



## Table of Contents

Welcome to Custom Integration Solutions .....	4
Overview.....	4
Package Contents.....	4
Power.....	4
Indoor use only .....	4
 Device Details.....	5
Ports.....	5
LED Indicators.....	5
Buttons .....	5
 Mounting Options .....	6
Wall Mount.....	6
Ceiling Mount .....	7
Low Voltage Mounting Brackets.....	8
 Quick Setup.....	9
 Accessing the Web Interface.....	10
The Status Page.....	10
Setting the Access Point's Identity .....	11
Undo / Redo .....	12
Show / Hide Passwords .....	12
Rebooting the Device.....	12
Changing the Default Password .....	13
Setting the Time Zone.....	13
 IP Addressing .....	14
The DHCP Client Tab .....	14
Renewing the IP Address .....	14
Setting a Static IP Address.....	15

Managing Access Points with the Wireless Manager .....	17
Linking CIS Access Points to the Wi-Fi Manager.....	17
Viewing the Connected Access Points.....	18
Viewing Connected Devices.....	18
Changing the SSID of Managed Access Points .....	19
Changing the Wi-Fi Password of Managed Access Points.....	19
Configuring Access Points in Standalone Mode .....	21
Setting the Wi-Fi Password for Standalone Access Points.....	22
Enabling the Guest Network on Standalone Access Points.....	23
To change the password, click the Security Profiles tab in the Wireless menu. Click the Guest security profile and change the password, just like you did for the main network. ....	23
View Connected Devices .....	24
Setting up the Access Point as a Repeater.....	24
Tools.....	25
UPnP.....	25
Ping.....	25
IP Scan .....	26
Wireless Scanner.....	26
Troubleshooting.....	27
Warranty Information.....	29
Contact Information.....	29

## Welcome to Custom Integration Solutions

Thank you for purchasing CIS devices. Our solutions make it easy for integrators to deploy networks in home and business settings with minimal configuration. Our support team is here to assist with setting up equipment and answering your network related questions.

### Overview

CIS wireless access points provide a compact and powerful solution for your home and commercial connectivity needs. The CIS WAPXL provides the power of our ACWAP with increased range. Link it to the Wi-Fi manager and control it with your CIS router, just like our other access points.

### Package Contents



AP



PoE Injector



DC Adapter



Mounting  
Bracket



Ceiling Plate



Screw Kit



Metal Strap

### Power

The WAPXL is powered via PoE through a PoE capable router or switch, or via the included PoE injector.

The PoE input on Ether1 accepts 24V passive PoE, or 48V 802.3af/at (PoE and PoE+).

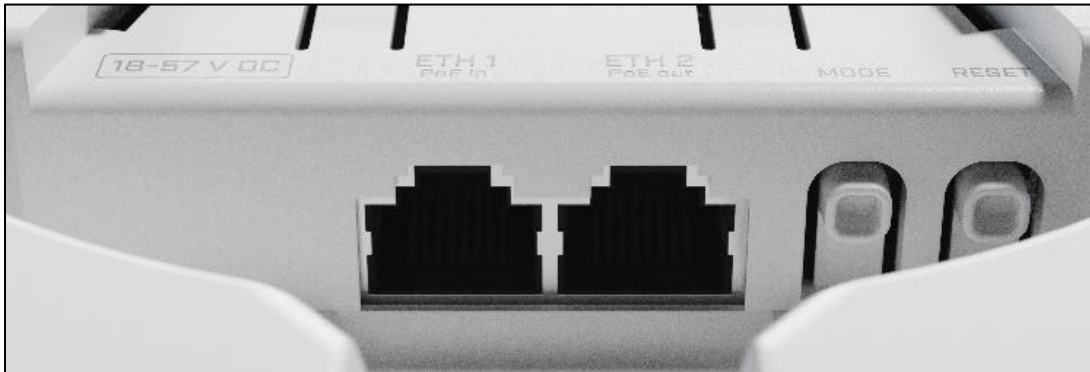
- Ether2 supports PoE passthrough (passive PoE only, up to 57V), so you can link multiple PoE devices together.

The maximum power consumption of the device is 24W with attachments, and 11W without.

### Indoor use only

The CIS-WAPXL is designed for indoor use only. Avoid installing the CIS-WAPXL in wet or damp areas.

## Device Details



### Ports

- ETHER1 (PoE in) – connect to your router or switch. Accepts passive and 802.3af/at PoE.
- ETHER2 – connect to another access point or device.
  - Can pass-through up to 57V passive PoE.

### LED Indicators

- USB (Top) – Flashes when the access point is about to be reset.
- 5G – Indicates activity on the 5 GHz interface
- 2G – Indicates activity on the 2.4 GHz interface
- E2 – Lights up when Ethernet 2 is connected. Indicates activity.
- E1 – Lights up when Ethernet 1 is connected. Indicates activity.
- PoE – Lights up when PoE is passed-through on Ether2.
- Power (bottom) – Lights up when the access point is powered.



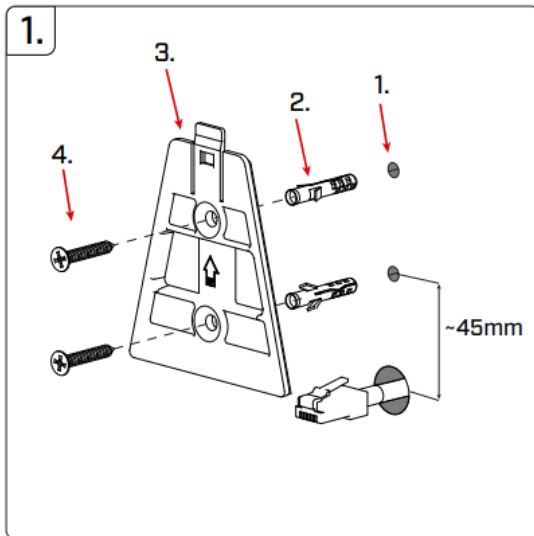
### Buttons

- Center button: Press to enable and disable the LEDs on the access point.
- Mode button (back) – Also enables and disables the LEDs on the access point.
- Reset button: Hold this button while the device is powered off, then apply power. Keeping holding until the USB LED light starts flashing, (5 seconds) then release the button to reset to the default CIS configuration. You can use this procedure if you have forgotten the password to access the device, or simply wish to return the unit to its default configuration state.

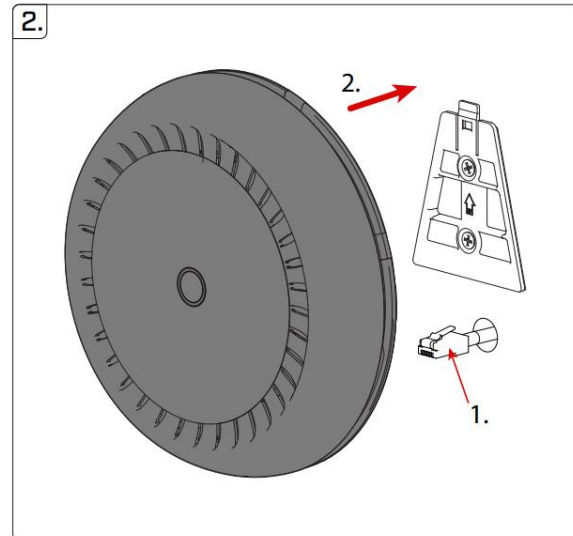
## Mounting Options

The CIS-WAPXL has multiple mounting options for walls, ceilings, and low-voltage mounting brackets.

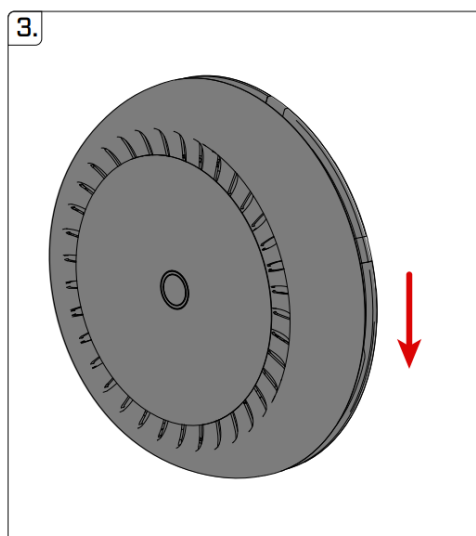
### Wall Mount



1. Drill two 4.5-5mm holes.
2. Insert the plastic anchors.
3. Place the mount on the wall.
4. Secure the mount with screws.

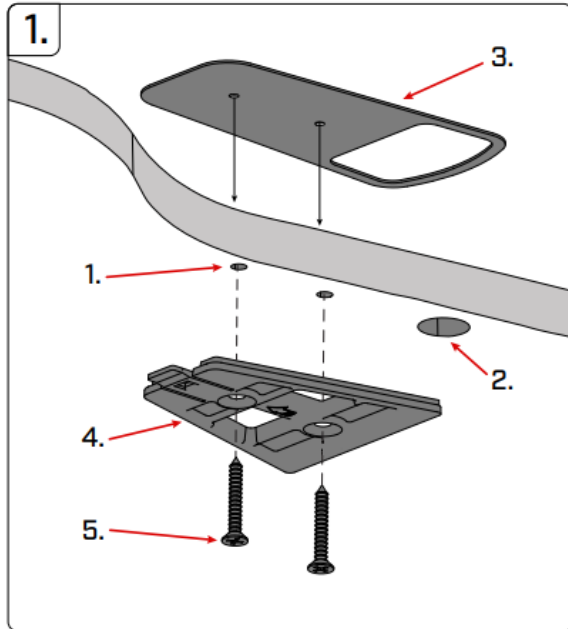


1. Plug the Ethernet cable into Ether1.
2. Move the access point into position.

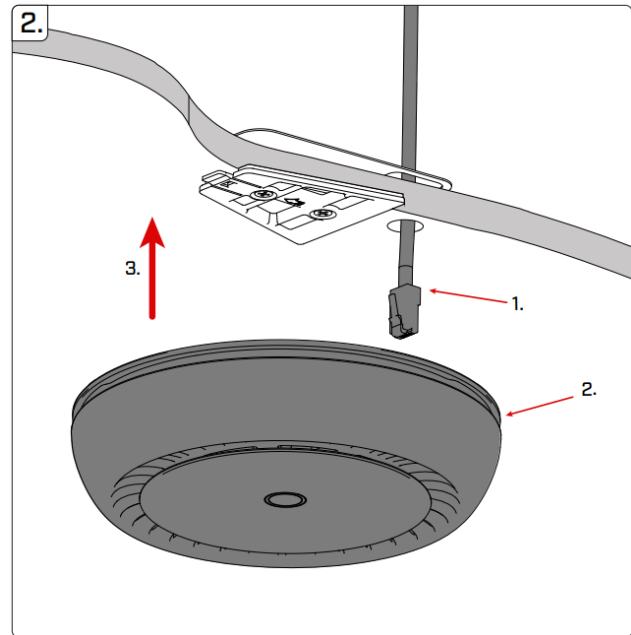


Slide the access point down until it snaps into place.

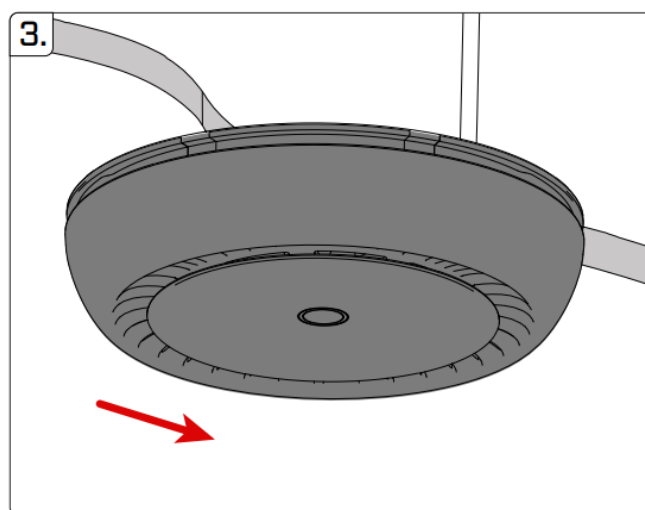
## Ceiling Mount



1. Drill two 4.5-5mm holes for the screws.
2. Drill a hole for the ethernet cable.
3. Attach the metal plate on the other side of the ceiling panel.
4. Align the access point mount with the screw holes.
5. Use the screws to tighten the mount to the plate.

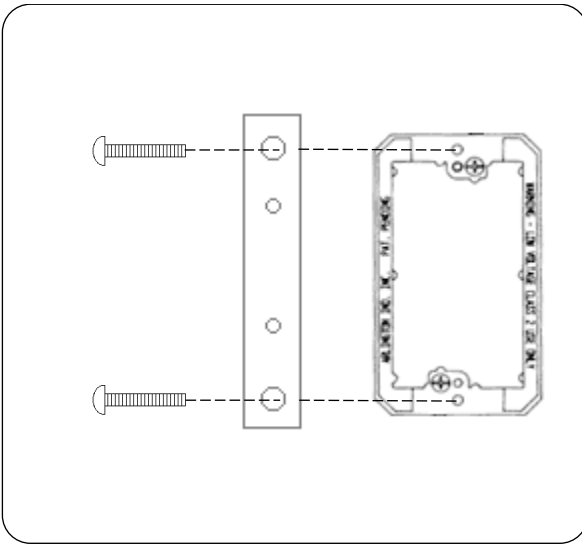


1. Thread the ethernet cable through the hole in the metal plate.
2. Insert the ethernet cable to Ether1 of the access point.
3. Position the access point ahead of the mount.

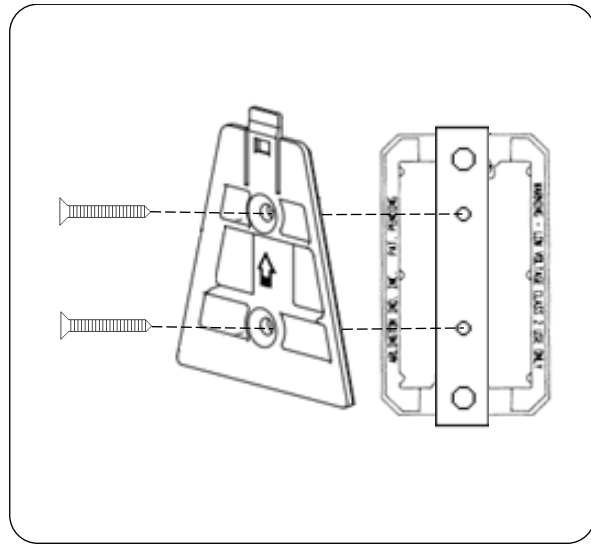


Slide the access point towards the mount until it snaps into place.

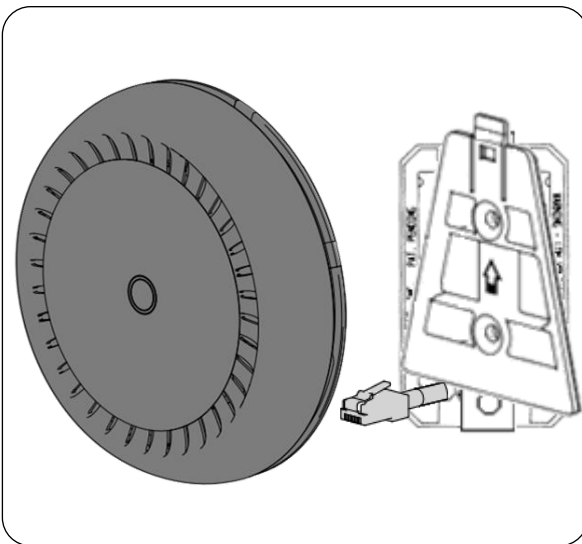
## Low Voltage Mounting Brackets



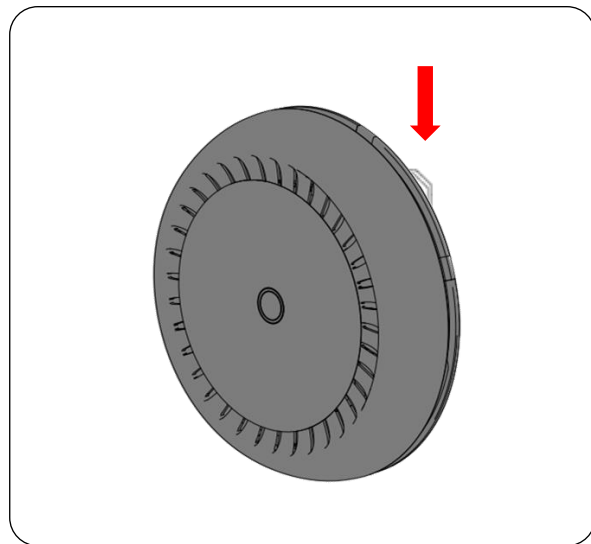
Attach the metal strip to the low voltage gang box using the included screws.



Attach the mounting bracket to the metal strip using the flathead screws.



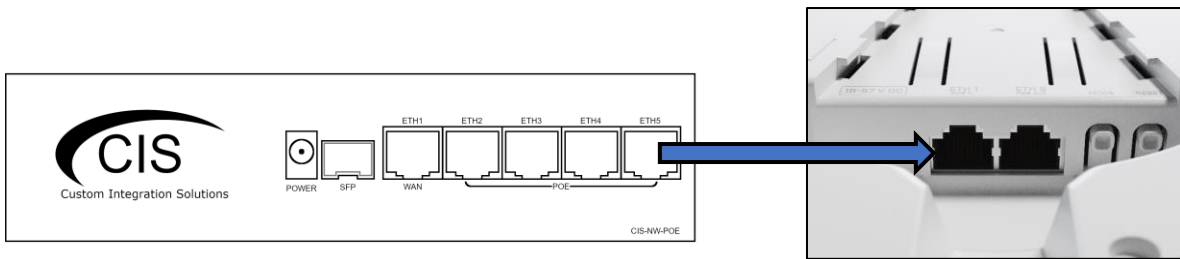
Connect the ethernet cable to Ether1 of the access point.



Slide the access point onto the mount until it snaps into place.



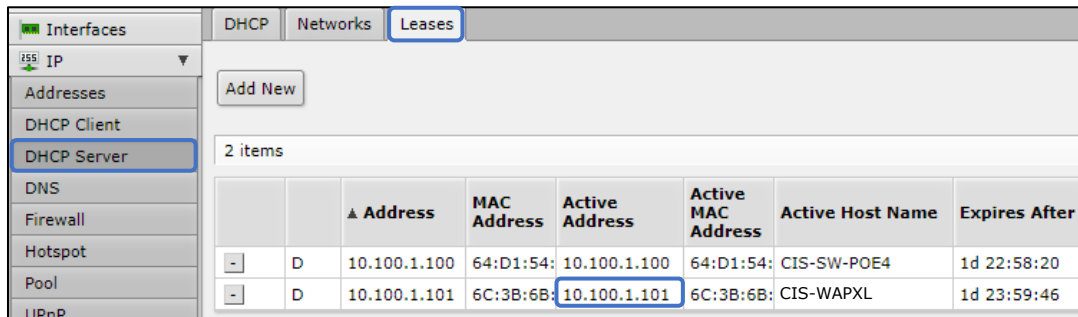
## Quick Setup



1. Connect the Ethernet cable from your router to Ether1 on the access point. If your router supports PoE, turn it on to power the device. If not, use the included PoE injector.
2. (Optional) Connect an additional access point or device to Ether2. The port is bridged, meaning it acts like a switch port. If the connected device supports passive PoE, it will be passed through to it.
3. The access point will receive an IP address via DHCP. Access the DHCP leases on your router page to find the IP address of the access point, then enter the IP address in a web browser to view the configuration (next page).

## Accessing the Web Interface

1. Connect your laptop or PC to the router.
2. Obtain the IP address of your access points. If you're using a CIS router, access the web configuration by typing 10.100.1.1 in a web browser (10.100.1.1 is the default, but some systems may be different). Once logged in with the default credentials of **cis** and **integration** as the password, select **IP > DHCP Server** and view the **Leases** tab.

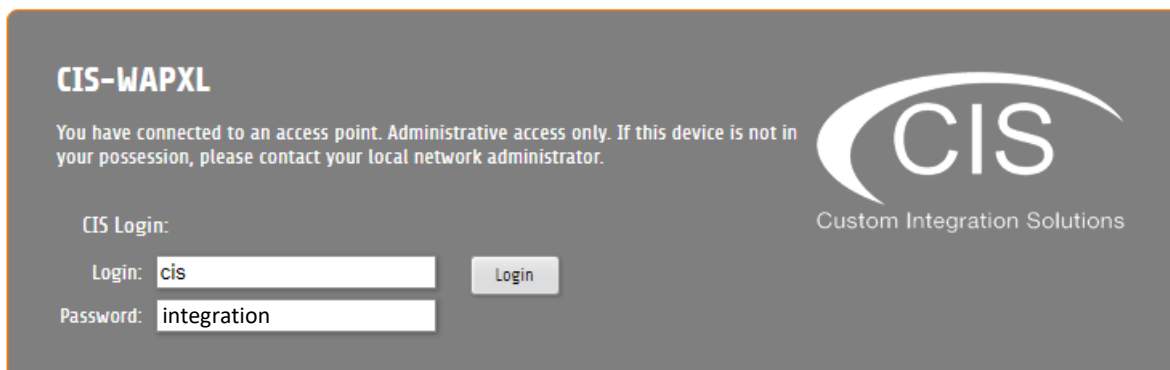


		▲ Address	MAC Address	Active Address	Active MAC Address	Active Host Name	Expires After
-	D	10.100.1.100	64:D1:54:	10.100.1.100	64:D1:54:	CIS-SW-POE4	1d 22:58:20
-	D	10.100.1.101	6C:3B:6B:	10.100.1.101	6C:3B:6B:	CIS-WAPXL	1d 23:59:46

3. Enter the IP address of the access point in the address bar of your web browser.
4. To login, use the default credentials **cis** and **integration** as the password.
5. Integrators may use the Get TeamViewer link if remote assistance is required.

## The Status Page

The status page provides basic diagnostic information. There is a CIS Support Address should you require assistance. You can view the identity (name) of the access point you are connected to, view it's public address, the traffic flowing through the device, and identify the MAC addresses of its interfaces.



**CIS-WAPXL**

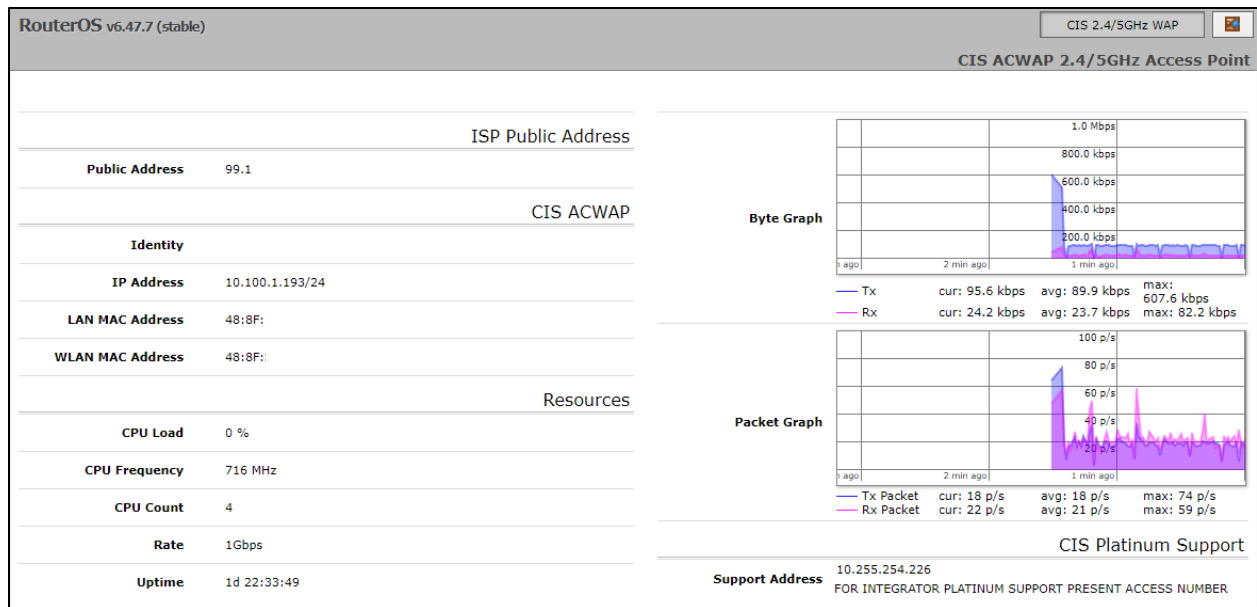
You have connected to an access point. Administrative access only. If this device is not in your possession, please contact your local network administrator.

CIS Login:

Login:  Login

Password:

**CIS**  
Custom Integration Solutions



## Setting the Access Point's Identity

The identity is used to identify your device on the network. Troubleshooting will become easier when you set the identity correctly. Set the identity of the access point based on its location E.g., Basement.

The **Identity** setting can be found in the **System** tab in the left toolbar.

**CIS ACWAP Status** RouterOS v6.47.7 (stable) CIS 2.4/5GHz WAP

**Identity**

Apply

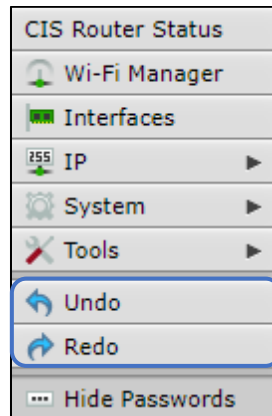
**Identity** Garage

Format "Location"

Wireless  
CIS Support  
IP  
System  
Clock  
Identity  
Note  
Password

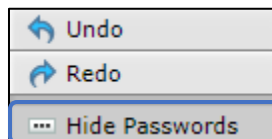
## Undo / Redo

Undo and Redo buttons are located in the left toolbar. You may use them to quickly undo/redo any changes made to configuration.



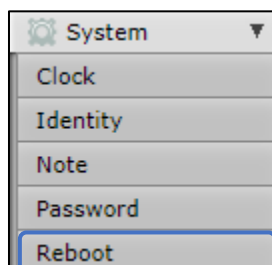
## Show / Hide Passwords

Selecting the **Hide Passwords** button in the left toolbar will toggle the displaying of passwords related to Wi-Fi, Hotspot, and more.



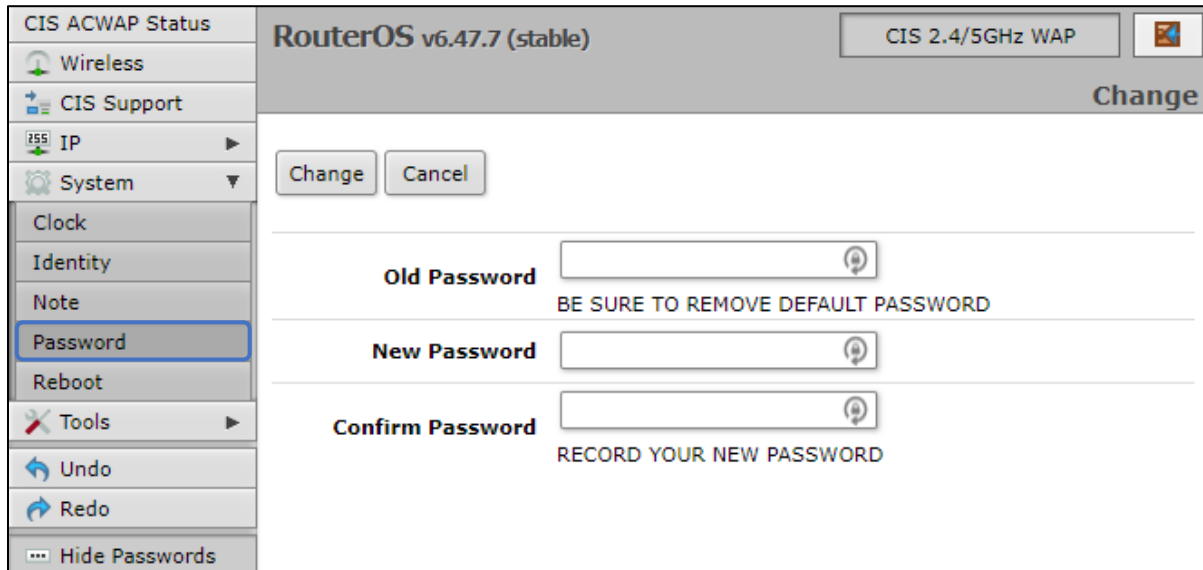
## Rebooting the Device

If you are having ongoing issues with your network and suspect a reboot will help, the **Reboot** option can be found in the **System** tab in the left toolbar. Clicking reboot will ask for confirmation before proceeding.



## Changing the Default Password

After you log in for the first time, please create a new password to increase the security of the device. Enter the old password in the top field and a secure password in the new and confirm password fields.

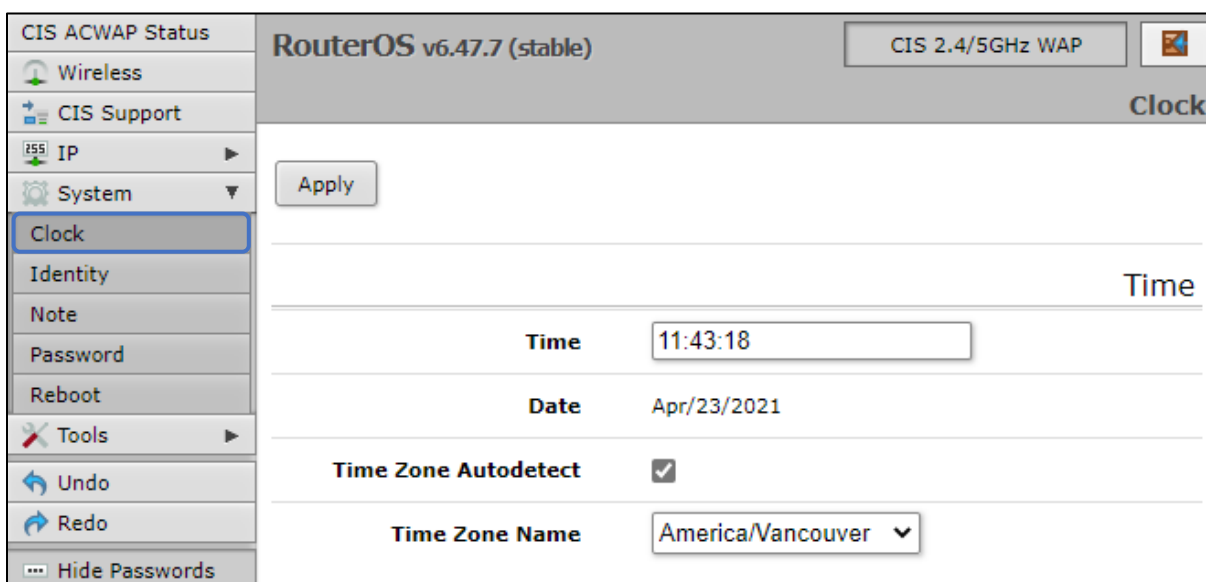


The screenshot shows the RouterOS v6.47.7 (stable) web interface. The left sidebar has the 'Password' option selected under the 'System' tab. The main content area is titled 'Change' and contains three password input fields: 'Old Password', 'New Password', and 'Confirm Password'. Below each field is a hint: 'BE SURE TO REMOVE DEFAULT PASSWORD' for the old password, and 'RECORD YOUR NEW PASSWORD' for the new and confirm passwords. There are 'Change' and 'Cancel' buttons at the top left of the main area.

Field	Hint
Old Password	BE SURE TO REMOVE DEFAULT PASSWORD
New Password	RECORD YOUR NEW PASSWORD
Confirm Password	RECORD YOUR NEW PASSWORD

## Setting the Time Zone

You can find the Clock settings under the System tab in the left toolbar. Select your time zone from the drop-down menu.



The screenshot shows the RouterOS v6.47.7 (stable) web interface with the 'Clock' option selected in the left sidebar. The main content area is titled 'Clock' and contains an 'Apply' button at the top left. Below it are fields for 'Time' (11:43:18), 'Date' (Apr/23/2021), 'Time Zone Autodetect' (checked), and 'Time Zone Name' (America/Vancouver).

Field	Value
Time	11:43:18
Date	Apr/23/2021
Time Zone Autodetect	<input checked="" type="checkbox"/>
Time Zone Name	America/Vancouver

## IP Addressing

### The DHCP Client Tab

The DHCP Client tab will present you with the IP address assigned to your access point from the router. CIS recommends creating a DHCP reservation for access points and other network infrastructure devices.

The screenshot shows the RouterOS v6.47.7 (stable) interface. On the left is a sidebar menu with options: CIS ACWAP Status, Wireless, CIS Support, IP (selected), Addresses, DHCP Client (highlighted), DHCP Server, DNS, Pool, and UPnP. The main panel is titled 'DHCP Client' and shows '1 item' in a table. The table has columns for Interface and IP Address. The entry shows 'bridge-operations' as the interface and '10.100.1.193/24' as the IP address.

Interface	IP Address
bridge-operations	10.100.1.193/24

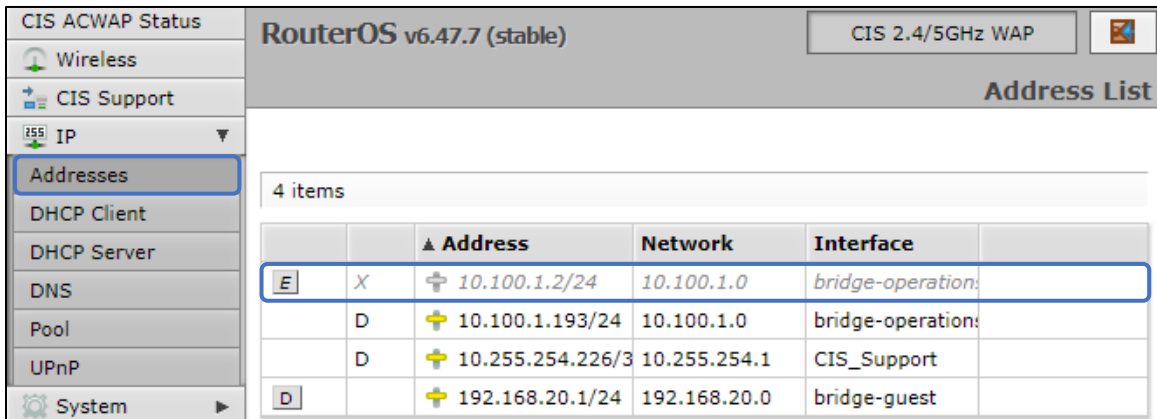
### Renewing the IP Address

Once you've clicked the entry under the **DHCP Client** option, click the **Renew** button to obtain a new lease.

This screenshot shows the same RouterOS interface, but the 'DHCP Client <bridge-operations>' configuration page is open. The sidebar menu is expanded to show 'System', 'Tools', 'Undo', 'Redo', and 'Hide Passwords'. The main panel has a title bar 'DHCP Client <bridge-operations>' and a row of buttons: OK, Cancel, Apply, and Renew (highlighted with a blue border). Below the buttons, the status is 'Status: bound' and 'not invalid'. There is a section for 'Enabled' with a checked checkbox. The 'Interface' is 'bridge-operations' and the 'IP Address' is '10.100.1.193/24'. The 'DHCP' and 'Status' labels are on the right side of the configuration area.

## Setting a Static IP Address

To set a static IP, select the **Addresses** tab under the **IP** section in the toolbar. There is an IP address entry that is disabled by default. Click on it.



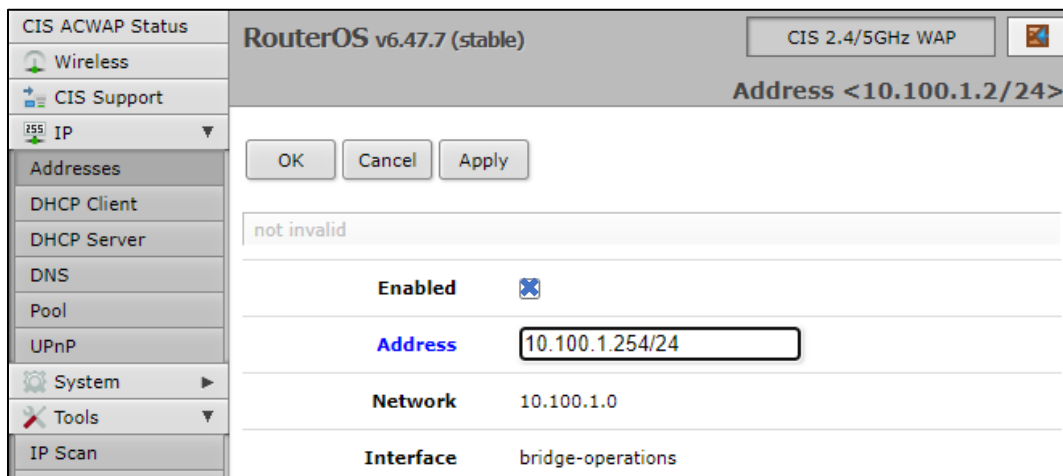
The screenshot shows the RouterOS v6.47.7 (stable) interface. On the left, the 'IP' section is expanded, and the 'Addresses' tab is selected. The main area displays the 'Address List' with 4 items. The first item is highlighted with a blue border.

		Address	Network	Interface
E	X	10.100.1.2/24	10.100.1.0	bridge-operations
	D	10.100.1.193/24	10.100.1.0	bridge-operations
	D	10.255.254.226/3	10.255.254.1	CIS_Support
D		192.168.20.1/24	192.168.20.0	bridge-guest

**If your network falls in one of the ranges below, you can set the static IP address yourself. If it is outside of these ranges, you must call CIS to have a route created on the access point!**

Available address ranges:			
172.16.1.0/24	10.100.1.0/24	192.168.1.0/24	192.168.0.0/24

Check the **Enabled** box, then enter the IP address you would like to use. It **MUST** be in the range of your network, and outside of the range of the DHCP pool. The format must include **/24** at the end. This is the subnet mask, which determines how many devices can be connected to this network.



The screenshot shows the RouterOS v6.47.7 (stable) interface with the 'Address' configuration dialog open. The dialog has a title bar 'Address <10.100.1.2/24>' and buttons for 'OK', 'Cancel', and 'Apply'. The 'Enabled' checkbox is checked. The 'Address' field contains '10.100.1.254/24'. The 'Network' field contains '10.100.1.0' and the 'Interface' field contains 'bridge-operations'.

Enabled	<input checked="" type="checkbox"/>
Address	10.100.1.254/24
Network	10.100.1.0
Interface	bridge-operations

Once the static IP address is set, disable the DHCP client. Go to **IP > DHCP Client** and click on the entry. Click on the small 'D' button to disable it.

CIS ACWAP Status

Wireless

CIS Support

IP

Addresses

DHCP Client

DHCP Server

DNS

RouterOS v6.47.7 (stable)

CIS 2.4/5GHz WAP

DHCP Client

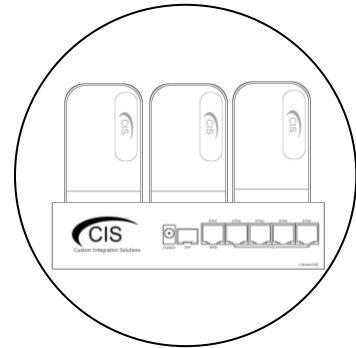
1 item

	▲ Interface	IP Address
<div>D</div>	bridge-operations	10.100.1.193/24



## Managing Access Points with the Wireless Manager

All CIS routers include a Wireless Manager that allows you to manage your access points from a single location. All changes to SSIDs, passwords and other options will be propagated to all CIS access points on the network.



### Linking CIS Access Points to the Wi-Fi Manager

Select the **Wireless** section in the left toolbar. Under the **WiFi Interfaces** tab, select **Wi-Fi Manager**.

CIS ACWAP Status RouterOS v6.47.7 (stable) CIS 2.4/5GHz WAP

Wireless WiFi Interfaces Access List Registration Security Profiles Wireless Tables

Wi-Fi Manager Setup Repeater Scanner

4 items

		Name	Type	Actual MTU	Tx
D	S	wlan1-2.4GHz	Wireless (IPQ4019)	1500	0 bps

Check the **Enabled** box, click Apply, then OK.

CIS ACWAP Status RouterOS v6.47.7 (stable) CIS 2.4/5GHz WAP

Wireless Wi-Fi Manager

OK Cancel Apply

Enabled ☒

The device will display the message --- managed by CAPsMAN. The Access point is now linked to your CIS router and can be managed through the router's configuration page.

--- managed by CAPsMAN					
E	XS	wlan1-2.4GHz	Wireless (IPQ4019)	1500	0 bps
--- managed by CAPsMAN					
E	XS	wlan2-5GHz	Wireless (IPQ4019)	1500	0 bps

## Viewing the Connected Access Points

On your CIS router, select the **Wi-Fi Manager** section in the left toolbar. The active Wi-Fi radios will be displayed.

	▲ Name	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx
D	RMB CIS 2.4GHz-RACK	0 bps	0 bps	0	0	0 bps

If you select the **WiFi Access points** tab, you'll be able to view the identity, MAC address and other information of the individual access points.

▲ Address	Version	Identity	State	Radios
6C:3B:6B:EA:36:1E	6.47.7	Rack	Run	1

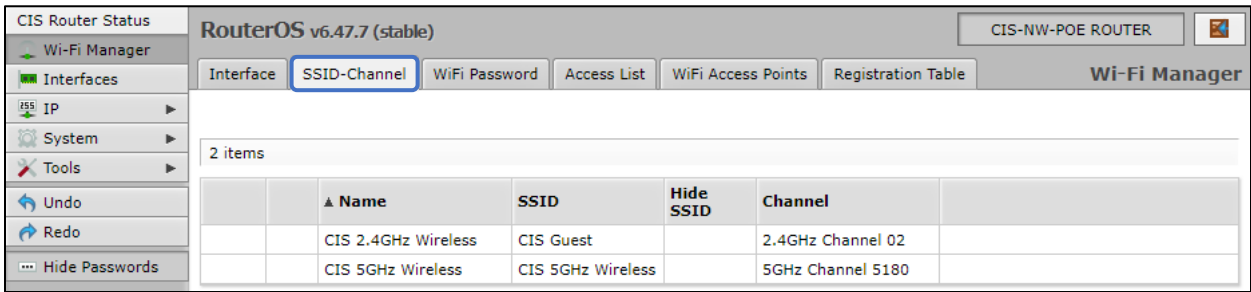
## Viewing Connected Devices

Select the **Registration Table** tab to view the connected devices.

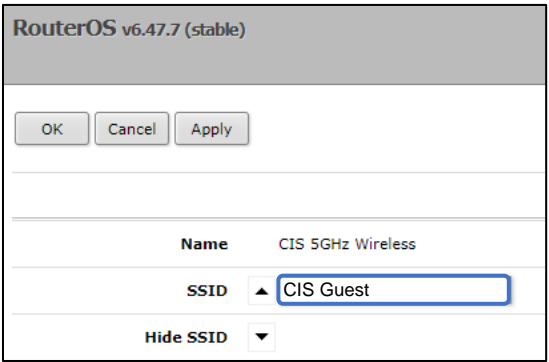
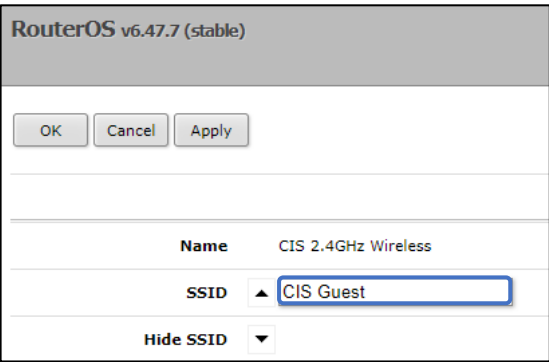
▲ Interface	SSID	MAC Address	Tx Rate	Rx Rate	Tx Signal	Rx Signal	Uptime
CIS 2.4GHz-RACK	CIS Guest		52Mbps-20	65Mbps-20	0	-66	00:02:49.24

## Changing the SSID of Managed Access Points

Select the **SSID-Channel** tab in the **Wi-Fi Manager** section. Click on the 2.4GHz network.

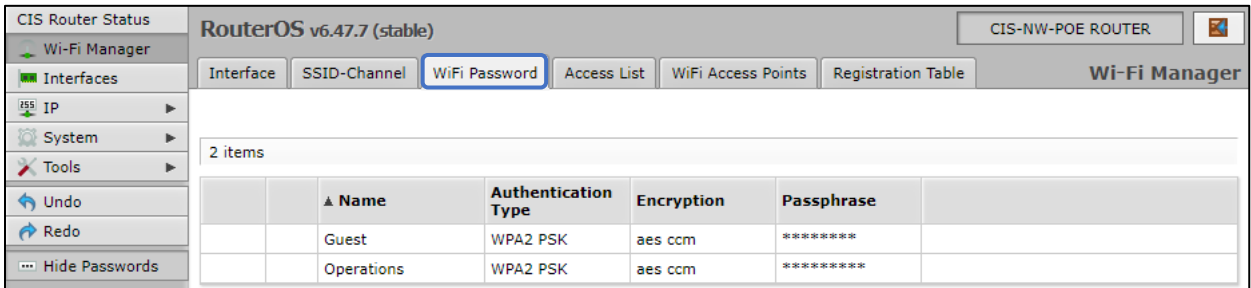


Enter the name of the SSID in the field. Copy and paste the SSID so that the 5GHz network has the same SSID.

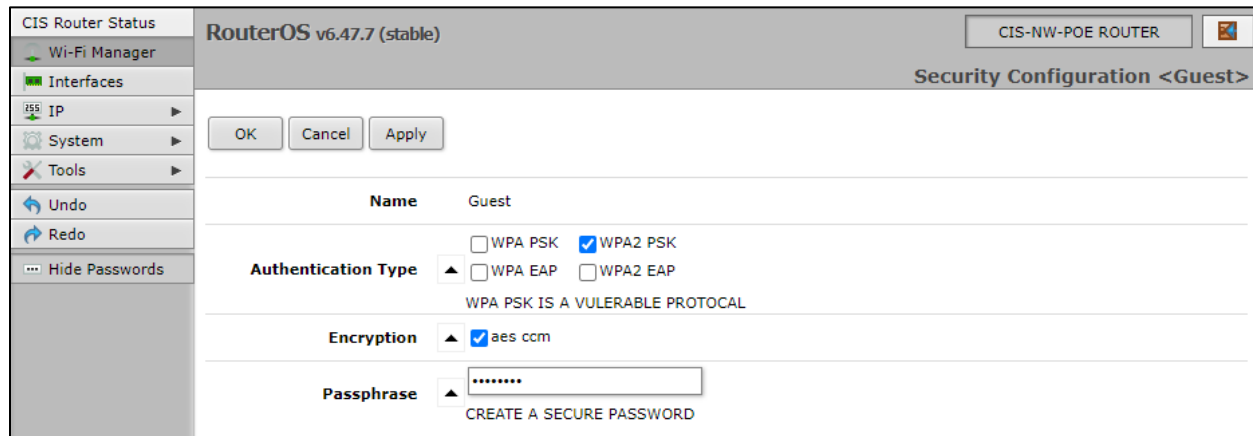


## Changing the Wi-Fi Password of Managed Access Points

Select the **Wi-Fi Password** tab. Click on the network that you'd like to change the password for. If you've purchased a guest network, it will appear here.



Click on the network you'd like to set the password for, then enter the passphrase in the box below. It is highly recommended you use only **WPA2 PSK** for security purposes. WPA is vulnerable to password cracking.

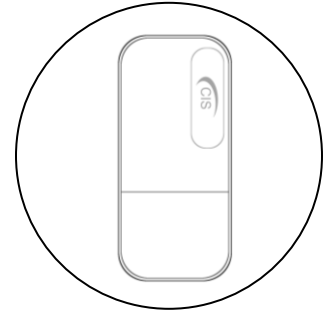


The image shows the RouterOS v6.47.7 (stable) Security Configuration <Guest> window. The left sidebar contains the following menu items: CIS Router Status, Wi-Fi Manager, Interfaces, IP, System, Tools, Undo, Redo, and Hide Passwords. The main content area has a title bar with 'RouterOS v6.47.7 (stable)' and 'CIS-NW-POE ROUTER'. Below the title bar are 'OK', 'Cancel', and 'Apply' buttons. The configuration section is titled 'Security Configuration <Guest>'. It includes a 'Name' field with the value 'Guest'. Under 'Authentication Type', there are checkboxes for WPA PSK, WPA2 PSK (checked), WPA EAP, and WPA2 EAP. A warning message 'WPA PSK IS A VULNERABLE PROTOCOL' is displayed. Under 'Encryption', there is a checkbox for 'aes ccm' which is checked. Under 'Passphrase', there is a text input field containing '\*\*\*\*\*' and a label 'CREATE A SECURE PASSWORD'.

Name	Guest
Authentication Type	<input type="checkbox"/> WPA PSK <input checked="" type="checkbox"/> WPA2 PSK <input type="checkbox"/> WPA EAP <input type="checkbox"/> WPA2 EAP WPA PSK IS A VULNERABLE PROTOCOL
Encryption	<input checked="" type="checkbox"/> aes ccm
Passphrase	***** CREATE A SECURE PASSWORD

## Configuring Access Points in Standalone Mode

CIS access points can be centrally managed via the Wi-Fi manager on CIS routers, or they can operate as standalone units. This section includes instructions for setting up access points as standalone units.



### Setting the SSID

Select the **Wireless** tab from the left toolbar. You can view the networks under the **WiFi** interfaces tab. The 2.4 and 5 GHz bands have their own separate networks you can modify individually. Use the 'E' and 'D' buttons to enable and disable the wireless networks.

A screenshot of the RouterOS v6.47.7 (stable) interface. The left sidebar shows the 'Wireless' tab selected. The main area displays the 'Wireless Tables' section with a table of 4 items. The table has columns for Name, Type, Actual MTU, and Tx. The first two items are wlan1-2.4GHz and wlan2-5GHz, both of type Wireless (IPQ4019) with an Actual MTU of 1500 and Tx of 0 bps. There are 'D' (disable) and 'S' (enable) buttons for each item.

		Name	Type	Actual MTU	Tx
D	S	wlan1-2.4GHz	Wireless (IPQ4019)	1500	0 bps
D	S	wlan2-5GHz	Wireless (IPQ4019)	1500	0 bps

Click on one of the networks, then enter your SSID in the **SSID** box. Remember to change it for both the 2.4 GHz network and 5 GHz network!

A screenshot of the RouterOS v6.47.7 (stable) interface showing the configuration for a wireless network. The 'Wireless' tab is selected. The 'General' section shows the 'Name' as wlan1-2.4GHz. The 'Wireless' section shows the 'Band' as 2GHz-B/G/N, 'Channel Width' as 20MHz, and 'Frequency' as auto MHz. The 'SSID' field is highlighted with a blue border and contains the text 'CIS AP-AC 2.4'. There are also buttons for 'running ap', 'not running', and 'slave' at the top.

running ap not running slave

Enabled ☒

General

Name wlan1-2.4GHz

Wireless

Band 2GHz-B/G/N

Channel Width 20MHz

Frequency auto MHz


SSID CIS AP-AC 2.4

## Setting the Wi-Fi Password for Standalone Access Points

Select the **Security Profiles** tab in the Wireless section. Click on the default network to change the password and security settings.

CIS ACWAP Status	RouterOS v6.47.7 (stable)						
Wireless	CIS 2.4/5GHz WAP						
CIS Support	WiFi Interfaces   Access List   Registration   <b>Security Profiles</b>   Wireless Tables						
IP	2 items						
System							
Tools							
Undo							
Redo							
Hide Passwords							
		▲ Name	Mode	Authentica... Types	Unicast Ciphers	Group Ciphers	WPA Pre-Shared Key
		Guest Security	dynamic keys	WPA PSK, WPA	aes ccm	aes ccm	*****
	*	default	dynamic keys	WPA2 PSK	aes ccm	aes ccm	

Enter the password in the **WPA2 Pre-Shared Key** field. CIS recommends you leave WPA PSK disabled, as it is a vulnerable protocol. If you have legacy devices that require it, enable it, and copy and paste the password into the WPA Pre-Shared Key field.

CIS ACWAP Status	RouterOS v6.47.7 (stable)						
Wireless	CIS 2.4/5GHz WAP						
CIS Support	Security Profile <default>						
IP	OK Cancel Apply						
System	default						
Tools							
Undo							
Redo							
Hide Passwords							
	General						
	Name default						
	Mode dynamic keys						
	Authentication Types <input type="checkbox"/> WPA PSK <input checked="" type="checkbox"/> WPA2 PSK						
	Unicast Ciphers <input checked="" type="checkbox"/> aes ccm <input type="checkbox"/> tkip						
	Group Ciphers <input checked="" type="checkbox"/> aes ccm <input type="checkbox"/> tkip						
	WPA Pre-Shared Key .....						
	WPA2 Pre-Shared Key ..... 						
	Comment						

## Enabling the Guest Network on Standalone Access Points

CIS access points running in standalone mode can run a simple guest network. To enable, click the **E** button in the **WiFi Interfaces** tab of the **Wireless** section. Enable both the 2.4 and 5 GHz networks.

The screenshot shows the RouterOS v6.47.7 (stable) interface. On the left is a sidebar with 'Wireless' selected. The main area is the 'WiFi Interfaces' tab. It contains buttons for 'Wi-Fi Manager', 'Setup Repeater', and 'Scanner'. Below these is a table with 4 items. The table has columns: Name, Type, Actual MTU, and Tx. The third row, 'wlan3-2.4GHz-guest', is highlighted, and its 'E' button is circled in blue.

		Name	Type	Actual MTU	Tx
D	S	wlan1-2.4GHz	Wireless (IPQ4019)	1500	0 bps
D	S	wlan2-5GHz	Wireless (IPQ4019)	1500	0 bps
E	X	◀▶ wlan3-2.4GHz-guest	Virtual		0 bps
E	X	◀▶ wlan4-5GHz-guest	Virtual		0 bps

Devices in the guest network will receive different IP addresses and will be isolated from clients on the main network. Change the SSID by clicking on the virtual network.

The configuration window for 'wlan3-2.4GHz-guest' is shown. It has an 'Enabled' checkbox. The 'General' tab is active, showing the 'Name' as 'wlan3-2.4GHz-guest' and 'Type' as 'Virtual'. The 'Wireless' tab is also visible. In the 'Wireless' section, the 'SSID' field is highlighted with a blue box and contains the text 'CIS AP-AC Guest 2.4'.

Enabled ☐

General

Name wlan3-2.4GHz-guest

Type Virtual

Wireless

Secondary Channel ▼

SSID ▲ CIS AP-AC Guest 2.4

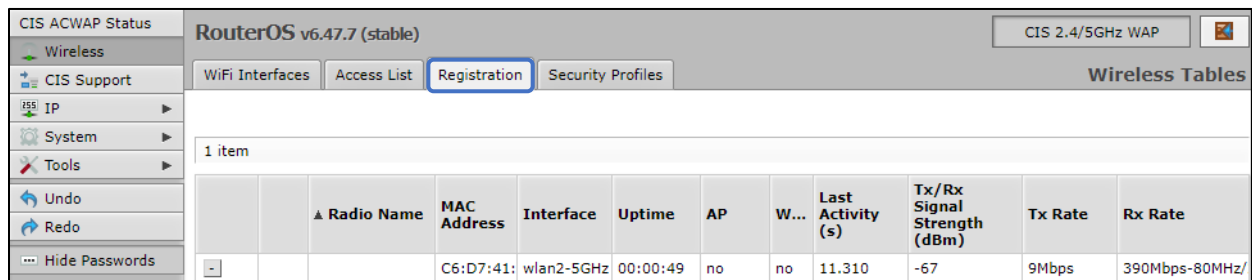
Master Interface wlan1-2.4GHz

Security Profile Guest Security

To change the password, click the **Security Profiles** tab in the Wireless menu. Click the **Guest security profile** and change the password, just like you did for the main network.

## View Connected Devices

In the **Wireless** section, click the **Registration** tab to view the connected devices. You can identify them based on their MAC address. You can view the uptime, signal strength, traffic flow, and more.

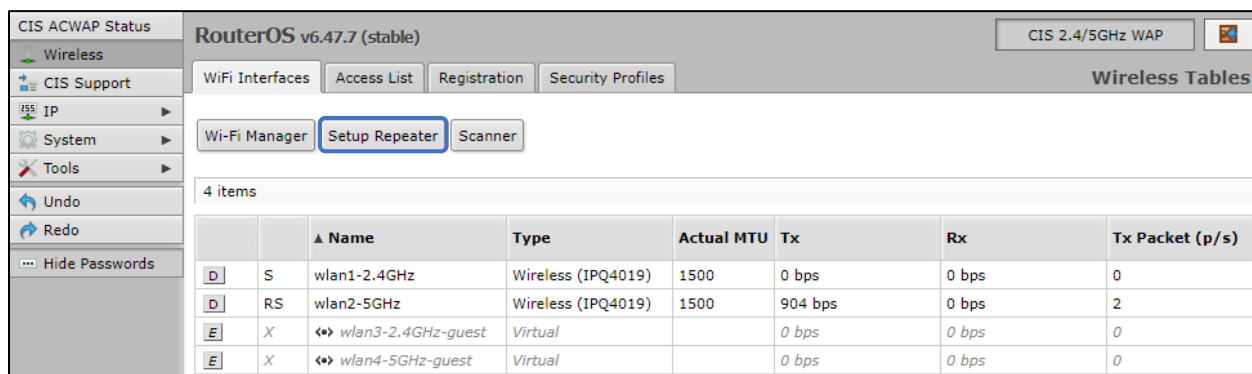


The screenshot shows the RouterOS v6.47.7 (stable) interface. The left sidebar contains the 'Wireless' menu with options like 'Wireless', 'CIS Support', 'IP', 'System', 'Tools', 'Undo', 'Redo', and 'Hide Passwords'. The main panel has tabs for 'WiFi Interfaces', 'Access List', 'Registration' (selected), and 'Security Profiles'. A 'Wireless Tables' header is on the right. Below the tabs, a table lists 1 item. The table has columns: Radio Name, MAC Address, Interface, Uptime, AP, W..., Last Activity (s), Tx/Rx Signal Strength (dBm), Tx Rate, and Rx Rate. The single entry shows a MAC address of C6:D7:41: and an interface of wlan2-5GHz.

Radio Name	MAC Address	Interface	Uptime	AP	W...	Last Activity (s)	Tx/Rx Signal Strength (dBm)	Tx Rate	Rx Rate
	C6:D7:41:	wlan2-5GHz	00:00:49	no	no	11,310	-67	9Mbps	390Mbps-80MHz/

## Setting up the Access Point as a Repeater

In the **Wireless** section, select the **WiFi Interfaces** tab. Click on **Setup Repeater**.

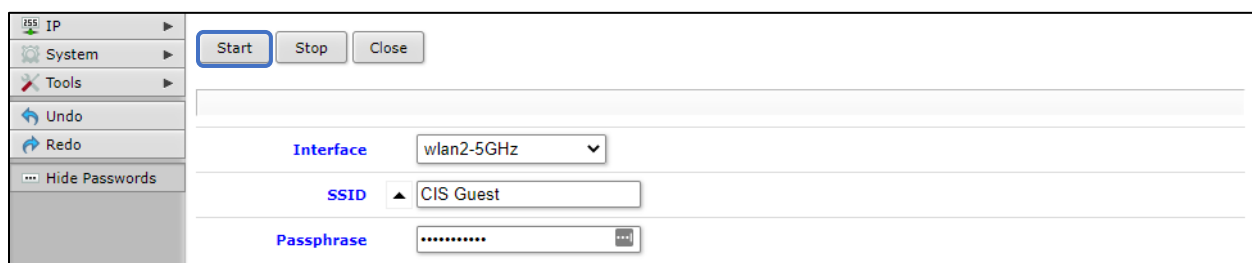


The screenshot shows the RouterOS v6.47.7 (stable) interface. The left sidebar is the same as the previous screenshot. The main panel has tabs for 'WiFi Interfaces', 'Access List', 'Registration', and 'Security Profiles'. The 'WiFi Interfaces' tab is selected, and within it, the 'Setup Repeater' sub-tab is active. Below the tabs, a table lists 4 items. The table has columns: Name, Type, Actual MTU, Tx, Rx, and Tx Packet (p/s). The entries show interfaces wlan1-2.4GHz, wlan2-5GHz, wlan3-2.4GHz-guest, and wlan4-5GHz-guest.

Name	Type	Actual MTU	Tx	Rx	Tx Packet (p/s)
wlan1-2.4GHz	Wireless (IPQ4019)	1500	0 bps	0 bps	0
wlan2-5GHz	Wireless (IPQ4019)	1500	904 bps	0 bps	2
wlan3-2.4GHz-guest	Virtual		0 bps	0 bps	0
wlan4-5GHz-guest	Virtual		0 bps	0 bps	0

Display the SSID field by clicking the down arrow next to it. Type the SSID and Passphrase of the wireless network you wish to extend the range of. Click **Start**.

**Note:** You can only run a repeater on one band at a time. The 2.4 GHz band will offer better range.



The screenshot shows the 'Start' dialog for setting up a repeater. It has buttons for 'Start', 'Stop', and 'Close'. Below the buttons, there are three fields: 'Interface' (set to wlan2-5GHz), 'SSID' (set to CIS Guest), and 'Passphrase' (masked with dots).

Interface: wlan2-5GHz

SSID: CIS Guest

Passphrase: .....



## Tools

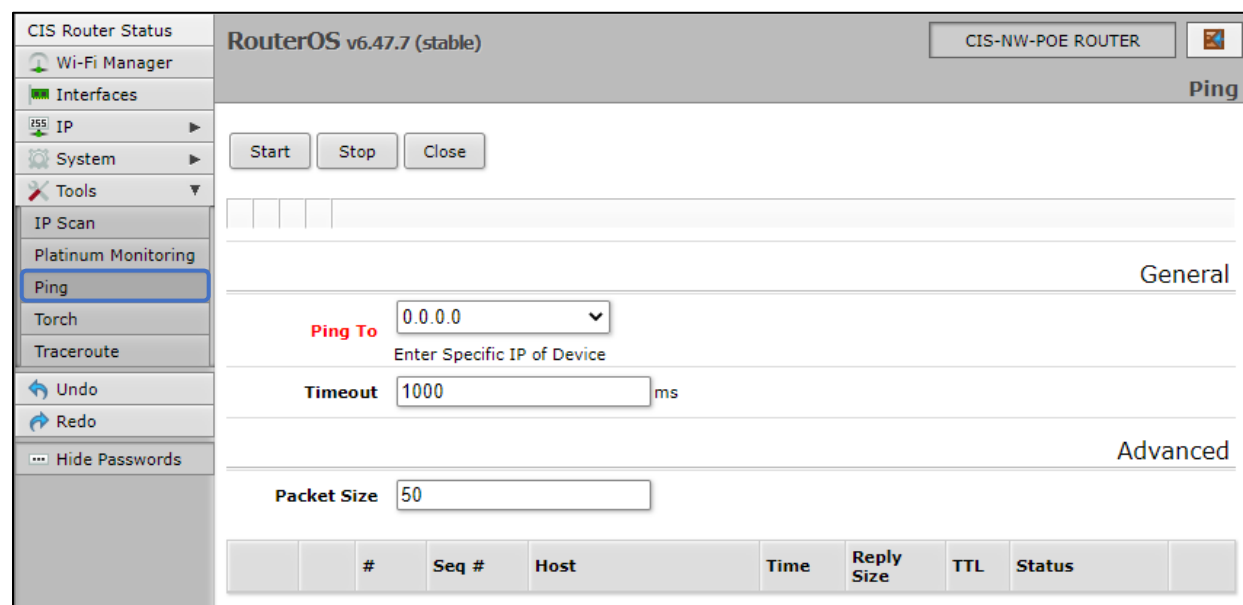
### UPnP

Universal Plug and Play enables the discovery other devices located on the network and vice-versa. If you require UPnP, select it under the **IP** tab in the toolbar, then enable it. UPnP has implications on the security of the device, and it is recommended you leave it disabled unless required.



### Ping

Ping uses Internet Control Message Protocol (ICMP) echo messages to determine if a remote host is active. It will also provide the round-trip time between the hosts. Enter the IP address of the device and select Start to begin.



## IP Scan

The IP scan tool locates devices on the network. It can also locate devices that have a static IP set internally if they are on the same network as your access point.

To use the IP scan tool, select the network you wish to scan on (bridge-operations is default), then enter the network address and subnet mask using CIDR notation.

CIS Router Status RouterOS v6.47.7 (stable) CIS-NW-POE ROUTER IP Scan

Start Stop Close

Interface bridge-operations  
Select Bridge Interface

Address Range 10.100.1.0/24  
Enter Network Address and Subnet Mask

#	Address	MAC Address	Time (ms)	DNS	SNMP	Netbios
---	---------	-------------	-----------	-----	------	---------

Select **bridge-operations** and enter **10.100.1.0/24** as the address range. You may have multiple interfaces and address ranges depending on your configuration. Most use a /24 network size.

## Wireless Scanner

You can use the access point to scan for other wireless networks in the area. This is immensely helpful if you need to discover networks that may be interfering with your wireless performance.

**Note:** You must disable the Wi-Fi manager on the access point prior to using this tool!

From the **Wireless** section, click on the **Scanner** button. Select the interface to use and click **Start**.

CIS ACWAP Status RouterOS v6.47.7 (stable) CIS 2.4/5GHz WAP Wireless Tables

WiFi Interfaces Access List Registration Security Profiles

Wi-Fi Manager Setup Repeater Scanner

Start Stop Close

Interface wlan1-2.4GHz

## Troubleshooting

Symptom	Possible causes
The devices are having trouble maintaining a connection to the wireless network.	<ul style="list-style-type: none"> <li>• Check the signal strength in the registration table. A healthy signal range is between -30 and -75 dB.</li> <li>• Avoid using the 2.4 GHz network when possible, as it is more prone to interference. Use the Scanner tool to detect interfering networks if necessary.</li> <li>• Try changing the channel of the access points. You can do this in the Wi-Fi manager by clicking on the Interface tab, then choose an access point radio. Click the down arrow to show the channel box.</li> </ul>
The device won't connect to the wireless network at all.	<ul style="list-style-type: none"> <li>• Ensure the device is in range of the access point.</li> <li>• Temporarily disable all access points except the one closest to the device. Some devices have issues with multiple access points with the same SSID. <ul style="list-style-type: none"> <li>• If this is the case, contact CIS and we will make a separate SSID for these devices that is only broadcast on one access point.</li> </ul> </li> <li>• 802.11b is disabled by default. If you have devices that require 802.11b you can enable it in the Wi-Fi manager or contact CIS for assistance.</li> <li>• Ensure that the passphrase is correct.</li> </ul>
I am not receiving the speed that I am expecting.	<ul style="list-style-type: none"> <li>• The CIS-WAPXL has been tested to achieve approximately 375 mbps in our testing.</li> <li>• The vast majority of access points and client devices will not provide or support the full throughput of a 1 Gbps internet connection.</li> <li>• Test the speed of your device when it is plugged into the wired network if possible. Compare the results.</li> </ul>

<p>The speed is particularly slow.</p>	<ul style="list-style-type: none"> <li>• Ensure there is adequate coverage throughout the building.</li> <li>• We recommend one access point for every 1000 sq ft for adequate 5 GHz coverage.</li> <li>• The placement of the access point can have a significant impact on performance as well as the nearby materials. The following materials can cause issues with reflecting or absorbing radio frequencies:</li> </ul> <table border="1" data-bbox="824 573 1416 951"> <thead> <tr> <th>Type of Barrier</th><th>Interference Potential</th></tr> </thead> <tbody> <tr> <td>Wood</td><td>Low</td></tr> <tr> <td>Synthetic material</td><td>Low</td></tr> <tr> <td>Glass</td><td>Low</td></tr> <tr> <td>Water</td><td>Medium</td></tr> <tr> <td>Bricks</td><td>Medium</td></tr> <tr> <td>Marble</td><td>Medium</td></tr> <tr> <td>Plaster</td><td>High</td></tr> <tr> <td>Concrete</td><td>High</td></tr> <tr> <td>Bulletproof glass</td><td>High</td></tr> <tr> <td>Metal</td><td>Very high</td></tr> </tbody> </table> <p>The following are sources of interference that can affect Wi-Fi performance:</p> <ul style="list-style-type: none"> <li>• Microwave ovens.</li> <li>• Power sources – breaker boxes, etc.</li> <li>• Cordless home phones.</li> <li>• Wireless video transmitters.</li> <li>• Wireless speakers.</li> <li>• Poorly shielded cabling.</li> </ul>	Type of Barrier	Interference Potential	Wood	Low	Synthetic material	Low	Glass	Low	Water	Medium	Bricks	Medium	Marble	Medium	Plaster	High	Concrete	High	Bulletproof glass	High	Metal	Very high
Type of Barrier	Interference Potential																						
Wood	Low																						
Synthetic material	Low																						
Glass	Low																						
Water	Medium																						
Bricks	Medium																						
Marble	Medium																						
Plaster	High																						
Concrete	High																						
Bulletproof glass	High																						
Metal	Very high																						
<p>The access point will not turn on.</p>	<ul style="list-style-type: none"> <li>• Most issues occur when the access point is used with PoE.</li> <li>• Ensure the router or switch is capable of providing PoE. Some devices only support PoE on specific ports.</li> <li>• Faulty cabling or bad terminations can cause issues with PoE. Try plugging the access point directly into the router or switch with a short cable.</li> <li>• CIS routers and switches provide more stable PoE when the port is set to “Forced On”. Review the user manuals for instructions.</li> </ul>																						

## Warranty Information

Custom Integration Solutions™ products have a 2-Year Limited Warranty. This warranty includes parts and labor repairs on all components found to be defective in material or workmanship under normal conditions of use. This warranty shall not apply to products that have been abused, modified, or disassembled. Products to be repaired under this warranty must be returned to Custom Integration Solutions™ or a designated service center with prior notification and an assigned return authorization (RA) number.

## Contact Information

Web: [www.custom-integration-solutions.com](http://www.custom-integration-solutions.com)

Phone: Technical Support - (888) 976-3651

Email: [activations@custom-integration-solutions.com](mailto:activations@custom-integration-solutions.com)



CIS Access Points are in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EC.