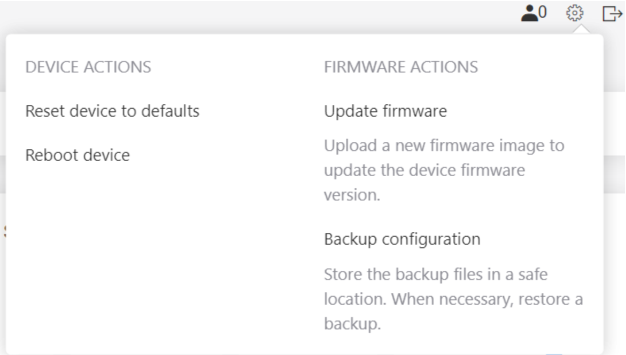
!

Please click **Save** to make changes effective, or click **Discard** to drop changes on top menu.



!

Reset device to defaults, **Reboot device**, **Update firmware** and **backup configuration** can be performed by clicking the tool button at top right.

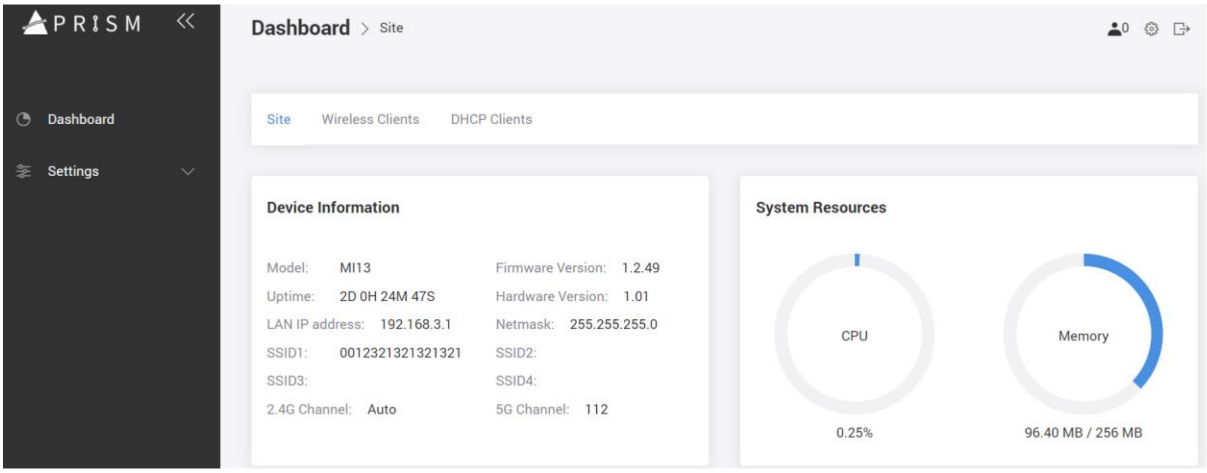


Upload a new firmware image to update the device firmware version.

Store the backup files in a safe location. When necessary, restore a backup.

Chapter 3 - Dashboard

This chapter describes the dashboard page of the MI13 In-Wall AP.



Device Information

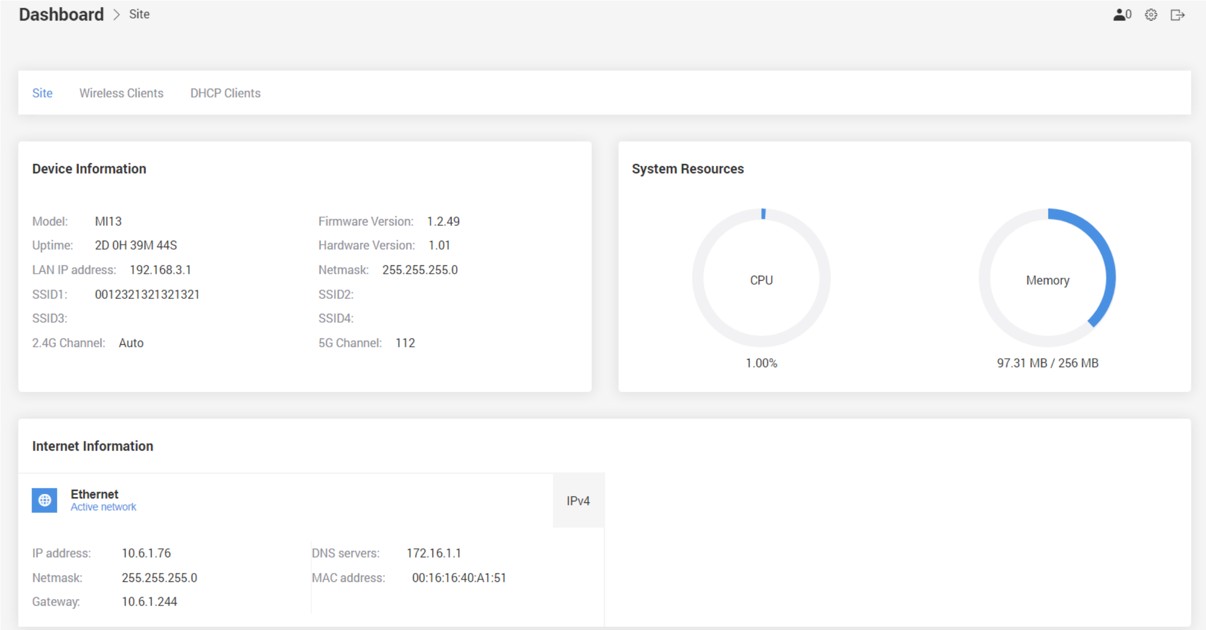
Model: MI13 Firmware Version: 1.2.49
Uptime: 2D 0H 24M 47S Hardware Version: 1.01
LAN IP address: 192.168.3.1 Netmask: 255.255.255.0
SSID1: 0012321321321321 SSID2:
SSID3: SSID4:
2.4G Channel: Auto 5G Channel: 112

System Resources

CPU 0.25%
Memory 96.40 MB / 256 MB

Dashboard > Site

The **Site** page shows important information of system and network status.



Device Information

Model: MI13 Firmware Version: 1.2.49
Uptime: 2D 0H 39M 44S Hardware Version: 1.01
LAN IP address: 192.168.3.1 Netmask: 255.255.255.0
SSID1: 0012321321321321 SSID2:
SSID3: SSID4:
2.4G Channel: Auto 5G Channel: 112

System Resources

CPU 1.00%
Memory 97.31 MB / 256 MB

Internet Information

Ethernet
Active network

IP address: 10.6.1.76 DNS servers: 172.16.1.1
Netmask: 255.255.255.0 MAC address: 00:16:16:40:A1:51
Gateway: 10.6.1.244

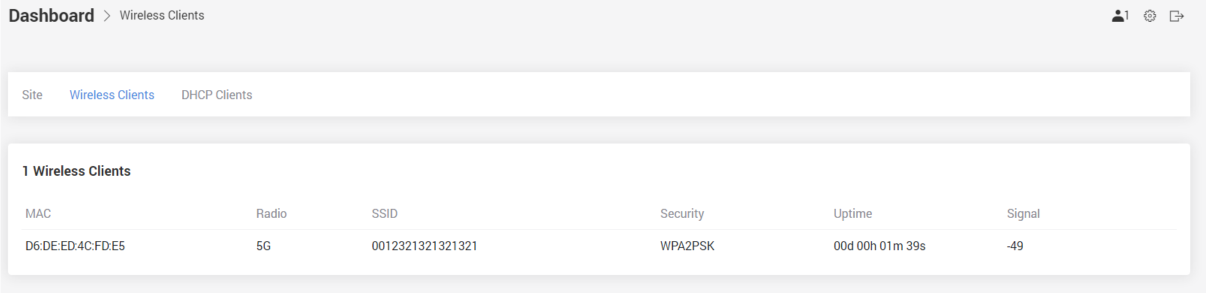
Device information – display the MI13 In-Wall AP’s basic information.

System resources – display the system utilization.

Internet Information – show the IP information on WAN port.

Dashboard > Wireless Clients

The **Wireless Clients** page shows the status of connected wireless clients information.



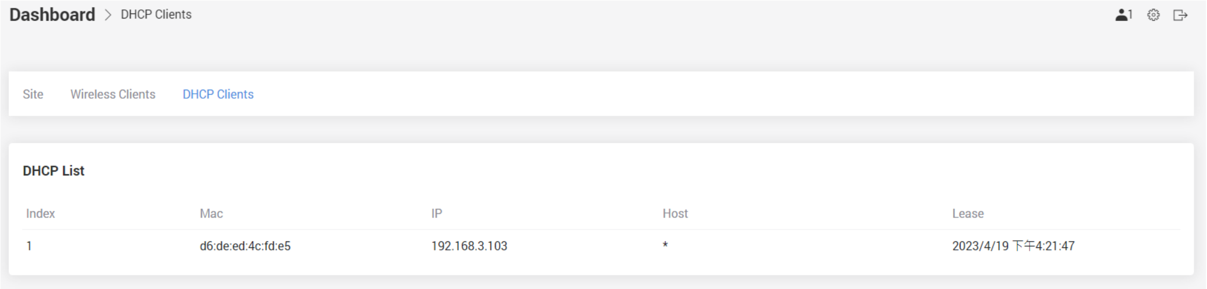
1 Wireless Clients

MAC	Radio	SSID	Security	Uptime	Signal
D6:DE:ED:4C:FD:E5	5G	0012321321321321	WPA2PSK	00d 00h 01m 39s	-49

Wireless Clients – show the connected wireless clients information, including MAC, Radio, SSID, Security, Uptime, and Signal strength.

Dashboard > DHCP Clients

The **DHCP Clients** page shows the status of connected DHCP clients information.



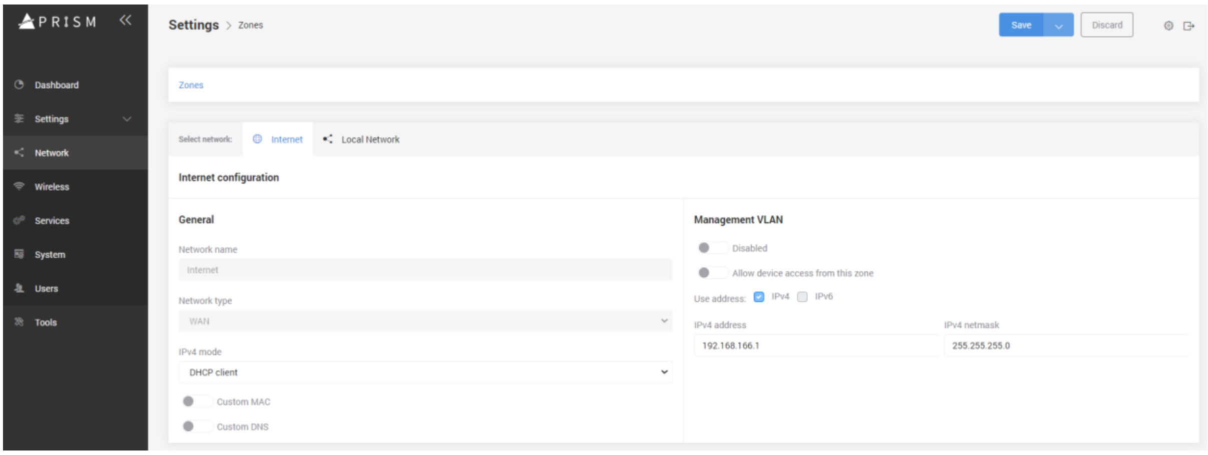
DHCP List

Index	Mac	IP	Host	Lease
1	d6:de:ed:4c:fd:e5	192.168.3.103	*	2023/4/19 下午4:21:47

DHCP Clients – show the assigned IP address DHCP clients information, including MAC, IP address, Host, and Lease time.

Chapter 4 - Settings

This chapter describes all configurations at the settings page of the MI13 In-Wall AP.



Internet configuration

General

Network name: Internet

Network type: WAN

IPv4 mode: DHCP client

○ Custom MAC

○ Custom DNS

Management VLAN

○ Disabled

○ Allow device access from this zone

Use address: ☑ IPv4 □ IPv6

IPv4 address: 192.168.166.1

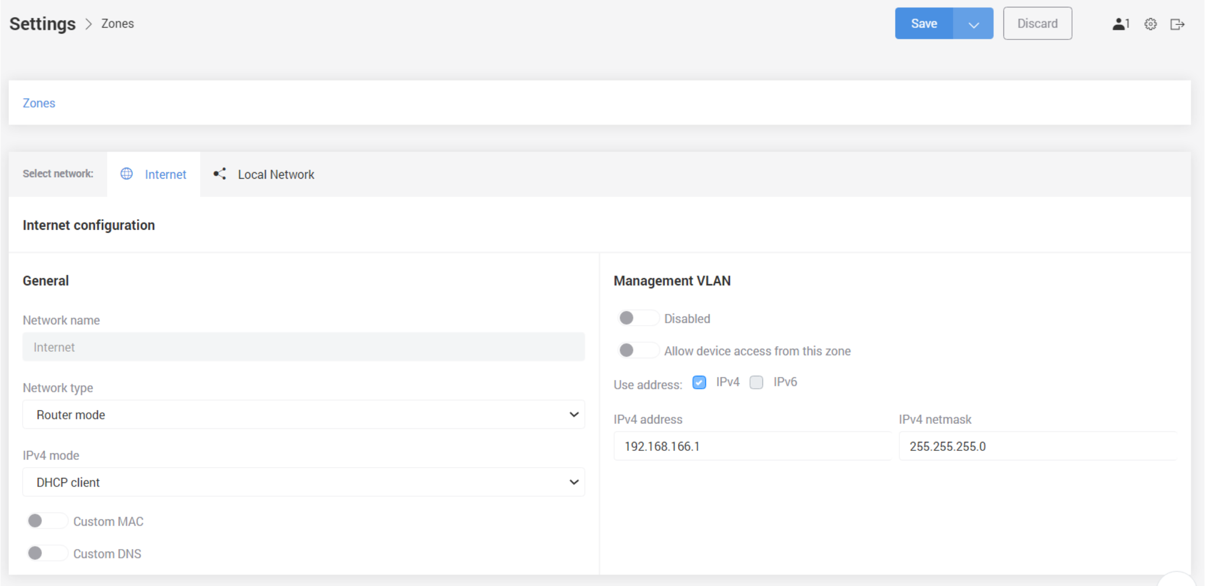
IPv4 netmask: 255.255.255.0

Settings > Network > Zone

There are two default interface type in network zones, **Internet** for WAN and **Local Network** for LAN with Router mode.

It would be only one interface in network zones, says **Internet** with AP mode.(Default is AP mode)

Internet configuration in default is defined as DHCP client. If no IP assigned by exteranl DHCP server to this interface, it will fall back to defined IP address.



Internet configuration

General

Network name: Internet

Network type: Router mode

IPv4 mode: DHCP client

○ Custom MAC

○ Custom DNS

Management VLAN

○ Disabled

○ Allow device access from this zone

Use address: ☑ IPv4 □ IPv6

IPv4 address: 192.168.166.1

IPv4 netmask: 255.255.255.0

Network name – Internet

Network type – AP mode in default, can be set the device as Router mode, AP mode and Repeater mode.

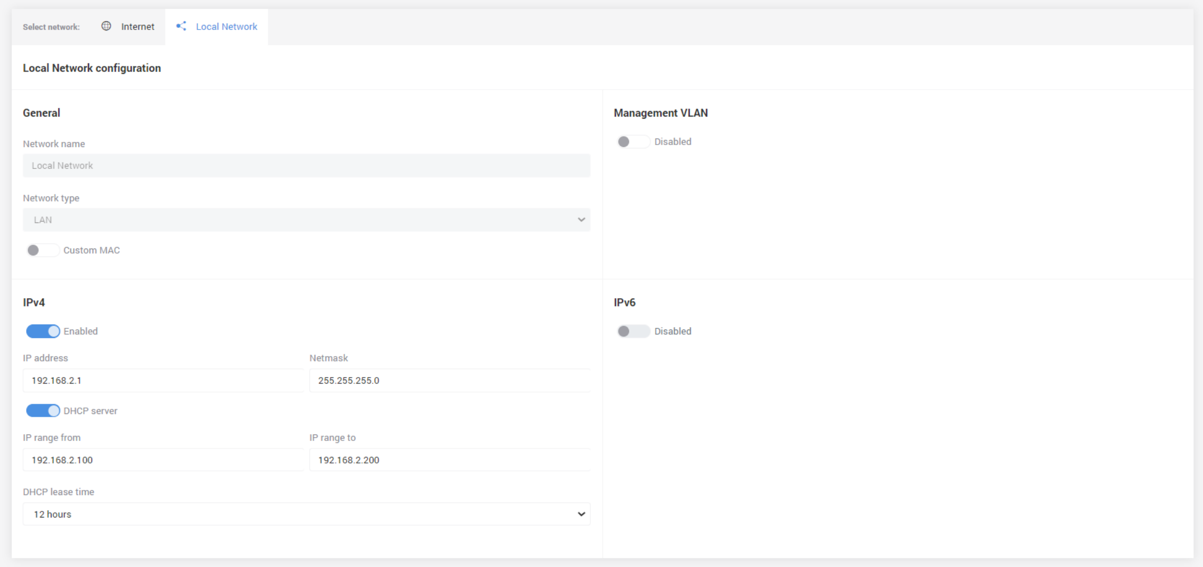
IPv4 mode – can be selected as DHCP client, static or PPPoE. Once the interface is assinged to a new IP, the web login IP address on WAN is changed accordingly.

Custom DNS – a DNS server can be specified.

Custom MAC – the MAC address of physical Ethernet port can be changed to meet network setting.

Management VLAN – disabled in default. Can be enabled to define VLAN IP addresses and ID.

Local Network configuration in default is defined as a IPv4 with DHCP server enabled. Only show when the Network type set as Router mode.



Local Network configuration

General

Network name: Local Network

Network type: LAN

Custom MAC

Management VLAN: Disabled

IPv4: Enabled

IP address: 192.168.2.1

Netmask: 255.255.255.0

DHCP server: Enabled

IP range from: 192.168.2.100

IP range to: 192.168.2.200

DHCP lease time: 12 hours

IPv6: Disabled

General – local netowork as network name and LAN as network type in default.

Custom MAC – the MAC address of physical Ethernet port can be changed to meet network setting.

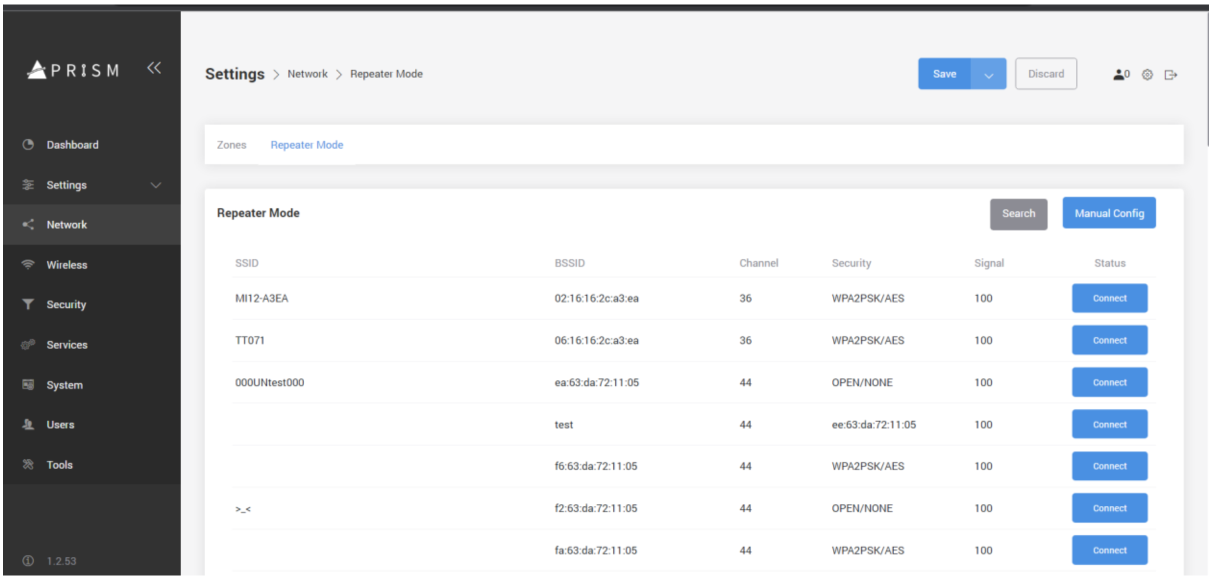
IPv4 – default is enabled with defined IP 192.168.2.1 and netmask 255.255.255.0.

DHCP server – default is enabled. IP range and lease time can be user-defined.

IPv6 – disabled in default.

Settings > Network > Repeater Mode

Only work when the Network type set as Repeater mode



Repeater Mode

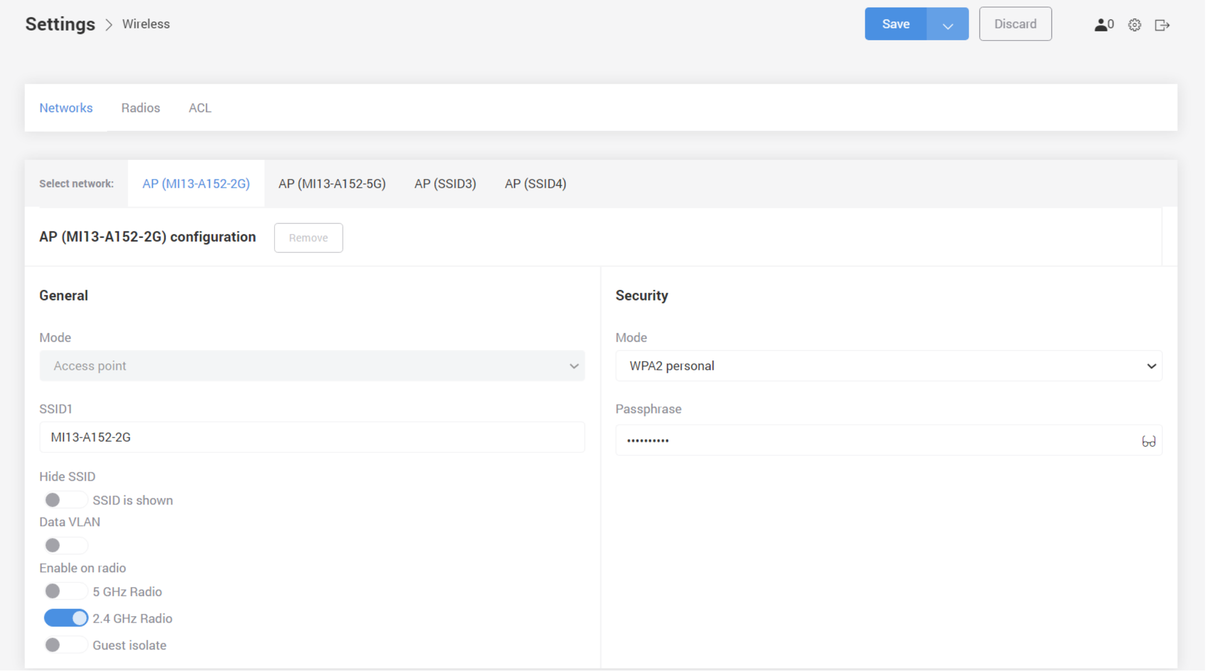
SSID	BSSID	Channel	Security	Signal	Status
MI12-A3EA	02:16:16:2c:a3:ea	36	WPA2PSK/AES	100	Connect
TT071	06:16:16:2c:a3:ea	36	WPA2PSK/AES	100	Connect
000UNtest000	ea:63:da:72:11:05	44	OPEN/NONE	100	Connect
	test	44	ee:63:da:72:11:05	100	Connect
	f6:63:da:72:11:05	44	WPA2PSK/AES	100	Connect
>_<	f2:63:da:72:11:05	44	OPEN/NONE	100	Connect
	fa:63:da:72:11:05	44	WPA2PSK/AES	100	Connect

Search – To site survey the available Wi-Fi networks in the environment.

Manual Config – To input the SSID, Band and Security manually for the desired Wi-Fi network.

Settings > Wireless

All wireless settings can be configured from here.



AP (MI13-A152-2G) configuration

General

Mode: Access point

SSID1: MI13-A152-2G

Hide SSID: SSID is shown

Data VLAN

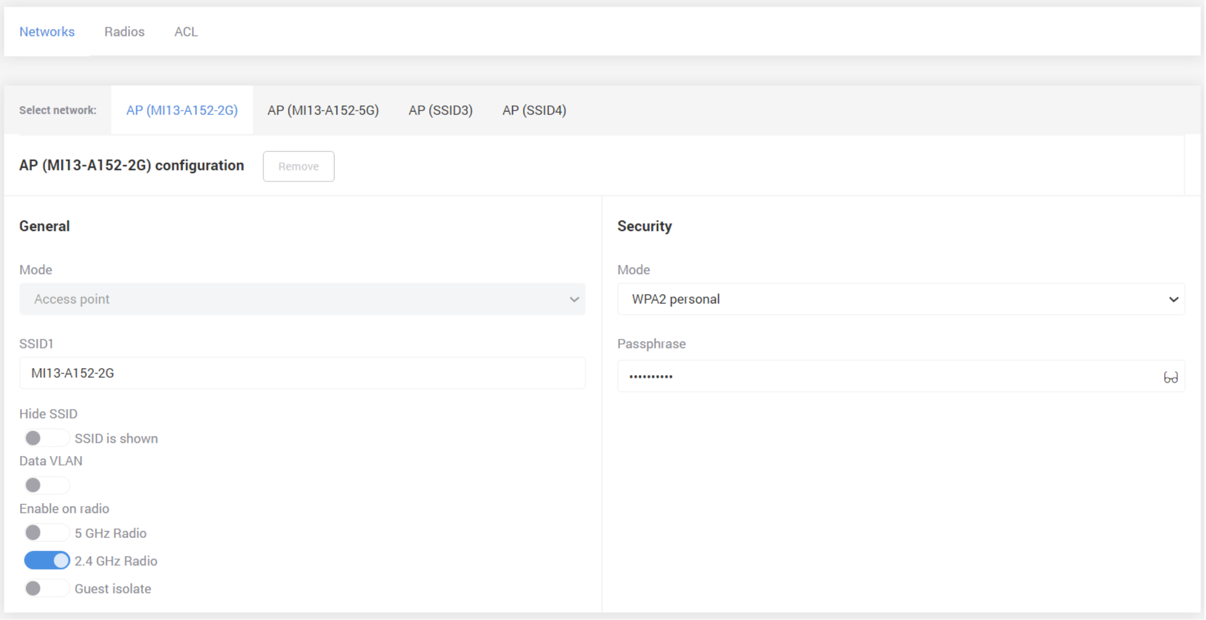
Enable on radio: 5 GHz Radio; 2.4 GHz Radio (on); Guest isolate

Security

Mode: WPA2 personal

Passphrase: ••••••••••

Select Network page is to show configured SSID and security mode. There are two pre-defined SSIDs and two user-defined SSIDs.



AP (MI13-A152-2G) configuration

General

Mode: Access point

SSID1: MI13-A152-2G

Hide SSID: SSID is shown

Data VLAN

Enable on radio: 5 GHz Radio; 2.4 GHz Radio (on); Guest isolate

Security

Mode: WPA2 personal

Passphrase: ••••••••••

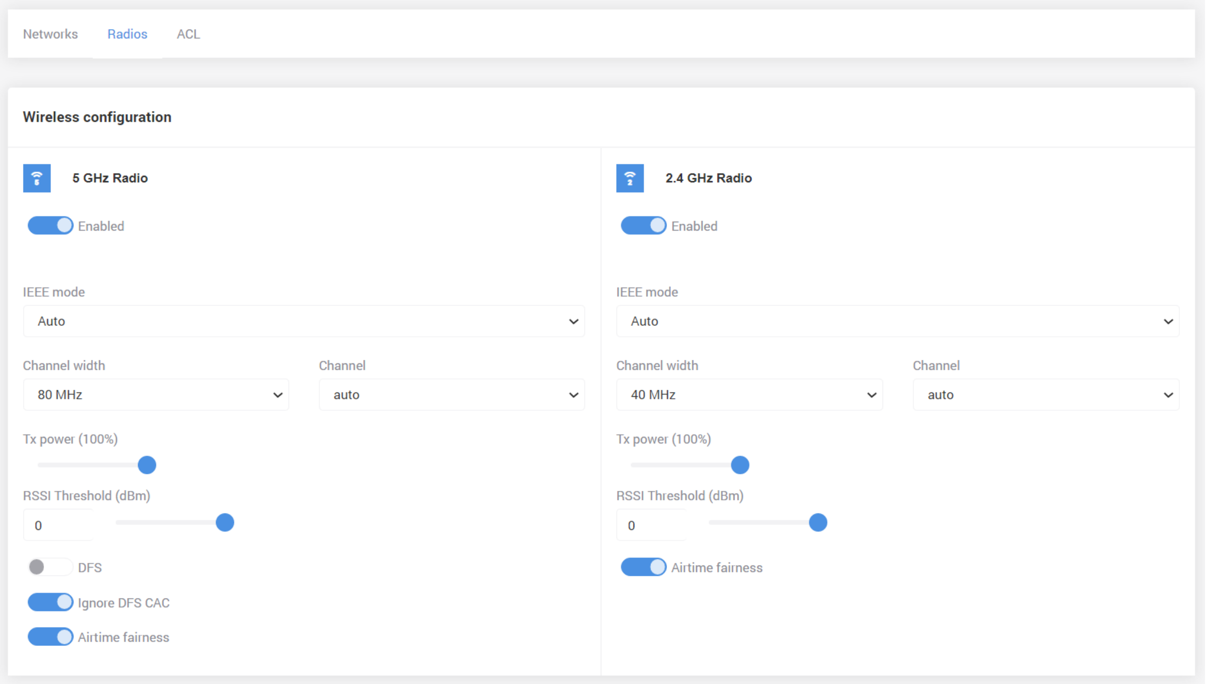
General – show the AP’s SSID name. Can be selected to hide SSID, set DATA VLAN, and assigned to radio.

Security – WAP2 in default. Choose the other secure mode to protect wireless connections.

Guest Isolate – default is disabled

ℹ	Guest isolate will only allow the traffic towards whitelisted destination MAC addresses. This is to isolate guest clients in accessing other devices except for the network gateway. This will efficiently block any undesirable connection attempt within the network.

Radio configuration page shows you the radio parameters for each radio.



Networks Radios ACL

Wireless configuration

5 GHz Radio

Enabled

IEEE mode: Auto

Channel width: 80 MHz

Channel: auto

Tx power (100%)

RSSI Threshold (dBm): 0

DFS

Ignore DFS CAC

Airtime fairness

2.4 GHz Radio

Enabled

IEEE mode: Auto

Channel width: 40 MHz

Channel: auto

Tx power (100%)

RSSI Threshold (dBm): 0

Airtime fairness

5 GHz Radio – Wi-Fi 5GHz 2x2 radio

2.4 GHz Radio – Wi-Fi 2.4GHz 2x2 radio

Enable – default is **enabled**

IEEE mode – **Auto** in default. 4 modes can be chosen: Auto, 802.11ac, 802.11ax or 802.11n.

Channel width – 4 channel width parameters can be chosen from drop-down menu: 20MHz, 40MHz and 80MHz, depending on radio’s capability.

Channel – **Auto** in default. Channel can be selected from drop-down menu.

Tx power (100%) – 100% in default, from minimal 10% to maximum 100%.

RSSI Threshold (dBm) – 0 in default, from minimal -99 to maximum 0 dBm.

ℹ	If the connected wireless client signal strength is less than the RSSI threshold setting, AP would disassociate the client automatically. 0 means disable.

DFS – default is disabled

ℹ	In many countries, regulatory requirements may limit the number of 5 GHz channels available or place additional restrictions on their use because the spectrum is shared with other technologies and services. For instance, some of the Unlicensed National Information Infrastructure (U-NII) bands are used by radar systems. Wi-Fi networks operating in those bands are required to employ a radar detection and avoidance capability.

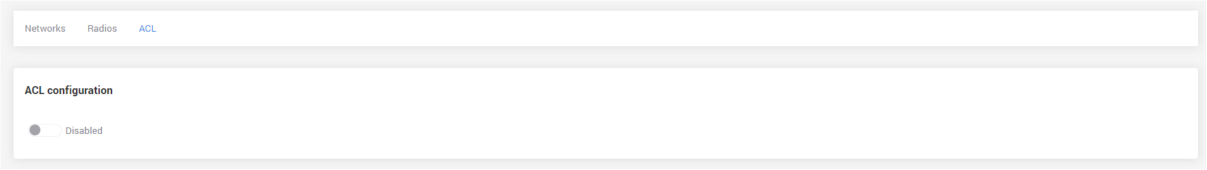
Ignore DFS CAC – default is disabled

ℹ	Channel Availability Check (CAC) is used to detect radar signals. The radio scans a target dynamic frequency selection (DFS) channel for radar signals for 60 seconds. After the 60-second scan, if no radar signals are detected, the radio can transmit on the target DFS channel. During the 60-second scan, if radar signals are detected on a target DFS channel, the radio must move to another DFS channel and restart the 60-second CAC.

Airtime fairness – default is enabled

ℹ	Airtime Fairness ensures that every client has equal access to air time, regardless of client capability (for example, operating system, 802.11 mode, low RSSI). The regulated wireless spectrum, where all wireless communication takes place, is shared amongst all clients on the wireless MI13 In-Wall AP as well as neighboring APs on the same channel.

ACL configuration page displays the deny and allow list.



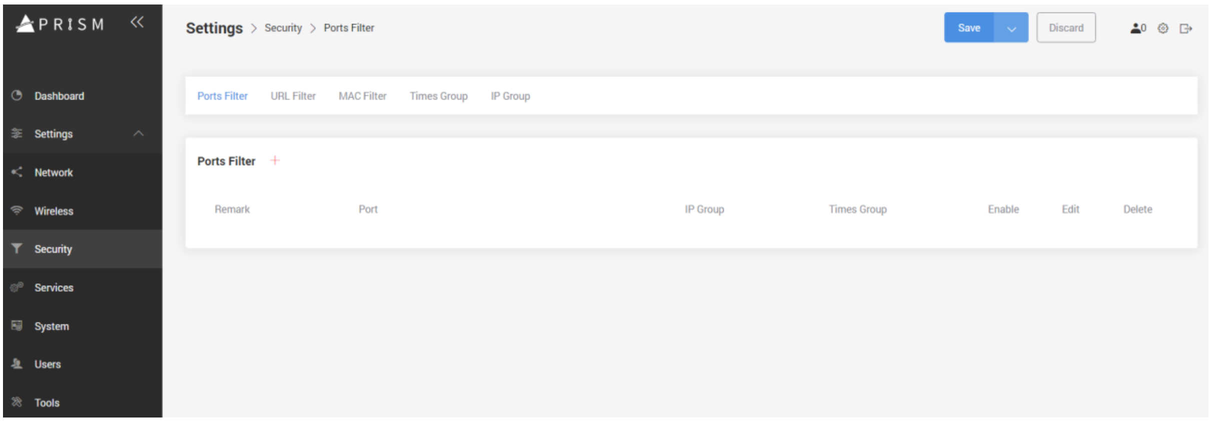
ACL configuration

○ Disabled

ACL configuration – disabled in default. You can add MAC address in the deny or allow list.

Settings > Security

The feature of security allows network administrator to set up filter rules for the MI13 In-Wall AP to limit ports, URLs, and MAC addresses for specific IP ranges or periods of time.



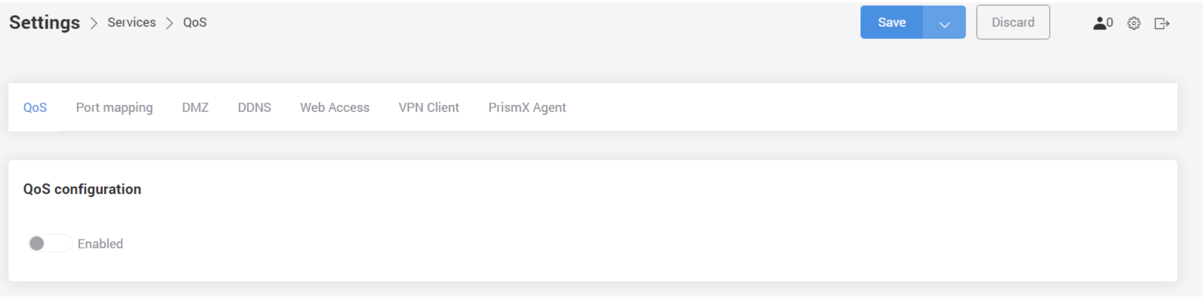
Settings > Security > Ports Filter

Ports Filter +

Remark	Port	IP Group	Times Group	Enable	Edit	Delete

Settings > Services

The features of services allow network administrator to set up the MI13 In-Wall AP with more network parameters.

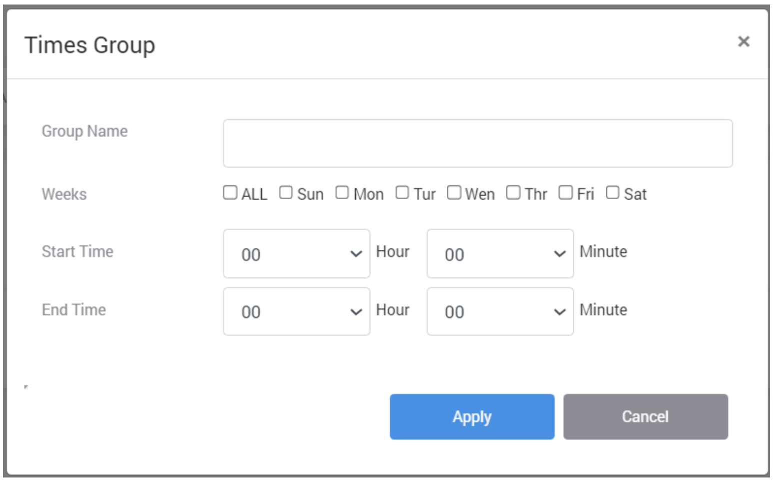


QoS configuration

Enabled

Settings > Security > Time Group

You can set the time schedule to apply the filter rule here.



Times Group

Group Name

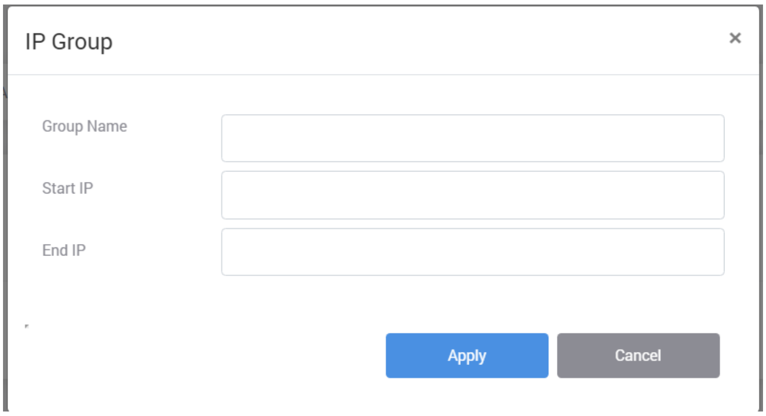
Weeks □ ALL □ Sun □ Mon □ Tur □ Wen □ Thr □ Fri □ Sat

Start Time 00 Hour 00 Minute

End Time 00 Hour 00 Minute

Settings > Security > IP Group

You can set the IP ranges to apply the filter rule here.



IP Group

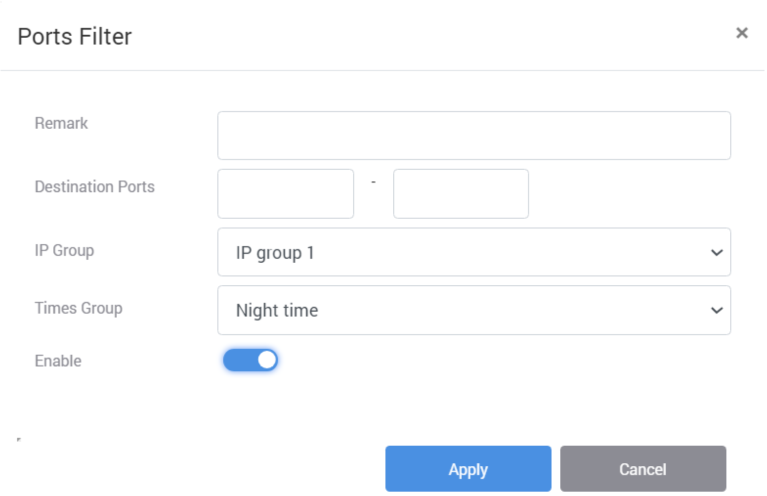
Group Name

Start IP

End IP

Settings > Security > Ports Filter

The ports filter allows you to set rules that determine which network ports are blocked for outgoing traffic for specific IPs during specific periods of time.



Ports Filter

Remark:

Destination Ports: -

IP Group: IP group 1

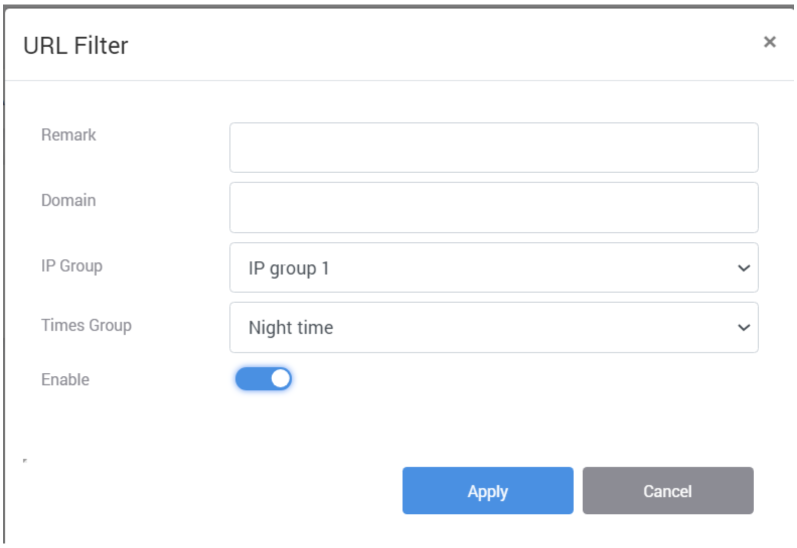
Times Group: Night time

Enable

To set ports filter, it needs to set IP group and Times group First.

Settings > Security > URL Filter

The URL filter allows you to set rules that determine which URLs are blocked from access for specific IPs during specific periods of time.



URL Filter

Remark:

Domain:

IP Group: IP group 1

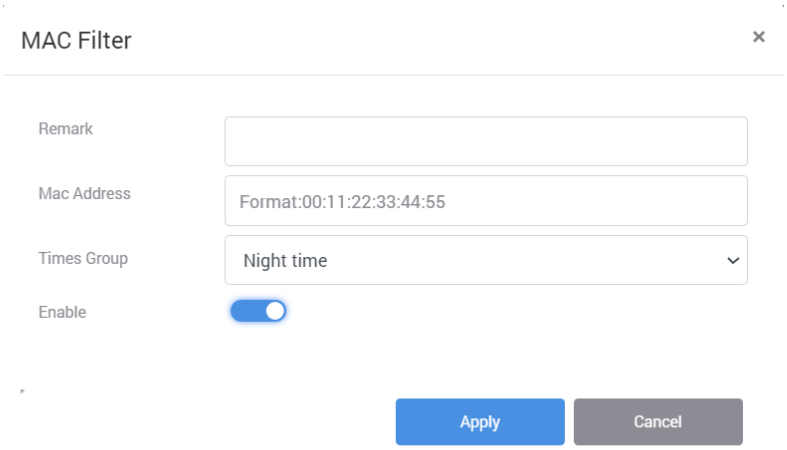
Times Group: Night time

Enable

To set ports filter, it needs to set IP group and Times group First.

Settings > Security > MAC Filter

The MAC filter allows you to set rules that determine which MAC addresses are blocked from access during specific periods of time



MAC Filter

Remark:

Mac Address: Format:00:11:22:33:44:55

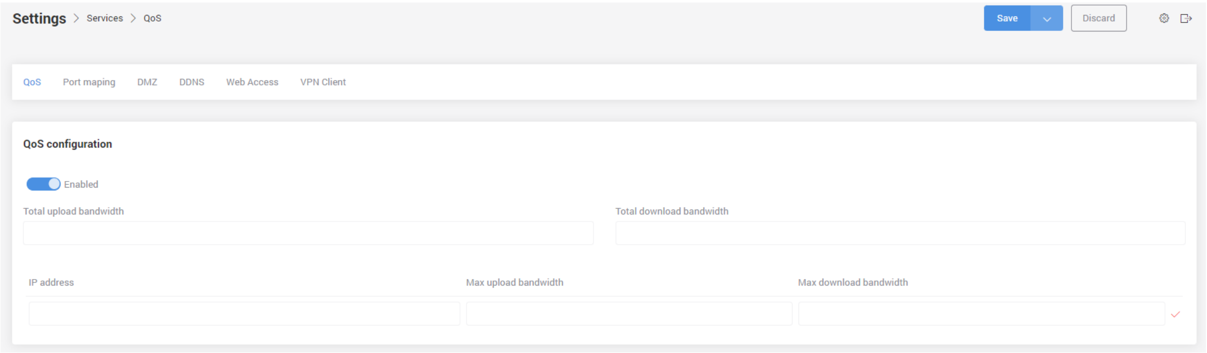
Times Group: Night time

Enable: ●

To set ports filter, it needs to set Times group First.

Settings > Services > QoS

Quality of Service (QoS) allows you prioritize the bandwidth for specific connected users.



Settings > Services > QoS

QoS configuration

● Enabled

Total upload bandwidth

Total download bandwidth

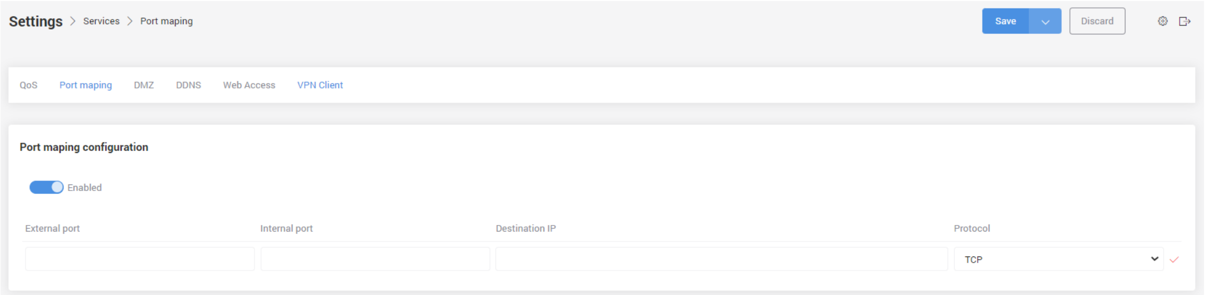
IP address	Max upload bandwidth	Max download bandwidth

QoS – default is disabled. When enabled, specify the total bandwidth of both uplink and downlink of the MI13 In-Wall AP, and define user’s IP with assigned maximum bandwidth of both uplink and downlink.

Bandwidth is also called data rate or throughput, in KB.

Settings > Services > Port maping

Port maping or port forward is to redirect a request from one address and port number combination to another while the packets are traversing a MI13 router mode.



Settings > Services > Port maping

Port maping configuration

● Enabled

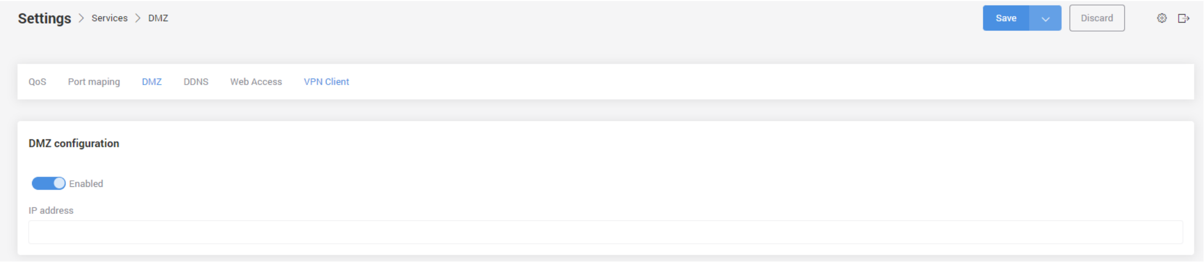
External port	Internal port	Destination IP	Protocol
			TCP

Port mapping configuration – default is disabled. When enabled, specify the external port and mapped internal port, destination IP and protocol.

ℹ	This function is most commonly used to make services on a host residing on a protected or masqueraded (internal) network available to hosts on the opposite side of the router (external network), by remapping the destination IP address and port number of the communication to an internal host.

Settings > Services > DMZ

Demilitarized Zone (DMZ) configuration allows you to segment a portion of your network to receive all inbound TCP/UDP ports. It opens up all the ports for one IP address on the LAN. DMZ can be used as an alternative for port forwarding all ports.



DMZ configuration

Enabled

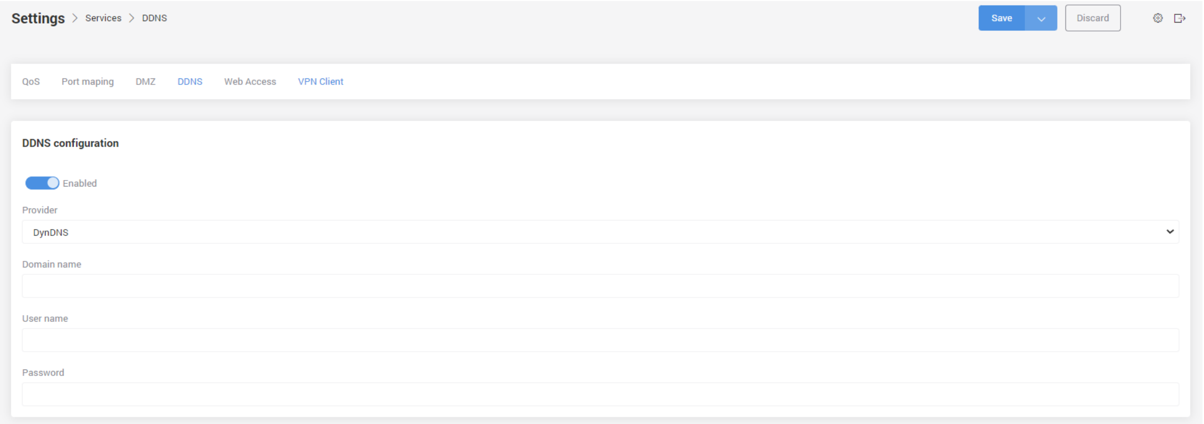
IP address

DMZ configuration – default is disabled. When enabled, specify the internal IP address.

ℹ	DMZ can be used as an alternative for port forwarding all ports.

Settings > Services > DDNS

The Dynamic Domain Name System (DDNS) is an advanced function that assigns your MI13 a fixed domain name even though you are using a dynamic Internet IP Address. DDNS keeps DNS records automatically up to date when MI13's WAN IP address changes.



DDNS configuration

Enabled

Provider

DynDNS

Domain name

User name

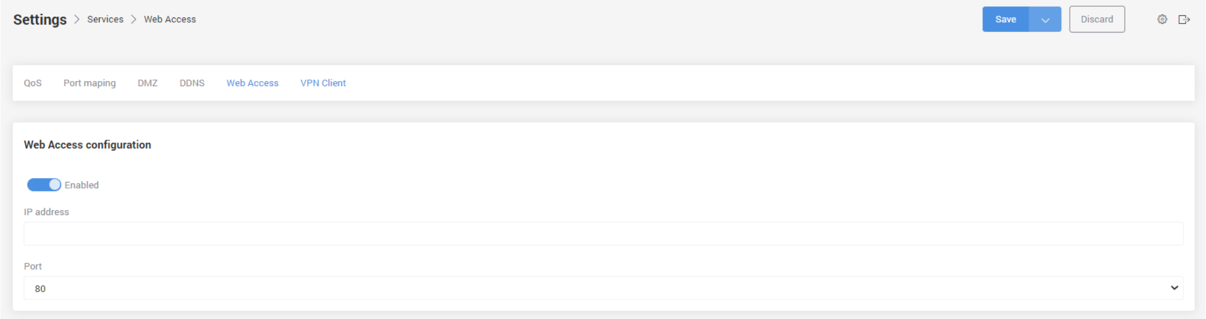
Password

DDNS configuration – default is disabled. When enabled, specify DDNS provider, Domain name and User name and password.

ℹ	Before configuring DDNS, you will need to register an effective account from DDNS providers (DynDNS or TZO).

Settings > Services > Web Access

It allows to define IP and port of web access on WAN.



Web Access configuration

Enabled

IP address

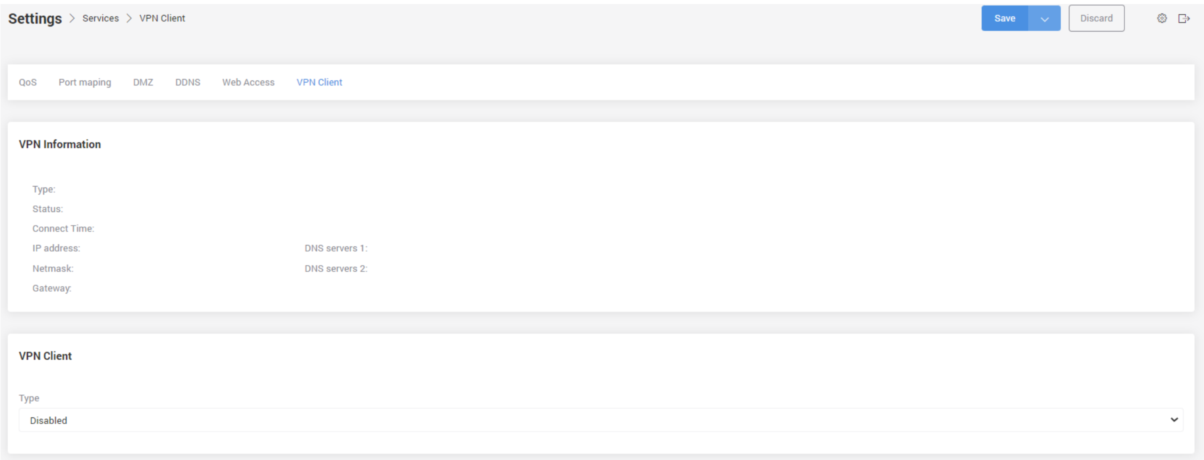
Port

80

Web Access configuration – default is disabled. When enabled, specify IP and port for accessing web management page remotely.

Settings > Services > VPN Client

Virtual Private Network (VPN) client is used to establish a secure connection between the MI13 In-Wall AP and a VPN server.



VPN Information

Type:
Status:
Connect Time:
IP address: DNS servers 1:
Netmask: DNS servers 2:
Gateway:

VPN Client

Type

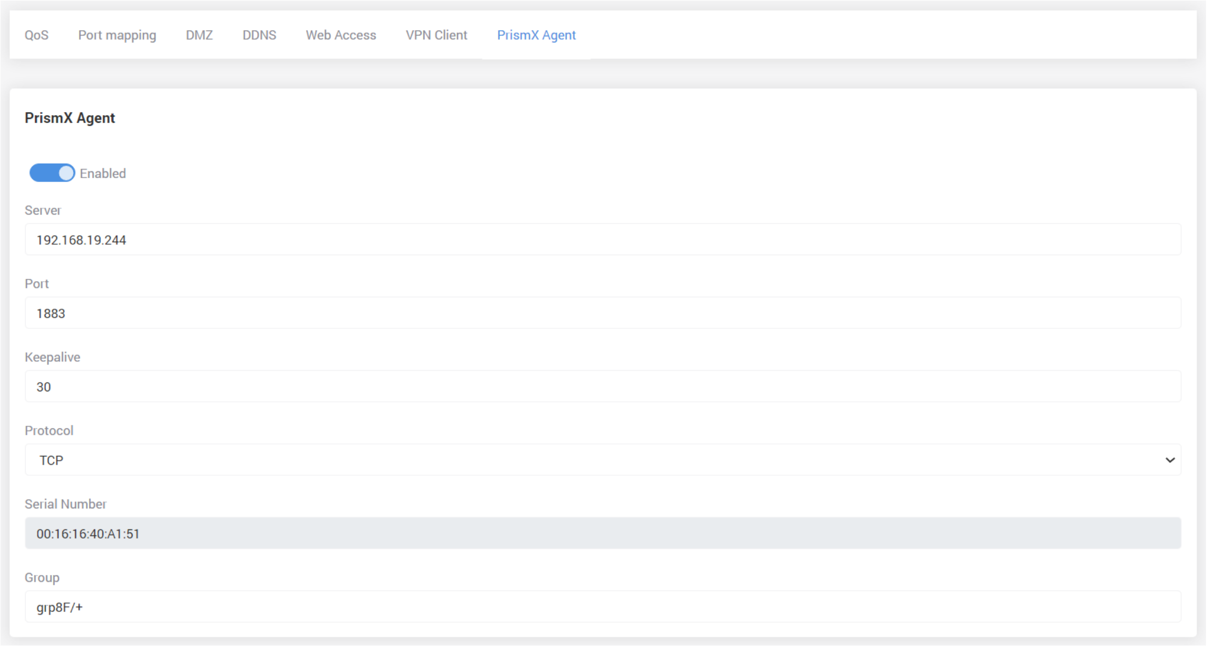
Disabled

VPN Client – default is disabled. Two VPN client types can be selected from drop-down menu: PPTP and L2TP. Specify VPN server’s IP and login credentials.

ℹ	After establishing connection to VPN server, you can see the VPN connection information including IP, gateway and DNS.

Settings > Services > PrismX Agent

It shows the PrismX agent and server information.



PrismX Agent

Enabled

Server: 192.168.19.244

Port: 1883

Keepalive: 30

Protocol: TCP

Serial Number: 00:16:16:40:A1:51

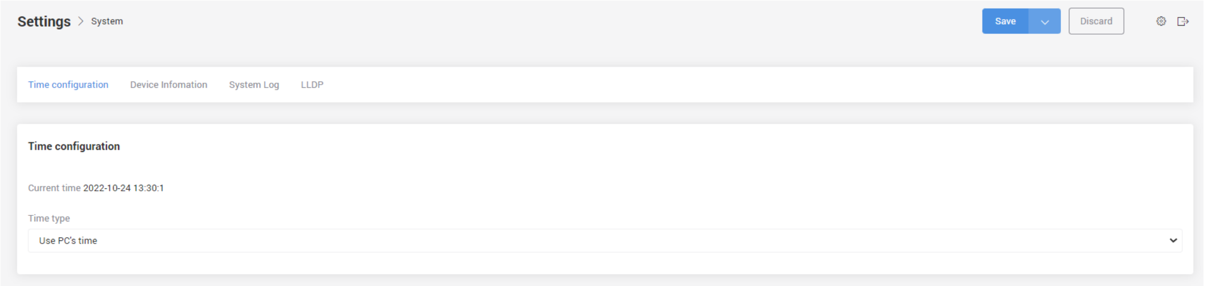
Group: grp8F/+

PrismX Agent – specify PrismX Controller's IP address, and related network parameters, including port protocol, serial number and group.

PrismX is a central management system for managing Wi-Fi network. PrismX Controller can be deployed on an on-site PC, Mac, or Linux machine; in a private cloud; or using a public cloud service. Network administrator can manage Wi-Fi network from PrismX Controller's dashboard with real-time analytics including signal quality, client count, wireless latency, channel utilization, network throughput as well as individual wireless clients.

Settings > System

The system related settings can be configured at this page.



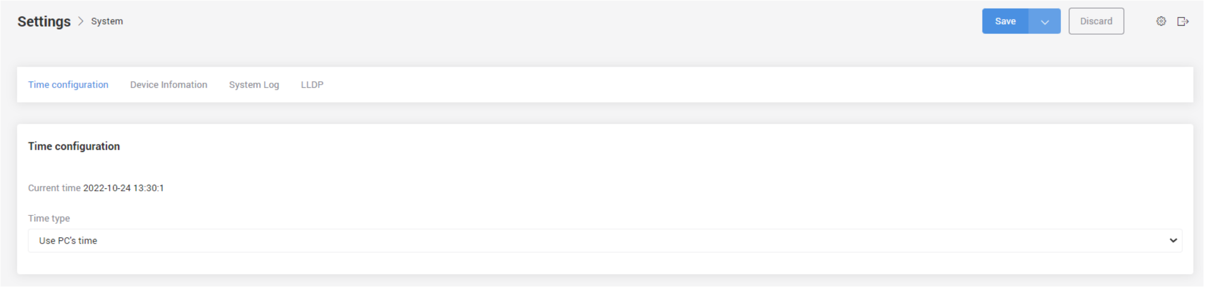
Time configuration

Current time 2022-10-24 13:30:1

Time type: Use PC's time

Settings > System > Time configuration

You can define MI13's system time at the page.



Time configuration

Current time 2022-10-24 13:30:1

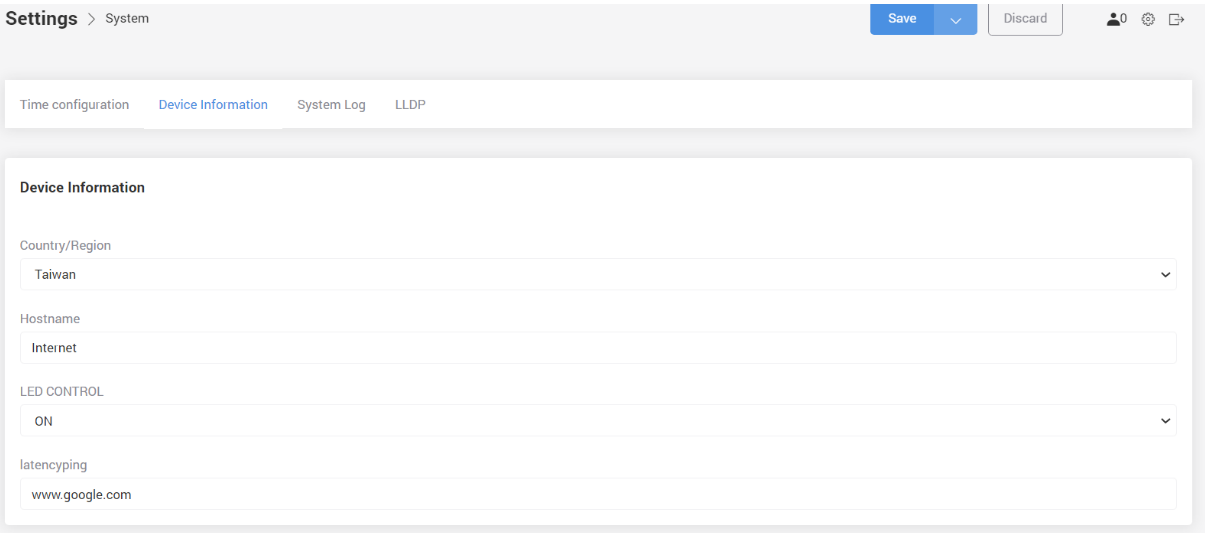
Time type

Use PC's time

Time configuration – default is “Use PC’s time”. You can also select “Auto sync NTP time” from drop-down menu.

Settings > System > Device information

You can define MI13’s device information at the page.



Device Information

Country/Region

Taiwan

Hostname

Internet

LED CONTROL

ON

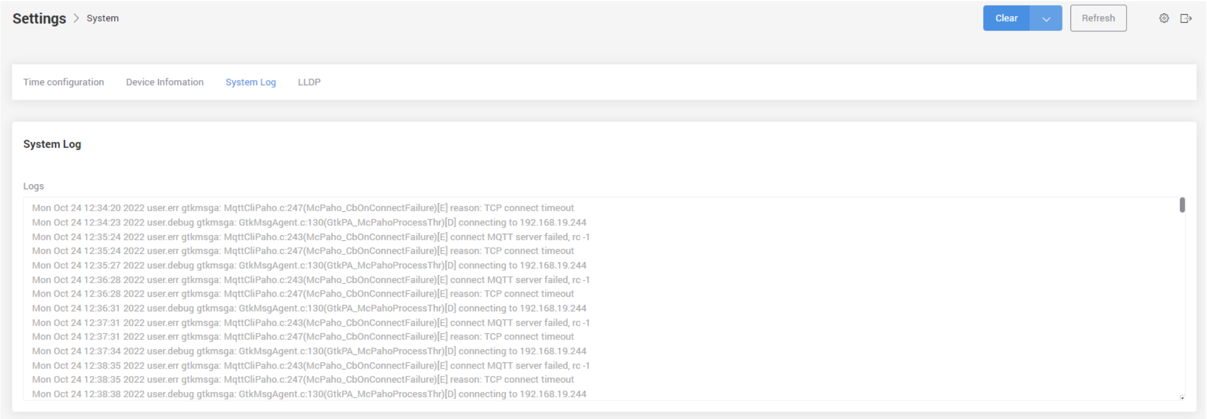
latencyping

www.google.com

Device information – country/region, hostname, LED control, and latencyping can be set up here.

Settings > System > System log

System log is displayed at this page.



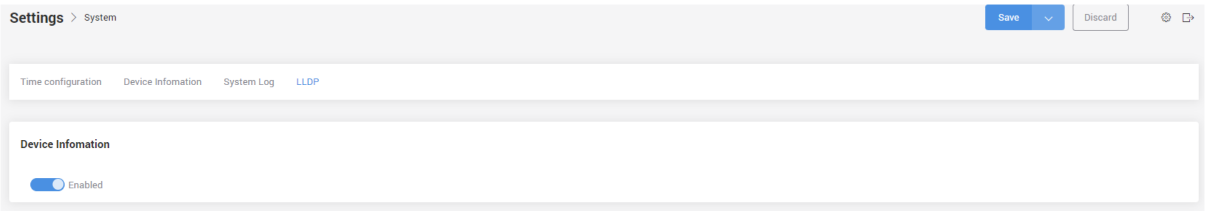
System Log

Logs

```
Mon Oct 24 12:34:20 2022 user.err gtkmsga: MqttCliPaho.c:247(McPaho_CbOnConnectFailure)[E] reason: TCP connect timeout
Mon Oct 24 12:34:23 2022 user.debug gtkmsga: GtkMsgAgent.c:130(GtkPA_McPahoProcessThr)[D] connecting to 192.168.19.244
Mon Oct 24 12:35:24 2022 user.err gtkmsga: MqttCliPaho.c:243(McPaho_CbOnConnectFailure)[E] connect MQTT server failed, rc -1
Mon Oct 24 12:35:24 2022 user.err gtkmsga: MqttCliPaho.c:247(McPaho_CbOnConnectFailure)[E] reason: TCP connect timeout
Mon Oct 24 12:35:27 2022 user.debug gtkmsga: GtkMsgAgent.c:130(GtkPA_McPahoProcessThr)[D] connecting to 192.168.19.244
Mon Oct 24 12:36:28 2022 user.err gtkmsga: MqttCliPaho.c:243(McPaho_CbOnConnectFailure)[E] connect MQTT server failed, rc -1
Mon Oct 24 12:36:28 2022 user.err gtkmsga: MqttCliPaho.c:247(McPaho_CbOnConnectFailure)[E] reason: TCP connect timeout
Mon Oct 24 12:36:31 2022 user.debug gtkmsga: GtkMsgAgent.c:130(GtkPA_McPahoProcessThr)[D] connecting to 192.168.19.244
Mon Oct 24 12:37:31 2022 user.err gtkmsga: MqttCliPaho.c:243(McPaho_CbOnConnectFailure)[E] connect MQTT server failed, rc -1
Mon Oct 24 12:37:31 2022 user.err gtkmsga: MqttCliPaho.c:247(McPaho_CbOnConnectFailure)[E] reason: TCP connect timeout
Mon Oct 24 12:37:34 2022 user.debug gtkmsga: GtkMsgAgent.c:130(GtkPA_McPahoProcessThr)[D] connecting to 192.168.19.244
Mon Oct 24 12:38:35 2022 user.err gtkmsga: MqttCliPaho.c:243(McPaho_CbOnConnectFailure)[E] connect MQTT server failed, rc -1
Mon Oct 24 12:38:35 2022 user.err gtkmsga: MqttCliPaho.c:247(McPaho_CbOnConnectFailure)[E] reason: TCP connect timeout
Mon Oct 24 12:38:38 2022 user.debug gtkmsga: GtkMsgAgent.c:130(GtkPA_McPahoProcessThr)[D] connecting to 192.168.19.244
```

Settings > System > LLDP

Link Layer Discovery Protocol LLDP) is used by MI13 In-Wall AP for advertising their identity, capabilities, and neighbors on a local area network based on IEEE 802 technology.



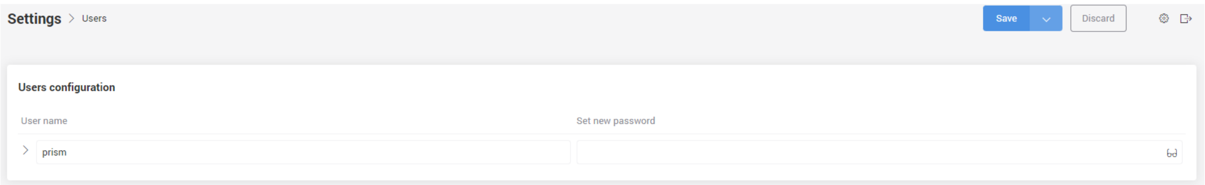
Device Infomation

Enabled

LLDP – default is disabled.

Settings > Users

Users configuration displays the username and password of web management page.



Users configuration

User name: prism

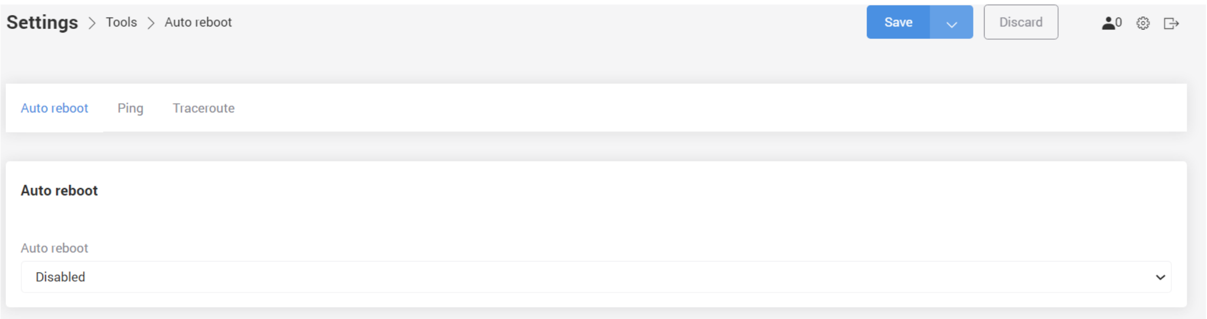
Set new password:

User name – default is “prism”.

Set new password – default is “prism”.

Settings > Tools

Built-in some tools that help to debug the connection.

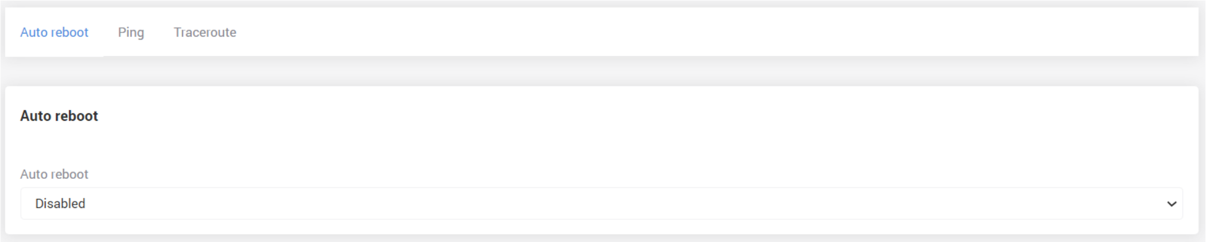


Auto reboot

Auto reboot: Disabled

Settings > Tools > Auto Reboot

This function allows you to define the periodical time to reboot MI13 In-Wall AP.

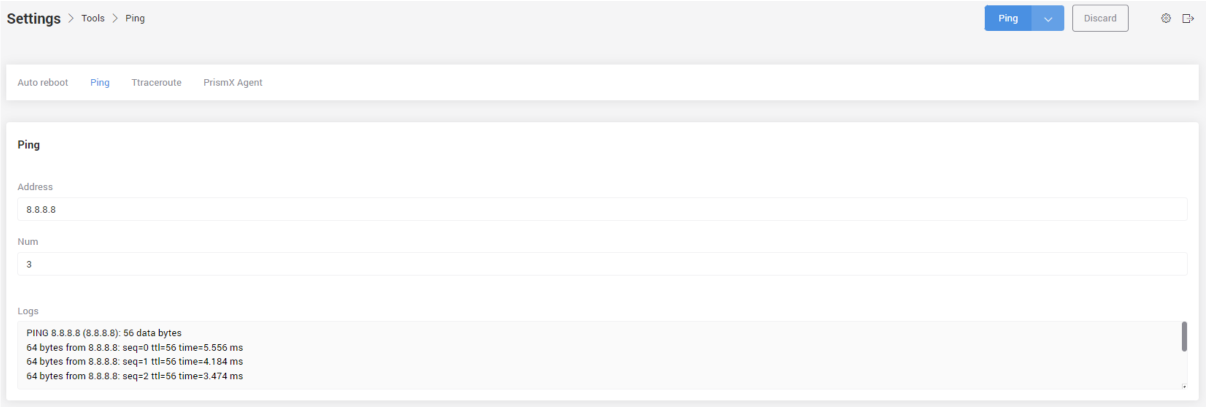


Auto reboot

Auto reboot: Disabled

Settings > Tools > Ping

The Ping function can verify wehther a domain/server is operating and network accessible.



Ping

Address: 8.8.8.8

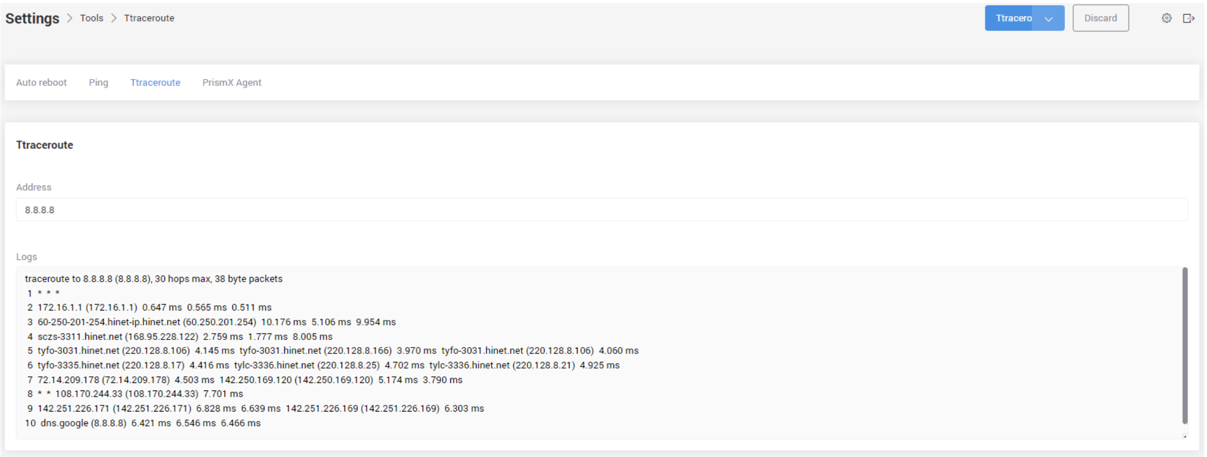
Num: 3

Logs

```
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=56 time=5.556 ms
64 bytes from 8.8.8.8: seq=1 ttl=56 time=4.184 ms
64 bytes from 8.8.8.8: seq=2 ttl=56 time=3.474 ms
```

Settings > Tools > Traceroute

The Traceroute is a utility that uses ICMP packets to record the route through the internet.



Ttraceroute

Address: 8.8.8.8

Logs

```
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 38 byte packets
 1  * * *
 2  172.16.1.1 (172.16.1.1)  0.647 ms  0.565 ms  0.511 ms
 3  60-250-201-254.hinet-ip.hinet.net (60.250.201.254)  10.176 ms  5.106 ms  9.954 ms
 4  sczs-3311.hinet.net (168.95.228.122)  2.759 ms  1.777 ms  8.005 ms
 5  tyfo-3031.hinet.net (220.128.8.106)  4.145 ms  tyfo-3031.hinet.net (220.128.8.166)  3.970 ms  tyfo-3031.hinet.net (220.128.8.106)  4.060 ms
 6  tyfo-3335.hinet.net (220.128.8.17)  4.416 ms  tylc-3336.hinet.net (220.128.8.25)  4.702 ms  tylc-3336.hinet.net (220.128.8.21)  4.925 ms
 7  72.14.209.178 (72.14.209.178)  4.503 ms  142.250.169.120 (142.250.169.120)  5.174 ms  3.790 ms
 8  * *  108.170.244.33 (108.170.244.33)  7.701 ms
 9  142.251.226.171 (142.251.226.171)  6.828 ms  6.639 ms  142.251.226.169 (142.251.226.169)  6.303 ms
10  dns.google (8.8.8.8)  6.421 ms  6.546 ms  6.466 ms
```

Traceroute – specify the address or domain name of a server and click Traceroute button on top-right to perform traceroute function. The traceroute result will be displayed in logs.

Appendix

FCC/IC Statement

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:
Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Country Code selection feature to be disabled for products marketed to the US/CANADA

Industry Canada statement:

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions:

(1) This device may not cause interference
(2) This device must accept any interference, including interference that may cause undesired operation of the device

L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :
(1) L'appareil ne doit pas produire de brouillage;
(2) L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Caution:
the device for operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;

Avertissement:
les dispositifs fonctionnant dans la bande de 5150 à 5250MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;

Radiation Exposure Statement:
This equipment complies with Canada radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator & your body.

Déclaration d'exposition aux radiations:
Cet équipement est conforme Canada limites d'exposition aux radiations dans un environnement non contrôlé. Cet équipement doit être installé et utilisé à distance minimum de 20 cm entre le radiateur et votre corps.