CGN3 Residential D3 WiFi Gateway

User's Guide

Version 1.1 - 08/2013

hitron

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the CGN3's features via its Graphical User Interface (GUI).

How to Use this User's Guide

This manual contains information on each the CGN3's GUI screens, and describes how to use its various features.

▸ Use the CGN3 Overview on page 14 to see an overview of the topics covered in this manual.

▸ Use the Table of Contents (page 6), List of Figures (page 10) and List of Tables (page 12) to quickly find information about a particular GUI screen or topic.

▸ Use the Index (page 110) to find information on a specific keyword.

▸ Use the rest of this User's Guide to see in-depth descriptions of the CGN3's features.

Related Documentation

▸ **Quick Installation Guide**: see this for information on getting your CGN3 up and running right away. It includes information on system requirements, package contents, the installation procedure, and basic troubleshooting tips.

▶ **Online Help**: each screen in the CGN3's Graphical User Interface (GUI) contains a **Help** button. Click this button to see additional information about configuring the screen.

Document Conventions

This User's Guide uses various typographic conventions and styles to indicate content type:

▶ Bulleted paragraphs are used to list items, and to indicate options.

1 Numbered paragraphs indicate procedural steps.

NOTE: Notes provide additional information on a subject.

💣 **Warnings provide information about actions that could harm you or your device.**

Product labels, field labels, field choices, etc. are in **bold** type. For example:

> Select **UDP** to use the User Datagram Protocol.

A mouse click in the Graphical User Interface (GUI) is denoted by a right angle bracket (>). For example:

> Click **Settings** > **Advanced Settings**.

means that you should click **Settings** in the GUI, then **Advanced settings**.

A key stroke is denoted by square brackets and uppercase text. For example:

> Press [ENTER] to continue.

Customer Support

For technical assistance or other customer support issues, please consult your Hitron representative.

Default Login Details

The CGN3's default IP address and login credentials are as follows. For more information, see Login to the CGN3 on page 23.

Table 1:   Default Credentials

IP Address	192.168.0.1
Username	cusadmin
Password	password

Table of Contents

List of Figures

Version 1.1, 08/2013. Copyright © 2013 Hitron Technologies

List of Tables

1

Introduction

This chapter introduces the CGN3 and its GUI (Graphical User Interface).

1.1 CGN3 Overview

Your CGN3 is a NAT-capable cable modem and wireless access point that allows you to connect your computers, wireless devices, and other network devices to one another, and to the Internet via the cable connection.

💣 **The CGN3 must be placed vertically on its stand, should not be positioned in either wall-mount or horizontal.**

Figure 1:   Application Overview
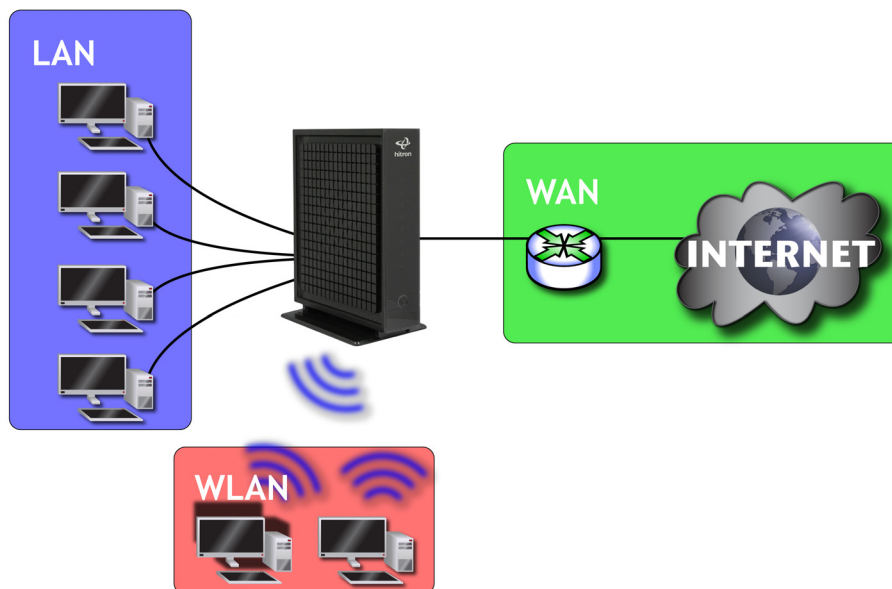
1.1.1 Key Features

The CGN3 provides:

▸ High-performance DOCSIS/EuroDOCSIS 3.0 (24-channel downstream, 8-channel upstream) Internet connection to cable modem service via the **CATV** port (F-type RF connector) at speeds of up to 960 Mbps (megabits per second)

▸ Full dual-stack IPv4/IPv6 support for routing and firewall (DSLite and 6RD)

▸ Local Area Network connection via four 10/100/1000 Mbps Ethernet ports

▸ Dynamic Host Configuration Protocol (DHCP) for devices on the LAN

▸ LAN troubleshooting tools (Ping and Traceroute)

▸ IEEE 802.11b/g/n concurrent dual band (2.4GHz and 5GHz) wireless MIMO (Multiple-In, Multiple-Out) networking, allowing speeds of up to 300Mbps

▸ Wireless security: WEP, WPA-PSK and WPA2-PSK encryption, Wifi Protected Setup (WPS) push-button and PIN configuration, MAC filtering,

▸ Wired security: stateful inspection firewall with intrusion detection system, IP and MAC filtering, port forwarding and port triggering, De-Militarized Zone (DMZ) and event logging

▸ Parental control: scheduled website blocking and access logs

▸ Settings backup and restore

▸ Secure configuration interface, accessible by Web browser

1.2 Hardware Connections

This section describes the CGN3's physical ports and buttons.

Figure 2: Hardware Connections

Table 2:   Hardware Connections

WPS	Press this button to begin the WiFi Protected Setup (WPS) Push-Button Configuration (PBC) procedure.
	Press the PBC button on your wireless clients in the coverage area within two minutes to enable them to join the wireless network.
	See WPS on page 68 for more information.
USB	The CGN3 provides two USB 2.0 host ports on the rear, allowing you to plug in USB flash disks for mounting and sharing through the LAN interfaces via the Samba protocol (network neighborhood).
	The CGN3 supports the following Windows file systems:
	‣ FAT16
	‣ FAT32
	‣ NTFS
	💣 **USB devices must not drain more than 500mA from the USB port. USB devices requiring more than 500mA should be provided with their own power source(s).**
Reset	Use this button to reboot or reset your CGN3.
	‣ Press the button and hold it for less than five seconds to reboot the CGN3. The CGN3 restarts, using your existing settings.
	‣ Press the button and hold it for more than five seconds to delete all user-configured settings and restart the CGN3 using its factory default settings. See Resetting the CGN3 on page 25 for more information on resetting the CGN3.
	NOTE: Unless you previously backed-up the CGN3's configuration settings prior to resetting the CGN3, the settings cannot be recovered.
LAN1	Use these ports to connect your computers and other network devices, using Category 5 or 6 Ethernet cables with RJ45 connectors.
LAN2	
LAN3	
LAN4	

Table 2:   Hardware Connections

CABLE	Use this to connect to the Internet via an F-type RF cable.
POWER	Use this to connect to the 12v/2A power adapter that came with your CGN3. 💣 **NEVER use another power adapter with your CGN3. Doing so could harm your CGN3.** Figure 3: Power Adaptor

1.3 LEDs

This section describes the CGN3's LEDs (lights).

Figure 4:   LEDs

Table 3:   LEDs

LED	STATUS	DESCRIPTION
POWER	Off	The CGN3 is not receiving power.
	On	The CGN3 is receiving power.

Table 3:   LEDs

DS	Green, blinking	The CGN3 is searching for a downstream frequency on the **CABLE** connection.
	Green, steady	The CGN3 has successfully located and locked onto a downstream frequency on the **CABLE** connection.
	Blue	The CGN3 is engaged in channel bonding on the downstream connection.
	Off	There is no downstream activity on the **CABLE** connection.
US	Green, blinking	The CGN3 is searching for an upstream frequency on the **CABLE** connection.
	Green, steady	The CGN3 has successfully located and locked onto an upstream frequency on the **CABLE** connection.
	Blue	The CGN3 is engaged in channel bonding on the upstream connection.
	Off	There is no upstream activity on the **CABLE** connection.
STATUS	Blinking	The CGN3's cable modem is registering with the service provider's CMTS.
	On	The CGN3's cable modem has successfully registered with the service provider and is ready for data transfer.
LAN	Off	No device is connected to one of the **LAN** ports.
	Green, blinking	A device is connected to one of the **LAN** ports via a Fast Ethernet (100Mbps) link, and is transmitting or receiving data.
	Green, steady	A device is connected to one of the **LAN** ports via a Fast Ethernet (100Mbps) link, but is not transmitting or receiving data.
	Blue, blinking	A device is connected to one of the **LAN** ports via a Gigabit Ethernet (1000Mbps) link, and is transmitting or receiving data.
	Blue, steady	A device is connected to one of the **LAN** ports via a Gigabit Ethernet (1000Mbps) link, but is not transmitting or receiving data.

Table 3:   LEDs

WIRELESS (2.4GHZ)	Off	The 2.4GHz wireless network is not enabled.
	Green, steady	The 2.4GHz wireless network is enabled, and no data is being transmitted or received over the 2.4GHz wireless network.
	Green, blinking	The 2.4GHz wireless network is enabled, and data is being transmitted or received over the 2.4GHz wireless network.
	Bi-color	Wi-Fi Protected Setup (WPS) is in operation on the 2.4GHz wireless network.
WIRELESS (5GHZ)	Off	The 5GHz wireless network is not enabled.
	Green, steady	The 5GHz wireless network is enabled, and no data is being transmitted or received over the 5GHz wireless network.
	Green, blinking	The 5GHz wireless network is enabled, and data is being transmitted or received over the 5GHz wireless network.
	Bi-color	Wi-Fi Protected Setup (WPS) is in operation on the 5GHz wireless network.
USB	Off	No USB device is connected to either USB port.
	Green, steady	A USB device is connected to one of the USB ports, and is not transmitting or receiving data.
	Green, blinking	A USB device is connected to one of the USB ports, and is transmitting or receiving data.

When you turn on the CGN3, the LEDs light up in the following order:

1 **POWER**

2 **DS**

3 **US**

4 **STATUS**

▸ The **LAN** LED lights up as soon as there is activity on the LAN ports, the **WIRELESS** LEDs light up once the wireless network is ready, and the **USB** LED lights up once a connected device on either USB port is detected.

1.4 IP Address Setup

Before you log into the CGN3's GUI, your computer's IP address must be in the same subnet as the CGN3. This allows your computer to communicate with the CGN3.

NOTE: See IP Addresses and Subnets on page 34 for background information.

The CGN3 has a built-in DHCP server that, when active, assigns IP addresses to computers on the LAN. When the DHCP server is active, you can get an IP address automatically. The DHCP server is active by default.

If your computer is configured to get an IP address automatically, or if you are not sure, try to log in to the CGN3 (see GUI Overview on page 24).

▸ If the login screen displays, your computer is already configured correctly.

▸ If the login screen does not display, either the CGN3's DHCP server is not active or your computer is not configured correctly. Follow the procedure in Manual IP Address Setup on page 22 and set your computer to get an IP address automatically. Try to log in again. If you cannot log in, follow the manual IP address setup procedure again, and set a specific IP address as shown. Try to log in again.

NOTE: If you still cannot see the login screen, your CGN3's IP settings may have been changed from their defaults. If you do not know the CGN3's new address, you should return it to its factory defaults. See Resetting the CGN3 on page 25. Bear in mind that ALL user-configured settings are lost.

1.4.1 Manual IP Address Setup

By default, your CGN3's local IP address is **192.168.0.1**. If your CGN3 is using the default IP address, you should set your computer's IP address to be between **192.168.0.2** and **192.168.0.254**.

NOTE: If your CGN3 DHCP server is active, set your computer to get an IP address automatically in step 5. The CGN3 assigns an IP address to your computer. The DHCP server is active by default.

Take the following steps to manually set up your computer's IP address to connect to the CGN3:

NOTE: This example uses Windows XP; the procedure for your operating system may be different.

1 Click **Start**, then click **Control Panel**.

2 In the window that displays, double-click **Network Connections**.

3 Right-click your network connection (usually **Local Area Connection**) and click **Properties**.

4 In the **General** tab's **This connection uses the following items** list, scroll down and select **Internet Protocol (TCP/IP)**. Click **Properties**.

5 You can get an IP address automatically, or specify one manually:

▸ If your CGN3's DHCP server is active, select **Get an IP address automatically**.

▸ If your CGN3's DHCP server is active, select **Use the following IP address**. In the **IP address** field, enter a value between **192.168.0.2** and **192.168.0.254** (default). In the **Subnet mask** field, enter **255.255.255.0** (default).

NOTE: If your CGN3 is not using the default IP address, enter an IP address and subnet mask that places your computer in the same subnet as the CGN3.

6 Click **OK**. The **Internet Protocol (TCP/IP)** window closes. In the **Local Area Connection Properties** window, click **OK**.

Your computer now obtains an IP address from the CGN3, or uses the IP address that you specified, and can communicate with the CGN3.

1.5 Login to the CGN3
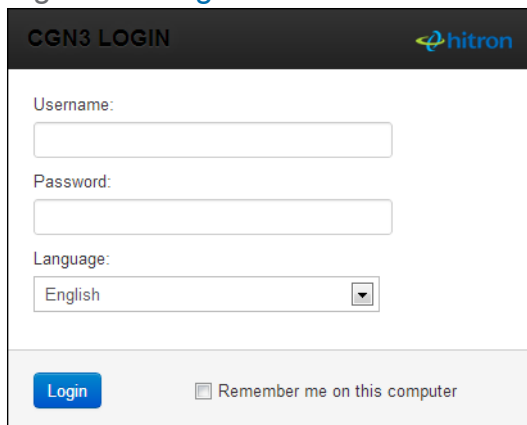
Take the following steps to login to the CGN3's GUI.

NOTE: You can login to the CGN3's GUI via the wireless interface. However, it is strongly recommended that you configure the CGN3 via a wired connection on the LAN.

1 Open a browser window.

2 Enter the CGN3's IP address (default **10.0.0.1**) in the URL bar. The **Login** screen displays.

Figure 5:   Login

3 Enter the **Username** and **Password**. The default login username is **admin**, and the default password is **password**.

NOTE: The Username and Password are case-sensitive; "password" is not the same as "Password".

4 Select the **Language**, if required. By default, the CGN3's interface displays in English.

5 Click **Login**. The **System Information** screen displays (see The System Information Screen on page 40).

1.6 GUI Overview

This section describes the CGN3's GUI.

Figure 6: GUI Overview
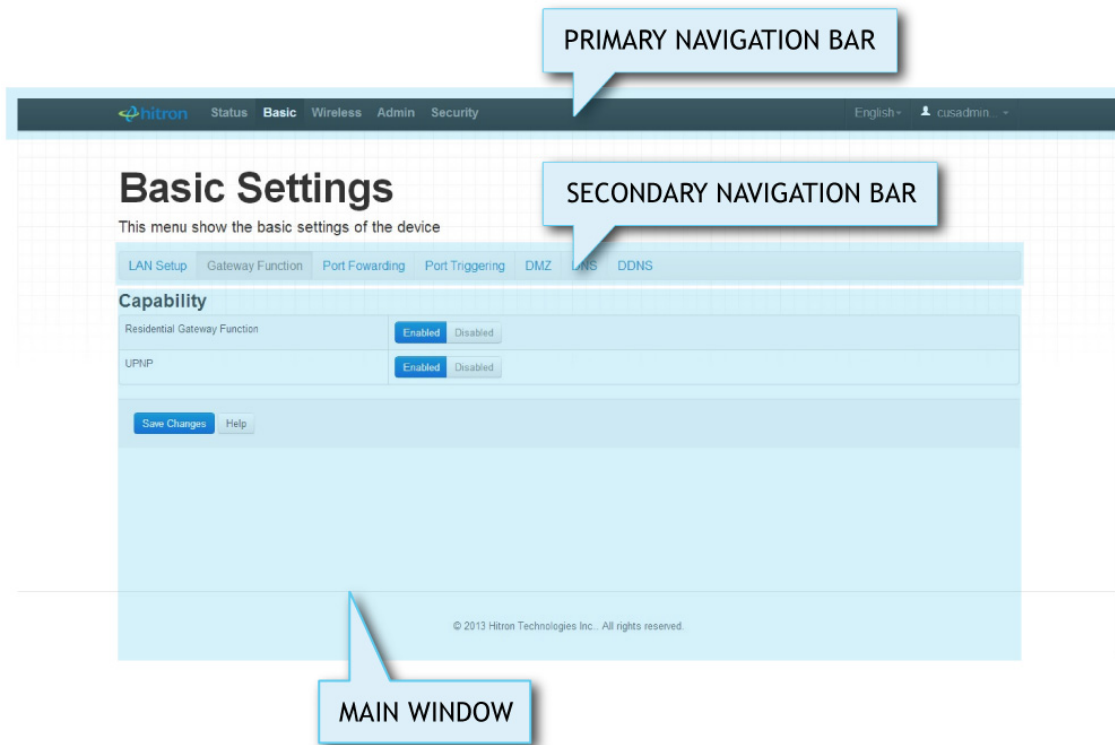
Table 4: GUI Overview

Primary Navigation Bar	Use this section to move from one part of the GUI to another, select the language and your login account.
Secondary Navigation Bar	Use this section to move from one related screen to another.
Main Window	Use this section to read information about your CGN3's configuration, and make configuration changes.

1.7 Resetting the CGN3

When you reset the CGN3 to its factory defaults, all user-configured settings are lost, and the CGN3 is returned to its initial configuration state.

There are two ways to reset the CGN3:

▸ Press the **RESET** button on the CGN3, and hold it in for ten seconds or longer.

‣ Click **Admin** > **Device Reset**. In the screen that displays, click the **Factory Reset** button.

After the operation, The CGN3 turns off and on again, using its factory default settings.

NOTE: Depending on your CGN3's previous configuration, you may need to re-configure your computer's IP settings; see IP Address Setup on page 22.

2

Setup Wizard

This chapter describes the CGN3's setup wizard, which displays when you click **Setup Wizard** in the toolbar. It contains the following sections:

2.1 Setup Wizard Overview

Your CGN3 possess a setup wizard that allows you to rapidly configure its most important settings, including password, LAN and wireless settings.
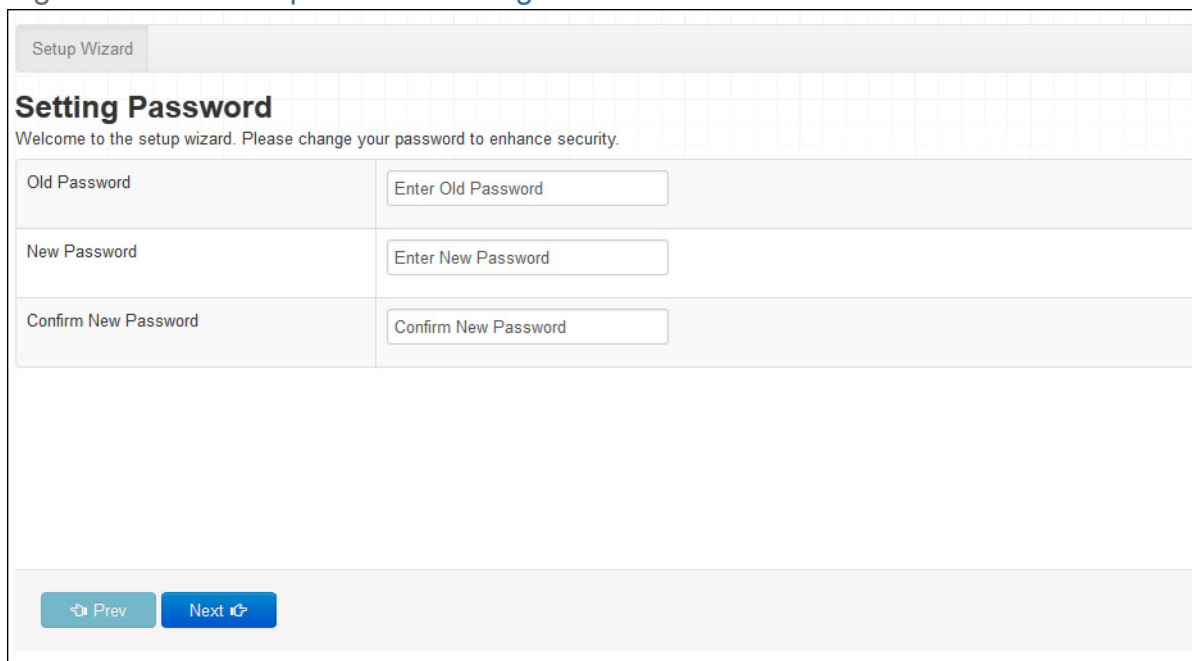
2.2 Setting Password

Use this screen to create a new password for the CGN3's user interface.

NOTE: It is strongly recommended that you change the CGN3's password from its factory default.

Click **Setup Wizard**. The following screen displays.

Figure 7:   The Setup Wizard: Setting Password Screen

The following table describes the labels in this screen.

Table 5:   The Setup Wizard: Setting Password Screen

Old Password	Enter the password with which you currently log into the CGN3 for this account.
New Password	Enter and re-enter the password you want to use to log into the CGN3 for this account.
Confirm New Password	
Prev	Click this to return to the previous screen.
Next	Click this to continue to the next screen.

2.3 LAN Settings

Use this screen to set up your CGN3's Local Area Network settings, including its IP address, subnet mask and DHCP status.

NOTE: If unsure about how to configure the fields in this screen, leave them at their defaults.

Click **Next** in the **Setup Wizard: Setting Password** screen. The following screen displays.

Figure 8: The Setup Wizard: LAN Settings Screen

The following table describes the labels in this screen.

Table 6: The Setup Wizard: LAN Settings Screen

Private LAN IP Address	Use this field to define the IP address of the CGN3 on the LAN.
Subnet Mask	Use this field to define the LAN subnet. Use dotted decimal notation (for example, **255.255.255.0**).
DHCP Status	Use this field to configure whether or not the CGN3's DHCP server is active. ▸ To turn the DHCP server on, click **Enabled**. ▸ To turn the DHCP server off, click **Disabled**.
DHCP Start IP	Use this field to specify the IP address at which the CGN3 begins assigning IP addresses to devices on the LAN (when DHCP is enabled).
DHCP End IP	Use this field to specify the IP address at which the CGN3 stops assigning IP addresses to devices on the LAN (when DHCP is enabled). NOTE: Devices requesting IP addresses once the DHCP pool is exhausted are not assigned an IP address.

Table 6:   The Setup Wizard: LAN Settings Screen (continued)
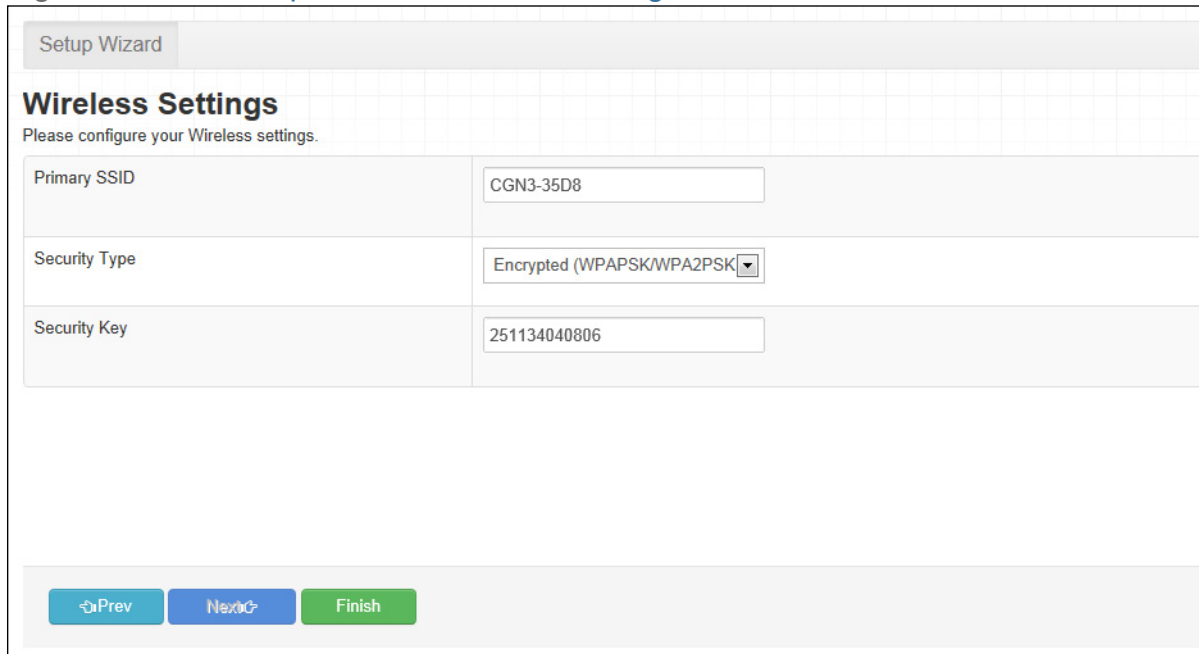
Prev	Click this to return to the previous screen.
Next	Click this to continue to the next screen.

2.4 Wireless Settings

Use this screen to configure the CGN3's wireless network.

Click **Next** in the **Setup Wizard: LAN Settings** screen. The following screen displays.

Figure 9:   The Setup Wizard: Wireless Settings Screen

The following table describes the labels in this screen.

Table 7:   The Setup Wizard: Wireless Settings Screen

Primary SSID	Enter the name that you want to use for your CGN3's wireless network. This is the name that identifies your network, and to which wireless clients connect.
Security Type	Use this field to apply security encryption to your wireless network. ▸ Select **Open** to use no wireless security. Anyone can join the network. ▸ Select **Encrypted** to require people who want to access your wireless network to use a password. Then, enter the password you want to use in the **Security Key** field that displays.
Prev	Click this to return to the previous screen.
Finish	Click this to continue to the next screen.

2.5 Summary

Use this screen to save your changes to the setup wizard's configuration.

Click **Finish** in the **Setup Wizard: Wireless Settings** screen. The following screen displays.

Figure 10: The Setup Wizard: Summary Screen

If you are happy with the settings, click **Save changes**. The following confirmation message displays.

Figure 11: The Setup Wizard: Summary Screen

NOTE: If you changed the **Private LAN IP Address**, **Primary SSID Name** or **Wireless Secure Key**, make sure you keep a note of the new details.

Alternatively, click **Go Back** to make further changes to the wizard's fields.

3

Status

This chapter describes the screens that display when you click **Status** in the toolbar. It contains the following sections:

3.1 Status Overview

This section describes some of the concepts related to the **Status** screens.

3.1.1 DOCSIS

The Data Over Cable Service Interface Specification (DOCSIS) is a telecommunications standard that defines the provision of data services) Internet access) over a traditional cable TV (CATV) network.

Your CGN3 supports DOCSIS version 3.0.

3.1.2 IP Addresses and Subnets

Every computer on the Internet must have a unique Internet Protocol (IP) address. The IP address works much like a street address, in that it identifies a specific location to which information is transmitted. No two computers on a network can have the same IP address.

3.1.2.1 IP Address Format

IP addresses consist of four octets (8-bit numerical values) and are usually represented in decimal notation, for example **192.168.1.1**. In decimal notation, this means that each octet has a minimum value of 0 and a maximum value of 255.

An IP address carries two basic pieces of information: the "network number" (the address of the network as a whole, analogous to a street name) and the "host ID" (analogous to a house number) which identifies the specific computer (or other network device).

3.1.2.2 IP Address Assignment

IP addresses can come from three places:

‣ The Internet Assigned Numbers Agency (IANA)

‣ Your Internet Service Provider

‣ You (or your network devices)

IANA is responsible for IP address allocation on a global scale, and your ISP assigns IP addresses to its customers. You should never attempt to define your own IP addresses on a public network, but you are free to do so on a private network.

In the case of the CGN3:

‣ The public network (Wide Area Network or WAN) is the link between the cable connector and your Internet Service Provider. Your CGN3's IP address on this network is assigned by your service provider.

▸ The private network (in routing mode - see Routing Mode on page 38) is your Local Area Network (LAN) and Wireless Local Area Network (WLAN), if enabled. You are free to assign IP addresses to computers on the LAN and WLAN manually, or to allow the CGN3 to assign them automatically via DHCP (Dynamic Host Configuration Protocol). IANA has reserved the following blocks of IP addresses to be used for private networks only:

Table 8: Private IP Address Ranges

FROM...	...TO
10.0.0.0	10.255.255.255
172.16.0.0	172.31.255.255
192.168.0.0	192.168.255.255

If you assign addresses manually, they must be within the CGN3's LAN subnet.

3.1.2.3 Subnets

A subnet (short for sub-network) is, as the name suggests, a separate section of a network, distinct from the main network of which it is a part. A subnet may contain all of the computers at one corporate local office, for example, while the main network includes several offices.

In order to define the extent of a subnet, and to differentiate it from the main network, a subnet mask is used. This "masks" the part of the IP address that refers to the main network, leaving the part of the IP address that refers to the sub-network.

Each subnet mask has 32 bits (binary digits), as does each IP address:

▸ A binary value of **1** in the subnet mask indicates that the corresponding bit in the IP address is part of the main network.

▸ A binary value of **0** in the subnet mask indicates that the corresponding bit in the IP address is part of the sub-network.

For example, the following table shows the IP address of a computer (**192.168.1.1**) expressed in decimal and binary (each cell in the table indicates one octet):

Table 9: IP Address: Decimal and Binary

192	168	0	1
11000000	10101000	00000000	00000001

The following table shows a subnet mask that "masks" the first twenty-four bits of the IP address, in both its decimal and binary notation.

Table 10: Subnet Mask: Decimal and Binary

255	255	255	0
11111111	11111111	11111111	00000000

This shows that in this subnet, the first three octets (**192.168.1**, in the example IP address) define the main network, and the final octet (**1**, in the example IP address) defines the computer's address on the subnet.

The decimal and binary notations give us the two common ways to write a subnet mask:

▸ Decimal: the subnet mask is written in the same fashion as the IP address: **255.255.255.0**, for example.

▸ Binary: the subnet mask is indicated after the IP address (preceded by a forward slash), specifying the number of binary digits that it masks. The subnet mask **255.255.255.0** masks the first twenty-four bits of the IP address, so it would be written as follows: 192.168.1.1**/24**.

3.1.3 DHCP

The Dynamic Host Configuration Protocol, or DHCP, defines the process by which IP addresses can be assigned to computers and other networking devices automatically, from another device on the network. This device is known as a DHCP server, and provides addresses to all the DHCP client devices.

In order to receive an IP address via DHCP, a computer must first request one from the DHCP server (this is a broadcast request, meaning that it is sent out to the whole network, rather than just one IP address). The DHCP server hears the requests, and responds by assigning an IP address to the computer that requested it.

If a computer is not configured to request an IP address via DHCP, you must configure an IP address manually if you want to access other computers and devices on the network. See IP Address Setup on page 22 for more information.

By default, the CGN3 is a DHCP client on the WAN (the CATV connection). It broadcasts an IP address over the cable network, and receives one from the service provider. By default, the CGN3 is a DHCP server on the LAN; it provides IP addresses to computers on the LAN which request them.

3.1.4 DHCP Lease

"DHCP lease" refers to the length of time for which a DHCP server allows a DHCP client to use an IP address. Usually, a DHCP client will request a DHCP lease renewal before the lease time is up, and can continue to use the IP address for an additional period. However, if the client does not request a renewal, the DHCP server stops allowing the client to use the IP address.

This is done to prevent IP addresses from being used up by computers that no longer require them, since the pool of available IP addresses is finite.

3.1.5 MAC Addresses

Every network device possesses a Media Access Control (MAC) address. This is a unique alphanumeric code, given to the device at the factory, which in most cases cannot be changed (although some devices are capable of "MAC spoofing", where they impersonate another device's MAC address).

MAC addresses are the most reliable way of identifying network devices, since IP addresses tend to change over time (whether manually altered, or updated via DHCP).

Each MAC address displays as six groups of two hexadecimal digits separated by colons (or, occasionally, dashes) for example **00:AA:FF:1A:B5:74**.

NOTE: Each group of two hexadecimal digits is known as an "octet", since it represents eight bits.

Bear in mind that a MAC address does not precisely represent a computer on your network (or elsewhere), it represents a network device, which may be part of a computer (or other device). For example, if a single computer has an Ethernet card (to connect to your CGN3 via one of the **LAN** ports) and also has a wireless card (to connect to your CGN3 over the wireless interface) the MAC addresses of the two cards will be different. In the case of the CGN3, each internal module (cable modem module, Ethernet module, wireless module, etc.) possesses its own MAC address.

3.1.6 Routing Mode

When your CGN3 is in routing mode, it acts as a gateway for computers on the LAN to access the Internet. The service provider assigns an IP address to the CGN3 on the WAN, and all traffic for LAN computers is sent to that IP address. The CGN3 assigns private IP addresses to LAN computers (when DHCP is active), and transmits the relevant traffic to each private IP address.

NOTE: When DHCP is not active on the CGN3 in routing mode, each computer on the LAN must be assigned an IP address in the CGN3's subnet manually.

When the CGN3 is not in routing mode, the service provider assigns an IP address to each computer connected to the CGN3 directly. The CGN3 does not perform any routing operations, and traffic flows between the computers and the service provider.

Routing mode is not user-configurable; it is specified by the service provider in the CGN3's configuration file.

3.1.7 Configuration Files

The CGN3's configuration (or config) file is a document that the CGN3 obtains automatically over the Internet from the service provider's server, which specifies the settings that the CGN3 should use. It contains a variety of settings that are not present in the user-configurable Graphical User Interface (GUI) and can be specified only by the service provider.

3.1.8 Downstream and Upstream Transmissions

The terms "downstream" and "upstream" refer to data traffic flows, and indicate the direction in which the traffic is traveling. "Downstream" refers to traffic from the service provider to the CGN3, and "upstream" refers to traffic from the CGN3 to the service provider.

3.1.9 Cable Frequencies

Just like radio transmissions, data transmissions over the cable network must exist on different frequencies in order to avoid interference between signals.

The data traffic band is separate from the TV band, and each data channel is separate from other data channels.

3.1.10 Modulation

Transmissions over the cable network are based on a strong, high frequency periodic waveform known as the "carrier wave." This carrier wave is so called because it "carries" the data signal. The data signal itself is defined by variations in the carrier wave. The process of varying the carrier wave (in order to carry data signal information) is known as "modulation." The data signal is thus known as the "modulating signal."

Cable transmissions use a variety of methods to perform modulation (and the "decoding" of the received signal, or "demodulation"). The modulation methods defined in DOCSIS 3 are as follows:

- **QPSK**: Quadrature Phase-Shift Keying

- **QAM**: Quadrature Amplitude Modulation

- **QAM TCM**: Trellis modulated Quadrature Amplitude Modulation

In many cases, a number precedes the modulation type (for example **16 QAM**). This number refers to the complexity of modulation. The higher the number, the more data can be encoded in each symbol.

NOTE: In modulated signals, each distinct modulated character (for example, each audible tone produced by a modem for transmission over telephone lines) is known as a symbol.

Since more information can be represented by a single character, a higher number indicates a higher data transfer rate.

3.1.11 TDMA, FDMA and SCDMA

Time Division Multiple Access (TDMA), Frequency Division Multiple Access (FDMA) and Synchronous Code Division Multiple Access (SCDMA) are channel access methods that allow multiple users to share the same frequency channel.

- TDMA allows multiple users to share the same frequency channel by splitting transmissions by time. Each user is allocated a number of time slots, and transmits during those time slots.

- FDMA allows multiple users to share the same frequency channel by assigning a frequency band within the existing channel to each user.

▶ SCDMA allows multiple users to share the same frequency channel by assigning a unique orthogonal code to each user.

3.2 The System Information Screen

Use this screen to see general information about your CGN3's hardware, its software, and its connection to the Internet.

NOTE: Most of the information that displays in this screen is for troubleshooting purposes only. However, you may need to use the MAC Address information when setting up your network.

Click **Status** > **System Information**. The following screen displays.

Figure 12: The Status: System Information Screen

System information

This menu displays general information of the device

HW Version	0D
SW Version	4.1.4.1
Serial Number	251134040806
RF MAC	68:b6:fc:fe:35:d5
WAN IP	none
System Time	Thu Jan 1 01:56:43 1970

The following table describes the labels in this screen.

Table 11: The Status: System Information Screen

HW Version	This displays the version number of the CGN3's physical hardware.
SW Version	This displays the version number of the software that controls the CGN3.
Serial Number	This displays a number that uniquely identifies the device.
RF MAC	This displays the Media Access Control (MAC) address of the CGN3's RF module. This is the module that connects to the Internet through the **Cable** connection.

Table 11:   The Status: System Information Screen (continued)

WAN IP	This field displays the CGN3's IP address on the WAN (Wide Area Network) interface.
System Time	This displays the current date and time.

3.3 The DOCSIS Provisioning Screen

This screen displays the steps successfully taken to connect to the Internet over the **Cable** connection.

Use this screen for troubleshooting purposes to ensure that the CGN3 has successfully connected to the Internet; if an error has occurred you can identify the stage at which the failure occurred.

Click **Status** > **DOCSIS Provisioning**. The following screen displays.

Figure 13:   The Status: DOCSIS Provisioning Status Screen

DOCSIS Provisioning Status

This menu displays the connectivity status of the modem and its boot state

HW init	Process...
Find Downstream	
Ranging	
DHCP	
Time of Day	
Download CM Config File	
Registration	
EAE status	Disable
BPI status	AUTH:start, TEK:start

For each step:

▸ **Process** displays when the CGN3 is attempting to complete a connection step.

▸ **Success** displays when the CGN3 has completed a connection step.

3.4 The DOCSIS WAN Screen

Use this screen to discover information about:

▸ The nature of the upstream and downstream connection between the CGN3 and the device to which it is connected through the **CABLE** interface.

▸ IP details of the CGN3's WAN connection.

Click **Status** > **DOCSIS WAN**. The following screen displays.

Figure 14:   The Status: DOCSIS WAN Screen

DOCSIS WAN

This menu displays both upstream and downstream signal parameters

DOCSIS Overview

CM Configuration file name	[N/A]
Network Access	Process...
IP Address	0.0.0.0
Subnet Mask	
Gateway IP	
DHCP Lease Time	D: -- H: -- M: -- S: --

Downstream Overview

Port ID	Frequency (MHz)	Modulation	Signal strength (dBmV)	Signal noise ratio (dB)	Channel ID

Upstream Overview

Port ID	Frequency (MHz)	BandWidth	SCDMA mode	Signal strength (dBmV)	Channel ID

The following table describes the labels in this screen.

Table 12:   The Status: DOCSIS WAN Screen

DOCSIS Overview	
CM Configurator file name	This displays the name of the configuration file that the CGN3 downloaded from your service provider. This file provides the CGN3 with the service parameter data that it needs to perform its functions correctly.
Network Access	This displays whether or not your service provider allows you to access the Internet over the **CABLE** connection. ▸ **Permitted** displays if you can access the Internet. ▸ **Denied** displays if you cannot access the Internet.

Table 12: The Status: DOCSIS WAN Screen (continued)

IP Address	This displays the CGN3's WAN IP address. This IP address is automatically assigned to the CGN3
Subnet Mask	This displays the CGN3's WAN subnet mask.
Gateway IP	This displays the IP address of the device to which the CGN3 is connected over the **CABLE** interface.
DHCP Lease Time	This displays the time that elapses before your device's IP address lease expires, and a new IP address is assigned to it by the DHCP server.
Downstream Overview NOTE: The downstream signal is the signal transmitted to the CGN3.	
Port ID	This displays the ID number of the downstream connection's port.
Frequency (MHz)	This displays the actual frequency in Megahertz (MHz) of each downstream data channel to which the CGN3 is connected.
Modulation	This displays the type of modulation that each downstream channel uses.
Signal Strength (dBmV)	This displays the power of the signal of each downstream data channel to which the CGN3 is connected, in dBmV (decibels above/below 1 millivolt).
Signal Noise Ratio (dB)	This displays the Signal to Noise Ratio (SNR) of each downstream data channel to which the CGN3 is connected, in dB (decibels).
Channel ID	This displays the ID number of each channel on which the downstream signal is transmitted.
Upstream Overview NOTE: The upstream signal is the signal transmitted from the CGN3.	
Port ID	This displays the ID number of the upstream connection's port.
Frequency (MHz)	This displays the actual frequency in Megahertz (MHz) of each upstream data channel to which the CGN3 is connected.
Modulation	This displays the type of modulation that each upstream channel uses.

Table 12:   The Status: DOCSIS WAN Screen (continued)

Signal Strength (dBmV)	This displays the power of the signal of each upstream data channel to which the CGN3 is connected, in dBmV (decibels above/below 1 millivolt).
Signal Noise Ratio (dB)	This displays the Signal to Noise Ratio (SNR) of each upstream data channel to which the CGN3 is connected, in dB (decibels).
Channel ID	This displays the ID number of each channel on which the upstream signal is transmitted.

3.5 The DOCSIS Event Screen

Use this screen to discover information about:

▶ The nature of the upstream and downstream connection between the CGN3 and the device to which it is connected through the **CABLE** interface.

▶ IP details of the CGN3's WAN connection.

Click **Status** > **DOCSIS Event**. The following screen displays.

Figure 15:   The Status: DOCSIS Event Screen

Docsis Logs

The docsis event logs is shown here

No	Time	type	Priority	Event
1	08/01/13 15:25:39	90000000	warning	MIMO Event MIMO: Stored MIMO=1 post cfg file MIMO=-1;CM-MAC=78:8d:f7:1b:a1:ed;CMTS-MAC=00:0e:39:d1:bc:54;CM-QOS=1.1;CM-VER=3.0;
2	08/01/13 15:48:40	84000500	critical	SYNC Timing Synchronization failure - Loss of Sync;CM-MAC=78:8d:f7:1b:a1:ed;CMTS-MAC=00:0e:39:d1:bc:54;CM-QOS=1.1;CM-VER=3.0;
3	08/01/13 15:48:44	84020200	warning	Lost MDD Timeout;CM-MAC=78:8d:f7:1b:a1:ed;CMTS-MAC=00:0e:39:d1:bc:54;CM-QOS=1.1;CM-VER=3.0;
4	08/01/13 15:48:59	82000400	critical	Received Response to Broadcast Maintenance Request, But no Unicast Maintenance opportunities received - T4 time out;CM-MAC=78:8d:f7:1b:a1:ed;CMTS-MAC=00:0e:39:d1:bc:54;CM-QOS=1.1;CM-VER=3.0;
5	08/01/13 16:00:43	90000000	warning	MIMO Event MIMO: Stored MIMO=1 post cfg file MIMO=-1;CM-MAC=78:8d:f7:1b:a1:ed;CMTS-MAC=00:0e:39:d1:bc:54;CM-QOS=1.1;CM-VER=3.0;
6	08/01/13 16:04:25	82000200	critical	No Ranging Response received - T3 time-out;CM-MAC=78:8d:f7:1b:a1:ed;CMTS-MAC=00:22:90:df:2c:38;CM-QOS=1.1;CM-VER=3.0;
7	08/01/13 08:04:55	90000000	warning	MIMO Event MIMO: Stored MIMO=1 post cfg file MIMO=-1;CM-MAC=78:8d:f7:1b:a1:ed;CMTS-MAC=00:22:90:df:2c:38;CM-QOS=1.1;CM-VER=3.0;
8	08/01/13 09:00:26	84000500	critical	SYNC Timing Synchronization failure - Loss of Sync;CM-MAC=78:8d:f7:1b:a1:ed;CMTS-MAC=00:22:90:df:2c:38;CM-QOS=1.1;CM-VER=3.0;
9	08/01/13 09:00:31	84020200	warning	Lost MDD Timeout;CM-MAC=78:8d:f7:1b:a1:ed;CMTS-MAC=00:22:90:df:2c:38;CM-QOS=1.1;CM-VER=3.0;
10	08/01/13 09:01:19	82000400	critical	Received Response to Broadcast Maintenance Request, But no Unicast Maintenance opportunities received - T4 time out;CM-MAC=78:8d:f7:1b:a1:ed;CMTS-MAC=00:22:90:df:2c:38;CM-QOS=1.1;CM-VER=3.0;
11	08/01/13 11:06:02	90000000	warning	MIMO Event MIMO: Stored MIMO=1 post cfg file MIMO=-1;CM-MAC=78:8d:f7:1b:a1:ed;CMTS-MAC=00:22:90:df:2c:38;CM-QOS=1.1;CM-VER=3.0;
12	08/02/13 06:07:09	82000200	critical	No Ranging Response received - T3 time-out;CM-MAC=78:8d:f7:1b:a1:ed;CMTS-MAC=00:22:90:df:2c:38;CM-QOS=1.1;CM-VER=3.0;

The following table describes the labels in this screen.

Table 13: The Status: DOCSIS Event Screen

No.	This displays the arbitrary, incremental index number assigned to the DOCSIS event.
Time	This displays the time and date of the DOCSIS event.
Type	This displays the type of the DOCSIS event. NOTE: The definitions of the type of DOCSIS event follow DOCSIS's specification accordingly.
Priority	This displays the priority of the DOCSIS event. NOTE: The definitions of the priority of DOCSIS event follow DOCSIS's specification accordingly.
Event	This displays a description of the DOCSIS event.

3.6 The Wireless Screen

Use this screen to view information about the CGN3's wireless network.

Click **Status** > **Wireless**. The following screen displays.

Figure 16:   The Status: Wireless Status Screen

The following table describes the labels in this screen.

Table 14:   The Status: Wireless Status Screen

Basic Overview	
Wireless Status	This field displays **ON** when the CGN3's 2.4 GHz wireless network is active, and displays **OFF** when it is inactive.
Wireless Mode	This displays the type of 2.4 GHz wireless network that the CGN3 is using.
Wireless Channel	This displays the wireless channel on which the CGN3's 2.4 GHz wireless network is transmitting and receiving.
5GHz Wireless Status	
Wireless Status (5GHz)	This field displays **ON** when the CGN3's 5 GHz wireless network is active, and displays **OFF** when it is inactive.
Wireless Mode (5GHz)	This displays the type of 5 GHz wireless network that the CGN3 is using.
Wireless Channel (5GHz)	This displays the wireless channel on which the CGN3's 5 GHz wireless network is transmitting and receiving.
SSID Overview	

Table 14:   The Status: Wireless Status Screen (continued)

(SSID)	This displays the 2.4 GHz wireless network's Service Set Identifier. This is the name of the wireless network, to which wireless clients connect.
Broadcast SSID	This field displays **Enabled** when the 2.4 GHz wireless network's SSID is being broadcast, and displays **Disabled** when it is not.
WMM	This field displays **Enabled** when the 2.4 GHz wireless network, and displays **Disabled** when it is not.
Security Mode	This displays the type of security the CGN3's 2.4 GHz wireless network is currently using.
Security Key	This displays the password for the CGN3's 2.4 GHz wireless network.
SSID Overview (5GHz)	
(SSID)	This displays the 5 GHz wireless network's Service Set Identifier. This is the name of the wireless network, to which wireless clients connect.
Broadcast SSID	This field displays **Enabled** when the 5 GHz wireless network's SSID is being broadcast, and displays **Disabled** when it is not.
WMM	This field displays **Enabled** when the 5 GHz wireless network, and displays **Disabled** when it is not.
Security Mode	This displays the type of security the CGN3's 5 GHz wireless network is currently using.
Security Key	This displays the password for the CGN3's 5 GHz wireless network.

4

Basic

This chapter describes the screens that display when you click **Basic** in the toolbar. It contains the following sections:

4.1 Basic Overview

This section describes some of the concepts related to the **Basic** screens.

4.1.1 WAN and LAN

A Local Area Network (LAN) is a network of computers and other devices that usually occupies a small physical area (a single building, for example). Your CGN3's LAN consists of all the computers and other networking devices connected to the **LAN 1~4** ports. This is your private network (in routing mode - see Routing Mode on page 38).

The LAN is a separate network from the Wide Area Network (WAN). In the case of the CGN3, the WAN refers to all computers and other devices available on the cable connection.

Version 1.1, 08/2013. Copyright © 2013 Hitron Technologies

By default, computers on the WAN cannot identify individual computers on the LAN; they can see only the CGN3. The CGN3 handles routing to and from individual computers on the LAN.

4.1.2 LAN IP Addresses and Subnets

IP addresses on the LAN are controlled either by the CGN3's built-in DHCP server (see LAN Settings on page 28), or by you (when you manually assign IP addresses to your computers).

For more information about IP addresses and subnets in general, see LAN Settings on page 28.

4.1.3 DNS and Domain Suffix

A domain is a location on a network, for instance **example.com**. On the Internet, domain names are mapped to the IP addresses to which they should refer by the Domain Name System. This allows you to enter "www.example.com" into your browser and reach the correct place on the Internet even if the IP address of the website's server has changed.

Similarly, the CGN3 allows you to define a **Domain Suffix** to the LAN. When you enter the domain suffix into your browser, you can reach the CGN3 no matter what IP address it has on the LAN.

4.1.4 Debugging (Ping and Traceroute)

The CGN3 provides a couple of tools to allow you to perform network diagnostics on the LAN:

‣ Ping: this tool allows you to enter an IP address and see if a computer (or other network device) responds with that address on the network. The name comes from the pulse that submarine SONAR emits when scanning for underwater objects, since the process is rather similar. You can use this tool to see if an IP address is in use, or to discover if a device (whose IP address you know) is working properly.

‣ Traceroute: this tool allows you to see the route taken by data packets to get from the CGN3 to the destination you specify. You can use this tool to solve routing problems, or identify firewalls that may be blocking your access to a computer or service.

4.1.5 Port Forwarding

Port forwarding allows a computer on your LAN to receive specific communications from the WAN. Typically, this is used to allow certain applications (such as gaming) through the firewall, for a specific computer on the LAN. Port forwarding is also commonly used for running a public HTTP server from a private network.

You can set up a port forwarding rule for each application for which you want to open ports in the firewall. When the CGN3 receives incoming traffic from the WAN with a destination port that matches a port forwarding rule, it forwards the traffic to the LAN IP address and port number specified in the port forwarding rule.

NOTE: For information on the ports you need to open for a particular application, consult that application's documentation.

4.1.6 Port Triggering

Port triggering is a means of automating port forwarding. The CGN3 scans outgoing traffic (from the LAN to the WAN) to see if any of the traffic's destination ports match those specified in the port triggering rules you configure. If any of the ports match, the CGN3 automatically opens the incoming ports specified in the rule, in anticipation of incoming traffic.

4.1.7 DMZ

In networking, the De-Militarized Zone (DMZ) is a part of your LAN that has been isolated from the rest of the LAN, and opened up to the WAN. The term comes from the military designation for a piece of territory, usually located between two opposing forces, that is isolated from both and occupied by neither.

4.1.8 DNS

Domain Name Server (DNS) runs special-purpose networking software, features a public IP address, and contains a database of network names and addresses for other Internet hosts. DNS translates Internet domain and host names to IP addresses. DNS automatically converts the names we type in the Web browser address bar to the IP addresses of Web servers hosting those sites.

4.1.9 DDNS

Dynamic Domain Name Server (DDNS) is a service that maps Internet domain names to IP addresses. Unlike DNS that only works with static IP addresses, DDNS is designed to also support dynamic IP addresses, such as those assigned by a DHCP server. That makes DDNS a good fit for home networks, which often receive dynamic public IP addresses from their Internet provider that occasionally change.

4.2 The LAN Setup Screen

Use this screen to:

▸ View information about the CGN3's connection to the WAN

▸ Configure the CGN3's LAN IP address, subnet mask and domain suffix

▸ Configure the CGN3's internal DHCP server

▸ Define how the CGN3 assigns IP addresses on the LAN

▸ See information about the network devices connected to the CGN3 on the LAN.

Click **Basic** > **LAN Setup**. The following screen displays.

Figure 17: The Basic: LAN Setup Screen

The following table describes the labels in this screen.

Table 15: The Basic: LAN Setup Screen

Private LAN Setting	
Private LAN IP Address	Use this field to define the IP address of the CGN3 on the LAN.
Subnet Mask	Use this field to define the LAN subnet. Use dotted decimal notation (for example, **255.255.255.0**).
Domain Suffix	Use this field to define the domain that you can enter into a Web browser (instead of an IP address) to reach the CGN3 on the LAN. NOTE: It is suggested that you make a note of your device's **Domain Suffix** in case you ever need to access the CGN3's GUI without knowledge of its IP address.
LAN DHCP Status	Use this field to configure whether or not the CGN3's DHCP server is active. ▸ To turn the DHCP server on, click **Enabled**. ▸ To turn the DHCP server off, click **Disabled**.

Table 15: The Basic: LAN Setup Screen (continued)
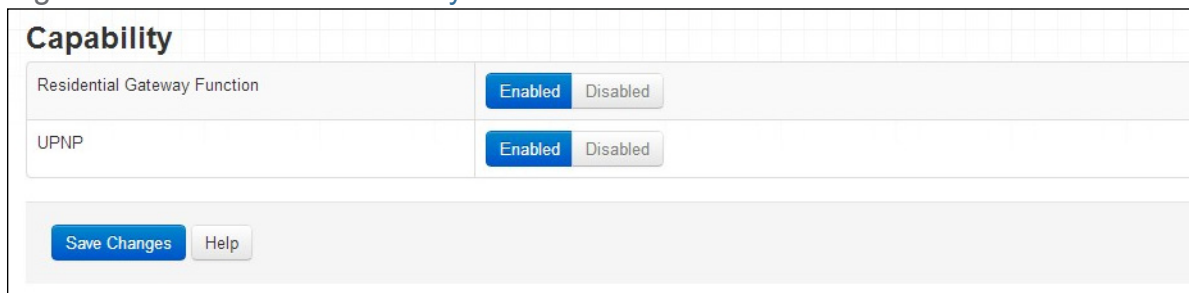
Lease Time	This displays the time that elapses before your device's IP address lease expires, and a new IP address is assigned to it by the DHCP server.
DHCP Start IP	Use this field to specify the IP address at which the CGN3 begins assigning IP addresses to devices on the LAN (when DHCP is enabled).
DHCP End IP	Use this field to specify the IP address at which the CGN3 stops assigning IP addresses to devices on the LAN (when DHCP is enabled). NOTE: Devices requesting IP addresses once the DHCP pool is exhausted are not assigned an IP address.
Save Changes	Click this to save your changes to the fields in this screen.
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.
WAN Info	
WAN Address	This field displays the CGN3's IP address on the WAN (Wide Area Network) interface.
Prefix Length	This displays the prefix length supplied by your ISP (typically 64).
DNS Server	This field displays the Domain Name Servers that the CGN3 uses to resolve domain names into IP addresses.
Connected Computers	
Host Name	This displays the name of each network device connected on the LAN.
IP Address	This displays the IP address of each network device connected on the LAN.
MAC Address	This displays the Media Access Control (MAC) address of each network device connected on the LAN.
Type	This displays whether the device's IP address was assigned by DHCP (**DHCP-IP**), or **self-assigned**.
Interface	This displays whether the device is connected on the LAN (**Ethernet**) or the WLAN (**Wireless(x)**, where **x** denotes the wireless mode; **b**, **g** or **n**).

4.3 The Gateway Function Screen

Use this screen to configure gateway function. You can turn port triggering on or off and configure new and existing port triggering rules.

Click **Basic** > **Gatewat Function**. The following screen displays.

Figure 18:   The Basic: Gateway Function Screen

The following table describes the labels in this screen.

Table 16:   The Basic: Gateway Function Screen

Residential Gateway Function	Use this field to turn gateway function on or off. ▶ Select **Enabled** to turn gateway function on. ▶ Select **Disabled** to turn gateway function off.
UPNP	Use this field to turn UPNP on or off. ▶ Select **Enabled** to turn UPNP on. ▶ Select **Disabled** to turn UPNP off.
Save Changes	Click this to save your changes to the fields in this screen.
Help	Click this to see information about the fields in this screen.

4.4 The Port Forwarding Screen

Use this screen to configure port triggering. You can turn port triggering on or off and configure new and existing port triggering rules.

Click **Basic** > **Port Forwarding**. The following screen displays.

Figure 19:   The Basic: Port Forwarding Screen

The following table describes the labels in this screen.

Table 17:   The Basic: Port Forwarding Screen

All Port Forwarding Rules	Use this field to turn port forwarding on or off.
	▸ Select **Enabled** to turn port forwarding on.
	▸ Select **Disabled** to turn port forwarding off.
Port Forwarding Rules	
Select	Select a port forwarding rule's radio button before clicking **Edit** or **Delete**.
#	This displays the arbitrary identification number assigned to the port forwarding rule.
Application Name	This displays the name you assigned to the rule when you created it.
Public	This field displays the incoming port range. These are the ports on which the CGN3 received traffic from the originating host on the WAN.
Private	This field displays the port range to which the CGN3 forwards traffic to the device on the LAN.
Protocol	This field displays the protocol or protocols to which this rule applies:
	▸ Transmission Control Protocol (**TCP**)
	▸ User Datagram Protocol (**UDP**)
	▸ Transmission Control Protocol and User Datagram Protocol (**TCP/UDP**)
	▸ Generic Routing Encapsulation (**GRE**)
	▸ Encapsulating Security Protocol (**ESP**)
Local IP Address	This displays the IP address of the computer on the LAN to which traffic conforming to the rule's conditions is forwarded.

Table 17: The Basic: Port Forwarding Screen (continued)

Remote IP Address	This displays the IP address range on the WAN from which traffic is forwarded (if configured).
Status	
Add	Click this to define a new port forwarding rule. Port forwarding must first be set to **Enabled**. See Adding or Editing a Port Forwarding Rule on page 56 for information on the screen that displays.
Edit	Select a port forwarding rule's radio button and click this to make changes to the rule. Port forwarding must first be set to **Enabled**. See Adding or Editing a Port Forwarding Rule on page 56 for information on the screen that displays.
Delete	Select a port forwarding rule's radio button and click this to remove the rule. The deleted rule's information cannot be retrieved.
Help	Click this to see information about the fields in this screen.
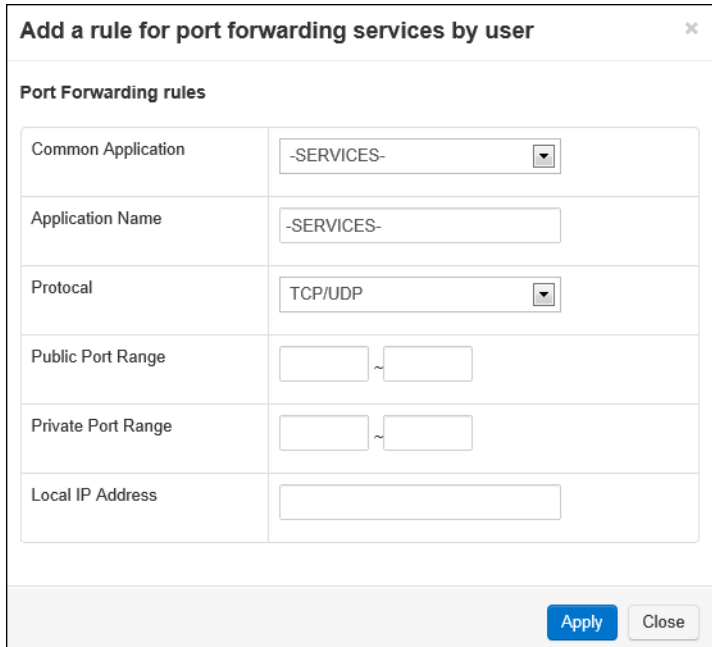
4.4.1 Adding or Editing a Port Forwarding Rule

‣ To add a new port forwarding rule, click **Add** in the **Basic** > **Port Forwarding** screen.

‣ To edit an existing port forwarding rule, select the rule's radio button in the **Basic** > **Forwarding** screen and click the **Edit** button.

NOTE: Ensure that **Enabled** is selected in the **Basic** > **Port Forwarding** screen in order to add or edit port forwarding rules.

The following screen displays.

Figure 20:   The Basic: Port Forwarding Add/Edit Screen

The following table describes the labels in this screen.

Table 18:   The Basic: Port Forwarding Add/Edit Screen

Common Application	Use this field to select the application for which you want to create a port forwarding rule, if desired.
Application Name	Enter a name for the application for which you want to create the rule. NOTE: This name is arbitrary, and does not affect functionality in any way.
Protocol	Use this field to specify whether the CGN3 should forward traffic via: ▸ Transmission Control Protocol (**TCP**) ▸ User Datagram Protocol (**UDP**) ▸ Transmission Control Protocol and User Datagram Protocol (**TCP/UDP**) ▸ Generic Routing Encapsulation (**GRE**) ▸ Encapsulating Security Protocol (**ESP**) NOTE: If in doubt, leave this field at its default (**TCP/ UDP**).

Table 18:   The Basic: Port Forwarding Add/Edit Screen
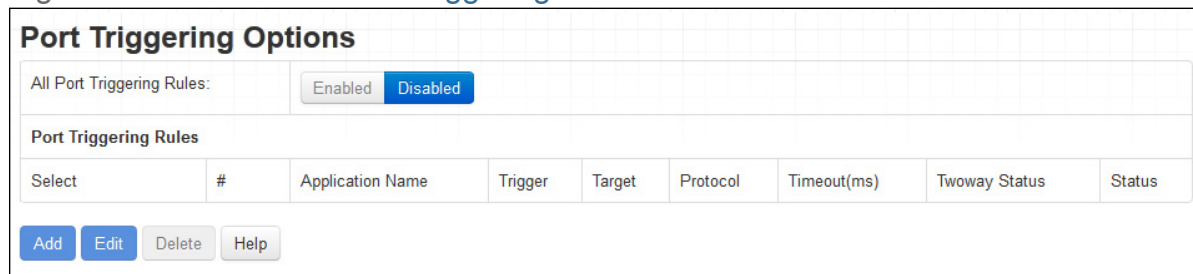
Public Port Range	Use these fields to specify the incoming port range. These are the ports on which the CGN3 receives traffic from the originating host on the WAN. Enter the start port number in the first field, and the end port number in the second field. To specify only a single port, enter its number in both fields.
Private Port Range	Use these fields to specify the ports to which the received traffic should be forwarded. Enter the start port number in the first field. The number of ports must match that specified in the **Public Port Range**, so the CGN3 completes the second field automatically.
Local IP Address	Use this field to enter the IP address of the computer on the LAN to which you want to forward the traffic.
Apply	Click this to save your changes to the fields in this screen.
Close	Click this to return to the **Port Forwarding** screen without saving your changes to the port forwarding rule.

4.5 The Port Triggering Screen

Use this screen to configure port triggering. You can turn port triggering on or off and configure new and existing port triggering rules.

Click **Basic** > **Port Triggering**. The following screen displays.

Figure 21:   The Basic: Port Triggering Screen

The following table describes the labels in this screen.

Table 19:   The Basic: Port Triggering Screen

All Port Triggering Rules	Use this field to turn port triggering on or off. ▸ Select **Enabled** to turn port triggering on. ▸ Select **Disabled** to turn port triggering off.
Port Triggering Rules	
Select	Select a port triggering rule's radio button before clicking **Edit** or **Delete**.
#	This displays the arbitrary identification number assigned to the port triggering rule.
Application Name	This displays the arbitrary name you assigned to the rule when you created it.
Trigger	This displays the range of outgoing ports. When the CGN3 detects activity (outgoing traffic) on these ports from computers on the LAN, it automatically opens the **Target** ports.
Target	This displays the range of triggered ports. These ports are opened automatically when the CGN3 detects activity on the **Trigger** ports from computers on the LAN.
Protocol	This displays the protocol of the port triggering rule (**TCP**, **UDP** or **Both**).
Timeout (ms)	This displays the time (in milliseconds) after the CGN3 opens the **Target** ports that it should close them.
Twoway Status	Usually a port triggering rule works for two IP addresses; when a rule is enabled, other IPs will also be allowed to use the rule as a trigger.
Status	Use this field to turn the rule **On** or **Off**.
Add	Click this to define a new port triggering rule. Port triggering must first be set to **Enabled**. See Adding or Editing a Port Triggering Rule on page 60 for information on the screen that displays.
Edit	Select a port triggering rule's radio button and click this to make changes to the rule. Port triggering must first be set to **Enabled**. See Adding or Editing a Port Triggering Rule on page 60 for information on the screen that displays.

Table 19:   The Basic: Port Triggering Screen (continued)

Delete	Select a port forwarding rule's radio button and click this to remove the rule. The deleted rule's information cannot be retrieved.
Help	Click this to see information about the fields in this screen.
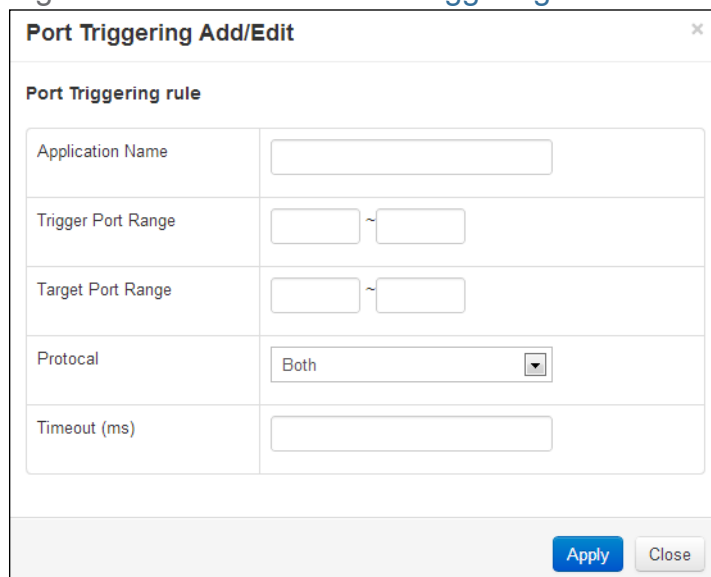
4.5.1 Adding or Editing a Port Triggering Rule

▸ To add a new port triggering rule, click **Add** in the **Basic** > **Port Triggering** screen.

▸ To edit an existing port triggering rule, select the rule's radio button in the **Basic** > **Port Triggering** screen and click the **Edit** button.

NOTE: Ensure that **Enabled** is selected in the **Basic** > **Port Triggering** screen in order to add or edit port triggering rules.

The following screen displays.

Figure 22:   The Basic: Port Triggering Add/Edit Screen

The following table describes the labels in this screen.

Table 20:   The Basic: Port Triggering Add/Edit Screen

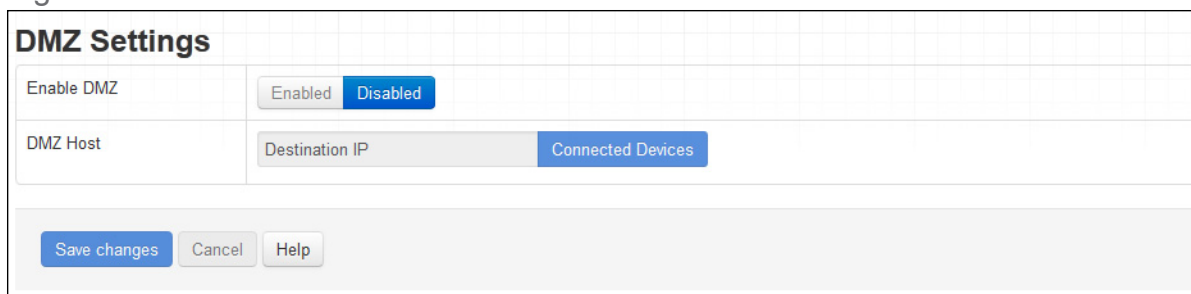| Application Name	Enter a name for the application for which you want to create the rule. NOTE: This name is arbitrary, and does not affect functionality in any way.
Trigger Port Range	Use these fields to specify the trigger ports. When the CGN3 detects activity on any of these ports originating from a computer on the LAN, it automatically opens the **Target** ports in expectation of incoming traffic. Enter the start port number in the first field, and the end port number in the second field. To specify only a single port, enter its number in both fields.
Target Port Range	Use these fields to specify the target ports. The CGN3 opens these ports in expectation of incoming traffic whenever it detects activity on any of the **Trigger** ports. The incoming traffic is forwarded to these ports on the computer connected to the LAN. Enter the start port number in the first field, and the end port number in the second field. To specify only a single port, enter its number in both fields.
Protocol	Use this field to specify whether the CGN3 should activate this trigger when it detects activity via: ▸ Transmission Control Protocol (**TCP**) ▸ User Datagram Protocol (**UDP**) ▸ Transmission Control Protocol and User Datagram Protocol (**Both**) NOTE: If in doubt, leave this field at its default (**Both**).
Timeout (ms)	Enter the time (in milliseconds) after the CGN3 opens the **Target** ports that it should close them.
Close	Click this to return to the **Firewall** > **Forwarding** screen without saving your changes to the port forwarding rule.
Apply	Click this to save your changes to the fields in this screen.

4.6 The DMZ Screen

Use this screen to configure your network's Demilitarized Zone (DMZ).

NOTE: Only one device can be on the DMZ at a time.

Click **Basic** > **DMZ**. The following screen displays.

Figure 23:   The Basic: DMZ Screen

The following table describes the labels in this screen.

Table 21:   The Basic: DMZ Screen

Enable DMZ	Use this field to turn the DMZ on or off.
	▶ Select **Enabled** to turn the DMZ on.
	▶ Select **Disabled** to turn the DMZ off. Computers that were previously in the DMZ are now on the LAN.
DMZ Host	Enter the IP address of the computer that you want to add to the DMZ.
Connected Devices	Click this to see a list of the computers currently connected to the CGN3 on the LAN.
Save Changes	Click this to save your changes to the fields in this screen.
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

4.7 The DNS Screen

Use this screen to configure your LAN DNS settings.

Click **Basic** > **DNS**. The following screen displays.

LAN DNS Settings
Configure your LAN DNS settings.

LAN DNS Obtain:	Auto Manual
DNS1	Dns IP
DNS2	Dns IP

Save Changes   Cancel   Help

The following table describes the labels in this screen.

Table 22:   The Basic: DNS Screen

LAN DNS Obtain	Use this field to obtain the DNS automatically or manually. ▶ Select **Auto** to obtain the DNS automatically. ▶ Select **Manual** to obtain the DNS manually.
DNS1	Enter the IP address of the computer that you want to add to the DNS manually.
DNS2	Enter the IP address of the computer that you want to add to the DNS manually.
Save Changes	Click this to save your changes to the fields in this screen.
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

4.8 The DDNS Screen

Use this screen to configure the Dynamic Domain Name Server (DDN).

Click **Basic** > **DDNS**. The following screen displays.

Figure 25: The Basic: DDNS Screen

DDNS Settings
Configure this page to enable the router work as a Dynamic DNS client.

Enable DDNS	ON **OFF**
Service Provider:	dyndns@dyndns.org
User Name:	
Password	
Host Name	

Save Changes   Cancel   Help

The following table describes the labels in this screen.

Table 23: The Basic: DDNS Screen

Enable DDNS	Use this field to turn the DDNS on or off. ‣ Select **On** to turn the DDNS on. ‣ Select **Off** to turn the DDNS off.
Service Provider	Use this field to select the service provider.
User Name	Enter the user name you registered.
Password	Enter the password you registered.
Host Name	Enter the host name you registered.
Save Changes	Click this to save your changes to the fields in this screen.
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

5
Wireless

This chapter describes the screens that display when you click **Wireless** in the toolbar. It contains the following sections:

5.1 Wireless Overview

This section describes some of the concepts related to the **Wireless** screens.

5.1.1 Wireless Networking Basics

Your CGN3's wireless network is part of the Local Area Network (LAN), known as the Wireless LAN (WLAN). The WLAN is a network of radio links between the CGN3 and the other computers and devices that connect to it.

5.1.2 Architecture

The wireless network consists of two types of device: access points (APs) and clients.

‣ The access point controls the network, providing a wireless connection to each client.

▶ The wireless clients connect to the access point in order to receive a wireless connection to the WAN and the wired LAN.

The CGN3 is the access point, and the computers you connect to the CGN3 are the wireless clients.

5.1.3 Wireless Standards

The way in which wireless devices communicate with one another is standardized by the Institute of Electrical and Electronics Engineers (IEEE). The IEEE standards pertaining to wireless LANs are identified by their 802.11 designation. There are a variety of WLAN standards, but the CGN3 supports the following (in order of adoption - old to new - and data transfer speeds - low to high):

▶ IEEE 802.11b

▶ IEEE 802.11g

▶ IEEE 802.11n

5.1.4 Service Sets and SSIDs

Each wireless network, including all the devices that comprise it, is known as a Service Set.

NOTE: Depending on its capabilities and configuration, a single wireless access point may control multiple Service Sets; this is often done to provide different service or security levels to different clients.

Each Service Set is identified by a Service Set IDentifier (SSID). This is the name of the network. Wireless clients must know the SSID in order to be able to connect to the AP. You can configure the CGN3 to broadcast the SSID (in which case, any client who scans the airwaves can discover the SSID), or to "hide" the SSID (in which case it is not broadcast, and only users who already know the SSID can connect).

5.1.5 Wireless Security

Radio is inherently an insecure medium, since it can be intercepted by anybody in the coverage area with a radio receiver. Therefore, a variety of techniques exist to control authentication (identifying who should be allowed to join the network) and encryption (signal scrambling so that only authenticated users can decode the transmitted data). The sophistication of each security method varies, as does its effectiveness. The CGN3 supports the following wireless security protocols (in order of effectiveness):

▶ **WEP** (the Wired Equivalency Protocol): this protocol uses a series of "keys" or data strings to authenticate the wireless client with the AP, and to encrypt data sent over the wireless link. WEP is a deprecated protocol, and should only be used when it is the only security standard supported by the wireless clients. WEP provides only a nominal level of security, since widely-available software exists that can break it in a matter of minutes.

▶ **WPA-PSK** (WiFi Protected Access - Pre-Shared Key): WPA was created to solve the inadequacies of WEP. There are two types of WPA: the "enterprise" version (known simply as WPA) requires the use of a central authentication database server, whereas the "personal" version (supported by the CGN3) allows users to authenticate using a "pre-shared key" or password instead. While WPA provides good security, it is still vulnerable to "brute force" password-guessing attempts (in which an attacker simply barrages the AP with join requests using different passwords), so for optimal security it is advised that you use a random password of thirteen characters or more, containing no "dictionary" words.

▶ **WPA2-PSK**: WPA2 is an improvement on WPA. The primary difference is that WPA uses the Temporal Key Integrity Protocol (TKIP) encryption standard (which has been shown to have certain possible weaknesses), whereas WPA2 uses the stronger Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP), which has received the US government's seal of approval for communications up to the Top Secret security level. Since WPA2-PSK uses the same pre-shared key mechanism as WPA-PSK, the same caveat against using insecure or simple passwords applies.

5.1.5.1 WPS

WiFi-Protected Setup (WPS) is a standardized method of allowing wireless devices to quickly and easily join wireless networks, while maintaining a good level of security. The CGN3 provides two methods of WPS authentication:

▶ **Push-Button Configuration (PBC)**: when the user presses the **PBC** button on the AP (either a physical button, or a virtual button in the GUI), any user of a wireless client that supports WPS can press the corresponding **PBC** button on the client within two minutes to join the network.

▶ **Personal Identification Number (PIN) Configuration**: all WPS-capable devices possess a PIN (usually to be found printed on a sticker on the device's housing). When you configure another device to use the same PIN, the two devices authenticate with one another.

Once authenticated, devices that have joined a network via WPS use the WPA2 security standard.

5.1.6 WMM

WiFi MultiMedia (WMM) is a Quality of Service (QoS) enhancement that allows prioritization of certain types of data over the wireless network. WMM provides four data type classifications (in priority order; highest to lowest):

▶ Voice

▶ Video

▶ Best effort

▶ Background

If you wish to improve the performance of voice and video (at the expense of other, less time-sensitive applications such as Internet browsing and FTP transfers), you can enable WMM. You can also edit the WMM QoS parameters, but are disadvised to do so unless you have an extremely good reason to make the changes.

5.1.7 Guest Networks

Your CGN3 supports the creation of a wireless guest network. A guest network enables you to allow temporary visitors to access your wireless Internet connection without revealing your primary network password(s). Computers connected to the guest network can access the Internet connection only, and have no access to other computers or devices on the wireless or wired network.

5.2 Basic Settings Screen

Use this screen to configure your CGN3's basic 2.4GHz and 5GHz wireless settings. You can turn the wireless modules on or off, select the wireless mode and channel, and configure the wireless networks' SSID settings.

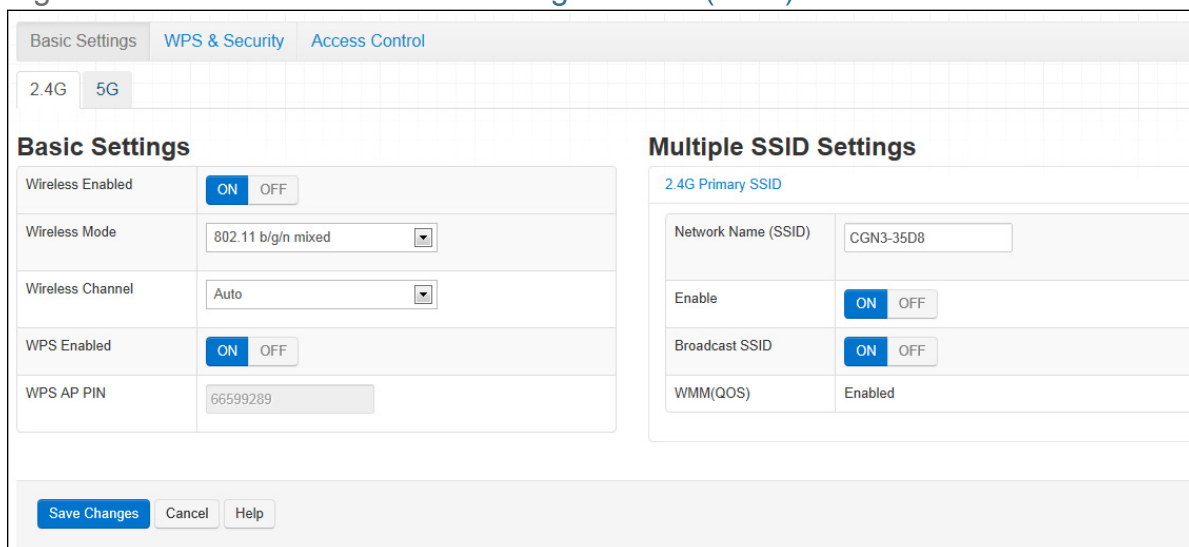The CGN3 has separate 2.4GHz and 5GHz wireless networks:

▸ To configure the CGN3's 2.4GHz wireless network, click **Wireless** > **Basic Settings**, then click the **2.4G** tab. See 2.4G Settings on page 70 for information on the screen that displays.

▸ To configure the CGN3's 5GHz wireless network, click **Wireless** > **Basic Settings**, then click the **5G** tab. See 5G Settings on page 72 for information on the screen that displays.

5.2.1 2.4G Settings

Use this screen to configure the CGN3's 2.4GHz wireless network.

Click **Wireless** > **Basic Settings**, then click the **2.4G** tab. The following screen displays.

Figure 26:   The Wireless: Basic Settings Screen (2.4G)

The following table describes the labels in this screen.

Table 24:   The Wireless: Basic Settings Screen (2.4G)

Basic Settings	
Wireless Enabled	Use this field to turn the 2.4GHz wireless network on or off. ▸ Select **ON** to enable the wireless network. ▸ Select **OFF** to disable the wireless network.
Wireless Mode	Select the type of 2.4GHz wireless network that you want to use: ▸ **802.11 B/G Mixed**: use IEEE 802.11b and 802.11n ▸ **802.11 11N Only**: use IEEE 802.11n ▸ **802.11 B/G/N Mixed**: use IEEE 802.11b, 802.11g and 802.11n ▸ **802.11 G/N Mixed**: use IEEE 802.11g and 802.11n NOTE: Only wireless clients that support the network protocol you select can connect to the wireless network. If in doubt, use **11B/G/N** (default).
Wireless Channel	Select the 2.4GHz wireless channel that you want to use, or select **Auto** to have the CGN3 select the optimum channel to use. NOTE: Use the **Auto** setting unless you have a specific reason to do otherwise.
WPS Enabled	Use this field to turn Wifi Protected Setup (WPS) on or off on the 2.4GHz network. ▸ Select **ON** to enable WPS. ▸ Deselect **OFF** to disable WPS.
WPS AP Pin	This field displays the Wifi Protected Setup (WPS) access point key for the 2.4GHz network.
Multiple SSID Settings	
NOTE: The CGN3 supports up to 3 SSIDs. If your service provider enabled multiple SSIDs, you will see their details here.	
Primary SSID	Click this to view settings for the main 2.4GHz SSID.

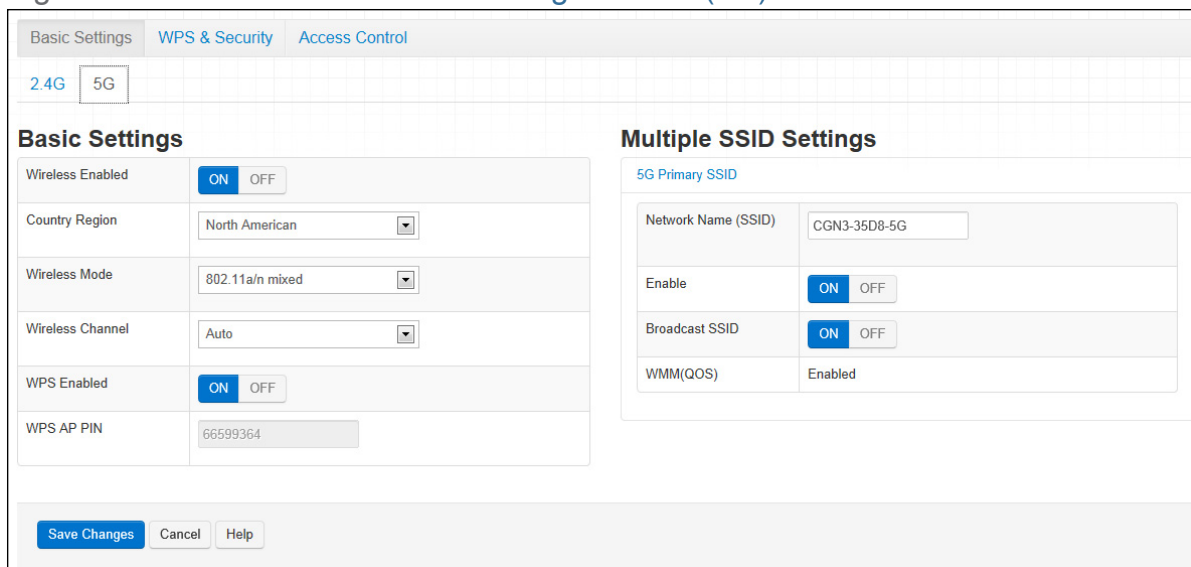Table 24: The Wireless: Basic Settings Screen (2.4G) (continued)

Network Name (SSID)	Enter the name that you want to use for this SSID. This is the name that identifies your network, and to which wireless clients connect. NOTE: It is suggested that you change the SSID from its default, for security reasons.
Enable	Use this field to enable or disable the SSID. ▸ Select **ON** to enable the SSID. ▸ Deselect **OFF** to disable the SSID.
Broadcast SSID	Use this field to make this SSID visible or invisible to other wireless devices. ▸ Select **ON** if you want your network name (SSID) to be public. Anyone with a wireless device in the coverage area can discover the SSID, and attempt to connect to the network. ▸ Select **OFF** if you do not want the CGN3 to broadcast the network name (SSID) to all wireless devices in the coverage area. Anyone who wants to connect to the network must know the SSID.
WMM (QoS)	Use this field to apply Wifi MultiMedia (WMM) Quality of Service (QoS) settings to this SSID. ▸ Select **ON** to enable WMM QoS on this SSID. ▸ Select **OFF** to disable WMM QoS on this SSID.
Save Changes	Click this to save your changes to the fields in this screen.
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

5.2.2 5G Settings

Use this screen to configure the CGN3's 5GHz wireless network.

Click **Wireless** > **Basic Settings**, then click the **5G** tab. The following screen displays.

Figure 27:   The Wireless: Basic Settings Screen (5G)

The following table describes the labels in this screen.

Table 25:   The Wireless: Basic Settings Screen (5G)

Basic Settings	
Wireless Enabled	Use this field to turn the 5GHz wireless network on or off. ▶ Select **ON** to enable the wireless network. ▶ Select **OFF** to disable the wireless network.
Country Region	Use this field to select the part of the world in which the CGN3 is operating.
Wireless Mode	Select the type of 5GHz wireless network that you want to use: ▶ **802.11n 5g**: use IEEE 802.11n 5GHz. NOTE: At the time of writing IEEE 802.11n is the only 5GHz network type available. NOTE: Only wireless clients that support the network protocol you select can connect to the wireless network.

Table 25: The Wireless: Basic Settings Screen (5G) (continued)

Wireless Channel	Select the 5GHz wireless channel that you want to use, or select **Auto** to have the CGN3 select the optimum channel to use. NOTE: Use the **Auto** setting unless you have a specific reason to do otherwise.
WPS Enabled	Use this field to turn Wifi Protected Setup (WPS) on or off on the 5GHz network. ▸ Select **ON** to enable WPS. ▸ Deselect **OFF** to disable WPS.
WPS AP Pin	This field displays the Wifi Protected Setup (WPS) access point key for the 5GHz network.
Multiple SSID Settings	
Primary SSID	Click this to view settings for the main 5GHz SSID.
Network Name (SSID)	Enter the name that you want to use for this SSID. This is the name that identifies your network, and to which wireless clients connect. NOTE: It is suggested that you change the SSID from its default, for security reasons.
Enable	Use this field to enable or disable the SSID. ▸ Select **ON** to enable the SSID. ▸ Deselect **OFF** to disable the SSID.
Broadcast SSID	Use this field to make this SSID visible or invisible to other wireless devices. ▸ Select **ON** if you want your network name (SSID) to be public. Anyone with a wireless device in the coverage area can discover the SSID, and attempt to connect to the network. ▸ Select **OFF** if you do not want the CGN3 to broadcast the network name (SSID) to all wireless devices in the coverage area. Anyone who wants to connect to the network must know the SSID.

Table 25:   The Wireless: Basic Settings Screen (5G) (continued)

WMM (QoS)	Use this field to apply Wifi MultiMedia (WMM) Quality of Service (QoS) settings to this SSID. ▸ Select **ON** to enable WMM QoS on this SSID. ▸ Select **OFF** to disable WMM QoS on this SSID.
Save Changes	Click this to save your changes to the fields in this screen.
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.
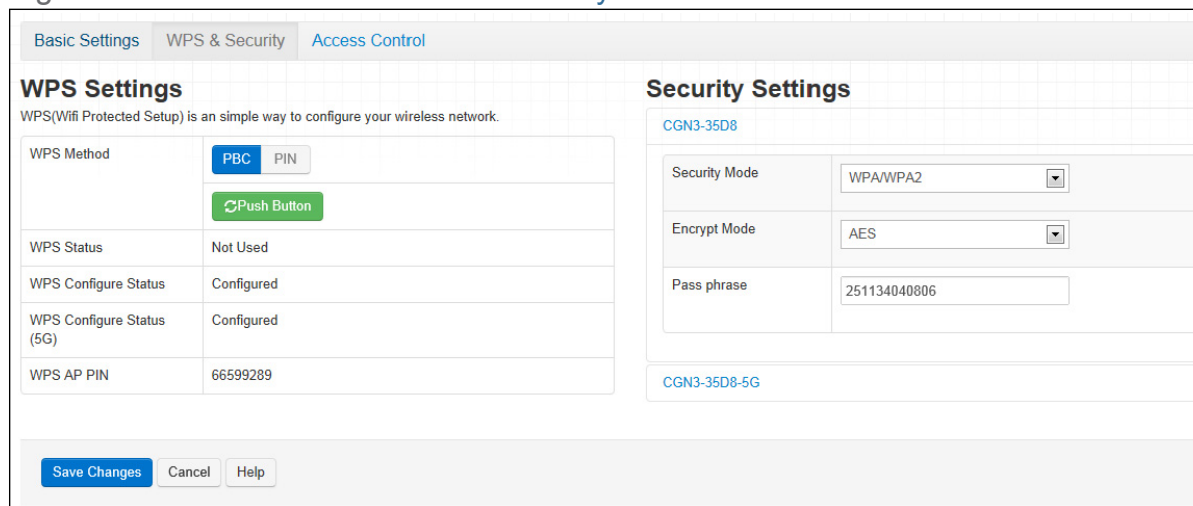
5.3 WPS & Security Screen

Use this screen to configure your CGN3's 2.4GHz and 5GHz wireless networks' authentication and encryption, and manage Wifi Protected Setup (WPS).

NOTE: It is strongly recommended that you set up security on your network; otherwise, anyone in the radio coverage area can access your network.

Click **Wireless** > **WPS & Security**. The following screen displays.

Figure 28:   The Wireless: WPS & Security Screen

The following table describes the labels in this screen.

Table 26:   The Wireless: WPS & Security Screen

WPS Settings	
WPS Method	Use these buttons to run Wifi Protected Setup (WPS): ▶ Click the **PBC** button and then **Push Button** to begin the Push-Button Configuration process. You must then press the PBC button on your client wireless devices within two minutes in order to register them on your wireless network. ▶ Click the **PIN** button to begin the PIN configuration process. In the screen that displays, enter the WPS PIN that you want to use for the CGN3, or the WPS PIN of the client device you want to add to the network.
WPS Status	This displays whether or not the CGN3 is using Wifi Protected Setup.
WPS Configure Status	This displays the Wifi Protected Setup configuration for the 2.4GHz wireless network.
WPS Configure Status (5G)	This displays the Wifi Protected Setup configuration for the 2.4GHz wireless network.
WPS AP PIN	This displays the Wifi Protected Setup Access Point password. When you use the WPS PIN method, this is the password you should enter in the other devices on the network.
Security Settings	
(SSID)	Your CGN3 has multiple SSIDs. Click the SSID you wish to configure to see its security fields.

Table 26: The Wireless: WPS & Security Screen (continued)

Security Mode	Select the type of security that you want to use.
	▸ Select **Open** to use no security. Anyone in the coverage area can enter your network.
	▸ Select **WEP** to use the Wired Equivalent Privacy security protocol.
	▸ Select **WPA** to use the WiFi Protected Access (Personal) security protocol.
	▸ Select **WPA2** to use the WiFi Protected Access 2 (Personal) security protocol.
	▸ Select **WPA/WPA2** to use both the WPA and the WPA2 security protocols; clients that support WPA2 connect using this protocol, whereas those that support only WPA connect using this protocol.
	NOTE: Due to inherent security vulnerabilities, it is suggested that you use **WEP** only if it is the only security protocol your wireless clients support. Under almost all circumstances, you should use one of the **WPA** options.
Encrypt Mode	Select the type of encryption you want to use. The options that display depend on the **Security Mode** you selected.
	WEP:
	▸ Select **WEP64** to use a ten-digit security key.
	▸ Select **WEP128** to use a twenty-six-digit security key.
	WPA, **WPA2** and **WPA/WPA2**:
	▸ Select **TKIP** to use the Temporal Key Integrity Protocol.
	▸ Select **AES** to use the Advanced Encryption Standard.
	▸ Select **TKIP/AES** to allow clients using either encryption type to connect to the CGN3.

Table 26:   The Wireless: WPS & Security Screen (continued)

Pass Phrase	Enter the security key or password that you want to use for your wireless network. You will need to enter this key into your wireless clients in order to allow them to connect to the network.
Save Changes	Click this to save your changes to the fields in this screen.
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

5.4 Access Control Screen
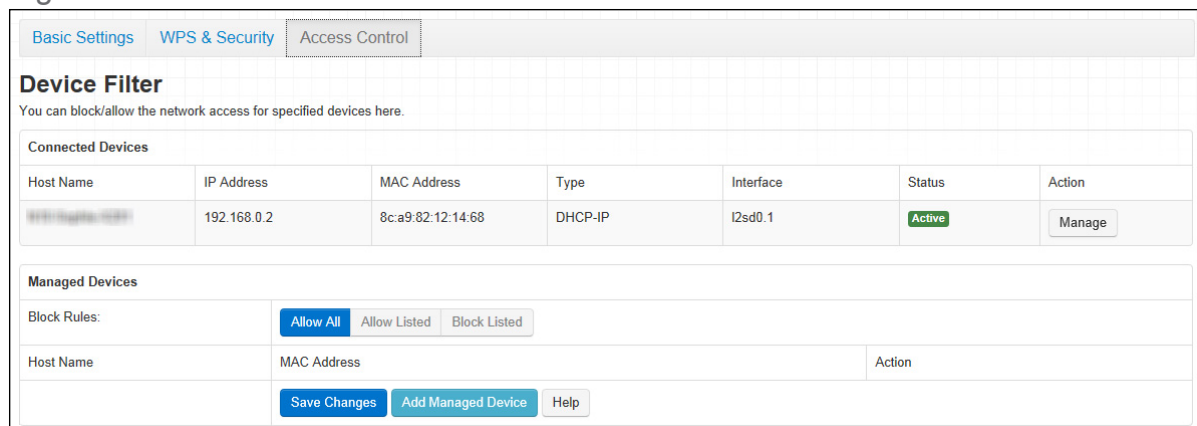
Use this screen to configure Media Access Control (MAC) address filtering on the wireless network.

NOTE: To configure MAC address filtering on the wired LAN, see The Device Filter Screen on page 97.

You can set the CGN3 to allow only certain devices to access the CGN3 and the network wirelessly, or to deny certain devices access.

Click **Wireless** > **Access Control**. The following screen displays.

Figure 29:   The Wireless: Wireless Access Control Screen

The following table describes the labels in this screen.

Table 27:   The Wireless: Access Control Screen

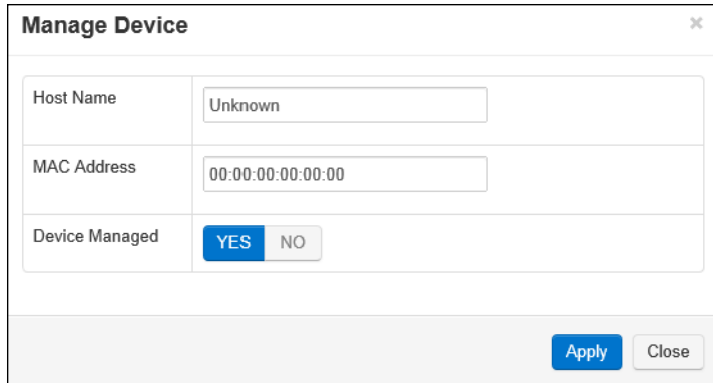| Connected Devices	
Host Name	This displays the name of each network device that has connected to the CGN3 on the wireless network.
IP Address	This displays the IP address of each network device that has connected to the CGN3 on the wireless network.
MAC Address	This displays the MAC address of each network device that has connected to the CGN3 on the wireless network.
Type	This displays whether the device's IP address was assigned by DHCP (**DHCP-IP**), or **self-assigned**.
Interface	This displays the name of the interface on which the relevant device is connected.
Action	Click **Manage** to make changes to the device's filtering status; see Adding or Editing a Wireless Device Filter Rule on page 79 for information on the screen that displays.
Managed Devices	
Block Rules	Use these buttons to control the action to be taken for the devices listed: ▸ Select **Allow All** to ignore the **Devices** list and let all devices connect wirelessly to the CGN3. ▸ Select **Allow** to permit only devices you added to the **Devices** list to access the CGN3 and the network wirelessly. All other devices are denied access. ▸ Select **Deny** to permit all devices except those you added to the **Devices** list to access the CGN3 and the network wirelessly. The specified devices are denied access.

5.4.1 Adding or Editing a Wireless Device Filter Rule

To add or edit an wireless device filter, locate the device in the **Wireless** > **Access Control** screen and click its **Manage** button.

The following screen displays.

Figure 30:   The Wireless: Access Control Add/Edit Screen

The following table describes the labels in this screen.

Table 28:   The Wireless: Access Control Add/Edit Screen

Host Name	This field displays the name of the wireless device.
MAC Address	This field displays the device's MAC (Media Access Control) address.
Device Managed	Use this field to define whether the device should have its access privileges filtered or not. ▸ Click **Yes** to filter the device's access privileges. ▸ Click **No** not to filter the device's access privileges.
Apply	Click this to save your changes to the fields in this screen.
Close	Click this to return to the **Wireless Access Control** screen without saving your changes to the rule.

6

Admin

This chapter describes the screens that display when you click **Admin** in the toolbar. It contains the following sections:

6.1 Admin Overview

This section describes some of the concepts related to the **Admin** screens.

6.1.1 Debugging (Ping and Traceroute)

The CGN3 provides a couple of tools to allow you to perform network diagnostics on the LAN:

▸ Ping: this tool allows you to enter an IP address and see if a computer (or other network device) responds with that address on the network. The name comes from the pulse that submarine SONAR emits when scanning for underwater objects, since the process is rather similar. You can use this tool to see if an IP address is in use, or to discover if a device (whose IP address you know) is working properly.

▸ Traceroute: this tool allows you to see the route taken by data packets to get from the CGN3 to the destination you specify. You can use this tool to solve routing problems, or identify firewalls that may be blocking your access to a computer or service.
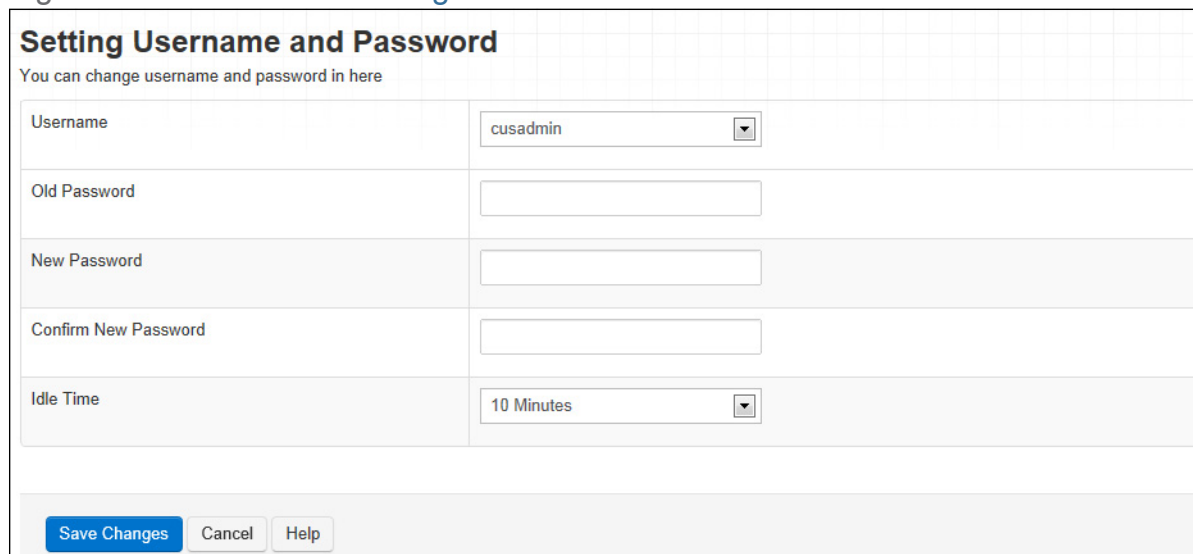
6.2 Management Screen

Use this screen to make changes to the CGN3's login credentials (username and password).

NOTE: If you forget your password, you will need to reset the CGN3 to its factory defaults.

Click **Admin** > **Management**. The following screen displays.

Figure 31:   The Admin: Management Screen

The following table describes the labels in this screen.

Table 29:   The Admin: Management Screen

Username	If your CGN3 supports multiple user accounts, select the account you want to modify from the list.
Old Password	Enter the password with which you currently log into the CGN3 for this account.
New Password	Enter and re-enter the password you want to use to log into the CGN3 for this account.
Confirm New Password	

Table 29:   The Admin: Management Screen (continued)

Idle Time	Use this to set your CGN3's idle time
Save Changes	Click this to save your changes to the fields in this screen.
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

6.3 Diagnostics Screen

Use this screen to perform ping and traceroute tests on IP addresses or URLs.

Click **Admin** > **Diagnostics**. The following screen displays.

Figure 32:   The Admin: Diagnostics Screen

The following table describes the labels in this screen.
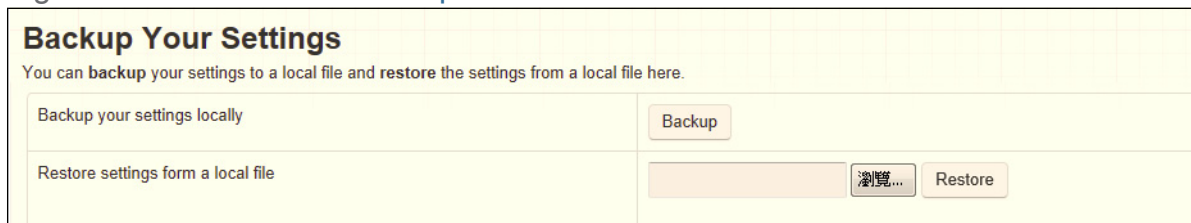
Table 30:   The Admin: Diagnostics Screen

Destination (IP or Domain)	Enter the IP address or URL that you want to test.
Ping	Select the type of test that you want to run on the **Destination** that you specified.
Traceroute	
Result	This field displays a report of the test most recently performed.
Apply	Click this to save your changes to the fields in this screen.
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

6.4 Backup Screen

Use this screen to back up your CGN3's settings to your computer, to load settings from a backup you created earlier, to reboot your CGN3, or to return it to its factory default settings.

Click **Admin** > **Backup**. The following screen displays.

Figure 33:   The Admin: Backup Screen

The following table describes the labels in this screen.

Table 31:   The Admin: Backup Screen

Back Up Your Settings Locally	Click this to create a backup of all your CGN3's settings on your computer.
Restore Settings From a Local File	Use these fields to return your CGN3's settings to those specified in a backup that you created earlier. Click **Browse** to select a backup, then click **Restore** to return your CGN3's settings to those specified in the backup.

6.5 Time Setting Screen

Use this screen to back up your CGN3's settings to your computer, to load settings from a backup you created earlier, to reboot your CGN3, or to return it to its factory default settings.

Click **Admin** > **Time Setting Screen**. The following screen displays.

Figure 34: The Admin: Time Setting Screen

The following table describes the labels in this screen.

Table 32: The Admin: Time Setting Screen

ToD Function	Use this field to select whether the ToD Function be active or not.
	▸ Select **Enabled** to activate the ToD Function.
	▸ Select **Disabled** to deactivate the ToD Function.
	NOTE: Time of Day (TOD) is mostly used in cable networks for cable modems to be able to get time to put a timestamp on the log entries in the cable modem itself for trouble shooting.
Time Zone	Use this fields to select the time zome when the ToD Function enabled .

Table 32:   The Admin: Time Setting Screen (continued)

SNTP Function	Use this field to select whether the SNTP Function be active or not. ▸ Select **Enabled** to activate the SNTP Function. ▸ Select **Disabled** to deactivate the SNTP Function. NOTE: The Simple Network Time Protocol (SNTP) is an adaptation of the Network Time Protocol (NTP) used to synchronize computer clocks in the Internet.
Time Zone	Use this fields to select the time zome when the SNTP Function enabled .
Assign SNTP Server	Enter the SNTP Server you want to assign manually.
Daylight Function	Use this field to select whether the Daylight Function be active or not. ▸ Select **Enabled** to activate the Daylight Function. ▸ Select **Disabled** to deactivate the Daylight Function.
Daylight Time	Enter the duration of the daylight time.

6.6 Device Reset Screen

Use this screen to reboot your CGN3, or to return it to its factory default settings.

Click **Admin** > **Device Reset**. The following screen displays.

Figure 35:   The Admin: Device Reset Screen

The following table describes the labels in this screen.

Table 33:   The Admin: Device Reset Screen

Reboot Device	Click **Reboot** to restart your CGN3.
Restore Factory Default Settings	Click **Factory Reset** to return your CGN3 to its factory default settings. When you do this, all your user-configured settings are lost, and cannot be retrieved.
Help	Click this to see information about the fields in this screen.

7
Security

This chapter describes the screens that display when you click **Security** in the toolbar. It contains the following sections:

7.1 Security Overview

This section describes some of the concepts related to the **Security** screens.

7.1.1 Firewall

The term "firewall" comes from a construction technique designed to prevent the spread of fire from one room to another. Similarly, your CGN3's firewall prevents intrusion attempts and other undesirable activity originating from the WAN, keeping the computers on your LAN safe. You can also use filtering techniques to specify the computers and other devices you want to allow on the LAN, and prevent certain traffic from going from the LAN to the WAN.

7.1.2 Intrusion detection system

An intrusion detection system monitors network activity, looking for policy violations, and malicious or suspicious activity. The CGN3's intrusion detection system logs all such activity to the **Security** > **Logs** screen.

7.1.3 Device Filtering

Every networking device has a unique Media Access Control (MAC) address that uniquely identifies it on the network. When you enable MAC address filtering on the CGN3's firewall, you can set up a list of devices, identified by their MAC addresses, and then specify whether you want to:

▸ Deny the devices on the list access to the CGN3 and the network (in which case all other devices can access the network)

or

▸ Allow the devices on the list to access the network (in which case no other devices can access the network).

7.1.4 Service Filtering

Service filtering is a way of preventing users on the LAN from connecting with devices on the WAN via specific services, protocols or applications. It achieves this by permitting or denying traffic from the LAN to pass to the WAN, based on the target port.

7.1.5 VPN

A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefitting from the functionality, security and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two.
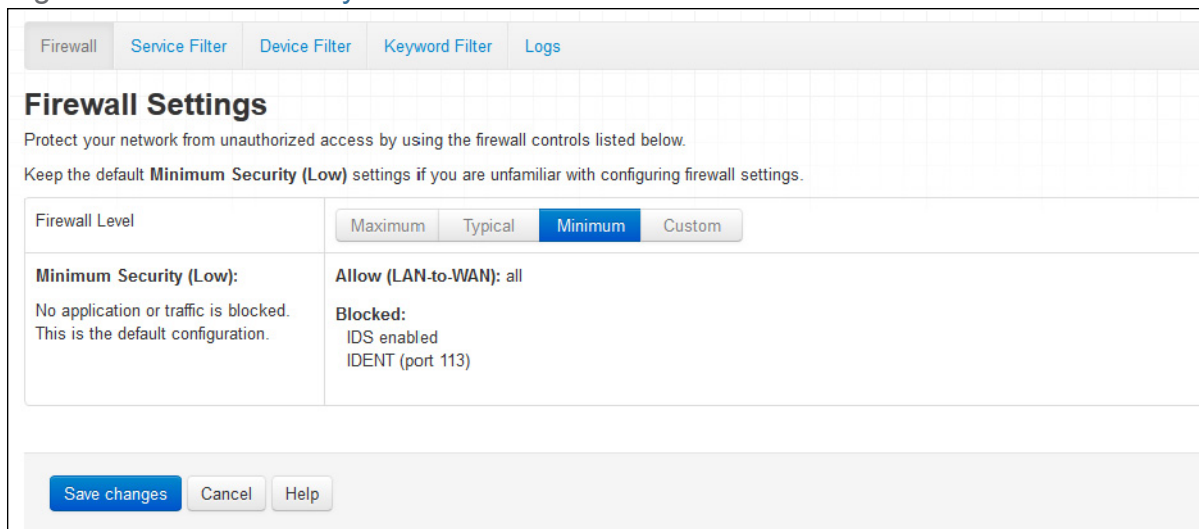
7.2 The Firewall Screen

Use this screen to turn firewall features on or off and to allow or permit certain applications and protocols. You can select the level of firewall protection from pre-defined options, or create a custom protection profile.

NOTE: To block specific ports, use the Service Filter screen (see The Service Filter Screen on page 92).

Click **Security** > **Firewall**. The following screen displays.

Figure 36:   The Security: Firewall Screen

The following table describes the labels in this screen.
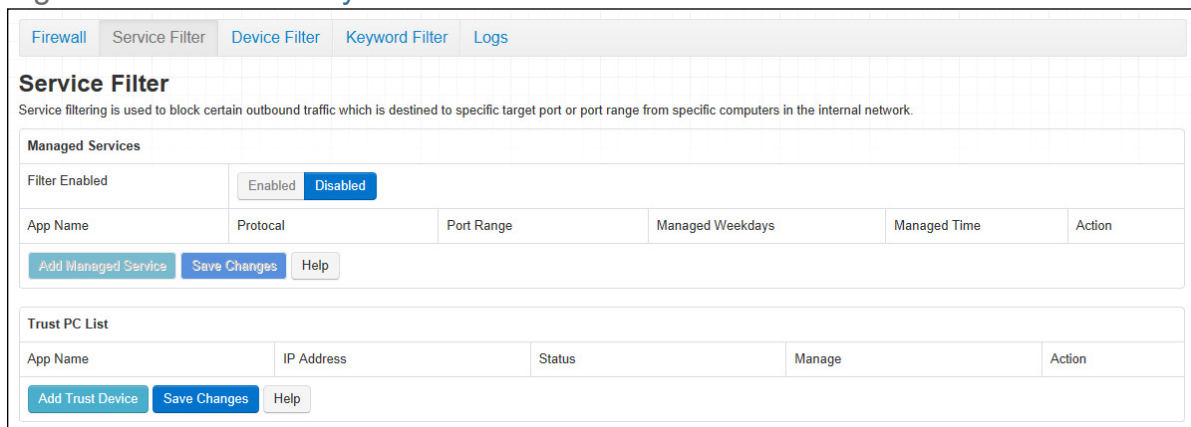
Table 34:   The Security: Firewall Screen

Firewall Level	Select the level of firewall protection that you want to apply to your LAN. Details about the protection level display beneath the buttons.
(Security Level)	These fields describe the specific protocols and applications that are permitted or denied by the firewall security level you select. When you select **Custom** in the **Firewall Level** field, additional fields display that allow you to toggle specific features on or off: ▸ **Entire Firewall**: select **ON** to enable firewall security protection, or select **OFF** to disable it (not recommended). ▸ **HTTP**: use this field to **Allow** or **Deny** HyperText Transfer Protocol traffic. ▸ **ICMP**: use this field to **Allow** or **Deny** Internet Control Message Protocol traffic. ▸ **Multicast**: use this field to **Allow** or **Deny** multicast traffic (sent to multiple devices at once). ▸ **P2P**: use this field to **Allow** or **Deny** peer-to-peer traffic (such as BitTorrent). ▸ **Ident**: use this field to **Allow** or **Deny** Identification protocol traffic. The Identification protocol allows remote hosts to request identifying information about users of a device.
Save Changes	Click this to save your changes to the fields in this screen.
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

7.3 The Service Filter Screen

Use this screen to configure service filtering. You can turn service filtering on or off and configure new and existing service filtering rules.

Click **Security** > **Service Filter**. The following screen displays.

Figure 37:   The Security: Service Filter Screen

The following table describes the labels in this screen.

Table 35:   The Security: Service Filter Screen

Managed Services	
Filter Enabled	Use this field to turn service filtering on or off. ▸ Select **Enabled** to turn service filtering on. ▸ Select **Disabled** to turn service filtering off.
App Name	This displays the name you assigned to the filtering rule when you created it.
Protocol	This field displays the protocol or protocols to which this filtering rule applies: ▸ Transmission Control Protocol (**TCP**) ▸ User Datagram Protocol (**UDP**)
Port Range	This displays the start and end port for which this filtering rule applies.
Managed Weekdays	This displays the days of the week on which this rule applies.

Table 35:   The Security: Service Filter Screen (continued)

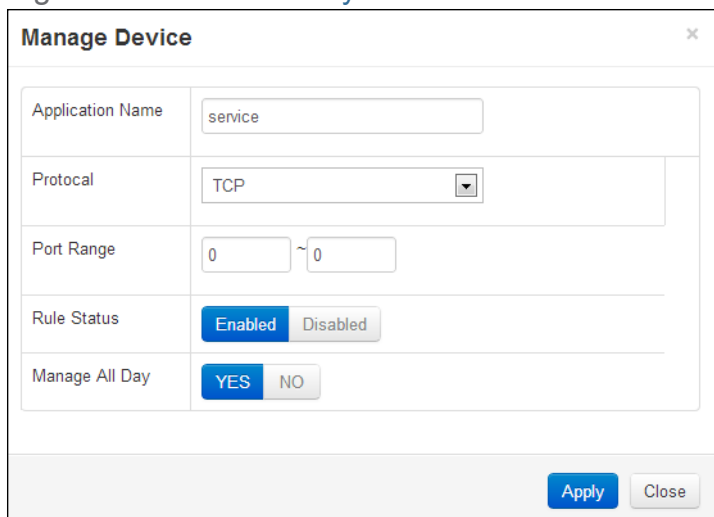|	
Managed Time	This displays the start (**From**) and end (**To**) of the time period during which this rule applies, on the specified **Managed Weekdays**.
Action	Click **Manage** to make changes to a filtering rule (see Adding or Editing a Service Filter Rule on page 93).
Add Managed Service	Click this to add a new service filtering rule (see Adding or Editing a Service Filter Rule on page 93).
Save Changes	Click this to save your changes to the fields in this screen.
Help	Click this to see information about the fields in this screen.
Trust PC List	
App Name	This displays the name of the trust device connected.
IP Address	This displays the IP address of the trust network device connected.
Status	This displays whether or not the service filter rule is enabled to the trust device connected.
Manage	Click **Manage** to make changes to the trust device's service filter status (see Adding or Editing a Trust PC List on page 96).
Action	Click **Delete** to remove the existing trust device from the list.
Add Trust Device	Click this to add a new Trust Device. (see Adding or Editing a Trust PC List on page 96).
Save Changes	Click this to save your changes to the fields in this screen.
Help	Click this to see information about the fields in this screen.

7.3.1 Adding or Editing a Service Filter Rule

▸ To add a new service filter rule, click **Add Managed Service** in the **Security** > **Service Filter** screen.

▸ To edit an existing service filter rule, locate the rule in the **Security** > **Service Filter** screen and click its **Manage** button.

NOTE: Ensure that **Enabled** is selected in the **Security** > **Service Filter** screen in order to add or edit service filtering rules.

The following screen displays.

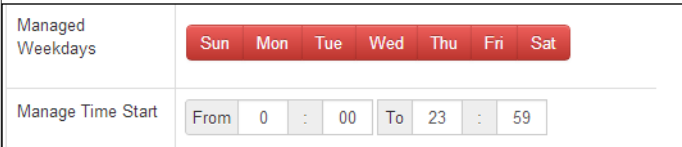Figure 38:   The Security: Service Filter Add/Edit Screen

The following table describes the labels in this screen.

Table 36:   The Security: Service Filter Add/Edit Screen

Application Name	Enter a name for the application for which you want to create the rule. NOTE: This name is arbitrary, and does not affect functionality in any way.
Protocol	Use this field to specify whether the CGN3 should filter via: ‣ Transmission Control Protocol (**TCP**) ‣ User Datagram Protocol (**UDP**) NOTE: If in doubt, leave this field at its default (**TCP**).
Port Range	Use these fields to specify the start and end port for which this filtering rule applies. These are the ports to which traffic will be blocked. Enter the start port number in the first field, and the end port number in the second field. To specify only a single port, enter its number in both fields.

Table 36: The Security: Service Filter Add/Edit Screen

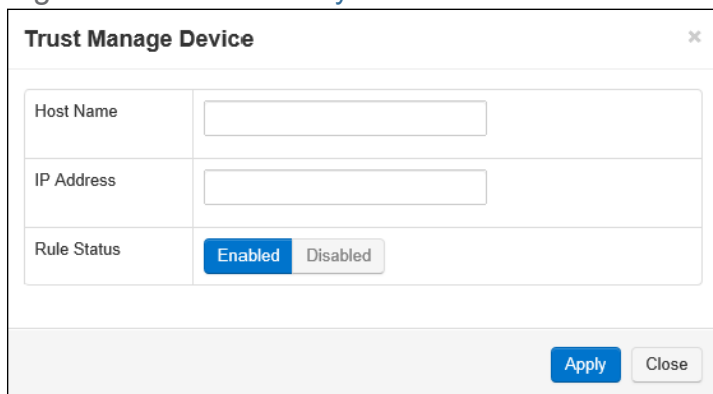| Rule Status	Use this field to select whether the filtering rule should be active or not. ▸ Select **Enabled** to activate the rule. Matching traffic will be blocked. ▸ Select **Disabled** to deactivate the rule. Matching traffic will not be blocked.
Manage All Day	Use this field to specify whether the filtering rule should apply on all days of the week, at all times, or whether the rule should be applied only at certain times. ▸ Select **YES** to apply the rule at all times. ▸ Select **NO** to apply the rule only at certain times. Additional fields display, allowing you to specify the times at which the rule should be applied. Figure 39: Additional Service Filtering Options Use the **Managed Weekdays** fields to specify the days on which the rule should be applied. A red background indicates that the rule will be applied (traffic will be blocked), and a green background indicates that the rule will not be applied (traffic will not be blocked). Click a day to toggle the rule on or off for the relevant day. Use the **Manage Time Start** fields to specify the period during which the rule should be applied. Enter the start time in the **From** fields, using twenty-four hour notation, and enter the end time in the **To** fields.
Apply	Click this to save your changes to the fields in this screen.
Close	Click this to return to the **Service Filter** screen without saving your changes to the rule.

7.3.2 Adding or Editing a Trust PC List

▶ To add a new trust PC to the list, click **Add Trust Device** in the **Security** > **Service Filter** screen.

▶ To edit an existing trust PC in the list, locate the device in the **Security** > **Service Filter** screen and click its **Manage** button.

NOTE: NOTE: Ensure that **Enabled** is selected in the **Security** > **Service Filter** screen in order to add or edit a trust PC.

The following screen displays.

Figure 40:   The Security: Service Filter > Trust PC List Add/Edit Screen

The following table describes the labels in this screen.

Table 37:   The Security: Service Filter Add/Edit Trust Manage Device Screen

Host Name	This displays the name of each network device connected.
IP Address	This displays the IP address of each network device connected.
Rule Status	Use this field to select whether the filtering rule should be active or not. ▶ Select **Enabled** to activate the rule. Matching traffic will be blocked. ▶ Select **Disabled** to deactivate the rule. Matching traffic will not be blocked.

Apply	Click this to save your changes to the fields in this screen.
Close	Click this to return to the **Service Filter** screen without saving your changes to the trust PC list.

7.4 The Device Filter Screen

Use this screen to configure Media Access Control (MAC) address filtering on the LAN, and to configure IP filtering.

NOTE: To configure MAC address filtering on the wireless network, see Access Control Screen on page 78.

You can set the CGN3 to allow only certain devices to access the CGN3 and the network, or to deny certain devices access.

You can turn filtering on or off, and configure new and existing filtering rules.

Click **Security** > **Device Filter**. The following screen displays.

Figure 41:   The Security: Device Filter Screen
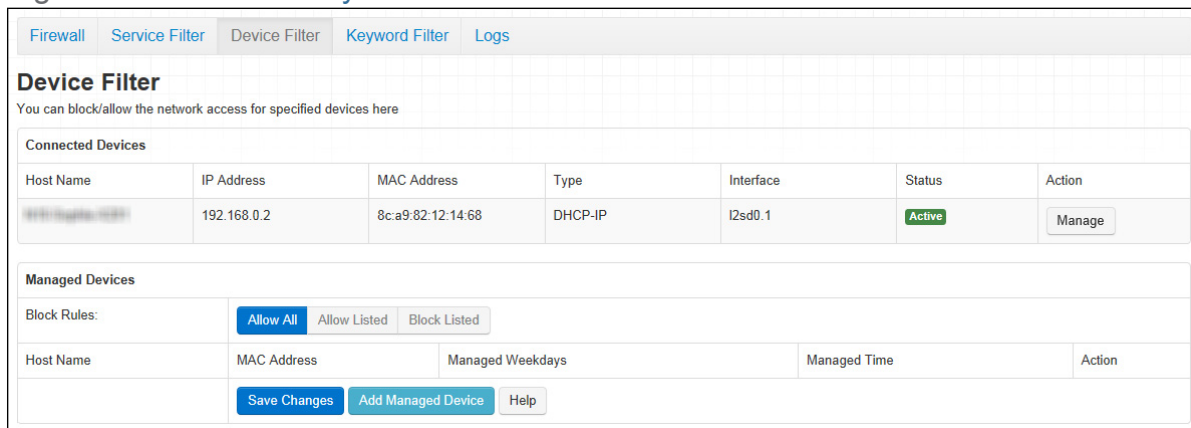
The following table describes the labels in this screen.

Table 38:   The Security: Device Filter Screen

Connected Devices	
Host Name	This displays the name of each network device connected on the LAN.

Table 38:   The Security: Device Filter Screen (continued)

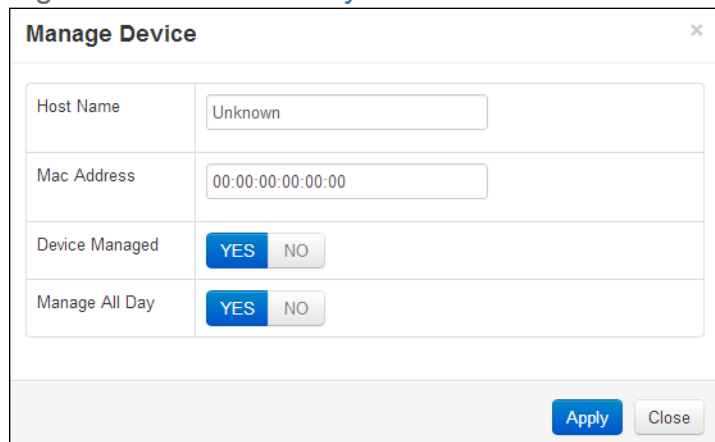|	
IP Address	This displays the IP address of each network device connected on the LAN.
MAC Address	This displays the Media Access Control (MAC) address of each network device connected on the LAN.
Type	This displays whether the device's IP address was assigned by DHCP (**DHCP-IP**), or **self-assigned**.
Interface	This displays the name of the interface on which the relevant device is connected.
Action	Click **Manage** to make changes to the device's filtering status; see Adding or Editing a Managed Device on page 99 for information on the screen that displays.
Managed Devices	
Block Rules	Use these buttons to control the action to be taken for the devices listed: ▶ Select **Allow All** to ignore the **Managed Devices** list and let all devices connect to the CGN3. ▶ Select **Allow** to permit only devices you added to the **Managed Devices** list to access the CGN3 and the network. All other devices are denied access. ▶ Select **Deny** to permit all devices except those you added to the **Managed Devices** list to access the CGN3 and the network. The specified devices are denied access.
Host Name	This displays the name of each network device in the list.
MAC Address	This displays the Media Access Control (MAC) address of each network device in the list.
Managed Weekdays	This displays the days of the week on which the device is managed.
Managed Time	This displays the start (**From**) and end (**To**) of the time period during which the device is managed, on the specified **Managed Weekdays**.
Action	Click **Manage** to make changes to a filtering rule (see Adding or Editing a Managed Device on page 99).
Save Changes	Click this to save your changes to the fields in this screen.

Table 38: The Security: Device Filter Screen (continued)

Add Managed Device	Click this to add a new service filtering rule (see Adding or Editing a Managed Device on page 99).
Help	Click this to see information about the fields in this screen.

7.4.1 Adding or Editing a Managed Device

▸ To add a new managed device, click **Add Managed Device** in the **Security** > **Device Filter** screen.

▸ To edit an existing managed device, locate the device in the **Security** > **Device Filter** screen and click its **Manage** button.

The following screen displays.

Figure 42: The Security: Device Filter Add/Edit Screen
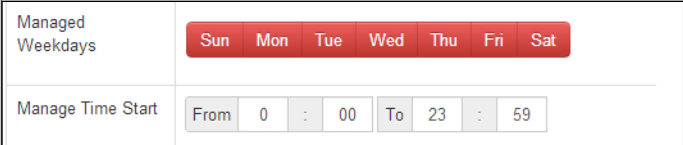
The following table describes the labels in this screen.

Table 39: The Security: Device Filter Add/Edit Screen

Host Name	If you are managing a device that already connected via the LAN, this field displays the device's name. Alternatively, if you are managing a device that is not connected via the LAN, you can enter its name here if you know it.
MAC Address	If you are managing a device that already connected via the LAN, this field displays the device's MAC (Media Access Control) address. Alternatively, if you are managing a device that is not connected via the LAN, you can enter its MAC address here if you know it.
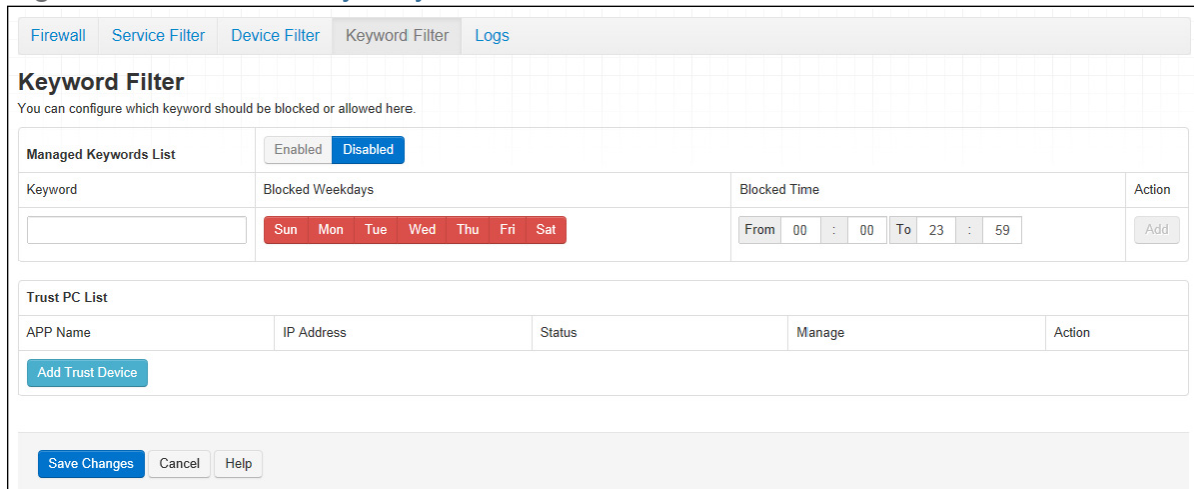
Version 1.1, 08/2013. Copyright © 2013 Hitron Technologies

Table 39:   The Security: Device Filter Add/Edit Screen

Device Managed	Use this field to define whether the device should have its access privileges filtered or not.
	▸ Click **Yes** to filter the device's access privileges.
	▸ Click **No** not to filter the device's access privileges.
	When a device is not being managed, the **Manage All Day** field, and related fields, do not display.
Manage All Day	Use this field to specify whether the device should be managed on all days of the week, at all times, or whether the device should be managed only at certain times.
	▸ Select **YES** to managed the device at all times.
	▸ Select **NO** to managed the device only at certain times. Additional fields display, allowing you to specify the times at which the device should be managed.
	Figure 43: Additional Service Filtering Options
	Use the **Managed Weekdays** fields to specify the days on which the device should be managed. A red background indicates that the device will be managed (access will be blocked), and a green background indicates that the device will not be managed (access will not be blocked). Click a day to toggle the rule on or off for the relevant day.
	Use the **Manage Time Start** fields to specify the period during which the device should be managed. Enter the start time in the **From** fields, using twenty-four hour notation, and enter the end time in the **To** fields.
Apply	Click this to save your changes to the fields in this screen.
Close	Click this to return to the **Device Filter** screen without saving your changes to the rule.

7.5 The Keyword Filter Screen

Use this screen to block access from the LAN to websites whose URLs (Web addresses) and page content (text) contain certain keywords. You can create multiple keyword blocking rules, and set them to apply on certain days and at certain times.

Click **Security** > **Keyword Filter**. The following screen displays.

Figure 44:   The Security: Keyword Filter Screen

The following table describes the labels in this screen.

Table 40:   The Security: Keyword Filter Screen

Managed Keywords List	Use this field to turn keyword filtering on or off. ▸ Select **Enabled** to turn keyword filtering on. ▸ Select **Disabled** to turn keyword filtering off.
Keyword	Enter the keyword that you want to block. The CGN3 examines both the page's URL (Internet address) and its page content (text).
Blocked Weekdays	Use these fields to specify the times at which the keyword should be blocked. A red background indicates that the rule will be applied (access will be blocked), and a green background indicates that the device will not be applied (access will not be blocked). Click a day to toggle the rule on or off for the relevant day.

Table 40: The Security: Keyword Filter Screen (continued)

Blocked Time	Use these fields to specify the period during which the rule should be applied. Enter the start time in the **From** fields, using twenty-four hour notation, and enter the end time in the **To** fields.
Action	Click **Add** to create a new keyword blocking rule; a new row of fields display.
Save Changes	Click this to save your changes to the fields in this screen.
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.
Trust PC List	
App Name	This displays the name of the trust device connected.
IP Address	This displays the IP address of the trust network device connected.
Status	This displays whether or not the keyword filter rule is enabled of the trust device connected.
Manage	Click **Manage** to make changes to the trust device's keyword filter status; see Adding or Editing a Trust PC List on page 102.
Action	Click to delete the existing trust device from the list.
Add Trust Device	Click this to add a new Trust Device. (see Adding or Editing a Trust PC List on page 102).
Save Changes	Click this to save your changes to the fields in this screen.
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.
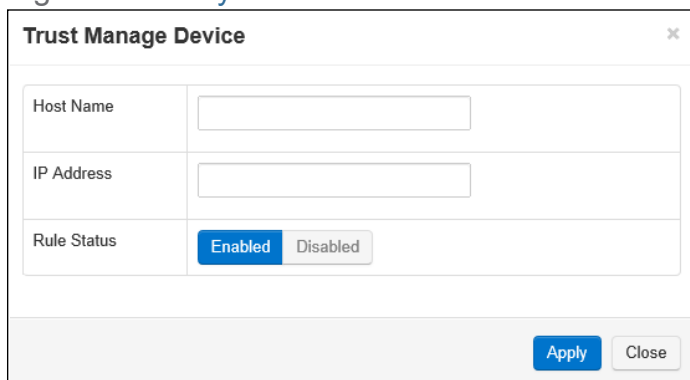
7.5.1 Adding or Editing a Trust PC List

▸ To add a new trust PC to the list, click **Add Trust Device** in the **Security** > **Keyword Filter** screen.

▸ To edit an existing trust PC in the list, locate the device in the **Security** > **Keyword Filter** screen and click its **Manage** button.

NOTE: Ensure that **Enabled** is selected in the **Security** > **Keyword Filter** screen in order to add or edit a trust PC.

The following screen displays.

Figure 45:   Keyword Filter > Trust PC List Add/Edit Screen

The following table describes the labels in this screen.

Table 41:   The Security: Keyword Filter Add/Edit Trust Manage Device Screen

Host Name	This displays the name of each network device connected.
IP Address	This displays the IP address of each network device connected.
Rule Status	Use this field to select whether the filtering rule should be active or not. ▸ Select **Enabled** to activate the rule. Matching traffic will be blocked. ▸ Select **Disabled** to deactivate the rule. Matching traffic will not be blocked.
Apply	Click this to save your changes to the fields in this screen.
Close	Click this to return to the **Keyword Filter** screen without saving your changes to the trust PC list.

7.6 The Logs Screen

Use this screen to view information about local firewall activity events.

Click **Security** > **Logs**. The following screen displays.

Figure 46:   The Security: Logs Screen
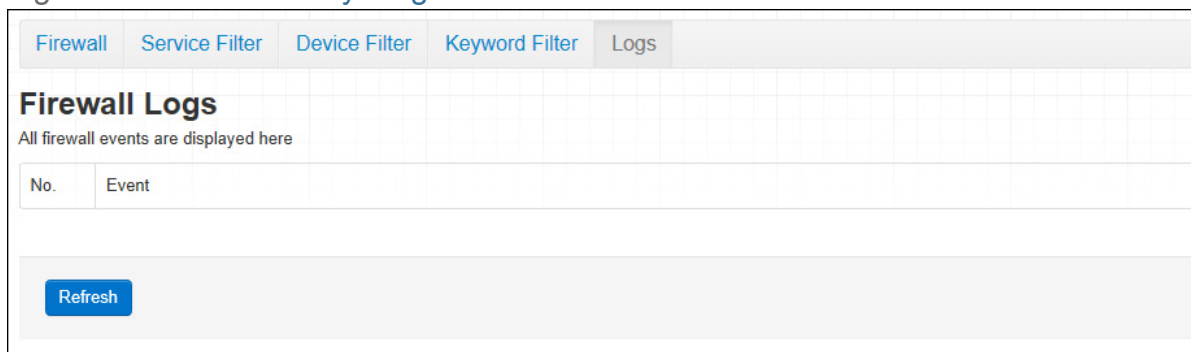
The following table describes the labels in this screen.

Table 42:   The Security: Logs Screen

No.	This displays the arbitrary, incremental index number assigned to the firewall event.
Event	This displays a description of the firewall event.

7.7 The VPN Pass-Through Screen

Use this screen to configure VPN Pass-through.

Click **Security** > **VPN Pass-through**. The following screen displays.

Figure 47:   The Security: VPN Pass-through Screen
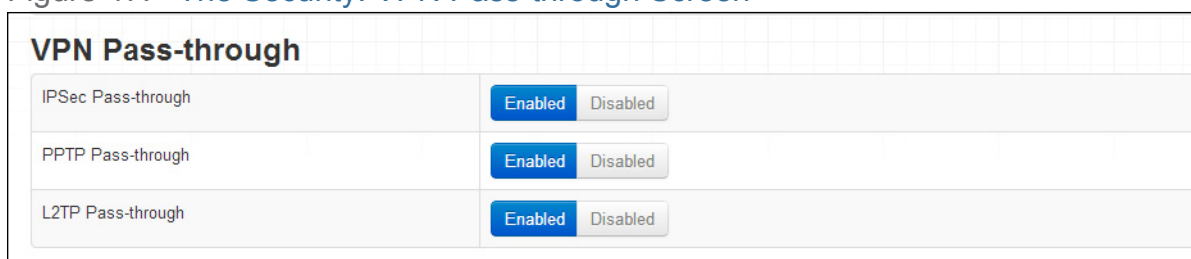
The following table describes the labels in this screen.

Table 43:   The Security: VPN Pass-through Screen

IPSec Pass-through	Use this field to select whether the IPSec Pass-through be active or not.
	▸ Select **Enabled** to activate the IPSec Pass-through.
	▸ Select **Disabled** to deactivate the IPSec Pass-through.
	NOTE: The Internet Protocol Security (IPsec) is a technology protocol suite for securing IP communications by authenticating and/or encrypting each IP packet of a communication session.
PPTP Pass-through	Use this field to select whether the PPTP Pass-through be active or not.
	▸ Select **Enabled** to activate the PPTP Pass-through.
	▸ Select **Disabled** to deactivate the PPTP Pass-through.
	NOTE: The Point-to-Point Tunneling Protocol (PPTP) is used for providing security levels and remote access levels comparable with typical VPN products.
L2TP Pass-through	Use this field to select whether the L2TP Pass-through be active or not.
	▸ Select **Enabled** to activate the L2TP Pass-through.
	▸ Select **Disabled** to deactivate the L2TP Pass-through.
	NOTE: The Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs.

8

Troubleshooting

Use this section to solve common problems with the CGN3 and your network. It contains the following sections:

Problem: None of the LEDs Turn On

The CGN3 is not receiving power, or there is a fault with the device.

1 Ensure that you are using the correct power adaptor.

🧨 **Using a power adaptor other than the one that came with your CGN3 can damage the CGN3.**

2 Ensure that the power adaptor is connected to the CGN3 and the wall socket (or other power source) correctly.

3 Ensure that the power source is functioning correctly. Replace any broken fuses or reset any tripped circuit breakers.

Version 1.1, 08/2013. Copyright © 2013 Hitron Technologies

4 Disconnect and re-connect the power adaptor to the power source and the CGN3.

5 If none of the above steps solve the problem, consult your vendor.

Problem: One of the LEDs does not Display as Expected

1 Ensure that you understand the LED's normal behavior (see LEDs on page 18).

2 Ensure that the CGN3's hardware is connected correctly; see the Quick Installation Guide.

3 Disconnect and re-connect the power adaptor to the CGN3.

4 If none of the above steps solve the problem, consult your vendor.

Problem: I Forgot the CGN3's IP Address

1 The CGN3's default LAN IP address is **192.168.0.1**.

2 You can locate the CGN3's GUI by entering the LAN domain suffix into your browser's address bar (on a computer connected to the LAN). The default LAN domain suffix is displayed in the **Basic** > **LAN Setup** screen's **Domain Suffix** field. See The LAN Setup Screen on page 51 for more information.

3 Depending on your operating system and your network, you may be able to find the CGN3's IP address by looking up your computer's default gateway. To do this on (most) Windows machines, click **Start** > **Run**, enter "cmd", and then enter "ipconfig". Get the IP address of the **Default Gateway**, and enter it in your browser's address bar.

4 If you still cannot access the CGN3, you need to reset the CGN3. See Resetting the CGN3 on page 25. All user-configured data is lost, and the CGN3 is returned to its default settings. If you previously backed-up a more recent version your CGN3's settings, you can now upload them to the CGN3; see Backup Screen on page 84.

Problem: I Forgot the CGN3's Admin Username or Password

1 The default username is **admin**, and the default password is **password**.

2 If the default username and password do not work, you need to reset the CGN3. See Resetting the CGN3 on page 25. All user-configured data is lost, and the CGN3 is returned to its default settings. If you previously backed-up a more recent version your CGN3's settings, you can now upload them to the CGN3; see Backup Screen on page 84.

Problem: I Cannot Access the CGN3 or the Internet

1 Ensure that you are using the correct IP address for the CGN3.

2 Check your network's hardware connections, and that the CGN3's LEDs display correctly (see LEDs on page 18).

3 Make sure that your computer is on the same subnet as the CGN3; see IP Address Setup on page 22.

4 If you are attempting to connect over the wireless network, there may be a problem with the wireless connection. Connect via a **LAN** port instead.

5 If the above steps do not work, you need to reset the CGN3. See Resetting the CGN3 on page 25. All user-configured data is lost, and the CGN3 is returned to its default settings. If you previously backed-up a more recent version your CGN3's settings, you can now upload them to the CGN3; see Backup Screen on page 84.

6 If the problem persists, contact your vendor.

Problem: I Cannot Access the Internet and the DS and US LEDs Keep Blinking

Your service provider may have disabled your Internet access; check the **Status > DOCSIS WAN** screen's **Network Access** field (see The DOCSIS WAN Screen on page 42).

Problem: I Cannot Connect My Wireless Device

1 Ensure that your wireless client device is functioning properly, and is configured correctly. See the wireless client's documentation if unsure.

2 Ensure that the wireless client is within the CGN3's radio coverage area. Bear in mind that physical obstructions (walls, floors, trees, etc.) and electrical

interference (other radio transmitters, microwave ovens, etc) reduce your CGN3's signal quality and coverage area.

3 Ensure that the CGN3 and the wireless client are set to use the same wireless mode and SSID (see Basic Settings Screen on page 70) and security settings (see WPS & Security Screen on page 75).

4 Re-enter any security credentials (WEP keys, WPA(2)-PSK password, or WPS PIN).

5 If you are using WPS's PBC (push-button configuration) feature, ensure that you are pressing the button on the CGN3 and the button on the wireless client within 2 minutes of one another.

Index

Numbers

A

B

C

(column 2)

D

E

Version 1.1, 08/2013. Copyright © 2013 Hitron Technologies

N

O

P

Q

R

S

T

U

W

X