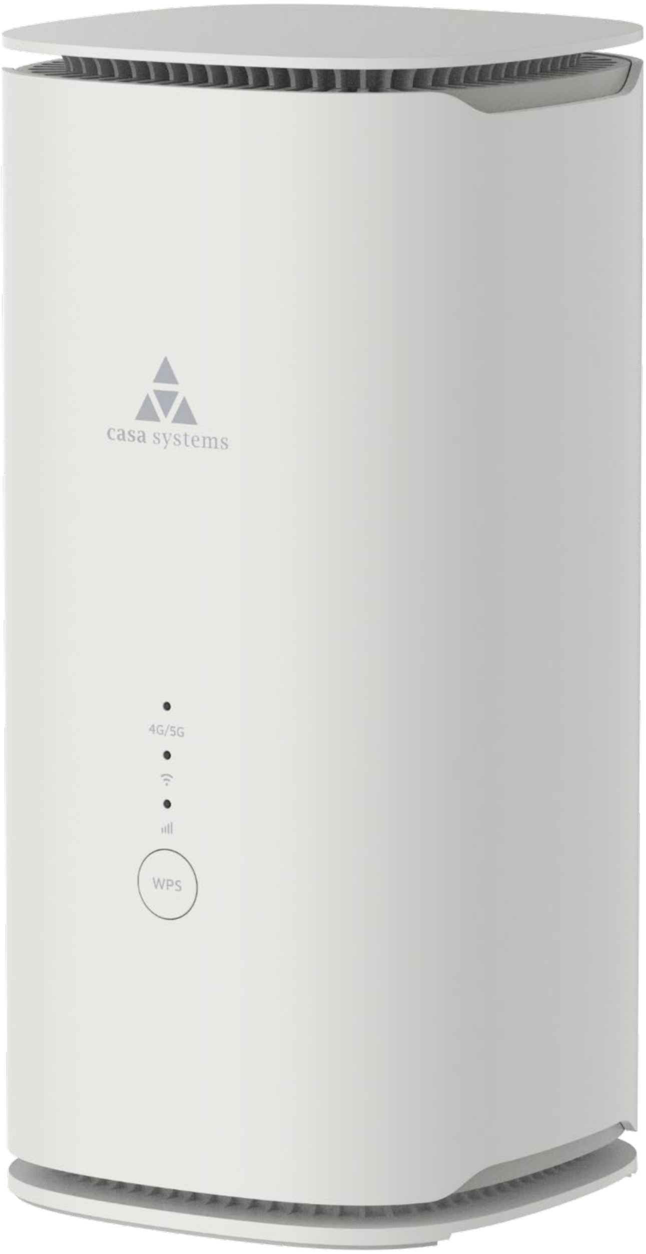
casa systems

User Guide

CFW-4221/4222



Doc No. UG01433

Important notice

This device, like any wireless device, operates using radio signals which cannot guarantee the transmission and reception of data in all conditions. While the delay or loss of signal is rare, you should not rely solely on any wireless device for emergency communications or otherwise use the device in situations where the interruption of data connectivity could lead to death, personal injury, property damage, data loss, or other loss. NetComm Wireless accepts no responsibility for any loss or damage resulting from errors or delays in transmission or reception, or the failure of the Casa CFW-4221/4222 to transmit or receive such data.

Copyright

Copyright© 2022 Casa Systems. All rights reserved.

The information contained herein is proprietary to Casa Systems. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without prior written consent of Casa Systems.

Trademarks and registered trademarks are the property of Casa Systems or their respective owners. Specifications are subject to change without notice. Images shown may vary slightly from the actual product.

NetComm Wireless Limited was acquired by Casa Systems in 2019.

ⓘ Note – This document is subject to change without notice.

Document history

This document relates to the following product:

Casa Systems AurusGate (CFW-4221/4222)

Ver.	Document description	Date
v0.03	DRAFT	n/a

Table i. – Document revision history

Contents

© Casa Systems 2022

© Casa Systems 2022

© Casa Systems 2022

Overview

Introduction

This document provides a detailed description of the device, including instructions on configuring and using the CFw-4221 or CFW-4222 gateway.

Prerequisites

To configure your gateway, you will require a computing device with a web browser and either a wired or wireless network adapter.

Notation

The following symbols may be used in this document:

ⓘ Note – This note contains useful information.

⚠ Important – This is important information that may require your attention.

⚠ Warning – This is a warning that may require immediate action in order to avoid damage or injury.

© Casa Systems 2022

Product overview

- Easy to install 5G/LTE WiFi 6 Indoor residential gateway
- Installed by the consumer allowing fast time to customer fulfilment
- Supporting a wide range of 3GPP Frequency Bands from 600MHz up to 4.2GHz, it is suitable for deployment in the majority of regions globally
- Includes an integrated 4x4 MIMO Low-Gain OMNI Directional Antenna
- Remotely manageable (FM, CM, PM, SM) via BBF TR-069, SSH and HTTP/S
- Additional consumer smartphone application available to provide efficient installation process suitable for a non-technical consumer audience.

Interfaces

The gateway is designed to be placed upright on a table.

Its LED indicators and **WPS** button are on the on the front of the gateway.

Cables exit from the rear for easy organization. The power input is located below the data sockets.

The power **ON/OFF** switch and the **Reset** buttons are on the bottom. The **SIM** slot is also located on the bottom of the gateway.

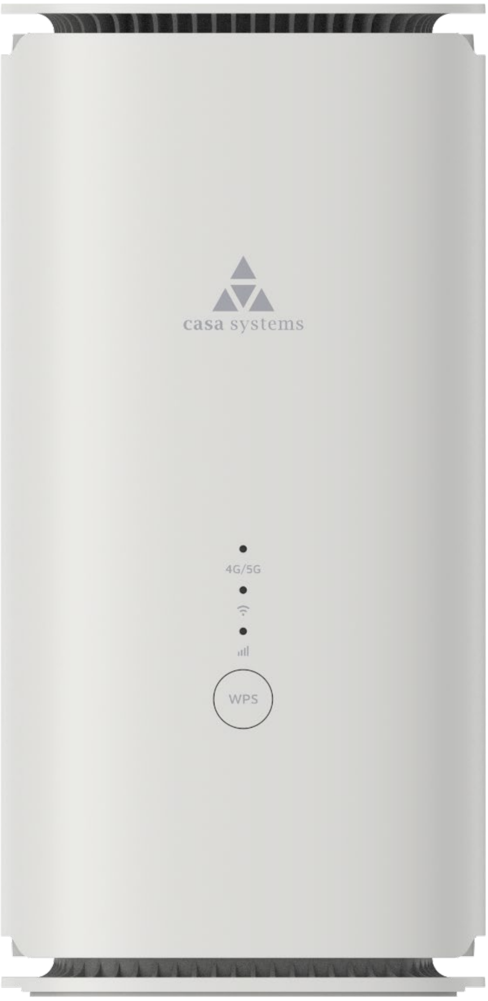


Figure 1 - LED icons

Front view

The LED display visible on the front of the gateway provides you with information about network activity and the device status.

The WPS button allows you to easily pair a Wi-Fi device with the gateway.

LED indicators

The following table contains an explanation of each of the indicators on the front of the gateway.

LED	Icon	Colour		Definition
All three LEDs simultaneously	● 4G/5G ● 🛜 ● 📶	🔴	Red blinking	Firmware upgrade in progress
		🔴		
		🔴		
4G / 5G	● 4G/5G	⚪	White solid	Gateway is connected to 5G network
		🔵	Blue solid	Gateway is connected to 4G network
		🔴	Red solid	SIM PIN/PUK is locked

© Casa Systems 2022

LED	Icon	Colour		Definition
		●	Orange solid	No network
		✺	Orange blinking	Gateway is powering up
Wi-Fi icon	● 🛜	○	White solid	Wi-Fi is normal
		✺	White blinking	Press the WPS button
		●	Off	Wi-Fi is unusual
Signal strength	● 📶	○	White solid	Signal strength is excellent
		●	Blue solid	Signal strength is good
		●	Orange solid	Signal strength is fair
		●	Red solid	Signal strength is poor

Table 1 - LED icon descriptions

Rear view

The following interfaces are located on the rear panel of the gateway:

Interface	Description
WAN/LAN1	The WAN/LAN1 port functions as a WAN port by default and may be toggled to function as a LAN port via the web user interface.
LAN2	The LAN2 port is a second LAN port. Connect a device to this port using Ethernet cable to provide it with internet access.
Power supply jack	Connect the supplied power supply to this jack. Only use the power adaptor supplied with the gateway.

Table 2 – Interface descriptions

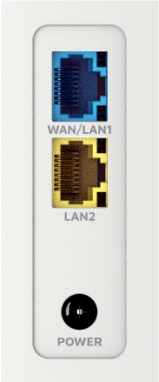


Figure 2 – Gateway rear view

Bottom view

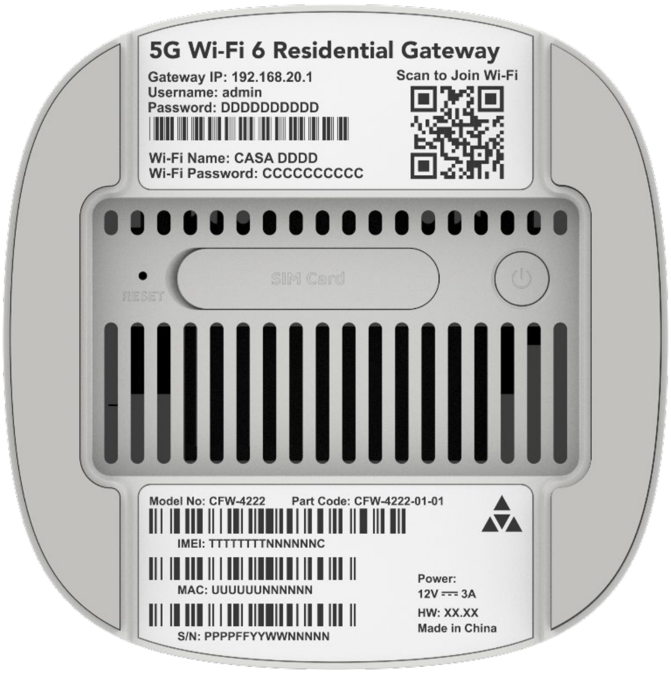


Figure 3 – Bottom view

Interface	Description
Reset button	
SIM Card slot	The SIM card slot is housed underneath a flap to prevent dust ingress. To access the SIM card slot, first open the flap.
On/Off button	Toggles the power on and off.

Table 3 - Side buttons

Safety and product care

Your gateway is an electronic device that sends and receives radio signals. Please take the time to read this list of precautions that should be taken when installing and using the router.

- Do not disassemble the gateway. There are no user-serviceable parts.
- Do not allow the gateway to come into contact with liquid or moisture at any time. To clean the device, wipe it with a damp cloth.
- Do not restrict airflow around the device. This can lead to the device overheating.
- Do not place the device in direct sunlight or in hot areas.

Transport and handling

When transporting the gateway, we recommend returning the product in its original packaging. This helps to reduce the risk of damage to the product.

⚠ Attention – In the event the product needs to be returned, ensure it is securely packaged with appropriate padding to prevent damage during courier transport.

Placement of your gateway

The wireless connection between your gateway and your wireless devices will be strong when they are in close proximity and have direct line of sight. As your client device moves further away from the gateway or solid objects block direct line of sight to the router, your wireless connection and performance may degrade. This may or may not be directly noticeable and is greatly affected by the individual installation environment.

If you have concerns about your network's performance that might be related to range or obstruction factors, try moving the computer to a position between three to five metres from the gateway to see if distance is the problem.

ℹ Note – While some of the items listed below can affect network performance, they will not prohibit your wireless network from functioning; if you are concerned that your network is not operating at its maximum effectiveness, this check list may help

Try not to place the gateway near a cordless telephone that operates at the same radio frequency as the gateway (2.4GHz/5GHz).

Avoiding obstacles and interference

Avoid placing your gateway near devices that may emit radio "noise," such as microwave ovens. Dense objects that can inhibit wireless communication include:

- Refrigerators
- Washers and/or dryers
- Metal cabinets
- Metallic-based, UV-tinted windows

If your wireless signal seems weak in some spots, make sure that objects such as those listed above are not blocking the signal's path (between your devices and the gateway).

Cordless phones

If the performance of your wireless network is impaired after considering the above issues, and you have a cordless phone:

Try moving cordless phones away from your gateway and your wireless-enabled computers.

Unplug and remove the battery from any cordless phone that operates on the 2.4GHz or 5GHz band (check manufacturer's information). If this fixes the problem, your phone may be interfering with the gateway.

If your phone supports channel selection, change the channel on the phone to the farthest channel from your wireless network. For example, change the phone to channel 1 and move your gateway to channel 11. See your phone's user manual for detailed instructions.

If necessary, consider switching to a 900MHz or 1800MHz cordless phone.

Choose the "quietest" channel for your wireless network

In locations where homes or offices are close together, such as apartment buildings or office complexes, there may be wireless networks nearby that can conflict with your wireless network. Your wireless adapter may include a utility to assist in scanning for the least congested network, otherwise you may be able to find another piece of software that can be used. These tools display a graphical representation of the wireless networks in range and the channels on which they are operating.

Try to find a channel which is not as busy and does not overlap with another one. Channels 1, 6 and 11 are the only channels on 2.4GHz which do not overlap with one another, and you should ideally choose one of these channels.

Experiment with more than one of the available channels to find the clearest connection and avoid interference from neighbouring cordless phones or other wireless devices.

© Casa Systems 2022

Advanced configuration

The AurusGate will function out of the box simply by inserting a SIM card and connecting your devices to its wireless network or local network ports. However, if you wish to change any of the default settings, you can access the web interface.

1 If the AurusGate has not been turned on, push the power button on the bottom of the gateway to turn it on. Wait for about two minutes for it to complete starting up.

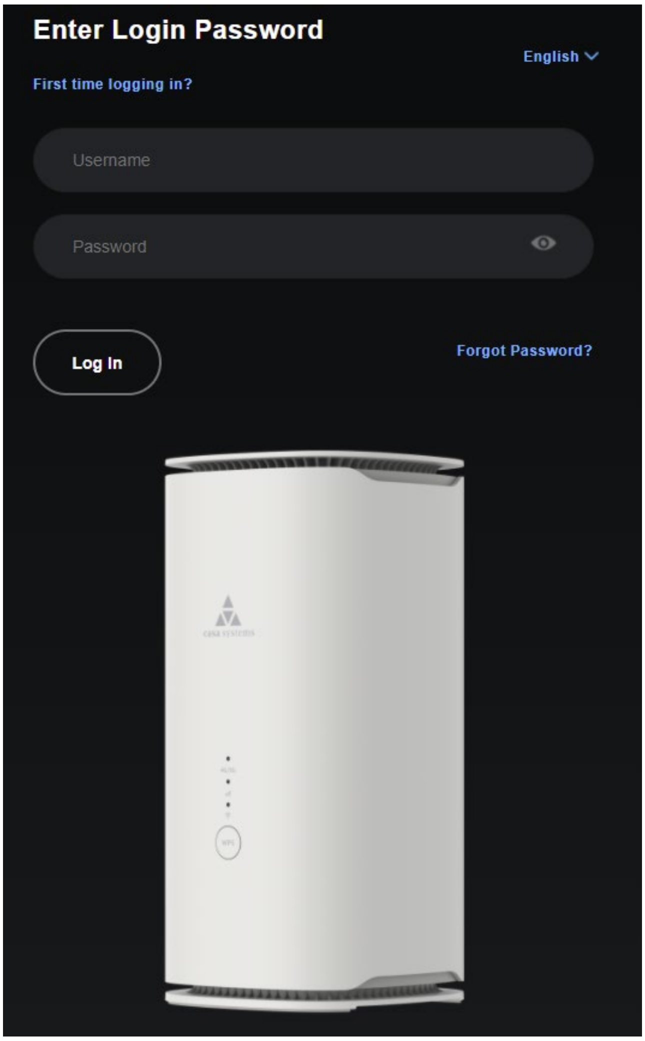
2 Open a web browser and type 192.168.1.1 into the address bar, then press Enter.

3 At the Enter Login Password screen:

   a Type admin into the Username field.

   b Type admin into the Password field.

   c Select the Log In button.



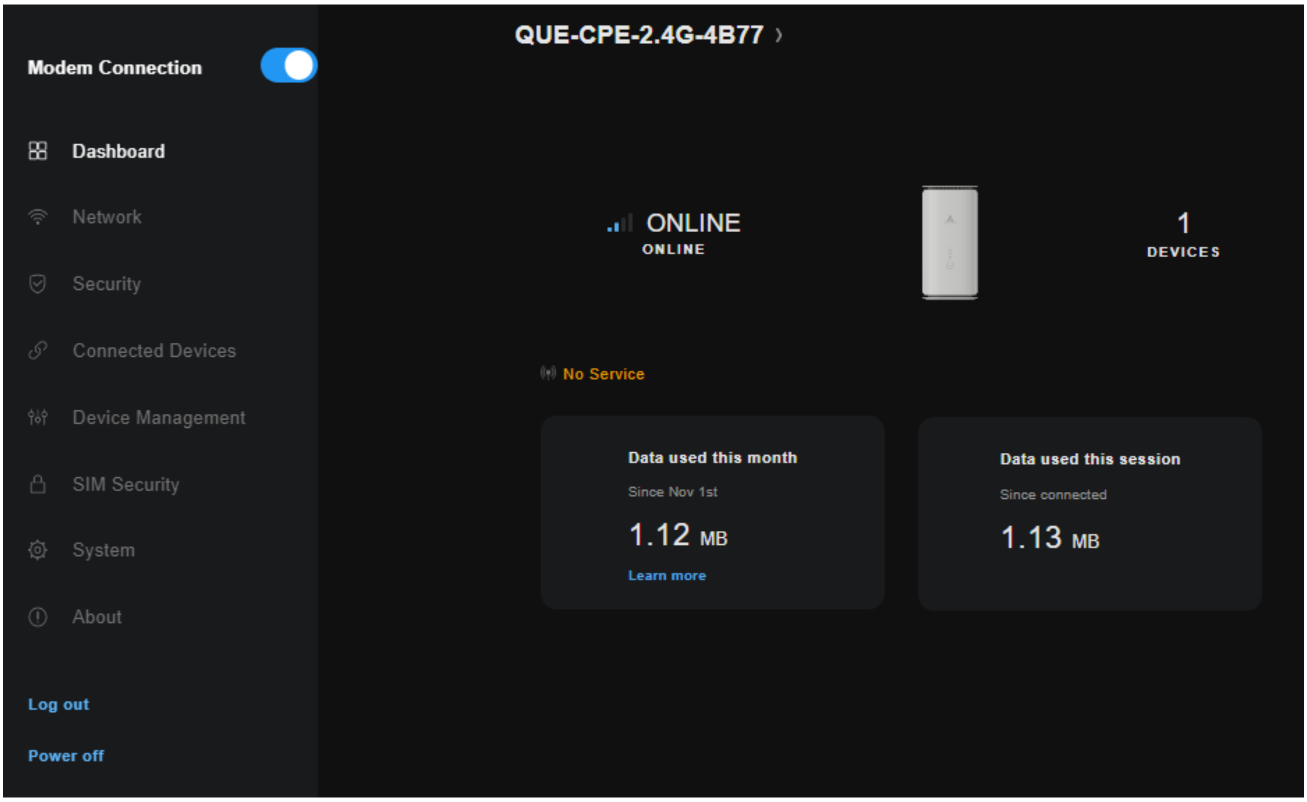
Enter Login Password

Figure 4 - Enter Login Password screen

Note – If you have previously changed the password, enter your chosen password instead.

Dashboard

The **Dashboard** page is first displayed after you have successfully logged into the gateway. This page gives you an overview of important information regarding the gateway and the configuration of your WAN connection.



QUE-CPE-2.4G-4B77 ›

ONLINE
ONLINE

1
DEVICES

No Service

Data used this month
Since Nov 1st
1.12 MB

Data used this session
Since connected
1.13 MB

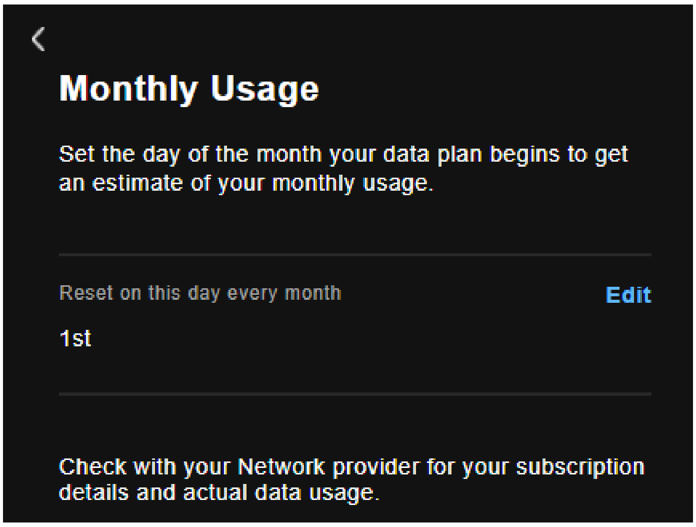
Figure 5 - Device Info page

The page provides an overview of

Field	Description
Modem Connection	
Wi-Fi link	
Connection status	
SIM status	
Devices	
Service Status	
Data used this month	
Data used this session	

Table 4 – Dashboard display table

Learn More



Monthly Usage

Set the day of the month your data plan begins to get an estimate of your monthly usage.

Reset on this day every month

1st

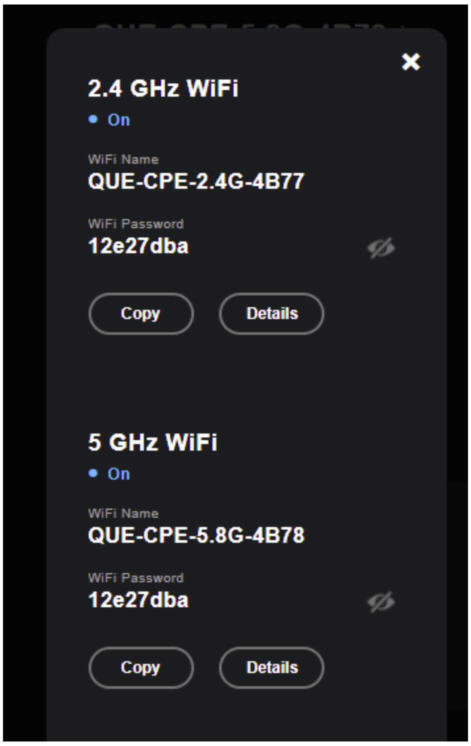
Check with your Network provider for your subscription details and actual data usage.

Figure 6 – Wi-Fi dashboard page

Click the **Edit** button to set the day of the month to begin the monthly report.

Wi-Fi details shortcut

At the top of the screen, select the Wi-Fi network name to view the status and credentials of your wireless networks as well as a Details link to take you to the advanced wireless settings page.



2.4 GHz WiFi

On

WiFi Name

QUE-CPE-2.4G-4B77

WiFi Password

12e27dba

5 GHz WiFi

On

WiFi Name

QUE-CPE-5.8G-4B78

WiFi Password

12e27dba

Figure 7 – Wi-Fi details shortcut

Network

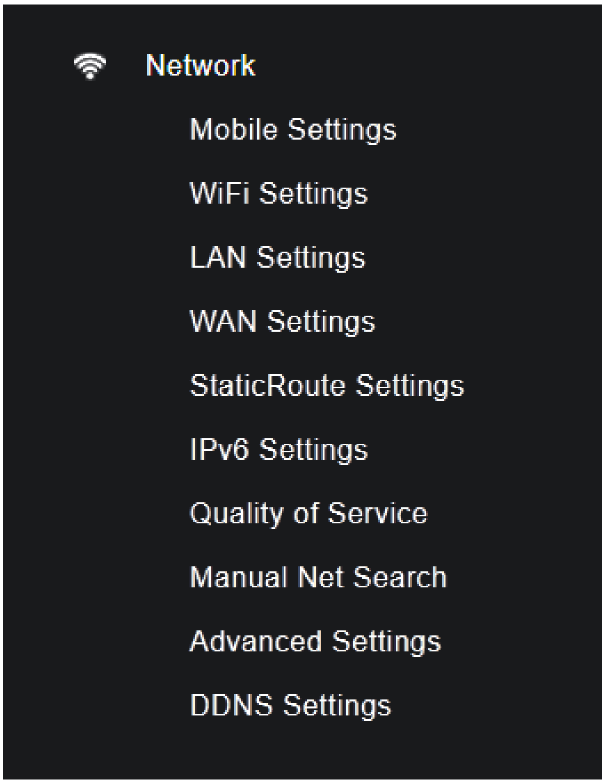


Figure 8 – Network menu

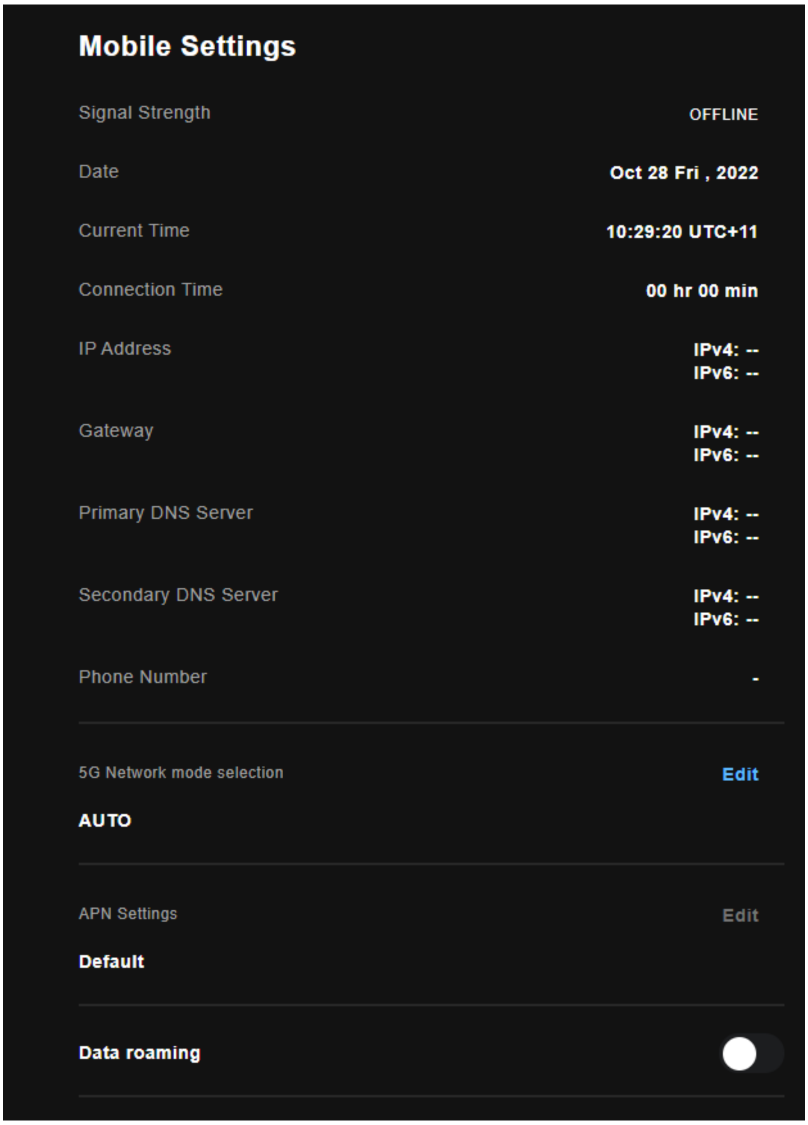
This Network section of the menu on the left side of the screen provides a variety of options for configuring advanced network settings on the gateway.

In most cases, you will not need to modify settings under the Network menu and we recommend that you do not change many of the settings unless you are sure of the effect that the changes will have, and have a backup of your current working configuration.

Mobile Settings

To view and make changes to the mobile service settings select **Mobile Settings** from the **Network** menu.

The **Mobile Settings** page opens:



Mobile Settings

Signal Strength	OFFLINE
Date	Oct 28 Fri , 2022
Current Time	10:29:20 UTC+11
Connection Time	00 hr 00 min
IP Address	IPv4: -- IPv6: --
Gateway	IPv4: -- IPv6: --
Primary DNS Server	IPv4: -- IPv6: --
Secondary DNS Server	IPv4: -- IPv6: --
Phone Number	-

5G Network mode selection: AUTO

APN Settings: Default

Figure 9 – Mobile settings

The following options are available to configure:

Parameter	Definition
Signal Strength	Parameters include: OFFLINE –
Date	
Current Time	
Connection Time	
IP Address	

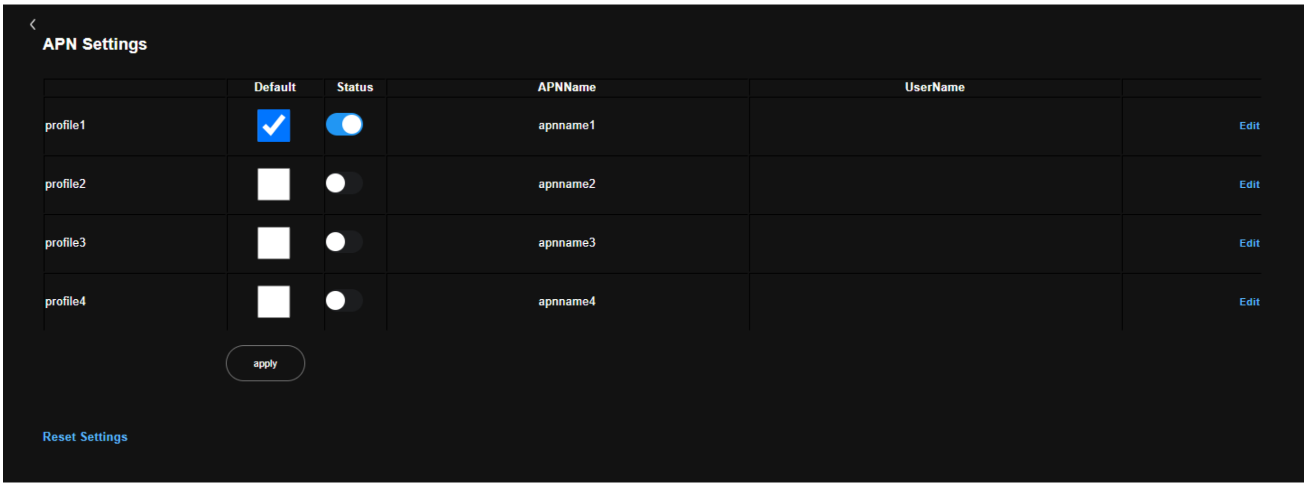
© Casa Systems 2022

Parameter	Definition
Gateway	
Primary DNS Server	
Secondary DNS Server	
Phone Number	
5G Network mode selection	Click the **Edit** link and select from the following options: • 4G – • 5G – • AUTO –
APN Settings	
Data Roaming selector switch	

Table 5 – LAN settings table

Edit APN Settings

When you select the APN Settings Edit button, you are presented at the APN Settings configuration screen. Here you can configure up to four profiles allowing multiple data connections on the mobile network.



‹

APN Settings

	Default	Status	APNName	UserName	
profile1	☑	●	apnname1		Edit
profile2	□	○	apnname2		Edit
profile3	□	○	apnname3		Edit
profile4	□	○	apnname4		Edit

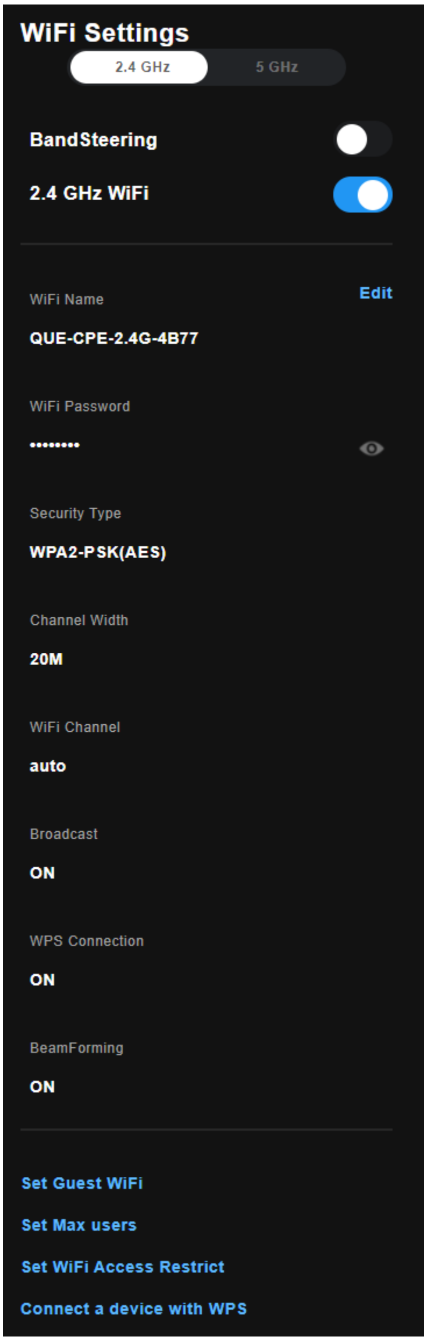
Figure 10 - APN Settings

WiFi Settings

To view and make changes to both 2.4 GHz and 5 GHz Wi-Fi connections select **WiFi Settings** from the **Network** menu. The **Mobile Settings** page opens.

Select Band

To view and edit the separate configurations click either **2.4 GHz** or **5 GHz** in the first set of buttons, this will switch the display between the **2.4 GHz** and **5 GHz** Wi-Fi bands settings.


WiFi Settings

2.4 GHz | 5 GHz

BandSteering

2.4 GHz WiFi

WiFi Name
QUE-CPE-2.4G-4B77

WiFi Password
••••••••

Security Type
WPA2-PSK(AES)

Channel Width
20M

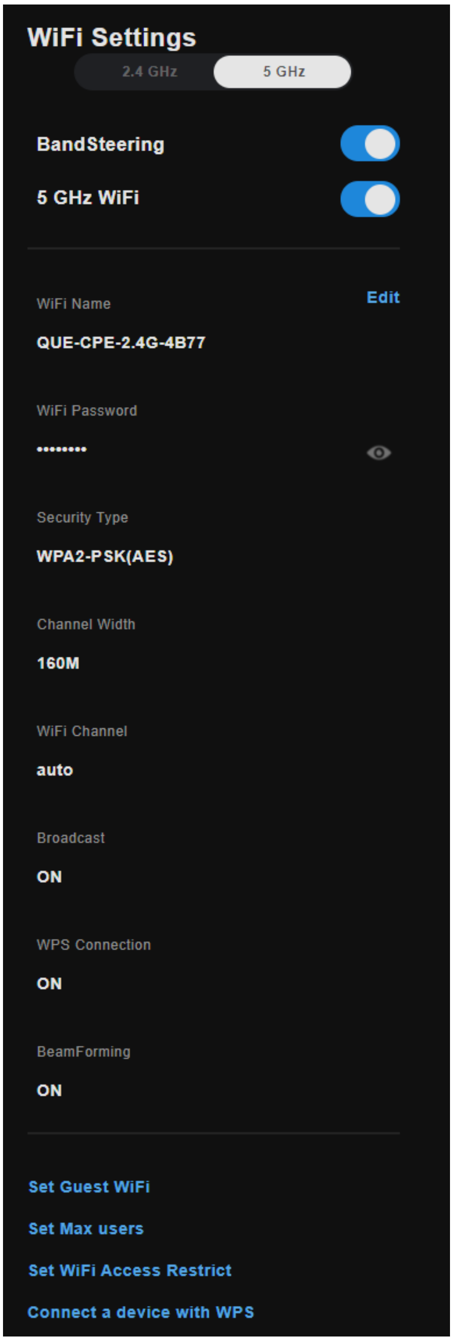
WiFi Channel
auto

Broadcast
ON

WPS Connection
ON

BeamForming
ON

Figure 11 – 2.4 GHz WiFi settings


WiFi Settings

2.4 GHz | 5 GHz

BandSteering

5 GHz WiFi

WiFi Name
QUE-CPE-2.4G-4B77

WiFi Password
••••••••

Security Type
WPA2-PSK(AES)

Channel Width
160M

WiFi Channel
auto

Broadcast
ON

WPS Connection
ON

BeamForming
ON

Figure 12 – 5 GHz WiFi settings

Wi-Fi Parameters

The following options are available to configure both bands:

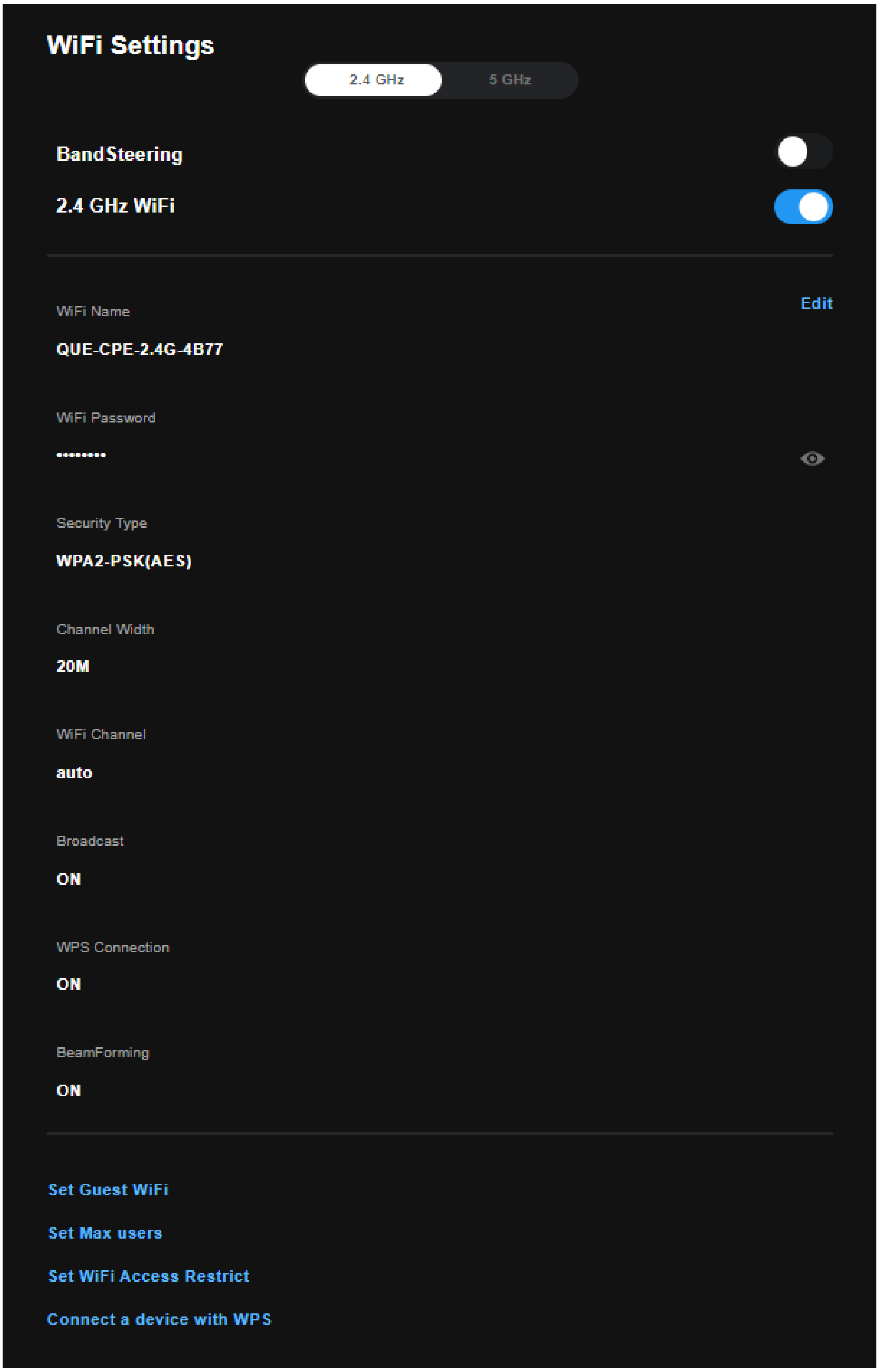
Parameter	2.4 GHz settings	5 GHz settings
Band Steering	Move button to the right to enable band steering. Move to the left to disable it.	Move button to the right to enable band steering. Move to the left to disable it.
Enable WiFi	Move button to the right to enable 2.4 GHz Wi-Fi network. Move to the left to disable it.	Move button to the right to enable 5 GHz Wi-Fi network. Move to the left to disable it.
	ℹ Note – 2.4 GHz alone, 5 GHz alone, both bands, or neither can be selected to be enabled or disabled.	
WiFi Name		
WiFi Password		
	ℹ Note – The names and password for both 2.4 GHz and 5 GHz can be the same or different. When the WiFi Name and Password are the same on both bands, your devices can seamlessly roam between them for the best performance.	
Security Type	Can be: WPA2-PSK(AES)	Can be: WPA2-PSK(AES)
Channel Width	Enter a range of:	Enter a range of:
WiFi Channel	Enter or **Auto**	Enter or **Auto**
Broadcast	Select **On** in order to…….	Select **On** in order to…….
WPS Connection	Select **On** in order to…….	Select **On** in order to…….
Beam Forming	Select **On** in order to…….	Select **On** in order to…….
Guest WiFi link	Click to view parameters and settings for **Guest WiFi**.	Same as for 2.4 GHz
Max Users link	Click to set the maximum number of users for this band.	Same as for 2.4 GHz
WiFi Access Restrict link	Click to view parameters and settings for **WiFi access restrictions**.	Same as for 2.4 GHz
Connect a device with WPS link	Click to connect to another device using the WPS service.	Same as for 2.4 GHz

Table 6 – LAN settings table

© Casa Systems 2022

Guest WiFi

The Guest WiFi Settings page allows you to configure a guest wireless network. This is a separate network from your main one that allows devices that connect to it to access the internet but not the devices on your main WiFi network.



WiFi Settings

BandSteering

2.4 GHz WiFi

WiFi Name

QUE-CPE-2.4G-4B77

WiFi Password

••••••••

Security Type

WPA2-PSK(AES)

Channel Width

20M

WiFi Channel

auto

Broadcast

ON

WPS Connection

ON

BeamForming

ON

Figure 13 - Guest WiFi Settings

Set Guest WiFi

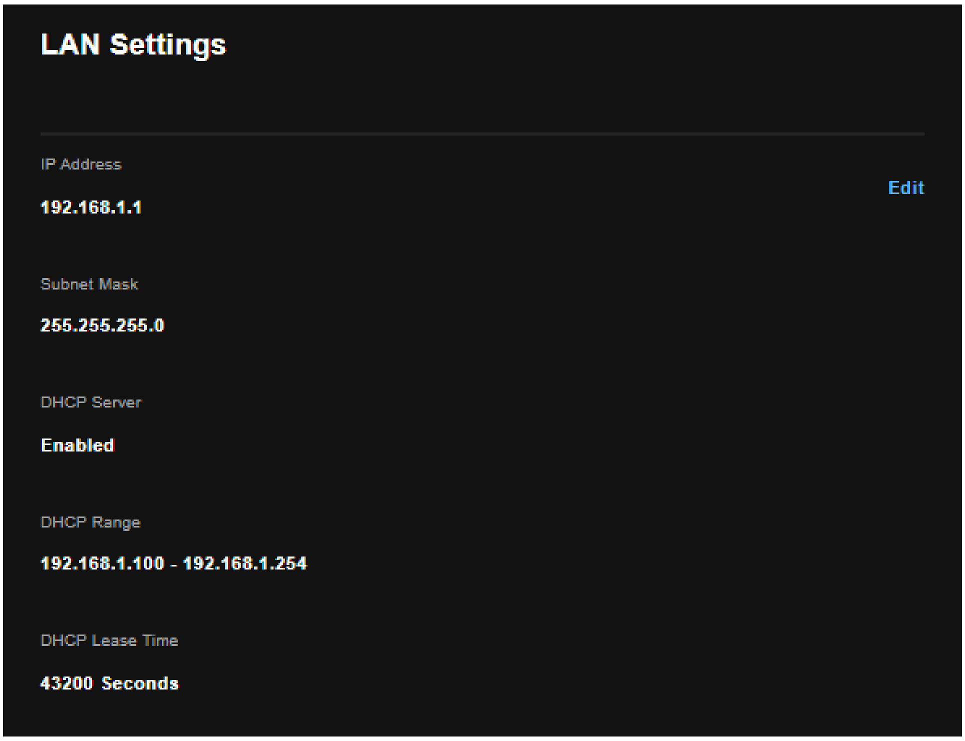
Max Users

Set WiFi Access Restrict

Connect a device with WPS

LAN Settings

The LAN Settings page allows you to modify the settings for your local area network (LAN).



LAN Settings

IP Address
192.168.1.1

Subnet Mask
255.255.255.0

DHCP Server
Enabled

DHCP Range
192.168.1.100 - 192.168.1.254

DHCP Lease Time
43200 Seconds

Figure 14 – LAN settings

The following options are available to configure:

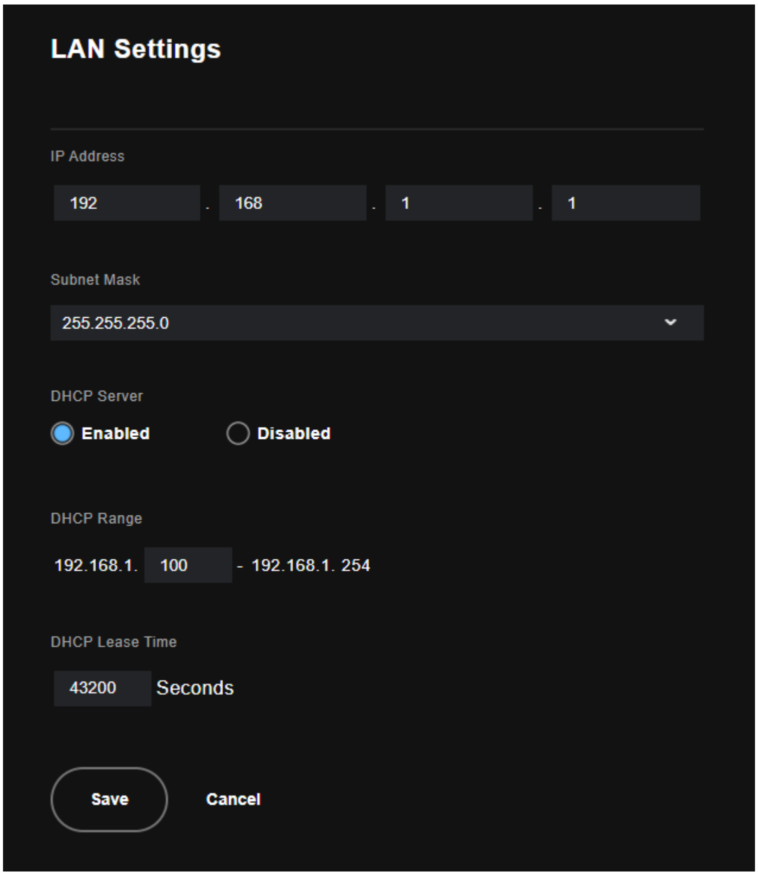
Parameter	Definition
IP Address	Enter the Local IP Address to use for the gateway.
Subnet Mask	Enter the subnet mask to define the subnet of the Local Network.
DHCP Server	Select to enable or disable the DHCP server and enter the start and end address for the DHCP IP Address pool.
DHCP Range	
DHCP Lease Time	
Edit button	

Table 7 – LAN settings table

© Casa Systems 2022

Edit LAN Settings

Click the **Edit** button to open the LAN Settings page:



LAN Settings

IP Address

192 . 168 . 1 . 1

Subnet Mask

255.255.255.0

DHCP Server

● Enabled ○ Disabled

DHCP Range

192.168.1. 100 - 192.168.1. 254

DHCP Lease Time

43200 Seconds

Figure 15 – Enter LAN settings

options are available to configure:

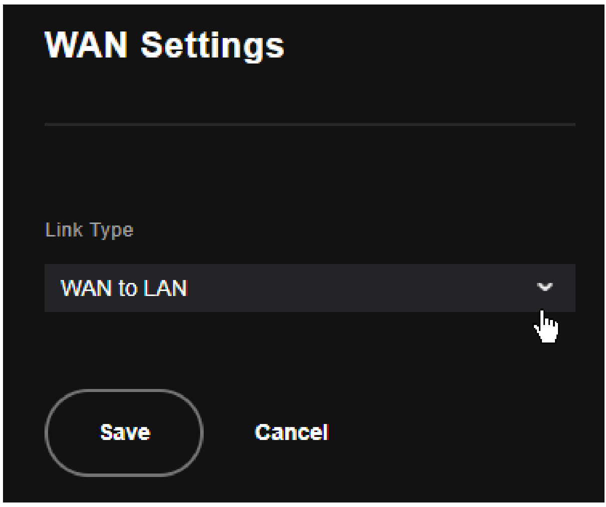
Parameter	Definition
IP Address	Enter the Local IP Address to use for the gateway.
Subnet Mask	Enter the subnet mask to define the subnet of the Local Network.
DHCP Server	Select to enable or disable the DHCP server and enter the start and end address for the DHCP IP Address pool.
DHCP Range	Enter a range of IP addresses.
DHCP Lease Time	Set in seconds Range permissible:
Save button	

Table 8 – LAN settings table

© Casa Systems 2022

WAN Settings

The **WAN Settings** page displays the current Wide Area Network service setup and allows you to configure the gateway to connect to a larger network for Internet access. The **WAN Settings** page allows you to modify the settings for your local area network (LAN).



WAN Settings

Link Type: WAN to LAN

Figure 16 – WAN settings

To add a WAN service, click the down ∇ button.

Select the **Link Type** from the drop-down list to use for the WAN service

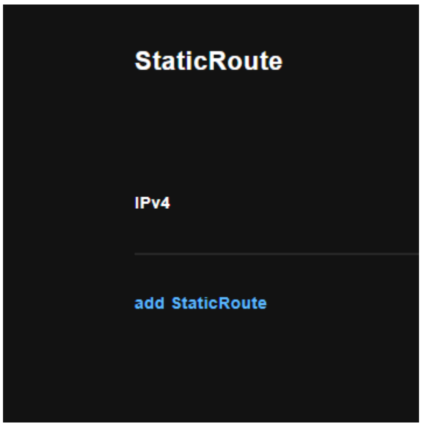
Parameter	Definition
WAN to LAN	Enter the Local IP Address to use for the gateway.
DHCP	Enter the subnet mask to define the subnet of the Local Network.
PPoE	Select to enable or disable the DHCP server and enter the start and end address for the DHCP IP Address pool.
Static	Enter a range of IP addresses.

Figure 17 – WAN Service – Select link type

Click the **Save** button to apply the new WAN settings.

Static Route Settings

The Static Route screen displays the configured static routes. Click the Add or Remove buttons to change settings.

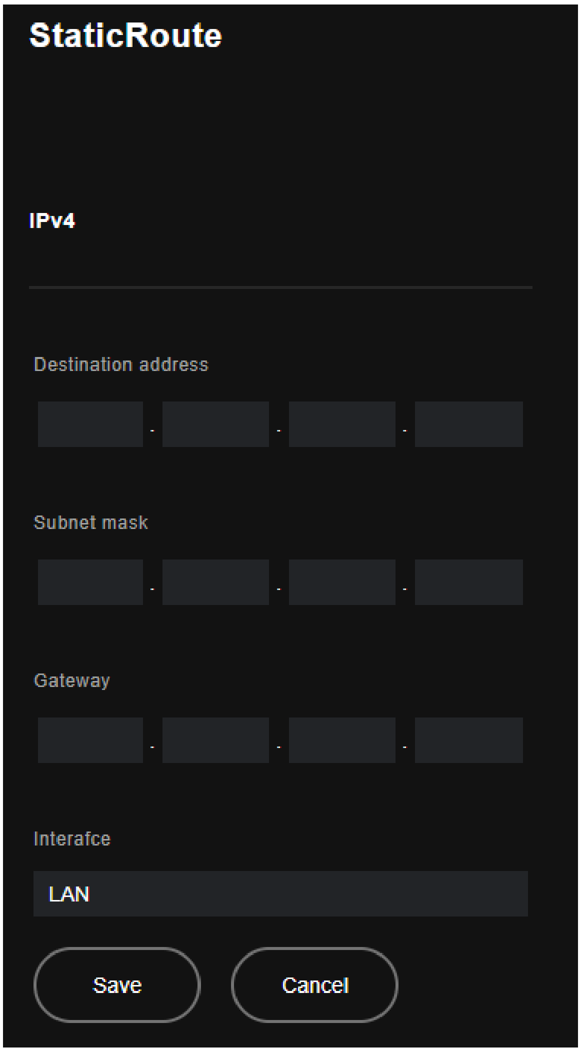


StaticRoute

IPv4

Figure 18 – Routing – Static Route list

To create a new static route rule, select the Add Static Route button. The following screen is displayed.



StaticRoute

IPv4

Destination address

Subnet mask

Gateway

Interafce

LAN

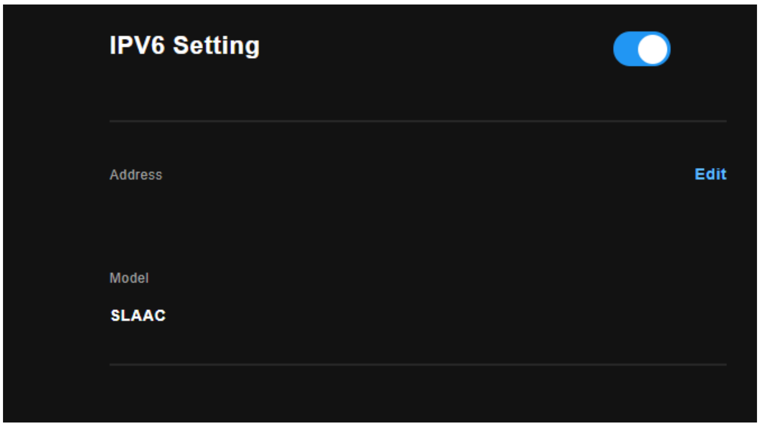
Figure 19 – Edit Static Route page

Options are available to configure:

Parameter	Definition
IPv4	Enter the Local IP Address to use for the gateway.
Destination address	Enter the subnet mask to define the subnet of the Local Network.
Subnet mask	Select to enable or disable the DHCP server and enter the start and end address for the DHCP IP Address pool.
Gateway	
Interface	Select an interface for the Static Route. Options include: • LAN – • WAN – • APN1 – • APN2 – • APN3 – • APN4 –
Save button	Click **Save** to add the changes to the Static Route

Table 9 – LAN settings table

IPv6 Settings



IPV6 Setting

Address

Model

SLAAC

Figure 20 – IPv6 settings

Options are available to configure:

Parameter	Definition
Enable/Disable button	
Address	
Model	

© Casa Systems 2022

Parameter	Definition
Edit button	

Table 10 – LAN settings table

To add a static route rule, click the Add button. The following screen is displayed.

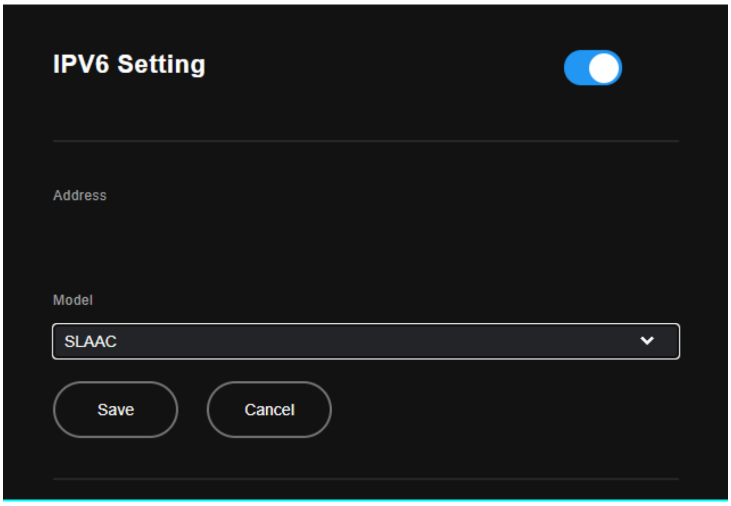


Figure 21 – Edit Static Route configuration

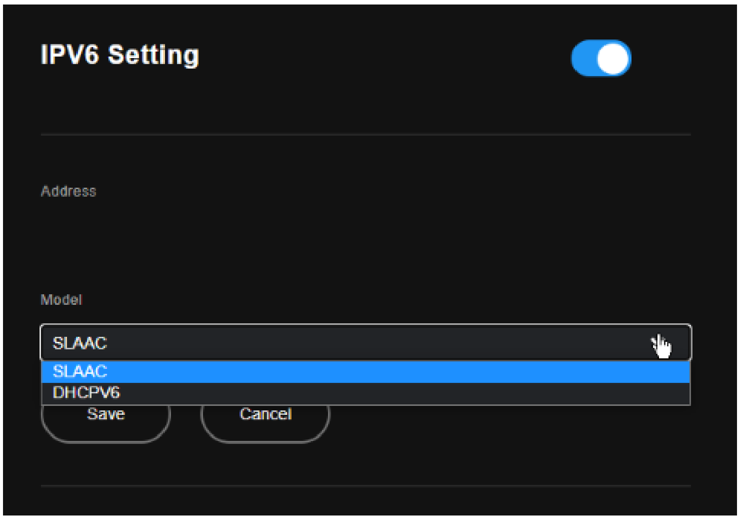


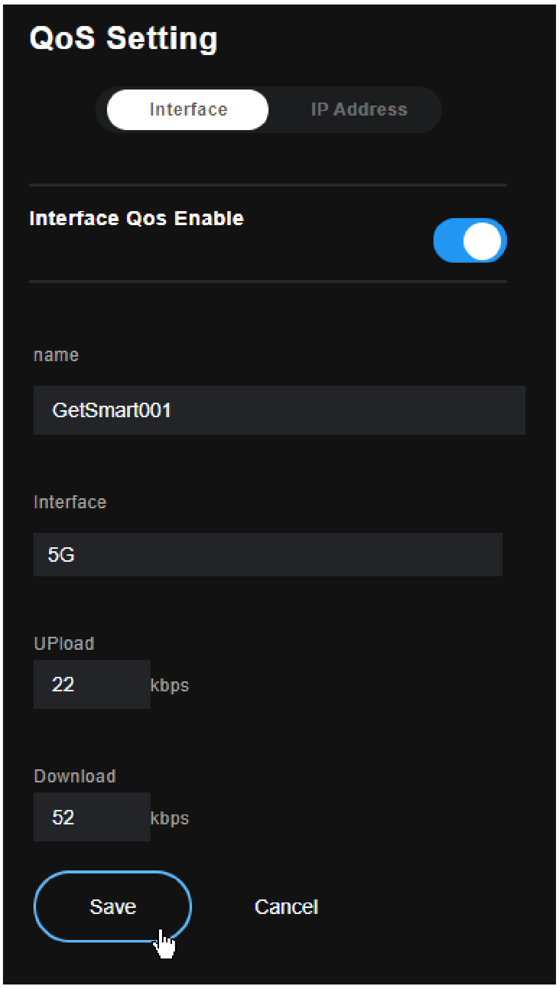
Figure 22 – Routing – Static Route list

Quality of Service

Quality of Service offers a defined level of performance in a data communications system - for example the ability to guarantee that video traffic is given priority over other network traffic to ensure that video streaming is not disrupted by other network traffic. This means that if you are streaming video and someone else in the house starts downloading a large file, the download won't disrupt the flow of video traffic.

To enable QoS select the Enable QoS checkbox and set the Default DSCP (Differentiated Services Code Point) Mark. Then press the Apply/Save button.

To view and edit the separate configurations click either 2.4 GHz or 5 GHz in the first set of buttons, this will switch the display between the 2.4 GHz and 5 GHz Wi-Fi bands settings.



QoS Setting

Interface Qos Enable

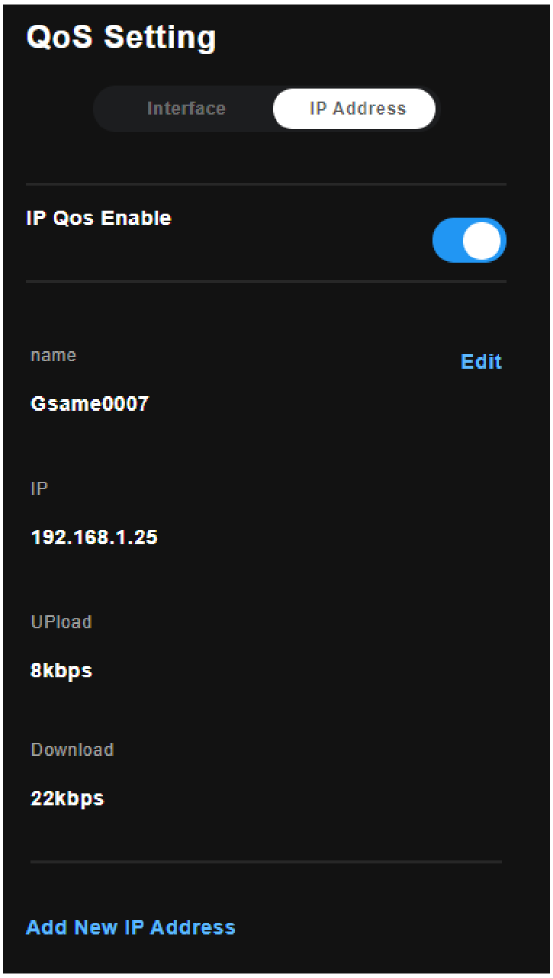
name: GetSmart001

Interface: 5G

UPload: 22 kbps

Download: 52 kbps

Figure 23 – Interface settings



QoS Setting

IP Qos Enable

name: Gsame0007

IP: 192.168.1.25

UPload: 8kbps

Download: 22kbps

Figure 24 – IP Address settings s

Parameters

The following options are available to configure:

Parameter	Interface settings	IP Address settings
name		

Parameter	Interface settings	IP Address settings
Interface		n/a
IP	n/a	
UPload		
Download		

Table 11 –QoS Settings table

Add New IP Address

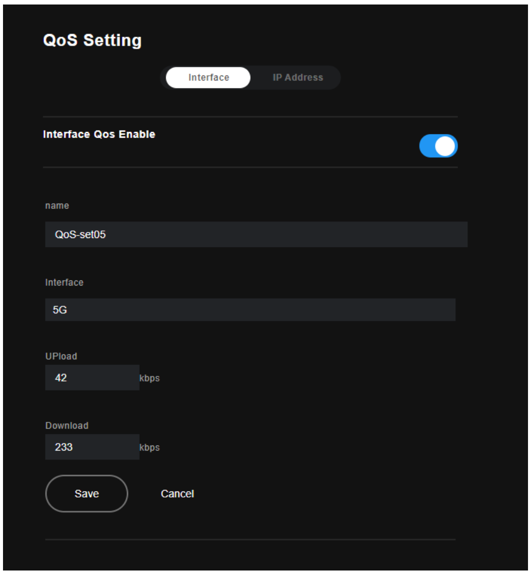
Figure 25 – Add new QoS IP Address dialog

Item	Description

Table 12 –Add new QoS IP Address

Manual Net Search

The **QoS WLAN Queue** page displays a summary of the QoS configuration.



QoS Setting

Interface Qos Enable

name: QoS-set05

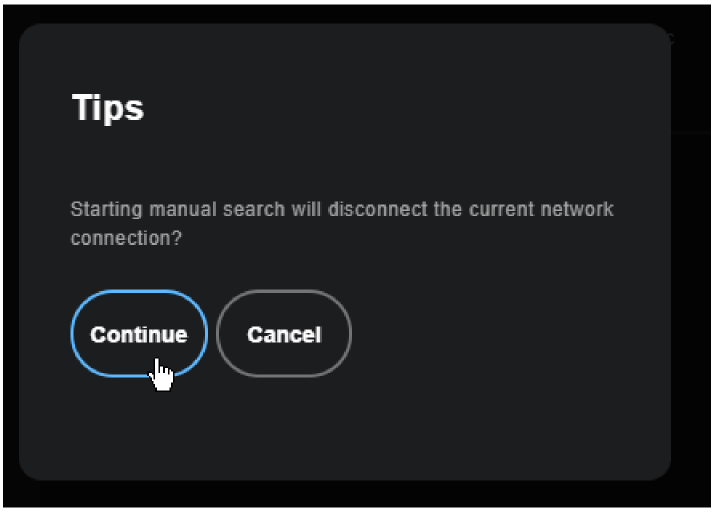
Interface: 5G

UPload: 42 kbps

Download: 233 kbps

Figure 26 – Advanced – QoS – WLAN Queue

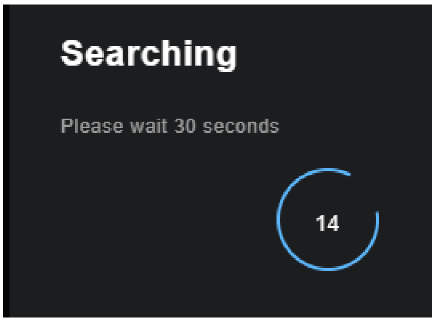
Manual Net Settings – IP Address



Tips

Starting manual search will disconnect the current network connection?

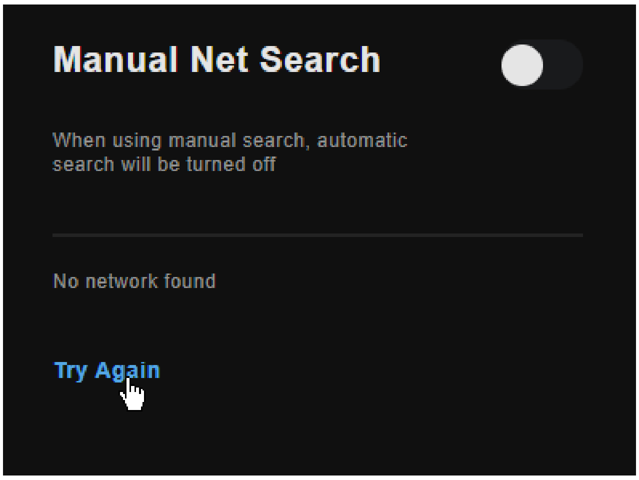
Figure 27 – Manual Net Search – Fail, try again



Searching

Please wait 30 seconds

Figure 28 – Manual Net Search – Fail, try again



Manual Net Search

When using manual search, automatic search will be turned off

No network found

Figure 29 – Manual Net Search – Fail, try again

The above screen creates a traffic class rule to classify the upstream traffic, assign queuing priority and optionally overwrite the IP header TOS (type of service) byte. A rule consists of a class name and at least one condition. All of the specified conditions in this classification rule must be satisfied for the rule to take effect.

Item	Description
Interface	Identifies the interface type.
Type	Identifies the connection type.

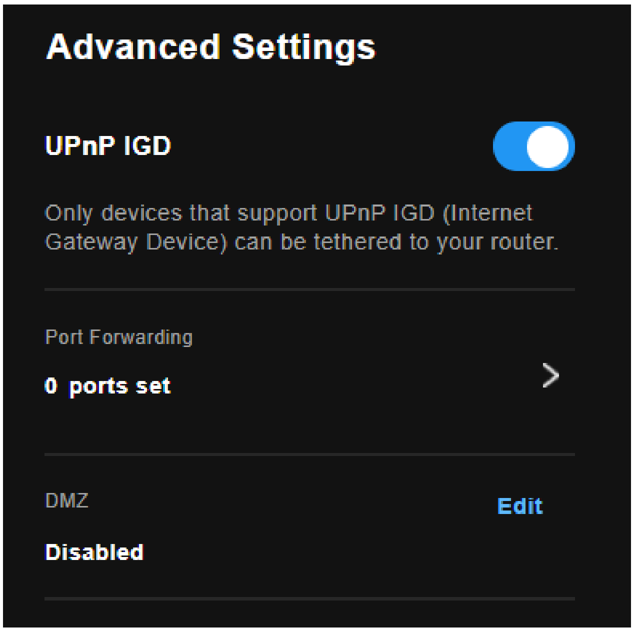
Shaping Rate	The speed you would limit the port to in Kbps (Kilobits per second) after the burst size.
Burst Size	Burst size should be more than 10x MTU (>=15000 bytes)
Apply/Save button	Click to save and apply your changes

Figure 30 – Advanced – QoS – Port Shaping settings

Note: 1 byte = 8 bits

Advanced Settings

The **QoS WLAN Queue** page displays a summary of the QoS configuration.



Advanced Settings

UPnP IGD

Only devices that support UPnP IGD (Internet Gateway Device) can be tethered to your router.

Port Forwarding

0 ports set

DMZ

Disabled

Figure 31 – Advanced – QoS – Network Traffic Class settings

The above screen creates a traffic class rule to classify the upstream traffic, assign queuing priority and optionally overwrite the IP header TOS (type of service) byte. A rule consists of a class name and at least one condition. All of the specified conditions in this classification rule must be satisfied for the rule to take effect.

Click the **Apply/Save** button to save and activate the rule.

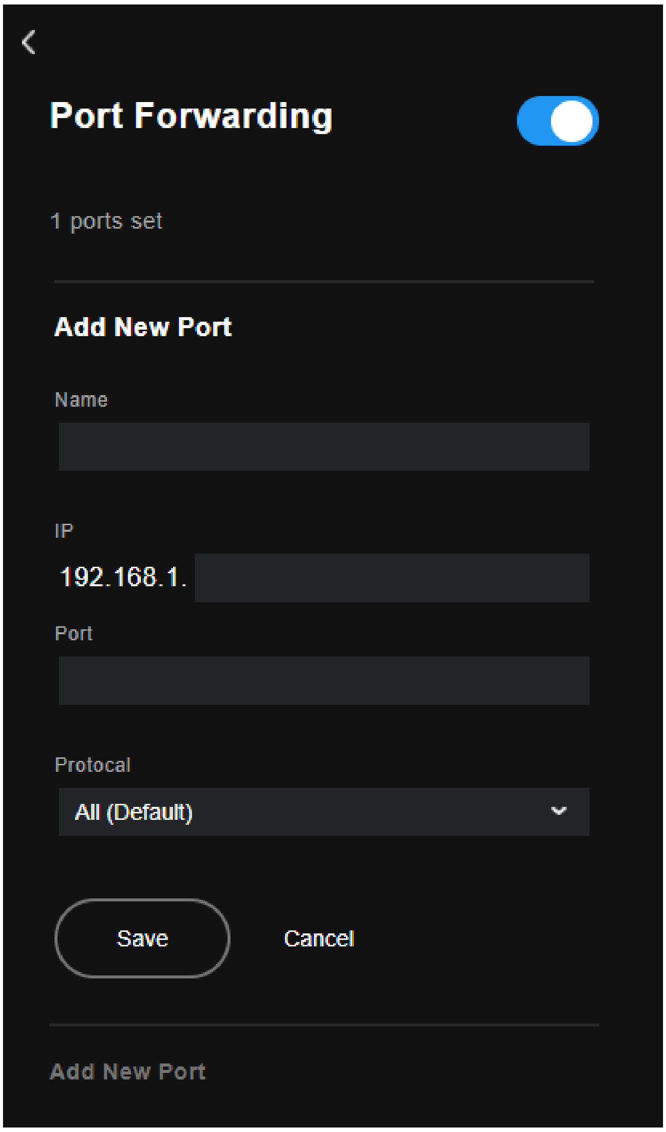
Item	Description
Interface	Identifies the interface type.
Type	Identifies the connection type.
Shaping Rate	The speed you would limit the port to in Kbps (Kilobits per second) after the burst size.
Burst Size	Burst size should be more than 10x MTU (>=15000 bytes)
Apply/Save button	Click to save and apply your changes

Figure 32 – Advanced – QoS – Port Shaping settings

ⓘ **Note:** 1 byte = 8 bits

> link

Click the > link



Port Forwarding

1 ports set

Add New Port

Name

IP 192.168.1.

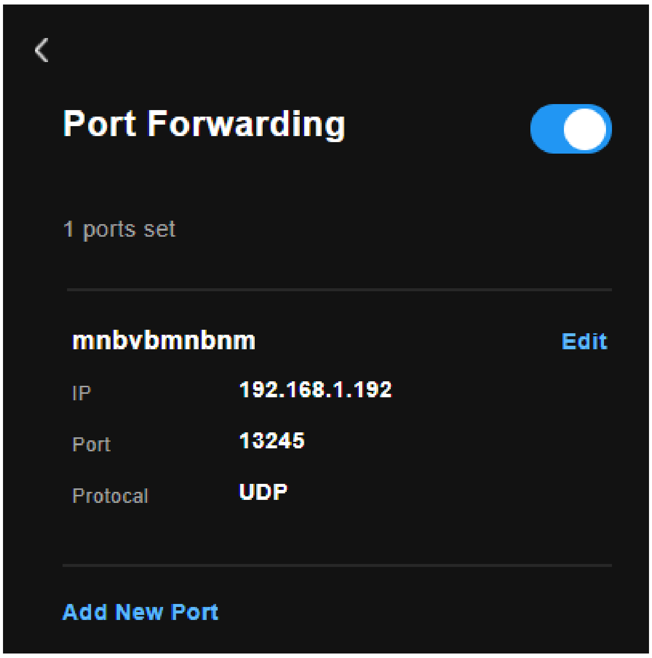
Port

Protocal: All (Default)

Figure 33 - Port Forwarding - Add New Port

Protocol: All (Default)

© Casa Systems 2022



Port Forwarding

1 ports set

mnbvbmnbnm

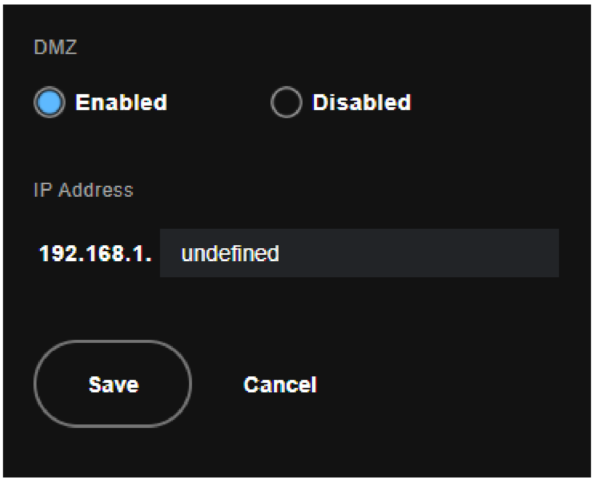
IP 192.168.1.192

Port 13245

Protocal UDP

Figure 34 - Port Forwarding Summary

Edit (DMZ)



DMZ

● Enabled ○ Disabled

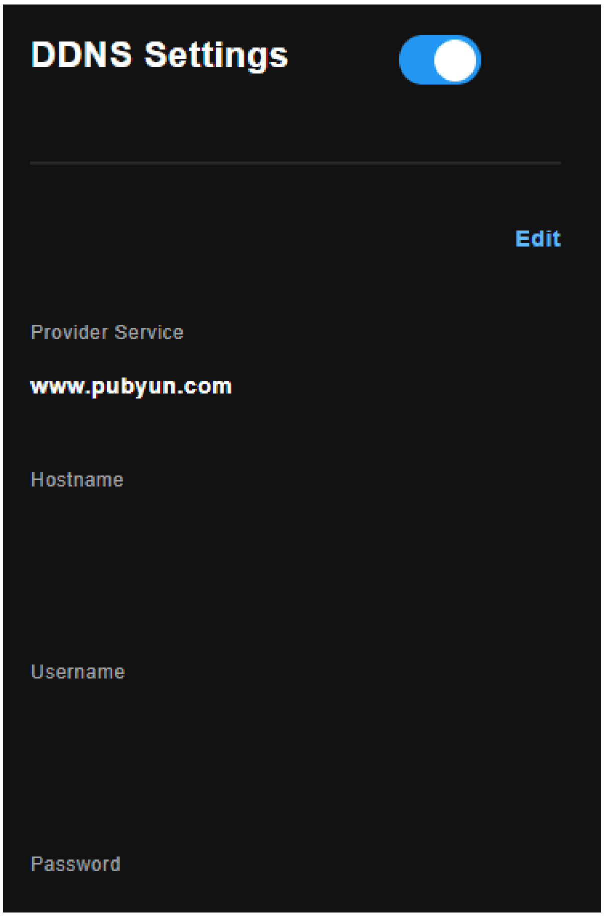
IP Address

192.168.1. undefined

Figure 35 - Edit DMZ

DDNS Settings

The DDNS Settings page displays a summary of the DDNS configuration.



DDNS Settings

Edit

Provider Service

www.pubyun.com

Hostname

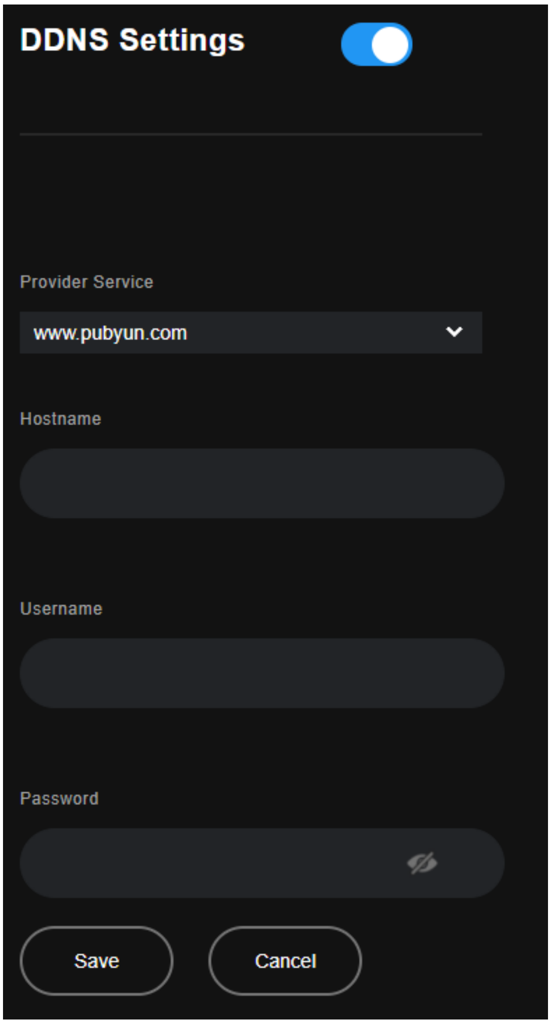
Username

Password

Figure 36 – DDNS Settings

Edit

© Casa Systems 2022



DDNS Settings

Provider Service: www.pubyun.com

Hostname:

Username:

Password:

Figure 37 - DDNS Settings - Edit

The above screen creates a traffic class rule to classify the upstream traffic, assign queuing priority and optionally overwrite the IP header TOS (type of service) byte. A rule consists of a class name and at least one condition. All of the specified conditions in this classification rule must be satisfied for the rule to take effect.

Click the Apply/Save button to save and activate the rule.

Item	Description
Interface	Identifies the interface type.
Type	Identifies the connection type.
Shaping Rate	The speed you would limit the port to in Kbps (Kilobits per second) after the burst size.
Burst Size	Burst size should be more than 10x MTU (>=15000 bytes)
Apply/Save button	Click to save and apply your changes

Figure 38 – Advanced – QoS – Port Shaping settings

Note: 1 byte = 8 bits

Security

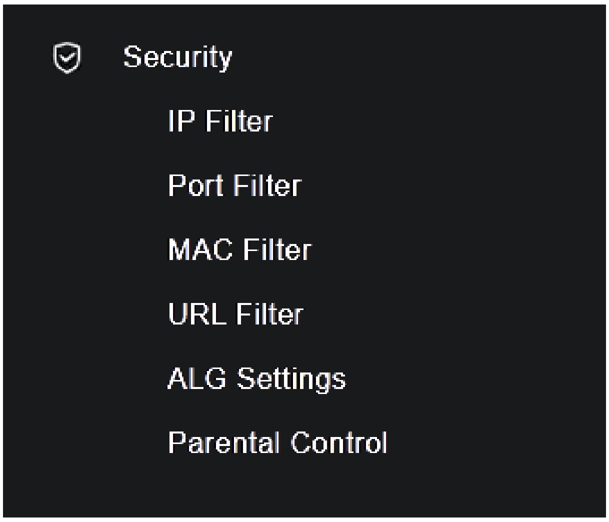
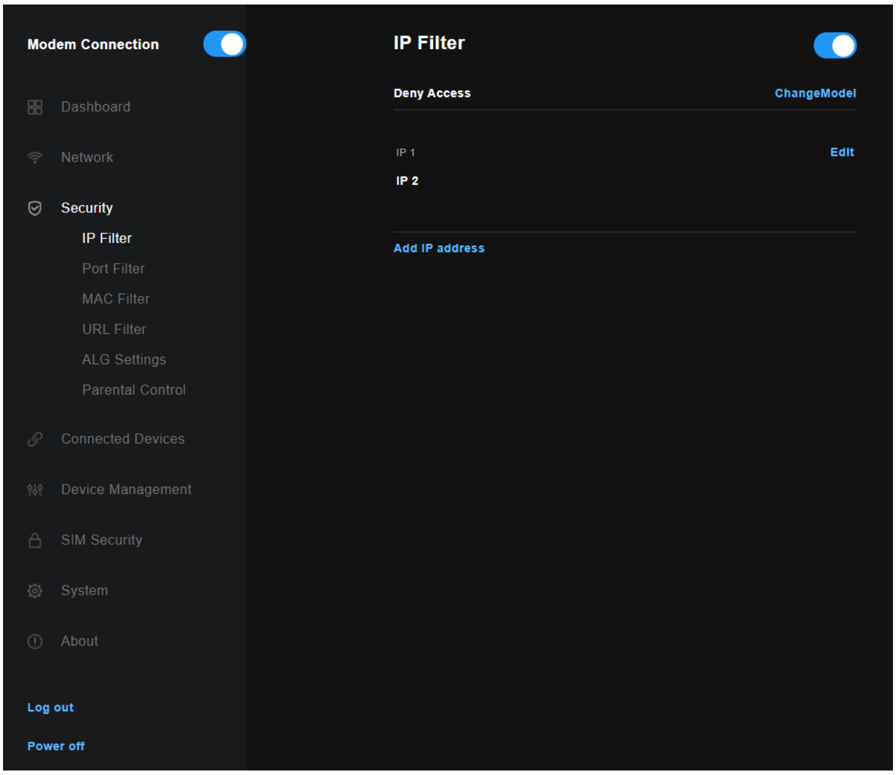


Figure 39 – Security menu

This section provides a variety of options for configuring the security functions of the gateway.

IP Filter

Settings – IP filters



IP Filter

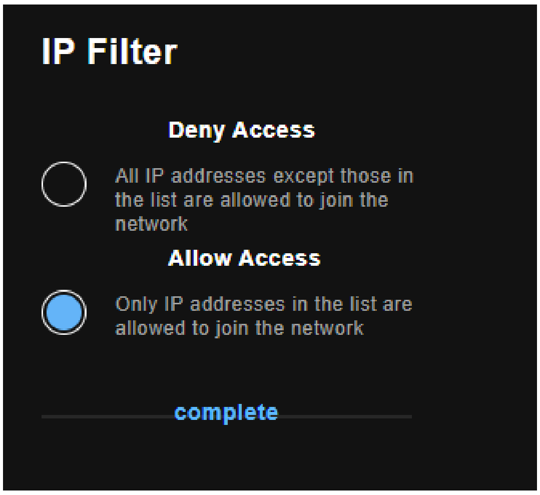
Deny Access ChangeModel

IP 1 Edit

IP 2

Add IP address

© Casa Systems 2022



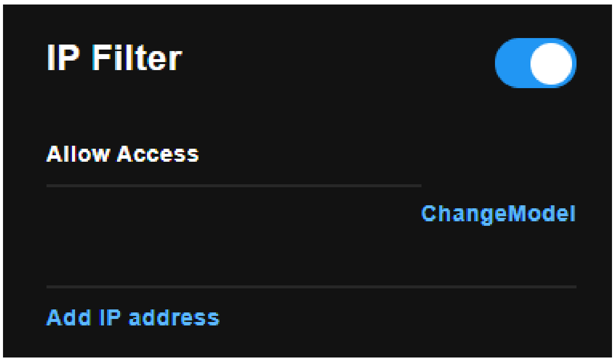
IP Filter

Deny Access

○ All IP addresses except those in the list are allowed to join the network

Allow Access

● Only IP addresses in the list are allowed to join the network



IP Filter

Allow Access

Figure 40 – Advanced – QoS – Network Traffic Class settings

The above screen creates a traffic class rule to classify the upstream traffic, assign queuing priority and optionally overwrite the IP header TOS (type of service) byte. A rule consists of a class name and at least one condition. All of the specified conditions in this classification rule must be satisfied for the rule to take effect.

Click the Apply/Save button to save and activate the rule.

Item	Description
Interface	Identifies the interface type.
Type	Identifies the connection type.
Shaping Rate	The speed you would limit the port to in Kbps (Kilobits per second) after the burst size.
Burst Size	Burst size should be more than 10x MTU (>=15000 bytes)
Apply/Save button	Click to save and apply your changes

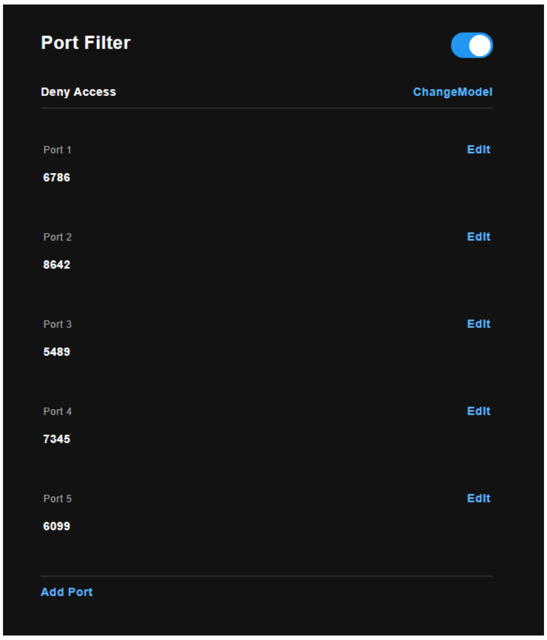
Figure 41 – Advanced – QoS – Port Shaping settings

Note: 1 byte = 8 bits

© Casa Systems 2022

Port Filter

Select **Port Filter** from the **Security** menu to view the current Port Filter settings:



Port Filter

Deny Access — ChangeModel

Port 1 — Edit
6786

Port 2 — Edit
8642

Port 3 — Edit
5489

Port 4 — Edit
7345

Port 5 — Edit
6099

Figure 42 – Port Filter settings

Push the **Enable/Disable** button to the right to activate Port Filtering on the gateway.

Item	Description
Deny Access	Change model
Port 1/2/3/4/5	
Edit Port button	
Add Port button	

Figure 43 – Port Filter settings

ⓘ Note: 1 byte = 8 bits

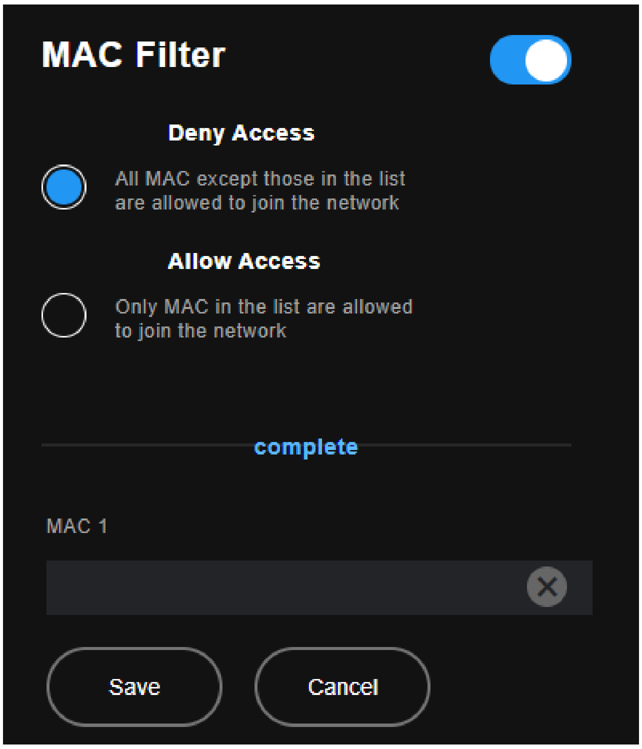
Edit Port Filter

Add Port

MAC Filter

MAC Filter allows you to add or remove the MAC Address of devices which will be allowed or denied access to the wireless network. First use the Wireless Interface drop-down list to select the wireless network you wish to configure, then change the MAC Restrict Mode setting from Disabled and select to either Allow or Deny access to the MAC addresses listed.

The gateway offers the ability to use MAC Address filtering on ATM PVCs. You can elect to block or allow connections based on MAC Address criteria. The default policy is to allow all connections.



MAC Filter

Deny Access

● All MAC except those in the list are allowed to join the network

Allow Access

○ Only MAC in the list are allowed to join the network

complete

MAC 1

Figure 44 –MAC Filter list

Push the Enable/Disable button to the right to activate MAC filtering on the gateway.

Item	Description
Deny Access	Change model
MAC name	
MAC address	
Save button	

Figure 45 – MAC Filter settings

1 Enter the Protocol type to which the filter should apply.

2 Enter the Source and Destination MAC Address.

3 Enter the Frame Direction of the traffic to filter.

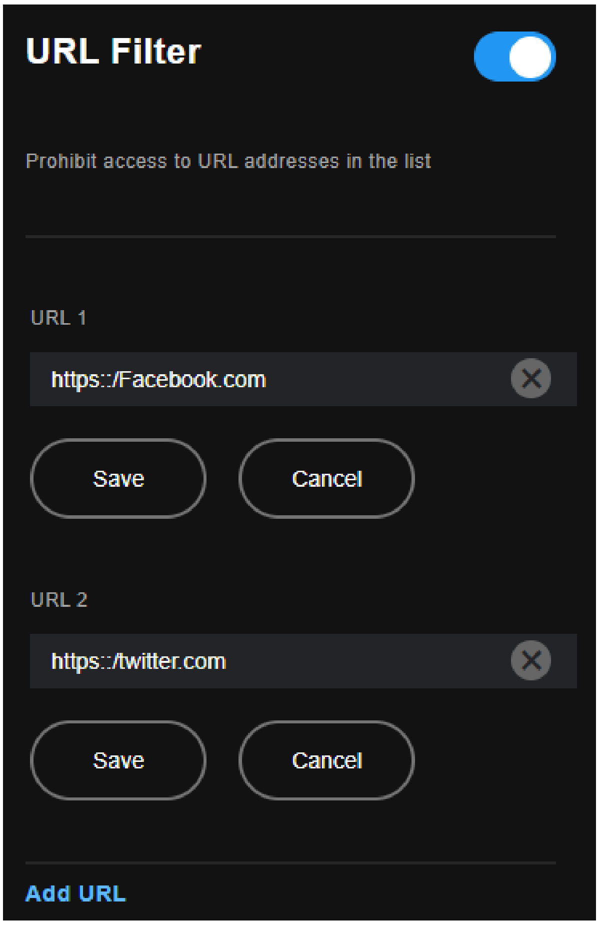
4 Select the WAN interface to which the filter should apply.

Click Apply/Save to save the new MAC filtering configuration.

Note – While giving a wireless network some additional protection, MAC filtering can be circumvented by scanning a valid MAC and then spoofing one's own MAC into a validated one, using MAC Filtering may lead to a false sense of security.

URL Filter

With the URL filter, you can add certain websites or URLs to a safe or blocked list. This will provide you added security to ensure any website you deem unsuitable will not be able to be seen by anyone who is accessing the Internet via the gateway.



URL Filter

Prohibit access to URL addresses in the list

URL 1

https::/Facebook.com

URL 2

https::/twitter.com

Figure 46 –URL Filter

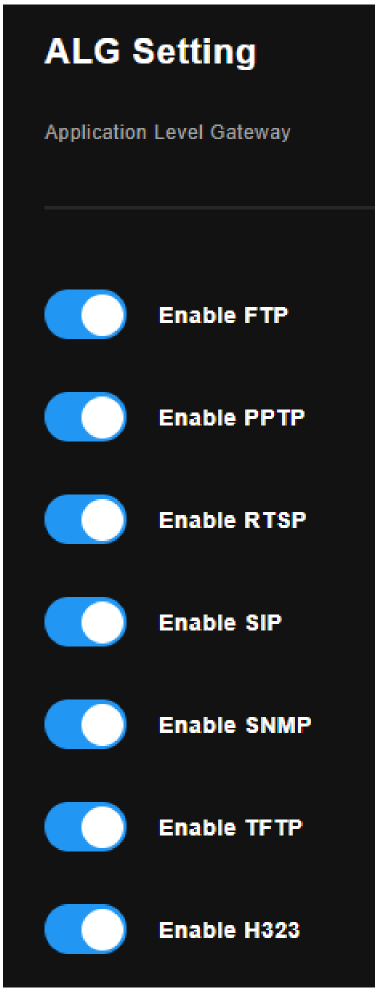
Push the **Enable/Disable** button to the right to activate URL filtering on the gateway.

Item	Description
Deny Access	Change model
URL name	
URL	
Edit button	
Add URL button	

Figure 47 – URL Filter settings

Add URL

ALG Setting



ALG Setting

Application Level Gateway

Enable FTP: on

Enable PPTP: on

Enable RTSP: on

Enable SIP: on

Enable SNMP: on

Enable TFTP: on

Enable H323: on

Figure 48 – ALG settings Get new graphic

Field	Description

Table 13 – Advanced – Parental Control – Add URL Restriction Settings

Edit URL Filter

Get screenshot and add description.

Add URL

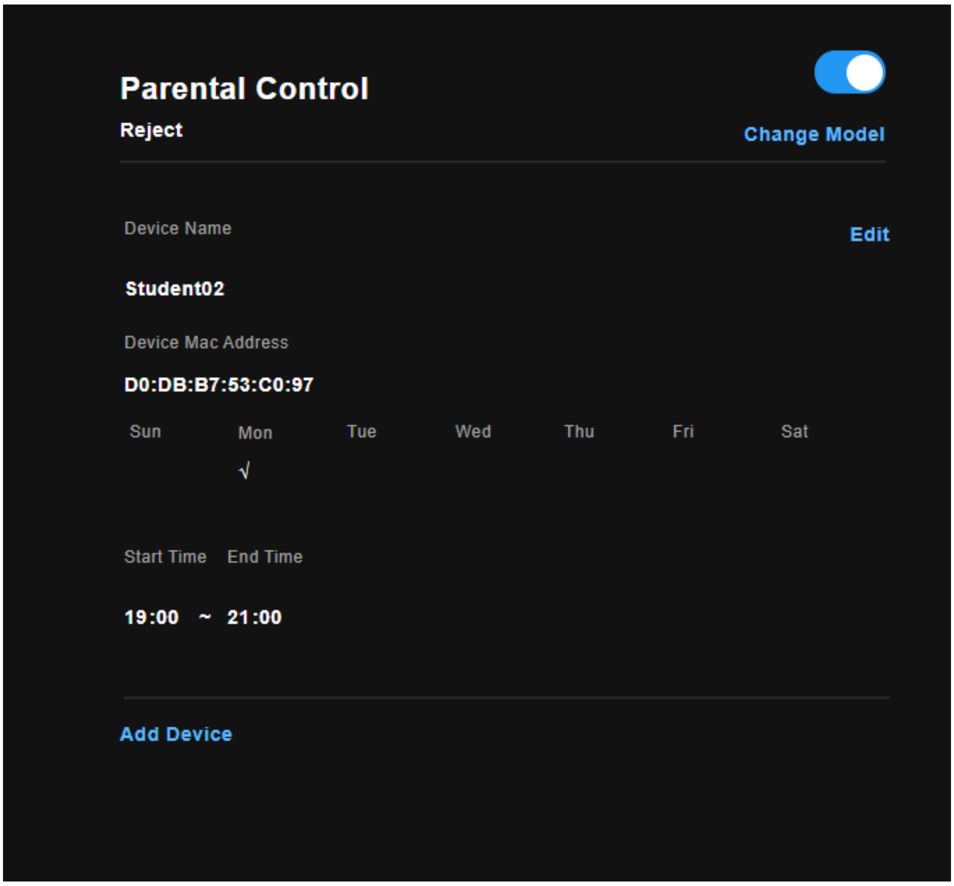
Get screenshot and add description.

Parental Control

The Parental Control feature allows you to take advanced measures to ensure that devices connected to the network are used only when and how you decide.

This Parental Control function allows you to restrict access from a network connected device to an outside network through the router on selected days and at certain times.

Make sure the NTP System Time settings are correct for your location (refer to the System > NTP System Time section) so that the scheduled times match your local time.



Parental Control

Reject

Change Model

Device Name

Edit

Student02

Device Mac Address

D0:DB:B7:53:C0:97

Sun	Mon	Tue	Wed	Thu	Fri	Sat
	√					

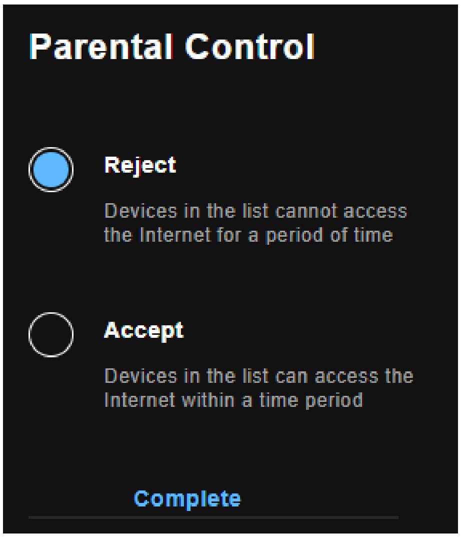
Start Time End Time

19:00 ~ 21:00

Add Device

Figure 49 – Advanced – Parental Control – Time Restriction

Change Model



Parental Control

● **Reject**

Devices in the list cannot access the Internet for a period of time

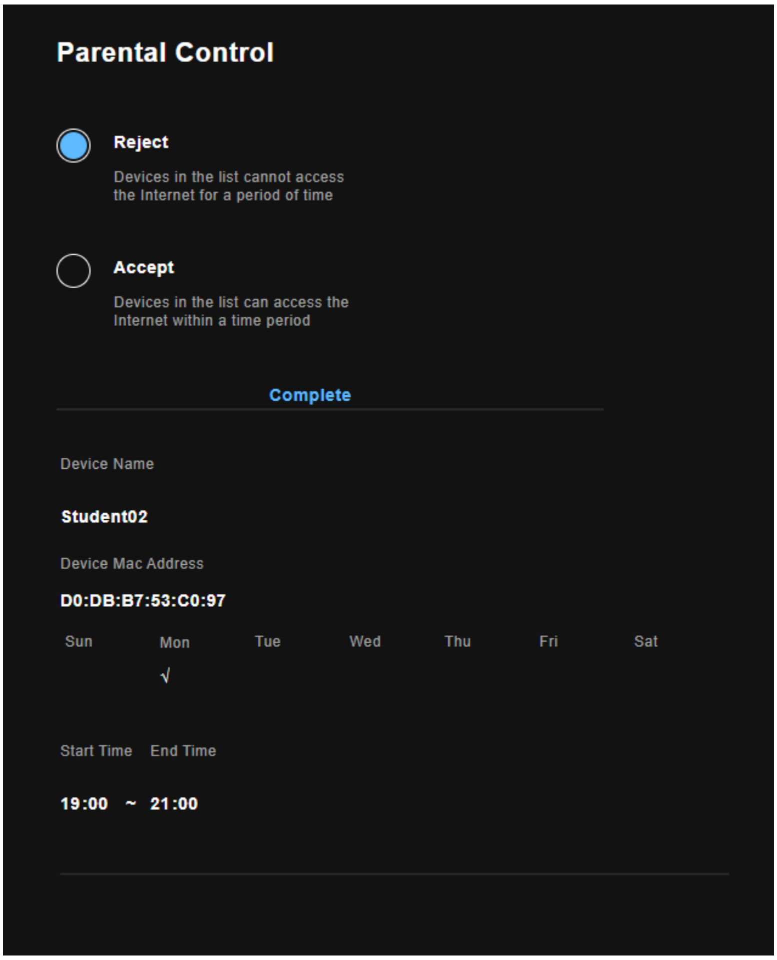
○ **Accept**

Devices in the list can access the Internet within a time period

Figure 50 – Advanced – Parental Control – Time Restriction

Add Device

To add a time restriction rule, press the Add Device button. The following screen appears.



Parental Control

● **Reject**

Devices in the list cannot access the Internet for a period of time

○ **Accept**

Devices in the list can access the Internet within a time period

Device Name

Student02

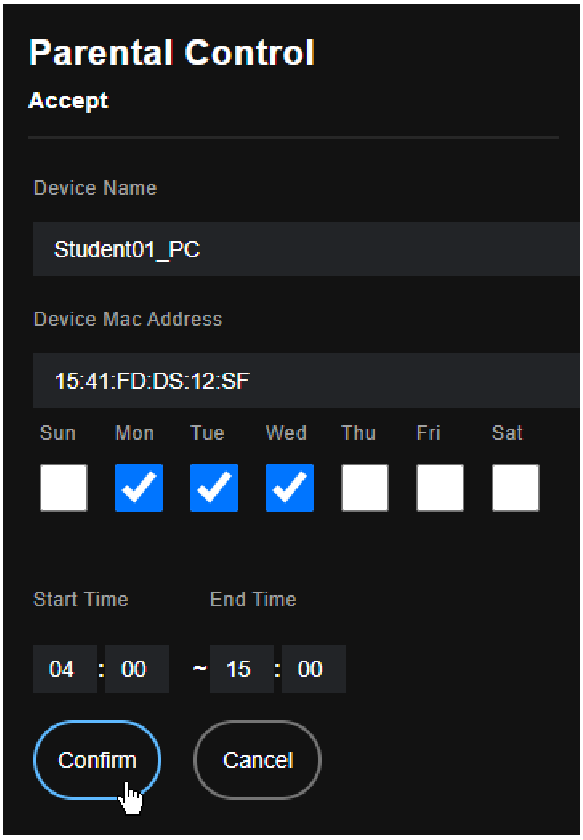
Device Mac Address

D0:DB:B7:53:C0:97

Sun	Mon	Tue	Wed	Thu	Fri	Sat
	√					

Start Time End Time

19:00 ~ 21:00



Parental Control

Accept

Device Name

Student01_PC

Device Mac Address

15:41:FD:DS:12:SF

Sun	Mon	Tue	Wed	Thu	Fri	Sat
□	☑	☑	☑	□	□	□

Start Time 04 : 00 ~ End Time 15 : 00

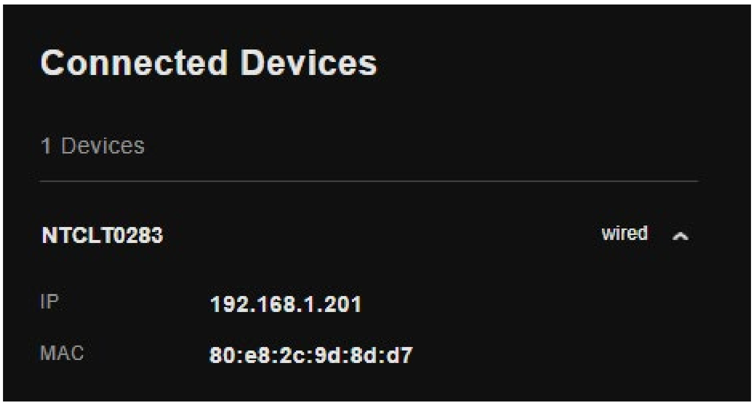
Figure 51 –Parental Control – Add Time Restriction

Field	Description
Reject / Accept selector	
Device Name	A user defined name for the time restriction rule.
Device MAC Address	The MAC address of the device to be affected by this rule.
Days of the Week	The days of the week for which the rules apply.
Start Time	The time of day when the restriction starts. (24 hour time: 00:00–23:59)
End time	The time of day when the restriction ends. (24 hour time: 00:00–23:59)

Table 14 – Advanced – Parental Control – Add Time Restriction Settings

Connected Devices

Select the Connected Devices menu item to view a list of all devices that are connected to the gateway.



Connected Devices

1 Devices

NTCLT0283 wired

IP 192.168.1.201

MAC 80:e8:2c:9d:8d:d7

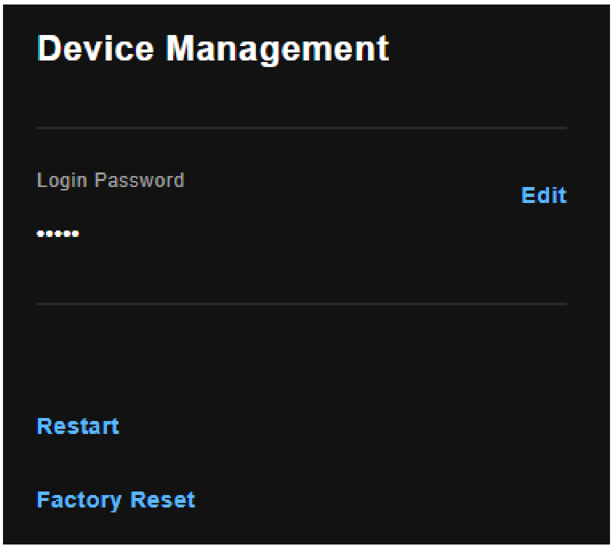
Figure 52 – Connected Devices list

Field	Description
Number	
Name	
Connection type	
IP address	
MAC address	

Table 15 – Connected Devices

Device Management

Select the Device Management menu item to edit the login password, restart the gateway, or perform a factory reset of the gateway.



Device Management

Login Password

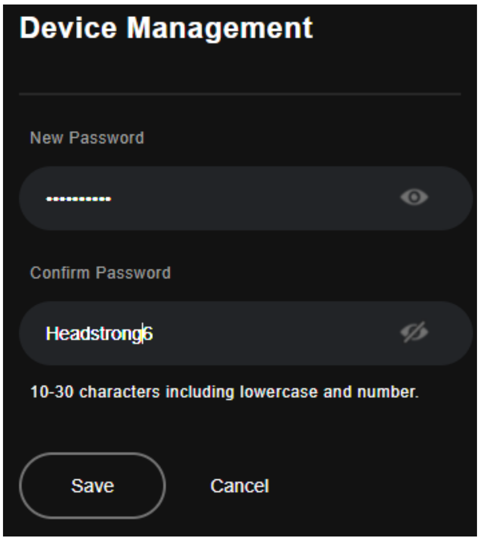
•••••

Figure 53 –Device Management details

Field	Description
Login Password	
Password display	
Edit button	
Restart button	
Factory Reset	

Table 16 – Device Management details table

Edit password



Device Management

New Password

•••••••••••

Confirm Password

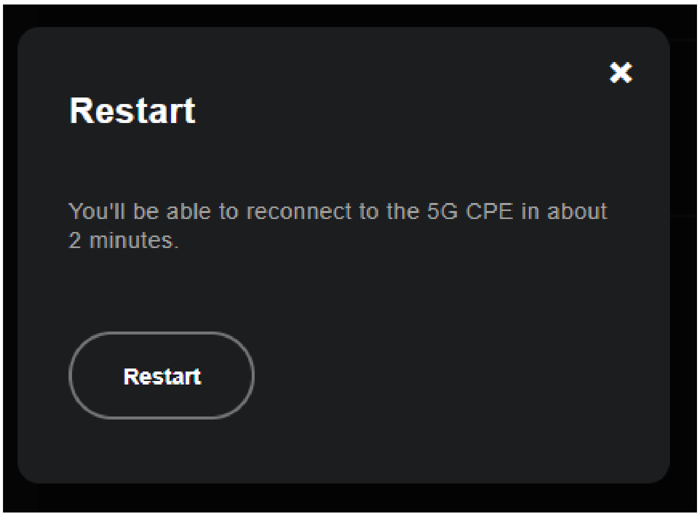
Headstrong6

10-30 characters including lowercase and number.

Figure 54 –Device Management details

© Casa Systems 2022

Restart

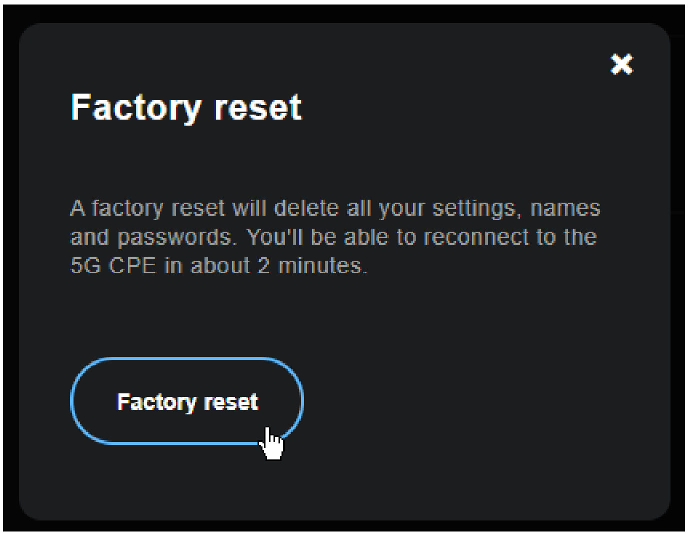


Restart

You'll be able to reconnect to the 5G CPE in about 2 minutes.

Figure 55 –Device Management details

Factory Reset



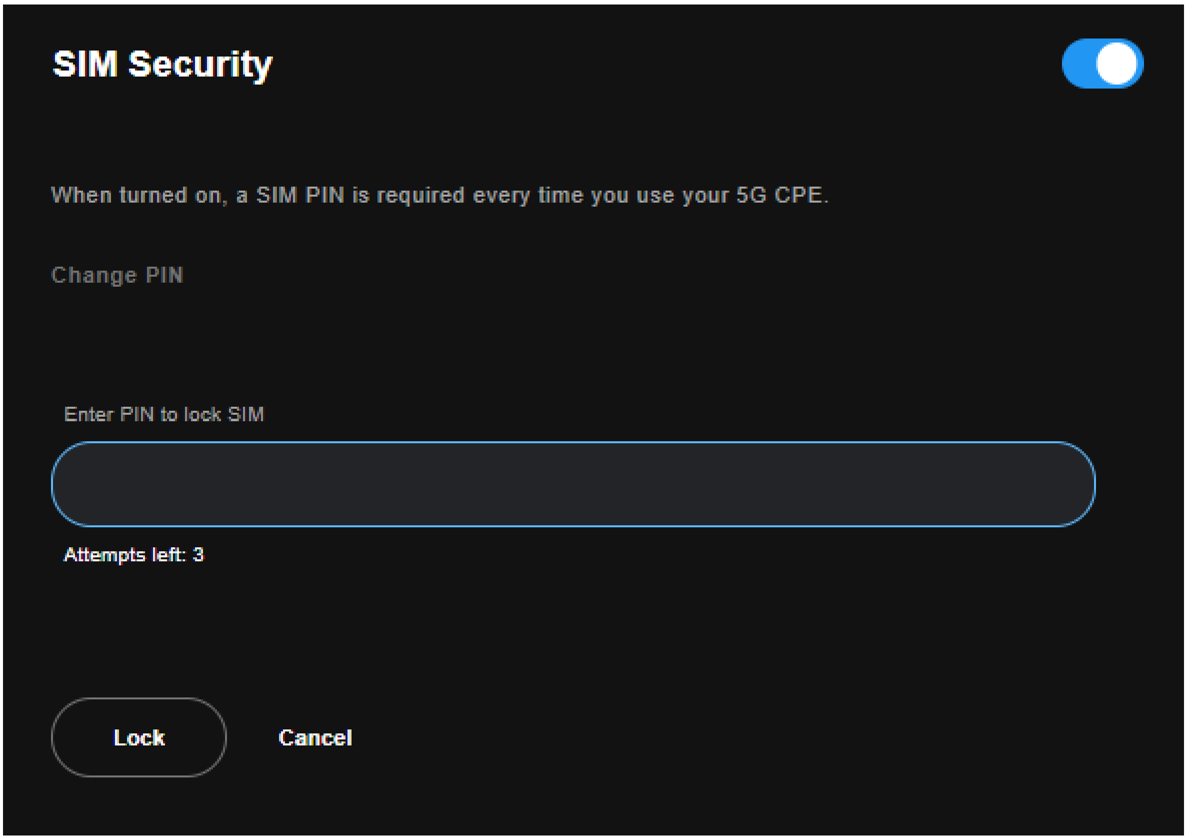
Factory reset

A factory reset will delete all your settings, names and passwords. You'll be able to reconnect to the 5G CPE in about 2 minutes.

Figure 56 –Device Management details

SIM Security

Click the SIM Security menu item to view a list of all devices



SIM Security

When turned on, a SIM PIN is required every time you use your 5G CPE.

Change PIN

Enter PIN to lock SIM

Attempts left: 3

Figure 57 – SM Security details

System

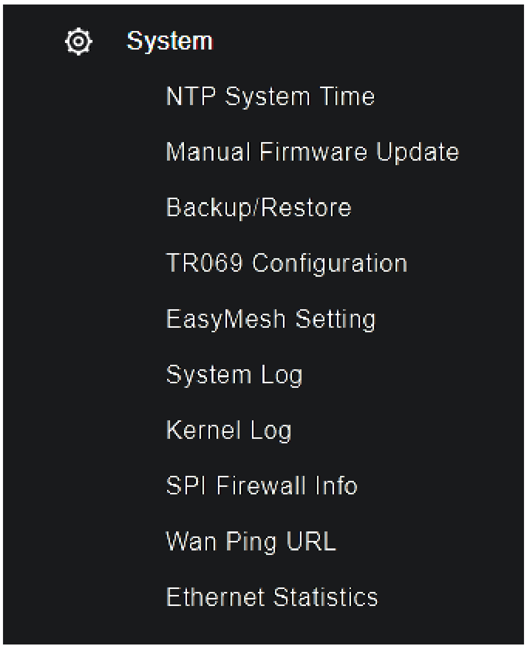
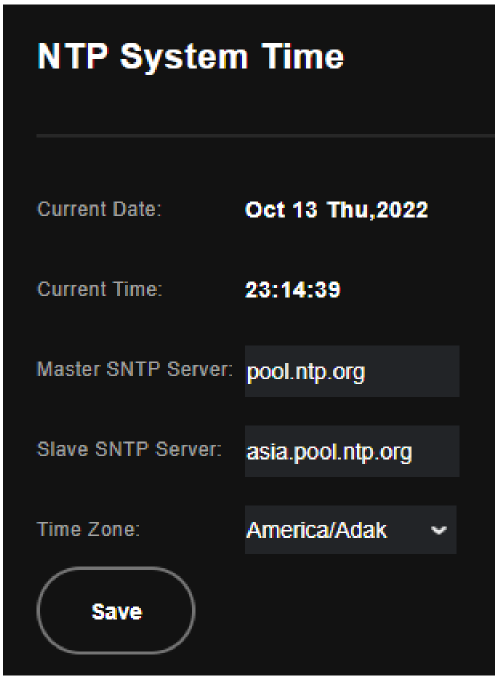


Figure 58 – System menu

This section provides a variety of options for configuring system related settings.

NTP System Time

The tools on this page allow you to use the Network Time Protocol (NTP) to configure specific time servers to synchronise time, set local time zones, etc. for the modem. The time servers are correct to within a few milliseconds of Coordinated Universal Time (UTC).



NTP System Time

Current Date: Oct 13 Thu,2022

Current Time: 23:14:39

Master SNTP Server: pool.ntp.org

Slave SNTP Server: asia.pool.ntp.org

Time Zone: America/Adak

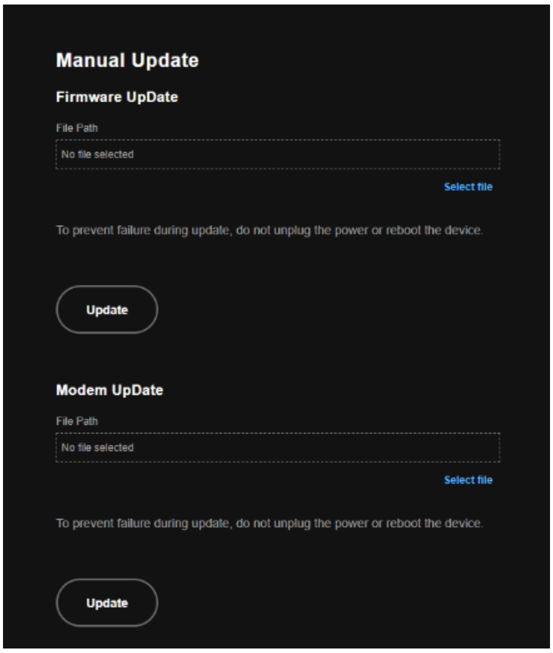
Figure 59 – NTP System Time settings

Field	Description
Current Date	
Current Time	
Master SNTP server	
Slave SNTP server	
Time Zone	Select a Time Zone for the gateway from the drop-down list.
Save button	

Table 17 – NTP System Time settings table

Manual Firmware Update

Use this feature to update the firmware of the gateway when future updates are available. Sometimes this can fix problems or add new features.



Manual Update

Firmware UpDate

File Path

No file selected

Select file

To prevent failure during update, do not unplug the power or reboot the device.

Update

Modem UpDate

File Path

No file selected

Select file

To prevent failure during update, do not unplug the power or reboot the device.

Update

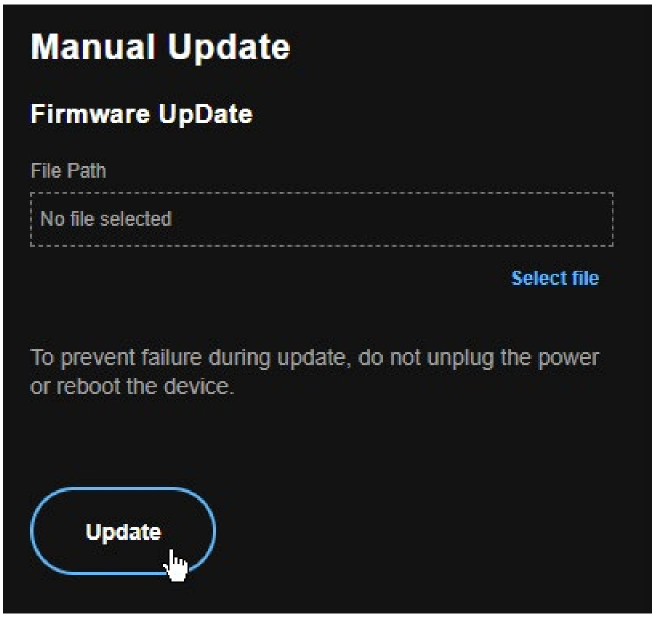
Figure 60 – Settings – Update Settings page

© Casa Systems 2022

Firmware Update

This page is used to manually update your gateway's firmware.

1. Save the firmware image file to a folder on your computer. Usually this will be your browser's default Downloads folder.
2. Choose the Select File button to locate the image file.
3. Select the Update button once to upload and install the file.


Manual Update

Firmware UpDate

File Path

No file selected

To prevent failure during update, do not unplug the power or reboot the device.

Figure 61 – Update Firmware page

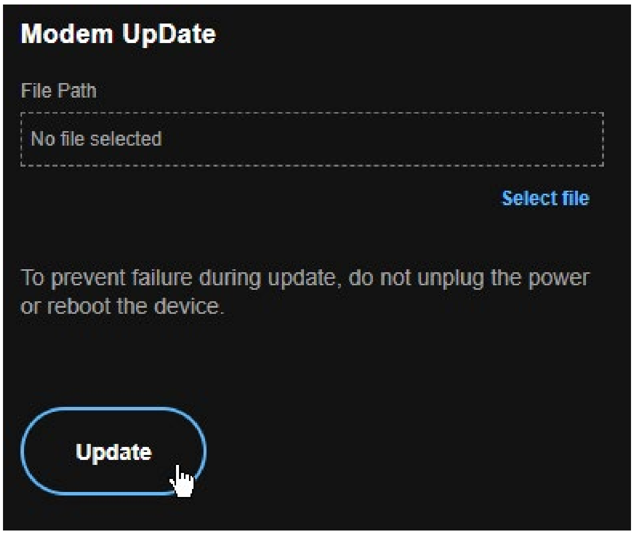
The gateway performs the firmware installation and reboots on completion.

Modem Update

This page is used to manually update your gateway's modem firmware.

1. Select the Choose File button to locate the image file.
2. Select the Update Firmware button once to upload and install the file.

© Casa Systems 2022



To prevent failure during update, do not unplug the power or reboot the device.

Figure 62 – Update Modem Firmware page

The gateway performs the firmware installation and reboots on completion

Backup/Restore

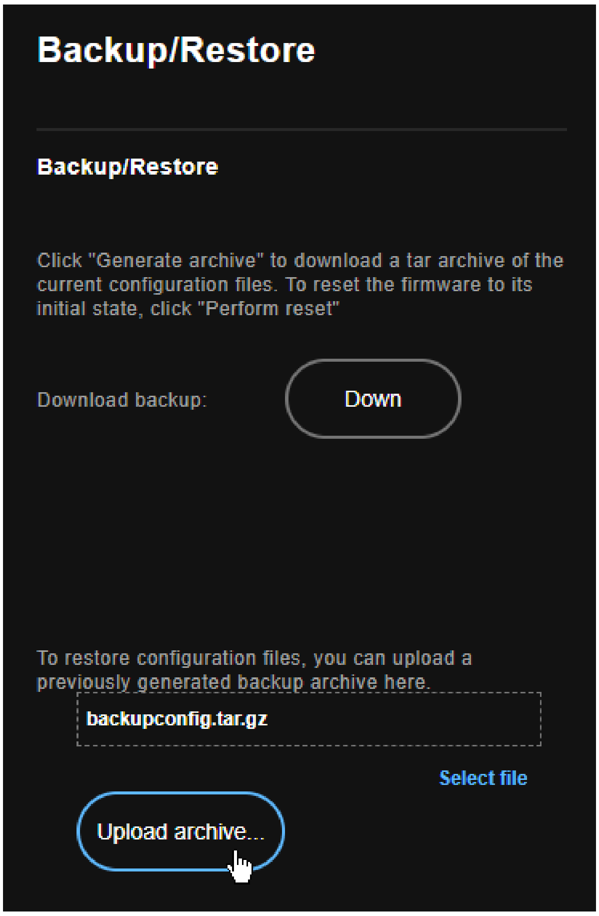
Use this feature to restore a previously saved configuration using the Backup feature. If you are restoring the configuration to a new gateway or if you previously changed the encryption key to the configuration file and then factory reset the device, you must first enter the encryption key in the Configurations Encryption Key field in the Settings – Backup page, and click on Apply/Save. To restore a saved configuration, click on the Browse button and locate a file that you have saved to restore a previous configuration. Click on the Update settings button to upload the selected file. Please allow up to 5 minutes for the system to apply the configuration and reboot.

Backup

This feature allows you to take a snapshot of the current configuration of your gateway so that you can roll back to the current configuration if you plan to make changes.

To back up the current configuration, select the Down button to save the current configuration settings. The configuration file is saved via your browser to the downloads folder configured in your browser.

© Casa Systems 2022



Backup/Restore

Backup/Restore

Click "Generate archive" to download a tar archive of the current configuration files. To reset the firmware to its initial state, click "Perform reset"

Download backup:

To restore configuration files, you can upload a previously generated backup archive here.

backupconfig.tar.gz

Figure 63 – Settings – Backup page

To restore the configuration on your gateway:

1. Choose the Select file link
2. Locate the configuration backup file on your computer.
3. Select the Upload archive button. The configuration is restored to the gateway.

Restore Default

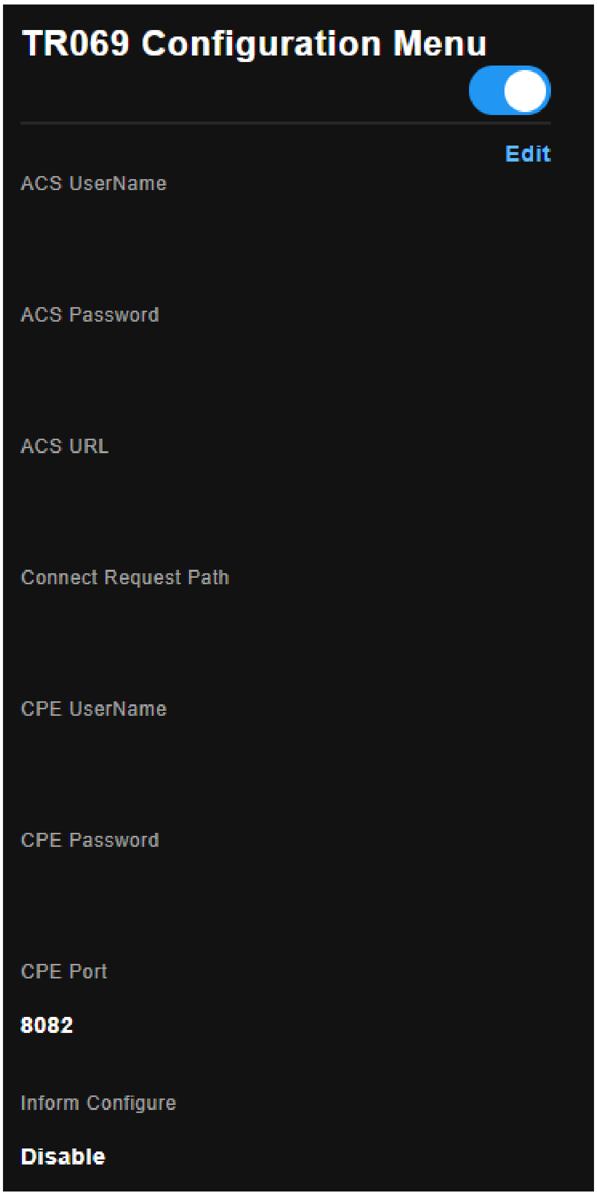
This feature resets all the settings of the gateway to the factory default settings. When you select this option, the settings will be erased and the gateway reboots. Please allow up to 2 minutes for the gateway to restart.

Figure 64 – Settings – Factory Reset page

TR069 Configuration

TR-069 enables provisioning, auto-configuration or diagnostics to be automatically performed on your gateway if supported by your Internet Service Provider (ISP).

View details mode



TR069 Configuration Menu

Edit

ACS UserName

ACS Password

ACS URL

Connect Request Path

CPE UserName

CPE Password

CPE Port

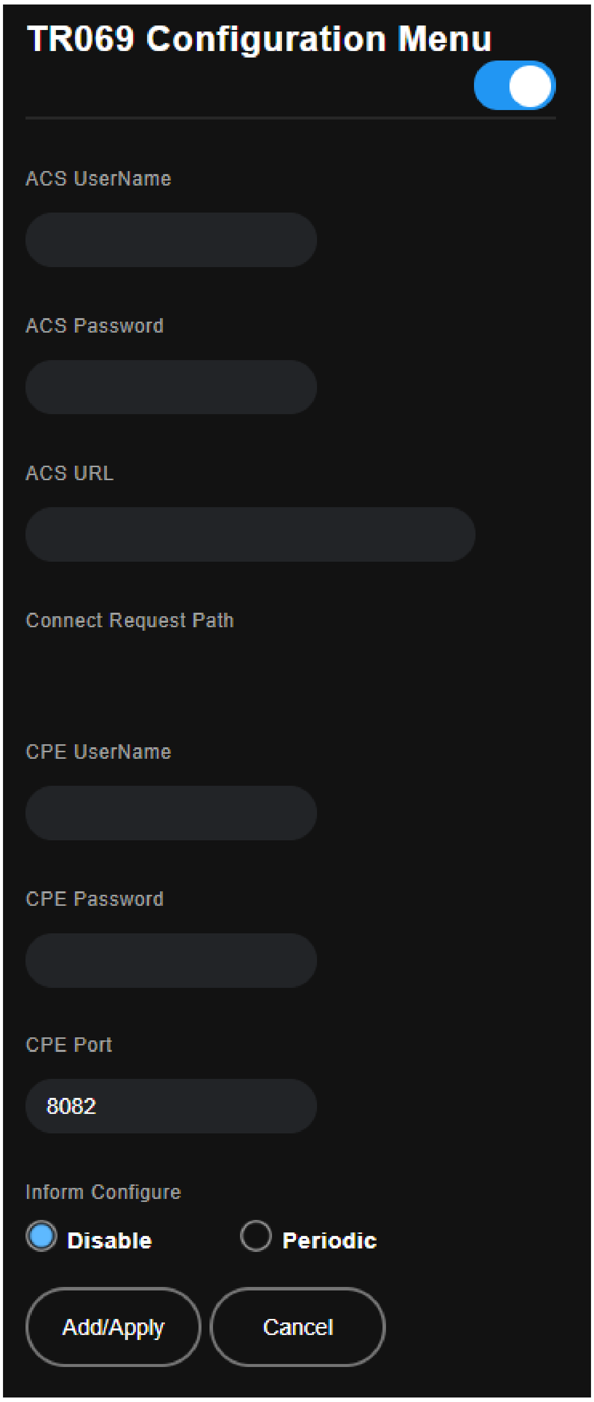
8082

Inform Configure

Disable

Figure 65 –TR-069 Configuration Menu

Edit mode



TR069 Configuration Menu

ACS UserName

ACS Password

ACS URL

Connect Request Path

CPE UserName

CPE Password

CPE Port

8082

Inform Configure

● Disable ○ Periodic

Figure 66 –TR-069 Configuration Menu

© Casa Systems 2022

Field	Description
Inform	Set to enable to TR-069 client inform session initialization.
Inform interval	Time in seconds that inform session data is sent to the Auto-Configuration Server (ACS).
ACS URL	The address where the ACS server is located.
ACS User Name	The user name to access the ACS server.
ACS Password	The password to access the ACS server.
	Disable – turns off Periodic – Enter the Peirodic Inverval in seconds.
WAN Interface used by TR-069 Client	The interface connection used to send and receive data to the ACS server.

Table 18 – TR-069 Client settings table

EasyMesh Setting

EasyMesh is a standard that allows you to easily create a mesh network with other EasyMesh compatible devices. To configure the EasyMesh function:

1 Select the **Edit** button, then select the **Model** from the drop-down list. The Model is the function of the gateway in the mesh network. Set the unit as Controller if it is the main unit that connects to the wide area network, select Agent if the unit is going to act as an extension node.

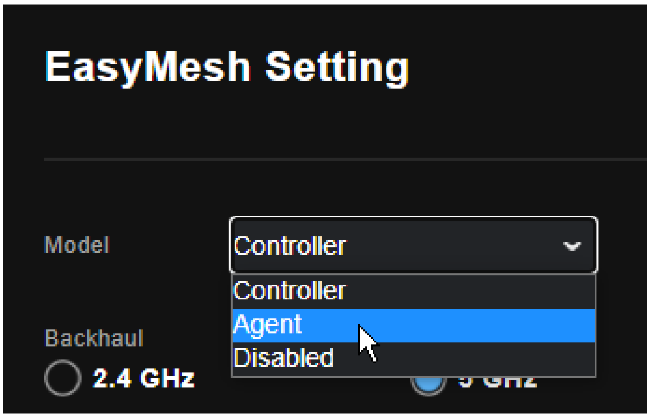
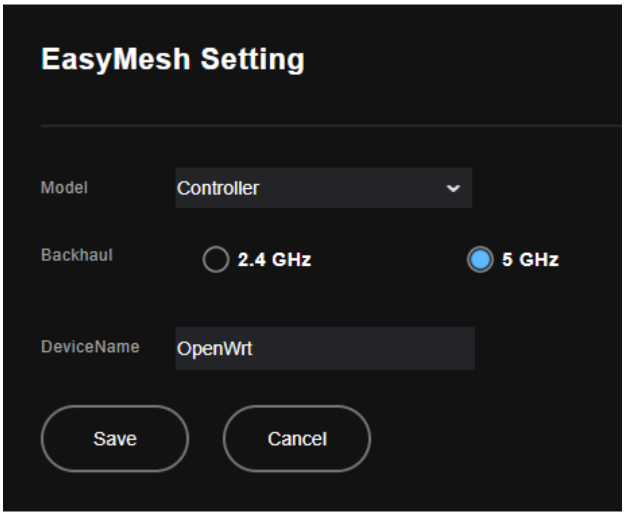


Figure 67 –EasyMesh Model setting



EasyMesh Setting

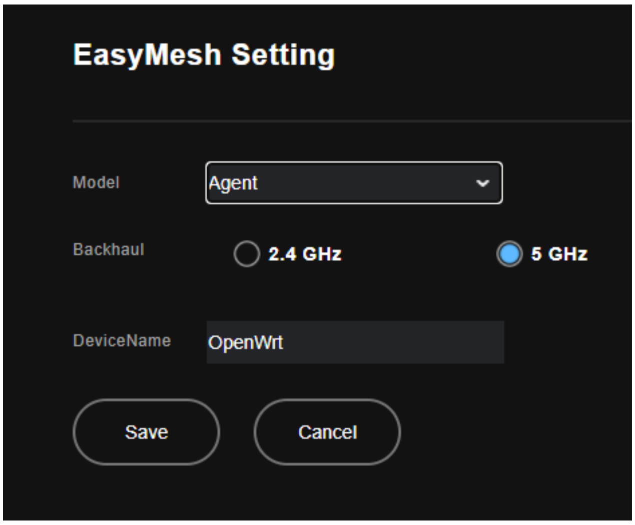
Model: Controller

Backhaul: ○ 2.4 GHz ● 5 GHz

DeviceName: OpenWrt

Figure 68 –EasyMesh Controller Settings page

2 Set a backhaul band. Since the 2.4GHz band is generally crowded with devices, it is best to select 5GHz for the backhaul. The 5GHz band also has higher throughput, at the cost of shorter range. If your Controller and Agent devices are quite far apart, or the 5GHz signal strength between them is not good, select the backhaul to operate on 2.4GHz.



EasyMesh Setting

Model: Agent

Backhaul: ○ 2.4 GHz ● 5 GHz

DeviceName: OpenWrt

Figure 69 –EasyMesh Agent Settings page

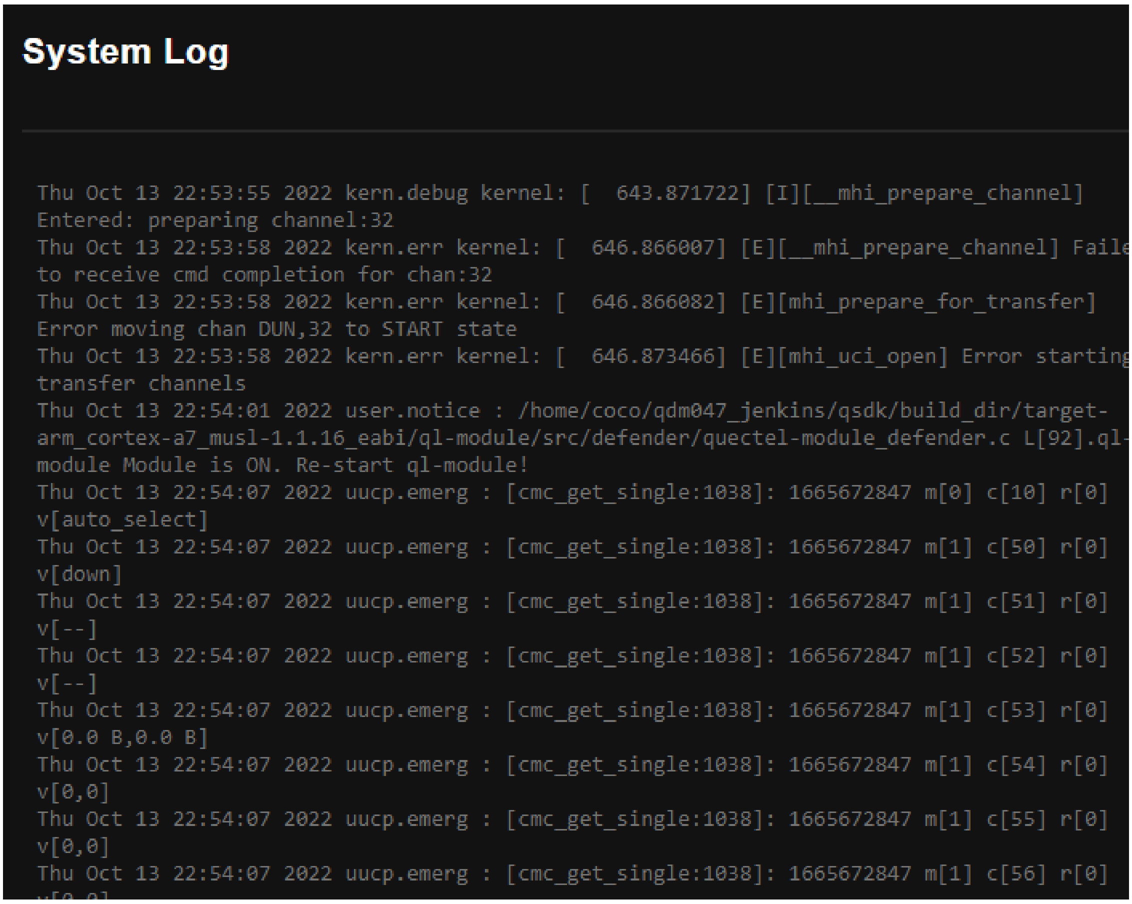
Field	Description
Model	Sets the function of the EasyMesh node. Set to Controller for the main unit and Agent for an extension node.
Backhaul	Select either 2.4 GHGz or 5 GHz
DeviceName	A name to identify the node on your network.

Table 19 – EasyMesh Agent settings table

© Casa Systems 2022

System Log

The System log page allows you to view the log of the gateway and configure the logging level also. To view the system log, click the View System Log button.



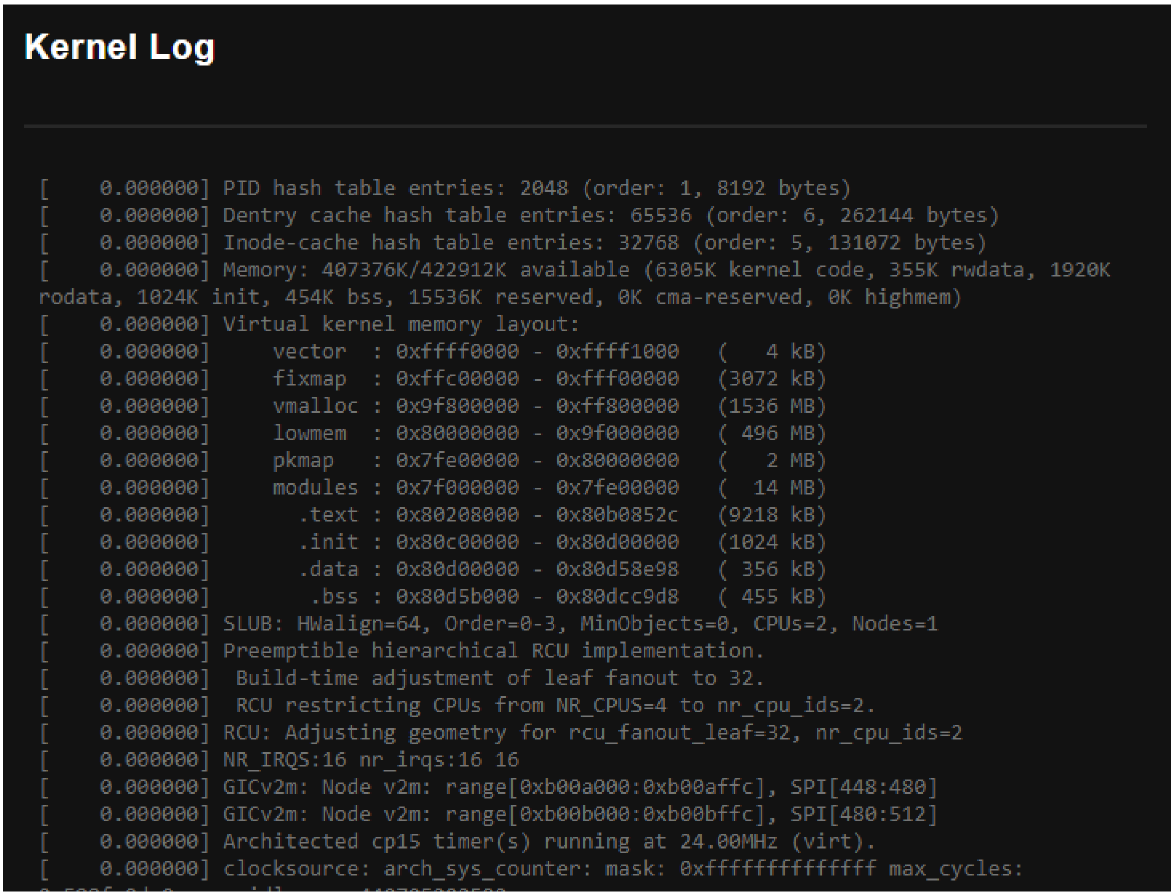
System Log

```
Thu Oct 13 22:53:55 2022 kern.debug kernel: [  643.871722] [I][__mhi_prepare_channel]
Entered: preparing channel:32
Thu Oct 13 22:53:58 2022 kern.err kernel: [  646.866007] [E][__mhi_prepare_channel] Faile
to receive cmd completion for chan:32
Thu Oct 13 22:53:58 2022 kern.err kernel: [  646.866082] [E][mhi_prepare_for_transfer]
Error moving chan DUN,32 to START state
Thu Oct 13 22:53:58 2022 kern.err kernel: [  646.873466] [E][mhi_uci_open] Error starting
transfer channels
Thu Oct 13 22:54:01 2022 user.notice : /home/coco/qdm047_jenkins/qsdk/build_dir/target-
arm_cortex-a7_musl-1.1.16_eabi/ql-module/src/defender/quectel-module_defender.c L[92].ql-
module Module is ON. Re-start ql-module!
Thu Oct 13 22:54:07 2022 uucp.emerg : [cmc_get_single:1038]: 1665672847 m[0] c[10] r[0]
v[auto_select]
Thu Oct 13 22:54:07 2022 uucp.emerg : [cmc_get_single:1038]: 1665672847 m[1] c[50] r[0]
v[down]
Thu Oct 13 22:54:07 2022 uucp.emerg : [cmc_get_single:1038]: 1665672847 m[1] c[51] r[0]
v[--]
Thu Oct 13 22:54:07 2022 uucp.emerg : [cmc_get_single:1038]: 1665672847 m[1] c[52] r[0]
v[--]
Thu Oct 13 22:54:07 2022 uucp.emerg : [cmc_get_single:1038]: 1665672847 m[1] c[53] r[0]
v[0.0 B,0.0 B]
Thu Oct 13 22:54:07 2022 uucp.emerg : [cmc_get_single:1038]: 1665672847 m[1] c[54] r[0]
v[0,0]
Thu Oct 13 22:54:07 2022 uucp.emerg : [cmc_get_single:1038]: 1665672847 m[1] c[55] r[0]
v[0,0]
Thu Oct 13 22:54:07 2022 uucp.emerg : [cmc_get_single:1038]: 1665672847 m[1] c[56] r[0]
v[0,0]
```

Figure 70 –System Log

Kernel Log

The kernel log is an advanced system log used by technical support during troubleshooting.



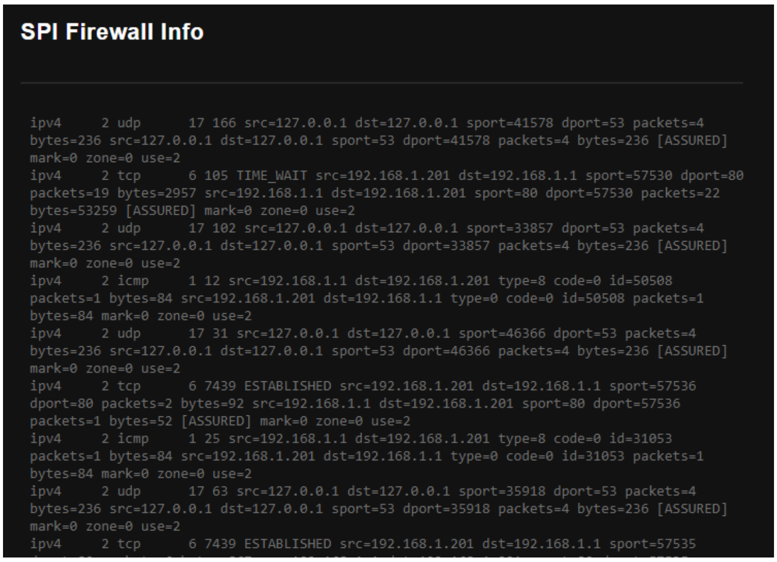
Kernel Log

```
[    0.000000] PID hash table entries: 2048 (order: 1, 8192 bytes)
[    0.000000] Dentry cache hash table entries: 65536 (order: 6, 262144 bytes)
[    0.000000] Inode-cache hash table entries: 32768 (order: 5, 131072 bytes)
[    0.000000] Memory: 407376K/422912K available (6305K kernel code, 355K rwdata, 1920K
rodata, 1024K init, 454K bss, 15536K reserved, 0K cma-reserved, 0K highmem)
[    0.000000] Virtual kernel memory layout:
[    0.000000]     vector  : 0xffff0000 - 0xffff1000   (   4 kB)
[    0.000000]     fixmap  : 0xffc00000 - 0xfff00000   (3072 kB)
[    0.000000]     vmalloc : 0x9f800000 - 0xff800000   (1536 MB)
[    0.000000]     lowmem  : 0x80000000 - 0x9f000000   ( 496 MB)
[    0.000000]     pkmap   : 0x7fe00000 - 0x80000000   (   2 MB)
[    0.000000]     modules : 0x7f000000 - 0x7fe00000   (  14 MB)
[    0.000000]       .text : 0x80208000 - 0x80b0852c   (9218 kB)
[    0.000000]       .init : 0x80c00000 - 0x80d00000   (1024 kB)
[    0.000000]       .data : 0x80d00000 - 0x80d58e98   ( 356 kB)
[    0.000000]        .bss : 0x80d5b000 - 0x80dcc9d8   ( 455 kB)
[    0.000000] SLUB: HWalign=64, Order=0-3, MinObjects=0, CPUs=2, Nodes=1
[    0.000000] Preemptible hierarchical RCU implementation.
[    0.000000]  Build-time adjustment of leaf fanout to 32.
[    0.000000]  RCU restricting CPUs from NR_CPUS=4 to nr_cpu_ids=2.
[    0.000000] RCU: Adjusting geometry for rcu_fanout_leaf=32, nr_cpu_ids=2
[    0.000000] NR_IRQS:16 nr_irqs:16 16
[    0.000000] GICv2m: Node v2m: range[0xb00a000:0xb00affc], SPI[448:480]
[    0.000000] GICv2m: Node v2m: range[0xb00b000:0xb00bffc], SPI[480:512]
[    0.000000] Architected cp15 timer(s) running at 24.00MHz (virt).
[    0.000000] clocksource: arch_sys_counter: mask: 0xffffffffffffff max_cycles:
```

Figure 71 – Kernel Log

SPI Firewall Info

The Stateful Packet Inspection Firewall log can be viewed by selecting the SPI Firewall Info link from the menu on the left.



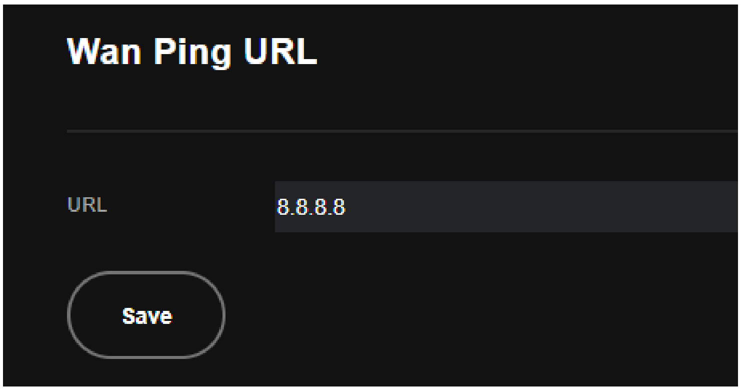
SPI Firewall Info

```
ipv4     2 udp      17 166 src=127.0.0.1 dst=127.0.0.1 sport=41578 dport=53 packets=4
bytes=236 src=127.0.0.1 dst=127.0.0.1 sport=53 dport=41578 packets=4 bytes=236 [ASSURED]
mark=0 zone=0 use=2
ipv4     2 tcp      6 105 TIME_WAIT src=192.168.1.201 dst=192.168.1.1 sport=57530 dport=80
packets=19 bytes=2957 src=192.168.1.1 dst=192.168.1.201 sport=80 dport=57530 packets=22
bytes=53259 [ASSURED] mark=0 zone=0 use=2
ipv4     2 udp      17 102 src=127.0.0.1 dst=127.0.0.1 sport=33857 dport=53 packets=4
bytes=236 src=127.0.0.1 dst=127.0.0.1 sport=53 dport=33857 packets=4 bytes=236 [ASSURED]
mark=0 zone=0 use=2
ipv4     2 icmp     1 12 src=192.168.1.1 dst=192.168.1.201 type=8 code=0 id=50508
packets=1 bytes=84 src=192.168.1.201 dst=192.168.1.1 type=0 code=0 id=50508 packets=1
bytes=84 mark=0 zone=0 use=2
ipv4     2 udp      17 31 src=127.0.0.1 dst=127.0.0.1 sport=46366 dport=53 packets=4
bytes=236 src=127.0.0.1 dst=127.0.0.1 sport=53 dport=46366 packets=4 bytes=236 [ASSURED]
mark=0 zone=0 use=2
ipv4     2 tcp      6 7439 ESTABLISHED src=192.168.1.201 dst=192.168.1.1 sport=57536
dport=80 packets=2 bytes=92 src=192.168.1.1 dst=192.168.1.201 sport=80 dport=57536
packets=1 bytes=52 [ASSURED] mark=0 zone=0 use=2
ipv4     2 icmp     1 25 src=192.168.1.1 dst=192.168.1.201 type=8 code=0 id=31053
packets=1 bytes=84 src=192.168.1.201 dst=192.168.1.1 type=0 code=0 id=31053 packets=1
bytes=84 mark=0 zone=0 use=2
ipv4     2 udp      17 63 src=127.0.0.1 dst=127.0.0.1 sport=35918 dport=53 packets=4
bytes=236 src=127.0.0.1 dst=127.0.0.1 sport=53 dport=35918 packets=4 bytes=236 [ASSURED]
mark=0 zone=0 use=2
ipv4     2 tcp      6 7439 ESTABLISHED src=192.168.1.201 dst=192.168.1.1 sport=57535
```

Figure 72 – SPI Firewall Info display

WAN Ping URL

The ping test page lets you ping a remote IP address or hostname to test the connection.



Wan Ping URL

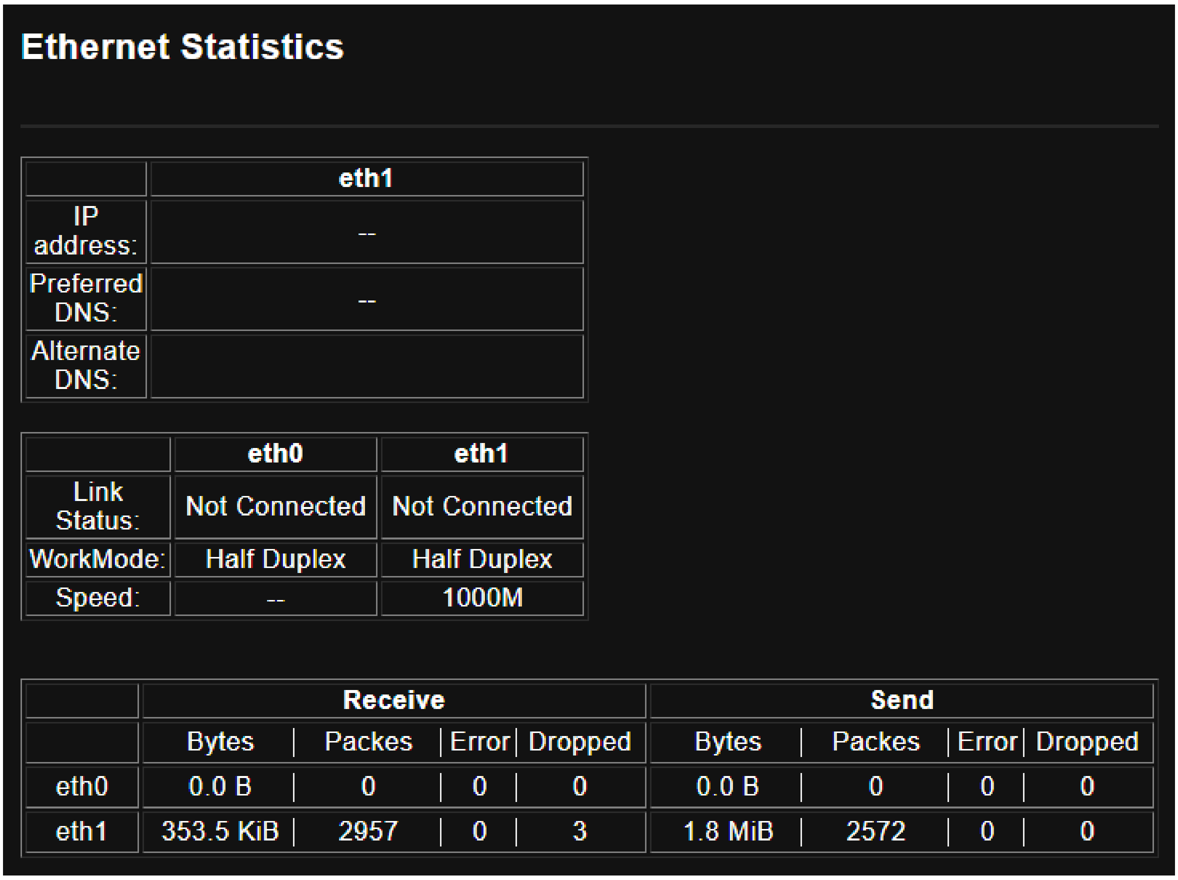
URL: 8.8.8.8

Figure 73 – Wang Ping URL

Enter a URL or IP address into the field that you want to use to conduct the ping test.

Click the Save button to save the URL/IP address that is used to verify that the internet connection is up.

Ethernet Statistics



Ethernet Statistics

	eth1
IP address:	--
Preferred DNS:	--
Alternate DNS:	

	eth0	eth1
Link Status:	Not Connected	Not Connected
WorkMode:	Half Duplex	Half Duplex
Speed:	--	1000M

	Receive				Send			
	Bytes	Packes	Error	Dropped	Bytes	Packes	Error	Dropped
eth0	0.0 B	0	0	0	0.0 B	0	0	0
eth1	353.5 KiB	2957	0	3	1.8 MiB	2572	0	0

Figure 74 – ATM PVC Configuration page

Field	Description

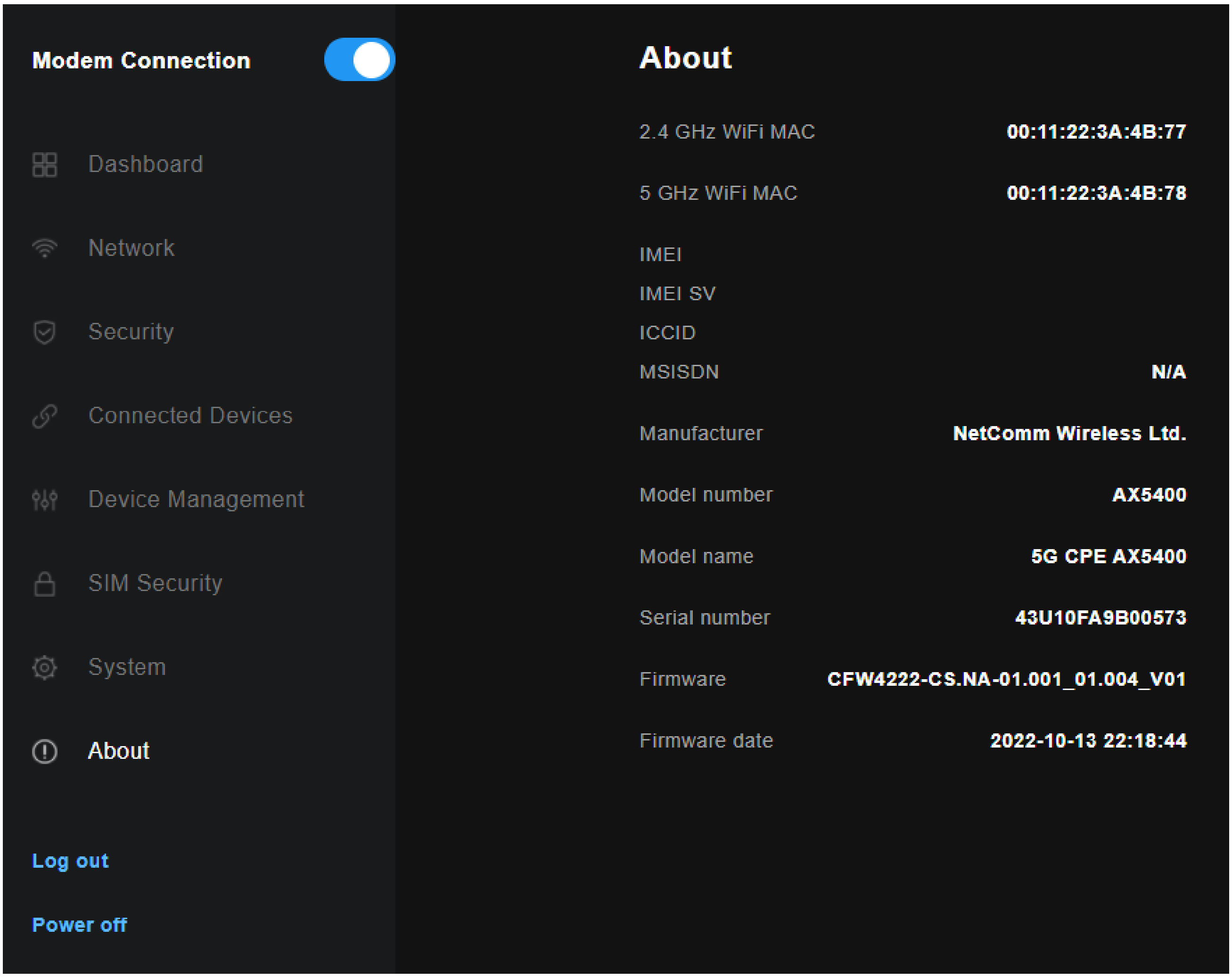
IP Addtess	
Preferred DNS	
Alternative DNS	
Link Status	
WorkMode Speed	
Receive/Send	
Eth0, Eth1, etc	
Bytes	
Packets	
Error	
Dropped	

Table 20 – DSL ATM Interface Configuration settings table

© Casa Systems 2022

About

The About page shows general information about your gateway such as model numbers and firmware versions.



About

2.4 GHz WiFi MAC	00:11:22:3A:4B:77
5 GHz WiFi MAC	00:11:22:3A:4B:78
IMEI	
IMEI SV	
ICCID	
MSISDN	N/A
Manufacturer	NetComm Wireless Ltd.
Model number	AX5400
Model name	5G CPE AX5400
Serial number	43U10FA9B00573
Firmware	CFW4222-CS.NA-01.001_01.004_V01
Firmware date	2022-10-13 22:18:44

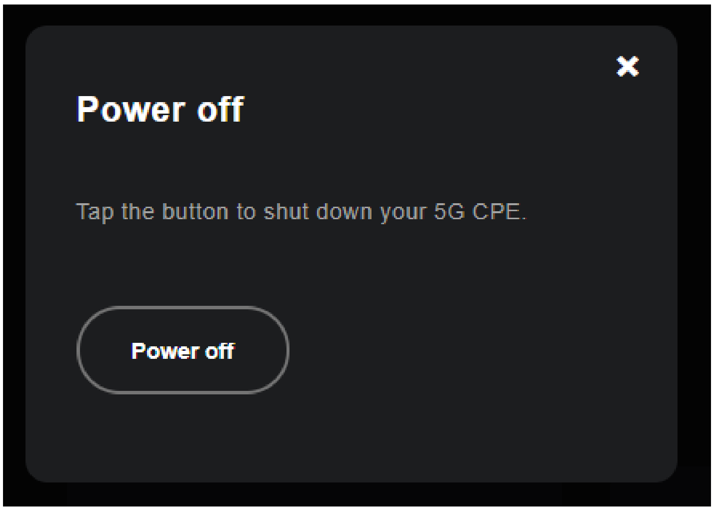
Log out

When you have finished configuring the gateway, log out to prevent unauthorized access to the configuration interface.

© Casa Systems 2022

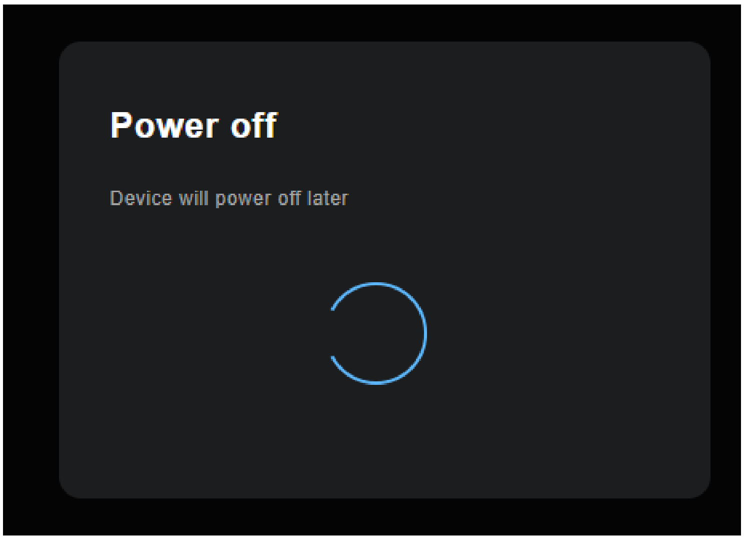
Power off

If you cannot reach the physical power button, you can use the web interface to turn off the gateway. Select the Power off button



Power off

Tap the button to shut down your 5G CPE.



Power off

Device will power off later

FCC regulation information

FCC Statement

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.

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 or more 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
- This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

CAUTION!

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

RF Exposure

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20cm between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

© Casa Systems 2022

Company contact details

Casa Systems, Inc.

100 Old River Road, Andover, Massachusetts 01810 USA

https://www.casa-systems.com/contact-us/

Product details

Product: 5G Wi-Fi 6 Residential Gateway

Model No: CFW-4222

© Casa Systems 2022