CODA-4x8x DOCSIS Wifi Gateway

User's Guide

Version 1.0 - 12/2016

hitron

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the CODA-4x8x's features via its Graphical User Interface (GUI).

How to Use this User's Guide

This manual contains information on each the CODA-4x8x's GUI screens, and describes how to use its various features.

- Use the Introduction 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 146) to find information on a specific keyword.
- Use the rest of this User's Guide to see in-depth descriptions of the CODA-4x8x's features.

Related Documentation

- **Quick Installation Guide**: see this for information on getting your CODA-4x8x 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 CODA-4x8x's Graphical User Interface (GUI) contains 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 CODA-4x8x's default IP address and login credentials are as follows. For more information, see Logging in to the CODA-4x8x on page 23.

Table 1: Default Credentials

IP Address	192.168.0.1
Username	cusadmin
Password	password

NOTE: When you have completed the EasyConnect setup wizard, the default password is replaced with the password you configured for the wireless network.

DISCLAIMER: The information in this User's Guide is accurate at the time of writing. This User's Guide is provided "as is" without express or implied warranty of any kind. Neither Hitron Technologies nor its agents assume any liability for inaccuracies in this User's Guide, or losses incurred by use or misuse of the information in this User's Guide.

Table of Contents

List of Figures

List of Tables

1

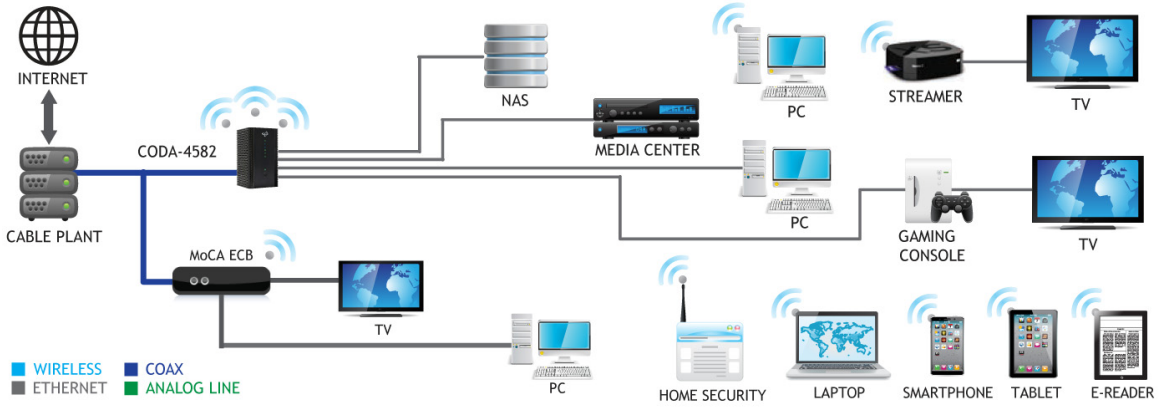
Introduction

This chapter introduces the CODA-4x8x and its GUI (Graphical User Interface).

1.1 CODA-4x8x Overview

Your CODA-4x8x is a DOCSIS cable modem, router, embedded Multimedia Terminal Adapter (eMTA) and wireless access point that allows you to connect your cabled Ethernet, wireless devices and analog telephones to one another and to the Internet via your building's cable connection.

Figure 1: Application Overview



For more information on MoCA, see MoCA Overview on page 58.

1.1.1 Model Differentiation

The models covered by this User's Guide differ in the following specifics:

- The CODA-4582 operates on cable data frequencies of 5 to 85MHz.

- The CODA-4682 operates on cable data frequencies of 5 to 42MHz and 5~85MHz (configurable by the operator).
- The CODA-4782 operates on cable data frequencies of 5 to 85MHz, and 5 to 204MHz (configurable by the operator).

1.1.2 Key Features

The CODA-4x8x provides:

- DOCSIS 3.1 compliant and DOCSIS 3.1 certified.
- WiFi 3x3 2.4GHz 802.11n and 4x4 5GHz 802.11ac Wave 2 dual-band.
- 16 SSIDs (8 SSIDs per radio).
- Individual configuration for each SSID (security, bridging, routing, firewall and WiFi).
- One USB 3.0 host, supporting Network Attached Storage (NAS) functionality.
- Integrated DLNA media server with support for video, audio and image serving.
- Extensive operator control via configuration file and SNMP.
- Well-defined LEDs clearly display device and network status.
- TR-069 and HNAP for easy setup and remote management.
- Enhanced management and stability for low total cost of ownership.
- MoCA channel bonding for high performance.

1.2 Hardware Connections

This section describes the CODA-4x8x's physical ports and buttons.

Figure 2: Hardware Connections

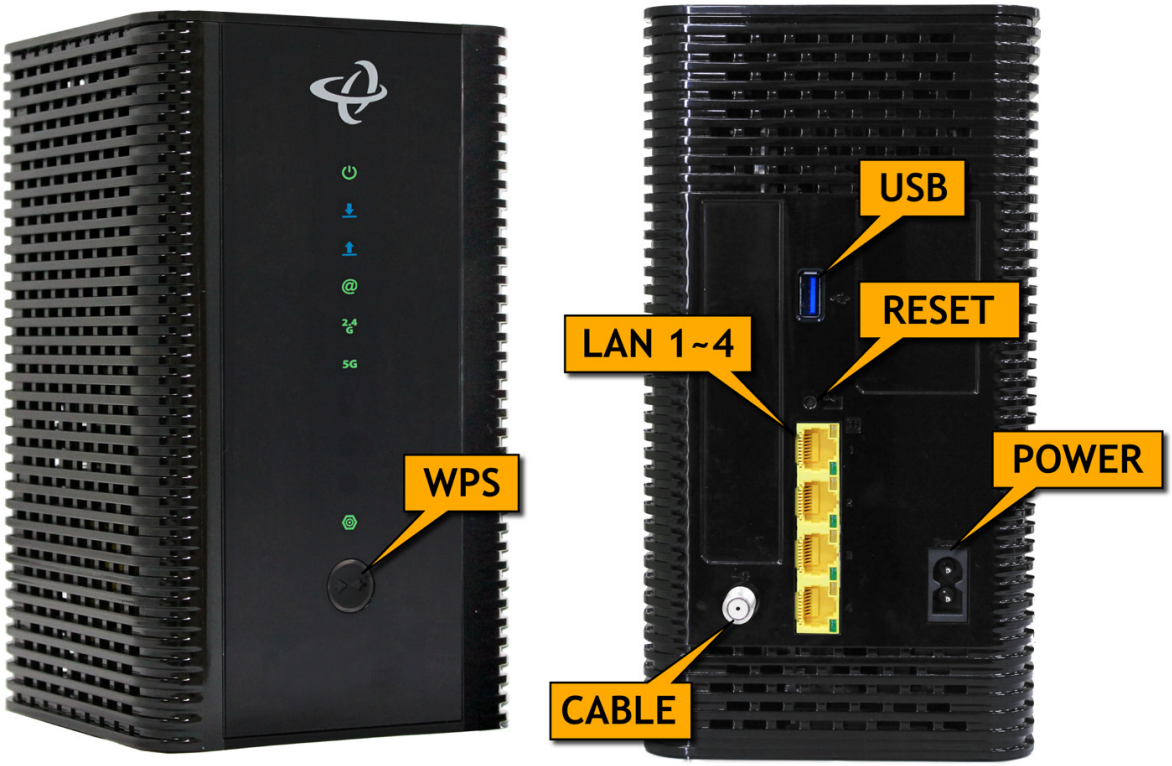


Table 2: Hardware Connections

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. The **WPS** LED displays WiFi Protected Setup connection status as follows: • **Bi-color, blinking**: the WPS connection is processing. • **Green, steady**: the WPS connection has been successful. • **Red, steady**: the WPS connection has failed, or an error has occurred. • **Off**: WPS is not active. See WPS on page 86 for more information.
USB	Use this port to plug in USB flash disks for mounting and sharing through the LAN interfaces via the Samba protocol (network neighborhood). The CODA-4x8x supports the following Windows file systems: • FAT16 • FAT32 **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).**

Table 2: Hardware Connections

RESET	Use this button to reboot or reset your CODA-4x8x to its factory default settings. To reboot the CODA-4x8x, press the button and hold it for less than five seconds. The CODA-4x8x restarts, using your existing settings. To reset the CODA-4x8x, press the button and hold it for five or more seconds. All user-configured settings are deleted, and the CODA-4x8x restarts using its factory default settings.
LAN 1 LAN 2 LAN 3 LAN 4	Use these ports to connect your computers and other network devices, using Category 5 or 6 Ethernet cables with RJ45 connectors. Each **LAN** port's yellow LED glows when the connection on the relevant port's is at 1Gbps, and its green LED glows when the connection is at 10/100Mbps.
CABLE	Use this to connect to the Internet via an F-type RF cable.
POWER	Use the **POWER** port to connect to the 100~125VAC power cable that came with your CODA-4x8x Figure 3: Power Cable 

1.3 LEDs

This section describes the CODA-4x8x's LEDs (lights).

Figure 4: LEDs

Table 3: LEDs

LED	STATUS	**DESCRIPTION**
POWER 	Off	The CODA-4x8x is not receiving power and is switched off.
	On	The CODA-4x8x is receiving power and is switched on.

Table 3: LEDs

DS 	Green, blinking	The CODA-4x8x is searching for a downstream frequency on the **CABLE** connection.
	Green, steady	The CODA-4x8x has successfully located and locked onto a single downstream frequency on the **CABLE** connection.
	Blue, steady	The CODA-4x8x is successfully engaged in channel bonding on the downstream connection.
	Off	There is no downstream activity on the **CABLE** connection.
US 	Green, blinking	The CODA-4x8x is searching for an upstream frequency on the **CABLE** connection.
	Green, steady	The CODA-4x8x has successfully located and locked onto a single upstream frequency on the **CABLE** connection.
	Blue, steady	The CODA-4x8x is successfully engaged in channel bonding on the upstream connection.
	Off	There is no upstream activity on the **CABLE** connection.
Online 	Green, blinking	The CODA-4x8x's cable modem is registering with the service provider's CMTS.
	Green, steady	The CODA-4x8x's cable modem has successfully registered with the service provider and is ready for data transfer.
	Off	The CODA-4x8x's cable modem is offline.
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.
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.

Table 3: LEDs

MoCA 	Off	The **CABLE IN/OUT** port is not connected to a coax socket, or the **CABLE IN/OUT** port is connected to a coax socket, but no other MoCA device has been detected on the coax network.
	Green, steady	Another MoCA device has been detected on the coax network, and the CODA-4x8x has successfully made a connection.
	Yellow, blinking	Data is being transferred to or from the CODA-4x8x over the coax network.

1.4 IP Address Setup

Before you log into the CODA-4x8x's GUI, your computer's IP address must be in the same subnet as the CODA-4x8x. This allows your computer to communicate with the CODA-4x8x.

NOTE: See When the CODA-4x8x is not in routing mode, the service provider assigns an IP address to each computer connected to the CODA-4x8x directly. The CODA-4x8x does not perform any routing operations, and traffic flows between the computers and the service provider. on page 65 for background information.

If your computer is configured to get an IP address automatically, or if you are not sure, try to log in to the CODA-4x8x (see GUI Overview on page 24).

- If the login screen displays, your computer is already configured correctly.
- If the login screen does not display, 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 CODA-4x8x's IP settings may have been changed from their defaults. If you do not know the CODA-4x8x's new address, you should return it to its factory defaults. See Resetting the CODA-4x8x on page 25. Bear in mind that ALL user-configured settings are lost.

1.4.1 Manual IP Address Setup

By default, your CODA-4x8x's local IP address is **192.168.0.1**. If your CODA-4x8x 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**.

Take the following steps to manually set up your computer's IP address to connect to the CODA-4x8x:

NOTE: This example uses Windows 7; the procedure for your operating system may be different.

1. Click the **Start Orb**, then click **Control Panel**.
2. In the window that displays, double-click **Network And Sharing Center**.
3. In the left-hand panel, click **Change Adapter Settings**.
4. Right-click your network connection (usually **Local Area Connection**) and click **Properties**.
5. In the **Networking** tab's **This connection uses the following items** list, scroll down and select **Internet Protocol (TCP/IPv4)**. Click **Properties**.
6. You can get an IP address automatically, or specify one manually:
   - If your network has an active DHCP server, select **Get an IP address automatically**.
   - If your network does not have an active DHCP server, 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). In the **Default Gateway** field, enter **192.168.0.1** (default).

NOTE: If your CODA-4x8x is not using the default IP address, enter an IP address and subnet mask that places your computer in the same subnet as the CODA-4x8x.

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

Your computer now obtains an IP address from the CODA-4x8x, or uses the IP address that you specified, and can communicate with the CODA-4x8x.

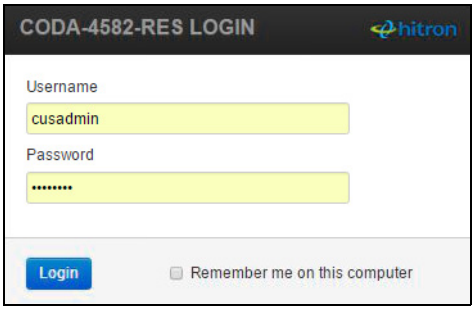
1.5 Logging in to the CODA-4x8x

Take the following steps to log into the CODA-4x8x's GUI.

NOTE: If you did not already complete the EasyConnect setup wizard (see EasyConnect on page 26) you will be prompted to do so before you can log in.

1. Open a browser window.
2. Enter the CODA-4x8x's IP address (default **192.168.0.1**) in the URL bar. The **Login** screen displays.

Figure 5: Login



3. Enter the **Username** and **Password**. The default user name is **cusadmin** and the password is the same as the password you configured for the wireless network in the EasyConnect wizard (see EasyConnect on page 26).

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

4. If you want to log in without entering the password in future, select **Remember me on this computer**. Only select this on your own, private computer (not public computers, or those easily-accessible by others).
5. Click **Login**. The **Status Overview** screen displays (see The Status: Overview Screen on page 44).

1.6 GUI Overview

This section describes the CODA-4x8x's GUI.

Figure 6: GUI Overview

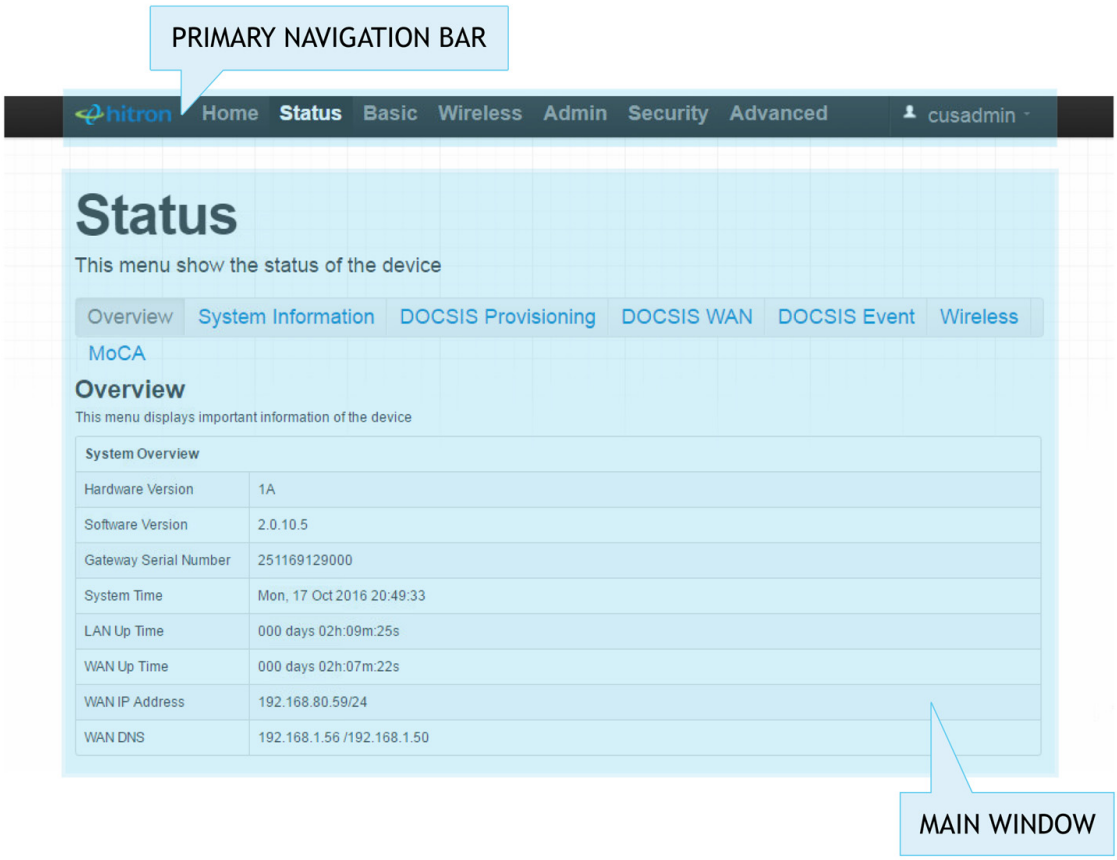


Table 4: GUI Overview

Primary Navigation Bar	Use this section to move from one part of the GUI to another.
Main Window	Use this section to read information about your CODA-4x8x's configuration, and make configuration changes.
Online Help	Use this section to learn more information about the fields in each screen.

1.7 Resetting the CODA-4x8x

When you reset the CODA-4x8x to its factory defaults, all user-configured settings are lost, and the CODA-4x8x is returned to its initial configuration state.

To reset the CODA-4x8x, press and hold the **RESET** button for ten seconds, or go to the **Admin** > **Device Reset** screen and click **Factory Reset** (see The Admin: Device Reset Screen on page 115). The CODA-4x8x turns off and on again, using its factory default settings.

NOTE: Depending on your CODA-4x8x's previous configuration, you may need to re-configure your computer's IP settings; see IP Address Setup on page 21.

2

EasyConnect

This chapter describes the screens that display when you first access the CODA-4x8x, and when you access the CODA-4x8x after a factory reset (see Resetting the CODA-4x8x on page 25). It contains the following sections:

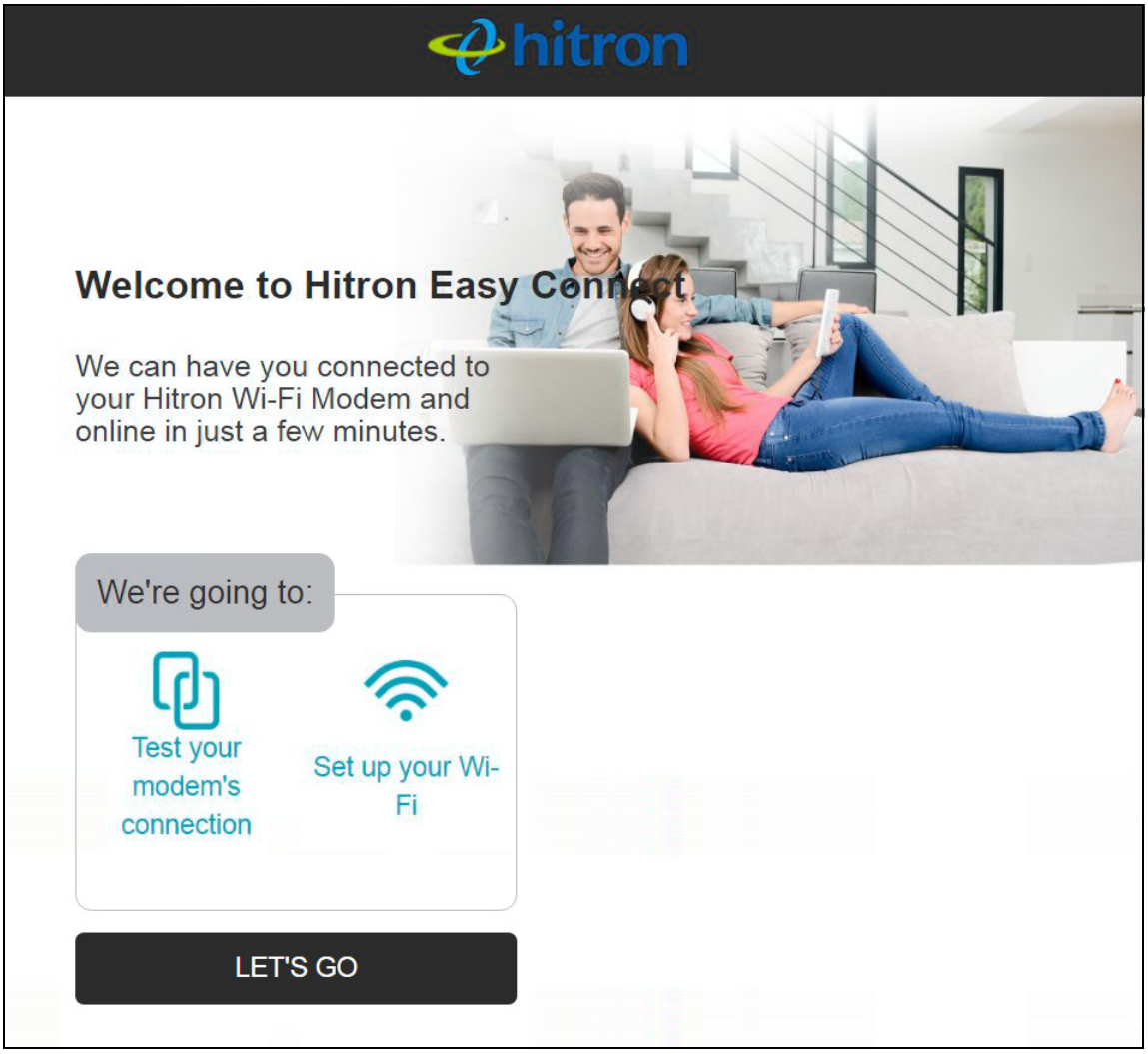
2.1 EasyConnect Overview

EasyConnect is a setup wizard that allows you to rapidly configure the CODA-4x8x's most important settings, including Internet connection, wireless and password settings.

2.2 EasyConnect: Welcome

This screen displays when you first access the CODA-4x8x, or immediately after you have performed a factory reset. Click **Let's Go** to proceed to the **Connection** screens (see EasyConnect: Internet Connection on page 27).

Figure 7: The EasyConnect: Welcome Screen

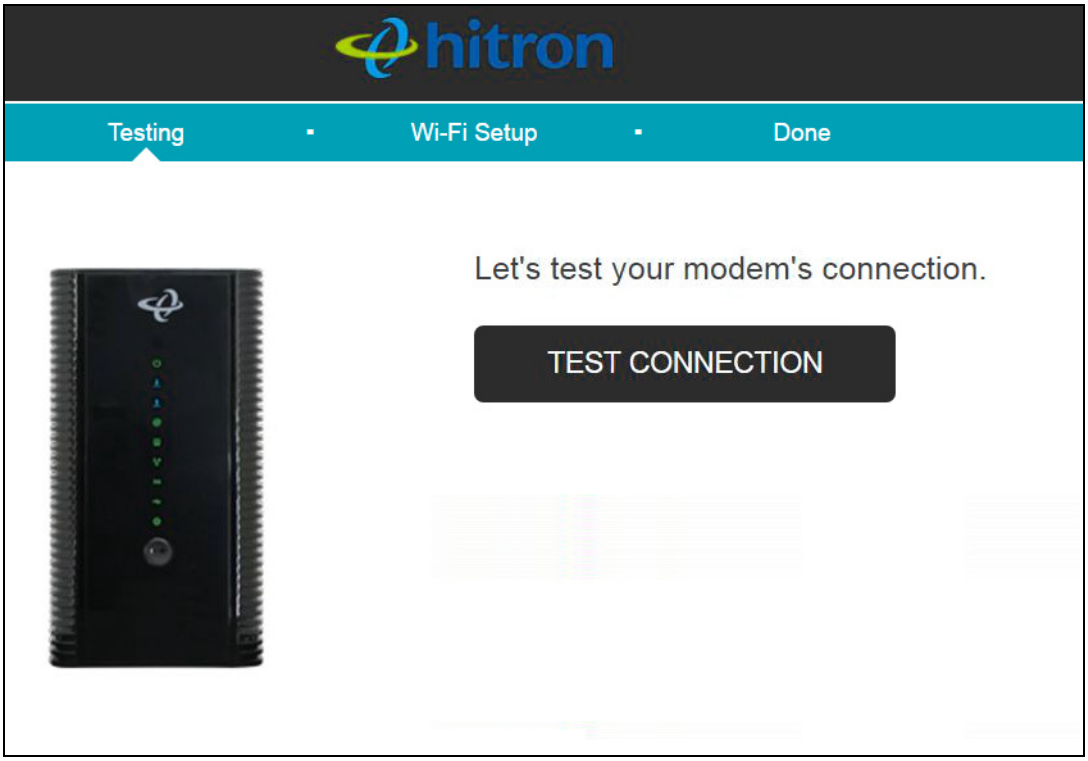


2.3 EasyConnect: Internet Connection

Use these screens to test the CODA-4x8x's connection to the Internet.

Click **Let's Go** in the EasyConnect **Welcome** screen. The following screen displays.

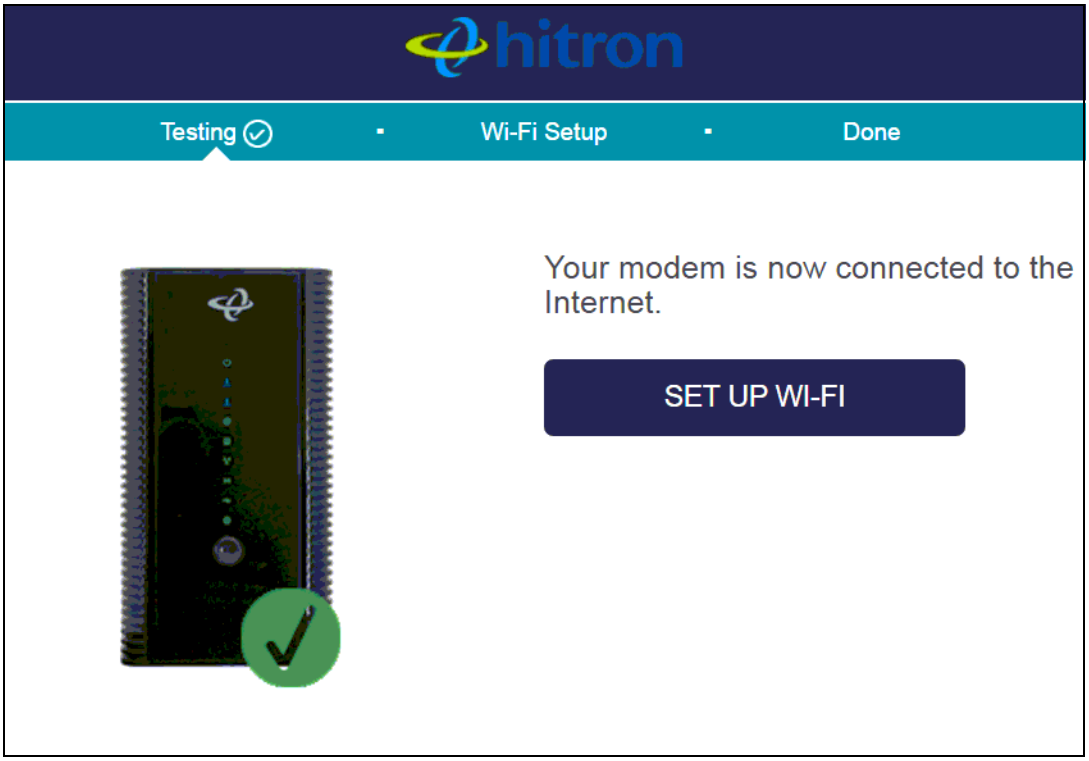
Figure 8: The EasyConnect: Internet Connection Start Screen



Click **Test Connection** to proceed. The Internet connection test begins.

If the test is successful, the following screen displays.

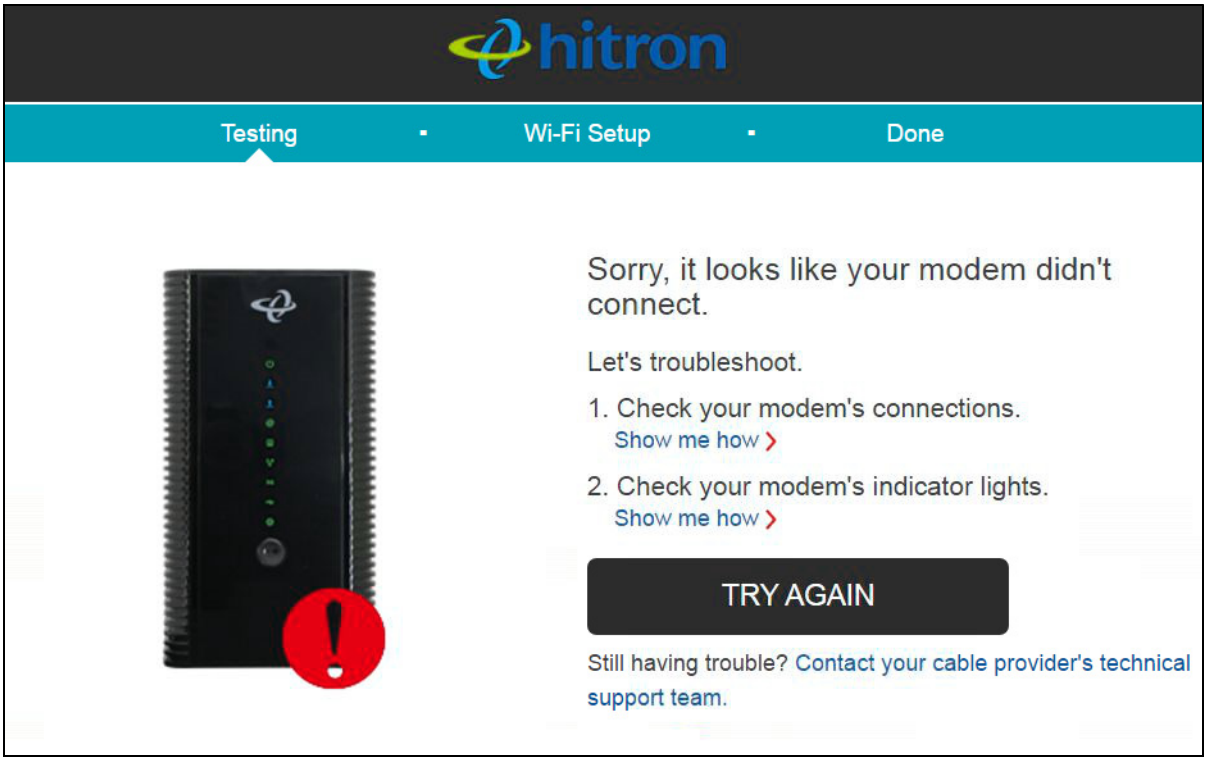
Figure 9: The EasyConnect: Internet Connection Success Screen



Click **Set up wi-fi** to proceed to the wireless network setup screens (see EasyConnect: Wireless Settings on page 30).

If the CODA-4x8x was unable to connect to the Internet, the Internet connection test fails and the following screen displays.

Figure 10: The EasyConnect: Internet Connection Fail Screen



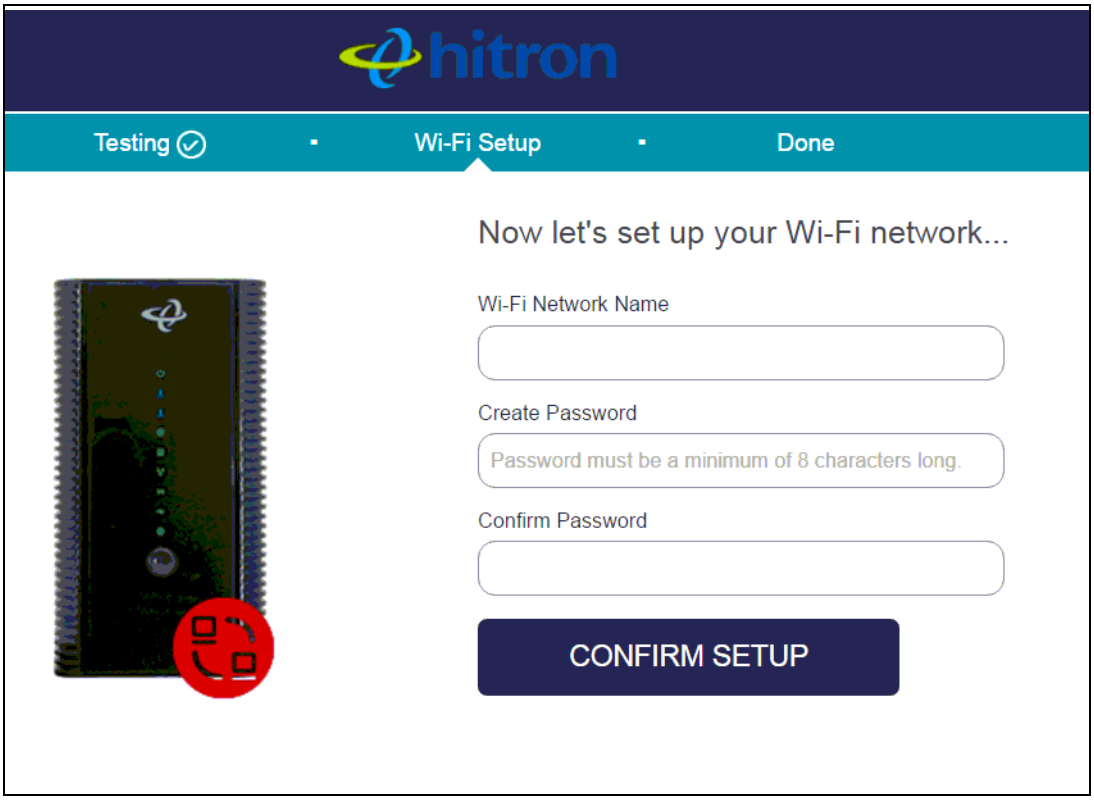
Follow the instructions on the screen and, when ready to run the Internet connection test again, click **Try again**.

2.4 EasyConnect: Wireless Settings

Use this screen to configure the CODA-4x8x's wireless network and set the administrative interface login password.

When EasyConnect's Internet Connection test has successfully completed, the following screen displays.

Figure 11: The EasyConnect: Wireless Settings Screen



- Enter the name you want to use for your wireless network in the **WiFi Network Name** field. You will use this name to identify and connect to the wireless network from your client device(s).
- Enter the password you want to use for your wireless network in the **Create Password** field, and re-enter it in the **Confirm Password** field.

NOTE: The password you enter in the EasyConnect **Wireless Settings** screen will replace the CODA-4x8x's default administrative interface password. When you log into the CODA-4x8x, you will need to use the password you entered in the **Create Password** and **Confirm Password** fields.

- Click **Confirm Setup** to proceed to the **Setup Completion** screen.

2.5 EasyConnect: Setup Completion

Use this screen to save your changes to the CODA-4x8x's EasyConnect configuration.

Click **Confirm Setup** in the **EasyConnect: Wireless Settings** screen. The following screen displays.

Figure 12: The EasyConnect: Setup Completion Screen

If you are happy with the settings, click **Complete my setup**.

NOTE: If you changed settings, make sure you keep a note of the new details.

Alternatively, click a setting's **Edit** link to modify it before clicking **Complete my setup**.

3

Status

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

NOTE: For background information on the concepts discussed in the **Wireless Status** screen, see Wireless Overview on page 81.

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 CODA-4x8x 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 CODA-4x8x:

- The public network (Wide Area Network or WAN) is the link between the cable connector and your Internet Service Provider. Your CODA-4x8x's IP address on this network is assigned by your service provider.

- The private network 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 CODA-4x8x 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 5: 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 CODA-4x8x'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 6: 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 7: 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 23 for more information.

By default, the CODA-4x8x 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 CODA-4x8x 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 CODA-4x8x via one of the **LAN** ports) and also has a wireless card (to connect to your CODA-4x8x over the wireless interface) the MAC addresses of the two cards will be different. In the case of the CODA-4x8x, each internal module (cable modem module, Ethernet module, wireless module, etc.) possesses its own MAC address.

3.1.6 Routing Mode

When your CODA-4x8x 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 CODA-4x8x on the WAN, and all traffic for LAN computers is sent to that IP address. The CODA-4x8x 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 CODA-4x8x in routing mode, each computer on the LAN must be assigned an IP address in the CODA-4x8x's subnet manually.

When the CODA-4x8x is not in routing mode, the service provider assigns an IP address to each computer connected to the CODA-4x8x directly. The CODA-4x8x 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 CODA-4x8x's configuration file.

3.1.7 Configuration Files

The CODA-4x8x's configuration (or config) file is a document that the CODA-4x8x obtains automatically over the Internet from the service provider's server, which specifies the settings that the CODA-4x8x 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 CODA-4x8x, and "upstream" refers to traffic from the CODA-4x8x 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.

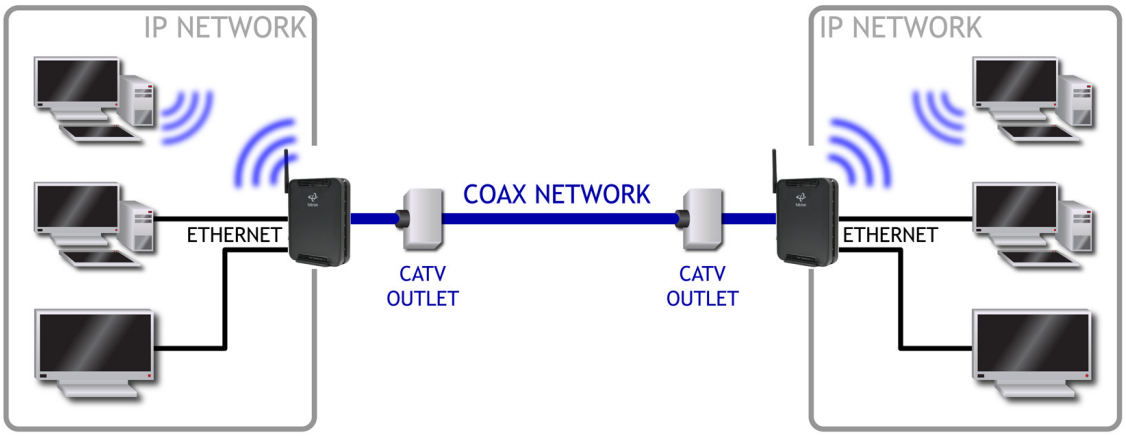
3.1.12 The Multimedia over Coax Alliance

The Multimedia over Coax Alliance (MoCA) is a non-profit technology alliance, which defines a set of specifications for the delivery of high-speed data, such as HD video, over your building's existing co-axial cabling network. Co-axial, or coax (pronounced "ko-axe") cable is already incorporated into most buildings for the transmission of RF signals, traditionally for relaying television broadcasts from a TV antenna, satellite or cable box to individual televisions around the building.

MoCA devices allow you use the coax cable network as an extension of your building's existing IP network, which includes both wired (Ethernet) and wireless (WiFi) traffic. Because they bridge the two networks, they are known as Ethernet-to-Coax Bridges, or ECBs.

NOTE: The Hitron device in the following diagrams are illustrative only, and may not resemble your device.

Figure 13: Bridging the Gap Between IP and Coaxial Networks



MoCA traffic on the coax network does not interfere with existing broadcasts from cable, telco, IPTV or satellite service providers, as it makes use of a previously-unused segment of the RF spectrum. The medium is ideal for real-time applications, providing high data throughput (100Mbps~1Gbps) with low latency, jitter or data loss. Also, coax cabling is generally better-shielded than IP networking media, especially wireless.

Applications to which MoCA networking is well-suited include:

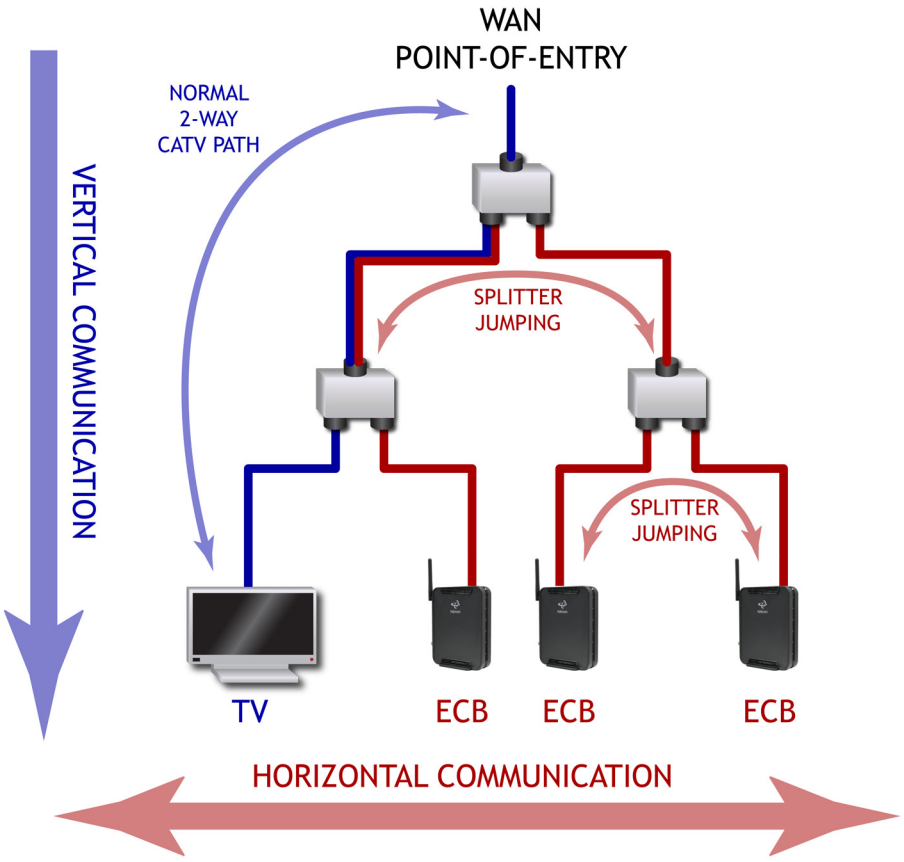
- Video on Demand (VoD)
- Multi-room, multi-camera Digital Video Recording (DVR)
- Gaming (LAN or online multiplayer)
- Internet video
- Home automation
- Video conferencing

3.1.12.1 Horizontal vs. Vertical Communications

Unlike traditional coax networking (TV, satellite, IPTV, etc.) MoCA devices do not need to receive data from a single source. It is "outlet-to-outlet". Each MoCA network uses a Network Controller (NC) to manage the network's communications, but any ECB on the network is capable of acting as the NC. By default, the NC is chosen by negotiation between all ECBs on the network, based on factors such as signal strength.

"Outlet-to-outlet" communications are also known as "splitter jumping". Traditional cable networking commonly utilized splitters to split a single incoming signal into two outgoing signals. With MoCA, communications between devices connected to each splitter output are possible. For this reason, MoCA communications can be considered "horizontal", as opposed to traditional "vertical" cable communications.

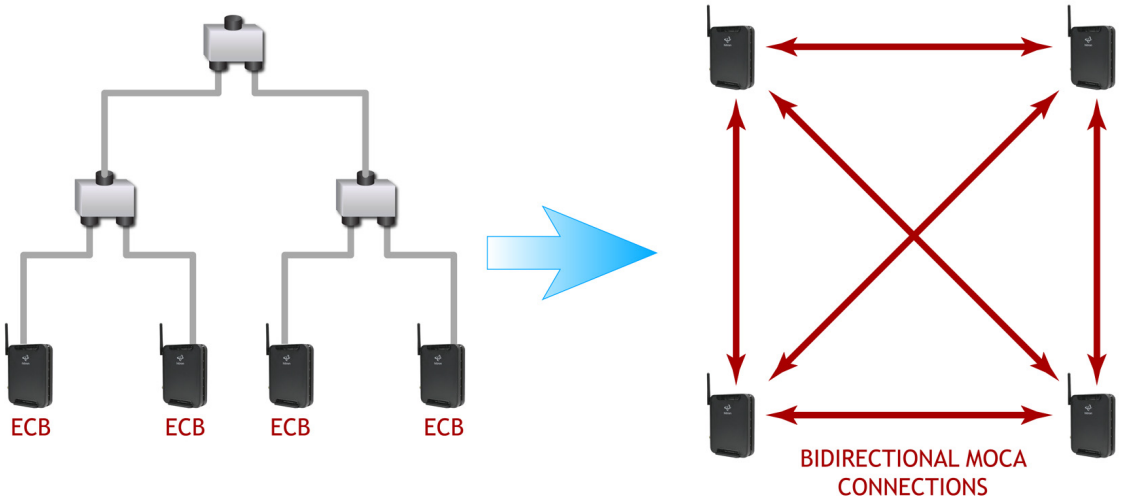
Figure 14: Traditional Vertical CATV vs. Horizontal MoCA Networking



3.1.12.2 Example MoCA Mesh Network

MoCA devices form a full "mesh", or peer-to-peer network (where all devices communicate directly with one another). In the following example, four MoCA devices connect directly to and from one another, via ECBs, forming 12 unique MoCA links (or 6 bidirectional links).

Figure 15: Example MoCA Peer-to-Peer Network



3.1.13 OFDM

Orthogonal Frequency-Division Multiplexing (OFDM) is a physical-layer data encoding method for transmitting and receiving data on Radio Frequency (RF) media, such as the CODA-4x8x's cable connection.

OFDM takes a single wide-band signal and separates it into multiple simultaneous subcarriers across the available RF spectrum, separated by the minimum frequency necessary to ensure non-interference among sub-carriers. "Orthogonal", in this usage, refers to this non-interfering quality of the technique.

The primary advantage of OFDM is that a signal encoded using the method can withstand suboptimal conditions on the RF medium. Depending on its implementation, OFDM can also enable faster signal throughput.

3.1.14 FFT

The Fast Fourier Transform (FFT) is an algorithm for rapidly implementing Fourier analysis of a data stream, used by modulation methods such as OFDM. Fourier analysis is a mathematical technique that enables the representation of data using simpler trigonometric functions.

In this implementation, Fourier analysis is used to construct the frequency data for transmission, and to deconstruct received frequency data.

3.1.15 OFDMA

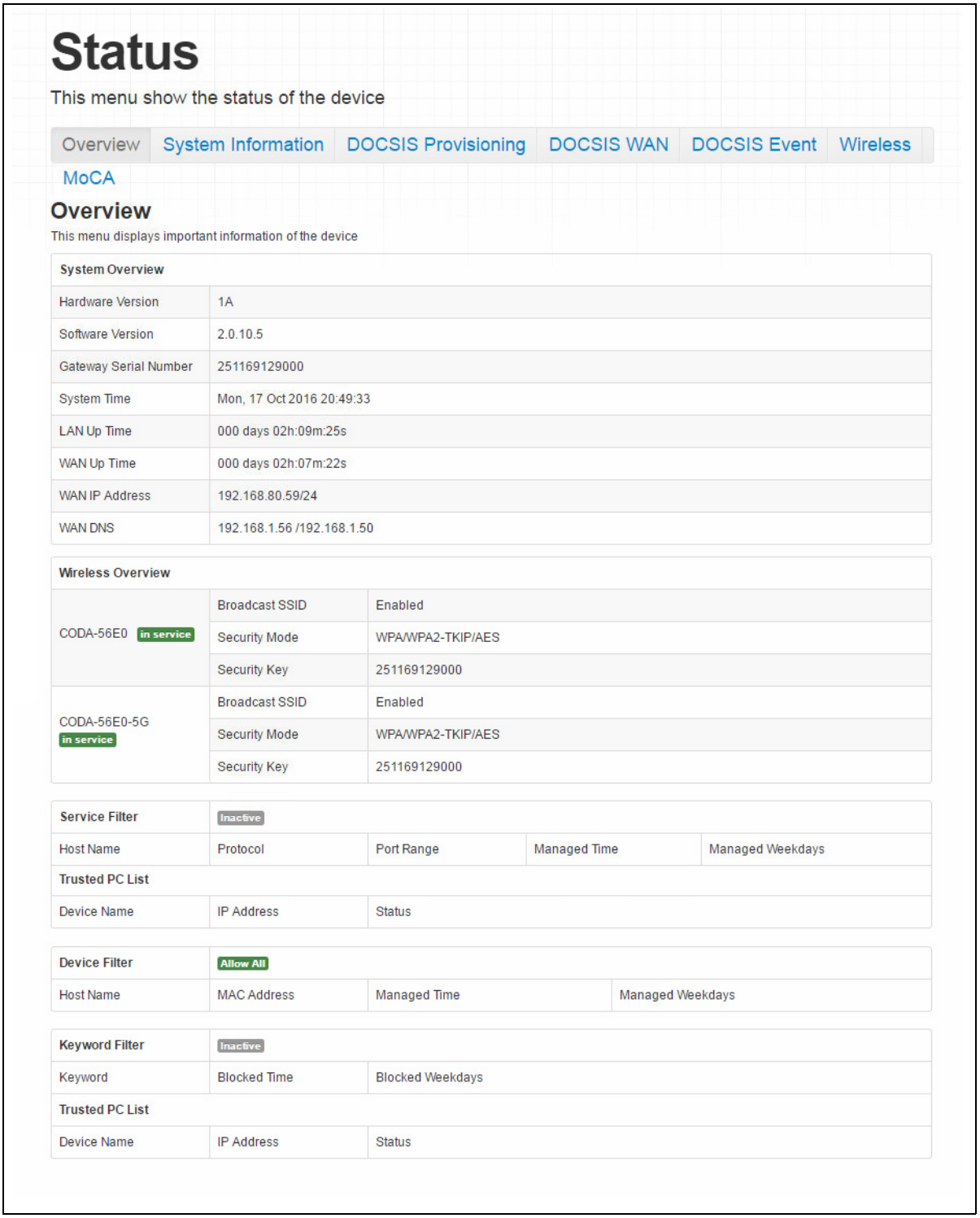
Orthogonal Frequency-Division Multiple Access (OFDMA) is a multiuser adaptation of OFDM (see OFDM on page 28) that permits simultaneous use by multiple users by assigning a specific group of OFDM subcarriers to each individual user.

3.2 The Status: Overview Screen

Use this screen to view information about the CODA-4x8x's system, wireless and filtering configuration and statistics.

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

Figure 16: The Status: Overview Screen



Status

This menu show the status of the device

Overview | System Information | DOCSIS Provisioning | DOCSIS WAN | DOCSIS Event | Wireless | MoCA

Overview

This menu displays important information of the device

System Overview	
Hardware Version	1A
Software Version	2.0.10.5
Gateway Serial Number	251169129000
System Time	Mon, 17 Oct 2016 20:49:33
LAN Up Time	000 days 02h:09m:25s
WAN Up Time	000 days 02h:07m:22s
WAN IP Address	192.168.80.59/24
WAN DNS	192.168.1.56 /192.168.1.50

Wireless Overview		
CODA-56E0 in service	Broadcast SSID	Enabled
	Security Mode	WPA/WPA2-TKIP/AES
	Security Key	251169129000
CODA-56E0-5G in service	Broadcast SSID	Enabled
	Security Mode	WPA/WPA2-TKIP/AES
	Security Key	251169129000

Service Filter	Inactive			
Host Name	Protocol	Port Range	Managed Time	Managed Weekdays
Trusted PC List				
Device Name	IP Address	Status		

Device Filter	Allow All		
Host Name	MAC Address	Managed Time	Managed Weekdays

Keyword Filter	Inactive	
Keyword	Blocked Time	Blocked Weekdays
Trusted PC List		
Device Name	IP Address	Status

The following table describes the labels in this screen.

Table 8: The Status: Overview Screen

System Overview	
Hardware Version	This displays the version number of the CODA-4x8x's physical hardware.
Software Version	This displays the version number of the software that controls the CODA-4x8x.
Gateway Serial Number	This displays the uniquely identifying number of the CODA-4x8x. If you contact your cable service provider for assistance, they may ask you for this number.
System Time	This displays the current date and time.
LAN Uptime	This displays the number of days, hours, minutes and seconds since the CODA-4x8x's LAN interface came online.
WAN Uptime	This displays the number of days, hours, minutes and seconds since the CODA-4x8x's WAN interface came online.
WAN IP Address	This displays the IP address automatically assigned to the CODA-4x8x's WAN interface, through which it connects to the Internet.
WAN DNS	This displays the IP addresses the CODA-4x8x uses for the Domain Name Service on the WAN interface.
Wireless Overview NOTE: This section contains information about your CODA-4x8x's wireless networks. The first line displays information about the 2.4 GHz wireless network, and the second line displays information about the 5 GHz wireless network.	
(2.4 GHz wireless network name)	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.
Security Mode	This displays the type of security the CODA-4x8x's 2.4 GHz wireless network is currently using.
Security Key	This displays the password for the CODA-4x8x's 2.4 GHz wireless network.

Table 8: The Status: Overview Screen (continued)

(2.4 GHz wireless network name)	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.
Security Mode	This displays the type of security the CODA-4x8x's 5 GHz wireless network is currently using.
Security Key	This displays the password for the CODA-4x8x's 5 GHz wireless network.
Service Filter	This field displays the filter status.
Host Name	This displays the name of each network device in the list.
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 Time	This displays the start (**From**) and end (**To**) of the time period during which this rule applies, on the specified **Managed Weekdays**.
Managed Weekdays	This displays the days of the week on which this rule applies.
Trusted PC List	
Device Name	This displays the arbitrary name of each trusted PC you configured, which will be exempt from the service filter rules.
IP Address	This displays the IP address of each trusted PC.
Status	This displays whether the device is currently trusted (**Enabled**) or untrusted (**Disabled**).
Device Filter	This field displays the filter status.
Host Name	This displays the name of each network device connected on the LAN.

Table 8: The Status: Overview Screen (continued)

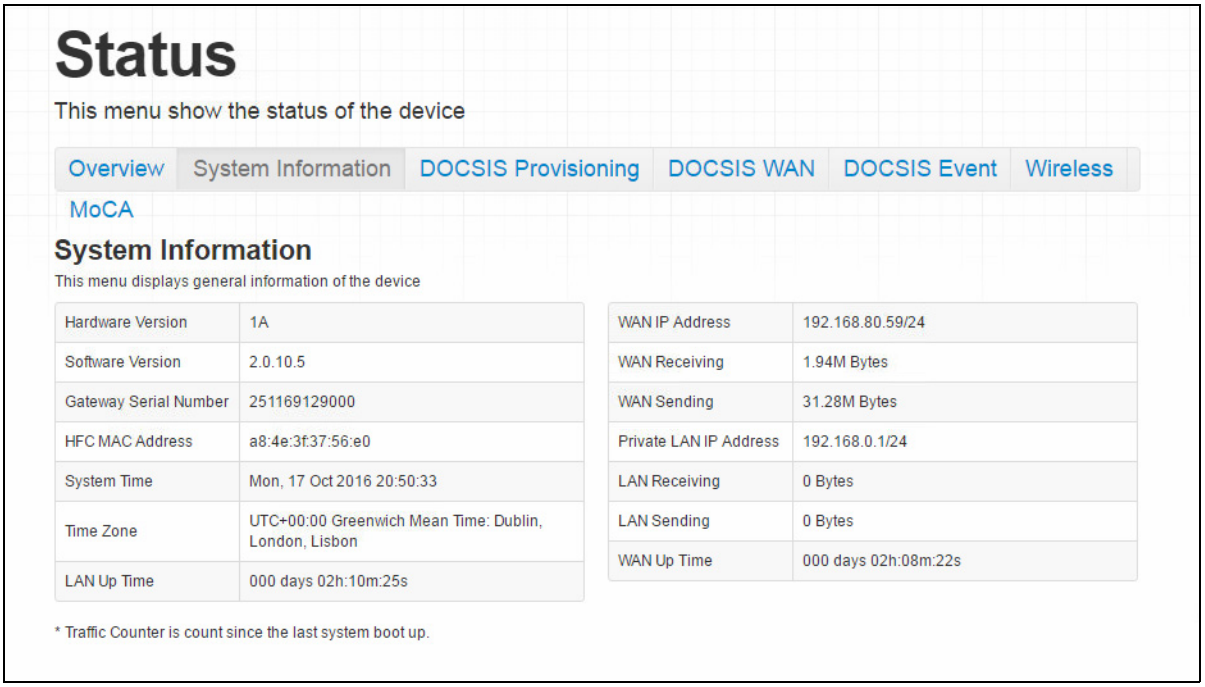
MAC Address	This displays the Media Access Control (MAC) address of each network device connected on the LAN. Each networking device has a MAC address, which uniquely identifies it.
Managed Time	This displays the start (**From**) and end (**To**) of the time period during which this rule applies, on the specified **Managed Weekdays**.
Managed Weekdays	This displays the days of the week on which this rule applies.
Keyword Filter	This field displays the filter status.
Keyword	This displays the keyword to be blocked. The CODA-4x8x examines both the page's URL (Internet address) and its page content (text).
Blocked Time	This displays the times at which the keyword will be blocked.
Blocked Weekdays	This displays the days on which the keyword will be blocked.
Trusted PC List	
Device Name	This displays the arbitrary name of each trusted PC you configured, which will be exempt from the keyword filter rules.
IP Address	This displays the IP address of each trusted PC.
Status	This displays whether the device is currently trusted (**Enabled**) or untrusted (**Disabled**).

3.3 The System Information Screen

Use this screen to see general information about your CODA-4x8x's hardware, its software, and its connection to the Internet.

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

Figure 17: The Status: System Information Screen



The following table describes the labels in this screen.

Table 9: The Status: System Information Screen

Hardware Version	This displays the version number of the CODA-4x8x's physical hardware.
Software Version	This displays the version number of the software that controls the CODA-4x8x.
Gateway Serial Number	This displays a number that uniquely identifies the device.
HFC MAC Address	This displays the Media Access Control (MAC) address of the CODA-4x8x's Hybrid-Fiber Coax (HFC) module. This is the module that connects to the Internet through the **CATV** connection.
System Time	This displays the current date and time.
Time Zone	This displays the time zone in which the CODA-4x8x is located.
LAN Up Time	This displays the amount of time that has elapsed since the CODA-4x8x's Local Area Network connection was last restarted.
WAN IP Address	This displays the CODA-4x8x's WAN IP address. This IP address is automatically assigned to the CODA-4x8x

Table 9: The Status: System Information Screen (continued)

WAN Receiving	This displays the amount of data received over the WAN connection since the device was last started.
WAN Sending	This displays the amount of data transmitted over the WAN connection since the device was last started.
Private LAN IP Address	This displays the CODA-4x8x's LAN subnet's IP information.
LAN Receiving	This displays the amount of data received over the LAN connection since the device was last started.
LAN Sending	This displays the amount of data transmitted over the LAN connection since the device was last started.
WAN Up Time	This displays the amount of time that has elapsed since the CODA-4x8x's Wide Area Network connection was last restarted.

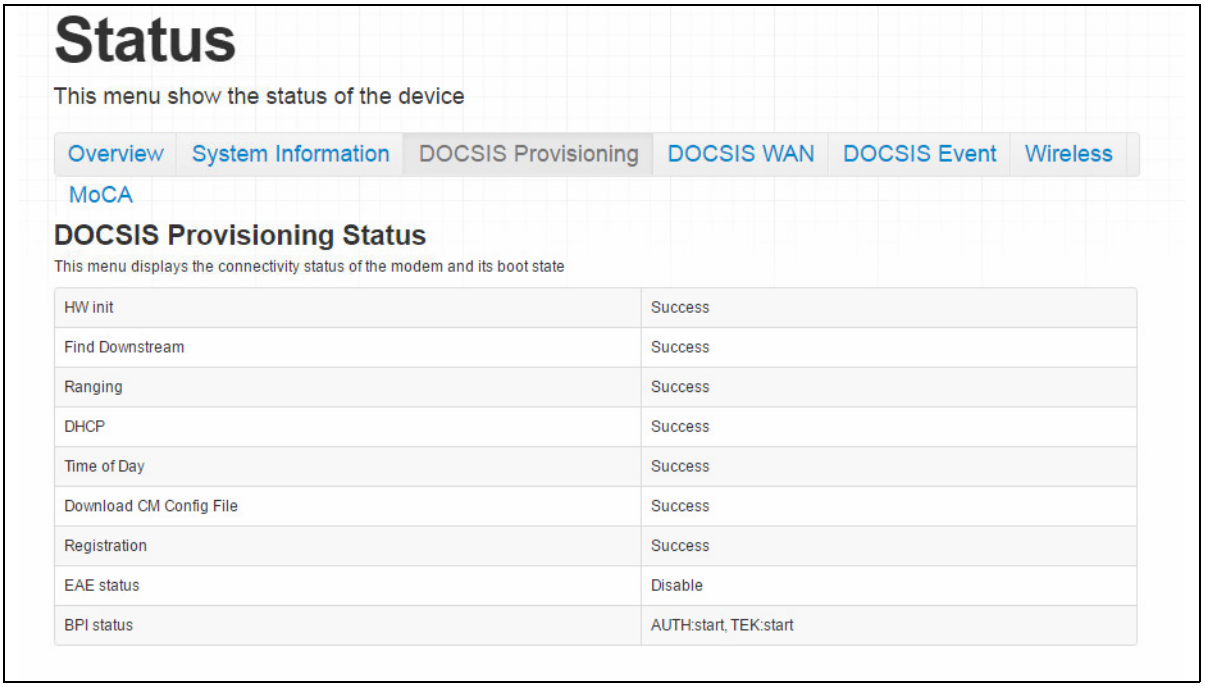
3.4 The Status: DOCSIS Provisioning Screen

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 CODA-4x8x 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.

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

Figure 18: The Status: DOCSIS Provisioning Screen



For each step:

- **Process** displays when the CODA-4x8x is attempting to complete a connection step.
- **Success** displays when the CODA-4x8x has completed a connection step.
- **Disable** displays when the relevant feature has been turned off.

3.5 The Status: DOCSIS WAN Screen

Use this screen to discover information about:

- The nature of the upstream and downstream connection between the CODA-4x8x and the device to which it is connected through the **CABLE** interface.
- IP details of the CODA-4x8x's WAN connection.

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

Figure 19: The Status: DOCSIS WAN Screen

Status

This menu show the status of the device

Overview | System Information | DOCSIS Provisioning | DOCSIS WAN | DOCSIS Event | Wireless | MoCA

DOCSIS WAN

This menu displays both upstream and downstream signal parameters

DOCSIS Overview

Network Access	Permitted
IP Address	192.168.50.34
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.50.254
DHCP Lease Time	D: 00 H: 01 M: 00 S: 00

Downstream Overview

Port ID	Frequency (Hz)	Modulation	Signal strength (dBmV)	Channel ID	Signal noise ratio (dB)	Octets	Correcteds	Uncorrectables
1	465000000	256QAM	11.100	536870912	43.377	355249373	0	0
2	471000000	256QAM	12.600	553648128	43.377	354090715	0	0
3	477000000	256QAM	12.900	570425344	43.377	354096623	0	0
4	483000000	256QAM	12.100	587202560	43.377	354081892	0	0
5	489000000	256QAM	11.500	603979776	43.377	354097065	0	0
6	495000000	256QAM	10.600	620756992	43.377	354102201	0	0
7	501000000	256QAM	10.100	637534208	40.946	354107334	1	0
8	507000000	256QAM	10.500	654311424	43.377	354087493	0	0

Reset FEC Counters

OFDM Downstream Overview

Receiver	FFT type	Subcarr 0 Frequency(MHz)	PLC locked	NCP locked	MDC1 locked	PLC power(dBmv)
0	NA	NA	NO	NO	NO	NA
1	NA	NA	NO	NO	NO	NA

Upstream Overview

Port ID	Frequency (Hz)	Modulation	Signal strength (dBmV)	Channel ID	BandWidth
1	38500000	ATDMA - 64QAM	43.250	3	1600000
2	40200000	ATDMA - 64QAM	43.250	4	1600000
3	36800000	ATDMA - 64QAM	43.250	2	1600000
4	35100000	ATDMA - 64QAM	45.250	1	1600000

OFDM/OFDMA Overview

Channel Index	State	Iin Digital Att	Digital Att	BW (sc's*fft)	Report Power	Report Power1_6	FFT Size
0	DISABLED	0.5000	0.0000	0.0000	-inf	-1.0000	4K
1	DISABLED	0.5000	0.0000	0.0000	-inf	-1.0000	4K

The following table describes the labels in this screen.

Table 10: The Status: DOCSIS WAN Screen

DOCSIS Overview	
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.
IP Address	This displays the CODA-4x8x's WAN IP address. This IP address is automatically assigned to the CODA-4x8x
Subnet Mask	This displays the CODA-4x8x's WAN subnet mask.
Gateway IP	This displays the IP address of the device to which the CODA-4x8x is connected on the WAN.
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 CODA-4x8x.	
Port ID	This displays the ID number of the downstream connection's port.
Frequency (Hz)	This displays the actual frequency in Hertz (Hz) of each downstream data channel to which the CODA-4x8x 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 CODA-4x8x is connected, in dBmV (decibels above/below 1 millivolt).
Channel ID	This displays the ID number of each channel on which the downstream signal is transmitted.
Signal Noise Ratio (dB)	This displays the Signal to Noise Ratio (SNR) of each downstream data channel to which the CODA-4x8x is connected, in dB (decibels).
Octets	This displays the total number of octets received.

Table 10: The Status: DOCSIS WAN Screen (continued)

Correcteds	This displays the number of blocks received that required correction due to corruption, and were corrected.
Uncorrectables	This displays the number of blocks received that required correction due to corruption, but were unable to be connected.
Reset FEC Counters	Click this to return the Forward Error Connection (FEC) columns (**Correcteds** and **Uncorrectables**).
OFDM Downstream Overview	
Receiver	This displays the index number of the OFDM receiver (see OFDM on page 43).
FFT Type	This displays the type of Fast Fourier Transform in use on the relevant OFDM receiver (see FFT on page 43).
Subcarr 0 Frequency (Hz)	Each OFDM signal consists of multiple subcarriers.This displays the frequency, in Hertz, of the first OFDM subcarrier on the relevant receiver.
PLC Locked	This displays whether or not the relevant OFDM connection's physical link channel (PLC) data is locked. The PLC tells the CODA-4x8x how to decode the OFDM signal, and what power level to use. Once the CODA-4x8x receives a PLC without uncorrectable errors, the PLC is locked and subsequent communication can continue.
NCP Locked	This displays whether or not the relevant OFDM connection's next codeword pointer (NCP) data is locked. The NCP tells the CODA-4x8x which codewords are to be used for OFDM communication, and which profile to use for each codeword. Once the CODA-4x8x receives an NCP without uncorrectable errors, the NCP is locked and subsequent communication can continue.
MDC1 Locked	This displays whether or not the relevant OFDM connection's Multipath Delay Commutator (MDC) data is locked. This provides information about the method of Fast Fourier Transform (FFT) to be used on the OFDM connection. Once the CODA-4x8x receives an MDC1 without errors, the MDC1 is locked and subsequent communication can continue.
PLC Power (dBmV)	This displays the power level the CODA-4x8x has been instructed to use on the relevant OFDM connection by the physical link channel (PLC) data, in dBmV (decibels above/below 1 millivolt).

Table 10: The Status: DOCSIS WAN Screen (continued)

Upstream Overview NOTE: The upstream signal is the signal transmitted from the CODA-4x8x.	
Port ID	This displays the ID number of the upstream connection's port.
Frequency (Hz)	This displays the actual frequency in Hertz (Hz) of each upstream data channel to which the CODA-4x8x is connected.
Modulation	This displays the type of modulation that each upstream channel uses.
Signal Strength (dBmV)	This displays the power of the signal of each upstream data channel to which the CODA-4x8x is connected, in dBmV (decibels above/below 1 millivolt).
Channel ID	This displays the ID number of each channel on which the upstream signal is transmitted.
Bandwidth	This displays the maximum available bandwidth on the relevant channel.
OFDM/OFDMA Overview NOTE: This section of the GUI provides data about upstream channels.	
Channel Index	This displays the index number of the OFDM/OFDMA channel.
State	This displays whether or not the relevant channel is currently in use, or not. • **ENABLED** displays when the channel is in use. • **DISABLED** displays when the channel is not in use.
Lin Digital Att.	This displays the digital attenuation, or signal loss, of the transmission medium on which the channel's signal is carried, in decibels (dB).
Digital Att.	This displays the measured digital attenuation of the channel's signal, in decibels (dB). Digital attenuation is affected by the frequency of the signal; a higher-frequency signal will suffer more attenuation than a lower-frequency signal.

Table 10: The Status: DOCSIS WAN Screen (continued)

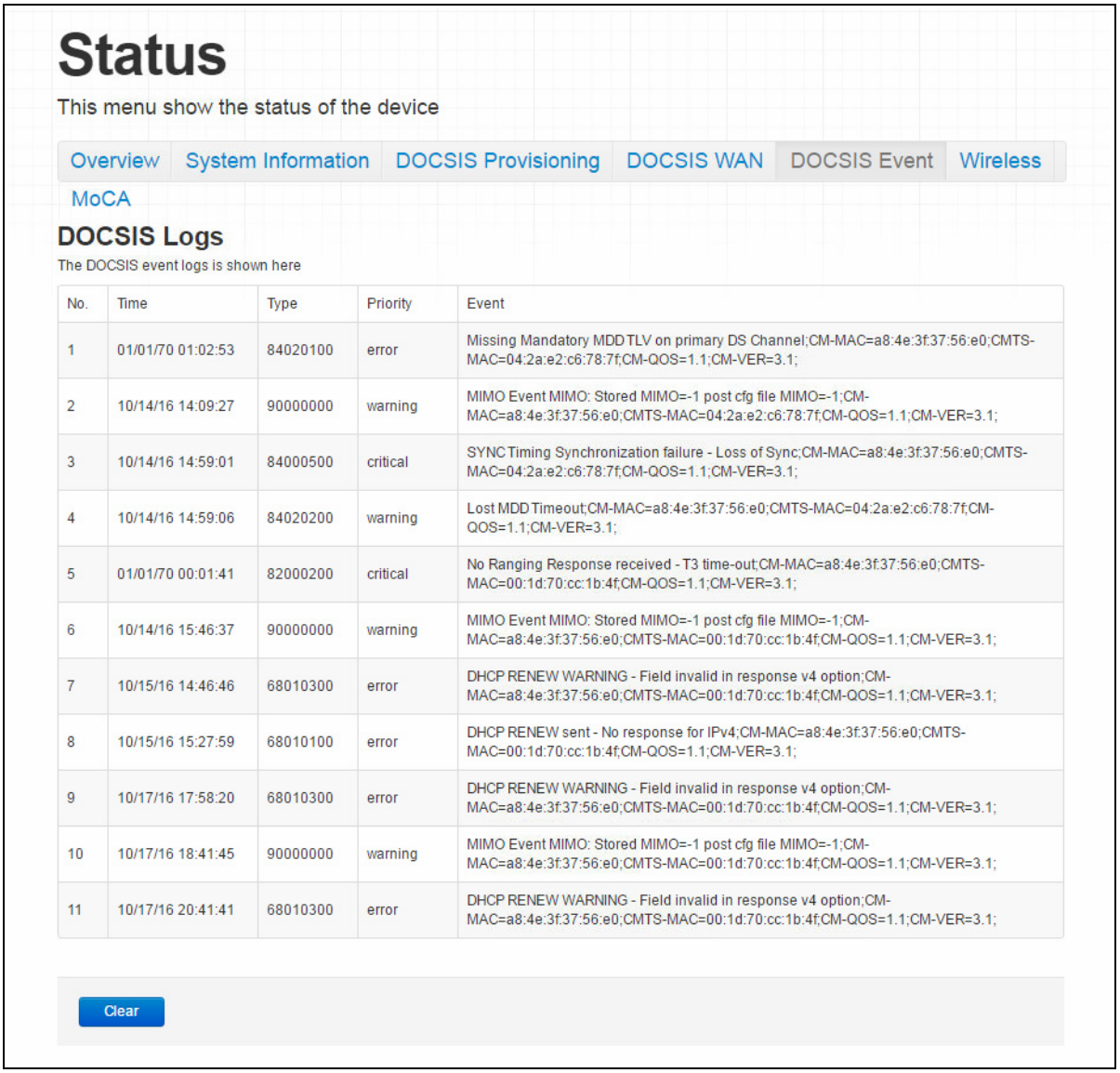
BW (sc's*fft)	This displays the bandwidth of the relevant channel, expressed as the number of subchannels multiplied by the channel's Fast Fourier Transform size, in megahertz (MHz).
Report Power	This displays the reported power of the relevant channel, in quarter-decibels above/below 1 millivolt (quarter-dBmV).
Report Power 1_6	This displays the target power (P1.6r_n, or power spectral density in 1.6MHz) of the relevant channel, in quarter-decibels above/below 1 millivolt (quarter-dBmV).
FFT Size	This displays the type of Fast Fourier Transform in use on the relevant channel.

3.6 The Status: DOCSIS Event Screen

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

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

Figure 20: The Status: DOCSIS Event Screen



The following table describes the labels in this screen.

Table 11: The Status: DOCSIS Event Screen

No	This displays the arbitrary, incremental index number assigned to the event.
Time	This displays the date and time at which the event occurred.
Type	This displays the nature of the event.
Priority	This displays the severity of the event.

Table 11: The Status: DOCSIS Event Screen (continued)

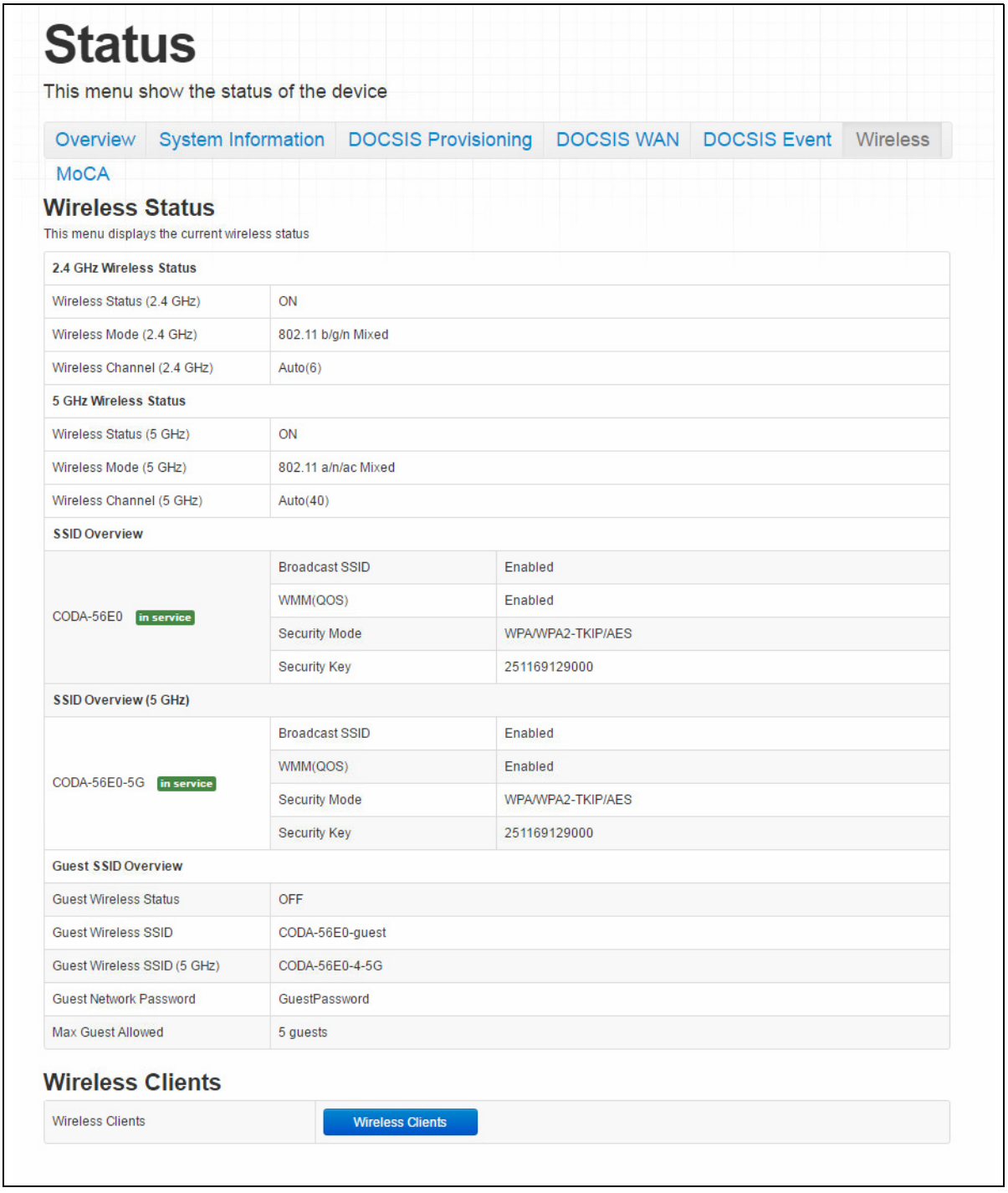
Event	This displays a description of the event.
Clear	Click this to remove all DOCSIS event logs from the system.

3.7 The Status: Wireless Screen

Use this screen to view information about the CODA-4x8x's wireless network.

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

Figure 21: The Status: Wireless Screen



Status

This menu show the status of the device

Overview | System Information | DOCSIS Provisioning | DOCSIS WAN | DOCSIS Event | Wireless | MoCA

Wireless Status

This menu displays the current wireless status

2.4 GHz Wireless Status		
Wireless Status (2.4 GHz)	ON	
Wireless Mode (2.4 GHz)	802.11 b/g/n Mixed	
Wireless Channel (2.4 GHz)	Auto(6)	
5 GHz Wireless Status		
Wireless Status (5 GHz)	ON	
Wireless Mode (5 GHz)	802.11 a/n/ac Mixed	
Wireless Channel (5 GHz)	Auto(40)	
SSID Overview		
CODA-56E0 in service	Broadcast SSID	Enabled
	WMM(QOS)	Enabled
	Security Mode	WPA/WPA2-TKIP/AES
	Security Key	251169129000
SSID Overview (5 GHz)		
CODA-56E0-5G in service	Broadcast SSID	Enabled
	WMM(QOS)	Enabled
	Security Mode	WPA/WPA2-TKIP/AES
	Security Key	251169129000
Guest SSID Overview		
Guest Wireless Status	OFF	
Guest Wireless SSID	CODA-56E0-guest	
Guest Wireless SSID (5 GHz)	CODA-56E0-4-5G	
Guest Network Password	GuestPassword	
Max Guest Allowed	5 guests	

Wireless Clients

Wireless Clients	Wireless Clients

The following table describes the labels in this screen.

Table 12: The Status: Wireless Screen

2.4G Wireless Status	
Wireless Status (2.4GHz)	This displays whether or not the CODA-4x8x's 2.4GHz wireless network is active.
Wireless Mode (2.4GHz)	This displays the type of wireless network that the CODA-4x8x's 2.4GHz network is using.
Wireless Channel (2.4GHz)	This displays the wireless channel on which the CODA-4x8x's 2.4GHz wireless network is transmitting and receiving.
5G Wireless Status	
Wireless Status (5GHz)	This displays whether or not the CODA-4x8x's 5GHz wireless network is active.
Wireless Mode (5GHz)	This displays the type of wireless network that the CODA-4x8x's 5GHz network is using.
Wireless Channel (5GHz)	This displays the wireless channel on which the CODA-4x8x's 5GHz wireless network is transmitting and receiving.
SSID Overview (2.4GHz)	
(SSID)	This displays the SSID (Service Set IDentifier) of the CODA-4x8x's 2.4GHz wireless network, and whether or not it is currently active.
Broadcast SSID	This displays whether the CODA-4x8x's 2.4GHz wireless network SSID is visible to client devices (**Enabled**) or not (**Disabled**).
WMM	This displays whether Wi-Fi Multimedia is active (**Enabled**) or inactive (**Disabled**) on the CODA-4x8x's 2.4GHz wireless network.
Security Mode	This displays the type of security and encryption method currently enabled on the CODA-4x8x's 2.4GHz wireless network.
Security Key	This displays the wireless security password for the CODA-4x8x's 2.4GHz wireless network.
SSID Overview (5GHz)	
(SSID)	This displays the SSID (Service Set IDentifier) of the CODA-4x8x's 5GHz wireless network, and whether or not it is currently active.

Table 12: The Status: Wireless Screen (continued)

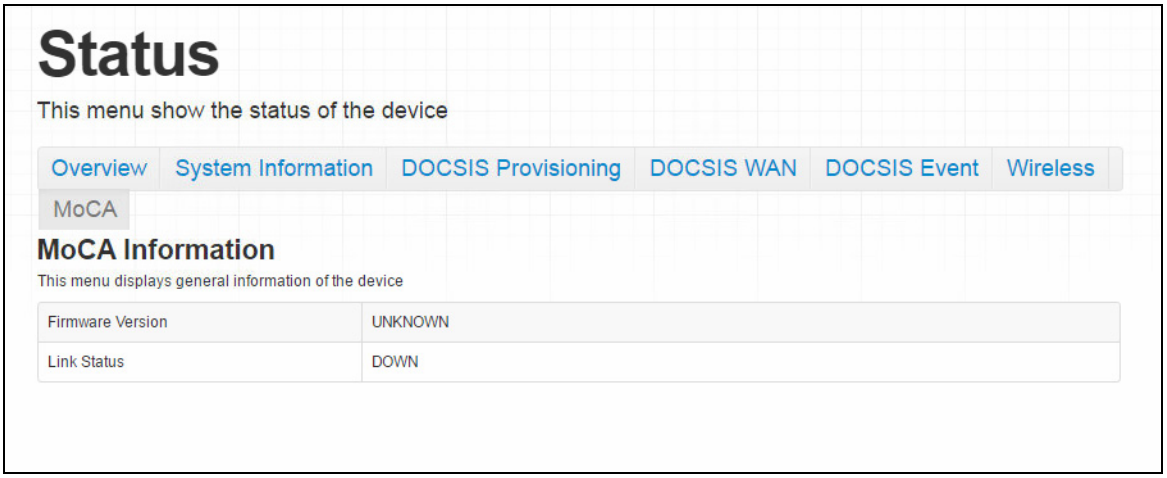
Broadcast SSID	This displays whether the CODA-4x8x's 5GHz wireless network SSID is visible to client devices (**Enabled**) or not (**Disabled**).
WMM	This displays whether Wi-Fi Multimedia is active (**Enabled**) or inactive (**Disabled**) on the CODA-4x8x's 5GHz wireless network.
Security Mode	This displays the type of security and encryption method currently enabled on the CODA-4x8x's 5GHz wireless network.
Security Key	This displays the wireless security password for the CODA-4x8x's 5GHz wireless network.
Guest SSID Overview	
Guest Wireless Status	This displays whether the guest wireless network is active (**ON**) or inactive (**OFF**).
Guest Wireless SSID	This displays the SSID (Service Set IDentifier) of the CODA-4x8x's 2.4GHz wireless guest network.
Guest Wireless SSID (5Ghz)	This displays the SSID (Service Set IDentifier) of the CODA-4x8x's 5GHz wireless guest network.
Guest Network Password	This displays the password of both the 2.4GHz and the 5GHz wireless guest networks.
Max Guest Allowed	This displays the maximum number of wireless devices that may connect to the wireless guest network at the same time.
Wireless Clients	
Wireless Clients	Click this to display a list of the wireless devices currently connected to the CODA-4x8x.

3.8 The Status: MoCA Screen

Use this screen to view general information about the CODA-4x8x's MoCA-related settings.

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

Figure 22: The Status: MoCA Screen



The following table describes the labels in this screen.

Table 13: The Status: MoCA Screen

Firmware Version	This displays the version number of the MoCA module's current firmware.
Link Status	This displays whether or not the CODA-4x8x is connected over the cable 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 The Domain Name System

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 (DNS). 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.

4.1.2 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 CODA-4x8x 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.

4.1.3 Port Triggering

Port triggering is a means of automating port forwarding. The CODA-4x8x 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 CODA-4x8x automatically opens the incoming ports specified in the rule, in anticipation of incoming traffic.

4.1.4 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.

4.1.5 Routing Mode

When your CODA-4x8x 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 CODA-4x8x on the WAN, and all traffic for LAN computers is sent to that IP address. The CODA-4x8x 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 CODA-4x8x in routing mode, each computer on the LAN must be assigned an IP address in the CODA-4x8x's subnet manually.

When the CODA-4x8x is not in routing mode, the service provider assigns an IP address to each computer connected to the CODA-4x8x directly. The CODA-4x8x does not perform any routing operations, and traffic flows between the computers and the service provider.

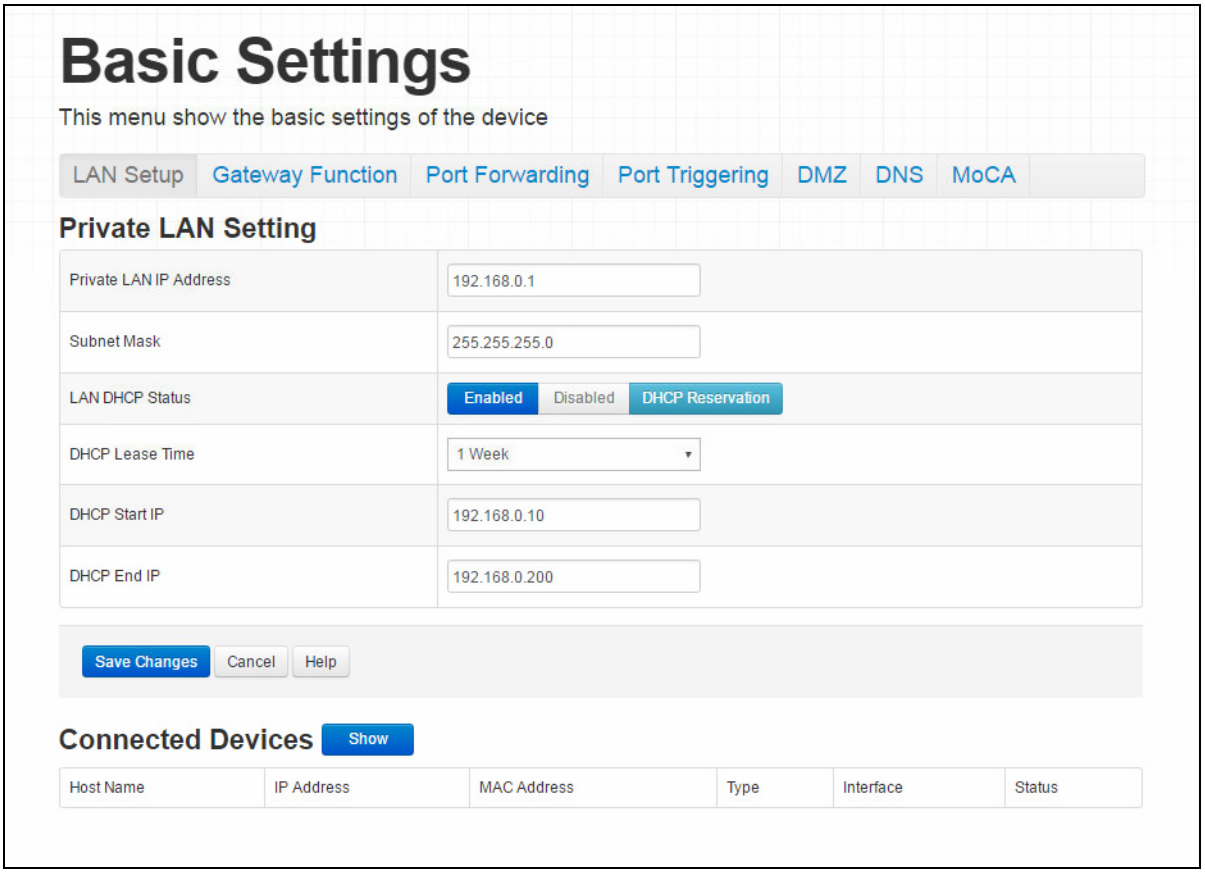
4.2 The Basic: LAN Setup Screen

Use this screen to:

- View information about the CODA-4x8x's connection to the WAN
- Configure the CODA-4x8x's internal DHCP server
- Define how the CODA-4x8x assigns IP addresses on the LAN
- See information about the network devices connected to the CODA-4x8x on the LAN.

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

Figure 23: The Basic: LAN Setup Screen



The following table describes the labels in this screen.

Table 14: The Basic: LAN Setup Screen

Private LAN Setting	
Private LAN IP Address	Use this field to define the IP address of the CODA-4x8x on the LAN.
Subnet Mask	Use this field to define the LAN subnet. Use dotted decimal notation (for example, **255.255.255.0**).
LAN DHCP Status	Use this field to configure whether or not the CODA-4x8x's DHCP server is active. ▸ To turn the DHCP server on, click **Enabled**. ▸ To turn the DHCP server off, click **Disabled**.
Lease Time	Use this to select 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.

Table 14: The Basic: LAN Setup Screen (continued)

DHCP Start IP	Use this field to specify the IP address at which the CODA-4x8x 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 CODA-4x8x 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.
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**).
Status	This displays **Active** when the connected computer is online, and **Inactive** when the connected computer is offline.
Refresh	Click this to refresh the information in this section.

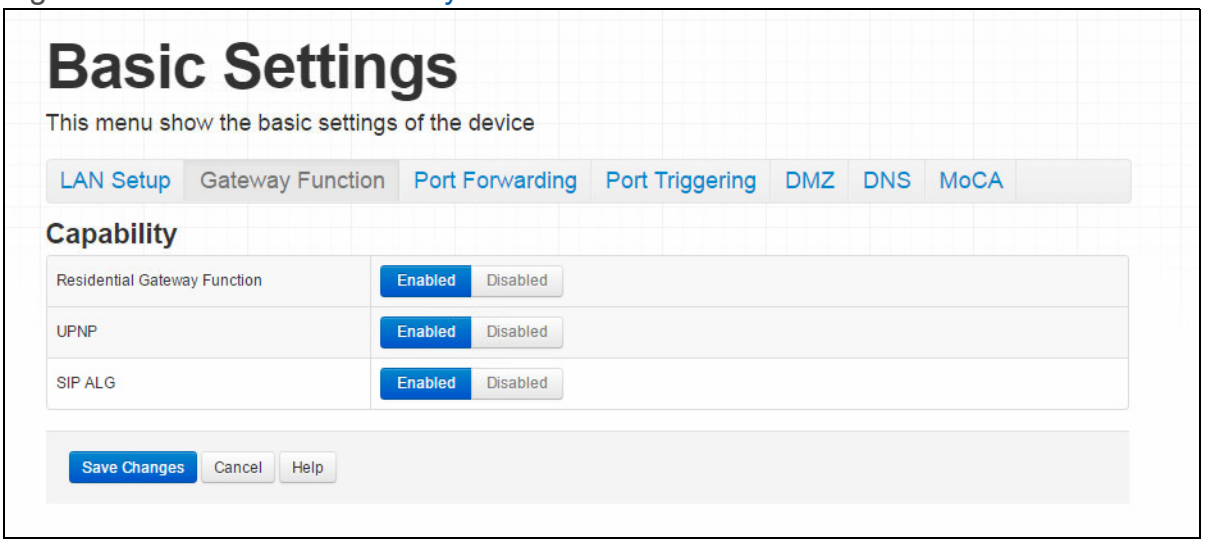
4.3 The Basic: Gateway Function Screen

Use this screen to enable or disable the CODA-4x8x's residential gateway, Universal Plug n Play (UPnP) and Session Initiation Protocol Application Layer Gateway (SIP ALG) functions.

Disabling the residential gateway feature sets the unit to use bridge mode only. Use this mode when your network is already using another router.

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

Figure 24: The Basic: Gateway Function Screen



The following table describes the labels in this screen.

Table 15: The Basic: Gateway Function Screen

Residential Gateway function	Select **Enabled** to turn on the CODA-4x8x's residential gateway features, or select **Disabled** to turn them off.
UPnP	Select **Enabled** to turn on the CODA-4x8x's Universal Plug n Play features, or select **Disabled** to turn them off.
SIP ALG	Select **Enabled** to turn on the CODA-4x8x's Session Initiation Protocol Application Layer Gateway for VoIP, or select **Disabled** to turn it off.
Save Changes	Click this to save your changes to the fields in this screen.

Table 15: The Basic: Gateway Function Screen (continued)

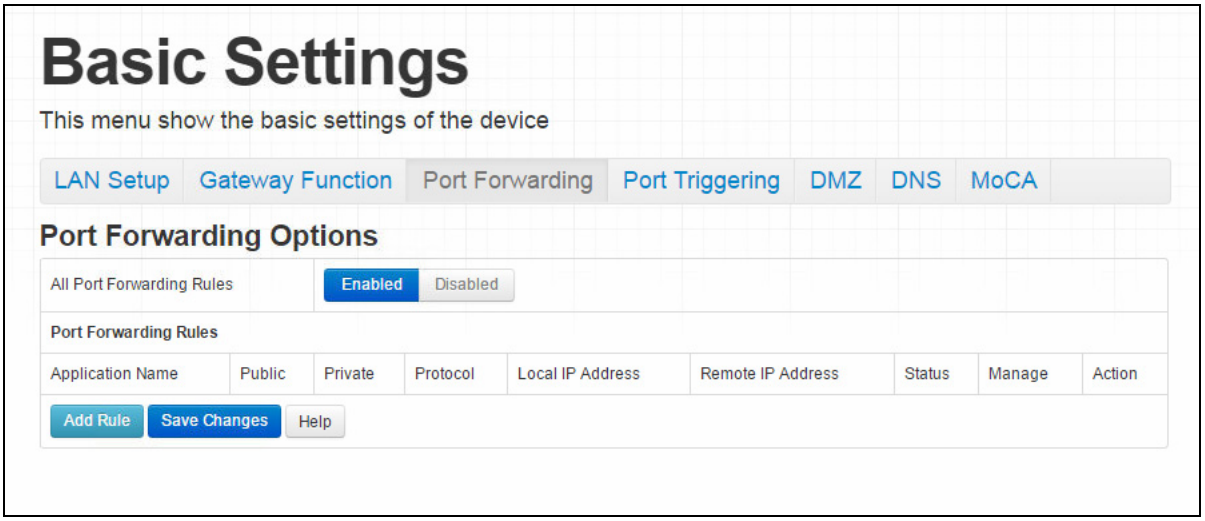
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

4.4 The Basic: Port Forwarding Screen

Use this screen to configure port forwarding between computers on the WAN and computers on the LAN. You can turn port forwarding on or off and configure new and existing port forwarding rules.

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

Figure 25: The Basic: Port Forwarding Screen



The following table describes the labels in this screen.

Table 16: 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	
Application Name	This displays the arbitrary name you assigned to the rule when you created it.

Table 16: The Basic: Port Forwarding Screen (continued)

Public Private	These fields display the ports to which the rule applies: ▸ The **Public** field displays the incoming port range. These are the ports on which the CODA-4x8x received traffic from the originating host on the WAN. ▸ The **Private** field displays the port range to which the CODA-4x8x 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 **Public Port Range** and **Protocol** conditions is forwarded.
Remote IP Address	This displays the IP address of the computer on the WAN from which traffic conforming to the **Public Port Range** and **Protocol** conditions is forwarded to the **Local IP Address**.
Status	Use this to turn the port forwarding rule on or off. ▸ Select **ON** to activate the port forwarding rule. ▸ Select **OFF** to deactivate the port forwarding rule.
Manage	Click this to make changes to the rule.
Action	Use this to delete the rule.
Add Rule	Click this to define a new port forwarding rule. See Adding or Editing a Port Forwarding Rule on page 71 for information on the screen that displays.
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.

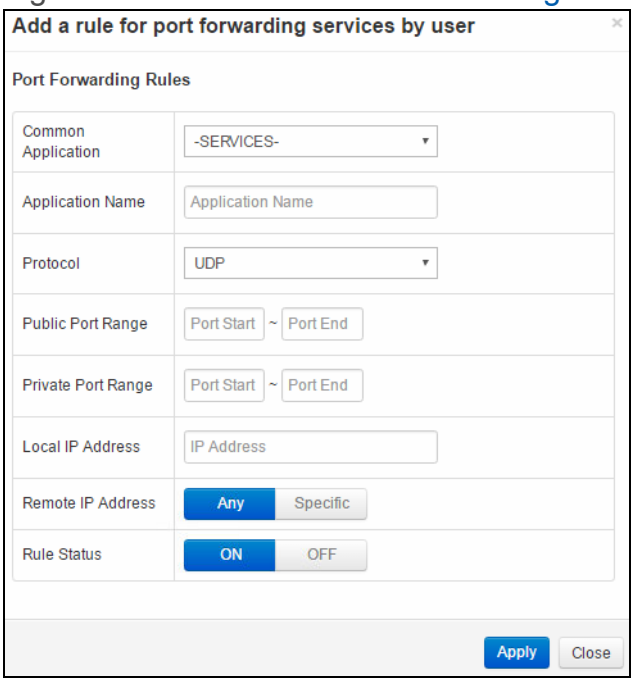
4.4.1 Adding or Editing a Port Forwarding Rule

- 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** > **Port 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 26: The Basic: Port Forwarding Add/Edit Screen



The following table describes the labels in this screen.

Table 17: 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.

Table 17: The Basic: Port Forwarding Add/Edit Screen

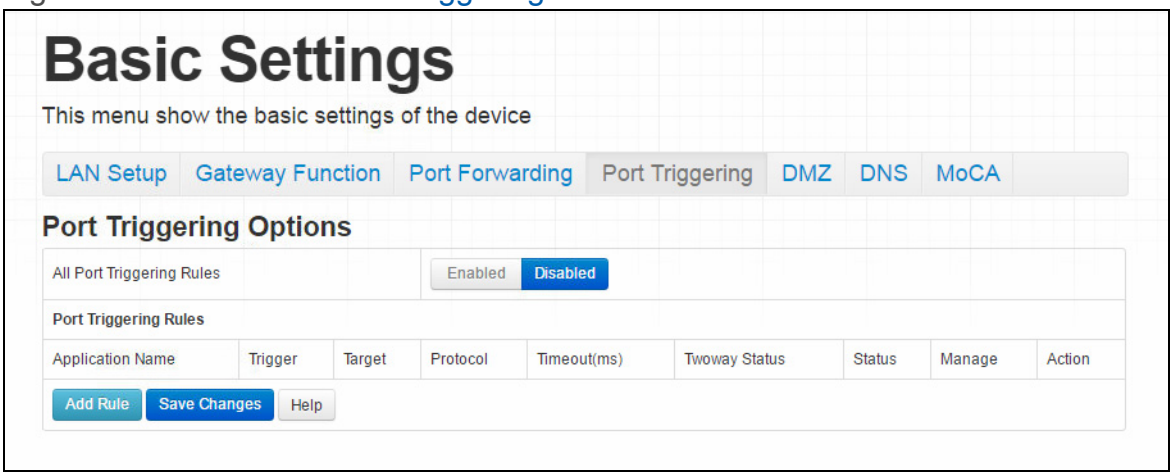
Protocol	Use this field to specify whether the CODA-4x8x should forward traffic via: • Transmission Control Protocol (**TCP**) • User Datagram Protocol (**UDP**) • Transmission Control Protocol and User Datagram Protocol (**TCP/UDP**) • Generic Routing Encapsulation (**GRE**) • Encapsulating Security Protocol (**ESP**) NOTE: If in doubt, leave this field at its default (**TCP/UDP**).
Public Port Range	Use these fields to specify the incoming port range. These are the ports on which the CODA-4x8x 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 CODA-4x8x 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.
Remote IP Address	Use this field to enter the IP address of the computer on the WAN from which you want to forward the traffic.
Rule Status	Select **ON** to enable this rule, or select **OFF** to disable it.
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 rule.

4.5 The Basic: 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 27: The Basic: Port Triggering Screen



The following table describes the labels in this screen.

Table 18: 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	
Application Name	This displays the name you assigned to the rule when you created it.
Trigger	This displays the range of outgoing ports. When the CODA-4x8x 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 CODA-4x8x 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**).

Table 18: The Basic: Port Triggering Screen (continued)

Timeout (ms)	This displays the time (in milliseconds) after the CODA-4x8x 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**.
Manage	Click this to make changes to the rule.
Action	Use this to delete the rule.
Add Rule	Click this to define a new port forwarding rule. See Adding or Editing a Port Forwarding Rule on page 71 for information on the screen that displays.
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.

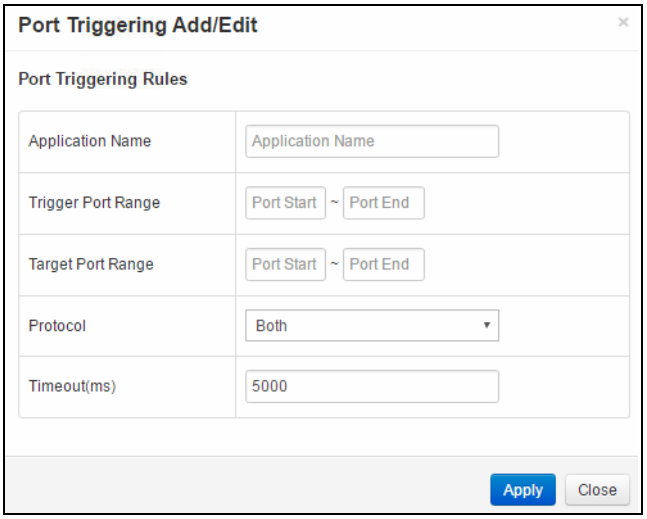
4.5.1 Adding or Editing a Port Triggering Rule

- 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 28: The Basic: Port Triggering Add/Edit Screen



The following table describes the labels in this screen.

Table 19: 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 CODA-4x8x 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 CODA-4x8x 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.

Table 19: The Basic: Port Triggering Add/Edit Screen

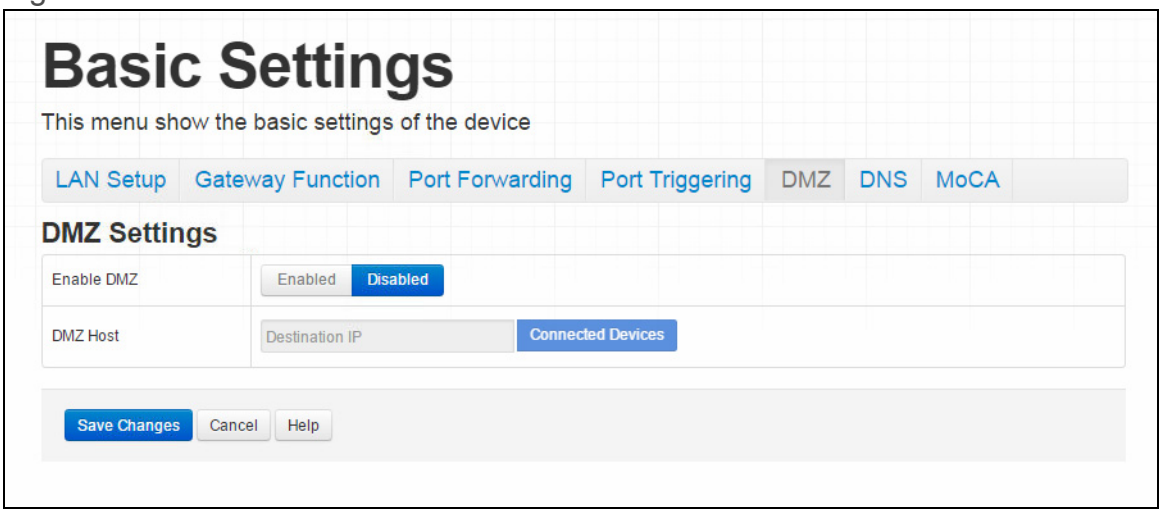
Protocol	Use this field to specify whether the CODA-4x8x should activate this trigger when it detects activity via: • Transmission Control Protocol (**TCP**) • User Datagram Protocol (**UDP**) • Transmission Control Protocol and User Datagram Protocol (**Both**) NOTE: If in doubt, leave this field at its default (**Both**).
Timeout (ms)	Enter the time (in milliseconds) after the CODA-4x8x opens the **Target** ports that it should close them.
Apply	Click this to save your changes to the fields in this screen.
Close	Click this to return to the **Port Triggering** screen without saving your changes to the rule.

4.6 The Basic: DMZ Screen

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

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

Figure 29: The Basic: DMZ Screen



The following table describes the labels in this screen.

Table 20: The Basic: DMZ Screen

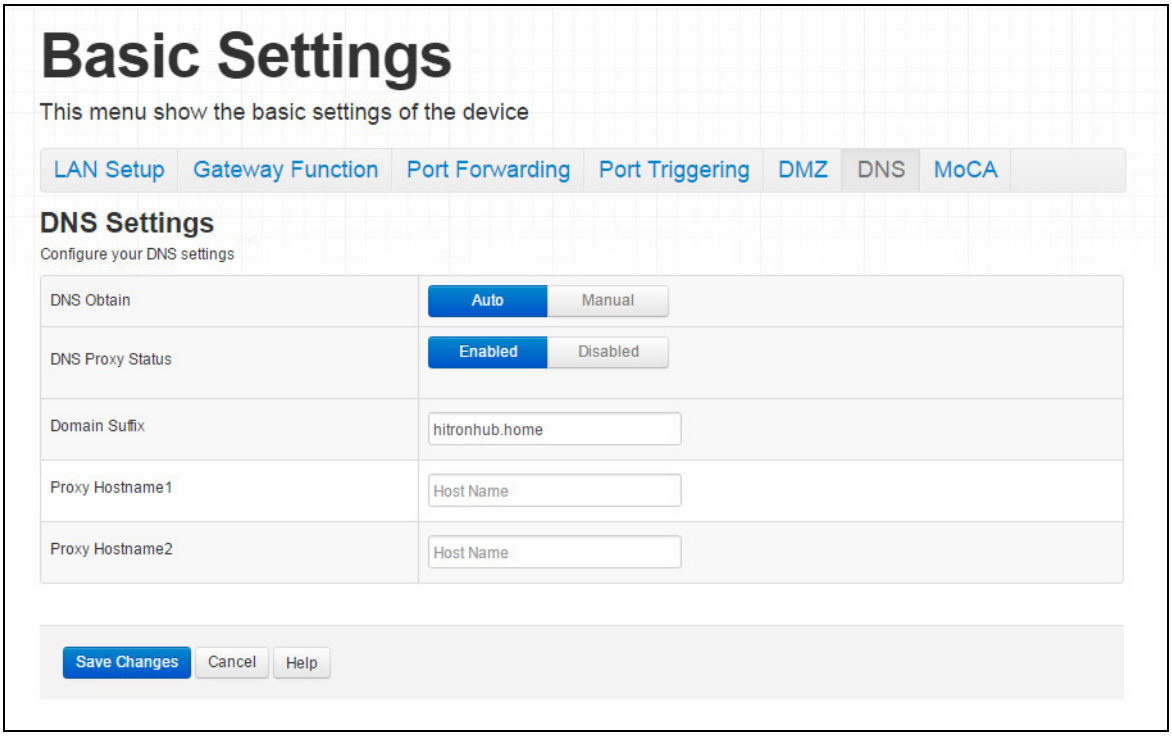
Enable DMZ	Use this field to turn the DMZ on or off. ▸ Select **Enabled** to turn the DMZ on. ▸ Select **Disabled** to turn the DMZ off. Computers that were previously in the DMZ are now on the LAN.
DMZ Host	Enter the IP address of the computer that you want to add to the DMZ.
Connected Devices	Click this to see a list of the computers currently connected to the CODA-4x8x 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 Basic: DNS Screen

Use this screen to configure the CODA-4x8x's LAN DNS settings, including its subnet mask, domain suffix and proxy hostname.

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

Figure 30: The Basic: DNS Screen



The following table describes the labels in this screen.

Table 21: The Basic: DNS Screen

DNS Obtain	Use this to select whether to obtain DNS information automatically over the network, or to define it manually. ▸ Select **Auto** to obtain DNS information automatically. ▸ Select **Manual** to obtain DNS information manually.
DNS Proxy Status	Use this to turn DNS proxy on or off on the LAN. When DNS proxy is turned on (default) the DHCP server provides the CODA-4x8x's LAN IP address as the DNS server for name resolution. ▸ Selected **Enabled** to turn DNS proxy on. ▸ Selected **Disabled** to turn DNS proxy off.

Table 21: The Basic: DNS Screen (continued)

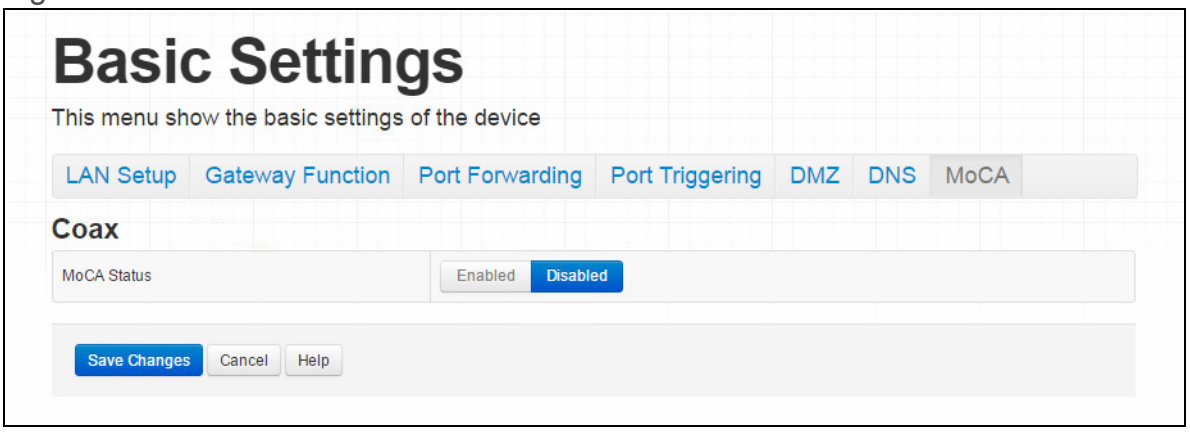
Domain Suffix	Use this field to define the domain that you can enter into a Web browser (instead of an IP address) to reach the CODA-4x8x on the LAN. NOTE: It is suggested that you make a note of your device's **Domain Suffix** in case you ever need to access the CODA-4x8x's GUI without knowledge of its IP address.
Proxy Hostname 1	When **LAN DNS Obtain** is set to **Manual**, enter the IP addresses of up to two computers for which you want to manually add to the DNS.
Proxy Hostname 2	
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 Basic: MoCA Screen

Use this screen to turn the CODA-4x8x's Multimedia over Cable Alliance (MoCA) features on or off.

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

Figure 31: The Basic: MoCA Screen



The following table describes the labels in this screen.

Table 22: The Basic: MoCA Screen

MoCA Status	▸ Select **Enabled** to turn the MoCA network off. ▸ Select **Disabled** to turn the MoCA network connection off.
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 CODA-4x8x'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 CODA-4x8x 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 CODA-4x8x is the access point, and the computers you connect to the CODA-4x8x are the wireless clients.

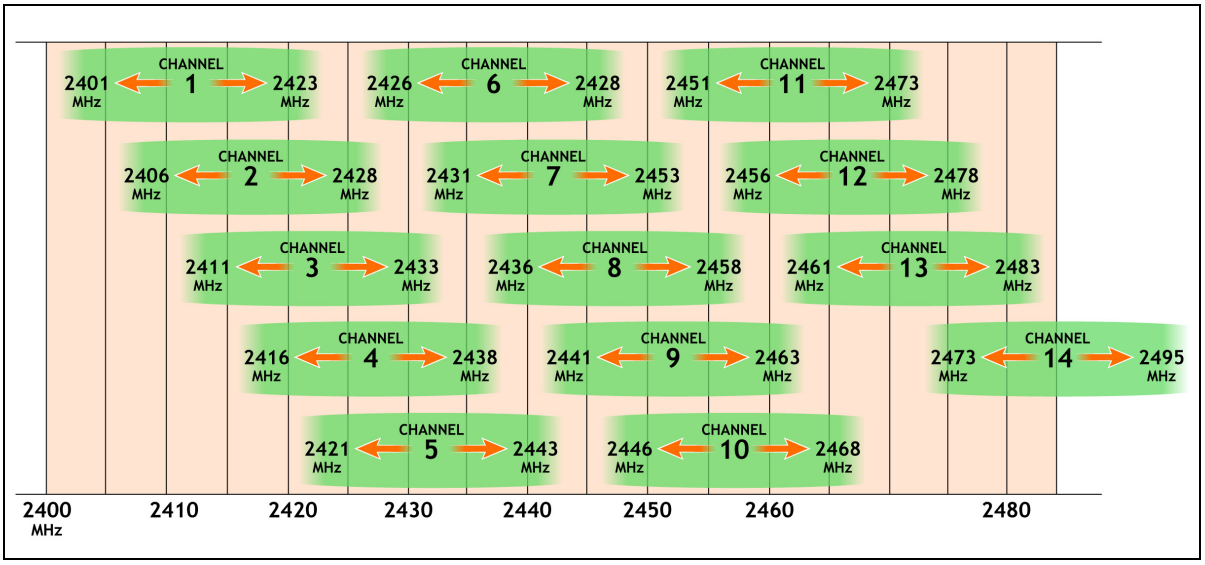
5.1.3 Wireless Frequency Ranges and Channels

Communication on the wireless network between the client and the access point takes place within specific ranges of the radio spectrum. The most common such ranges are 2400MHz ~ 2500MHz, known as the 2.4GHz band, and 5725MHz ~ 5875MHz, known as the 5GHz band.

These frequency ranges are themselves divided into multiple channels, in order to allow multiple networks to operate in the same location or overlapping locations. In a wireless network, the access point and its clients all communicate on the same radio channel.

In the 2.4GHz band, there are fourteen channels, although not all are available in all parts of the world; for instance, in North America only eleven are allowed. Each channel is 20MHz wide (although many devices can improve bandwidth by combining two channels into a single 40MHz channel) and each channel's center frequency is 5MHz greater than that of the previous channel. This means that channels overlap, potentially creating signal interference between networks competing in the same space. Therefore, selecting channels that are not used by neighboring devices, and as far as possible do not overlap with the channels ued by such devices, is important in order to minimize interference and maximize performance. The situation in the 5GHz band is more complex, but the same principles apply.

Figure 32: 2.4GHz Wireless Channel Overlap



5.1.3.1 Automatic Channel Selection

The CODA-4x8x's Automatic Channel Selection (ACS) feature enables the wireless module to scan the wireless network environment, discover the channel on which interference is least present, and use that channel automatically for wireless communications on the relevant network.

Environmental analysis and channel selection occurs when the CODA-4x8x's wireless network first starts (when the relevant wireless network's radio channel is already set to **Auto** mode), when **Auto** mode is first selected, when the **Refresh** button is pressed, or under certain specific circumstances when Dynamic Channel Change is enabled (see Dynamic Channel Change on page 84).

5.1.3.2 Band Steering

When wireless client devices are capable of operating on both the 2.4GHz band and the 5GHz band, it is generally desirable for them to connect to the CODA-4x8x on the 5GHz wireless network, due to the likelihood of there being less interference on that band. When enabled, band steering does this by detecting whether wireless clients are also 5GHz-capable and, if so, encouraging the client to connect on the 5GHz wireless network rather than the 2.4GHz wireless network.

5.1.3.3 Dynamic Channel Change

Dynamic Channel Change (DCC) improves strength and continuity of wireless signal even when environmental conditions change, by enabling Automatic Channel Selection (see Automatic Channel Selection on page 83) to be triggered when the current channel's interference reduces the data transmission rate below a threshold level.

NOTE: At the time of writing, the data transmission threshold level is 150Mbps; this is the bandwidth required to simultaneously transmit four high-definition video streams to the CODA-4x8x's wireless clients.

When DCC is enabled, a check of all available wireless channels is performed regularly. If the signal quality of the current channel deteriorates below the threshold level, the CODA-4x8x switches to a channel with superior signal quality.

NOTE: At the time of writing, the DCC check is performed sixty times a minute.

When environmental conditions mean there is no available channel with acceptable signal quality, DCC is automatically disabled if channel switching occurs too often in any period, in order to avoid the inconvenience of rapid unnecessary switching.

NOTE: At the time of writing, DCC is automatically disabled if automatic channel switching occurs more than three times in any five minute period.

NOTE: At the time of writing, DCC is only available on the 5GHz wireless network.

5.1.4 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 CODA-4x8x 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
- IEEE 802.11ac

5.1.5 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 CODA-4x8x 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).

5.1.6 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 CODA-4x8x supports the following wireless security protocols (in order of effectiveness):

- **WPA-PSK** (WiFi Protected Access - Pre-Shared Key): WPA was created to solve the inadequacies of WEP, the Wired Equivalency Protocol, which is now considered obsolete. 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 CODA-4x8x) 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.

NOTE: The CODA-4x8x can be configured to use the TKIP encryption standard; however, this limits the wireless network speed to 54Mbps (802.11g speed).

5.1.6.1 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 CODA-4x8x 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.

5.1.7 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.

5.2 The Wireless: Basic Settings Screen

Use this screen to configure your CODA-4x8x's 2.4GHz, 5GHz, Wifi Protected Setup (WPS) and guest network wireless settings.

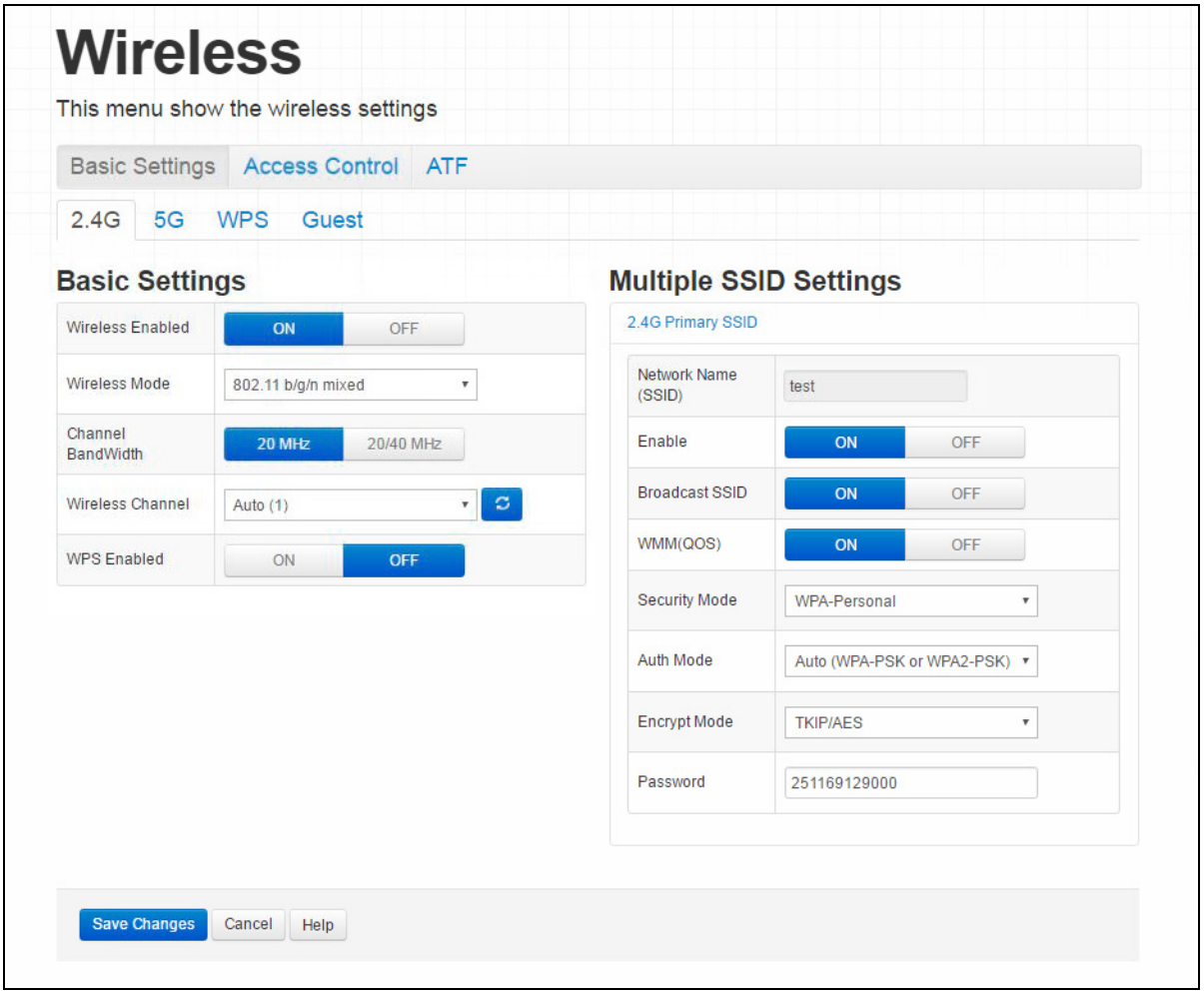
- Use the 2.4GHz network screen to enable 2.4GHz wireless clients to connect to the CODA-4x8x. See The Wireless: Basic Settings: 2.4G Screen on page 87.
- Use the 5GHz network screen to enable 5GHz wireless clients to connect to the CODA-4x8x. See The Wireless: Basic Settings: 5G Screen on page 93.
- Use the WPS screen to enable WPS-capable wireless clients to connect to the CODA-4x8x via a simple push-button, or by entering a password. See The Wireless: Basic Settings: WPS Screen on page 98.
- Use the Guest Network screen to enable wireless clients to connect to the CODA-4x8x with reduced privileges. See The Wireless: Basic Settings: Guest Screen on page 99.

5.2.1 The Wireless: Basic Settings: 2.4G Screen

Use this screen to configure the CODA-4x8x's 2.4GHz wireless network.

Click **Wireless** > **Basic Settings** > **2.4G**. The following screen displays.

Figure 33: The Wireless: Basic Settings: 2.4G Screen



The following table describes the labels in this screen.

Table 23: The Wireless: Basic Settings: 2.4G Screen

Basic Settings	
Wireless Enabled	▸ Select **On** to enable the 2.4GHz wireless network. ▸ Select **Off** to enable the 2.4GHz wireless network.

Table 23: The Wireless: Basic Settings: 2.4G Screen (continued)

Wireless Mode	Select the type of 2.4GHz wireless network that you want to use: • **802.11 11b Only**: use IEEE 802.11b. • **802.11 g Only**: use IEEE 802.11g. • **802.11 b/g Mixed**: use IEEE 802.11b and 802.11g. • **802.11 n Only**: use IEEE 802.11n. • **802.11 g/n Mixed**: use IEEE 802.11g and 802.11n. • **802.11 b/g/n Mixed**: use IEEE 802.11b, 802.11g and 802.11n. Only wireless clients that support the network protocol you select can connect to the wireless network. If in doubt, use **11b/g/n Mixed** (default).
Channel Bandwidth	Use this field to configure the width of the radio channel the CODA-4x8x uses to communicate with its wireless clients (IEEE 802.11n only) on the 2.4GHz network. Using the full 40MHz bandwidth can double your data speed. • Select **20 MHz** to only use a 20 megahertz band. • Select **20/40 MHz** to use a 40 megahertz band when possible, and a 20 megahertz band when a 40 megahertz band is unavailable.
Wireless Channel	Select the 2.4GHz wireless channel that you want to use, or select **Auto** to have the CODA-4x8x select the optimum channel to use. NOTE: Use the **Auto** setting unless you have a specific reason to do otherwise. Click the **Refresh** button ( ) to have the CODA-4x8x recheck the current wireless network conditions and select the optimum 2.4GHz wireless channel afresh (see Automatic Channel Selection on page 83).

Table 23: The Wireless: Basic Settings: 2.4G Screen (continued)

WPS Enabled	Use this field to turn Wifi Protected Setup (WPS) on or off on the 2.4GHz network (see WPS on page 86). • Select **ON** to enable WPS. • Select **OFF** to disable WPS.
Multiple SSID Settings	
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. • Select **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 CODA-4x8x 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)	This field displays whether Wifi MultiMedia (WMM) Quality of Service (QoS) settings are **Enabled** or **Disabled** on this SSID.

Table 23: The Wireless: Basic Settings: 2.4G Screen (continued)

Security Mode	Select the type of security that you want to use on the 2.4GHz network. • Select **Open** to use no security. Anyone in the coverage area can enter your network. • Select **WPA-Personal** to use the WiFi Protected Access (Personal) security protocol. • Select **WPA-Enterprise** to use the WiFi Protected Access (Enterprise) security protocol. NOTE: The Enterprise variants of WPA require the use of a Remote Authentication Dial-In User Service (RADIUS) server for security management. Only select the **WPA-Enterprise** if you have a RADIUS server on your network. Otherwise, select **WPA-Personal**.
Auth Mode	Select the type of authentication that you want to use. The following options display when you select **WPA-Personal** in the **Security Mode** field: • Select **WPA-PSK** to use the WiFi Protected Access (Personal) security protocol. • Select **WPA2-PSK** to use the WiFi Protected Access 2 (Personal) security protocol. • Select **Auto (WPA-PSK or WPA2-PSK)** 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. The following options display when you select **WPA-Enterprise** in the **Security Mode** field: • Select **WPA** to use the WPA Enterprise security protocol. • Select **WPA2** to use the WPA2 Enterprise security protocol.

Table 23: The Wireless: Basic Settings: 2.4G Screen (continued)

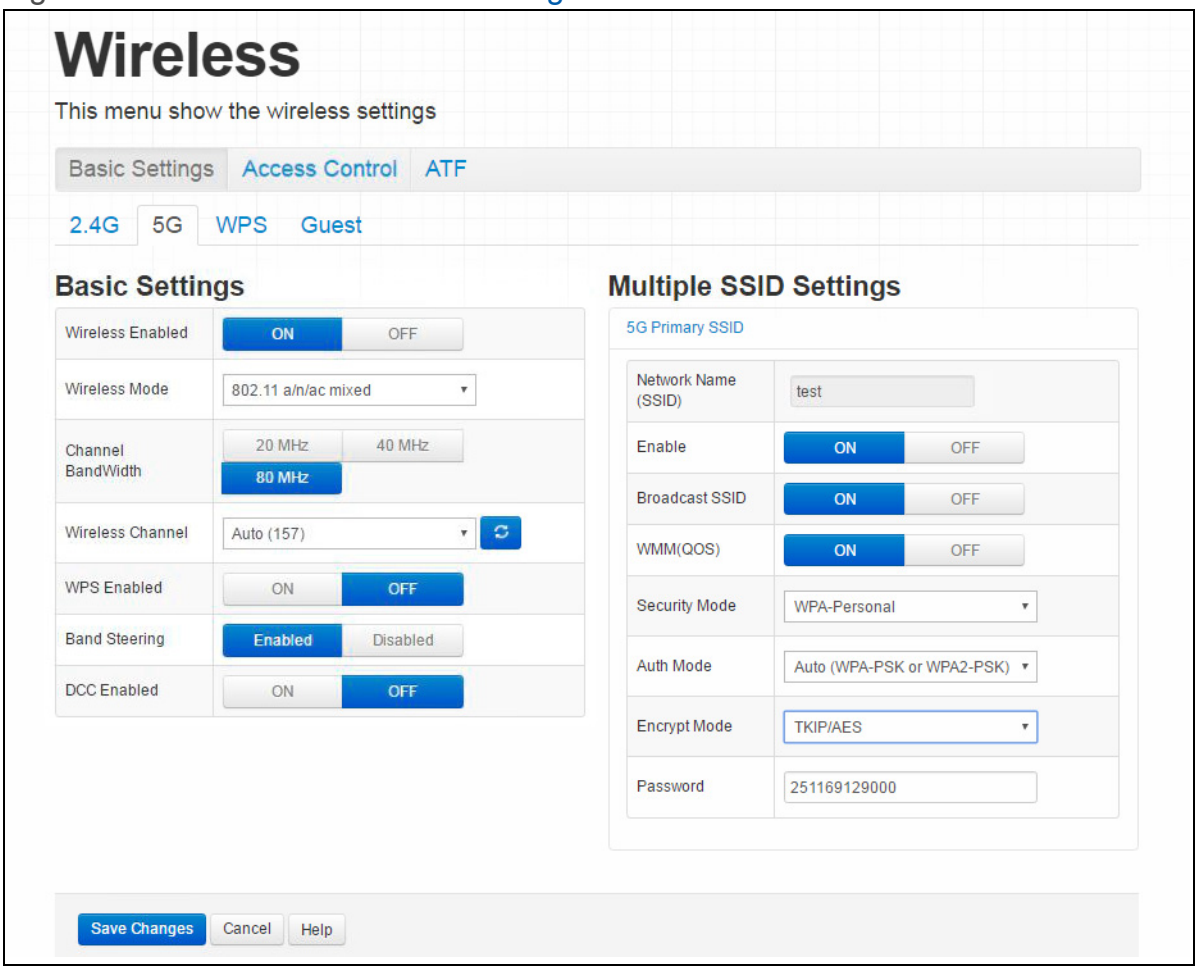
Encrypt Mode	Select the type of encryption you want to use on the 2.4GHz network. The options that display depend on the options you selected in the other fields in this screen. • Select **AES** to use the Advanced Encryption Standard. • Select **TKIP** to use the Temporal Key Integrity Protocol. • Select **TKIP/AES** to allow clients using either encryption type to connect to the CODA-4x8x. NOTE: Use of the TKIP encryption standard limits the wireless network speed to 54Mbps (802.11g speed).
Password	Enter the security key or password that you want to use for the 2.4GHz wireless network. You will need to enter this key into your wireless clients in order to allow them to connect to the network.
RADIUS Auth Server Address (0.0.0.0~255.255.255.255)	When using the **WPA-Enterprise** security mode, enter the IP address of the RADIUS server on the network, which the CODA-4x8x will use for security management.
RADIUS Auth Server Port (0~65535)	When using the **WPA-Enterprise** security mode, enter the port on which the CODA-4x8x should connect to the RADIUS server on the network.
RADIUS Auth Shared Secret	When using the **WPA-Enterprise** security mode, enter the authentication key that will allow the CODA-4x8x to communicate with the RADIUS server on the network.
Max Inactive Time (in seconds)	When using the **WPA-Enterprise** security mode, enter the maximum number of seconds a wireless client may remain inactive on the network before it must re-authenticate.
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 The Wireless: Basic Settings: 5G Screen

Use the 5GHz network screen to enable 5GHz wireless clients to connect to the CODA-4x8x.

Click **Wireless** > **Basic Settings** > **5G**. The following screen displays.

Figure 34: The Wireless: Basic Settings: 5G Screen



The following table describes the labels in this screen.

Table 24: The Wireless: Basic Settings: 5G Screen

Basic Settings	
Wireless Enabled	▸ Select **On** to enable the 5GHz wireless network. ▸ Select **Off** to enable the 5GHz wireless network.

Table 24: The Wireless: Basic Settings: 5G Screen (continued)

Wireless Mode	Select the type of 5GHz wireless network that you want to use: • **802.11a only**: use IEEE 802.11a. • **802.11n only**: use IEEE 802.11n. • **802.11a/n mixed**: allow clients using both IEEE 802.11a and IEEE 802.11n to access the network. • **802.11ac only**: use IEEE 802.11ac. • **802.11a/n/ac mixed** (default): allow clients using and of IEEE 802.11n, IEEE 802.11ac, or IEEE 802.11a to access the network. NOTE: Only wireless clients that support the network protocol you select can connect to the wireless network. If in doubt, use **802.11n/ac Mixed** (default).
Channel Bandwidth	Use this field to configure the width of the radio channel the CODA-4x8x uses to communicate with its wireless clients on the 5GHz network. Using the full 80MHz bandwidth can double your data speed, in comparison to the 40MHz bandwidth. • Select **20 MHz** to only use a 20 megahertz band. • Select **40 MHz** to use a 40 megahertz band (only clients supporting IEEE 802.11n and IEEE 802.11ac may connect). • Select **80 MHz** to use an 80 megahertz band (only clients supporting IEEE 802.11ac may connect).
Wireless Channel	Select the 5GHz wireless channel that you want to use, or select **Auto** to have the CODA-4x8x select the optimum channel to use. NOTE: Use the **Auto** setting unless you have a specific reason to do otherwise. Click the **Refresh** button () to have the CODA-4x8x recheck the current wireless network conditions and select the optimum 5GHz wireless channel afresh (see Automatic Channel Selection on page 83).

Table 24: The Wireless: Basic Settings: 5G Screen (continued)

WPS Enabled	Use this field to turn Wifi Protected Setup (WPS) on or off on the 5GHz network (see WPS on page 86). • Select **ON** to enable WPS. • Select **OFF** to disable WPS.
Band Steering	Use this to turn band steering on or off on the 5GHz network (see Band Steering on page 83). • Select **Enabled** to turn band steering on. • Select **Disabled** to turn band steering off.
DCC Enabled	Use this to turn Dynamic Channel Change on or off on the 5GHz network (see Dynamic Channel Change on page 84). • Select **ON** to enable Dynamic Channel Change. • Select **OFF** to disable Dynamic Channel Change.
Multiple SSID Settings	
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. • Select **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 CODA-4x8x 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 24: The Wireless: Basic Settings: 5G Screen (continued)

WMM(QoS)	This field displays whether Wifi MultiMedia (WMM) Quality of Service (QoS) settings are **Enabled** or **Disabled** on this SSID.
Security Mode	Select the type of security that you want to use on the 5GHz network. • Select **Open** to use no security. Anyone in the coverage area can enter your network. • Select **WPA-Personal** to use the WiFi Protected Access (Personal) security protocol. • Select **WPA-Enterprise** to use the WiFi Protected Access (Enterprise) security protocol. NOTE: The Enterprise variants of WPA require the use of a Remote Authentication Dial-In User Service (RADIUS) server for security management. Only select the **WPA-Enterprise** if you have a RADIUS server on your network. Otherwise, select **WPA-Personal**.
Auth Mode	Select the type of authentication that you want to use. The following options display when you select **WPA-Personal** in the **Security Mode** field: • Select **WPA-PSK** to use the WiFi Protected Access (Personal) security protocol. • Select **WPA2-PSK** to use the WiFi Protected Access 2 (Personal) security protocol. • Select **Auto (WPA-PSK or WPA2-PSK)** 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. The following options display when you select **WPA-Enterprise** in the **Security Mode** field: • Select **WPA** to use the WPA Enterprise security protocol. • Select **WPA2** to use the WPA2 Enterprise security protocol.

Table 24: The Wireless: Basic Settings: 5G Screen (continued)

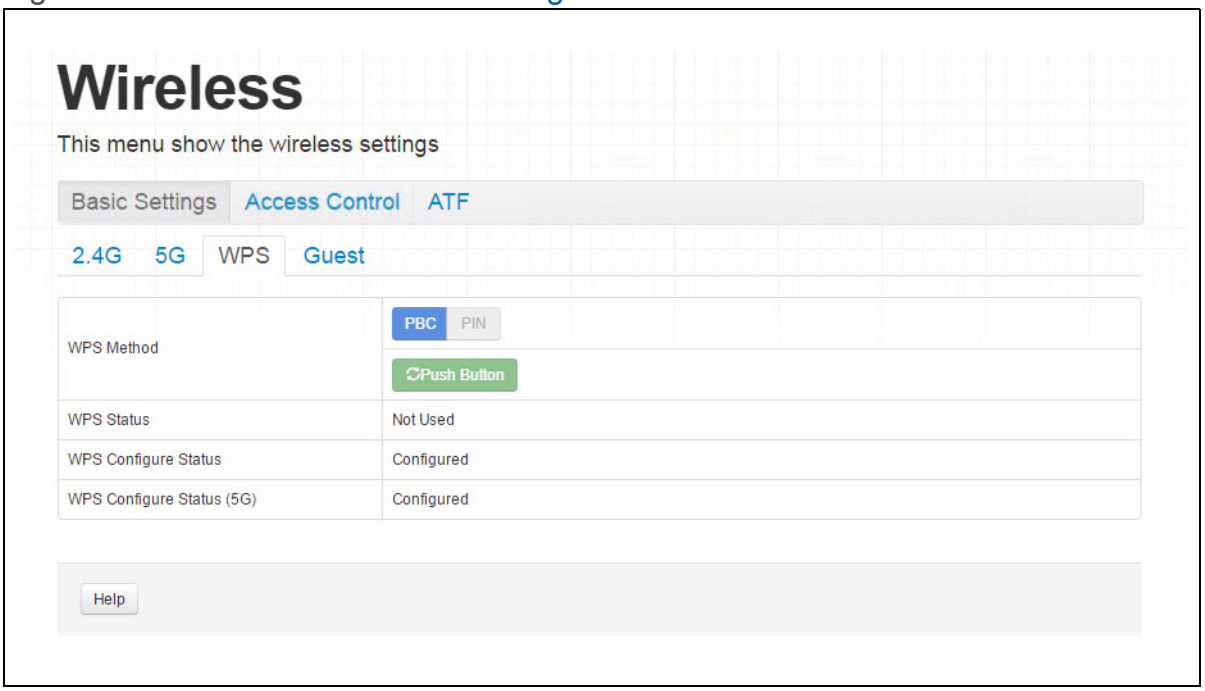
Encrypt Mode	Select the type of encryption you want to use on the 5GHz network. The options that display depend on the options you selected in the other fields in this screen. • Select **TKIP** to use the Temporal Key Integrity Protocol. • Select **AES** to use the Advanced Encryption Standard. • Select **TKIP/AES** to allow clients using either encryption type to connect to the CODA-4x8x. NOTE: Use of the TKIP encryption standard limits the wireless network speed to 54Mbps (802.11g speed).
Password	Enter the security key or password that you want to use for the 5GHz wireless network. You will need to enter this key into your wireless clients in order to allow them to connect to the network.
RADIUS Auth Server Address (0.0.0.0~255.255.255.255)	When using the **WPA-Enterprise** security mode, enter the IP address of the RADIUS server on the network, which the CODA-4x8x will use for security management.
RADIUS Auth Server Port (0~65535)	When using the **WPA-Enterprise** security mode, enter the port on which the CODA-4x8x should connect to the RADIUS server on the network.
RADIUS Auth Shared Secret	When using the **WPA-Enterprise** security mode, enter the authentication key that will allow the CODA-4x8x to communicate with the RADIUS server on the network.
Max Inactive Time (in seconds)	When using the **WPA-Enterprise** security mode, enter the maximum number of seconds a wireless client may remain inactive on the network before it must re-authenticate.
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.

5.2.3 The Wireless: Basic Settings: WPS Screen

Use the WPS screen to enable WPS-capable wireless clients to connect to the CODA-4x8x via a simple push-button, or by entering a password. See WPS on page 86.

Click **Wireless** > **Basic Settings** > **WPS**. The following screen displays.

Figure 35: The Wireless: Basic Settings: WPS Screen



The following table describes the labels in this screen.

Table 25: The Wireless: Basic Settings: WPS Screen

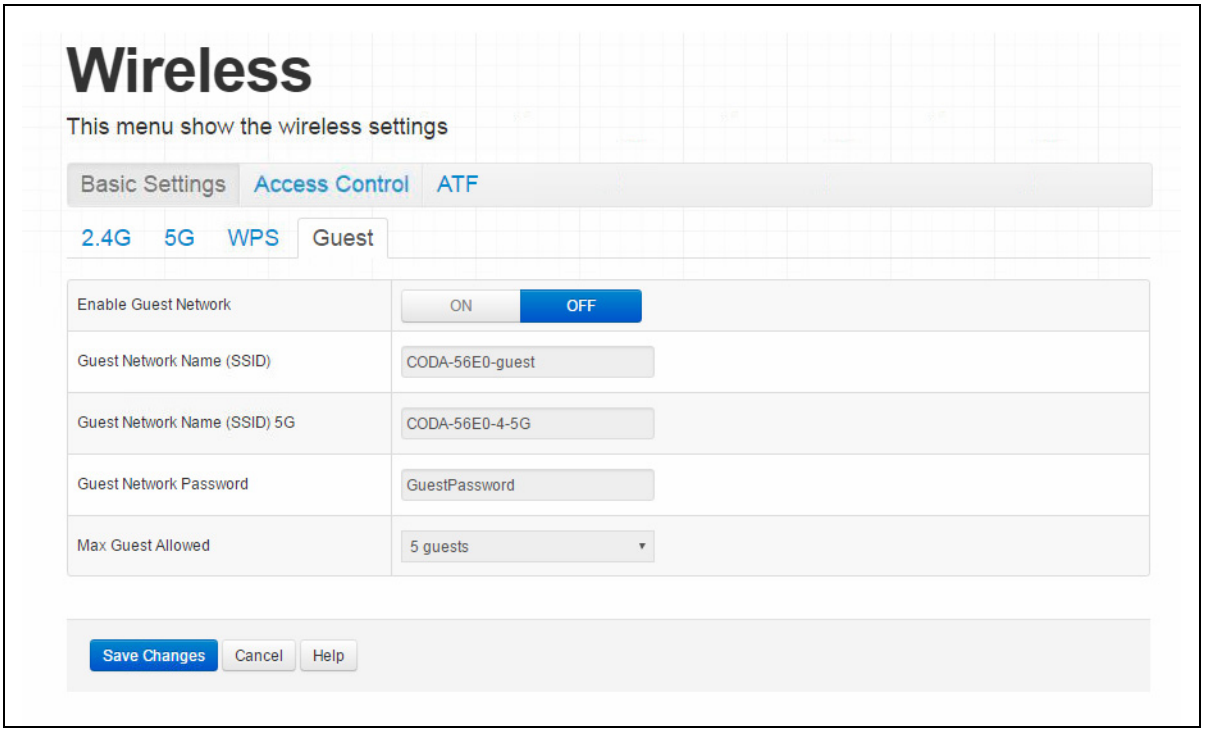
WPS Method	Use these buttons to run Wifi Protected Setup (WPS): • Click the **PBC** button and then **Push Button** to begin the Push-Button Configuration process. You must then press the PBC button on your client wireless devices within two minutes in order to register them on your wireless network. • 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 CODA-4x8x, or the WPS PIN of the client device you want to add to the network.
WPS Status	This displays whether or not the CODA-4x8x is using Wifi Protected Setup.
WPS Configure Status	This displays the Wifi Protected Setup configuration.
Help	Click this to see information about the fields in this screen.

5.2.4 The Wireless: Basic Settings: Guest Screen

Use the Guest Network screen to enable wireless clients to connect to the CODA-4x8x with reduced privileges.

Click **Wireless** > **Basic Settings** > **Guest**. The following screen displays.

Figure 36: The Wireless: Basic Settings: Guest Screen



The following table describes the labels in this screen.

Table 26: The Wireless: Basic Settings: Guest Screen

Enable Guest Network	Use this field to enable or disable the guest network. ▸ Select **ON** to enable the guest network. ▸ Select **OFF** to disable the guest network.
Guest Network Name (SSID)	Enter the SSID to use on the 2.4GHz wireless guest network.
Guest Network Name (SSID) 5G	Enter the SSID to use on the 5GHz wireless guest network.
Guest Network Password	Enter the password that wireless clients must be configured to use to connect to either the 2.4GHz or the 5GHz wireless guest network.
Max Guest Allowed	Select the maximum number of wireless clients that may concurrently connect to the wireless guest network.
Save Changes	Click this to save your changes to the fields in this screen.

Table 26: The Wireless: Basic Settings: Guest Screen (continued)

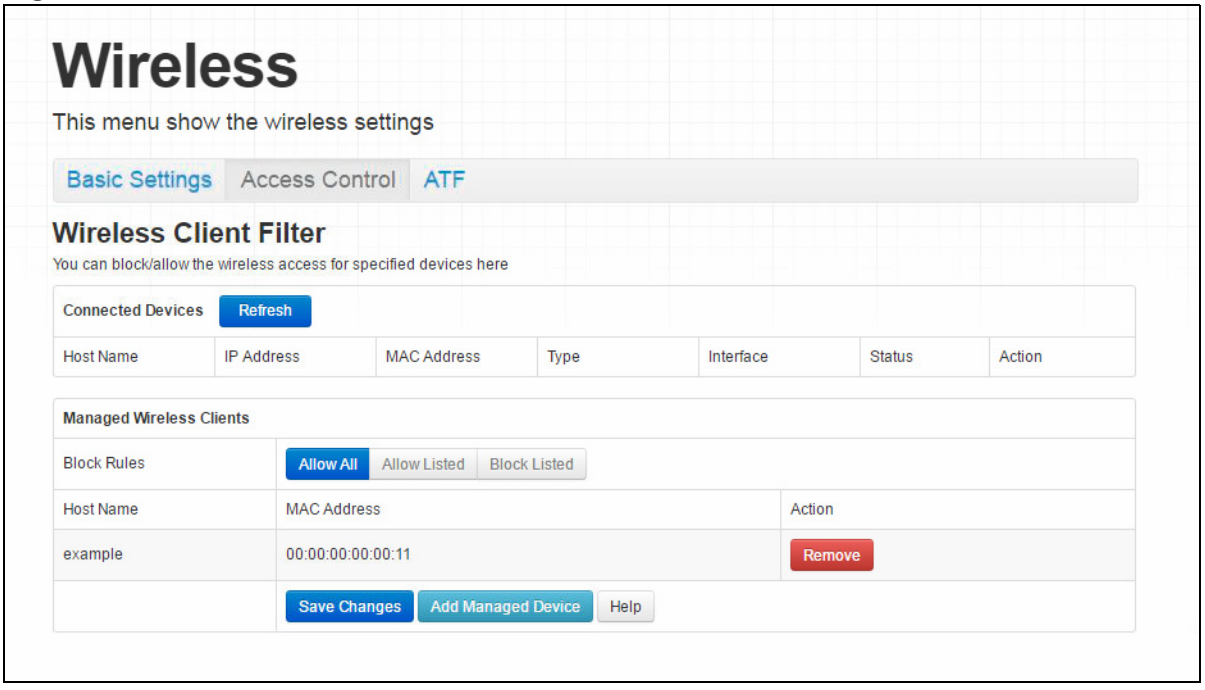
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

5.3 The Wireless: Access Control Screen

Use this screen to modify the CODA-4x8x's wireless networks' Service Set Identifiers (SSIDs) and manage the devices that connect to the wireless network.

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

Figure 37: The Wireless: Access Control Screen



The following table describes the labels in this screen.

Table 27: The Wireless: Access Control Screen

Connected Devices	
Refresh	Click this to reload the **Connected Devices** list.
Host Name	This displays the name of each network device connected on the wireless network.

Table 27: The Wireless: Access Control Screen (continued)

IP Address	This displays the IP address of each network device connected on the wireless network.
MAC Address	This displays the Media Access Control (MAC) address of each network device connected 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.
Status	This displays whether or not the connected device is active.
Action	Click **Manage** to make changes to the device's filtering status; see Adding or Editing a Managed Device on page 112 for information on the screen that displays.
Managed Wireless Clients	
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 CODA-4x8x. • Select **Allow Listed** to permit only devices you added to the **Managed Devices** list to access the CODA-4x8x and the network. All other devices are denied access. • Select **Block Listed** to permit all devices except those you added to the **Managed Devices** list to access the CODA-4x8x 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.
Action	Click **Remove** to remove a managed device rule from the list.
Save Changes	Click this to save your changes to the fields in this screen.
Add Managed Device	Click this to add a new managed device rule (see Adding or Editing a Managed Device on page 112).

Table 27: The Wireless: Access Control Screen (continued)

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 The Wireless: ATF Screen

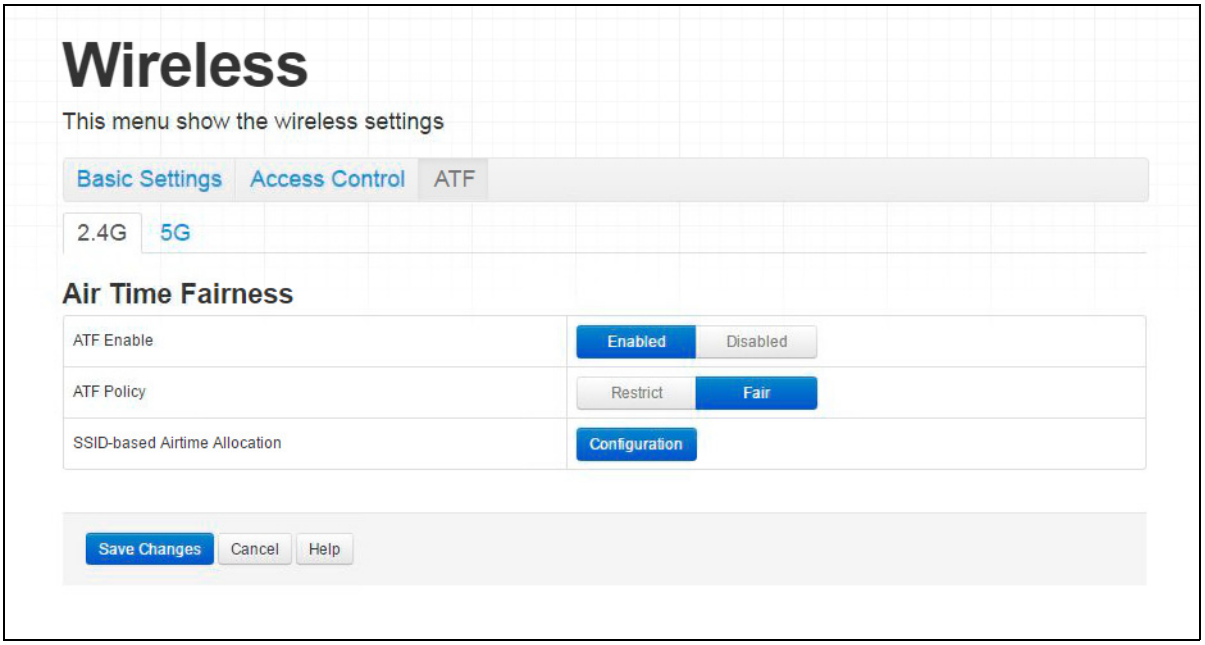
Use this screen to configure AirTime Fairness (ATF) settings. ATF is a wireless quality-of-service feature that allows you to assign a percentage of the available wireless resources to each of the CODA-4x8x's various wireless network SSIDs.

"Airtime", in this usage, refers to the amount of time required to transmit data over the wireless network from the CODA-4x8x to its wireless clients. This is distinct from the actual amount of data transmitted, as different connections may transmit data at different speeds.

This enables you to, for instance, ensure that usage of the guest network does not impinge on more important traffic. It also enables you to prevent traffic on slower SSIDs from affecting the performance of faster ones.

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

Figure 38: The Wireless: ATF Screen



The following table describes the labels in this screen.

Table 28: The Wireless: ATF Screen

2.4G 5G	Use this to configure ATF settings for the 2.4GHz wireless network, or the 5GHz wireless network. • Click **2.4G** to configure ATF settings for the 2.4GHz wireless network. • Click **5G** to configure ATF settings for the 5GHz wireless network. NOTE: The fields that display in the 2.4GHz and the 5GHz screens are identical.
ATF Enable	Use this to turn ATF on or off for the relevant wireless network. • Click **Enable** to turn ATF on for the relevant wireless network. • Click **Disable** to turn ATF off for the relevant wireless network.
ATF Policy	Use this to determine what the CODA-4x8x does with unused airtime (based on the settings you configure in Configuring Airtime Allocation Policy on page 105). Airtime is unused when an SSID's resource usage does not reach the limit you assigned it; unused airtime can therefore be assigned to other SSIDs that may require it. • Select **Restrict** to ensure that SSIDs receive no more than the percentage of resources you assigned them. Unused airtime is not reassigned. • Select **Fair** to evenly distribute unused airtime amongst SSIDs whose traffic has exceeded the percentage of resources you assigned them.
SSID-based Airtime Allocation	Use this to configure the percentage of available wireless transmission resources that should be assigned to each of the CODA-4x8x's wireless SSIDs. See Configuring Airtime Allocation Policy on page 105.
Save Changes	Click this to save your changes to the fields in this screen.

Table 28: The Wireless: ATF Screen (continued)

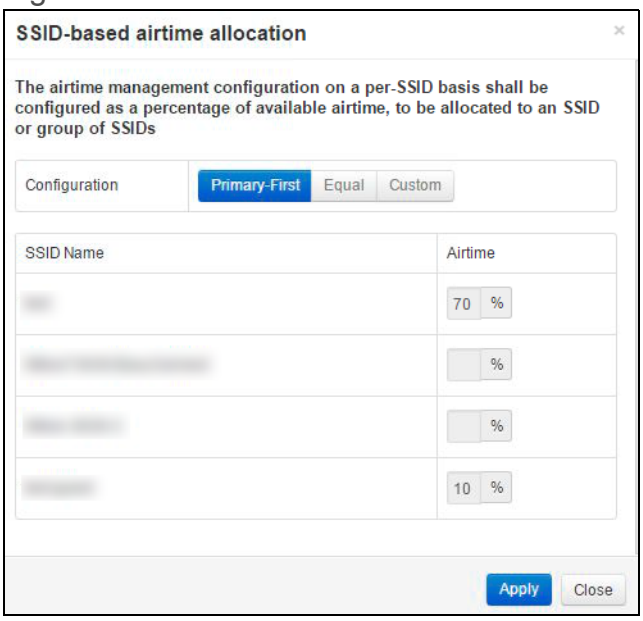
Cancel	Click this to return the fields in this screen to their last-saved values without saving your changes.
Help	Click this to see information about the fields in this screen.

5.4.0.1 Configuring Airtime Allocation Policy

Use this screen to configure the percentage of available wireless transmission resources that should be assigned to each of the CODA-4x8x's wireless SSIDs.

Click **SSID-based Airtime Allocation** in the **Wireless** > **ATF** screen. The following screen displays.

Figure 39: The Wireless: ATF: SSID-based Airtime Allocation Screen



The following table describes the labels in this screen.

Table 29: The Wireless: ATF: SSID-based Airtime Allocation Screen

Configuration	Use this to select the ATF policy you wish to use. The values in the **Airtime** column update to indicate the percentage of available wireless resources each of the CODA-4x8x's SSIDs is assigned. ▸ Select **Primary-First** to provide the CODA-4x8x's primary SSID with 70% of the resources, and restrict the guest SSID to 10% of the resources. ▸ Select **Equal** to provide each of the CODA-4x8x's SSIDs with an equal portion of resources (25% each, on a device with four SSIDs). ▸ Select **Custom** to enter your own values into the **Airtime** column's fields for each SSID.
SSID Name	This displays the name of each of the CODA-4x8x's wireless networks.
Airtime	This displays the percentage of the available wireless transmission resources to be assigned to the relevant SSID. When a percentage value does not display in an SSID's **Airtime** field, it receives equal access to the wireless resources not assigned to other SSIDs.
Save Changes	Click this to save your changes to the fields in this screen.
Cancel	Click this to close the popup without saving your changes.
Help	Click this to see information about the fields in this screen.

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 CODA-4x8x 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 CODA-4x8x 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.

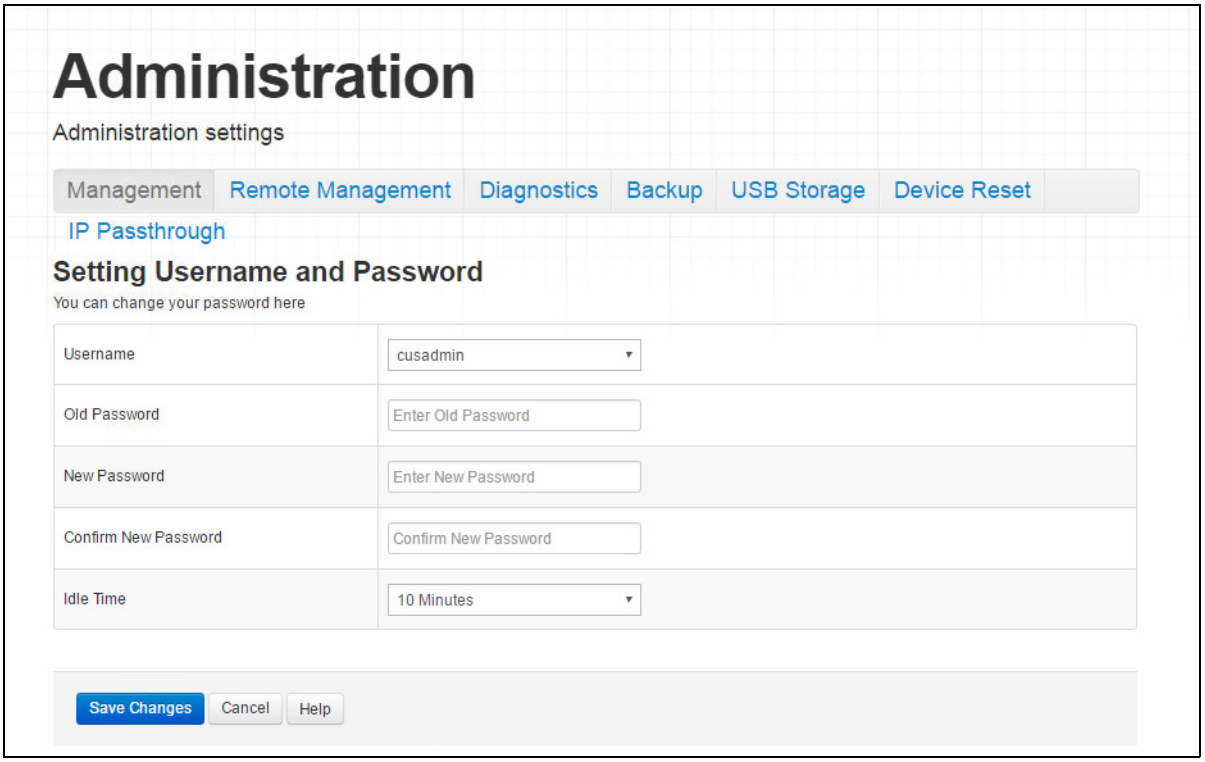
6.2 The Admin: Management Screen

Use this screen to make changes to the CODA-4x8x's login credentials (username and password) and inactivity idle time.

NOTE: If you forget your password, you will need to reset the CODA-4x8x to its factory defaults.

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

Figure 40: The Admin: Management Screen



The following table describes the labels in this screen.

Table 30: The Admin: Management Screen

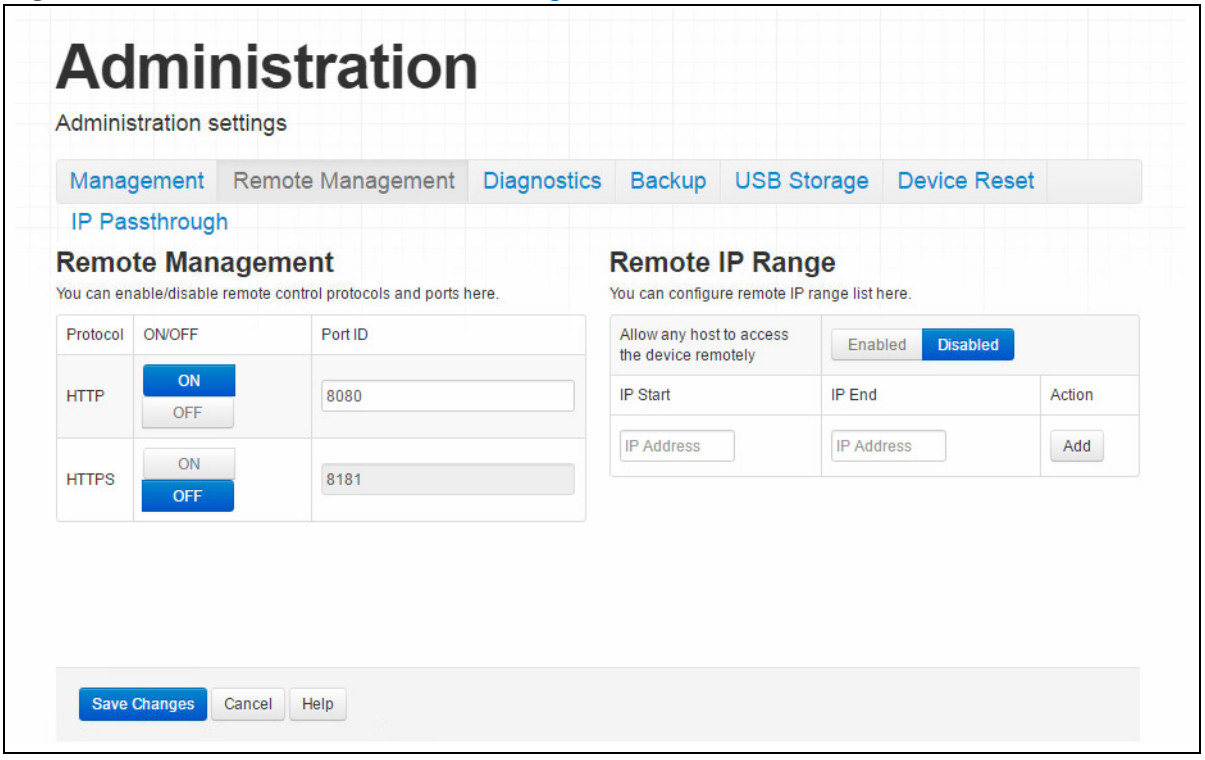
Username	If your CODA-4x8x supports multiple user accounts, select the account you want to modify from the list.
Old Password	Enter the password with which you currently log into the CODA-4x8x for this account.
New Password	Enter and re-enter the password you want to use to log into the CODA-4x8x for this account.
Confirm New Password	
Idle Time	Select the time interval after which an inactive user should be logged out of the CODA-4x8x's admin interface.
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 The Admin: Remote Management Screen

Use this screen to configure remote management of the CODA-4x8x via HTTP and/or HTTPS.

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

Figure 41: The Admin: Remote Management Screen



The following table describes the labels in this screen.

Table 31: The Admin: Remote Management Screen

Protocol	Use the relevant row to permit or forbid remote management via the relevant protocol.
ON/OFF	▸ Select **On** to permit remote management via the relevant protocol. ▸ Select **Off** to forbid remote management via the relevant protocol.
Port ID	This displays the port number through which remote management can be performed, for the relevant protocol.

Table 31: The Admin: Remote Management Screen (continued)

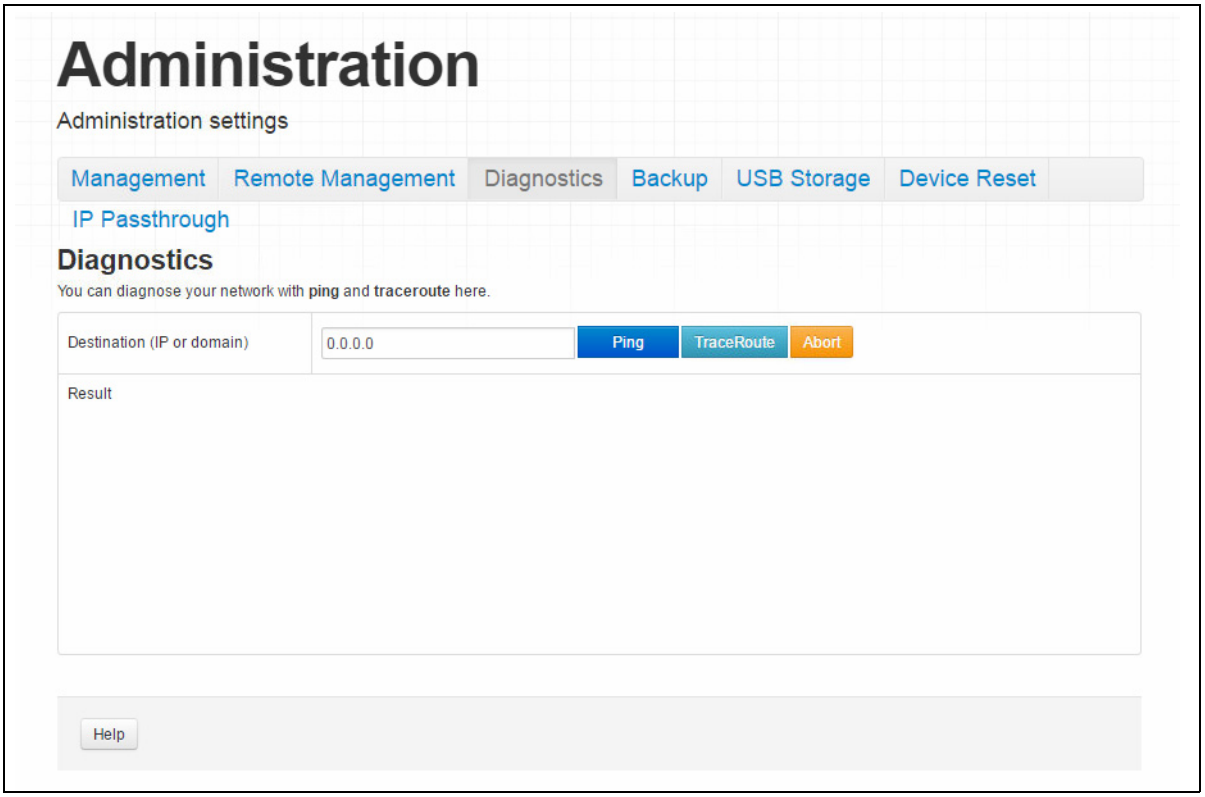
Remote IP Range	▸ Select **Enabled** to permit remote management, for all protocols, from computers with IP addresses in the range specified. ▸ Select **Disabled** to allow computers with any IP address to manage the CODA-4x8x remotely.
Save Changes	Click this to save your changes to the fields in this 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.

6.4 The Admin: Diagnostics Screen

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

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

Figure 42: The Admin: Diagnostics Screen



The following table describes the labels in this screen.

Table 32: The Admin: Diagnostics Screen

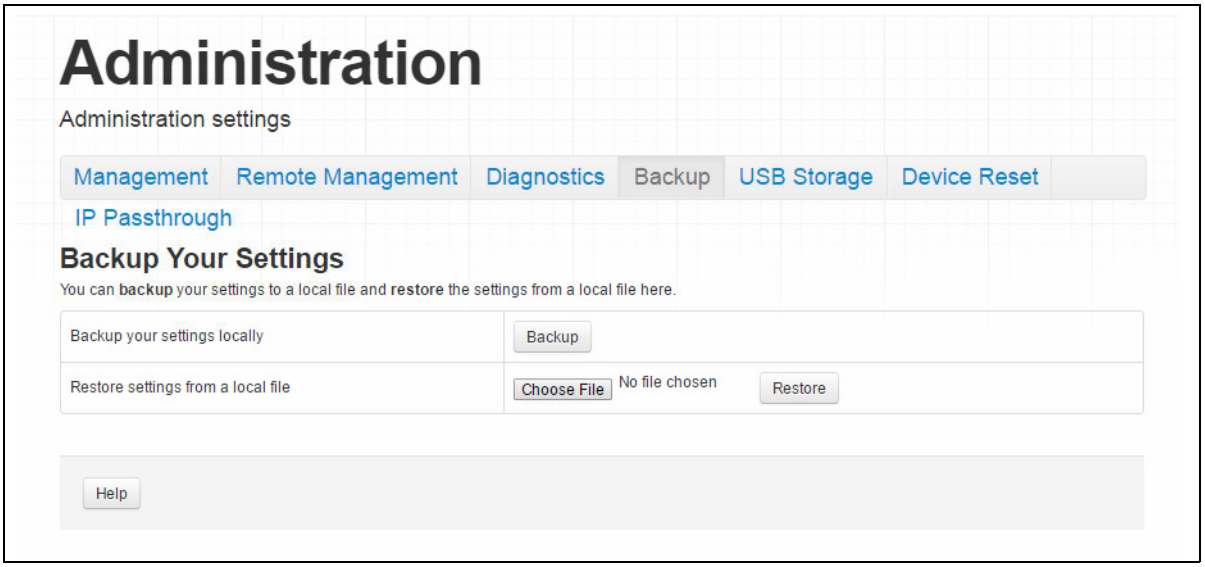
Destination (IP or Domain)	Enter the IP address or URL that you want to test.
Ping	Select the type of test that you want to run on the **Destination** that you specified.
Traceroute	
Result	This field displays a report of the test most recently performed.
Abort	Click this to terminate a test in progress.

6.5 The Admin: Backup Screen

Use this screen to back up your CODA-4x8x's settings to your computer or load settings from a backup you created earlier.

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

Figure 43: The Admin: Backup Screen



The following table describes the labels in this screen.

Table 33: The Admin: Backup Screen

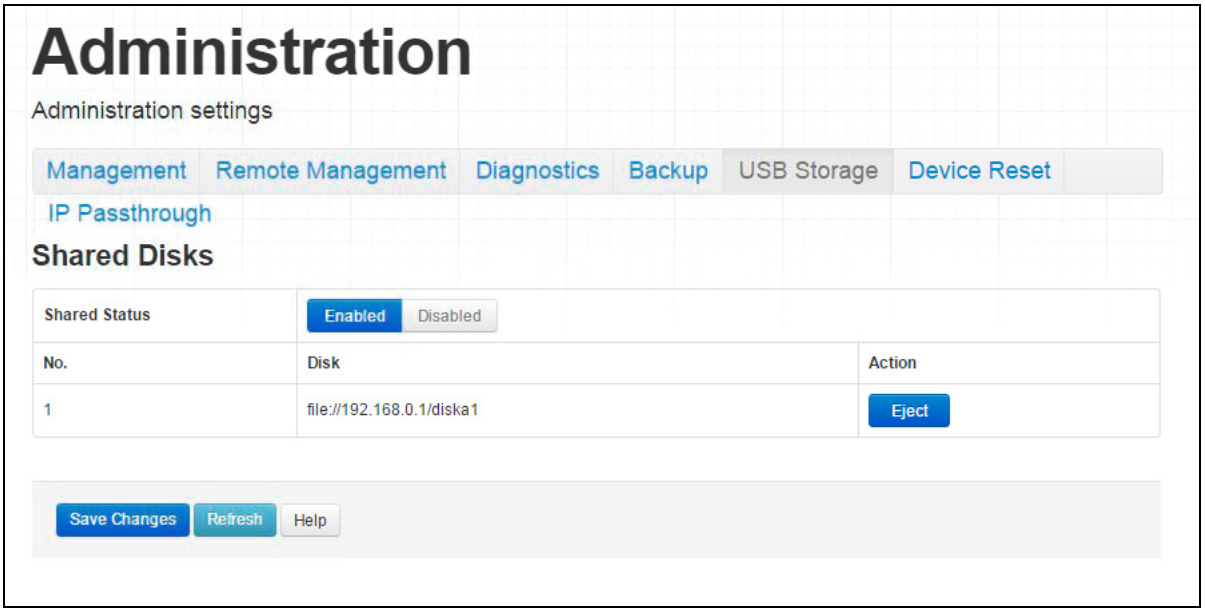
Back Up Your Settings Locally	Click this to create a backup of all your CODA-4x8x's settings on your computer.
Restore Settings From a Local File	Use these fields to return your CODA-4x8x's settings to those specified in a backup that you created earlier. Click **Choose File** to select a backup, then click **Restore** to return your CODA-4x8x's settings to those specified in the backup.

6.6 The Admin: USB Storage Screen

Use this screen to manage and share data stored on devices connected to the CODA-4x8x's **USB** port. The CODA-4x8x provides one USB 2.0 host port, allowing you to plug in a USB flash disk for mounting and sharing through the LAN interfaces via the Samba protocol (network neighborhood).

Click **Admin** > **USB Storage**. The following screen displays.

Figure 44: The Admin: USB Storage Screen



The following table describes the labels in this screen.

Table 34: The Admin: USB Storage Screen

Shared Status	This displays whether USB sharing is active or inactive. • Select **Enabled** to turn USB sharing on. USB devices connected to the CODA-4x8x will be accessible on the network. • Select **Disabled** to turn USB sharing off. USB devices connected to the CODA-4x8x will not be accessible on the network.
No.	This displays the index number of the connected USB device. When no USB device is connected, no number displays.
Disk	This displays the name of the connected USB device, by which it may be accessed on the network.
Action	Click **Eject** before physically removing a connected USB device from the CODA-4x8x, in order to ensure all operations are correctly terminated and no data loss occurs.
Save Changes	Click this to save your changes to the fields in this screen.

Table 34: The Admin: USB Storage Screen (continued)

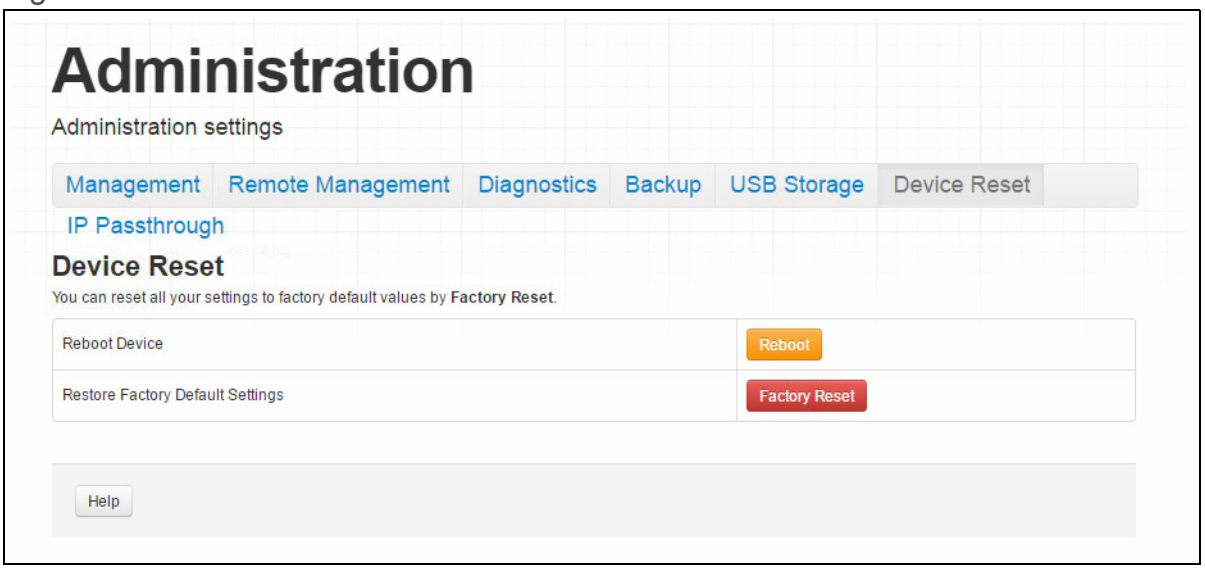
Refresh	Click this to refresh the data in this screen.
Help	Click this to see information about the fields in this screen.

6.7 The Admin: Device Reset Screen

Use this screen to reboot your CODA-4x8x, or to return it to its factory default settings.

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

Figure 45: The Admin: Device Reset Screen



The following table describes the labels in this screen.

Table 35: The Admin: Device Reset Screen

Reboot Device	Click this to restart your CODA-4x8x.
Restore Factory Default Settings	Click this to return your CODA-4x8x to its factory default settings. When you do this, all your user-configured settings are lost, and cannot be retrieved.

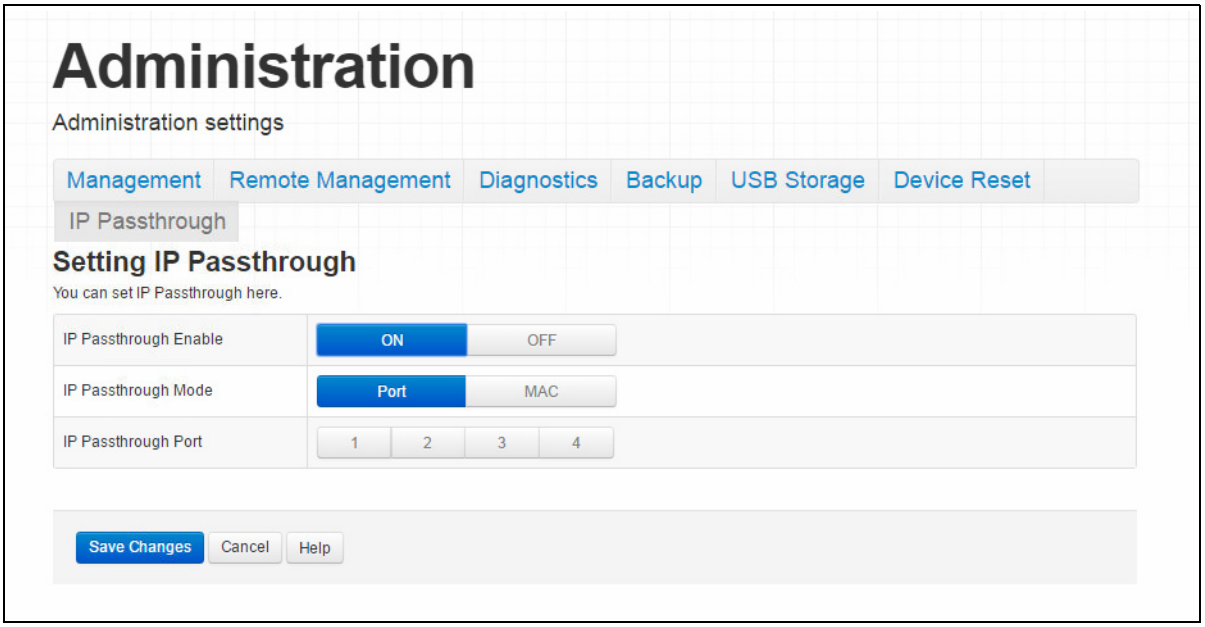
6.8 The Admin: IP Passthrough Screen

Use this screen to assign a public IP address to a device attached to your CODA-4x8x on the LAN.

NOTE: Before enabling IP passthrough, bear in mind that once IP passthrough is enabled, you will no longer be able to access the CODA-4x8x's GUI from the relevant device on the LAN. You may also require additional configuration to be performed by your Internet Service Provider on your account. Check documentation from your ISP, or contact their customer service department, if unsure.

Click **Admin** > **IP Passthrough**. The following screen displays.

Figure 46: The Admin: IP Passthrough Screen



The following table describes the labels in this screen.

Table 36: The Admin: IP Passthrough Screen

IP Passthrough Enable	Use this to enable or disable IP passthrough. • Click **ON** to enable IP passthrough. • Click **OFF** to disable IP passthrough.
IP Passthrough Mode	You can configure IP passthrough by LAN port, or Media Access Control (MAC) address. • Click **Port** to enable IP passthrough for any device attached to the LAN ports you specify in the **IP Passthrough Port**. • Click **MAC** to enable IP passthrough for the specific device whose MAC address you specify in the **IP Passthrough MAC** field. NOTE: If you select **MAC** and enter a device's MAC address, you will not be able to access the CODA-4x8x's GUI via the LAN from that device. In the event you are unable to access the CODA-4x8x's GUI, you may need to reset the CODA-4x8x to its factory default settings.
IP Passthrough Port	If you selected **Port** in the **IP Passthrough Mode** field, select the LAN port or ports for which you wish to enable IP passthrough.
IP Passthrough MAC	If you selected **MAC** in the **IP Passthrough Mode** field, enter the MAC address of the device for which you wish to enable IP passthrough.
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

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 CODA-4x8x'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 CODA-4x8x'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 CODA-4x8x'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 CODA-4x8x 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 Port Blocking

Port blocking 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.

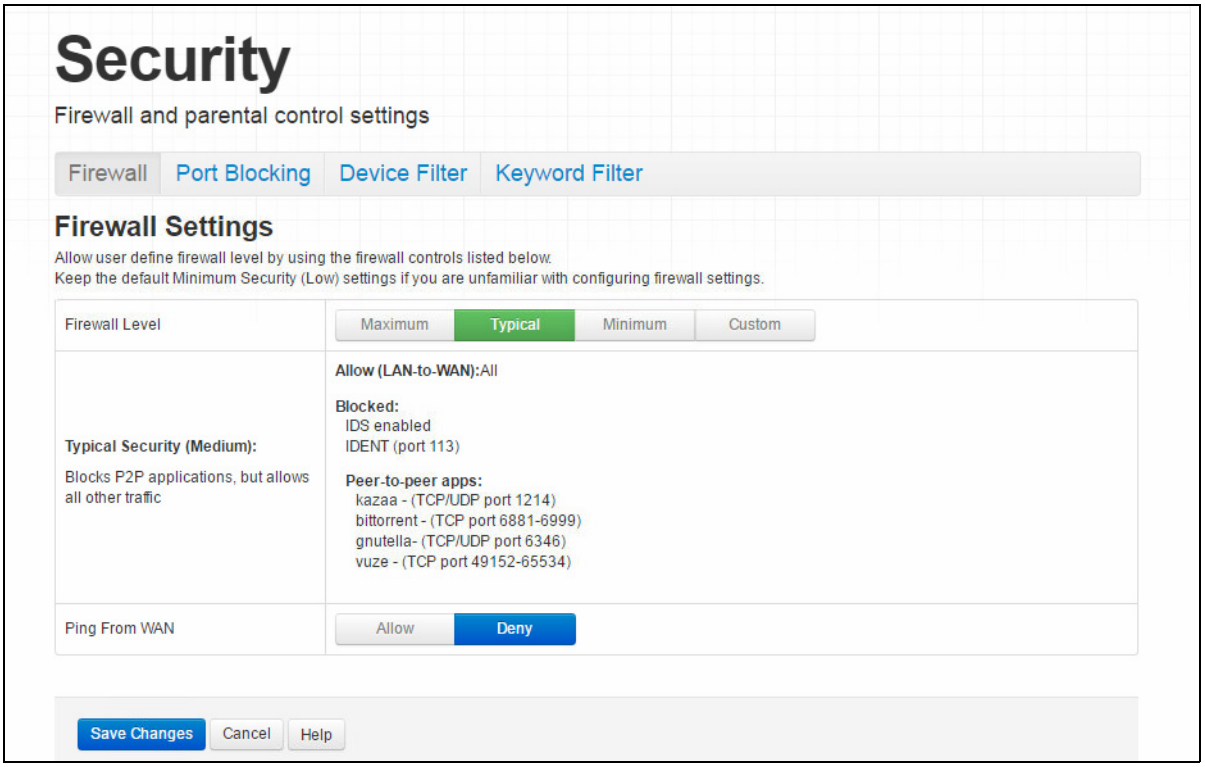
7.2 The Security: Firewall Screen

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 **Port Blocking** screen (see The Security: Port Blocking Screen on page 121).

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

Figure 47: The Security: Firewall Screen



The following table describes the labels in this screen.

Table 37: 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).

Table 37: The Security: Firewall Screen (continued)

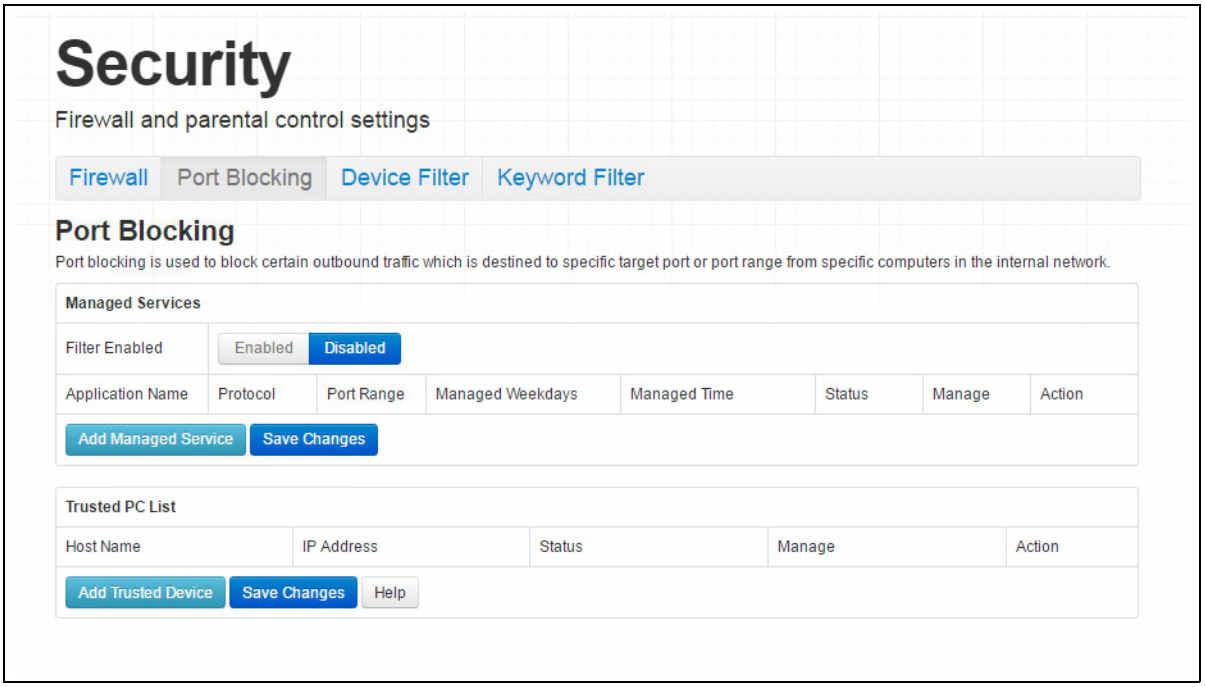
Ping from WAN	Use this field to permit or prohibit Internet Control Message Protocol (ICMP) echo requests from the WAN to the LAN. • Select **Allow** to permit pinging from the WAN. • Select **Deny** to prohibit pinging from the WAN. Echo requests from the WAN to the LAN are silently ignored.
Save Changes	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 Security: Port Blocking Screen

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

Click **Security** > **Port Blocking**. The following screen displays.

Figure 48: The Security: Port Blocking Screen



The following table describes the labels in this screen.

Table 38: The Security: Port Blocking Screen

Managed Services	
Filter Enabled	Use this field to turn port blocking on or off. ▸ Select **Enabled** to turn port blocking on. ▸ Select **Disabled** to turn port blocking off.
Application Name	This displays the name you assigned to the blocking 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 blocking rule applies.
Managed Weekdays	This displays the days of the week on which this rule applies.
Managed Time	This displays the start (**From**) and end (**To**) of the time period during which this rule applies, on the specified **Managed Weekdays**.

Table 38: The Security: Port Blocking Screen (continued)

Status	This displays whether the blocking rule is currently in force (**Enabled**) or not (nothing displays).
Managed	Click **Manage** to make changes to a blocking rule (see Adding or Editing a Port Blocking Rule on page 123).
Action	Click **Remove** to delete a rule from the CODA-4x8x.
Add Managed Service	Click this to add a new port blocking rule (see Adding or Editing a Port Blocking Rule on page 123).
Save Changes	Click this to save your changes to the fields in this screen.
Trusted PC List	
Host Name	This displays the arbitrary name of each trusted PC you configured.
IP Address	This displays the LAN IP address of each trusted PC.
Status	This displays whether the device is currently trusted (**Enabled**) or untrusted (**Disabled**).
Manage	Click **Manage** to make changes to the trusted device rule. See Adding or Editing a Port Blocking Trusted Device Rule on page 126 for information on the screen that displays.
Action	Click **Delete** to remove the trusted device rule.
Add Trusted Device	Click this to create a new trusted device rule. See Adding or Editing a Port Blocking Trusted Device Rule on page 126 for information on the screen that displays.
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.

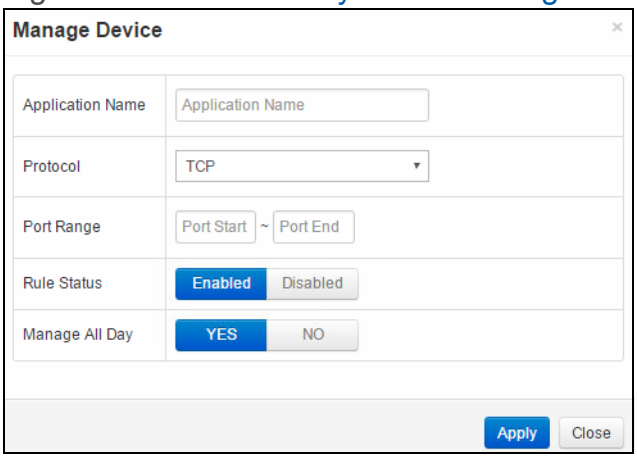
7.3.1 Adding or Editing a Port Blocking Rule

- To add a new port forwarding rule, click **Add Managed Service** in the **Security** > **Port Blocking** screen.
- To edit an existing port blocking rule, locate the rule in the **Security** > **Port Blocking** screen and click its **Manage** button.

NOTE: Ensure that **Enabled** is selected in the **Security** > **Port Blocking** screen in order to add or edit port blocking rules.

The following screen displays.

Figure 49: The Security: Port Blocking Add/Edit Screen

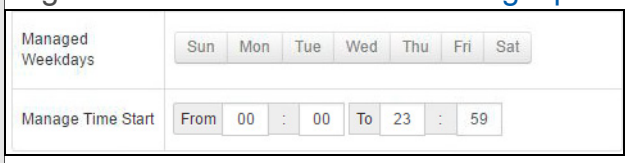


The following table describes the labels in this screen.

Table 39: The Security: Port Blocking 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 CODA-4x8x should filter via: • Transmission Control Protocol (**TCP**) • User Datagram Protocol (**UDP**) • Both TCP and UDP (**TCP/UDP**). NOTE: If in doubt, leave this field at its default.
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 39: The Security: Port Blocking Add/Edit Screen

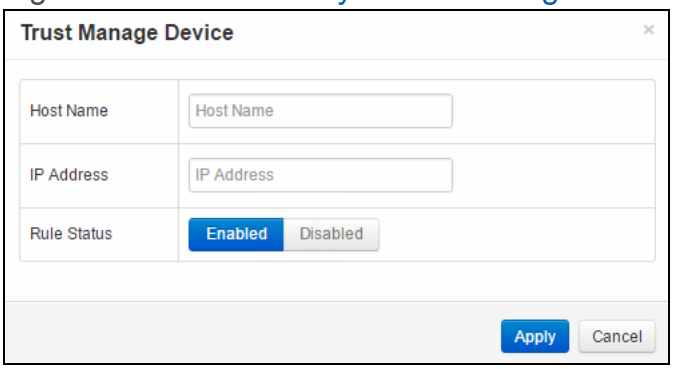
Rule Status	Use this field to select whether the filtering rule should be active or not. • Select **Enabled** to activate the rule. Matching traffic will be blocked. • Select **Disabled** to deactivate the rule. Matching traffic will not be blocked.
Manage All Day	Use this field to specify whether the 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 50: Additional Port blocking 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 **Port Blocking** screen without saving your changes to the rule.

7.3.2 Adding or Editing a Port Blocking Trusted Device Rule

- To add a new trusted device rule, click **Add Trusted PC** in the **Security** > **Port Blocking** screen.
- To edit an existing trusted device rule, locate the rule in the **Security** > **Port Blocking** screen and click its **Manage** button.

The following screen displays.

Figure 51: The Security: Port Blocking Trusted Device Add/Edit Screen



The following table describes the labels in this screen.

Table 40: The Security: Port Blocking Trusted Device Add/Edit Screen

Host Name	Enter a name to identify the device.
IP Address	Enter the local IP address of the device.
Rule Status	Use this field to define whether the trusted device rule should be active or not. - Select **Enabled** to activate the trusted device rule. - Select **Disabled** to deactivate the trusted device rule.
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.

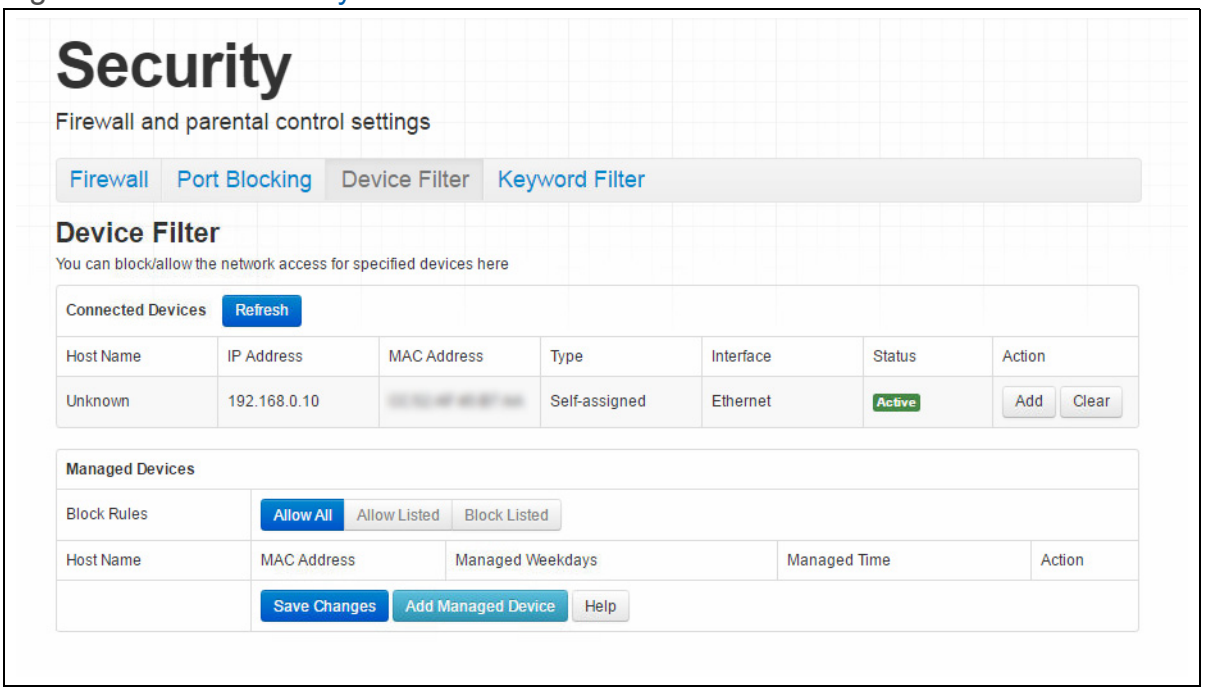
7.4 The Security: Device Filter Screen

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 The Wireless Access Control Screen on page 75.

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

Figure 52: The Security: Device Filter Screen



The following table describes the labels in this screen.

Table 41: The Security: Device Filter Screen

Connected Devices	
Show	Click this to load the **Connected Devices** list.
Refresh	Click this to reload the **Connected Devices** list.
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.

Table 41: The Security: Device Filter Screen (continued)

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.
Status	This displays whether or not the connected device is active.
Action	▸ Click **Add** to make changes to the device's filtering status; see Adding or Editing a Managed Device on page 129 for information on the screen that displays. ▸ Click **Clear** to remove the device from the list.
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 CODA-4x8x. ▸ Select **Allow Listed** to permit only devices you added to the **Managed Devices** list to access the CODA-4x8x and the network. All other devices are denied access. ▸ Select **Block Listed** to permit all devices except those you added to the **Managed Devices** list to access the CODA-4x8x 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**.

Table 41: The Security: Device Filter Screen (continued)

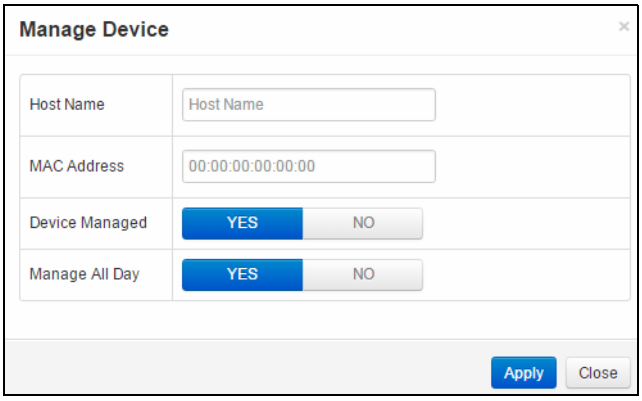
Action	Click **Manage** to make changes to a managed device rule (see Adding or Editing a Managed Device on page 129).
Save Changes	Click this to save your changes to the fields in this screen.
Add Managed Device	Click this to add a new managed device rule (see Adding or Editing a Managed Device on page 129).
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 LAN device, click **Add Managed Device** in the **Security** > **Device Filter** screen.
- To edit an existing managed LAN device, locate the device in the **Security** > **Device Filter** screen and click its **Add** button.
- To add a new managed wireless network device, click **Add Managed Device** in the **Wireless** > **Access Control** screen.
- To edit an existing managed wireless network device, locate the device in the **Wireless** > **Access Control** screen and click its **Manage** button.

The following screen displays.

Figure 53: The Security: Device Filter Add/Edit Screen

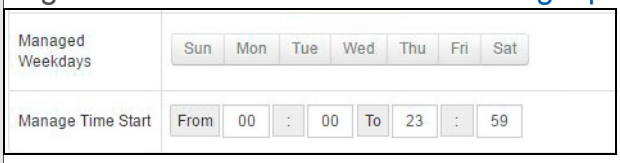


The following table describes the labels in this screen.

Table 42: 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.
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.

Table 42: The Security: Device Filter Add/Edit Screen

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 54: Additional Device 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.

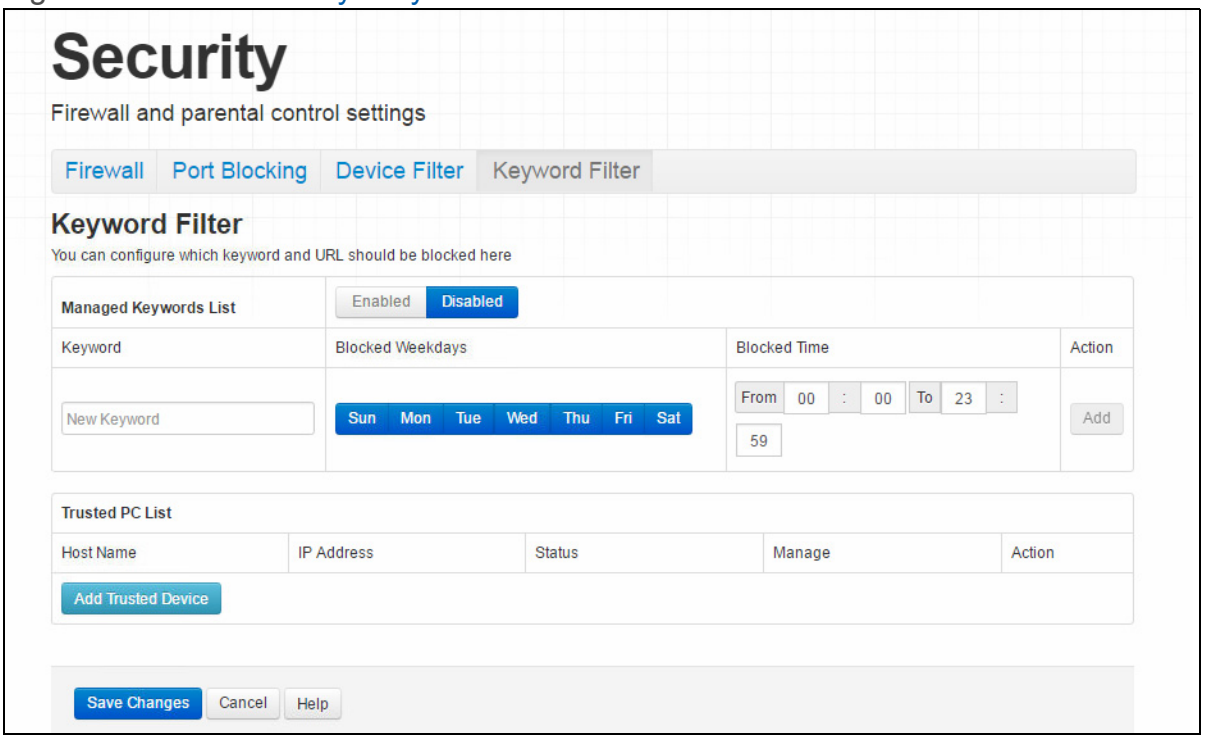
7.5 The Security: Keyword Filter Screen

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.

You can also create and edit trusted device rules. Trusted devices are those to which keyword filtering rules are not applied.

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

Figure 55: The Security: Keyword Filter Screen



The following table describes the labels in this screen.

Table 43: 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 CODA-4x8x 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.
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.

Table 43: The Security: Keyword Filter Screen (continued)

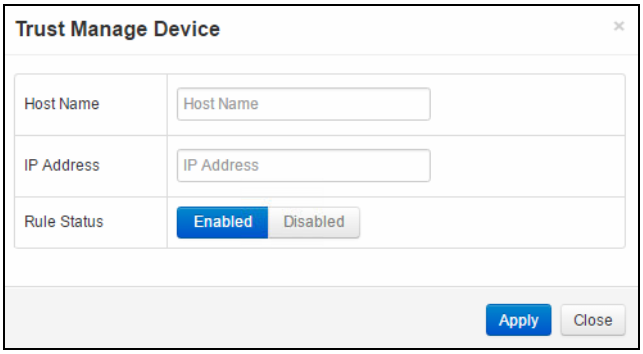
Action	Click **Add** to create a new keyword blocking rule; a new row of fields display.
Trusted PC List	
Host Name	This displays the arbitrary name of each trusted PC you configured.
IP Address	This displays the IP address of each trusted PC. Every network device has a MAC address that uniquely identifies it.
Status	This displays whether the device is currently trusted (**Enabled**) or untrusted (**Disabled**).
Manage	Click **Manage** to make changes to the trusted device rule. See Adding or Editing a Keyword Filter Trusted Device Rule on page 133 for information on the screen that displays.
Action	Click **Delete** to remove the trusted device rule.
Add Trusted Device	Click this to create a new trusted device rule. See Adding or Editing a Keyword Filter Trusted Device Rule on page 133 for information on the screen that displays.
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 Keyword Filter Trusted Device Rule

- To add a new trusted device rule, click **Add Trusted PC** in the **Security** > **Keyword Filter** screen.
- To edit an existing trusted device rule, locate the rule in the **Security** > **Keyword Filter** screen and click its **Manage** button.

The following screen displays.

Figure 56: The Security: Keyword Filter Trusted Device Add/Edit Screen



The following table describes the labels in this screen.

Table 44: The Security: Keyword Filter Trusted Device Add/Edit Screen

Host Name	Enter a name to identify the device.
IP Address	Enter the IP address of the device.
Rule Status	Use this field to define whether the trusted device rule should be active or not. ▸ Select **Enabled** to activate the trusted device rule. ▸ Select **Disabled** to deactivate the trusted device rule.
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 rule.

8

Advanced

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

8.1 Advanced Overview

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

8.1.1 DDNS

The Dynamic Domain Name System allows simple, easy-to-remember names, like domain names such as "example.com", to be mapped on to dynamic, often-changing, IP addresses. such as "123.123.123.123". In the context of home and office networking, DDNS allows you to make data and systems on your local area network available over the Internet, via an human-friendly name (just like a domain name).

The benefits of DDNS in this context are not merely that it provides a human-friendly name by which systems may be accessed, rather than requiring users to remember an IP address. IP addresses assigned to customers by Internet Service Providers often change from day to day, unlike the static IP addresses on which websites tend to run (except those on more inexpensive shared hosting systems, usually). This means even remembering an IP address of a system would be of only very short-

term value to a user. DDNS dynamically solves this problem by allowing a DDNS client, like a home or office network router, to periodically update a DDNS host when its IP address changes. The DDNS host is therefore able to point a name like "myofficerouter.ddnshost.com" to whatever the router's current IP address actually is.

NOTE: In order to use DDNS, you will need an account with a DDNS service provider, who will act as your DDNS host.

8.1.2 RIP

The Routing Instruction Protocol (RIP) is a distance-vector routing protocol that the CODA-4x8x uses to exchange routing information with other routers in order not only to enable routing across devices, but to determine the most efficient path the routed data should take. RIP utilizes "hop count" - the number of journeys from one device to another required to deliver data to its destination - as a metric on which to base routing decisions.

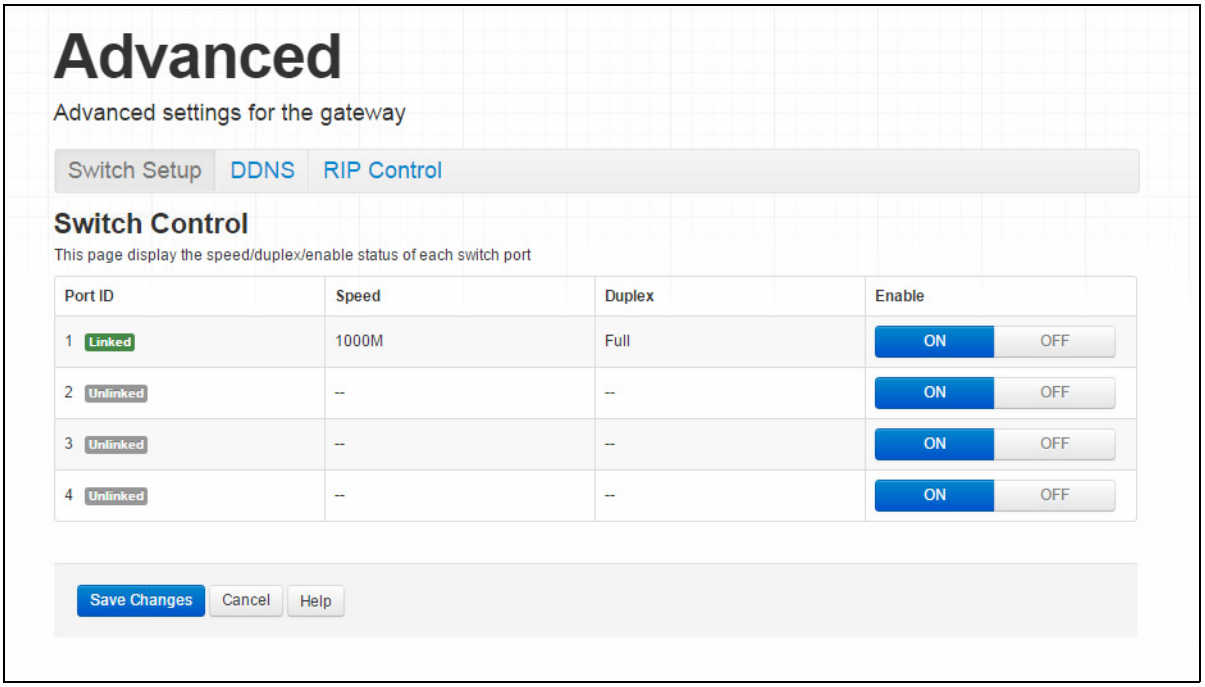
RIP version 1 and RIP version 2 differ significantly, particularly in that version 1 broadcasts information, whereas version 2 multicasts it (and carries more data).

8.2 The Advanced: Switch Setup Screen

Use this screen to see information about the data rate and flow of each of the CODA-4x8x's **LAN** ports, and to activate or deactivate each port.

Click **Advanced** > **Switch Setup**. The following screen displays.

Figure 57: The Advanced: Switch Setup Screen



The following table describes the labels in this screen.

Table 45: The Advanced: Switch Setup Screen

Port	This displays the physical LAN port number.
Speed	This displays the maximum achievable data speed in megabits per second (Mbps).
Duplex	▸ This displays **Full** when data can flow between the CODA-4x8x and the connected device in both directions simultaneously. ▸ This displays **Half** when data can flow between the CODA-4x8x and the connected device in only one direction at a time.
Enable	▸ Select **ON** to enable communications between the CODA-4x8x and devices connected to the port. ▸ Select **OFF** to disable communications between the CODA-4x8x and devices connected to the port.
Save Changes	Click this to save your changes to the fields in this screen.

Table 45: The Advanced: Switch Setup Screen (continued)

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.

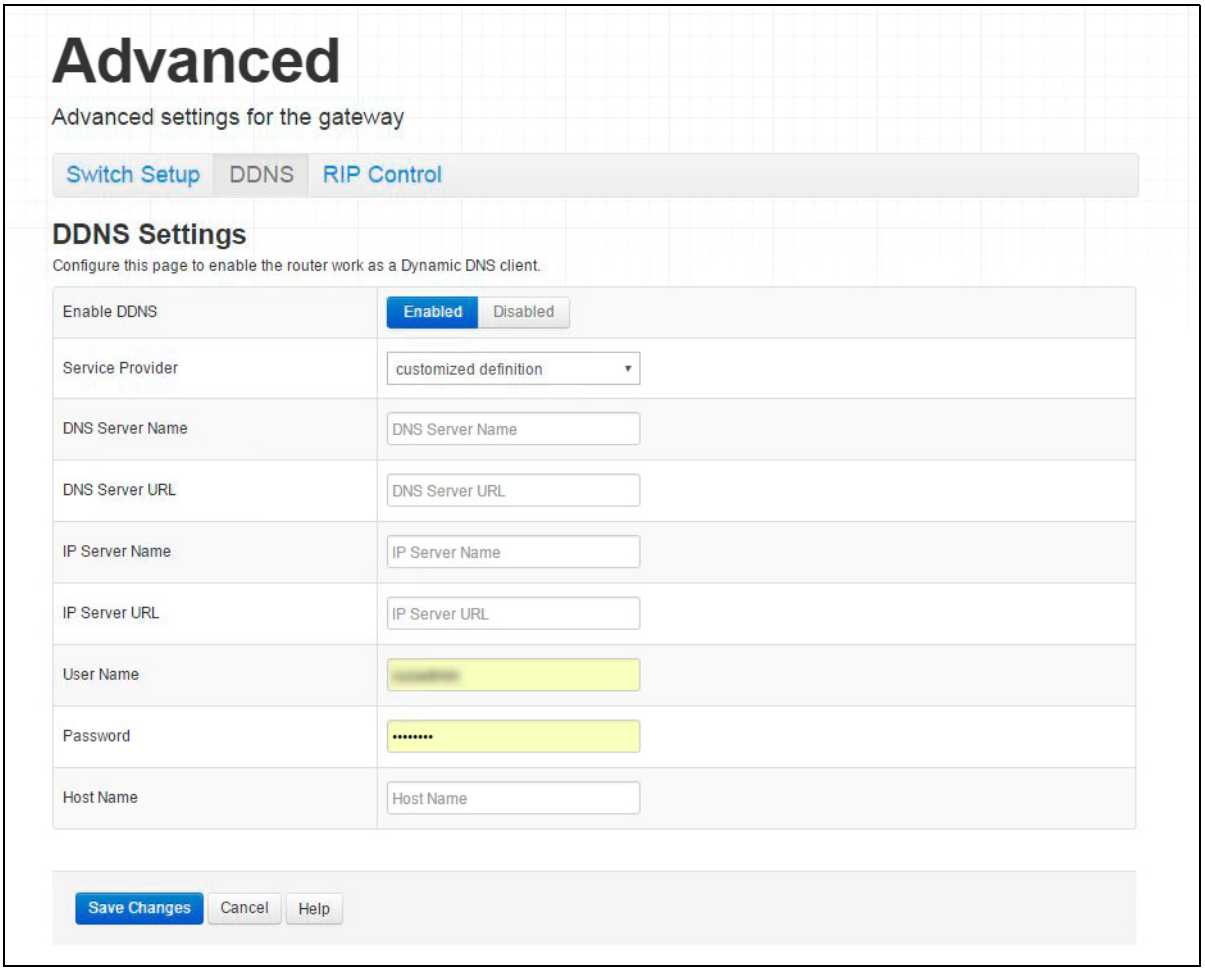
8.3 The Advanced: DDNS Screen

Use this screen to enable or disable Dynamic Domain Name System (DDNS) services on the CODA-4x8x. When DDNS is enabled, the CODA-4x8x acts as a DDNS client, meaning that users can access it by entering an easy-to-remember name in their browser address bar.

NOTE: Using DDNS on your CODA-4x8x requires a DDNS server, such as those operated by DDNS service providers. If you want to use DDNS but do not yet have access to such a service, this screen's Service Provider list contains the names of many popular DDNS service providers.

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

Figure 58: The Advanced: DDNS Screen



The following table describes the labels in this screen.

Table 46: The Advanced: DDNS Screen

Enable DDNS	Use this field to turn DDNS on or off. ▸ Select **Enabled** to turn DDNS on. The CODA-4x8x acts as a DDNS client. ▸ Select **Disabled** to turn DDNS off. The CODA-4x8x will no longer act as a DDNS client.
Service Provider	Select your DDNS service provider from the list or, if your service provider is not in the list, select **Customized Definition**. The customized definition fields display.
Customized Definition Fields	These fields display only when you select **Customized Definition** in the **Service Provider** field.

Table 46: The Advanced: DDNS Screen (continued)

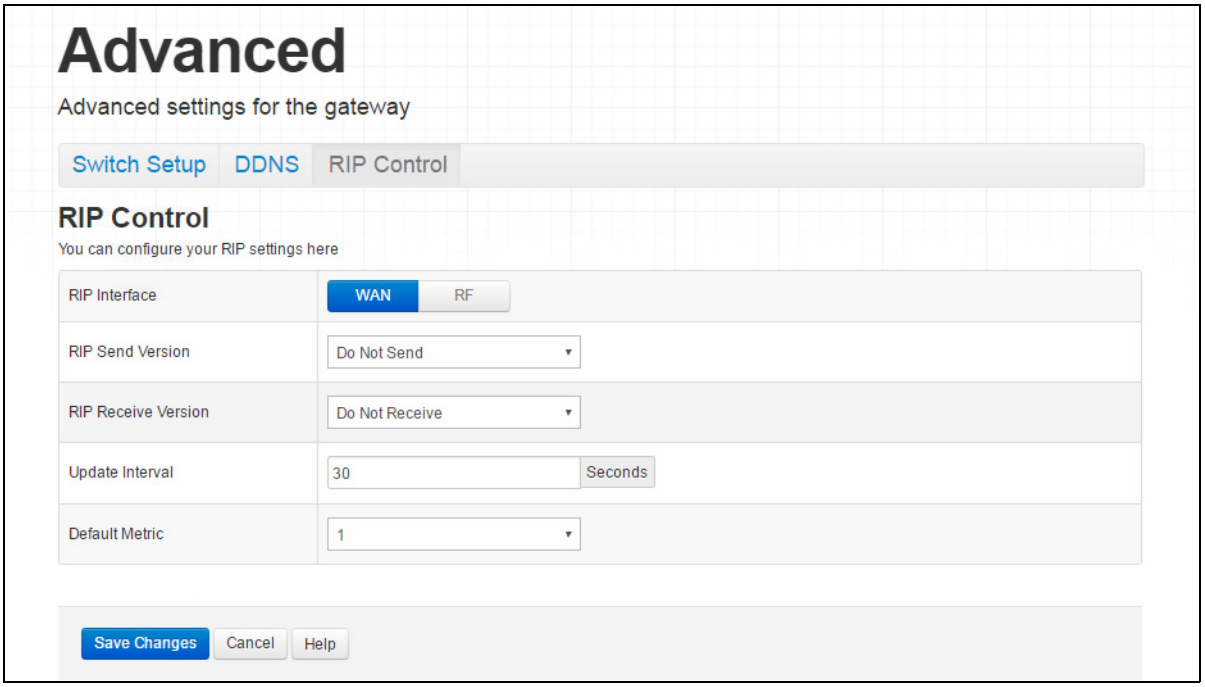
DNS Server Name	Enter the name of the DNS server, as supplied by the service's operator.
DNS Server URL	Enter the web address of the DNS server, as supplied by the service's operator.
IP Server Name	Enter the name of the IP address server, as supplied by the service's operator.
IP Server URL	Enter the web address of the IP address server, as supplied by the service's operator.
User Name	Enter your DDNS account's username, as supplied by the service's operator.
Password	Enter your DDNS account's password, as supplied by the service's operator.
Host Name	Enter the name by which you will access the CODA-4x8x, as supplied by the service's operator.
Save	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.

8.4 The Advanced: RIP Control Screen

Use this screen to configure the CODA-4x8x's Routing Instruction Protocol (RIP) settings.

Click **Advanced** > **RIP Control**. The following screen displays.

Figure 59: The Advanced: RIP Control Screen



The following table describes the labels in this screen.

Table 47: The Advanced: RIP Control Screen

RIP Interface	Use this field to control the interface on which RIP networking should occur. ▸ Select **WAN** to exchange RIP information on the CODA-4x8x's **Cable** connection. ▸ Select **RF** to exchange RIP information on the CODA-4x8x's wireless network.
RIP Send Version	Use this field to control the type of RIP information to be sent on the specified interface. ▸ Select **Do not send** to have the CODA-4x8x not send RIP information. ▸ Select **RIP 1** to send only RIP version 1 information. ▸ Select **RIP 2** to send only RIP version 2 information. ▸ Select **RIP 1/2** to send both RIP version 1 and version 2 information.

Table 47: The Advanced: RIP Control Screen (continued)

RIP Receive Version	Use this field to control the type of RIP information that the CODA-4x8x will forward from the specified interface to devices on the LAN. • Select **Do not receive** to have the CODA-4x8x not send RIP information. • Select **RIP 1** to receive and forward only RIP version 1 information. • Select **RIP 2** to receive and forward only RIP version 2 information. • Select **RIP 1/2** to receive and forward both RIP version 1 and version 2 information.
Update interval	Enter the number of seconds that should elapse between transmission of RIP information.
Default Metric	Select the metric value to be used for RIP data redistribution when routing metrics are incompatible.

9

Troubleshooting

Use this section to solve common problems with the CODA-4x8x and your network. It contains the following sections:

Problem: None of the LEDs Turn On

The CODA-4x8x 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 CODA-4x8x can damage the CODA-4x8x.

2. Ensure that the power adaptor is connected to the CODA-4x8x 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.
4. Disconnect and re-connect the power adaptor to the power source and the CODA-4x8x.
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 CODA-4x8x's hardware is connected correctly; see the Quick Installation Guide.
3. Disconnect and re-connect the power adaptor to the CODA-4x8x.
4. If none of the above steps solve the problem, consult your vendor.

Problem: I Forgot the CODA-4x8x's Admin Username or Password

The default username is cusadmin, and the password is the same as the password you configured for the wireless network in the EasyConnect setup wizard (see EasyConnect on page 26).

Problem: I Cannot Access the CODA-4x8x or the Internet

1. Ensure that you are using the correct IP address for the CODA-4x8x.
2. Check your network's hardware connections, and that the CODA-4x8x's LEDs display correctly (see LEDs on page 18).
3. Make sure that your computer is on the same subnet as the CODA-4x8x; see IP Address Setup on page 21.
4. If the above steps do not work, you need to reset the CODA-4x8x. See Resetting the CODA-4x8x on page 25. All user-configured data is lost, and the CODA-4x8x is returned to its default settings. If you previously backed-up a more recent version your CODA-4x8x's settings, you can now upload them to the CODA-4x8x; see The Admin: Backup Screen on page 112.
5. If the problem persists, contact your vendor.

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 CODA-4x8x'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 CODA-4x8x's signal quality and coverage area.

3 Ensure that the CODA-4x8x and the wireless client are set to use the same wireless mode, SSID and security settings (see The Wireless Basic Settings Screen on page 64 and The WPS & Security Screen on page 72).

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 CODA-4x8x and the button on the wireless client within 2 minutes of one another.

Index

Numbers

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

