CIS Access Points – User Manual

Table of Contents

Welcome to Custom Integration Solutions 4
- Overview 4
- Package Contents 4
- Power 4

Device Details 5
- Ports 5
- LED Indicators 5
- Buttons 5

Mounting Options 6

Quick Setup 7

Accessing the Web Interface 8
- The Status Page 9
- Setting the Access Point's Identity 9
- Undo / Redo 10
- Show / Hide Passwords 10
- Rebooting the Device 10
- Changing the Default Password 11
- Setting the Time Zone 11

IP Addressing 12
- The DHCP Client Tab 12
- Renewing the IP Address 12
- Setting a Static IP Address 13

Managing Access Points with the Wireless Manager 15
Linking CIS Access Points to the Wi-Fi Manager 15
Viewing the Connected Access Points 16
Viewing Connected Devices 16
Changing the SSID of Managed Access Points 17
Changing the Wi-Fi Password of Managed Access Points 17

Configuring Access Points in Standalone Mode 19
Setting the Wi-Fi Password for Standalone Access Points 20
Enabling the Guest Network on Standalone Access Points 21
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. 21
View Connected Devices 22
Setting up the Access Point as a Repeater 22

Tools 23
UPnP 23
Ping 23
IP Scan 24
Wireless Scanner 24

Troubleshooting 25

Warranty Information 27
Contact Information 27

Welcome to Custom Integration Solutions

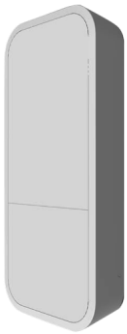
Thank you for purchasing CIS devices. Our solutions make it easy for integrators to deploy networks in home and business settings with minimal configuration. Our support team is here to assist with setting up equipment and answering your network related questions.

Overview

CIS wireless access points provide a compact and powerful solution to your home and commercial connectivity needs. CIS Access points are weatherproof and can be fixed to any external wall or ceiling. The 360° coverage pattern makes these access points ideal for business and residential applications. Keep your cable runs hidden by routing the Ethernet cables through an access slot in the rear of the access points.

- The CIS-ACWAP provides high speed connectivity on the 2.4 and 5 GHz bands with support for wireless standards 802.11 a, b, g, n, and ac.
- The CIS-WAP is a low-cost option providing 2.4 GHz connectivity with support for wireless 802.11b, g, and n.

Package Contents


AP

PoE Injector

DC Adapter

Mounting Bracket

Ceiling Plate

Screw Kit

Pole mount (AC-WAP only)

Power

CIS access points are powered by via the DC Jack or PoE on ETH1. Use the included DC adapter, PoE injector, or connect to a router or switch that provides PoE.

- The CIS-ACWAP accepts 10-57v via the DC jack or 18-57v via PoE on ETH1. It can accept 802.3af/at power and consumes a maximum of 10W.

- The CIS-WAP accepts 11-57v via the DC jack or PoE. It can accept 802.3af/at power and consumes a maximum of 4W.

Device Details

CIS-ACWAP

CIS-WAP

Ports

- ETH1 – Gigabit Ethernet port. Accepts PoE power.
- ETH2 – Gigabit Ethernet port. Connect other devices to bridge them to the network.
- DC jack – Use when PoE is not an option.

- ETHERNET – 10/100 Ethernet port. Accepts PoE power.
- DC jack – use when PoE is not an option.

LED Indicators

- PWR – Lit when the device is powered on.
- USR – An LED that can be customized by CIS.
- ETHERNET – Green indicates network activity. An amber light indicates the link is operating at 10/100 mbps.

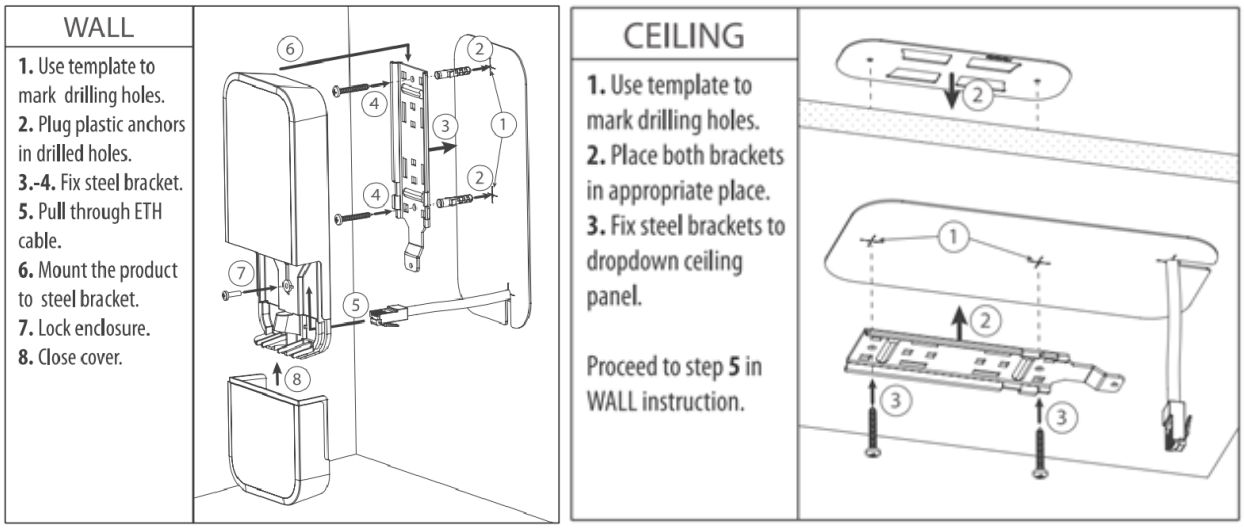
- PWR – Lit when the device is powered on.
- AP/CAP – Off when operating in standalone mode. On when controlled by the Wi-Fi manager.
- 2 GHz – Flashes when wireless activity is detected.
- ETH – flashes when activity is detected on the ethernet port.

Buttons

Reset button: This button is located on the side next to the USB port. Hold this button while the device is powered off, then apply power. Keeping holding until the USR 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

CIS access points provide flexible mounting options. Mount it on a wall, ceiling, or pole to broadcast your wireless network in all directions.



Detailed Steps

1. Use the template (included in the box) to mark the location of the screw holes.

2. If mounting to a wall, use the included plastic anchors.

3. If mounting to a ceiling, place the steel plate on the other side (if possible) for reinforcement and thread the screws through it.

4. Use the included screws to attach the mounting plate to the wall or ceiling.

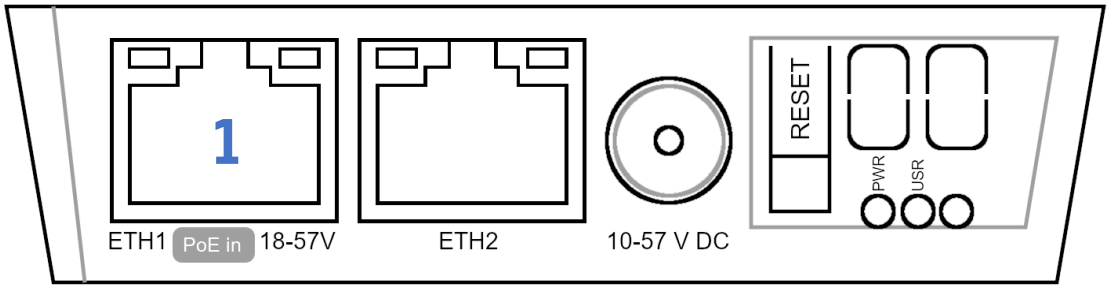
5. Punch out the square hole in the bottom section of the access point. Run the Ethernet cable through the hole.

6. Attach the access point to the mounting bracket. Align the tracks on the bracket, then slide the access point until it is held in place.

7. Thread the included screw through the center of the access point as in the diagram above. Tighten the screw to secure the access point to the mounting bracket.

8. Connect the Ethernet cable to ETH1. Close the cover and tighten the screw on the bottom to keep it in place and prevent access.

Quick Setup



CIS-ACWAP connections

1. Connect the Ethernet cable from your router to ETH1 on the access point. If your router supports PoE, turn it on to power the device. You may also use the included PoE injector.

2. (Optional) If PoE is unavailable or you prefer to plug in the DC adapter near the access point, connect the DC adapter directly to the DC jack on the access point.

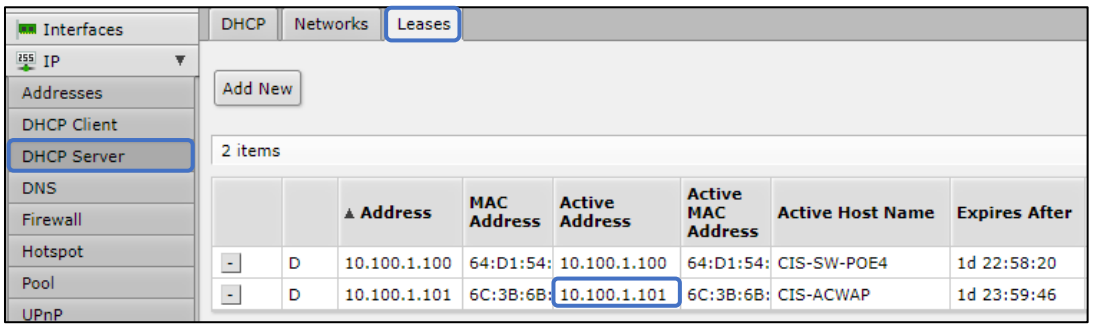
3. (Optional – AC WAP only) Connect an additional access point or device to ETH2. The port is bridged, meaning it acts like a switch port.

4. 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.

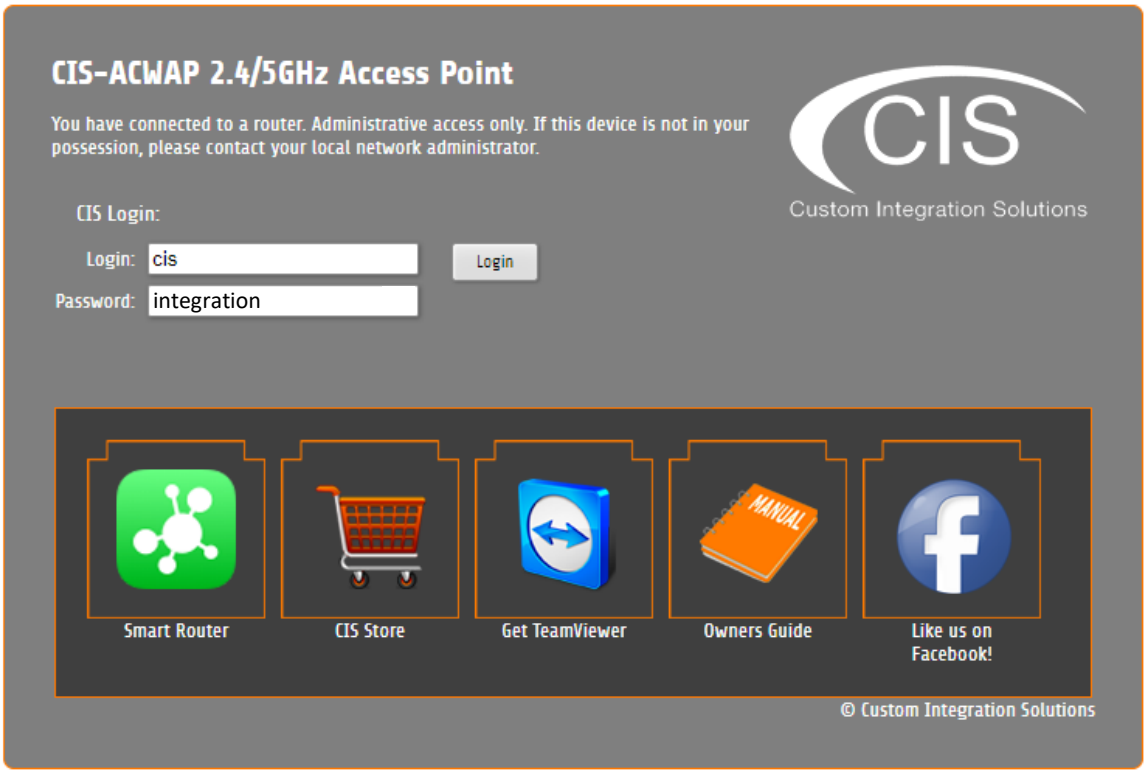
2. Obtain the IP address of your access points. If you're using a CIS router, access the web configuration by typing 10.100.1.1 in a web browser (10.100.1.1 is the default, but some systems may be different). Once logged in with the default credentials of **cis** and **integration** as the password,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



3. Enter the IP address of the access point in the address bar of your web browser.

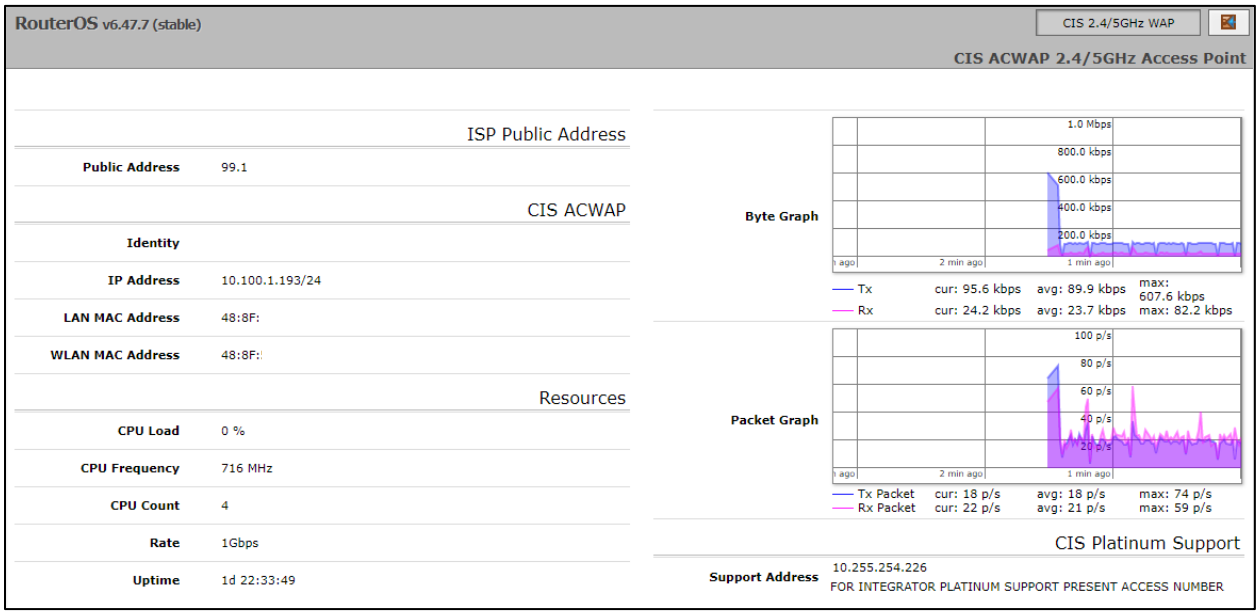
4. To login, use the default credentials **cis** and **integration** as the password.

5. Integrators may use the Get TeamViewer link if remote assistance is required.



The Status Page

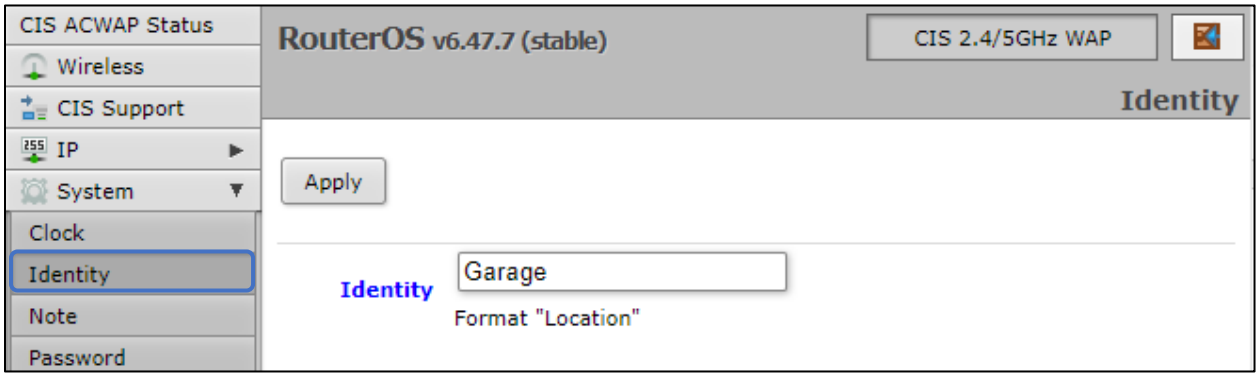
The status page provides basic diagnostic information. There is a CIS Support Address should you require assistance. You can view the identity (name) of the access point you are connected to, view it's public address, the traffic flowing through the device, and identify the MAC addresses of its interfaces.



Setting the Access Point's Identity

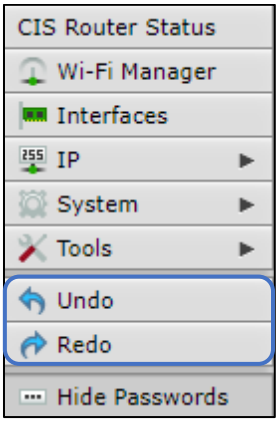
The identity is used to identify your device on the network. Troubleshooting will become easier when you set the identity correctly. Set the identity of the access point based on its location E.g., Basement.

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



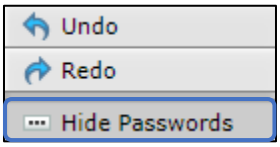
Undo / Redo

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



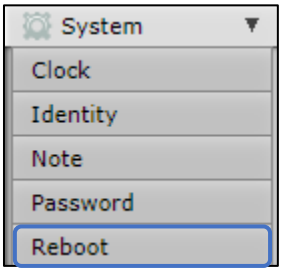
Show / Hide Passwords

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



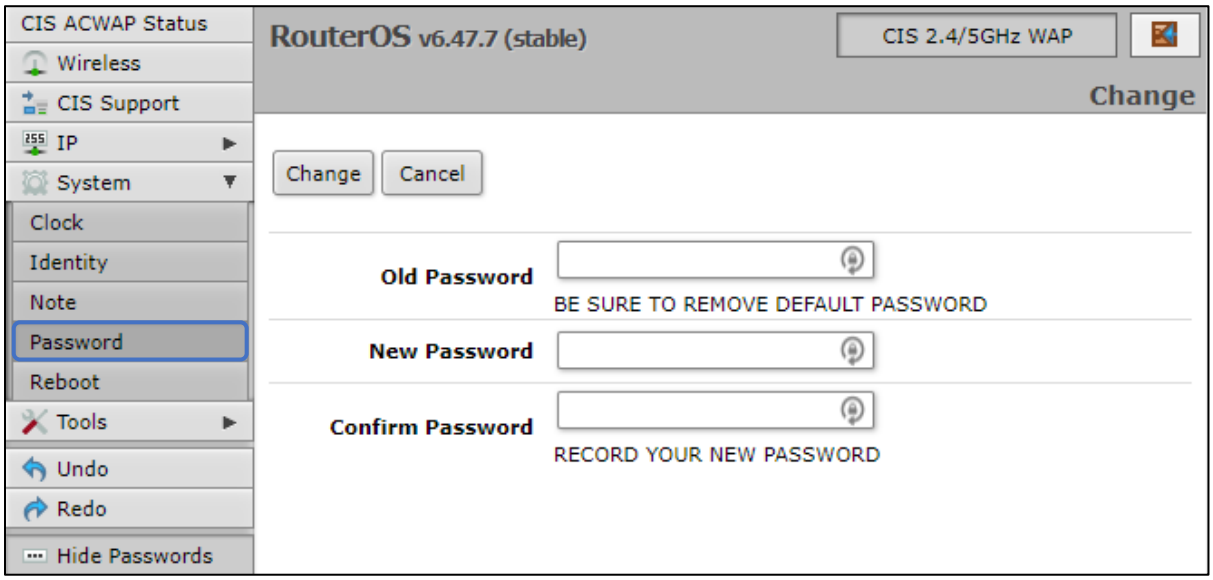
Rebooting the Device

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.



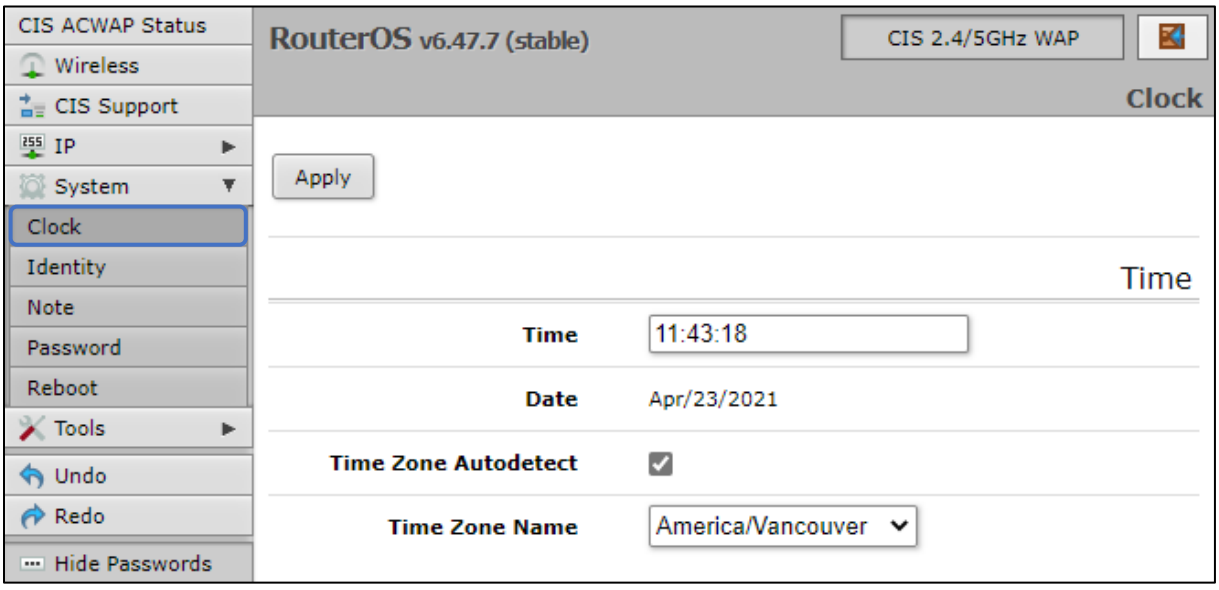
Changing the Default Password

After you log in for the first time, please create a new a 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.



Setting the Time Zone

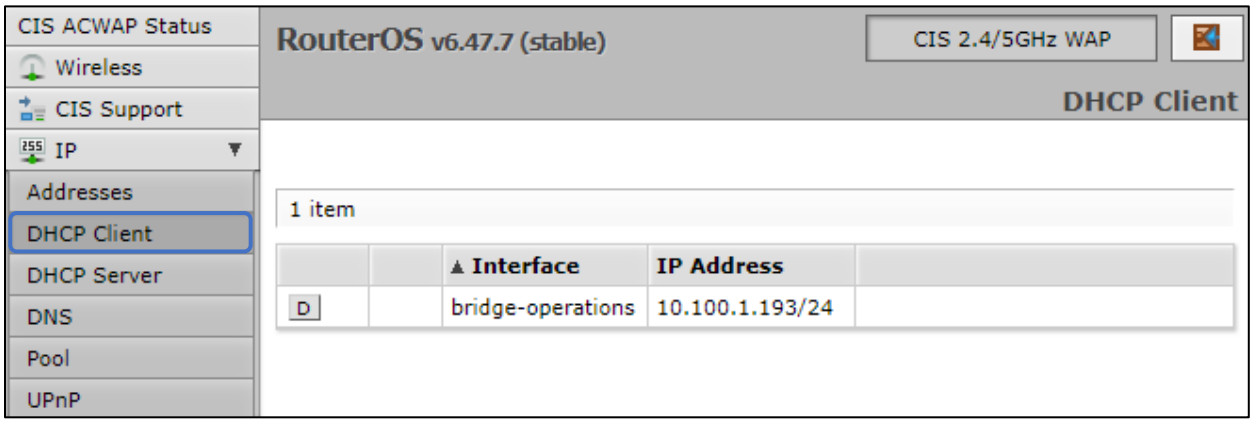
You can find the Clock settings under the System tab in the left toolbar. Select your time zone from the drop-down menu.



IP Addressing

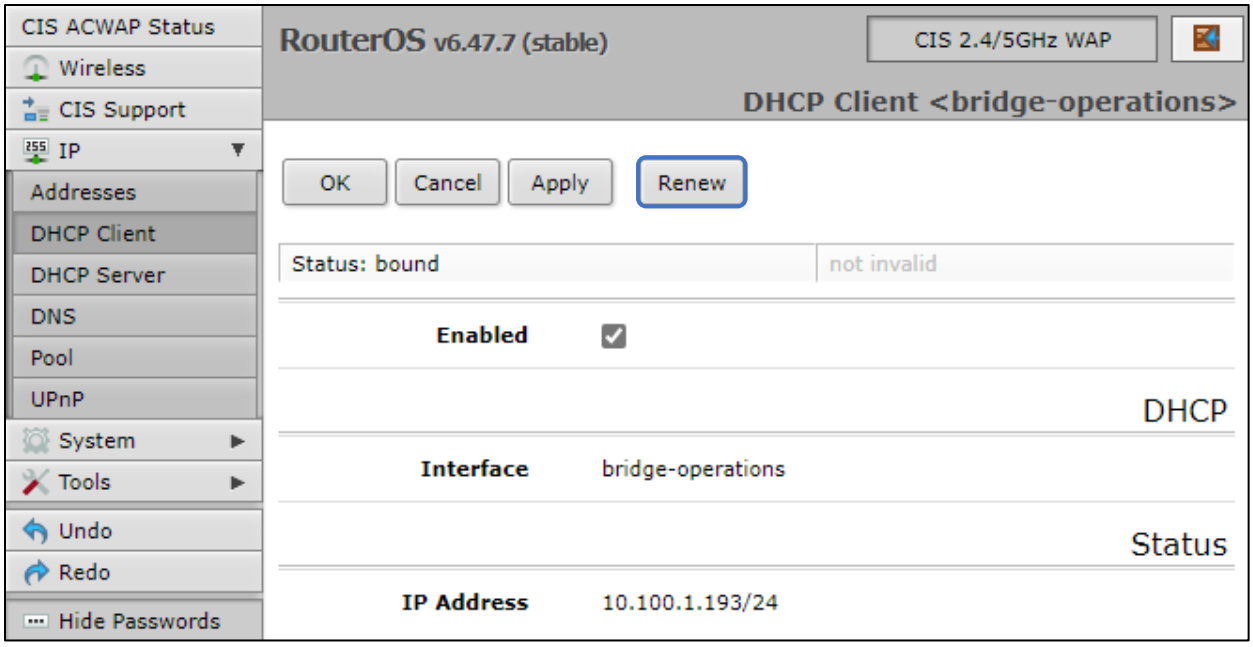
The DHCP Client Tab

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.



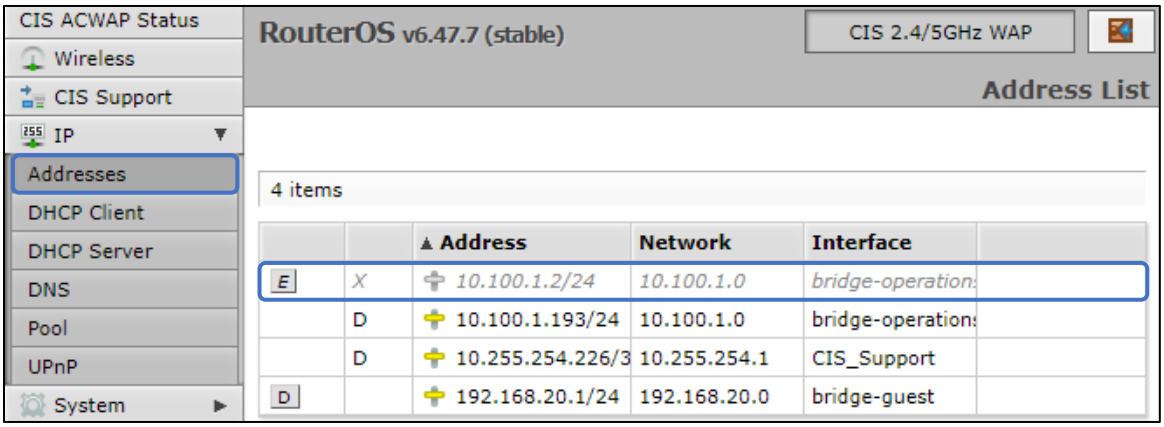
Renewing the IP Address

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



Setting a Static IP Address

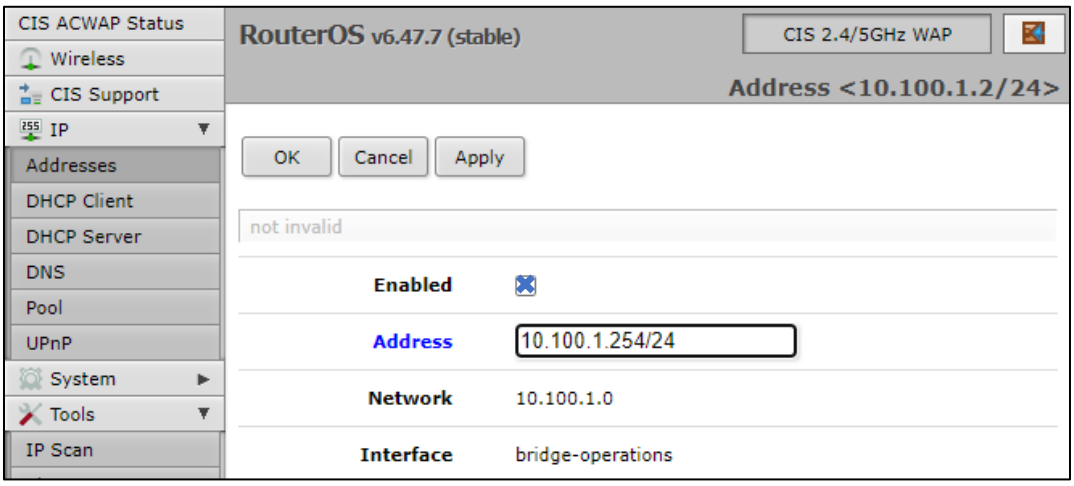
To set a static IP, select the **Addresses** tab under the **IP** section in the toolbar. There is an IP address entry that is disabled by default. Click on it.



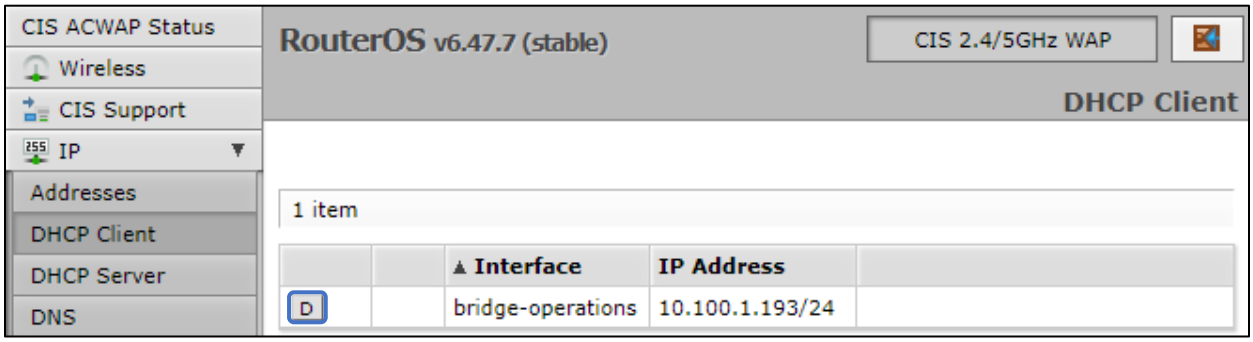
If your network falls in one of the ranges below, you can set the static IP address yourself. If it is outside of these ranges, you must call CIS to have a route created on the access point!

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

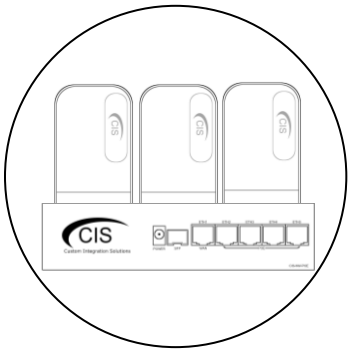
Check the **Enabled** box, then enter the IP address you would like to use. It MUST be in the range of your network, and outside of the range of the DHCP pool. The format must include **/24** at the end. This is the subnet mask, which determines how many devices can be connected to this network.



Once the static IP aSddress 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.



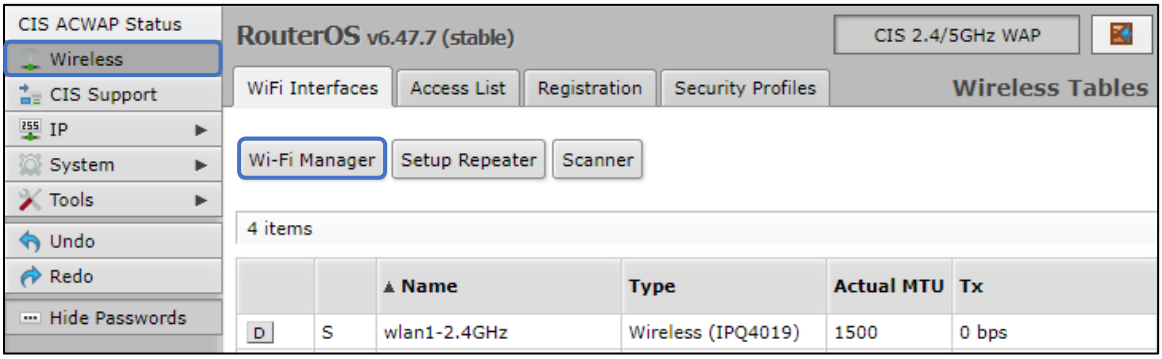
Managing Access Points with the Wireless Manager



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**.



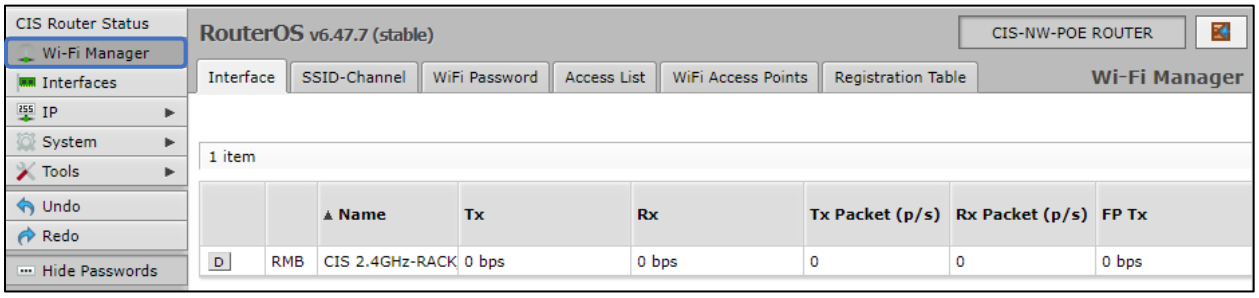
Check the **Enabled** box, click Apply, then OK.

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.

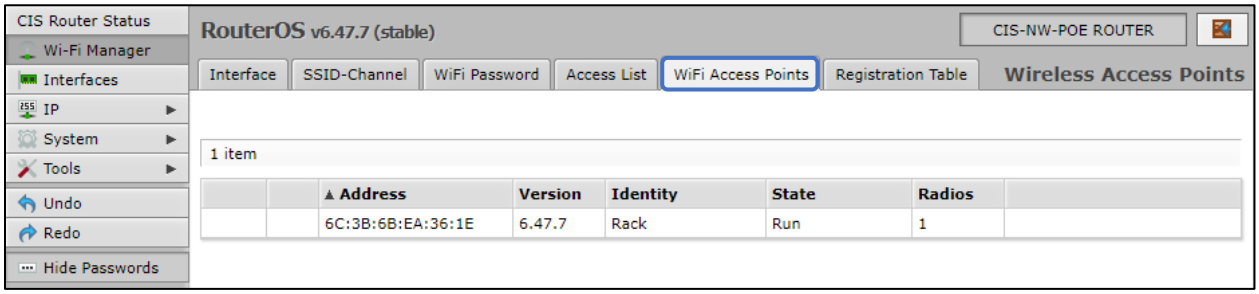
--- managed by CAPsMAN					
E	XS	wlan1-2.4GHz	Wireless (IPQ4019)	1500	0 bps
--- managed by CAPsMAN					
E	XS	wlan2-5GHz	Wireless (IPQ4019)	1500	0 bps

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.

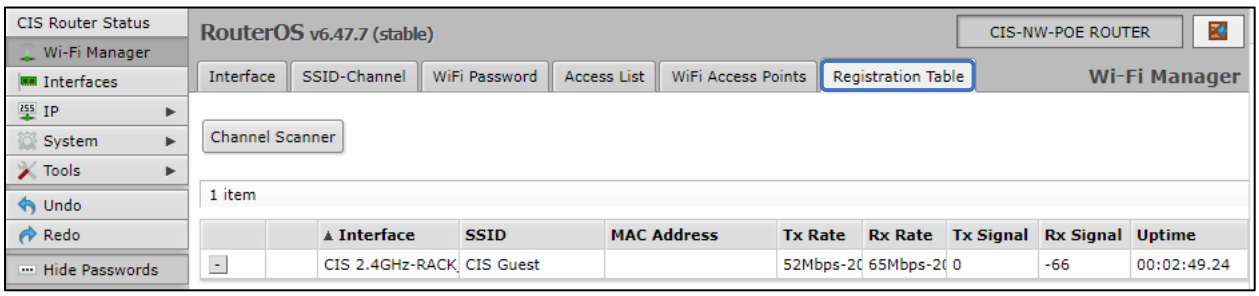


If you select the **WiFi Access points tab**, you'll be able to view the identity, MAC address and other information of the individual access points.



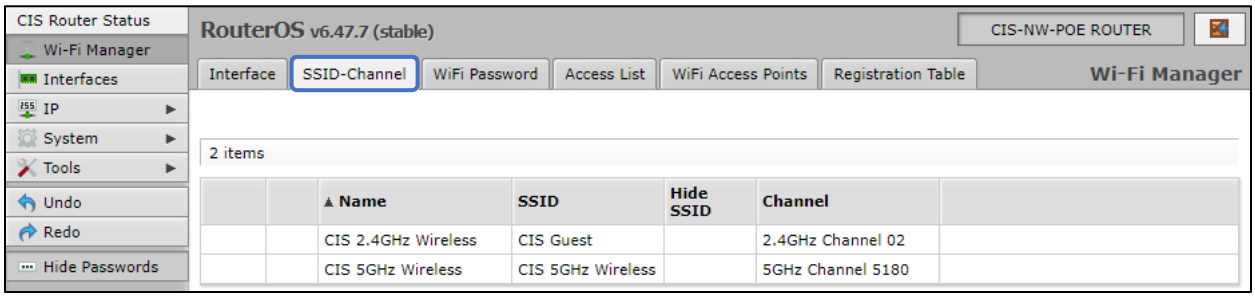
Viewing Connected Devices

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

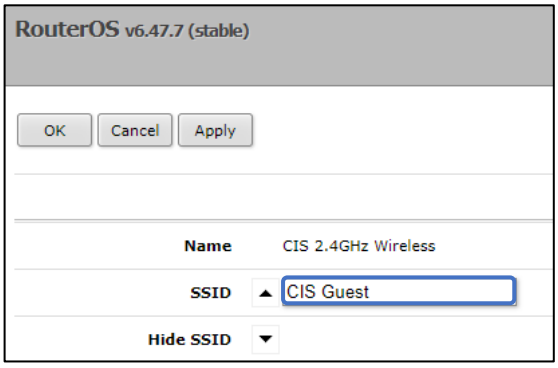


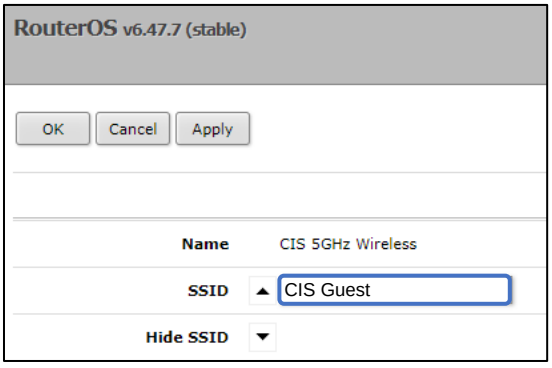
Changing the SSID of Managed Access Points

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



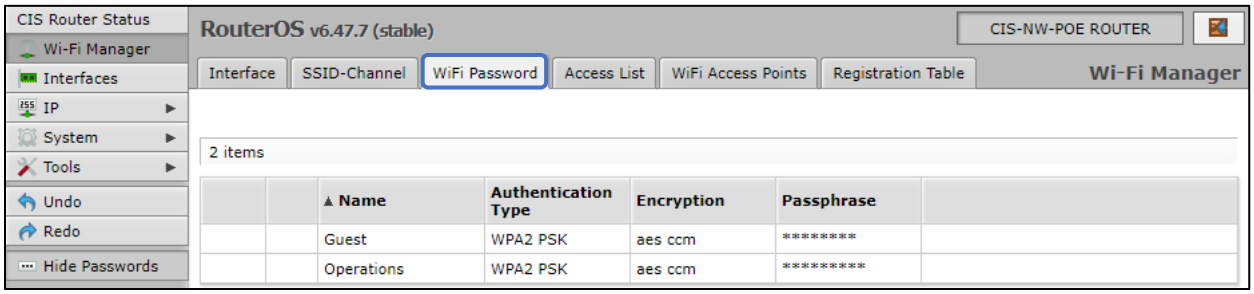
Enter the name of the SSID in the field. Copy and paste the SSID so that the 5GHz network has the same SSID.



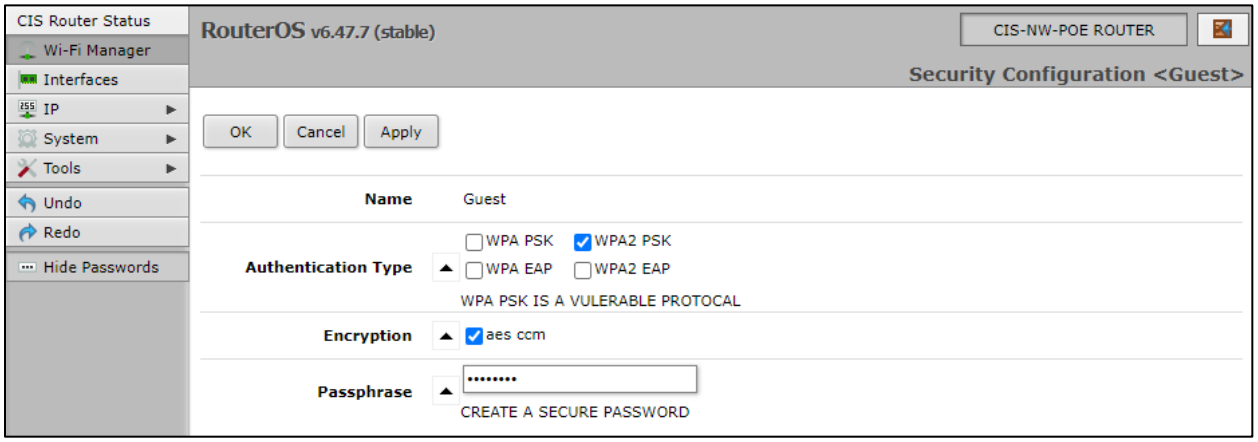


Changing the Wi-Fi Password of Managed Access Points

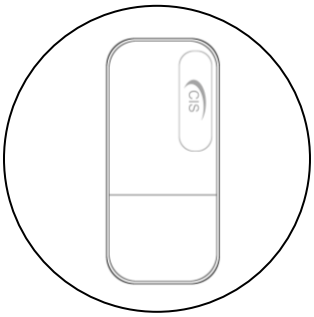
Select the **Wi-Fi Password** tab. Click on the network that you'd like to change the password for. If you've purchased a guest network, it will appear here.



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.



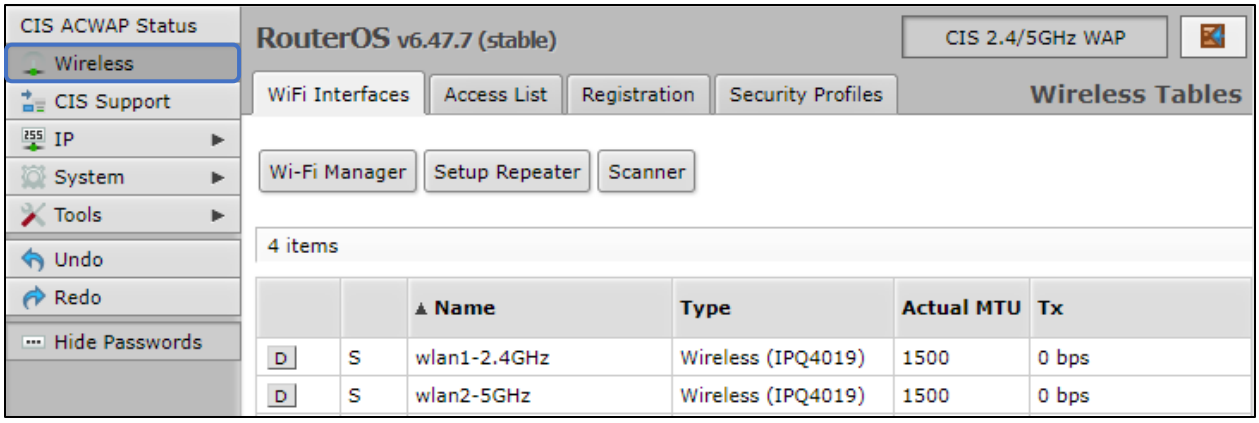
Configuring Access Points in Standalone Mode



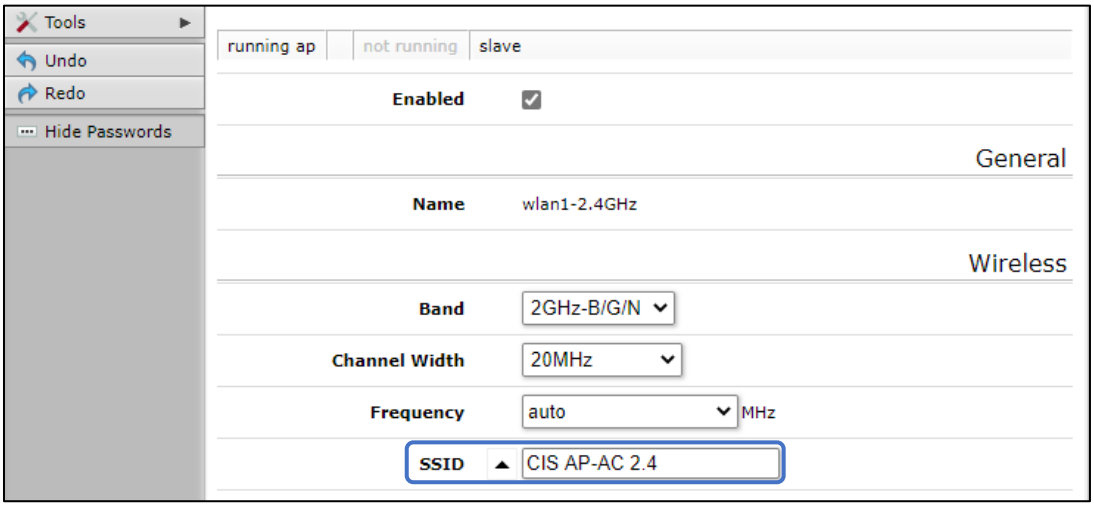
CIS access points can be centrally managed via the Wi-Fi manager on CIS routers, or they can operate as standalone units. This section includes instructions for setting up access points as standalone units.

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.

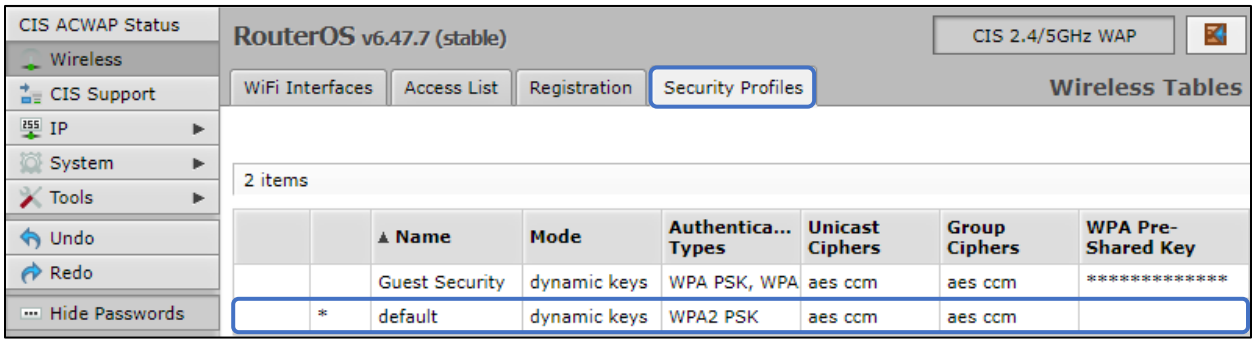


Click on one of the networks, then enter your SSID in the **SSID** box. Remember to change it for both the 2.4 GHz network and 5 GHz network! (CIS-ACWAP only).

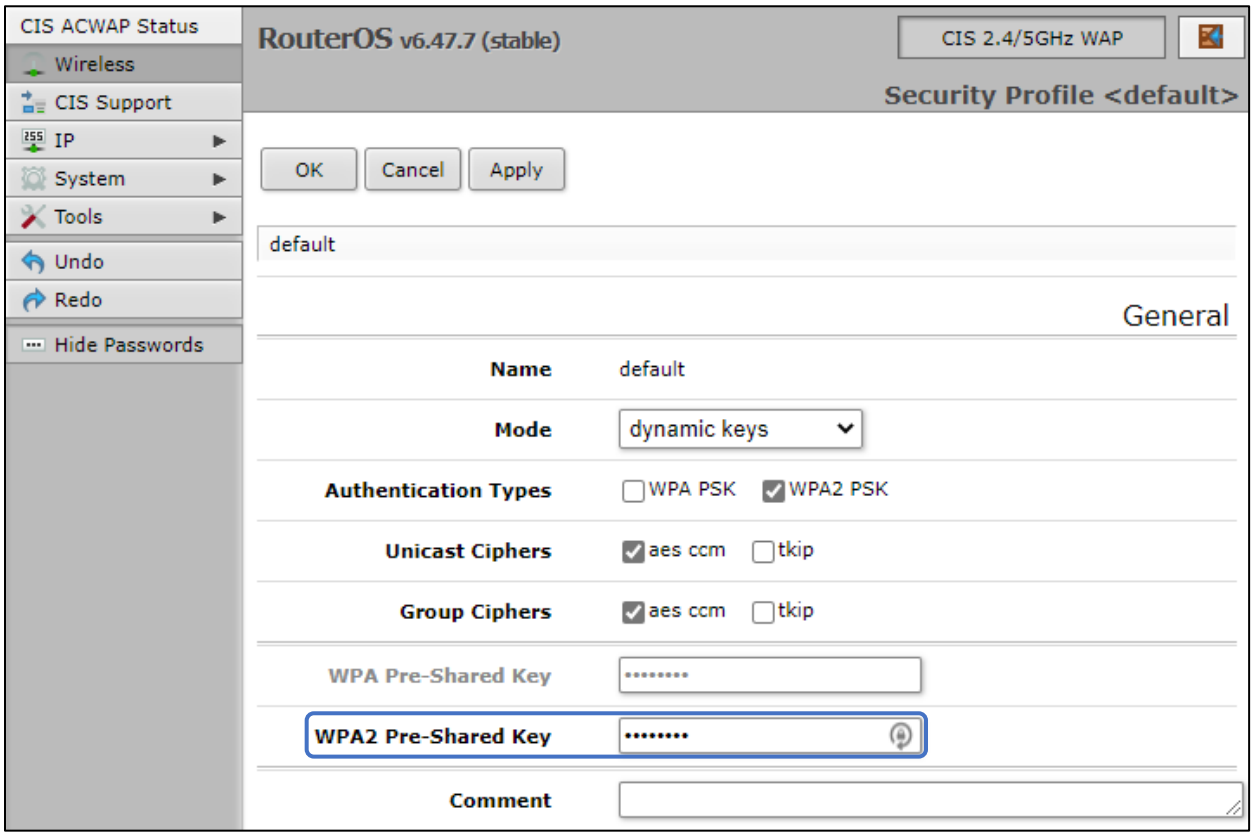


Setting the Wi-Fi Password for Standalone Access Points

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

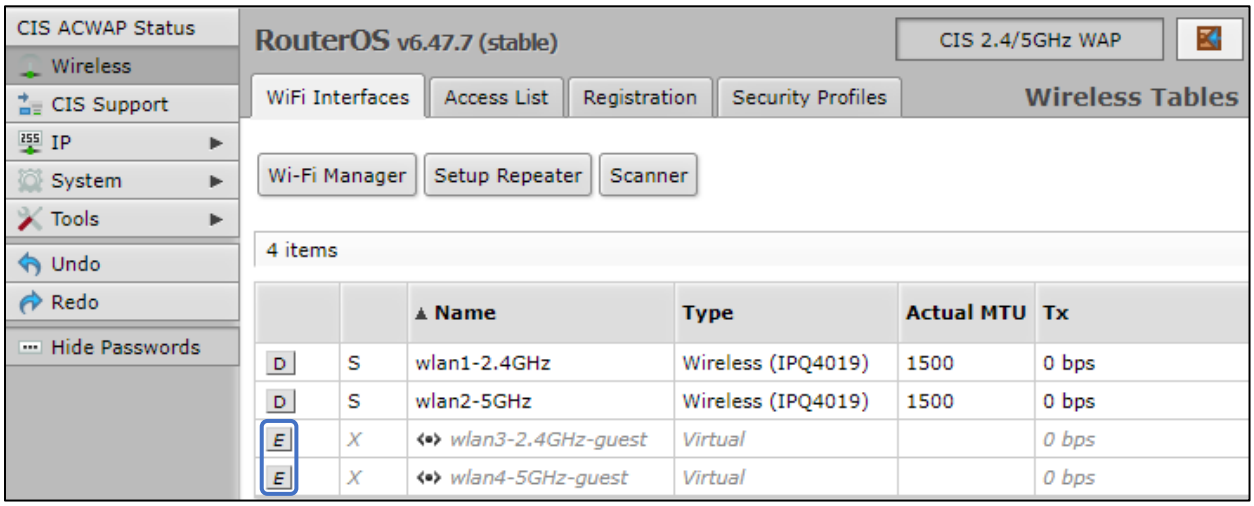


Enter the password in the **WPA2 Pre-Shared Key** field. CIS recommends you leave WPA PSK disabled, as it is a vulnerable protocol. If you have legacy devices that require it, enable it, and copy and paste the password into the WPA Pre-Shared Key field.

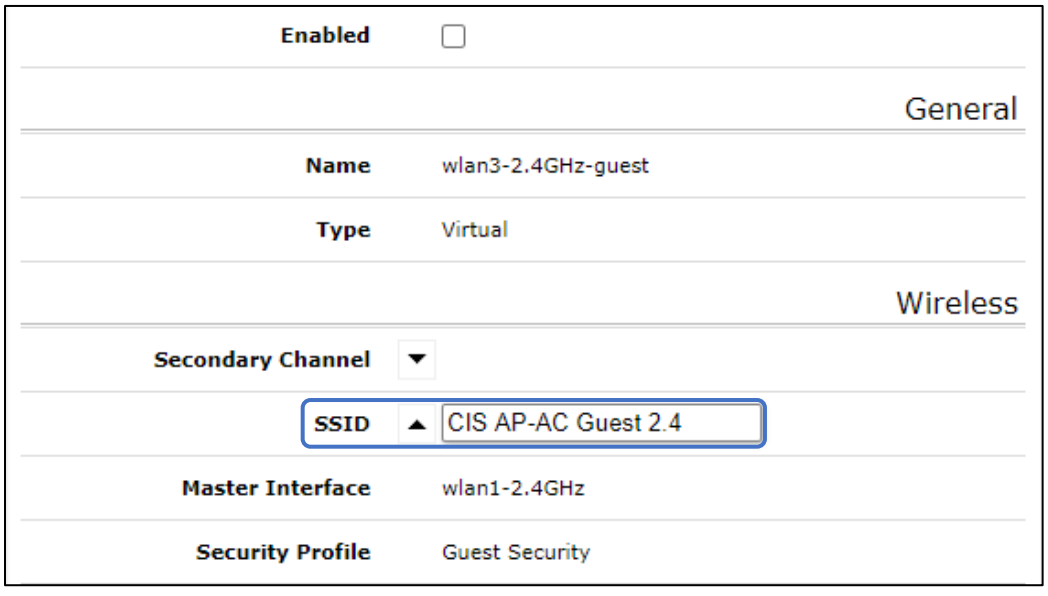


Enabling the Guest Network on Standalone Access Points

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 (CIS-ACWAP only).



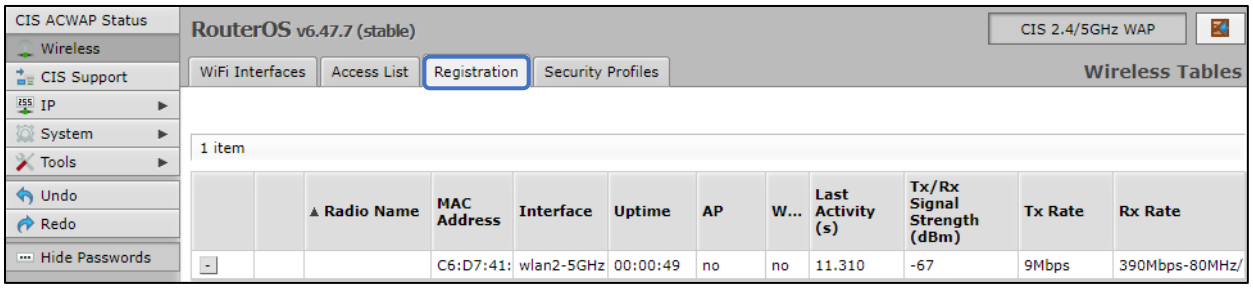
Devices in the guest network will receive different IP addresses and will be isolated from clients on the main network. Change the SSID by clicking on the virtual network.



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.

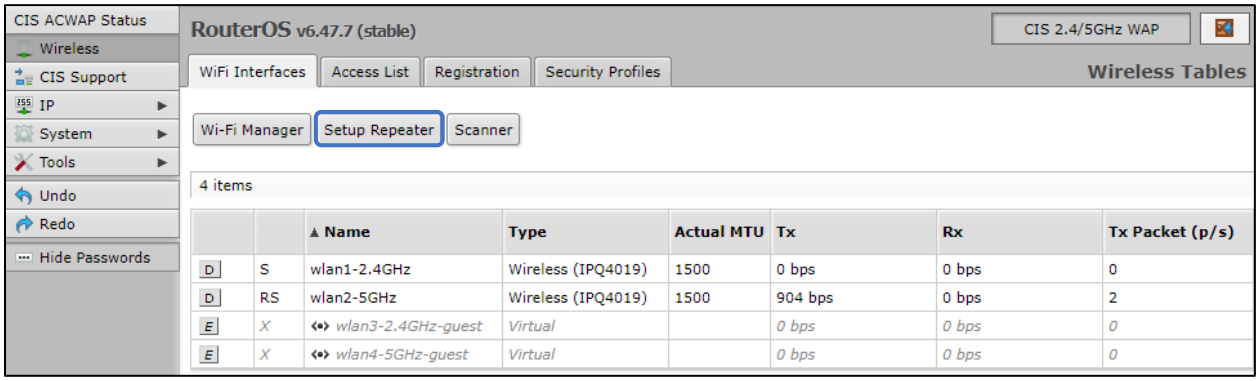
View Connected Devices

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.



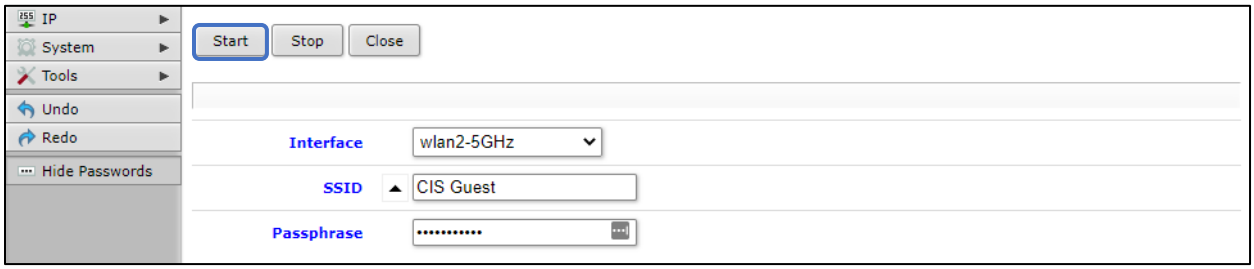
Setting up the Access Point as a Repeater

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



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**.

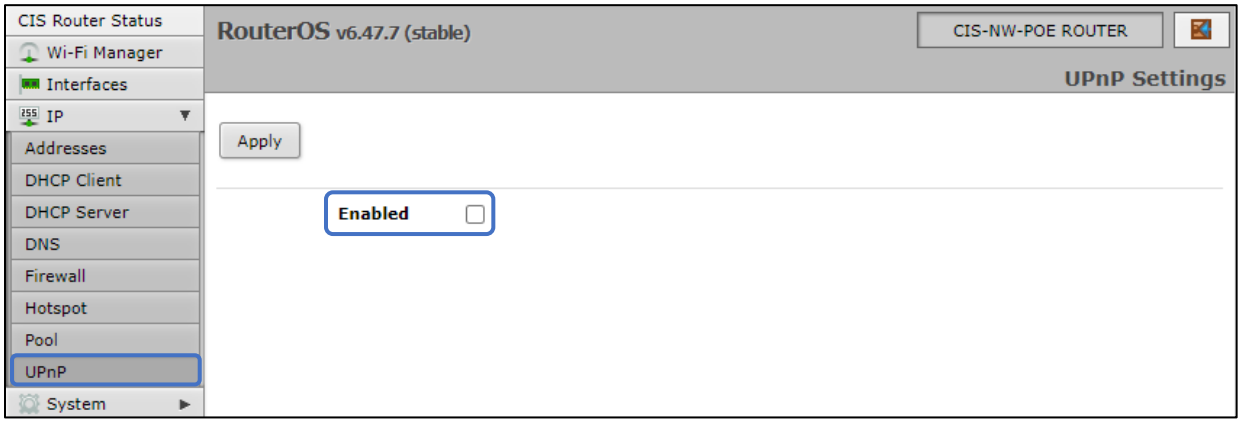
Note: You can only run a repeater on one band at a time. The 2.4 GHz band will offer better range.



Tools

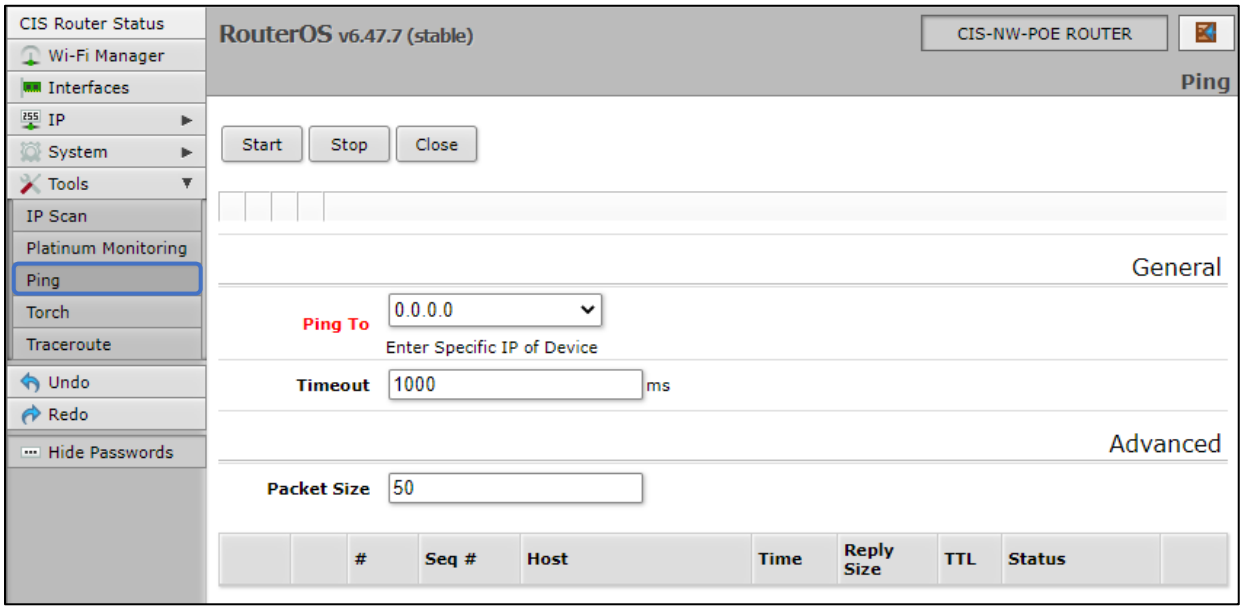
UPnP

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

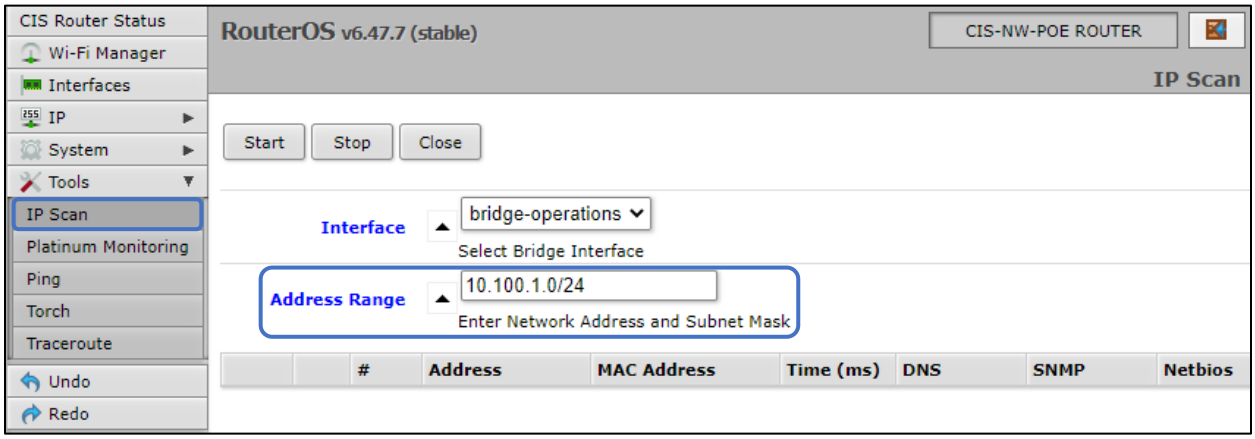
Ping uses Internet Control Message Protocol (ICMP) echo messages to determine if a remote host is active. It will also provide the round-trip time between the hosts. Enter the IP address of the device and select Start to begin.



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.



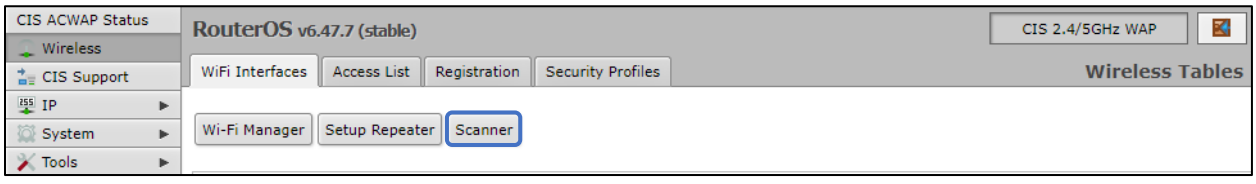
*Select **bridge-operations** and enter **10.100.1.0/24** as the address range. You may have multiple interfaces and address ranges depending on your configuration. Most use a /24 network size.*

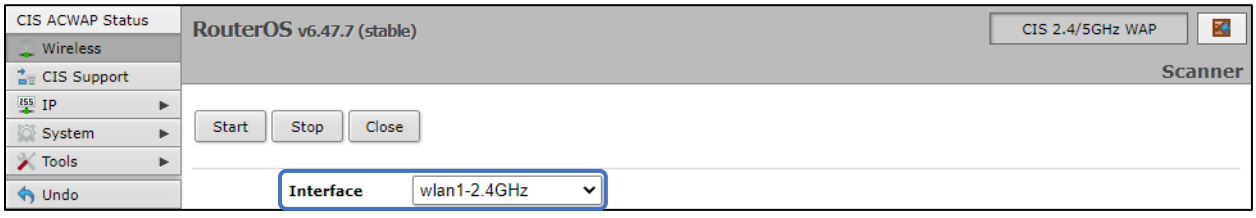
Wireless Scanner

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**.





Troubleshooting

Symptom	Possible causes
The devices are having trouble maintaining a connection to the wireless network.	• Check the signal strength in the registration table. A healthy signal range is between -30 and -75 dB. • 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. • 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.
The device won't connect to the wireless network at all.	• Ensure the device is in range of the access point. • Temporarily disable all access points except the one closest to the device. Some devices have issues with multiple access points with the same SSID. • 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. • 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. • Ensure that the passphrase is correct.
I am not receiving the speed that I am expecting.	• The CIS-ACWAP has been tested to achieve approximately 480 mbps in our testing. • The vast majority of access points and client devices will not provide or support the full throughput of a 1 Gbps internet connection. • Test the speed of your device when it is plugged into the wired network if possible. Compare the results.

<table>
<tr>
<td>The speed is particularly slow.</td>
<td>

Ensure there is adequate coverage throughout the building.
We recommend one access point for every 1000 sq ft for adequate 5 GHz coverage.
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:

<table>
<tr><th>Type of Barrier</th><th>Interference Potential</th></tr>
<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>
</table>
The following are sources of interference that can affect Wi-Fi performance:

Microwave ovens.
Power sources – breaker boxes, etc.
Cordless home phones.
Wireless video transmitters.
Wireless speakers.
Poorly shielded cabling.

</td>
</tr>
<tr>
<td>The access point will not turn on.</td>
<td>

Most issues occur when the access point is used with PoE.
Ensure the router or switch is capable of providing PoE. Some devices only support PoE on specific ports.
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.
CIS routers and switches provide more stable PoE when the port is set to “Forced On”. Review the user manuals for instructions.

</td>
</tr>
</table>

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

Phone: Technical Support - (888) 976-3651

Email: activations@custom-integration-solutions.com

CE

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