CyberData

The IP Endpoint Company

Singlewire InformaCast Indoor Intercom with Keypad, Flush Mount

Operations Guide

Part #011308

Document Part #*930931I*
for Firmware Version *11.9.2*

CyberData Corporation
3 Justin Court
Monterey, CA 93940
(831) 373-2601

PoE VoIP Intercom Operations Guide 930931I
Part # 011308

CyberData
The IP Endpoint Company

Technical Support

The fastest way to get technical support for your VoIP product is to submit a VoIP Technical Support form at the following website:
http://support.cyberdata.net/

Phone: (831) 373-2601, Ext. 333
Email: support@cyberdata.net
Fax: (831) 373-4193
Company and product information is at **www.cyberdata.net**.

Revision Information

Revision 930931I, which corresponds to firmware version 11.9.2, was released on October 27, 2017, and has the following changes:

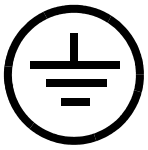
- Updates Figure 1-1, "Model Number Label"
- Updates Figure 2-20, "Home Page"
- Updates Figure 2-21, "Device Configuration Page"
- Adds Section 2.6.7, "Configure the Security"
- Updates Figure 2-23, "Button Configuration Page"
- Updates Figure 2-26, "Network Configuration Page"
- Updates Figure 2-27, "SIP Configuration Page"
- Updates Figure 2-28, "SIP Page Set to Point-to-Point Mode"
- Updates Figure 2-29, "Multicast Configuration Page"
- Updates Figure 2-30, "Sensor Configuration Page"
- Updates Figure 2-31, "Audiofiles Configuration Page"
- Updates Figure 2-36, "Event Configuration Page"
- Updates Figure 2-38, "Autoprovisioning Page"
- Updates Figure 2-40, "Firmware Page"
- Updates Figure 2-41, "Home Page"

Browsers Supported

The following browsers have been tested against firmware version 11.9.2:

- Chrome (version 570.02987.98)
- Firefox: (version 55.0.2)
- Internet Explorer (version 11.0.9600.18314)

Pictorial Alert Icons

 GENERAL ALERT	General Alert *This pictoral alert indicates a potentially hazardous situation. This alert will be followed by a hazard level heading and more specific information about the hazard.*
	Ground *This pictoral alert indicates the Earth grounding connection point.*

Hazard Levels

Danger: Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury. This is limited to the most extreme situations.

Warning: Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.

Caution: Indicates a potentially hazardous situation which, if not avoided, could result in minor or moderate injury. It may also alert users against unsafe practices.

Notice: Indicates a statement of company policy (that is, a safety policy or protection of property).

The safety guidelines for the equipment in this manual do not purport to address all the safety issues of the equipment. It is the responsibility of the user to establish appropriate safety, ergonomic, and health practices and determine the applicability of regulatory limitations prior to use. Potential safety hazards are identified in this manual through the use of words Danger, Warning, and Caution, the specific hazard type, and pictorial alert icons.

Important Safety Instructions

1. Read these instructions.
2. Keep these instructions.
3. Heed all warnings.
4. Follow all instructions.
5. Do not use this apparatus near water.
6. Clean only with dry cloth.
7. Do not block any ventilation openings. Install in accordance with the manufacturer's instructions.
8. Do not install near any heat sources such as radiators, heat registers, stoves, or other apparatus (including amplifiers) that produce heat.
9. Do not defeat the safety purpose of the polarized or grounding-type plug. A polarized plug has two blades with one wider than the other. A grounding type plug has two blades and a third grounding prong. The wide blade or the third prong are provided for your safety. If the provided plug does not fit into your outlet, consult an electrician for replacement of the obsolete outlet.
10. Protect the power cord from being walked on or pinched particularly at plugs, convenience receptacles, and the point where they exit from the apparatus.
11. Only use attachments/accessories specified by the manufacturer.
12. Refer all servicing to qualified service personnel. Servicing is required when the apparatus has been damaged in any way, such as power-supply cord or plug is damaged, liquid has been spilled or objects have fallen into the apparatus, the apparatus has been exposed to rain or moisture, does not operate normally, or has been dropped.
13. Prior to installation, consult local building and electrical code requirements.

Warning

Electrical Hazard: This product should be installed by a licensed electrician according to all local electrical and building codes.

Warning

Electrical Hazard: To prevent injury, this apparatus must be securely attached to the floor/wall in accordance with the installation instructions.

Warning

The PoE connector is intended for intra-building connections only and does not route to the outside plant.

Contents

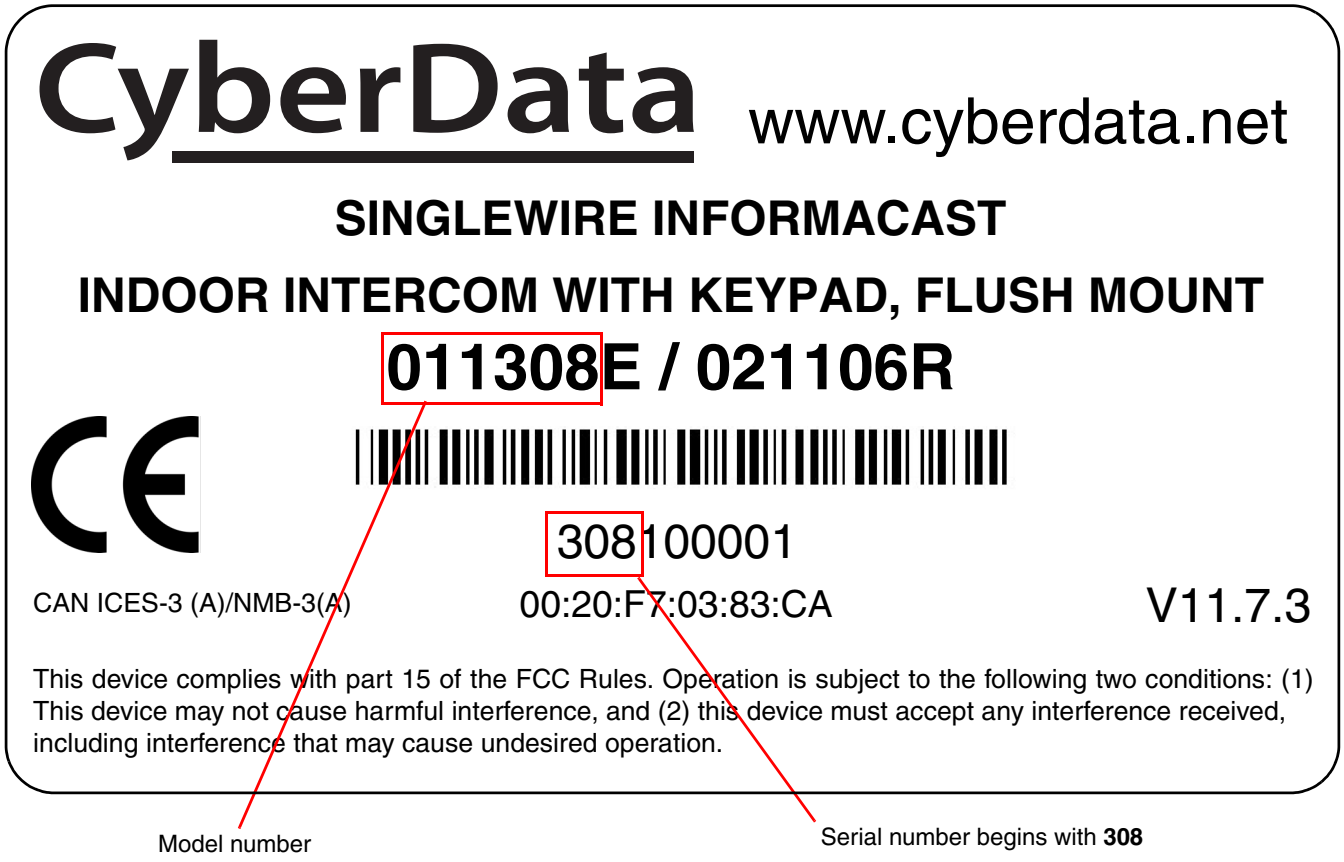
1 Product Overview

1.1 How to Identify This Product

To identify the Singlewire InformaCast Indoor Intercom with Keypad, Flush Mount, look for a model number label similar to the one shown in Figure 1-1. Confirm the following:

- The model number on the label should be **011308**.
- The serial number on the label should begin with **308**.

Figure 1-1. Model Number Label



1.2 Typical System Installation

The following figures illustrate how the Singlewire InformaCast Indoor Intercom with Keypad, Flush Mount can be installed as part of a VoIP phone system.

Figure 1-2. Typical Installation

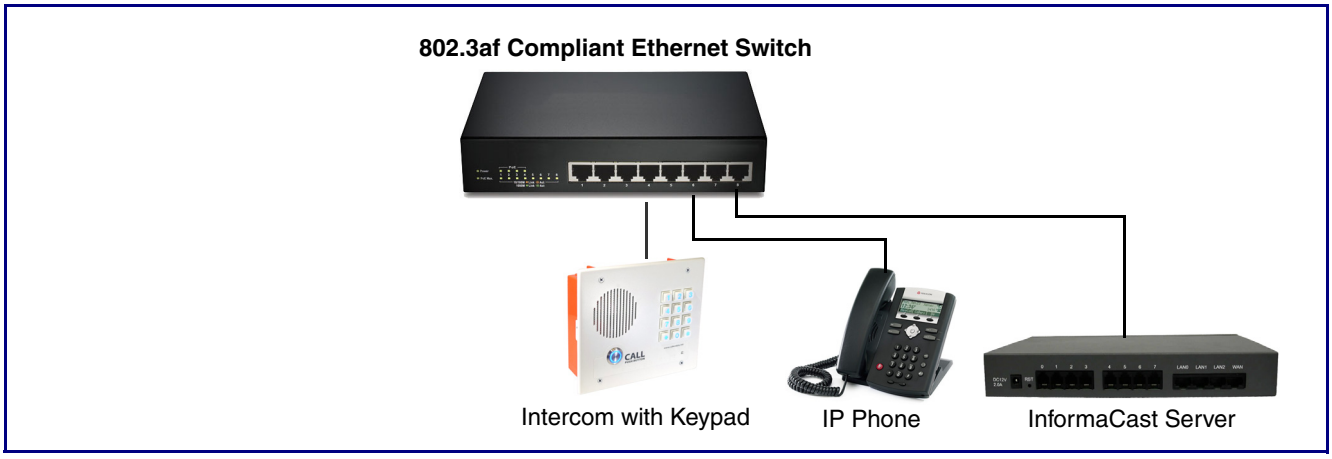


Figure 1-3. Installation with the Auxiliary RGB Strobe or the SIP RGB Strobe

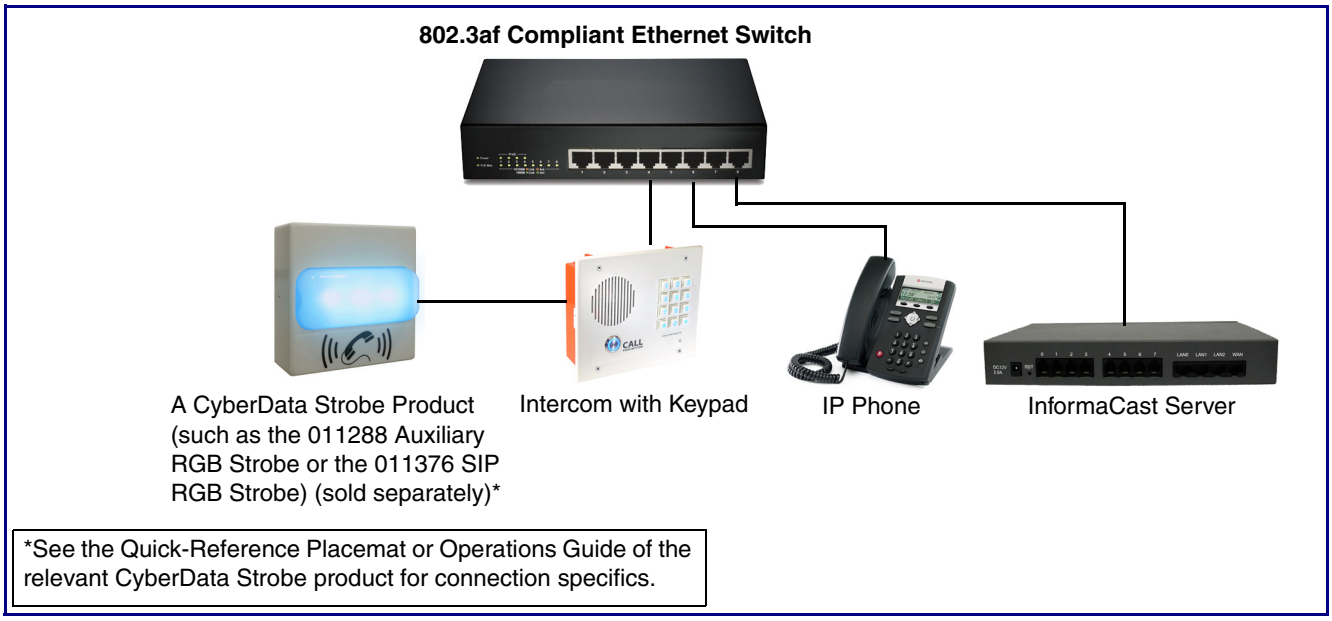


Figure 1-4. Installation with the Door Strike Relay Module

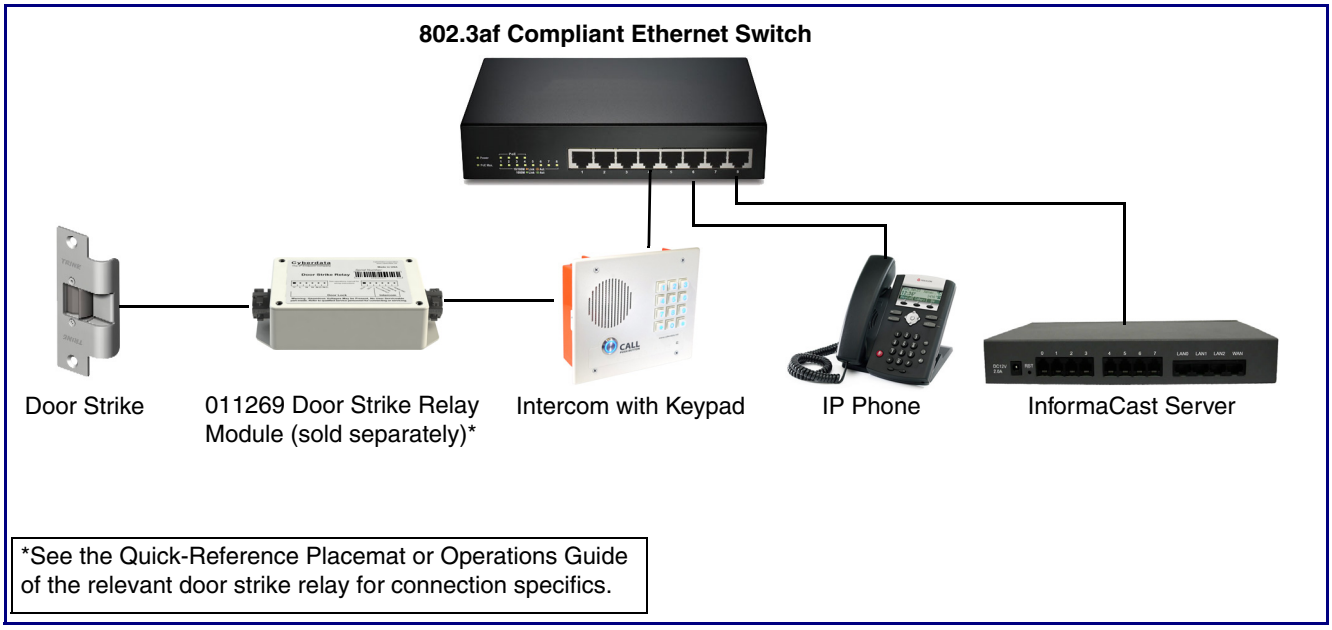
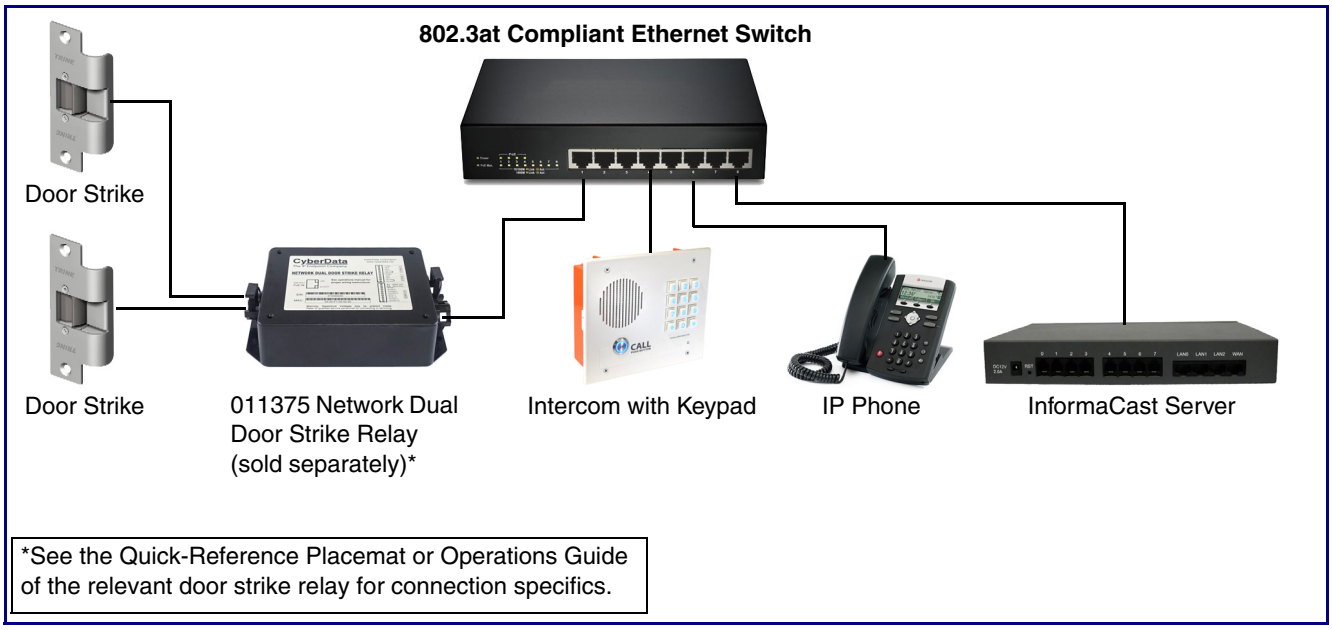


Figure 1-5. Installation with the Network Dual Door Strike Relay



1.3 Product Features

The Singlewire InformaCast Indoor Intercom with Keypad, Flush Mount has the following features:

- InformaCast® compliant
- InformaCast® resiliency protocol
- Capable of receiving SingleWire Informacast, SIP, and Multicast messages
- Supports 500 Access Codes
- Optional red/green/blue/white strobe kit connection available (part# 011288)
- Integrates with Network Dual Door Strike Relay Module (part# 011375) and Door Strike Relay Module (part# 011269)
- Enhanced acoustic echo canceler
- PoE 802.3af enabled (Power-over-Ethernet)
- 12-key keypad with backlight
- Programmable speed dial
- SIP compliant
- Full-duplex voice operation
- Now supports SRST (Survivable Remote Site Telephony) in a Cisco environment
- Streamlined case design
- Optional weather shroud for even greater weather protection
- Network web management and firmware download
- Network adjustable speaker volume
- Concurrent SIP and multicast paging
- Dry relay contact for auxiliary control
- Door closure and tamper alert signal

1.4 Supported Protocols

The Intercom supports the following protocols:

- SIP
- Singlewire InformaCast
- Singlewire Failover
- HTTP Web-based configuration

  Provides an intuitive user interface for easy system configuration and verification of Intercom operations.
- DHCP Client

  Dynamically assigns IP addresses in addition to the option to use static addressing.
- TFTP Client

  Facilitates hosting for the Autoprovisioning configuration file.
- RTP
- Facilitates autoprovisioning configuration values on boot
- Audio Encodings

  PCMU (G.711 mu-law)

  PCMA (G.711 A-law)

  G.722

  Packet Time 20 ms

1.5 Supported SIP Servers

The following link contains information on how to configure the device for the supported SIP servers:

http://www.cyberdata.net/connecting-to-ip-pbx-servers/

1.6 Specifications

Table 1-1. Specifications

Specification	
Ethernet I/F	10/100 Mbps
Protocol	SIP RFC 3261 Compatible and InformaCast v4.0 and later
Power Input	PoE 802.3af compliant or +8 to +12VDC @ 1000mA Regulated Power Supply[a]
Speaker Output	2 Watts Peak Power
On-Board Relay	1A at 30 VDC
Operating Range	Temperature: -40° C to 55° C (-40° F to 131° F) Humidity: 5-95%, non-condensing
Storage Temperature	-40° C to 70° C (-40° F to 158° F)
Storage Altitude	Up to 15,000 ft. (4573 m)
IP Rating	IP65
Payload Types	G711, A-law and µ-law, G.722
Dimensions[b]	7.480 in. [190 mm] Length 2.284 in. [58 mm] Width 5.118 in. [130 mm] Height
Weight	2.8 lbs. [1.27 kg]
Boxed Weight	4.0 lbs. [1.81 kg] Weather Shroud is 1.2 lbs. [0.54 kg]
Compliance	CE; EMC Directive – Class A EN 55032 & EN 55024, LV Safety Directive – EN 60950-1, RoHS Compliant, FCC; Part 15 Class A, Industry Canada; ICES-3 Class A, IEEE 802.3 Compliant
Part Number	011308

a. Contacts 1 and 2 on the terminal block are only for powering the device from a non-PoE 12VDC power source as an alternative to Network PoE power. Use of these contacts for any other purpose will damage the device and void the product warranty.

b. Dimensions are measured from the perspective of the product being upright with the front of the product facing you.

1.7 Compliance

1.7.1 CE Testing

CE testing has been performed according to EN ISO/IEC 17050 for Emissions, Immunity, and Safety. The Declaration of Conformity can be supplied upon request.

1.7.2 FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

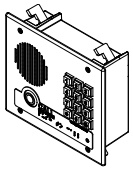
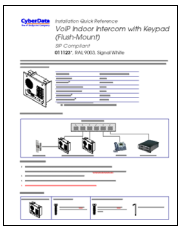
2 Installing the Singlewire InformaCast Indoor Intercom with Keypad, Flush Mount

2.1 Parts List

Table 2-2 illustrates the parts for the Singlewire InformaCast Indoor Intercom with Keypad, Flush Mount.

Note See Appendix A, "Mounting the Singlewire InformaCast Indoor Intercom with Keypad, Flush Mount" for physical mounting information.

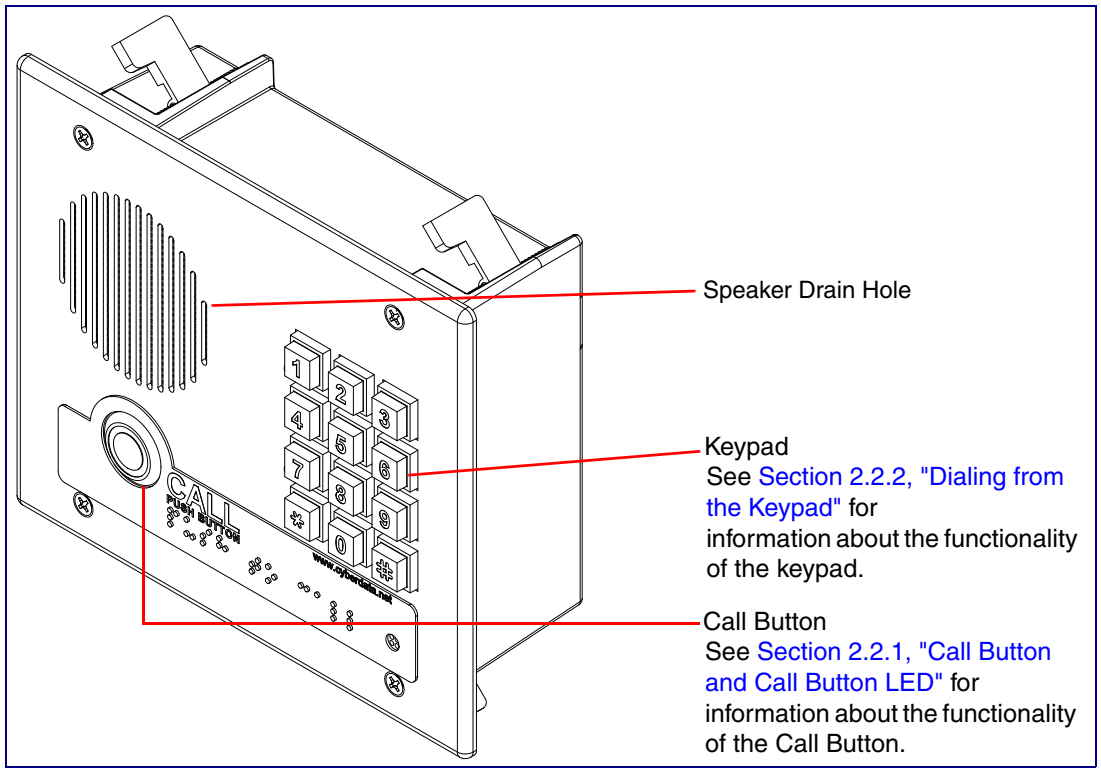
Table 2-2. Parts List

Quantity	Part Name	Illustration
1	Singlewire InformaCast Indoor Intercom with Keypad, Flush Mount Assembly	
1	Installation Quick Reference Guide	
1	Mounting Accessory Kit	

2.2 Intercom Components

Figure 2-1 shows the components of the Intercom.

Figure 2-1. Intercom Components

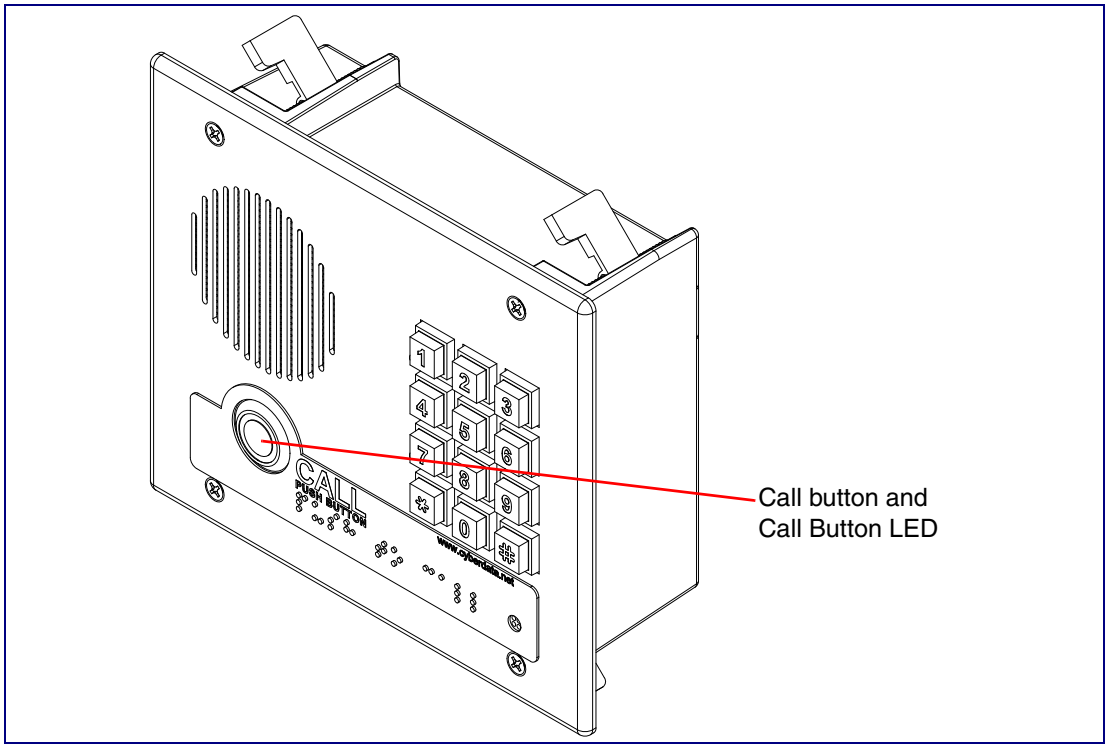


2.2.1 Call Button and Call Button LED

2.2.1.1 Call Button LED Function

- Upon initial power or reset, the Call Button LED will illuminate.
- During network setup the Call Button LED will blink 10 times per second until the device can find a network address. This can take from 5 to 60 seconds.
- The device “autoprovisions” by default, and the initial process may take several minutes as the device searches for and downloads updates. The Call Button LED will blink during this process. During the initial provisioning, or after the factory defaults have been reset, the device may download firmware twice. The device will blink, remain solid for 10 to 20 seconds, and then resume blinking. This process will take longer if there are many audio files downloading.
- When the software has finished initialization, the Call Button LED will blink twice.
- When a call is established (not just ringing), the Call Button LED will blink.
- On the **Device Configuration Page**, there is an option called **Button and Keypad Lit when Idle**. This option sets the normal state for the Call Button LED. The Call Button LED will still blink during initialization and calls.
- The Call Button LED flashes briefly at the beginning of RTFM mode.

Figure 2-2. Call Button and Call Button LED



2.2.2 Dialing from the Keypad

- See the Enable Telephone Operation setting in Section 2.6.6, "Configure the Button Parameters".

2.3 Intercom Setup

2.3.1 Intercom Connections

Figure 2-3 shows the pin connections on the terminal block. This terminal block can accept 16 AWG gauge wire.

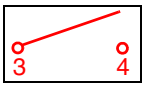
Note As an alternative to using PoE power, you can supply +8 to +12VDC @ 1000mA Regulated Power Supply into the terminal block.

Caution

Equipment Hazard: Contacts 1 and 2 on the terminal block are only for powering the device from a non-PoE 12 VDC power source as an alternative to Network PoE power. Use of these contacts for any other purpose will damage the device and void the product warranty.

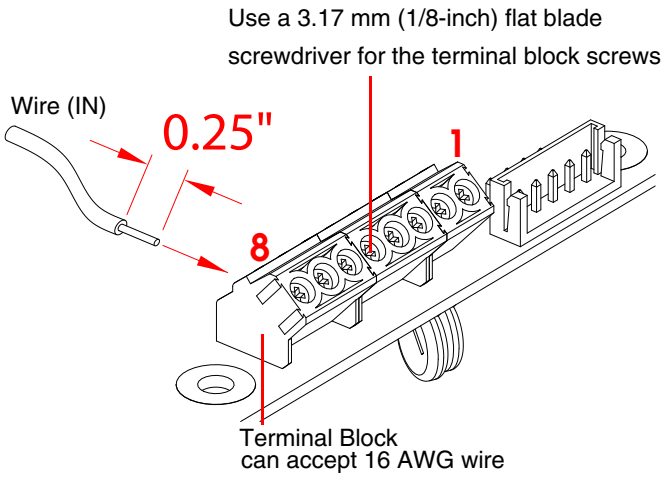
Figure 2-3. Connections and Alternate Power Input

Alternate Power Input:
1 = +8 to +12VDC @ 1000mA Regulated Power Supply*
2 = Power Ground*



Relay Contact:
(1 A at 30 VDC for continuous loads)
3 = Relay Common
4 = Relay Normally Open Contact
5 = Sense Input
6 = Sense Ground
7 = Remote Switch "A"
8 = Remote Switch "B"

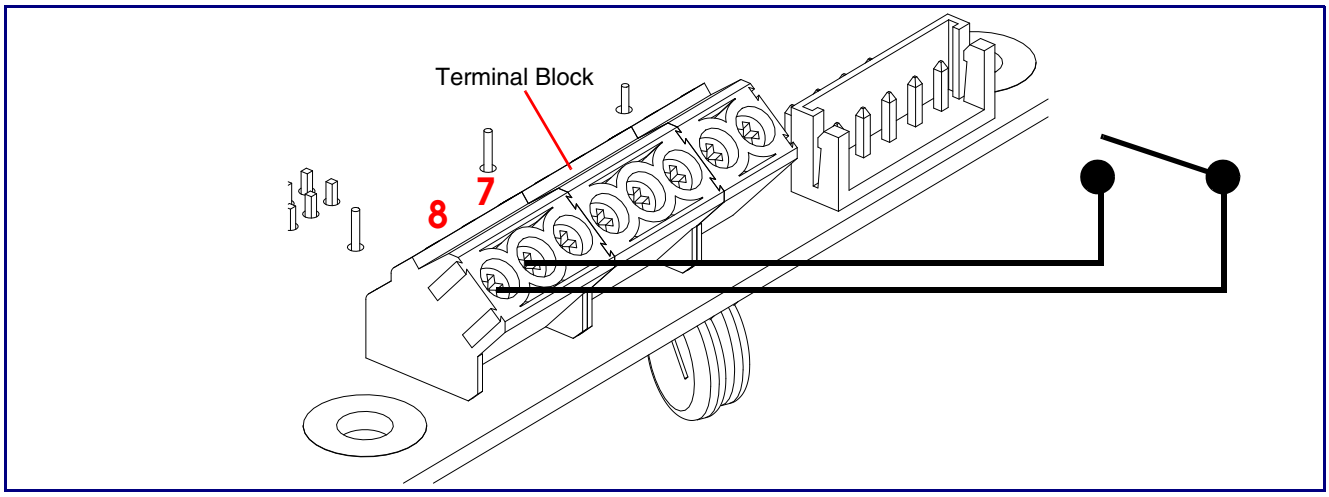
*Contacts 1 and 2 on the terminal block are only for powering the device from a non-PoE 12VDC power source as an alternative to Network PoE power. Use of these contacts for any other purpose will damage the device and void the product warranty.



2.3.1.1 Remote Switch Connection

Wiring pins 7 and 8 of the terminal block to a switch will initiate a SIP call when the switch is closed. The call will go to the extension specified as the dial out extension on the **SIP** page.

Figure 2-4. Remote Switch Connection



2.3.2 Using the On-Board Relay

Warning

Electrical Hazard: This product should be installed by a licensed electrician according to all local electrical and building codes.

Warning

Electrical Hazard: The relay contacts are dry and provided for a normally open and momentarily closed configuration. Neither the alternate power input nor PoE power can be used to drive a door strike.

Warning

Electrical Hazard: The relay does not support AC powered door strikes.
Any use of this relay beyond its normal operating range can cause damage to the product and is not covered under our warranty policy.

The device has a built-in relay that can be activated by a web configurable DTMF string that can be received from a VoIP phone supporting out of band (RFC2833) DTMF as well as a number of other triggering events. See the **Device Configuration Page** on the web interface for relay settings.

This relay can be used to trigger low current devices like LED strobes and security camera input signals as long as the load is not an inductive type and the relay is limited to a maximum of 1 Amp @ 30 VDC. Inductive loads can cause excessive “hum” and can interfere with or damage the unit’s electronics.

We highly recommend that inductive load and high current devices use our Door Strike Intermediate Relay product (CD# 011375) (see Section 2.3.3.2, "Network Dual Door Strike Relay Wiring Diagram with External Power Source").

This relay interface also has a general purpose input port that can be used to monitor an external switch and generate an event.

For more information on the sensor options, see the **Sensor Configuration Page** on the web interface.

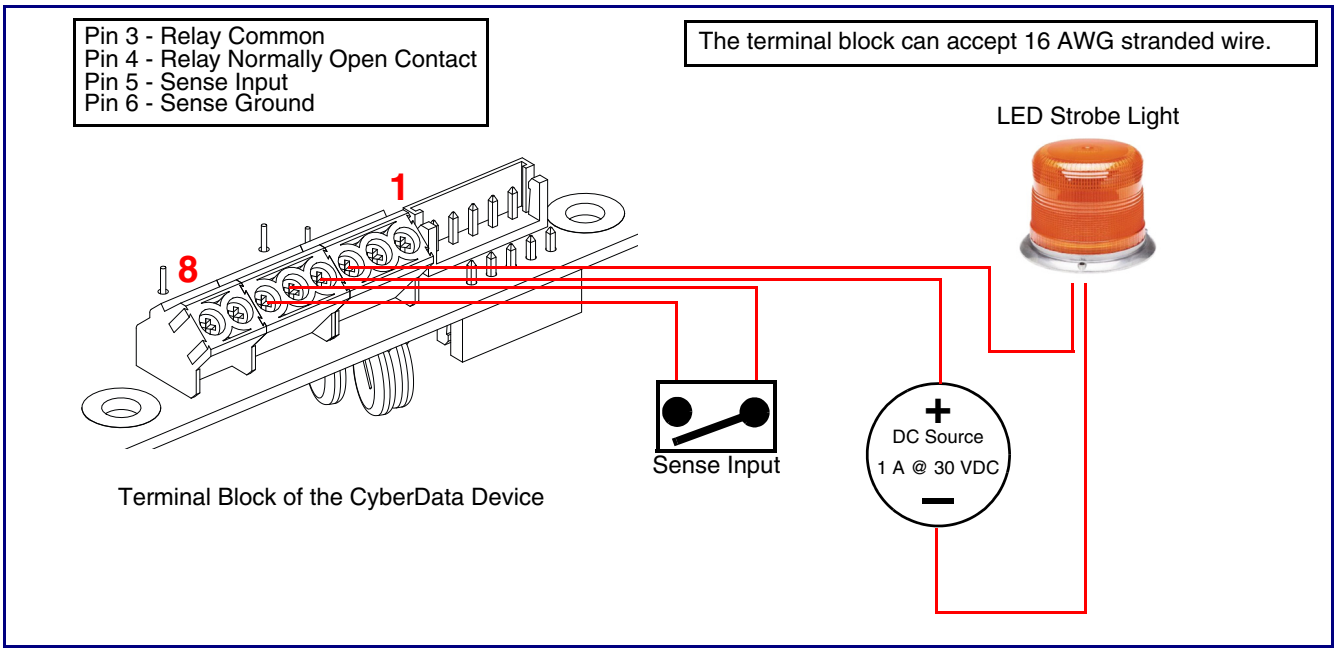
2.3.3 Wiring the Circuit

2.3.3.1 Devices Less than 1A at 30 VDC

If the power for the device is less than 1A at 30 VDC and is not an inductive load, then see Figure 2-5 for the wiring diagram.

When configuring with an inductive load, please use an intermediary relay with a High PIV Ultrafast Switching Diode. We recommend using the CyberData Network Dual Door Strike Relay (CD# 011375) (see Section 2.3.3.2, "Network Dual Door Strike Relay Wiring Diagram with External Power Source").

Figure 2-5. Devices Less than 1A at 30 VDC



2.3.3.2 Network Dual Door Strike Relay Wiring Diagram with External Power Source

For wiring an electronic door strike to work over a network, we recommend the use of our external Network Dual Door Strike Relay (CD# 011375).

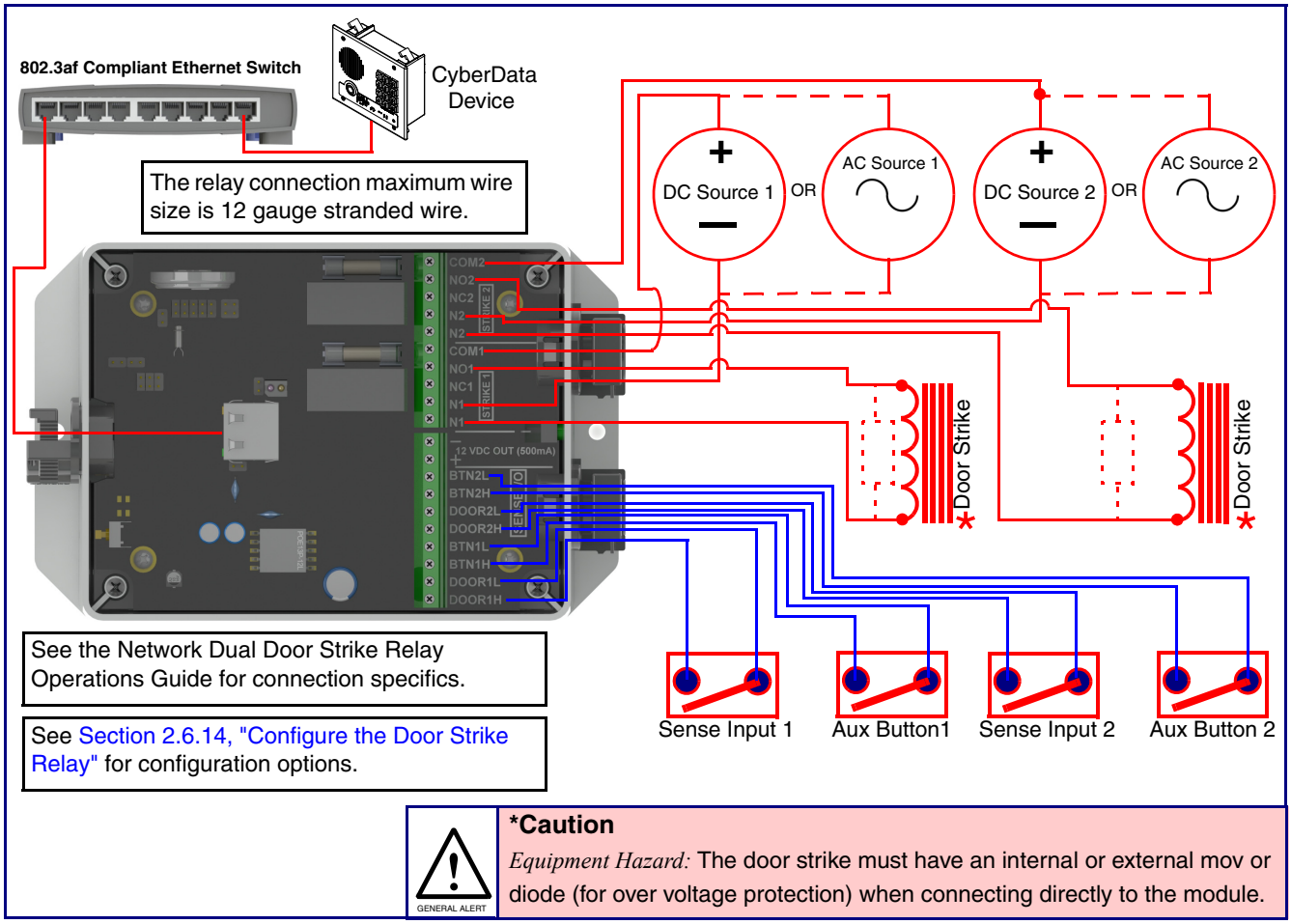
This product provides an easier method of connecting standard door strikes as well as AC and higher voltage devices. See Figure 2-6 and Figure 2-7 for the wiring diagrams.

GENERAL ALERT

Warning

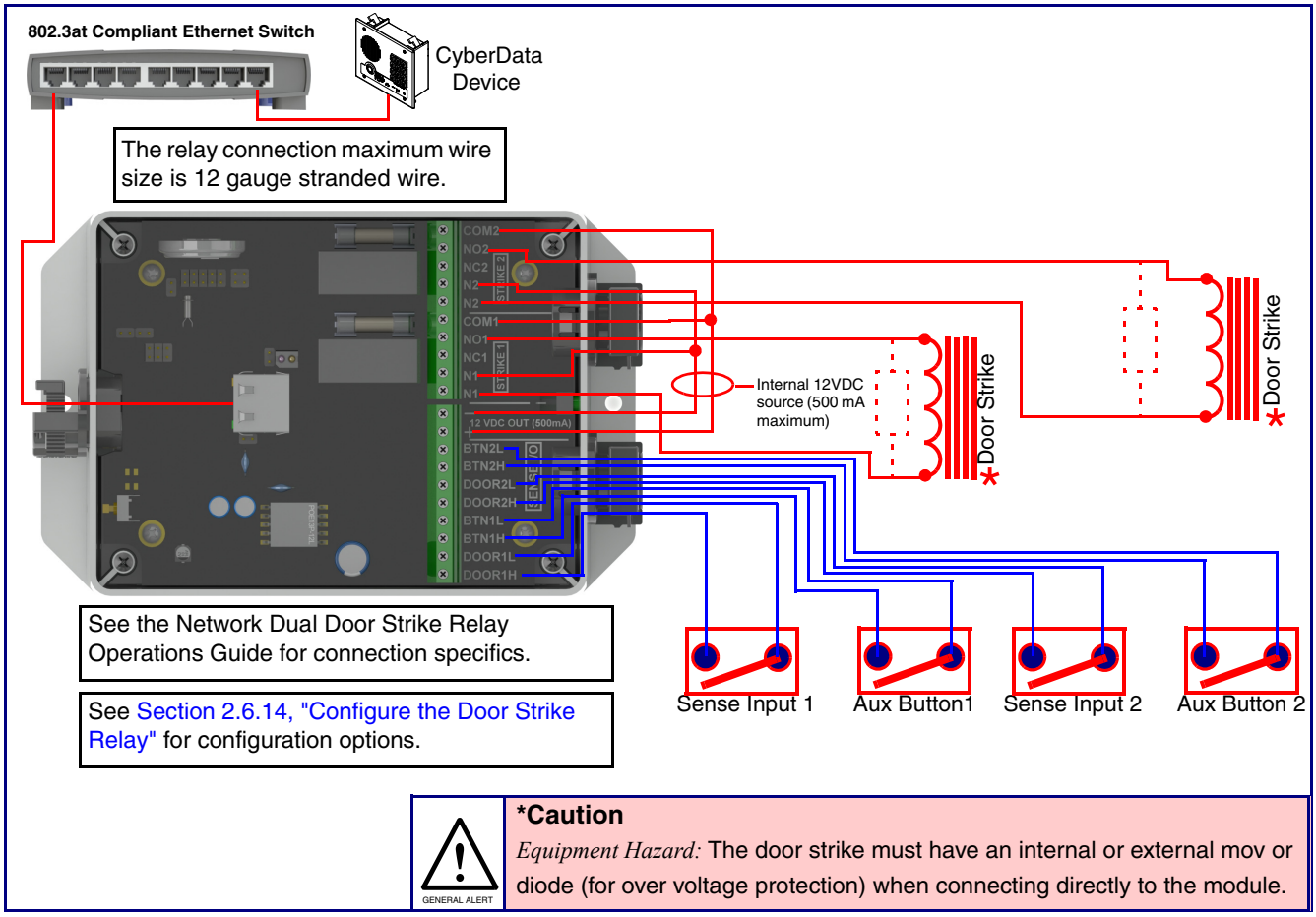
Electrical Hazard: Hazardous voltages may be present. No user serviceable part inside. Refer to qualified service personnel for connecting or servicing.

Figure 2-6. Network Dual Door Strike Relay Wiring Diagram with External Power Source



2.3.3.3 Network Dual Door Strike Relay Wiring Diagram Using PoE+

Figure 2-7. Network Dual Door Strike Relay Wiring Diagram Using PoE+



If you have questions about connecting door strikes or setting up the web configurable options, please contact our support department at the following website:

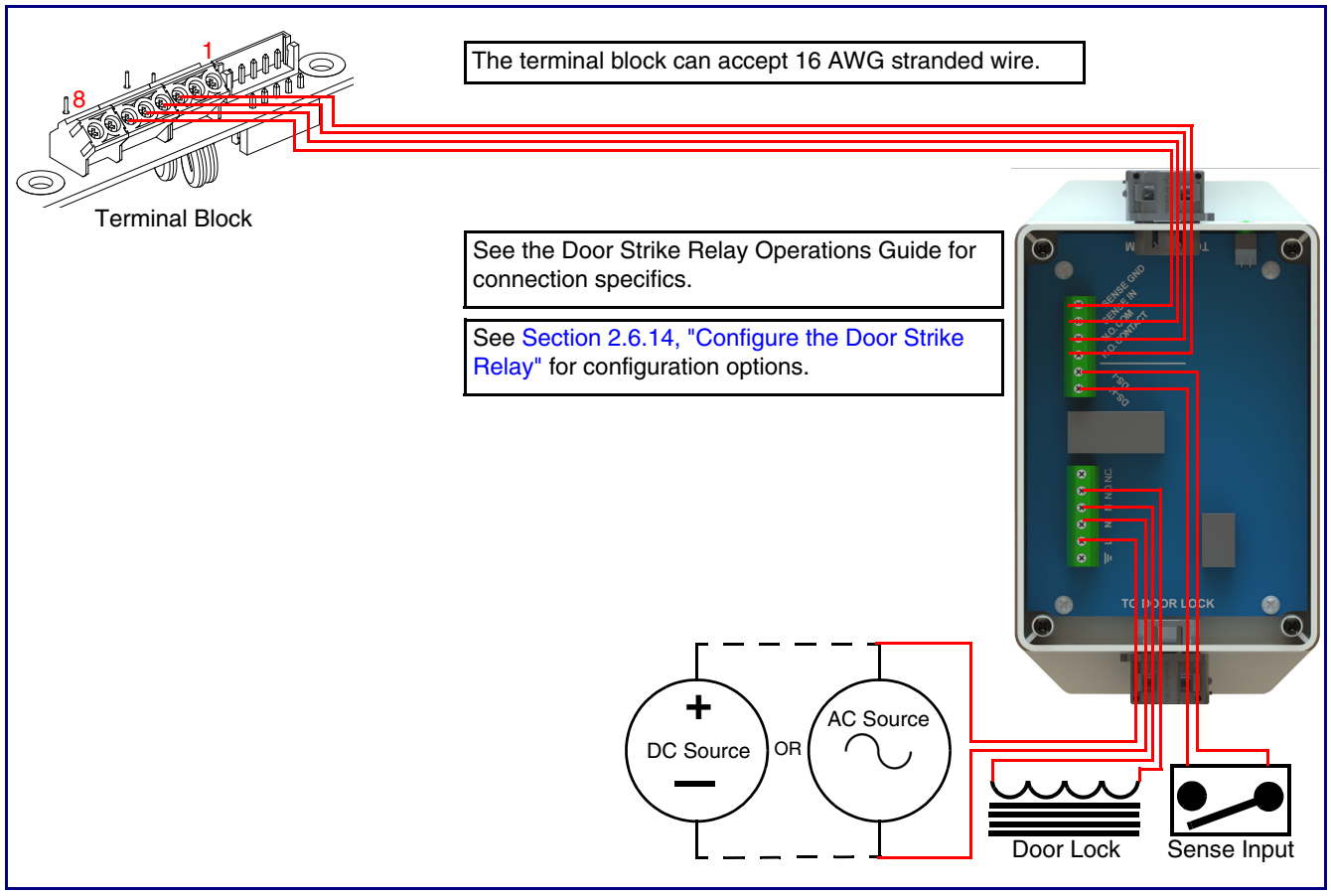
http://support.cyberdata.net/

2.3.3.4 Door Strike Relay Module Wiring Diagram from Intercom

For wiring an electronic door strike, we recommend the use of our external Door Strike Relay Module (CD# 011269).

This product provides an easier method of connecting standard door strikes as well as AC and higher voltage devices. See Figure 2-8 for the wiring diagram.

Figure 2-8. Door Strike Relay Module Wiring Diagram from Intercom



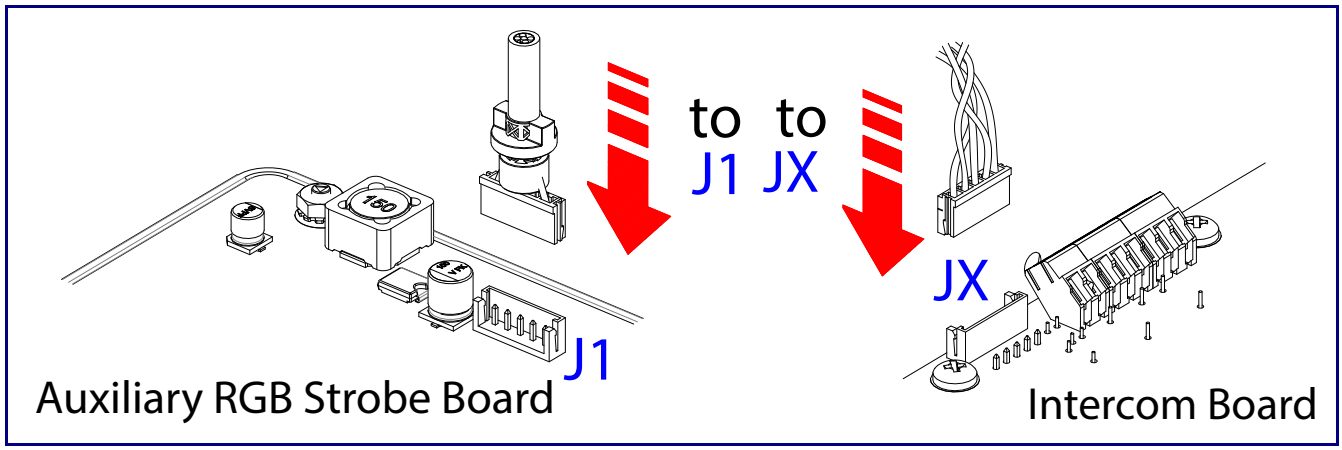
If you have questions about connecting door strikes or setting up the web configurable options, please contact our support department at the following website:

http://support.cyberdata.net/

2.4 Connecting an Auxiliary RGB Strobe to the Intercom

1. Connect the strobe cable to the board of the Auxiliary RGB Strobe and the board of the Intercom as shown in Figure 2-9.

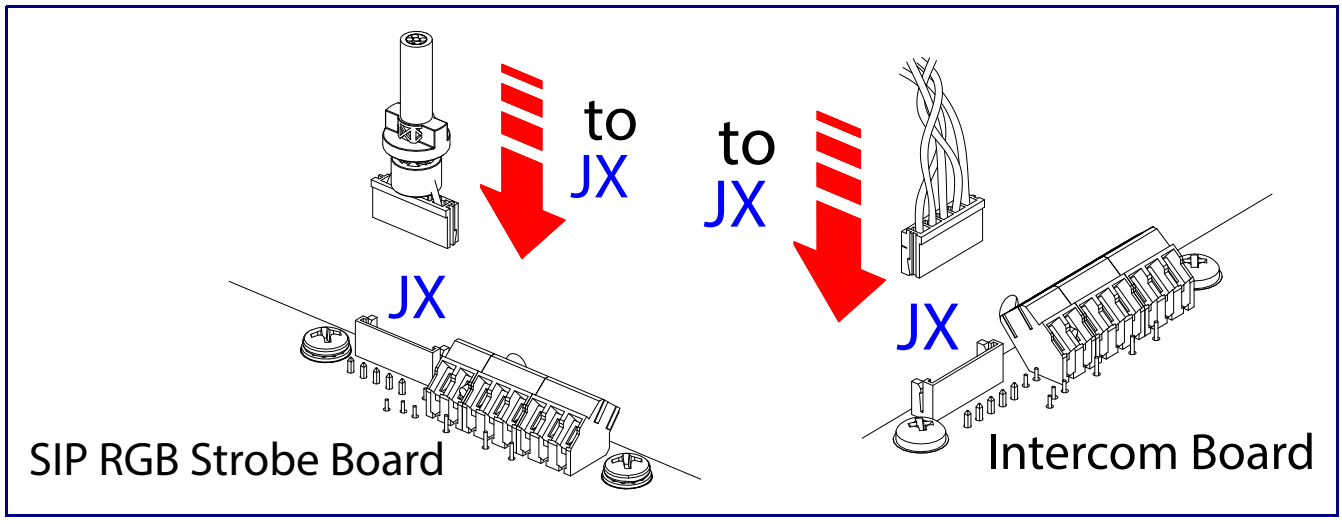
Figure 2-9. Connecting the Auxiliary RGB Strobe Kit to the Intercom



2.5 Connecting a SIP RGB Strobe to the Intercom

1. Connect the strobe cable to the board of the SIP RGB Strobe and the board of the Intercom as shown in Figure 2-10.

Figure 2-10. Connecting the SIP RGB Strobe to the Intercom



2.5.1 Intercom Connectors

See the following figures and tables to identify the connectors and functions of the Intercom.

Figure 2-11. Connector Locations

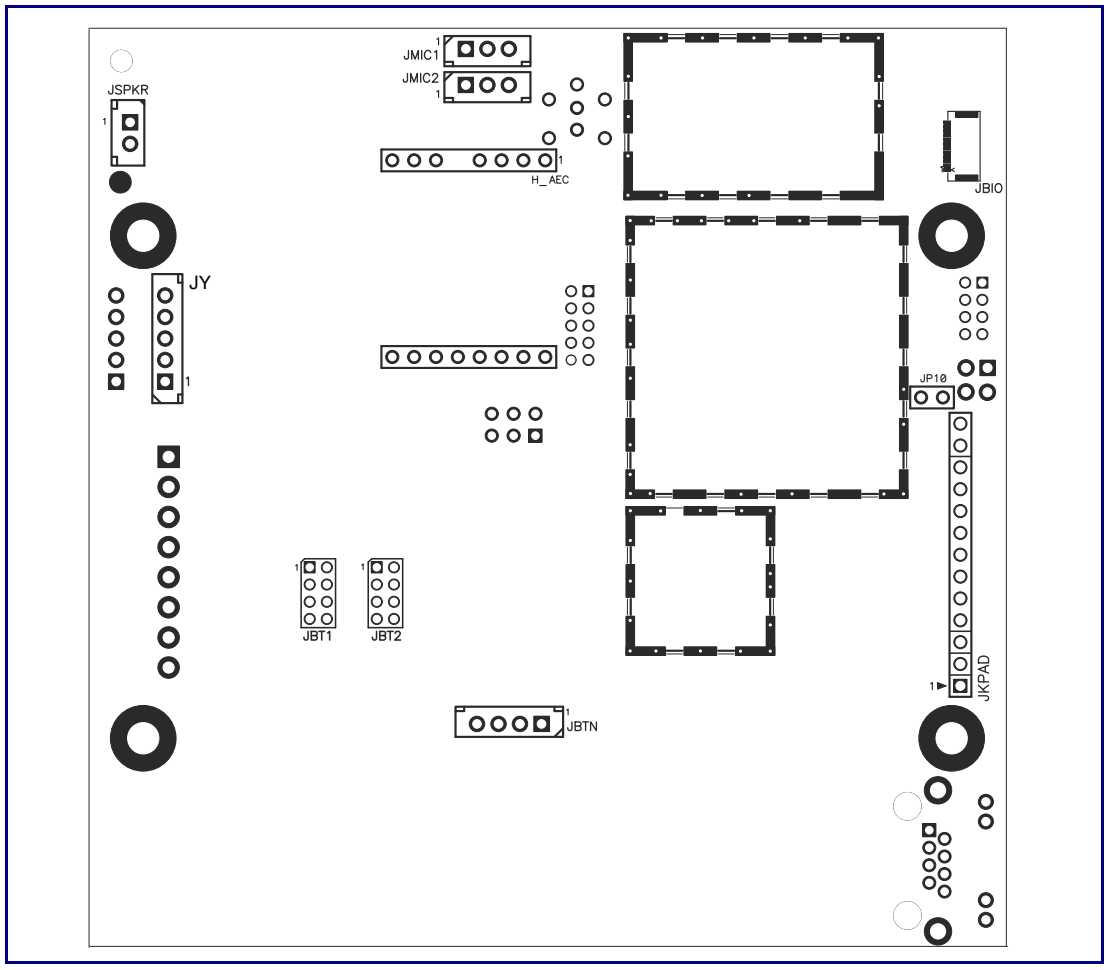


Table 2-3. Connector Functions

Connector	Function
JBTN	Call Button LED Interface
JMIC1	Microphone Interface
JSPKR	Speaker Interface
JKPAD	Keypad Interface (Not Used)
JY	I²C 5V Peripheral Bus
JP10	Disables the intrusion sensor when installed.
JBT1	Touch Button — 1 Interface (Not Used)
JBT2	Touch Button — 2 Interface (Not Used)

Figure 2-12. Connector Locations

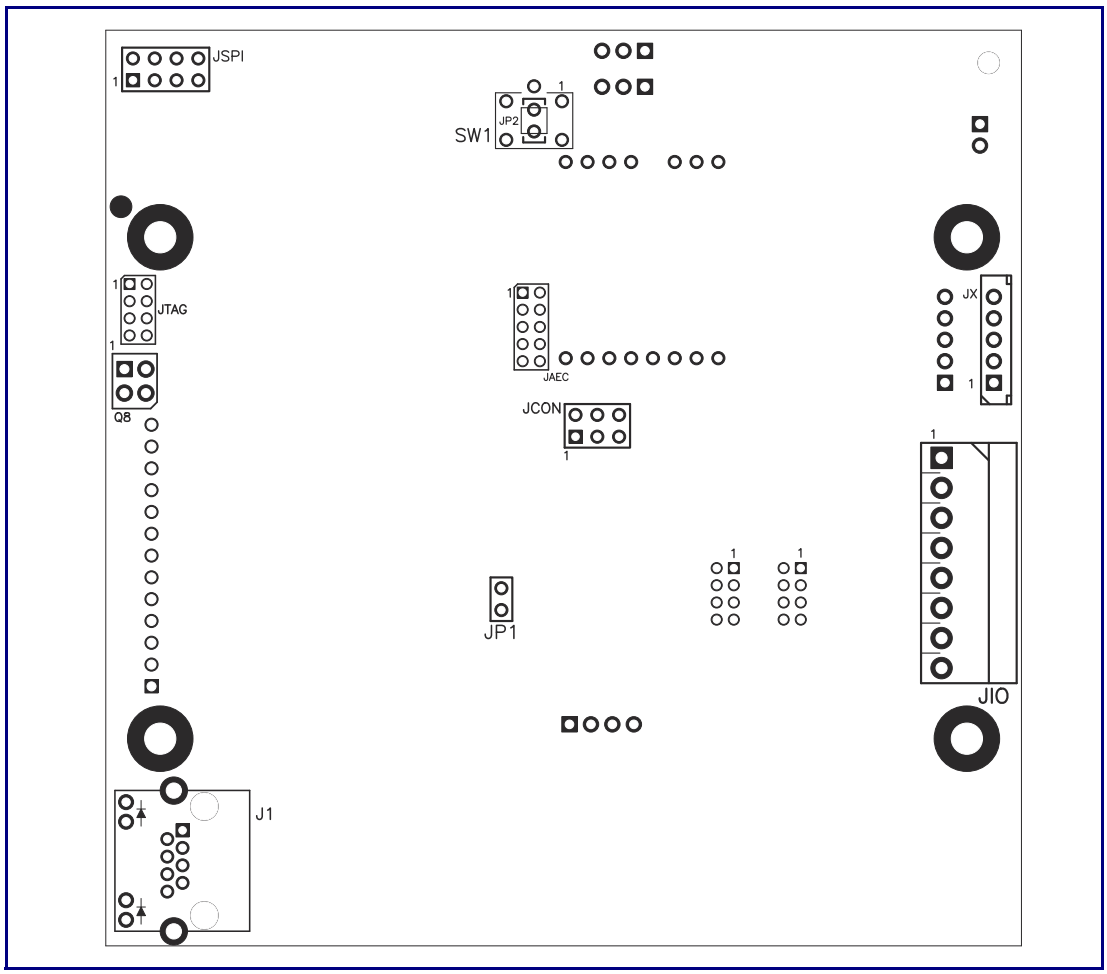


Table 2-4. Connector Functions

Connector	Function
J1	PoE Network Connection (RJ-45 ethernet)
JAEC	AEC Configuration Interface (Factory Use Only)
JIO	Terminal Block (see Figure 2-3)
JCON	Console Port (Factory Use Only)
JP1	Reset jumper[a]
JSPI	Reserved (Factory Use Only)
JTAG	JTAG (Factory Use Only)
JX	Auxiliary Strobe Connector
SW1	See Section 2.5.3, "RTFM Button"

a.Do not install a jumper. Momentary short to reset. Permanent installation of a jumper would prevent the board from running all together.

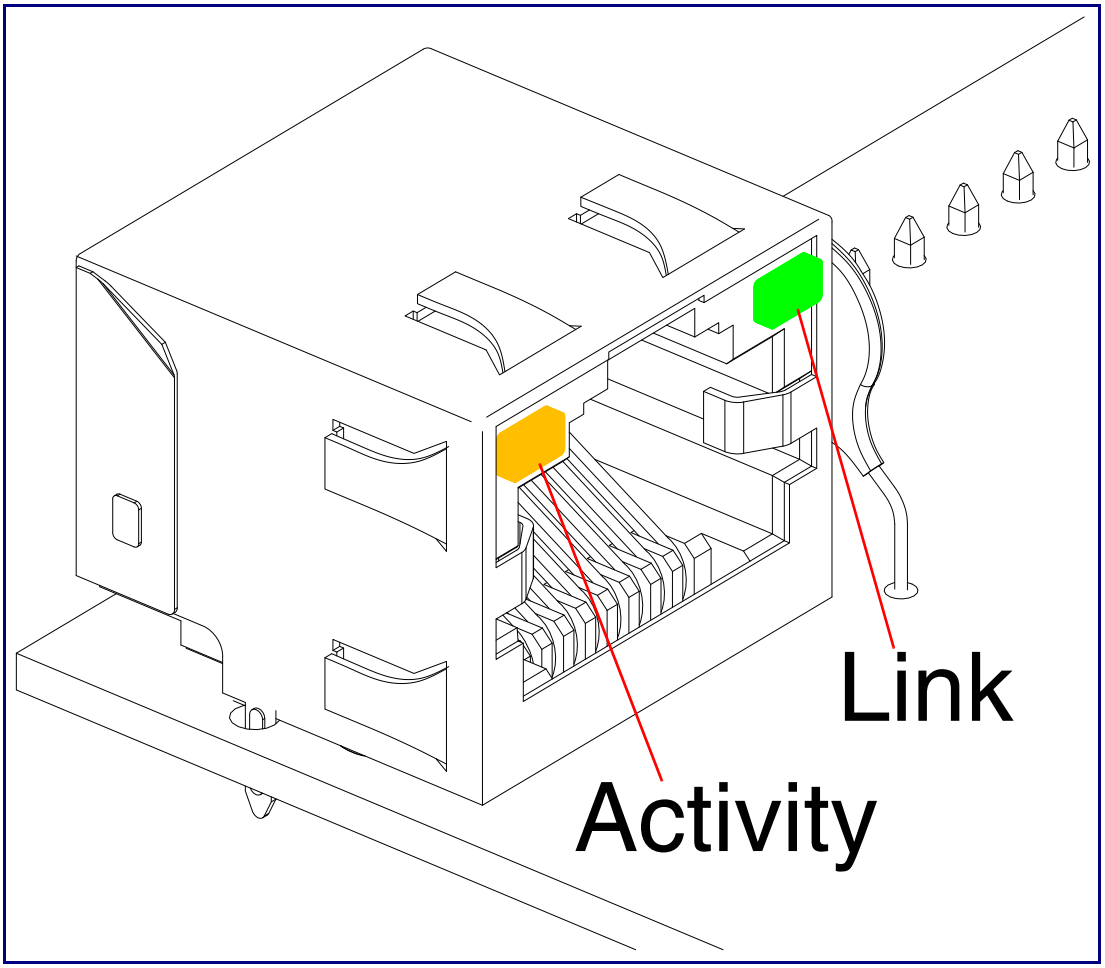
2.5.2 Activity and Link LEDs

2.5.2.1 Verifying the Network Connectivity and Data Rate

When you plug in the Ethernet cable or power supply to the Intercom, the following occurs:

- The square, **AMBER** **Link/Activity** LED blinks when there is network activity (see Figure 2-13).
- The square, **GREEN** **100Mb Link** LED above the Ethernet port indicates that the network connection has been established (see Figure 2-13).

Figure 2-13. Activity and Link LED

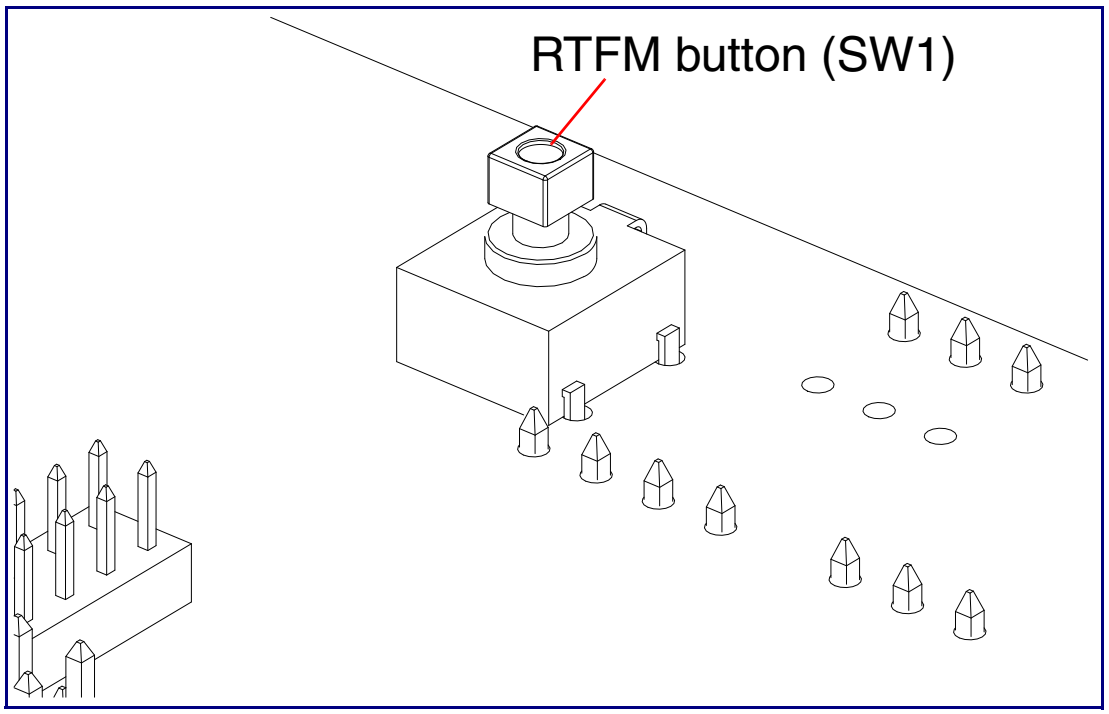


2.5.3 RTFM Button

When the Intercom is operational and linked to the network, you can use the Reset Test Function Management **(RTFM)** button (see **SW1** in Figure 2-14) on the Intercom board to announce and confirm the Intercom's IP Address and test to see if the audio is working.

Note You must do these tests prior to final assembly.

Figure 2-14. RTFM Button



2.5.3.1 Announcing the IP Address

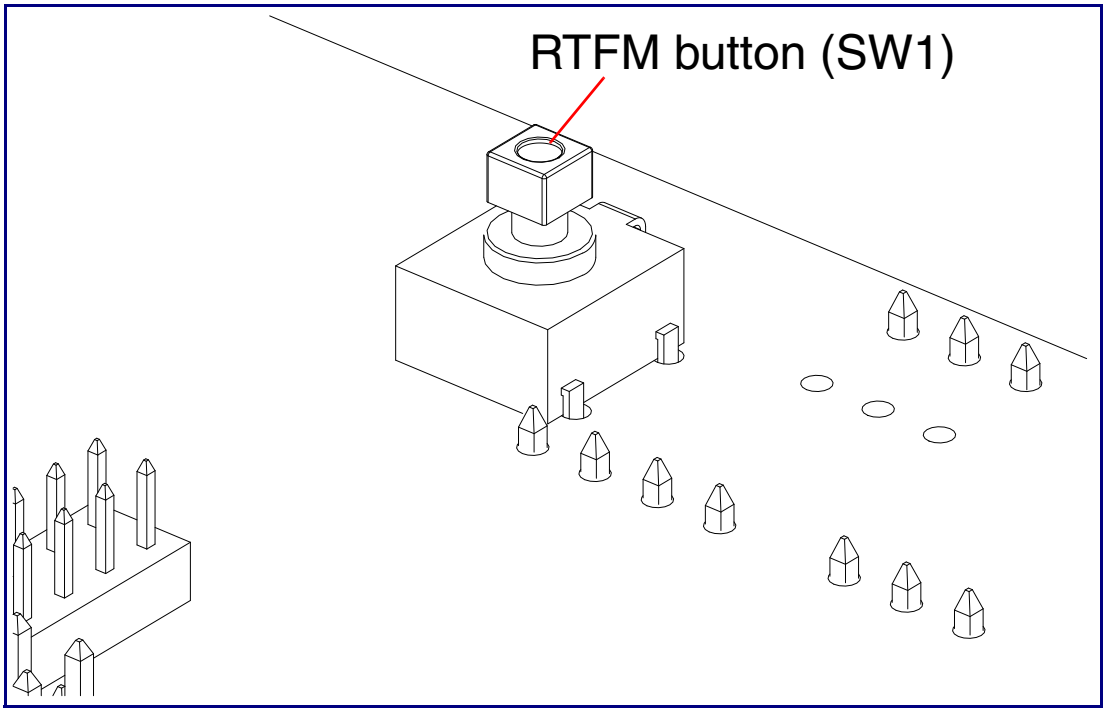
To announce a device's current IP address:

1. Press and release the RTFM button (see **SW1** in Figure 2-15) within a five second window.

Note The device will use DHCP to obtain the new IP address (DHCP-assigned address or default to 10.10.10.10 if a DHCP server is not present).

Note Pressing and holding the RTFM button for longer than five seconds will restore the device to the factory default settings.

Figure 2-15. RTFM Button



2.5.3.2 Restoring the Factory Default Settings

When troubleshooting configuration problems, it is sometimes convenient to restore the device to a known state.

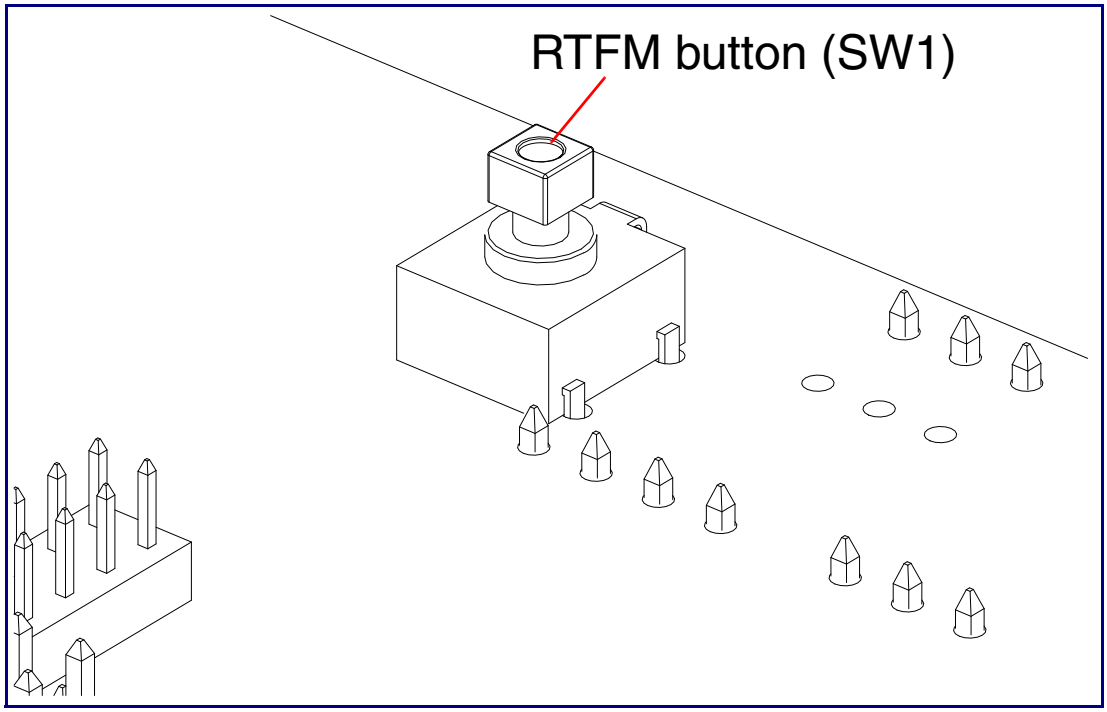
Note Each Intercom is delivered with factory set default values.

To restore the factory default settings:

1. Press and hold the **RTFM button** (see **SW1** in Figure 2-16) for more than five seconds.
2. The device announces that it is restoring the factory default settings.

Note The device will use DHCP to obtain the new IP address (DHCP-assigned address or default to 10.10.10.10 if a DHCP server is not present).

Figure 2-16. RTFM Button



2.5.4 Adjust the Volume

You can adjust the volume through the Device Configuration Page.

2.6 Configure the Intercom Parameters

To configure the Intercom online, use a standard web browser.

Configure each Intercom and verify its operation *before* you mount it. When you are ready to mount an Intercom, refer to Appendix A, "Mounting the Singlewire InformaCast Indoor Intercom with Keypad, Flush Mount" for instructions.

2.6.1 Factory Default Settings

All Intercoms are initially configured with the following default IP settings:

When configuring more than one Intercom, attach the Intercoms to the network and configure one at a time to avoid IP address conflicts.

Table 2-5. Factory Default Settings

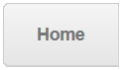
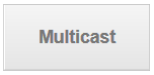
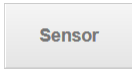
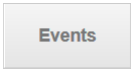
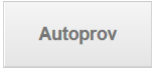
Parameter	Factory Default Setting
IP Addressing	DHCP
IP Address[a]	10.10.10.10
Web Access Username	admin
Web Access Password	admin
Subnet Mask[a]	255.0.0.0
Default Gateway[a]	10.0.0.1

a. Default if there is not a DHCP server present.

2.6.2 Intercom Web Page Navigation

Table 2-6 shows the navigation buttons that you will see on every Intercom web page.

Table 2-6. Web Page Navigation

Web Page Item	Description
	Link to the **Home** page.
	Link to the **Device** page.
	Link to the **Buttons** page.
	Link to the **Security** page.
	Link to the **Network** page.
	Link to go to the **SIP** page.
	Link to the **Multicast** page.
	Link to the **Sensor** page.
	Link to the **Audiofiles** page.
	Link to the **Events** page.
	Link to the **Door Strike Relay** page.
	Link to the **Autoprovisioning** page.
	Link to the **Firmware** page.

2.6.3 Using the Toggle Help Button

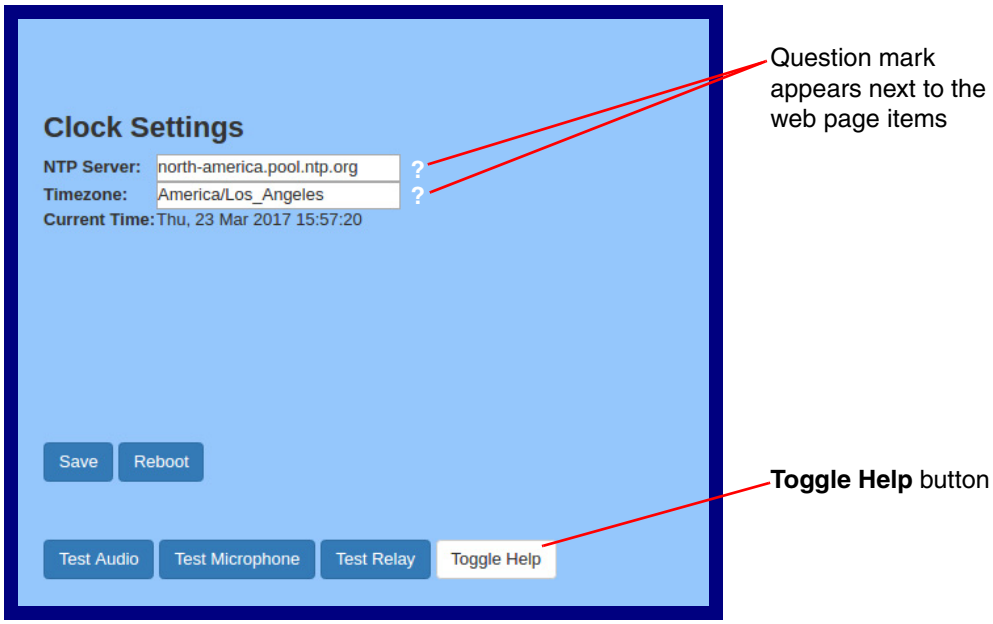
The **Toggle Help** button allows you to see a short description of some of the settings on the webpage. To use the **Toggle Help** button, do the following:

1. Click on the **Toggle Help** button that is on the UI webpage. See Figure 2-17 and Figure 2-18.

Figure 2-17. Toggle/Help Button

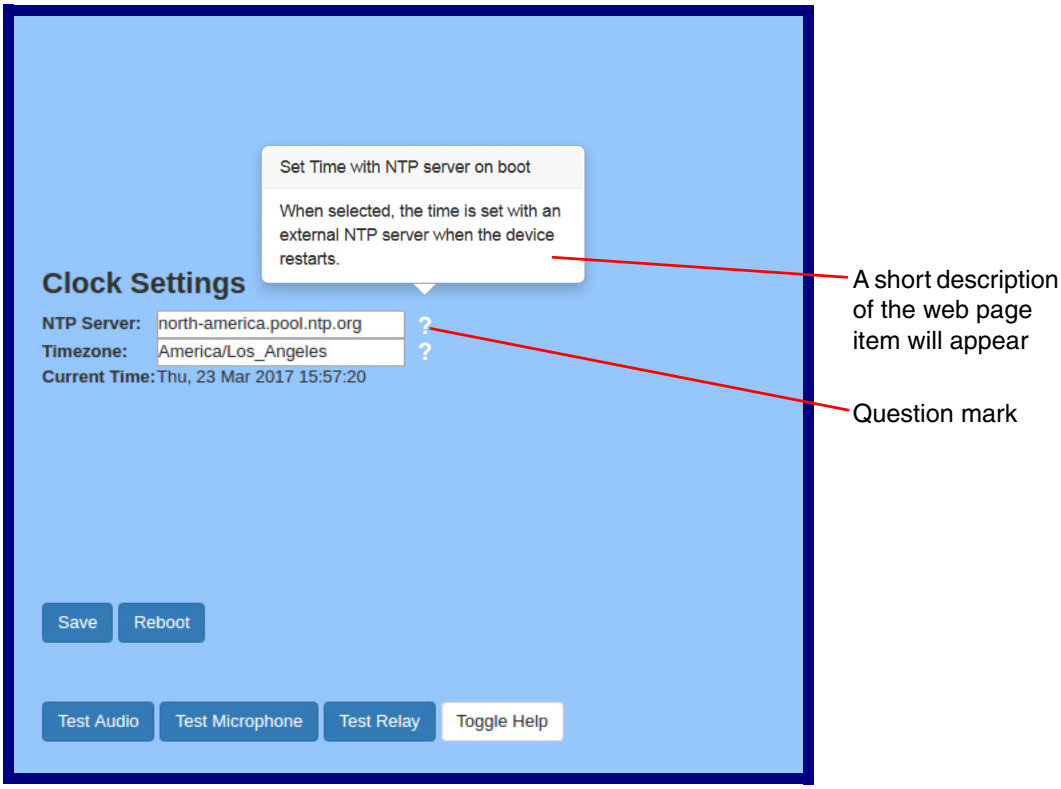
2. You will see a question mark (?) appear next to each web page item that has been provided with a short description by the Help feature. See Figure 2-18.

Figure 2-18. Toggle Help Button and Question Marks



3. Move the mouse pointer to hover over the question mark (?), and a short description of the web page item will appear. See Figure 2-19.

Figure 2-19. Short Description Provided by the Help Feature



2.6.4 Log in to the Configuration Home Page

1. Open your browser to the Intercom IP address.

Note If the network does not have access to a DHCP server, the device will default to an IP address of 10.10.10.10.

Note Make sure that the PC is on the same IP network as the Intercom.

Note You may also download CyberData's VoIP Discovery Utility program which allows you to easily find and configure the default web address of the CyberData VoIP products.

CyberData's VoIP Discovery Utility program is available at the following link:

http://www.cyberdata.net/assets/common/discovery.zip

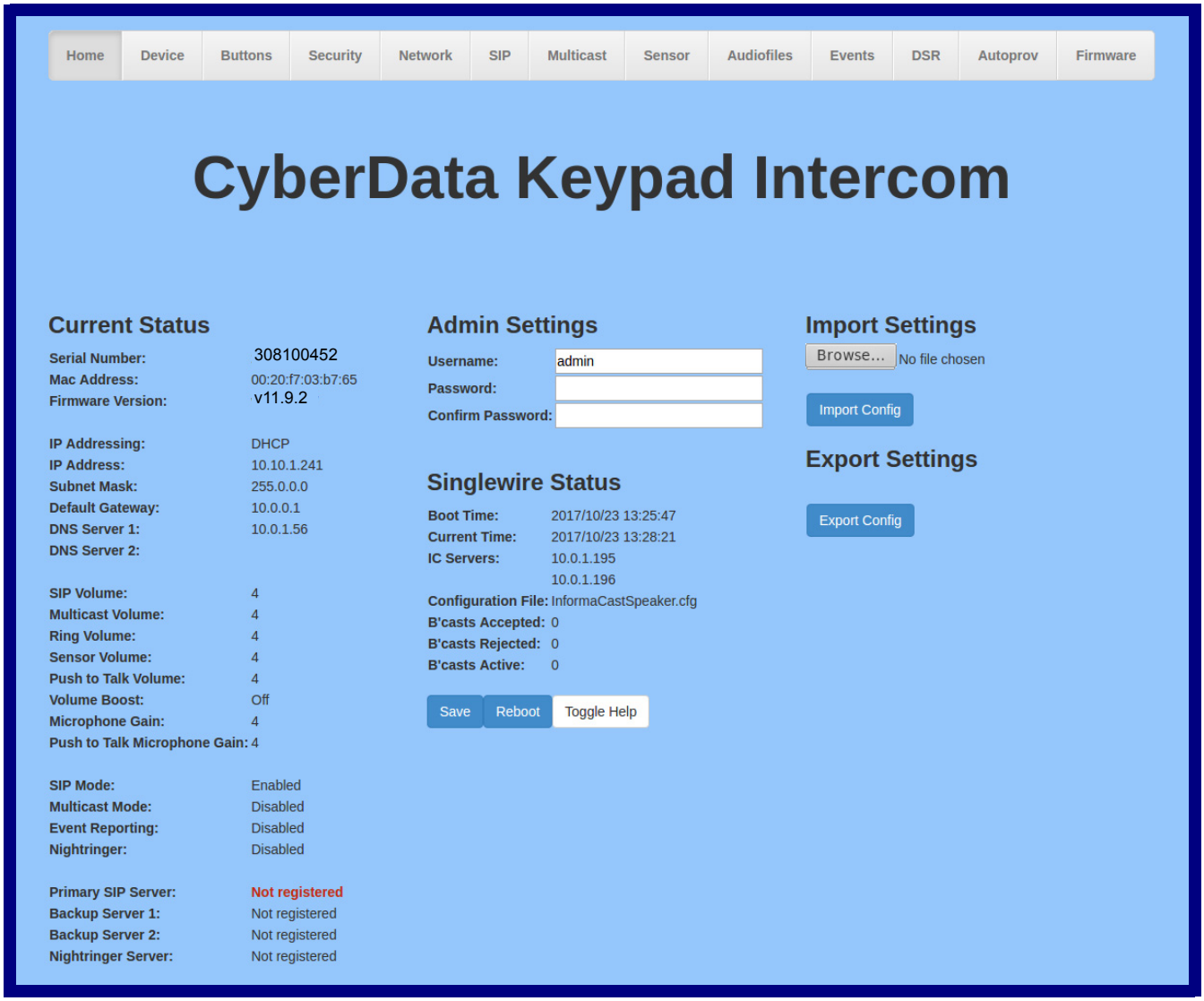
Note The Intercom ships in DHCP mode. To get to the **Home** page, use the discovery utility to scan for the device on the network and open your browser from there.

2. When prompted, use the following default **Web Access Username** and **Web Access Password** to access the **Home Page** (Figure 2-20):

   Web Access Username: **admin**

   Web Access Password: **admin**

Figure 2-20. Home Page



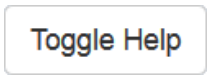
3. On the **Home** page, review the setup details and navigation buttons described in Table 2-7.

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-7. Home Page Overview

Web Page Item	Description
Admin Settings	
Username ?	The username to access the web interface. Enter up to 25 characters.
Password ?	The password to access the web interface. Enter up to 25 characters.
Confirm Password ?	Confirm the web interface password.
Current Status	
Serial Number	Shows the device serial number.
Mac Address	Shows the device Mac address.
Firmware Version	Shows the current firmware version.
IP Addressing	Shows the current IP addressing setting (**DHCP** or **static**).
IP Address	Shows the current IP address.
Subnet Mask	Shows the current subnet mask address.
Default Gateway	Shows the current default gateway address.
DNS Server 1	Shows the current DNS Server 1 address.
DNS Server 2	Shows the current DNS Server 2 address.
SIP Volume	Shows the current SIP volume level.
Multicast Volume	Shows the current Multicast volume level.
Ring Volume	Shows the current Ring volume level.
Sensor Volume	Shows the current Sensor volume level.
Push to Talk Volume	Shows the current Push to Talk volume level.
Volume Boost	Shows the current Volume Boost level.
Microphone Gain	Shows the current Microphone Gain level.
Push to Talk Microphone Gain	Shows the current Push to Talk Microphone Gain level.
SIP Mode	Shows the current status of the SIP mode.
Multicast Mode	Shows the current status of the Multicast mode.
Event Reporting	Shows the current status of the Event Reporting mode.
Nightringer	Shows the current status of the Nightringer mode.
Primary SIP Server	Shows the current status of the Primary SIP Server.
Backup Server 1	Shows the current status of Backup Server 1.
Backup Server 2	Shows the current status of Backup Server 2.
Nightringer Server	Shows the current status of Nightringer Server.
Singlewire Settings	
Boot Time	Shows the boot time.
Current Time	Shows the current time.

Table 2-7. Home Page Overview (continued)

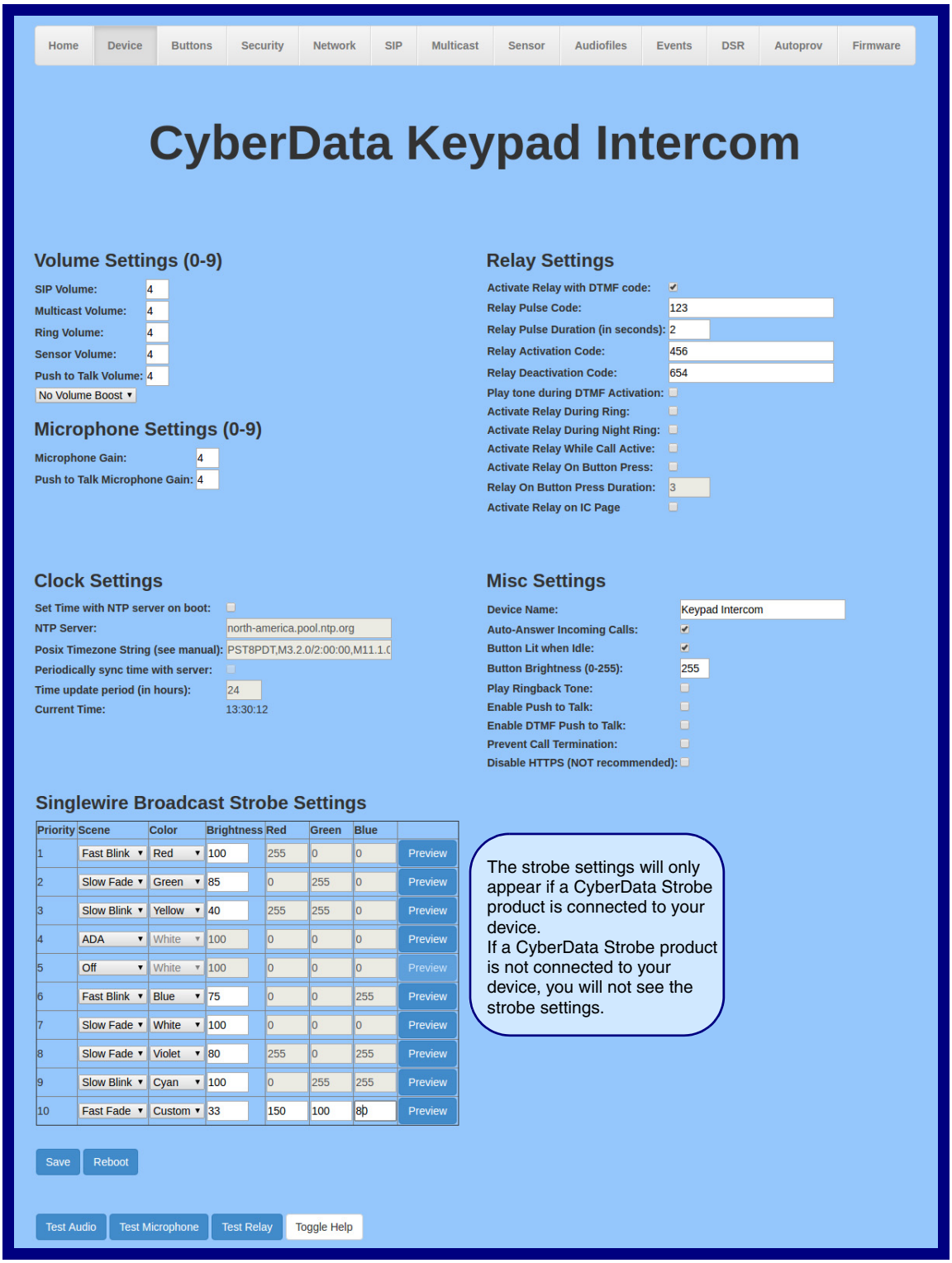
Web Page Item	Description
IC Servers	Shows the InformaCast server IP addresses.
Configuration File	Shows the configuration file.
B'casts Accepted	Shows the number of B'casts accepted.
B'casts Rejected	Shows the number of B'casts rejected.
B'casts Active	Shows the number of active B'casts.
Import Settings	
	Use this button to select a configuration file to import.
	After selecting a configuration file, click Import to import the configuration from the selected file. Then, click Save and Reboot to store changes.
Export Settings	
	Click Export to export the current configuration to a file.
	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
	Click on the **Reboot** button to reboot the system.
	Click on the **Toggle Help** button to see a short description of some of the web page items. First click on the **Toggle Help** button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

Note The user name and password will be saved immediately, but the user will not be prompted to enter them until there is a reboot. It is advisable to restart the web browser after this change.

2.6.5 Configure the Device

1. Click the **Device** menu button to open the **Device** page. See Figure 2-21.

Figure 2-21. Device Configuration Page



2. On the **Device** page, you may enter values for the parameters indicated in Table 2-8.

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-8. Device Configuration Parameters

Web Page Item	Description
Volume Settings (0-9)	
SIP Volume ?	Set the speaker volume for a SIP call. A value of 0 will mute the speaker during SIP calls. **Note**: This setting does not require a reboot for the changes to take effect.
Multicast Volume ?	Set the speaker volume for multicast audio streams. A value of 0 will mute the speaker during multicasts. **Note**: This setting does not require a reboot for the changes to take effect.
Ring Volume ?	Set the ring volume for incoming calls. A value of 0 will mute the speaker instead of playing the ring tone when Auto-Answer Incoming Calls is disabled. **Note**: This setting does not require a reboot for the changes to take effect.
Sensor Volume ?	Set the speaker volume for playing sensor activated audio. A value of 0 will mute the speaker during sensor activated audio. **Note**: This setting does not require a reboot for the changes to take effect.
Push to Talk Volume ?	Set the speaker volume for Push to Talk operation. A value of 0 will mute the speaker in Push to Talk mode. **Note**: This setting does not require a reboot for the changes to take effect.
Volume Boost: ? No Volume Boost Volume Boost 1 Volume Boost 2 Volume Boost 3	Set the Boost level to increase the volume output of the speaker. Using Volume Boost may introduce audio clips or cause the device to drop from full duplex to half duplex operation. Normal operation of the product can be met with volume levels **0** through **9**. **0** being mute and **9** being the loudest volume that in a normal arm's length and average background noise, will enable full duplex operation and give the best quality of sound output. If the user would like a higher output from the speaker, the Boost settings are available. However, operation in **Boost Mode** may overdrive or clip the audio if, for example, the phone that is connected has a high microphone gain or if the person has a loud voice talking too close to the microphone. The acoustic echo canceller also has a harder time maintaining full duplex operation when in the **Boost Mode**. The product may drop from full duplex operation into half/duplex mode while in **Boost Mode**. Contact CyberData support for additional information if needed.
Microphone Settings (0-9)	
Microphone Gain ?	Set the microphone gain level.
Push to Talk Microphone Gain ?	Set the microphone gain level for Push to Talk operation.
Clock Settings	
Set Time with NTP Server on boot ?	When selected, the time is set with an external NTP server when the device restarts.

Table 2-8. Device Configuration Parameters (continued)

Web Page Item	Description
NTP Server	Use this field to set the address (in IPv4 dotted decimal notation or as a canonical name) for the NTP Server. This field can accept canonical names of up to 64 characters in length. **Note**: The **NTP Server** setting needs to be restarted to spawn NTP or to change the server.
Posix Timezone String	See Section 2.6.5.1, "Time Zone Strings" for information about how to use the Posix Timezone String to specify time zone and daylight savings time where applicable. Enter up to 63 characters.
Periodically sync time with server	When selected, the time is periodically updated with the NTP server at the configured interval below.
Time update period (in hours)	The time interval after which the device will contact the NTP server to update the time. Enter up to 4 digits. **Note**: Syncing and changing the **Time update period (in hours)** setting does not require a reboot for the changes to take effect.
Current Time	Displays current time.
Relay Settings	**Note**: None of the **Relay Settings** require a reboot for the changes to take effect.
Activate Relay with DTMF Code	Activates the relay when the DTMF Activation Code is entered on the phone during a SIP call with the device. RFC2833 DTMF payload types are supported.
Relay Pulse Code	DTMF code used to pulse the relay when entered on a phone during a SIP call with the device. Relay will activate for Relay Pulse Duration seconds then deactivate. Activate Relay with DTMF Code must be enabled. Enter up to 25 digits (* and # are supported).
Relay Pulse Duration (in seconds)	The length of time (in seconds) during which the relay will be activated when the DTMF Relay Activation Code is detected. Enter up to 5 digits.
Relay Activation Code	Activation code used to activate the relay when entered on a phone during a SIP call with the device. Relay will be active indefinitely, or until the DTMF Relay Deactivation code is entered. Activate Relay with DTMF Code must be enabled. Enter up to 25 digits (* and # are supported).
Relay Deactivation Code	Code used to deactivate the relay when entered on a phone during a SIP call with the device. Activate Relay with DTMF Code must be enabled. Enter up to 25 digits (* and # are supported).
Play tone during DTMF Activation	When selected, the device will play a tone out of the speaker upon DTMF relay activation. The tone plays for the DTMF Activation Duration (in seconds).
Activate Relay During Ring	When selected, the relay will be activated for as long as the device is ringing. When Auto-Answer Incoming Calls is enabled, the device will not ring and this option does nothing.
Activate Relay During Night Ring	When selected, the relay will be activated as long as the Nightringer extension is ringing.
Activate Relay While Call Active	When selected, the relay will be activated as long as the SIP call is active.
Activate Relay on Button Press	When selected, the relay will be activated when the Call button is pressed.

Table 2-8. Device Configuration Parameters (continued)

Web Page Item	Description
Relay on Button Press Duration	The length of time (in seconds) during which the relay will be activated when the Call button is pressed. Enter up to 5 digits. A Relay on Button Press Duration value of 0 will pulse the relay once when the Call button is pressed.
Misc Settings	
Device Name	Type the device name. Enter up to 25 characters.
Auto-Answer Incoming Calls	When selected, the device will automatically answer incoming calls. When Auto-Answer Incoming Calls is disabled, the device will play a ring tone (corresponds to Ring Tone on the Audiofiles page) out of the speaker until someone presses the Call button to answer the call or the caller disconnects before the call can be answered.
Button Lit When Idle	When selected, the Call button LED is illuminated while the device is idle (a call is not in progress).
Button Brightness (0-255)	The desired Call button LED brightness level. Acceptable values are 0-255, where 0 is the dimmest and 255 is the brightest. Enter up to three digits.
Play Ringback Tone	When selected, the device will play a ringback tone (corresponds to Ringback Tone on the Audiofiles page) out of the speaker while placing an outbound call. The Ringback Tone will play until the call is answered.
Enable Push to Talk	This option is for noisy environments. When enabled, the microphone will be muted normally. When the Call button is pressed and held, it will unmute the microphone and allow the operator to send audio back. Using Push to Talk prevents the operator from terminating a call by pressing the Call button. The call must be terminated by the phone user.
Enable DTMF Push to Talk	This option is for noisy environments. When enabled, in an active call, the remote phone can force receive only audio (setting the mic gain to max and muting the speaker) by pressing the * key. Pressing the # key will force send only audio (setting the max speaker volume and muting the mic). Pressing the **0** key will restore full duplex operation with the normal microphone and speaker volume.
Prevent Call Termination	When this option is enabled, a call cannot be terminated using the call button.
Disable HTTPS (NOT recommended)	Disables the encrypted connection to the webpage. We do not recommend disabling HTTPS for security reasons. **Note**: You must click on the **Save** button and then the **Reboot** button for the changes to take effect.
Singlewire Broadcast Strobe Settings	For up to 10 Singlewire pages, when a priority is specified for the page, a corresponding strobe scene will be activated. The color may be selected from the drop down menu, or customized by the user with the 0-255 scale. Brightness is specified with a value between 0 and 100. **The following strobe settings will only appear if a CyberData Strobe product is connected to your device. If a CyberData Strobe product is not connected to your device, you will not see the strobe settings.**
Priority	Indicates the priority of the Singlewire broadcast, with 1 the highest priority and 10 the lowest.
Scene	Use this section to select the strobe flashing behavior for the Singlewire Broadcast.

Table 2-8. Device Configuration Parameters (continued)

Web Page Item	Description
ADA Compliant	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.
Slow Fade	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.
Fast Blink	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.
Color	Select the desired color (only one may be chosen).
Brightness	How bright the strobe will blink when there is a Singlewire Broadcast. This is the maximum brightness for “fade” type scenes.
Red	The red LED value for the Singlewire Broadcast.
Green	The green LED value for the Singlewire Broadcast.
Blue	The blue LED value for the Singlewire Broadcast.
Test Audio	Click on the **Test Audio** button to do an audio test. When the **Test Audio** button is pressed, you will hear a voice message for testing the device audio quality and volume.
Test Microphone	Click on the **Test Microphone** button to do a microphone test. When the **Test Microphone** button is pressed, the following occurs: 1. The device will immediately start recording 3 seconds of audio. 2. The device will beep (indicating the end of recording). 3. The device will play back the recorded audio.
Test Relay	Click on the **Test Relay** button to do a relay test.
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.
Toggle Help	Click on the **Toggle Help** button to see a short description of some of the web page items. First click on the **Toggle Help** button, and you will see a question mark ( ) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

Note You must click on the **Save** button and then the **Reboot** button for the changes to take effect.

2.6.5.1 Time Zone Strings

The posix time zone string tells the internal date and time utilities how to handle daylight savings time for different time zones. Table 2-9 shows some common strings.

Table 2-9. Common Time Zone Strings

Time Zone	Time Zone String
US Pacific time	PST8PDT,M3.2.0/2:00:00,M11.1.0/2:00:00
US Mountain time	MST7MDT,M3.2.0/2:00:00,M11.1.0/2:00:00
US Eastern Time	EST5EDT,M3.2.0/2:00:00,M11.1.0/2:00:00
Phoenix Arizona[a]	MST7
US Central Time	CST6DST,M3.2.0/2:00:00,M11.1.0/2:00:00

a.Phoenix, Arizona does not use daylight savings time.

Table 2-10 shows a breakdown of the parts that constitute the following time zone string:

- ***CST6DST,M3.2.0/2:00:00,M11.1.0/2:00:00***

Table 2-10. Time Zone String Parts

Time Zone String Part	Meaning
CST6CDT	The time zone offset from GMT and three character identifiers for the time zone.
CST	Central Standard Time
6	The (hour) offset from GMT/UTC
CDT	Central Daylight Time
M3.2.0/2:00:00	The date and time when daylight savings begins.
M3	The third month (March)
.2	The 2nd occurrence of the day (next item) in the month
.0	Sunday
/2:00:00	Time of day to change
M11.1.0/2:00:00	The date and time when daylight savings ends.
M11	The eleventh month (November)
.1	The 1st occurrence of the day (next item) in the month
.0	Sunday
/2:00:00	Time of day to change

Time Zone String Examples

Table 2-11 has some more examples of time zone strings.

Table 2-11. Time Zone String Examples

Time Zone	Time Zone String
Tokyo[a]	IST-9
Berlin[b]	CET-1MET,M3.5.0/1:00,M10.5.0/1:00

a.Tokyo does not use daylight savings time.
b.For Berlin, daylight savings time starts on the last Sunday in March at 01:00 UTC, and ends on the last Sunday in October at 01:00 UTC, and is one hour ahead of UTC.

Time Zone Identifier

A user-definable three or four character time zone identifier (such as PST, EDT, IST, MUT, etc) is needed at the beginning of the posix time zone string to properly set the time. However, the specific letters or numbers used for the time zone identifier are not important and can be any three or four letter or number combination that is chosen by the user. However, the time zone identifier cannot be blank.

Figure 2-22. Three or Four Character Time Zone Identifier

You can also use the following URL when a certain time zone applies daylight savings time:

http://www.timeanddate.com/time/dst/2011.html

World GMT Table

Table 2-12 has information about the GMT time in various time zones.

Table 2-12. World GMT Table

Time Zone	City or Area Zone Crosses
GMT-12	Eniwetok
GMT-11	Samoa
GMT-10	Hawaii
GMT-9	Alaska
GMT-8	PST, Pacific US
GMT-7	MST, Mountain US
GMT-6	CST, Central US
GMT-5	EST, Eastern US
GMT-4	Atlantic, Canada
GMT-3	Brazilia, Buenos Aries
GMT-2	Mid-Atlantic
GMT-1	Cape Verdes
GMT	Greenwich Mean Time, Dublin
GMT+1	Berlin, Rome
GMT+2	Israel, Cairo
GMT+3	Moscow, Kuwait
GMT+4	Abu Dhabi, Muscat

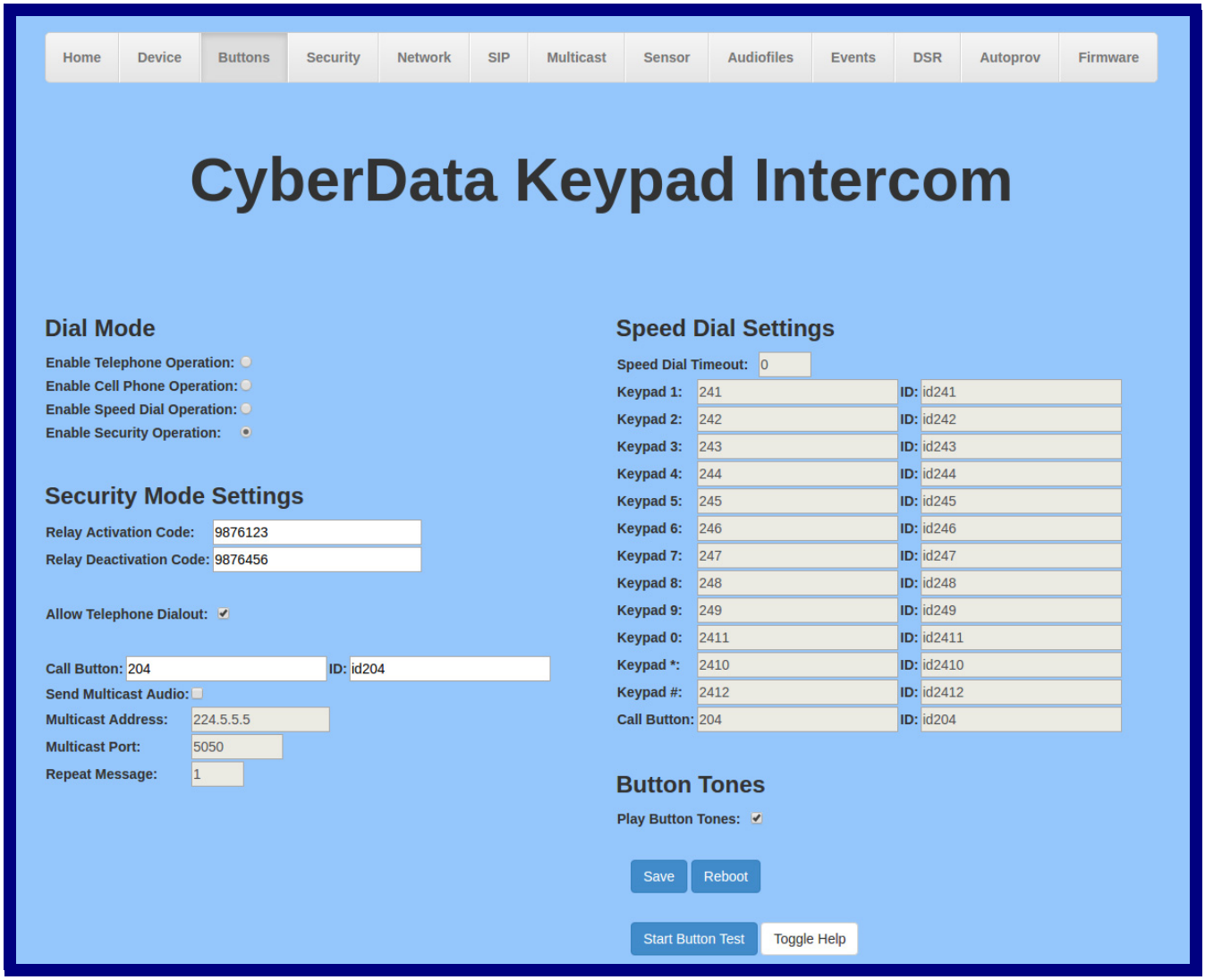
Table 2-12. World GMT Table (continued)

Time Zone	City or Area Zone Crosses
GMT+5	Islamabad, Karachi
GMT+6	Almaty, Dhaka
GMT+7	Bangkok, Jakarta
GMT+8	Hong Kong, Beijing
GMT+9	Tokyo, Osaka
GMT+10	Sydney, Melbourne, Guam
GMT+11	Magadan, Soloman Is.
GMT+12	Fiji, Wellington, Auckland

2.6.6 Configure the Button Parameters

1. Click the **Button Config** button to open the **Button Configuration** page. See Figure 2-23.

Figure 2-23. Button Configuration Page



2. On the **Button Configuration** page, you may enter values for the parameters indicated in Table 2-13.

Table 2-13. Button Configuration Parameters

Web Page Item	Description
Dial Mode	
Enable Telephone Operation	Dial extensions like a normal telephone. Pressing the call button will start a dial tone. Pressing the call button in a call will cancel a call.
Enable Cellphone Operation	Enter your extension and press the call button to start the call. Press the call button again to cancel the call.
Enable Speed Dial Operation	In speed dial mode every button can be configured to call a different extension when pressed.
Enable Security Operation	Security mode allows the user to secure the local or remote relay by requiring a code (up to 8 digits) to be entered into the device's keypad. The security codes may be entered within a phone call to a preset extension or independently. Security codes start with the pound key (#) and will be recognized when the user stops pressing buttons or hits the pound key again.
Security Mode Settings	
Relay Activation Code	Activation code used to activate the relay when entered on a phone during a SIP call with the device. Relay will be active indefinitely, or until the DTMF Relay Deactivation code is entered. Enter up to 25 digits (* and # are supported).
Relay Deactivation Code	Code used to deactivate the relay when entered on a phone during a SIP call with the device. Enter up to 25 digits (* and # are supported).
Allow Telephone Dialout	When enabled, the user will be able to use the call button to dial a pre-set extension, specified on the web page.
Call Button	Dial this extension when the call button is pressed. Up to 64 characters.
ID	Type the desired Extension ID. Up to 64 characters.
Send Multicast Audio	When selected, the device will play an audio file to the specified multicast address and port. **Note**: The keypad must be in Security mode to send Multicast Audio.
Multicast Address	The multicast address used for multicasting an audio file. **Note**: You must click on the **Save** button and then the **Reboot** button for the changes to take effect.
Multicast Port	The multicast port used for multicasting an audio file. **Note**: You must click on the **Save** button and then the **Reboot** button for the changes to take effect.
Repeat Message	The number of times to repeat the audio message to the remote endpoint. Enter a value from 1-65536.
Speed Dial Settings	
Speed Dial Timeout	The amount of time you must hold the button before it calls the configured extension. When this is set to 0 the phone will dial the configured extension as soon as the button is released.
Keypad 1	Dial this extension when the 1 key is pressed.
Keypad 2	Dial this extension when the 2 key is pressed.
Keypad 3	Dial this extension when the 3 key is pressed.

Table 2-13. Button Configuration Parameters (continued)

Web Page Item	Description
Keypad 4	Dial this extension when the 4 key is pressed.
Keypad 5	Dial this extension when the 5 key is pressed.
Keypad 6	Dial this extension when the 6 key is pressed.
Keypad 7	Dial this extension when the 7 key is pressed.
Keypad 8	Dial this extension when the 8 key is pressed.
Keypad 9	Dial this extension when the 9 key is pressed.
Keypad 0	Dial this extension when the 0 key is pressed.
Keypad *	Dial this extension when the * key is pressed.
Keypad #	Dial this extension when the # key is pressed.
Call Button	Dial this extension when the call button is pressed.
Button Tones	
Play Button Tones	Play a tone when the keypad buttons are pressed.
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.
Start Button Test	Click on the **Start** button to start a button test.
Toggle Help	Click on the **Toggle Help** button to see a short description of some of the web page items. First click on the **Toggle Help** button, and you will see a question mark ( ) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

Note You must click on the **Save** button for the changes to take effect.

2.6.6.1 Dial Out Extension Strings and DTMF Tones (using rfc2833)

On the **Button Configuration** page, dial out extensions support the addition of comma delimited pauses and sending additional DTMF tones (using rfc2833). The first comma will pause three seconds after a call is first established with a remote device. Subsequent commas will pause for 2 seconds. A pause of one second will be sent after each numerical digit.

Table 2-14. Examples of Dial-Out Extension Strings

Extension String	Resulting Action
302	Dial out extension 302 and establish a call
302,2	Dial out extension 302 and establish a call, wait 3 seconds then send the DTMF tone '2'
302,25,,,4,,1	Dial out extension 302 and establish a call, wait 3 seconds then send the DTMF tone '2', send out DTMF tone 5, wait 6 seconds, send out DTMF tone 4, wait 4 seconds, send out DTMF tone 1

Note The maximum number of total characters in the dial-out field is 25.

2.6.6.2 Triggering a Dial Out Call or Security Code

You can instantly trigger a dial out call or security code by pressing the **#** key after dialing a number. Table 2-15 shows the various actions that result from different keypad input.

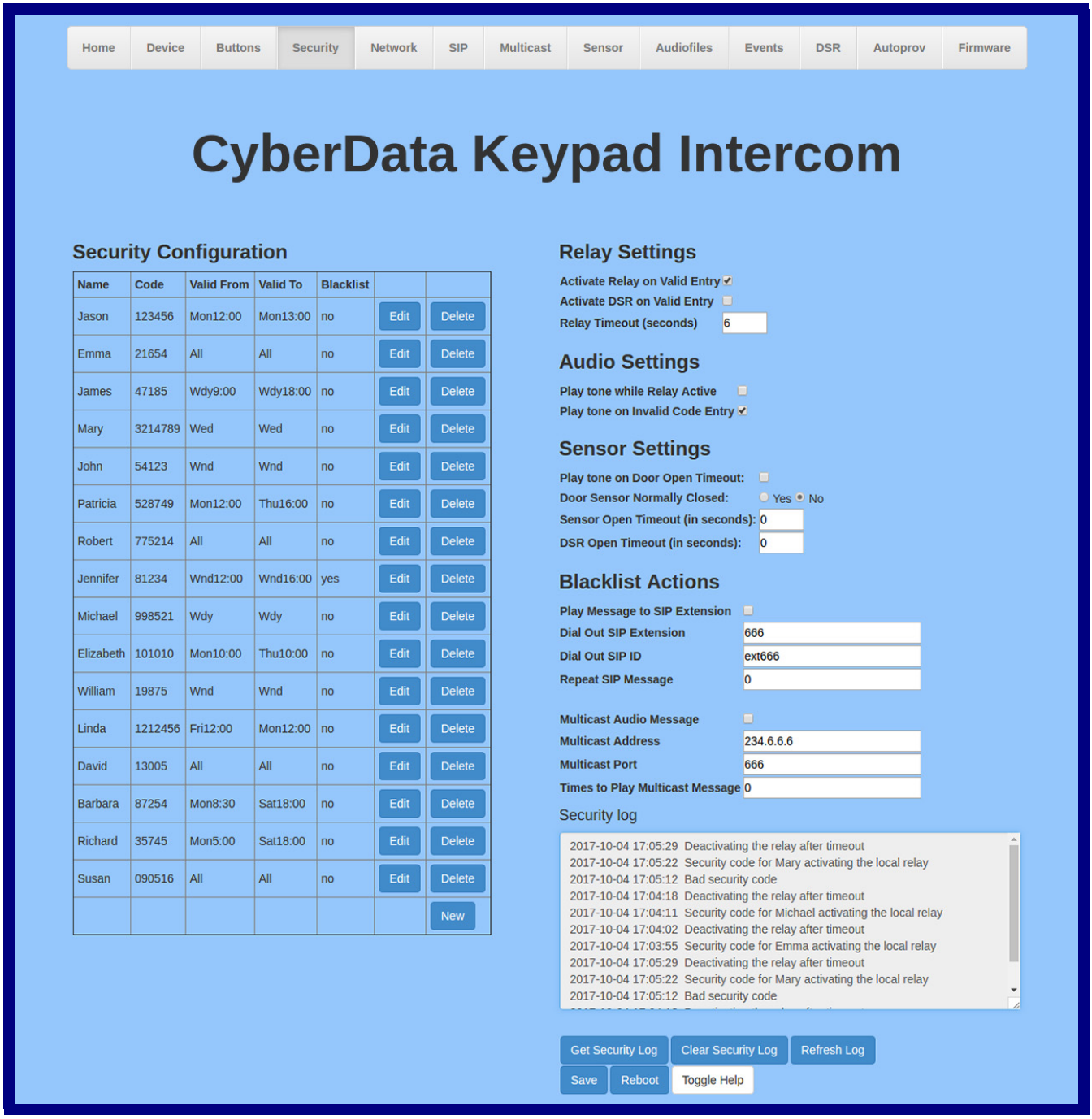
Table 2-15. Triggering a Dial Out Call or Security Code

Allow Telephone Dialout Option Enabled (in security mode with default security settings)	
Input	**Resulting Action**
Dialing **123** (and waiting for several seconds)	The device will call extension **123** through the default SIP server.
Dialing **#123** (and waiting for several seconds)	The device will do nothing. The entry is an unrecognized security entry.
Dialing **#1234560** (and waiting for several seconds)	The device will activate the relay for **Security Code 0** for **6** seconds.
Dialing **#124560#**	The device will instantly activate the relay for **6** seconds.
Dialing **123#**	The device will instantly call extension **123** through the default SIP server.
Allow Telephone Dialout Option Disabled (in security mode with default security settings)	
Input	**Resulting Action**
Dialing **1234560** (and waiting for several seconds)	The device will activate the relay for **Security Code 0** for **6** seconds.

2.6.7 Configure the Security

1. Click the **Security** menu button to open the **Security** page. See Figure 2-21.

Figure 2-24. Security Configuration Page



2. On the **Security** page, you may enter values for the parameters indicated in Table 2-16.

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-16. Security Configuration Parameters

Web Page Item	Description
Security Configuration (Record)	
Name ?	Displays the name associated with this security record.
Code ?	Displays the security code associated with this security record.
Valid From ?	See Section 2.6.7.2, "The “Valid From” and “Valid To” Settings".
Valid To ?	See Section 2.6.7.2, "The “Valid From” and “Valid To” Settings".
Blacklist ?	Displays the Blacklisted status of this security record. Blacklist is used to deny entry to the specified security code. Entering a blacklisted code will trigger the buzzer, and can trigger a call to an extension or a multicast of a pre-recorded message.
Edit	Opens the **Configure Security Code Page**. See Section 2.6.7.1, "Configure the Security Code Page".
Delete	Removes the security code record.
New	Opens a new Configure Security Code window.
Relay Settings	
Activate Relay on Valid Entry ?	Activates the relay when a valid code is entered. This would likely be used to open a door.
Activate DSR on Valid Entry ?	Activates the remote relay when a valid code is entered. This would likely be used to open a door.
Relay Timeout (seconds) ?	Specifies how many seconds the relay will be activated after a valid code entry. In a typical use case, this would specify how long the door is unlocked.
Audio Settings	
Play tone while Relay Active ?	When selected, an audible tone will indicate the relay is active.
Play tone on Invalid Code Entry ?	When selected, a tone will play on the speaker to indicate an invalid code was entered.
Sensor Settings	
Buzz on Door Open Timeout ?	When selected, the buzzer will beep until the on board sensor is deactivated.
Door Sensor Normally Closed ?	Select the inactive state of the door sensor. The door sensor is also known as the Sense Input on the device's terminal block.
Sensor Open Timeout (in seconds) ?	The time (in seconds) the device will wait before it triggers the buzzer when the door sensor is active.
DSR Open Timeout (in seconds) ?	The time (in seconds) the device will wait before it triggers the buzzer when the remote door sensor (DSR) is active.

Table 2-16. Security Configuration Parameters (continued)

Web Page Item	Description
Blacklist Actions	
Play Message to SIP Extension	When selected, the device will make a SIP call and play the “blacklist” audio file when a blacklisted code is entered.
Dial Out SIP Extension	The extension that will be dialed if “Play Mesage to SIP Extension” is selected above. Enter up to 64 alphanumeric characters.
Dial Out SIP ID	Additional caller identification string added to outbound calls. Enter up to 64 alphanumeric characters.
Repeat SIP Message	The number of times to repeat the “blacklist” audio file played during the SIP call. Enter a value between 0 and 65535. 0 will cause the message to play indefinitely, until the call is terminated.
Multicast Audio Message	When selected, the device will multicast the “blacklist” audio file to the specified address and port.
Multicast Address	The multicast address that the “blacklist” audiofile will be played to.
Multicast Port	The multicast port that the “blacklist” audofile will be played to.
Times to Play Multicast Message	The number of times the “blacklist” audio file will be played via multicast. Enter a value between 1 and 65535.
Get Security Log	Downloads a file with a maximum of 3 log files, each 1 M.
Clear Security Log	Clears the on screen display of the log.
Refresh Log	Refreshes the on screen display of the log to show the most recent activity.
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.
Toggle Help	Click on the **Toggle Help** button to see a short description of some of the web page items. First click on the **Toggle Help** button, and you will see a question mark ( ) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

Note You must click on the **Save** button and then the **Reboot** button for the changes to take effect.

Note The device must set time with an **NTP Server** (see the **Device Configuration Page**). If an NTP server is not used, all **Valid From** and **Valid To** fields must be set to **All**.

2.6.7.1 Configure the Security Code Page

1. Click the **Edit** button to open the **Configure Security Code** page. See Figure 2-25.

Figure 2-25. Configure Security Code Page

2. On the **Configure Security Code** page, you may enter values for the parameters indicated in Table 2-16.

Table 2-17. Security Code Page Parameters

Web Page Item	Description
Security Configuration	
Name	Enter name.
Code	Enter a security code, maximum 8 digits, must be distinct.
Valid From	See Section 2.6.7.2, "The “Valid From” and “Valid To” Settings".
Valid To	See Section 2.6.7.2, "The “Valid From” and “Valid To” Settings".
Blacklist	Blacklist is used to deny entry to the specified security code. Entering a blacklisted code will trigger the buzzer, and can trigger a call to an extension or a multicast of a pre-recorded message.
Save Changes	Saves the changes of the security configuration.
Cancel	Cancels the changes of the security configuration.

2.6.7.2 The "Valid From" and "Valid To" Settings

ValidFrom and **ValidTo** fields specify the day(s) a security code is valid, and, optionally the time, in 24:00 format.

The Day of the week can be **Mon**, **Tue**, **Wed**, **Thu**, **Fri**, **Sat**, **Sun**, or one of the special identifiers: **All**, **Wnd**, and **Wdy**.

Wdy indicates weekdays (Monday-Friday).

Wnd indicates weekends (Saturday-Sunday).

All allows entrance at all times.

A valid string consists of a day of the week or a special identifier, plus an optional time, except if using **All**, which will not use a time.

Some examples:

<ValidFrom0>Mon9:00</ValidFrom0>

<ValidTo0>Fri17:00</ValidTo0> monday through friday 9am to 5pm

<ValidFrom0>All</ValidFrom0>

<ValidTo0>All</ValidTo0> all day every day

<ValidFrom0>All</ValidFrom0>

<ValidTo0>All12:00</ValidTo0> every day till 12:00

<ValidFrom0>Mon12:00</ValidFrom0>

<ValidTo0>Mon12:00</ValidTo0> times are inclusive - this code is only valid on monday at 12:00

<ValidFrom0>Wdy9:00</ValidFrom0>

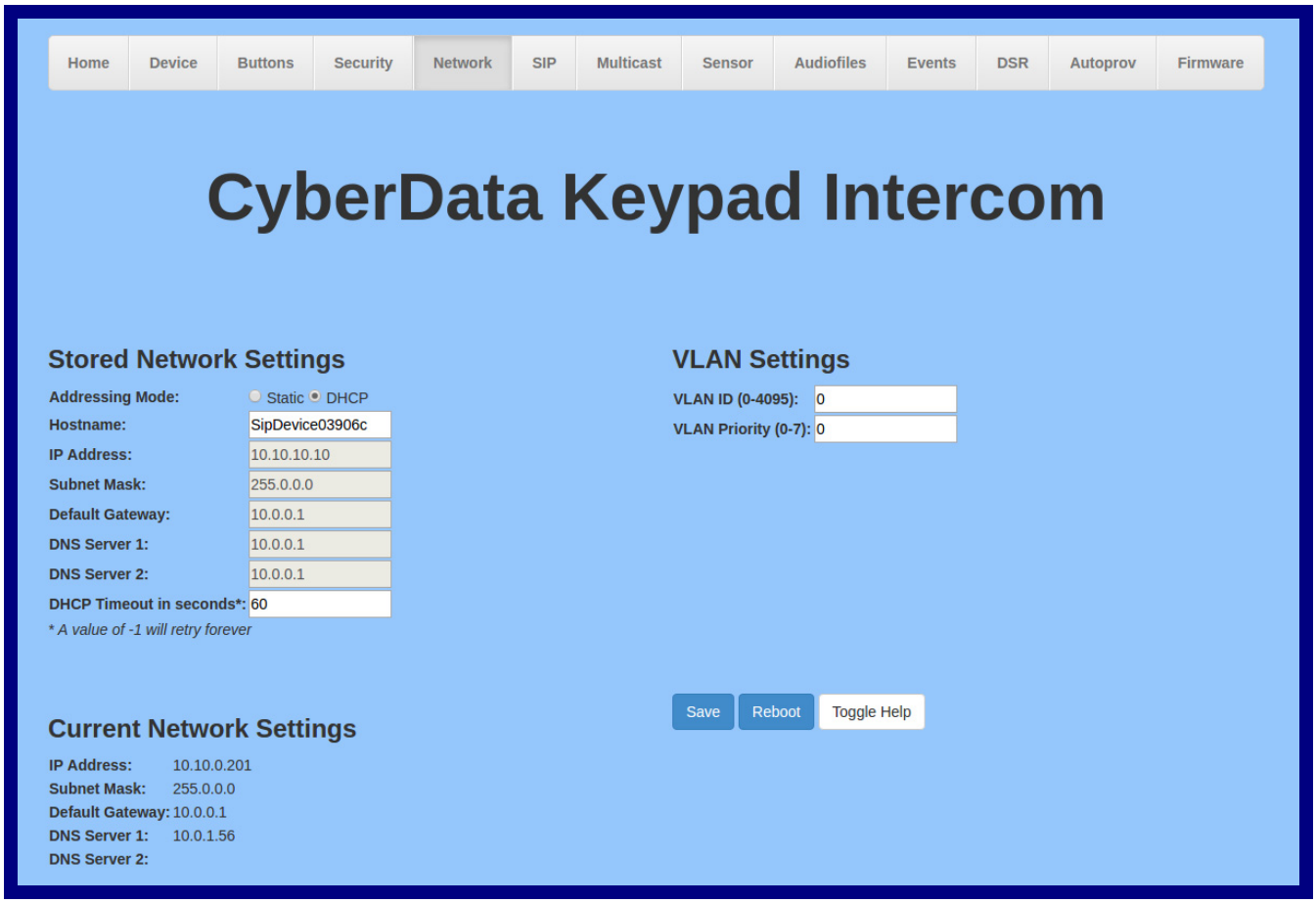
<ValidTo0>Wdy17:00</ValidTo0> Weekdays from 9am to 5pm

Note The identifiers in **to** and **from** must match (for example, **named day/named day**, **Wdy/Wdy**, **Wnd/Wnd**, **All/All**).

2.6.8 Configure the Network Parameters

1. Click the **Network** menu button to open the **Network** page (Figure 2-26).

Figure 2-26. Network Configuration Page



2. On the **Network** page, enter values for the parameters indicated in Table 2-18.

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-18. Network Configuration Parameters

Web Page Item	Description
Stored Network Settings	
Addressing Mode ?	Select either DHCP IP Addressing or Static Addressing by marking the appropriate radio button. DHCP Addressing mode is enabled on default and the device will attempt to resolve network addressing with the local DHCP server upon boot. If DHCP Addressing fails, the device will revert to the last known IP address or the factory default address if no prior DHCP lease was established. See Section 2.6.1, "Factory Default Settings" for factory default settings. Be sure to click **Save** and **Reboot** to store changes when configuring a Static address.
Hostname ?	This is the hostname provided by the DHCP server. See the DHCP/DNS server documentation for more information. Enter up to 64 characters.
IP Address ?	Enter the Static IPv4 network address in dotted decimal notation.
Subnet Mask ?	Enter the Subnet Mask in dotted decimal notation.
Default Gateway ?	Enter the Default Gateway IPv4 address in dotted decimal notation.
DNS Server 1 ?	Enter the primary DNS Server IPv4 address in dotted decimal notation.
DNS Server 2 ?	Enter the secondary DNS Server IPv4 address in dotted decimal notation.
DHCP Timeout in seconds ?	Specify the desired time-out duration (in seconds) that the device will wait for a response from the DHCP server before reverting back to the stored static IP address. The stored static IP address may be the last known IP address or the factory default address if no prior DHCP lease was established. Enter up to 8 characters. A value of -1 will retry forever.
VLAN Settings	
VLAN ID (0-4095) ?	Specify the IEEE 802.1Q VLAN ID number. Enter up to 4 digits. **Note**: The device supports 802.1Q VLAN tagging support. The switch port connected to the device will need to be in “trunking mode” for the VLAN tags to propagate.
VLAN Priority (0-7) ?	Specify the IEEE 802.1p VLAN priority level. Enter 1 digit. A value of 0 may cause the VLAN ID tag to be ignored.
Current Network Settings	Shows the current network settings.
IP Address	Shows the current Static IP address.
Subnet Mask	Shows the current Subnet Mask address.
Default Gateway	Shows the current Default Gateway address.
DNS Server 1	Shows the current DNS Server 1 address.
DNS Server 2	Shows the current DNS Server 2 address.

Table 2-18. Network Configuration Parameters (continued)

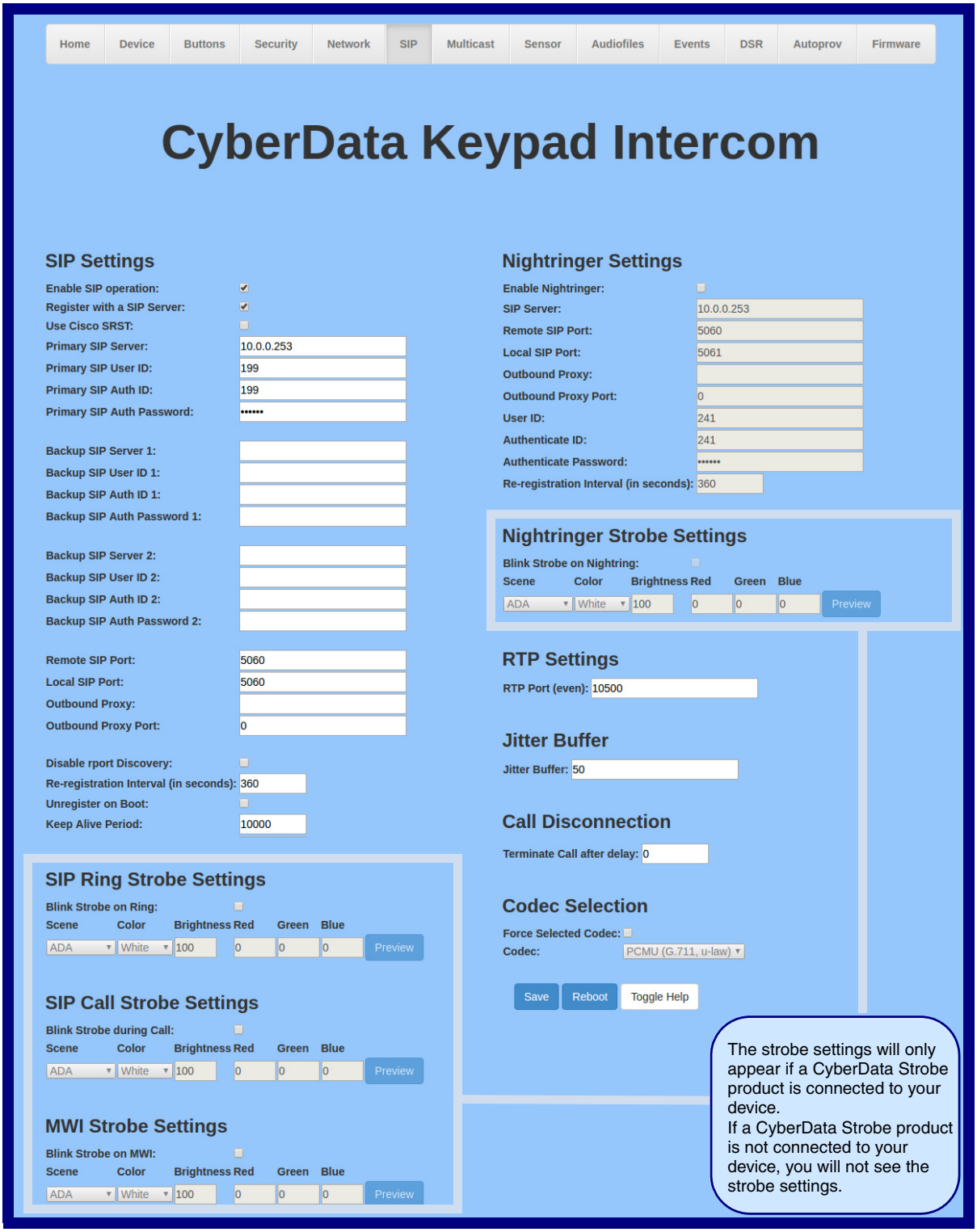
Web Page Item	Description
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.
Toggle Help	Click on the **Toggle Help** button to see a short description of some of the web page items. First click on the **Toggle Help** button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

Note You must click on the **Save** button and then the **Reboot** button for the changes to take effect.

2.6.9 Configure the SIP Parameters

1. Click on the **SIP** menu button to open the **SIP** page (Figure 2-27).

Figure 2-27. SIP Configuration Page



2. On the **SIP** page, enter values for the parameters indicated in Table 2-19.

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-19. SIP Configuration Parameters

Web Page Item	Description
SIP Settings	
Enable SIP Operation ?	When enabled, the device will transmit, receive, and process SIP messages according to the configured SIP settings below.
Register with a SIP Server ?	When enabled, the device will attempt to register to the configured SIP Server(s) on this page. To configure the device to send and receive point-to-point SIP calls, enable **SIP Operation** and disable **Register with a SIP Server** (see Section 2.6.9.1, "Point-to-Point Configuration").
Use Cisco SRST ?	When enabled, the backup servers are handled according to Cisco SRST (Survivable Remote Site Telephony). It is required for use in clustered Cisco Unified Communications Manager topologies.
Primary SIP Server ?	Enter the SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the primary SIP server. This field can accept entries of up to 255 characters in length.
Primary SIP User ID ?	Specify the SIP User ID for the Primary SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the primary SIP server. Enter up to 64 alphanumeric characters.
Primary SIP Auth ID ?	Specify the Authenticate ID for the Primary SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Primary SIP Auth Password ?	Specify the Authenticate Password for the Primary SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Server 1 ?	Enter the backup SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the backup SIP server. This field can accept entries of up to 255 characters in length.
Backup SIP User ID 1 ?	Specify the SIP User ID for the first backup SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the first backup SIP server. Enter up to 64 alphanumeric characters.
Backup SIP Auth ID 1 ?	Specify the Authenticate ID for the first backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Auth Password 1 ?	Specify the Authenticate Password for the first backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Server 2 ?	Enter a second backup SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the second backup SIP server. This field can accept entries of up to 255 characters in length.
Backup SIP User ID 2 ?	Specify the SIP User ID for the second backup SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the second backup SIP server. Enter up to 64 alphanumeric characters.
Backup SIP Auth ID 2 ?	Specify the Authenticate ID for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.

Table 2-19. SIP Configuration Parameters (continued)

Web Page Item	Description
Backup SIP Auth Password 2	Specify the Authenticate Password for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Remote SIP Port	The Remote SIP Port is the port number the device will use as the destination port when sending SIP messages. The default Remote SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
Local SIP Port	The Local SIP Port is the port number the device will use to receive SIP messages. The default Local SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
Outbound Proxy	Enter the Outbound Proxy address as an IPv4 address in dotted decimal notation or a fully qualified domain name (FQDN). When an IP address is configured, the device will send all SIP messages to this IP address. When an FQDN is configured, the device will run DNS NAPTR, SRV, and A queries on the FQDN to resolve an IP address to which it will send all SIP messages. This field can accept entries of up to 255 characters in length.
Outbound Proxy Port	The Outbound Proxy Port is port number used as the destination port when sending SIP messages to the outbound proxy. A value of 0 will default to 5060. The supported range is 0-65536. Enter up to 5 digits.
Disable rport Discovery	Disabling rport Discovery will prevent the device from including the public WAN IP address and port number in the contact information that is sent to the remote SIP servers. This will generally only need to be enabled when using an SBC or SIP ALG in conjunction with a remote SIP server.
Re-registration Interval (in seconds)	The SIP Re-registration interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
Unregister on Boot	When enabled, the device will send one registration with an expiry of 0 on boot.
Keep Alive Period	The minimum time in milliseconds between keep-alive packets sent for nat traversal. A value of 0 will disable keep alive packets.

Table 2-19. SIP Configuration Parameters (continued)

Web Page Item	Description
SIP Ring Strobe Settings	**The following strobe settings will only appear if a CyberData Strobe product is connected to your device. If a CyberData Strobe product is not connected to your device, you will not see the strobe settings.**
Blink Strobe on Ring	When selected, the Strobe will blink a scene when ringing.
Scene	Select desired scene (only one may be chosen).
ADA Compliant	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.
Slow Fade	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.
Fast Blink	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.
Color	Select desired color (only one may be chosen).
Brightness	How bright the strobe will blink when there is a SIP Ring. This is the maximum brightness for “fade” type scenes.
Red	The red LED value for SIP Ring.
Green	The green LED value for SIP Ring.
Blue	The blue LED value for SIP Ring.
Preview	Use this button to preview the strobe flashing behavior for the **SIP Ring Strobe Settings**.
SIP Call Strobe Settings	**The following strobe settings will only appear if a CyberData Strobe product is connected to your device. If a CyberData Strobe product is not connected to your device, you will not see the strobe settings.**
Blink Strobe during Call	When selected, the Strobe will blink a scene during a call.
Scene	Select desired scene (only one may be chosen).
ADA Compliant	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.
Slow Fade	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.
Fast Blink	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.
Color	Select desired color (only one may be chosen).
Brightness	How bright the strobe will blink when there is a SIP Call. This is the maximum brightness for “fade” type scenes.
Red	The red LED value for SIP Call.

Table 2-19. SIP Configuration Parameters (continued)

Web Page Item	Description
Green	The green LED value for SIP Call.
Blue	The blue LED value for SIP Call.
Preview	Use this button to preview the strobe flashing behavior for the **SIP Call Strobe Settings**.
MWI Strobe Settings	**The following strobe settings will only appear if a CyberData Strobe product is connected to your device. If a CyberData Strobe product is not connected to your device, you will not see the strobe settings.**
Blink Strobe on MWI	When selected, the strobe will blink a scene when a voicemail is waiting for its extension.
Scene	Select desired scene (only one may be chosen).
ADA Compliant	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.
Slow Fade	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.
Fast Blink	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.
MWI Call Color	Select desired color (only one may be chosen).
Brightness	How bright the strobe will blink when there is a message waiting. This is the maximum brightness for “fade” type scenes.
Red	The red LED value for MWI.
Green	The green LED value for MWI.
Blue	The blue LED value for MWI.
Preview	Use this button to preview the strobe flashing behavior for the **MWI Strobe Settings**.
Nightringer Settings	
Enable Nightringer	When Nightringer is enabled, the device will attempt to register a second extension with the SIP server. Any calls made to this extension will play a ringtone (corresponds to **Night Ring** on the **Audiofiles** page). By design, it is not possible to answer a call to the Nightringer extension.
SIP Server	Enter the SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's Nightringer extension on the SIP server. This field can accept entries of up to 255 characters in length.
Remote SIP Port	The Remote SIP Port is the port number the device will use as the destination port when sending SIP messages for the Nightringer extension. The default Remote SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.

Table 2-19. SIP Configuration Parameters (continued)

Web Page Item	Description
Local SIP Port	The Local SIP Port is the port number the device will use to receive SIP messages for the Nightringer extension. This value cannot be the same as the **Local SIP Port** for the primary extension. The default Local SIP Port is 5061. The supported range is 0-65536. Enter up to 5 digits.
Outbound Proxy	Enter the Outbound Proxy address as an IPv4 address in dotted decimal notation or a fully qualified domain name (FQDN). When an IP address is configured, the device will send all SIP messages to this IP address for the Nightringer extension. When an FQDN is configured, the device will run DNS NAPTR, SRV, and A queries on the FQDN to resolve an IP address to which it will send all SIP messages for the Nightringer extension. This field can accept entries of up to 255 characters in length.
Outbound Proxy Port	The Outbound Proxy Port is port number used as the destination port when sending SIP messages to the outbound proxy for the Nightringer extension. A value of 0 will default to 5060. The supported range is 0-65536. Enter up to 5 digits.
User ID	Specify the SIP User ID for the SIP server. This parameter becomes the user portion of the SIP-URI for the device's Nightringer extension. Enter up to 64 alphanumeric characters.
Authenticate ID	Specify the Authenticate ID for the SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Authenticate Password	Specify the Authenticate Password for the SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Re-registration Interval (in seconds)	The SIP Re-registration Interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
Nightringer Strobe Settings	**The following strobe settings will only appear if a CyberData Strobe product is connected to your device. If a CyberData Strobe product is not connected to your device, you will not see the strobe settings.**
Blink Strobe on Nightring	When selected, the Strobe will blink a scene when the Nightringer is ringing.
Scene	Select desired scene (only one may be chosen).
ADA Compliant	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.
Slow Fade	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.
Fast Blink	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.
Color	Select desired color (only one may be chosen).
Brightness	How bright the strobe will blink when the Nightringer is ringing. This is the maximum brightness for “fade” type scenes.
Red	The red LED value for Nightringer.
Green	The green LED value for Nightringer.
Blue	The blue LED value for Nightringer.

Table 2-19. SIP Configuration Parameters (continued)

Web Page Item	Description
Preview	Use this button to preview the strobe flashing behavior for the **Nightringer Strobe Settings**.
RTP Settings	
RTP Port (even)	Specify the port number used for the RTP stream after establishing a SIP call. This port number must be an even number and defaults to 10500. The supported range is 0-65536. Enter up to 5 digits.
Call Disconnection	
Terminate Call After Delay	Automatically terminate an active call after a given delay in seconds. A value of 0 will disable this function. Enter up to 8 digits.

Table 2-19. SIP Configuration Parameters (continued)

Web Page Item	Description
Codec Selection	
Force Selected Codec	When configured, this option will allow you to force the device to negotiate for the selected codec. Otherwise, the device will perform codec negotiation using the default list of supported codecs.
Codec	Select the desired codec (only one may be chosen).
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.
Toggle Help	Click on the **Toggle Help** button to see a short description of some of the web page items. First click on the **Toggle Help** button, and you will see a question mark ( ) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

Note You must click on the **Save** button and then the **Reboot** button for the changes to take effect.

Note The **Terminate Call After Delay** setting does not require a reboot for the changes to take effect.

Note For specific server configurations, go to the following website address:

http://www.cyberdata.net/connecting-to-ip-pbx-servers/

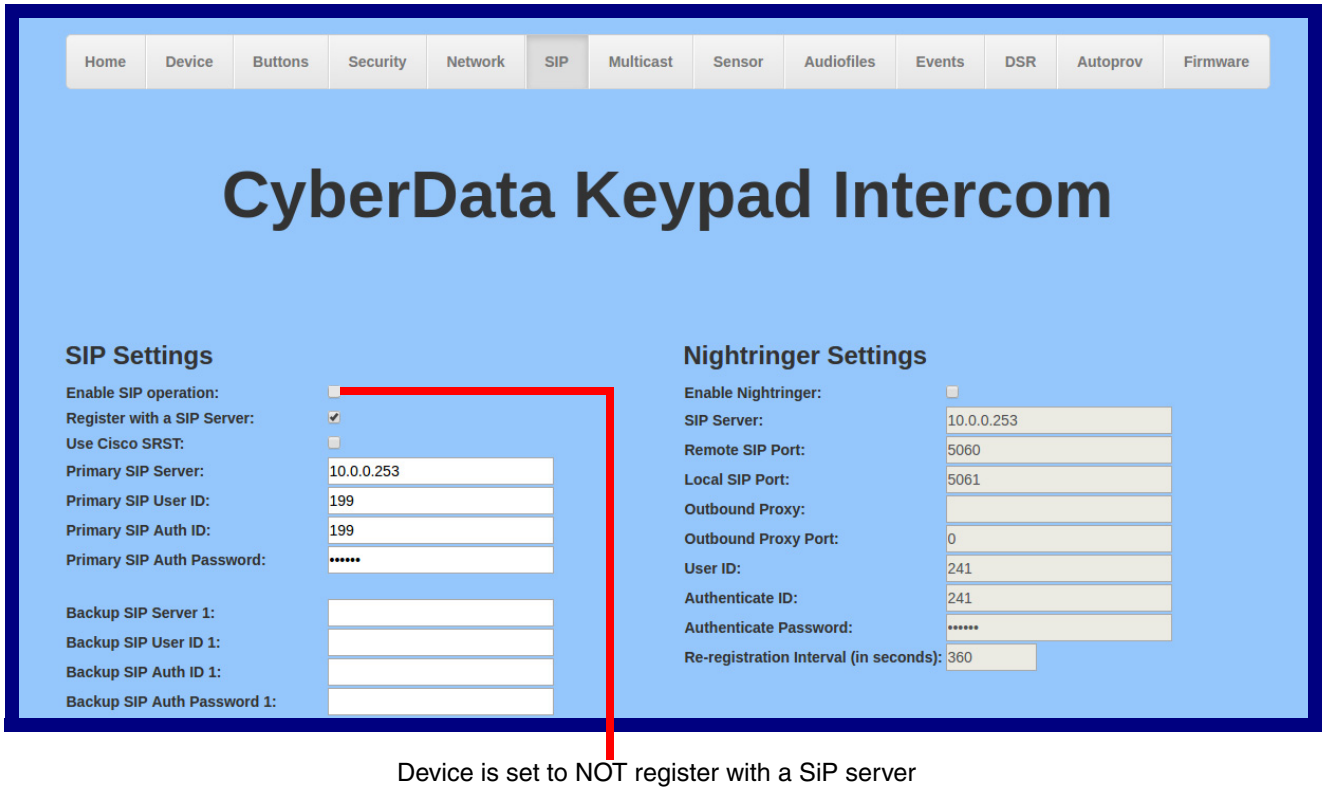
2.6.9.1 Point-to-Point Configuration

When the device is set to not register with a SIP server (see Figure 2-28), it is possible to set the device to dial out to a single endpoint.

In this case, the dial-out extension should be the IP address of the remote device. The device can also receive Point-to-Point calls. The delayed DTMF functionality is available in the Point-to-Point Mode.

Note Receiving point-to-point SiP calls may not work with all phones.

Figure 2-28. SIP Page Set to Point-to-Point Mode



2.6.10 Configure the Multicast Parameters

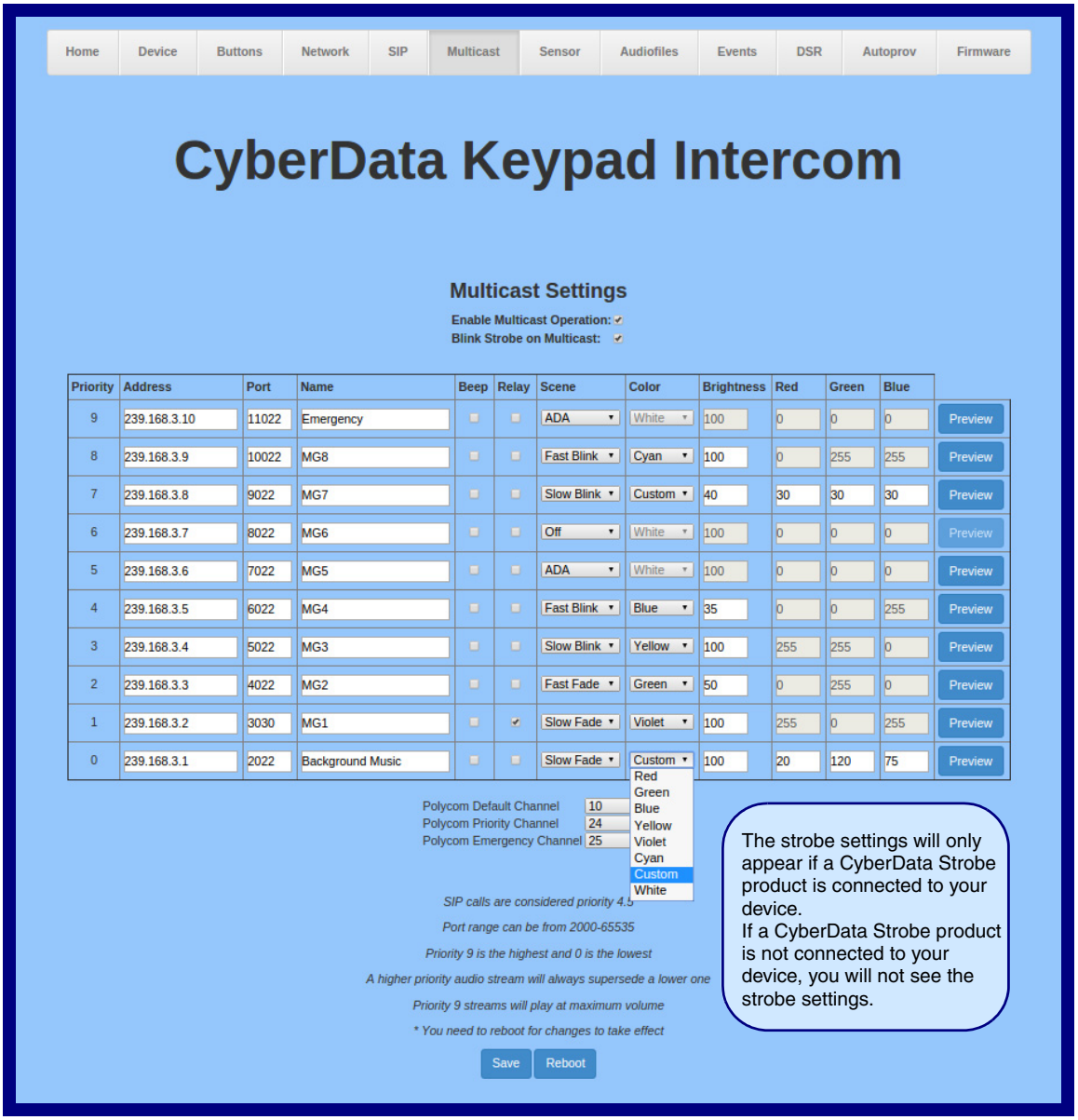
The Multicast Configuration page allows the device to join up to ten paging zones for receiving ulaw/alaw encoded RTP audio streams.

A paging zone can consist of one or many CyberData multicast group-enabled products. There is no limit to how many speakers can be in a given paging zone. Each multicast group is defined by a multicast address and port number.

Each multicast group is assigned a priority, allowing simultaneously arriving pages to be serviced based on importance. Multicast groups are compatible with IGMP through version 3. The device supports simultaneous SIP and Multicast.

1. Click on the **Multicast** menu button to open the **Multicast** page. See Figure 2-29.

Figure 2-29. Multicast Configuration Page



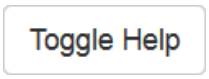
2. On the **Multicast** page, enter values for the parameters indicated in Table 2-20.

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-20. Multicast Page Parameters

Web Page Item	Description
Enable Multicast Operation	Enables or disables multicast operation.
Blink Strobe on Multicast ?	When selected, the Strobe will blink a scene when a multicast is received. **Note: The following strobe settings will only appear if a CyberData Strobe product is connected to your device. If a CyberData Strobe product is not connected to your device, you will not see the strobe settings.**
Priority	Indicates the priority for the multicast group. Priority **9** is the highest (emergency streams). **0** is the lowest (background music). SIP calls are considered priority **4.5**. See Section 2.6.10.1, "Assigning Priority" for more details.
Address	Enter the multicast IP Address for this multicast group (15 character limit).
Port	Enter the port number for this multicast group (5 character limit [range can be from 2000 to 65535]). **Note**: The multicast ports have to be even values. The webpage will enforce this restriction.
Name	Assign a descriptive name for this multicast group (25 character limit).
Buffer	Device will buffer up to four minutes of audio and then play back the recording after the multicast stream finishes or after the buffer is full.
Beep	When selected, the device will play a beep before multicast audio is sent.
Relay	When selected, the device will activate a relay before multicast audio is sent.
Scene ?	Select desired scene (only one may be chosen). **Note: The following strobe settings will only appear if a CyberData Strobe product is connected to your device. If a CyberData Strobe product is not connected to your device, you will not see the strobe settings.**
ADA Compliant ?	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.
Slow Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink ?	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.
Fast Blink ?	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.
Color ?	Select desired color (only one may be chosen).
Brightness ?	How bright the strobe will blink on a multicast page. This is the maximum brightness for “fade” type scenes.
Red ?	The red LED value for Multicast.
Green ?	The green LED value for Multicast.
Blue ?	The blue LED value for Multicast.

Table 2-20. Multicast Page Parameters (continued)

Web Page Item	Description
Polycom Default Channel	When a default Polycom channel/group number is selected, the device will subscribe to the default channel for one-way group pages. Group Numbers 1-25 are supported. Or, select **Disabled** to disable this channel.
Polycom Priority Channel	When a priority Polycom channel/group number is selected, the device will subscribe to the priority channel for one-way group pages. Group Numbers 1-25 are supported. Or, select **Disabled** to disable this channel.
Polycom Emergency Channel	When an emergency Polycom channel/group number is selected, the device will subscribe to the default channel for one-way group pages. Group Numbers 1-25 are supported. Or, select **Disabled** to disable this channel.
	Use this button to preview the strobe flashing behavior for the **Multicast Strobe Settings**.
	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
	Click on the **Reboot** button to reboot the system.
	Click on the **Toggle Help** button to see a short description of some of the web page items. First click on the **Toggle Help** button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

Note You must click on the **Save** button for the changes to take effect.

Note Changing the **Enable Multicast Operation**, **Address**, **Beep**, or **Relay** settings require a reboot for the changes to take effect.

Note Enabling or disabling the strobe or changing any of the strobe options require you to click on the **Save** button for the changes to take effect.

2.6.10.1 Assigning Priority

The device will prioritize simultaneous audio streams according to their priority in the list.

If both SIP and Multicast is enabled, SIP audio streams are considered priority **4.5**. SIP audio will interrupt multicast streams with priority **0** through **4** and will be interrupted by multicast streams with priority **5** through **9**.

During priority **9** multicast streams, the volume is set to maximum.

Note SIP calls, multicast streams, ring tones, ringback tones, and nightring tones are all prioritized.

Ringtones and Nightringtones

Ringtones all play at the same priority level. This means that it is possible to have a nightring tone and a normal ringtone playing at the same time.

2.6.11 Configure the Sensor Configuration Parameters

The door sensor (pins 5 and 6) on the header can be used to monitor a door's open or closed state. There is an option on the **Sensor** page to trigger on an open or short condition on these pins. The door sensor alarm will be activated when the **Door Open Timeout** parameter has been met.

The intrusion sensor is an optical sensor installed on the Intercom board and will be activated when the Intercom is removed from the case.

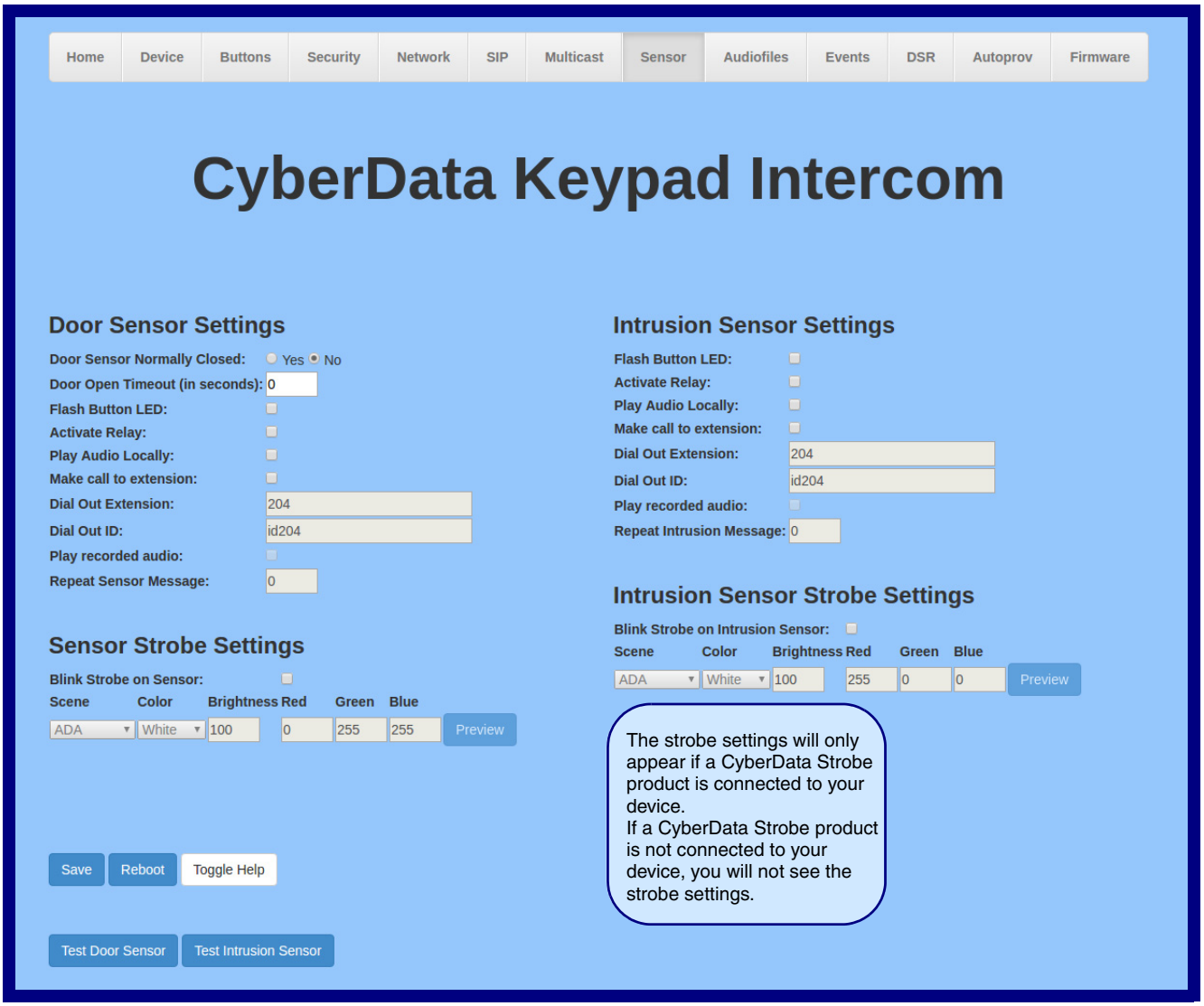
Each sensor can trigger up to five different actions:

- Flash the LED until the sensor is deactivated (roughly 10 times/second)
- Activate the relay until the sensor is deactivated
- Loop an audio file out of the Intercom speaker until the sensor is deactivated
- Call an extension and establish two way audio
- Call an extension and play a pre-recorded audio file

Note Calling a preset extension can be set up as a point-to-point call, but currently can't send delayed DTMF tones.

1. Click **Sensor** menu button to open the **Sensor** page (Figure 2-30).

Figure 2-30. Sensor Configuration Page



2. On the **Sensor** page, enter values for the parameters indicated in Table 2-21.

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-21. Sensor Configuration Parameters

Web Page Item	Description
Door Sensor Settings	
Door Sensor Normally Closed ?	Select the inactive state of the door sensor. The door sensor is also known as the Sense Input on the device's terminal block.
Door Open Timeout (in seconds) ?	The time (in seconds) the device will wait before it performs an action when the on-board door sensor is activated. The action(s) performed are based on the configured Door Sensor Settings below. Enter up to 5 digits.
Flash Button LED ?	When selected, the Call button LED will flash until the on-board door sensor is deactivated (roughly 10 times/second).
Activate Relay ?	When selected, the device's on-board relay will be activated until the on-board door sensor is deactivated.
Play Audio Locally ?	When selected, the device will loop an audio file out of the speaker until the door sensor is deactivated.
Make call to extension ?	When selected, the device will call an extension when the on-board door sensor is activated. Use the **Dial Out Extension** field below to specify the extension the device will call.
Dial Out Extension ?	Specify the extension the device will call when the on-board door sensor is activated. Enter up to 64 alphanumeric characters.
Dial Out ID ?	An additional Caller identification string added to outbound calls. Enter up to 64 alphanumeric characters.
Play recorded audio ?	When selected, the device will call the **Dial Out Extension** and play an audio file to the phone answering the SIP call (corresponds to **Door Ajar** on the **Audiofiles** page).
Repeat Sensor Message ?	The number of times to repeat the audio message through the local speaker or to the remote endpoint. A value of 0 will repeat forever. Enter a value from 0-65536.
Sensor Strobe Settings	**The following strobe settings will only appear if a CyberData Strobe product is connected to your device. If a CyberData Strobe product is not connected to your device, you will not see the strobe settings.**
Blink Strobe on Sensor ?	When selected, the Strobe will blink a scene when the sensor is triggered.
Scene ?	Select desired scene (only one may be chosen).
ADA Compliant ?	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.
Slow Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink ?	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.
Fast Blink ?	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.

Table 2-21. Sensor Configuration Parameters (continued)

Web Page Item	Description
Color	Select desired color (only one may be chosen).
Brightness	How bright the strobe will blink when the sensor is triggered. This is the maximum brightness for “fade” type scenes.
Red	The red LED value for the Sensor.
Green	The green LED value for the Sensor.
Blue	The blue LED value for the Sensor.
Preview	Use this button to preview the strobe flashing behavior for the **Sensor Strobe Settings**.
Intrusion Sensor Settings	
Flash Button LED	When selected, the Call button LED will flash until the intrusion sensor is deactivated (roughly 10 times/second).
Activate Relay	When selected, the device's on-board relay will be activated until the intrusion sensor is deactivated.
Play Audio Locally	When selected, the device will loop an audio file out of the speaker until the intrusion sensor is deactivated.
Make call to extension	When selected, the device will call an extension when the intrusion sensor is activated. Use the **Dial Out Extension** field below to specify the extension the device will call.
Dial Out Extension	Specify the extension the device will call when the intrusion sensor is activated. Enter up to 64 alphanumeric characters.
Dial Out ID	An additional Caller identification string added to outbound calls. Enter up to 64 alphanumeric characters.
Play recorded audio	When selected, the device will call the **Dial Out Extension** and play an audio file (corresponds to **Intrusion Sensor Triggered** on the **Audiofiles** page) to the phone answering the SIP call when the intrusion sensor is activated.
Repeat Intrusion Message	The number of times to repeat the audio message through the local speaker or to the remote endpoint. A value of 0 will repeat forever. Enter a value from 0-65536.
Intrusion Sensor Strobe Settings	**The following strobe settings will only appear if a CyberData Strobe product is connected to your device. If a CyberData Strobe product is not connected to your device, you will not see the strobe settings.**
Blink Strobe on Intrusion Sensor	When selected, the Strobe will blink a scene when the intrusion sensor is triggered.
Scene	Select desired scene (only one may be chosen).
ADA Compliant	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.
Slow Fade	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.

Table 2-21. Sensor Configuration Parameters (continued)

Web Page Item	Description
Fast Blink	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.
Color	Select desired color (only one may be chosen).
Brightness	How bright the strobe will blink when the intrusion sensor is triggered. This is the maximum brightness for “fade” type scenes.
Red	The red LED value for the Intrusion Sensor.
Green	The green LED value for the Intrusion Sensor.
Blue	The blue LED value for the Intrusion Sensor.
Preview	Use this button to preview the strobe flashing behavior for the **Intrusion Sensor Strobe Settings**.
Test Door Sensor	Click the T**est Door Sensor** button to test the door sensor.
Test Intrusion Sensor	Click the T**est Intrusion Sensor** button to test the Intrusion sensor.
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.
Toggle Help	Click on the **Toggle Help** button to see a short description of some of the web page items. First click on the **Toggle Help** button, and you will see a question mark ( ) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

Note You must click on the **Save** button for the changes to take effect.

Note None of the **Sensor Configuration Page** settings require a reboot for the changes to take effect.

2.6.12 Configure the Audio Configuration Parameters

The **Audiofiles** page is used to add custom audio to the board. User uploaded audio will take precedence over the audio files shipped with the Intercom.

1. Click on the **Audiofiles** menu button to open the **Audiofiles** page (Figure 2-31).

Figure 2-31. Audiofiles Configuration Page

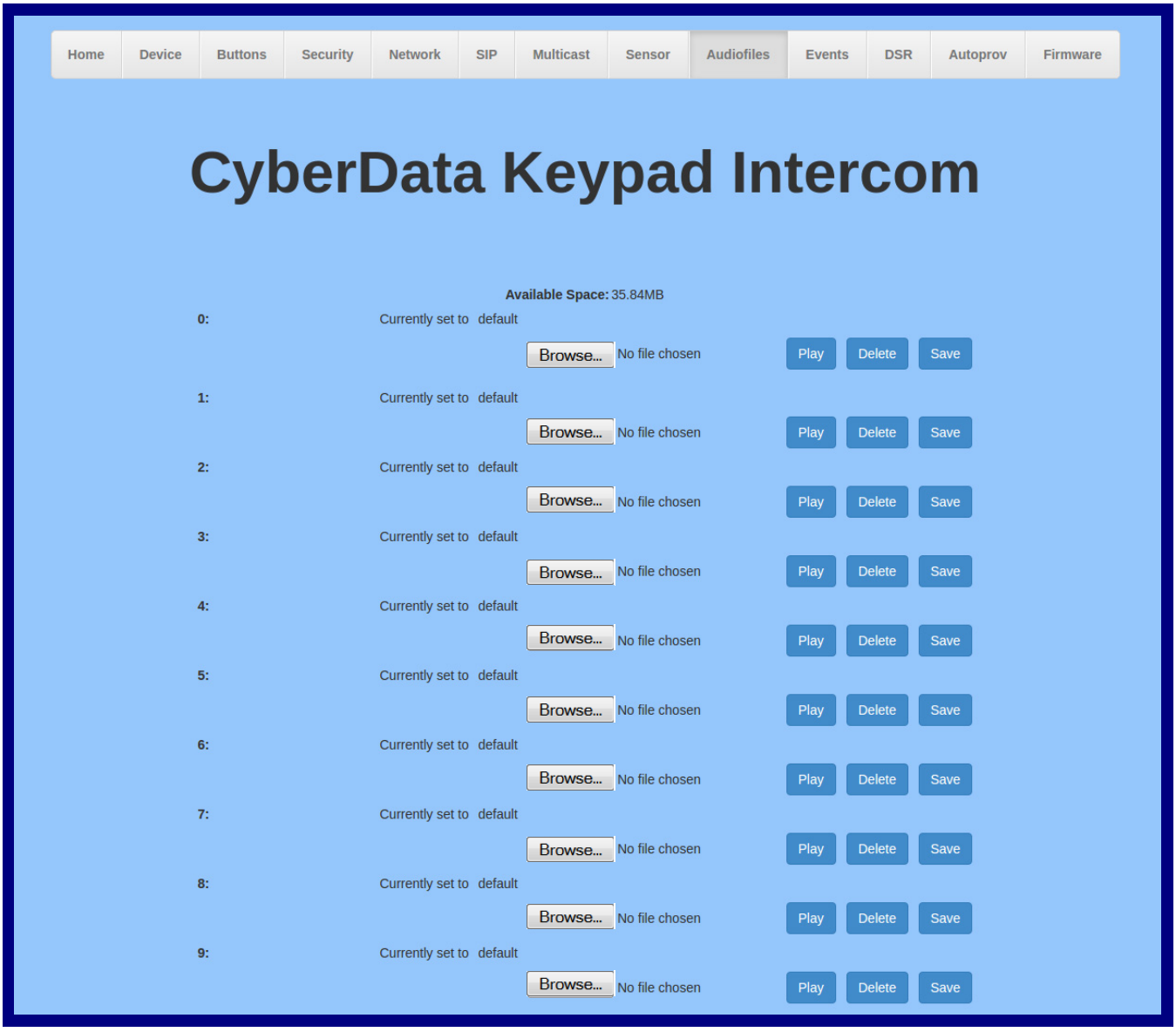


Figure 2-32. Audiofiles Configuration Page (continued)

2. On the **Audiofiles** page, enter values for the parameters indicated in Table 2-22.

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-22. Audiofiles Configuration Parameters

Web Page Item	Description
Available Space	Shows the space available for the user to save custom audio files if they want to change the message when the door or sensor is triggered.
0-9	The name of the audio configuration option is the same as the spoken audio that plays on the board (24 character limit). '0' corresponds to the spoken word “zero.” '1' corresponds to the spoken word “one.” '2' corresponds to the spoken word “two.” '3' corresponds to the spoken word “three.” '4' corresponds to the spoken word “four.” '5' corresponds to the spoken word “five.” '6' corresponds to the spoken word “six.” '7' corresponds to the spoken word “seven.” '8' corresponds to the spoken word “eight.” '9' corresponds to the spoken word “nine.”
Dot	Corresponds to the spoken word “dot.” (24 character limit)
Audiotest	Corresponds to the message ***“This is the CyberData IP speaker test message...”*** (24 character limit)
Page tone	Corresponds to a simple tone used for beep on initialization and beep on page (24 character limit).
Your IP Address is	Corresponds to the message “Your IP address is...” (24 character limit).
Rebooting	Corresponds to the spoken word “Rebooting” (24 character limit).
Restoring default	Corresponds to the message “Restoring default” (24 character limit).
Ringback Tone	This is the ringback tone that plays when calling a remote extension (24 character limit).
Ring Tone	This is the tone that plays when set to ring when receiving a call (24 character limit).
Intrusion Sensor Triggered	Corresponds to the message “Intrusion Sensor Triggered” (24 character limit).
Door Ajar	Corresponds to the message “Door Ajar” (24 character limit).
Night Ring	Specifies the ringtone for nightring. By default this parameter uses the same audio file that is selected for the **Ring Tone** parameter.
SIP Multicast Message	This is the message that plays when multicast audio is initiated by the call button.
Blacklist Message	The audio file that will play if a blacklisted security code is entered.
Browse...	Click on the **Browse** button to navigate to and select an audio file.
Play	The **Play** button will play that audio file.

Table 2-22. Audiofiles Configuration Parameters (continued)

Web Page Item	Description
Delete	The **Delete** button will delete any user uploaded audio and restore the stock audio file.
Save	The **Save** button will download a new user audio file to the board once you've selected the file by using the **Browse** button. The **Save** button will delete any pre-existing user-uploaded audio files.

2.6.12.1 User-created Audio Files

User created audio files should be saved in the following format:

RIFF (little-endian) data, WAVE audio, Microsoft PCM, 16 bit, mono 8000 Hz

You can use the free utility *Audacity* to convert audio files into this format. See Figure 2-33 through Figure 2-35.

Figure 2-33. Audacity 1

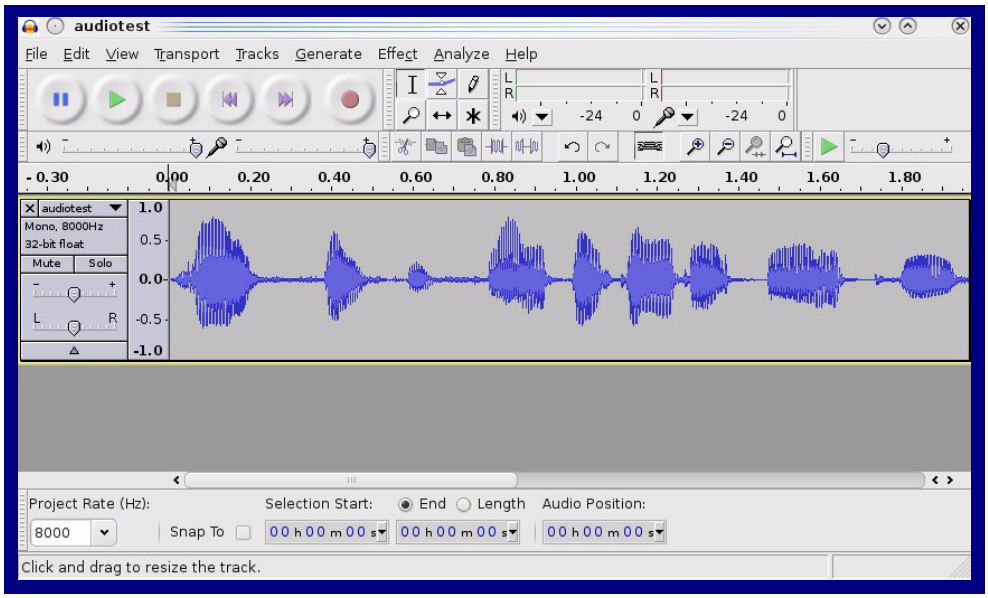
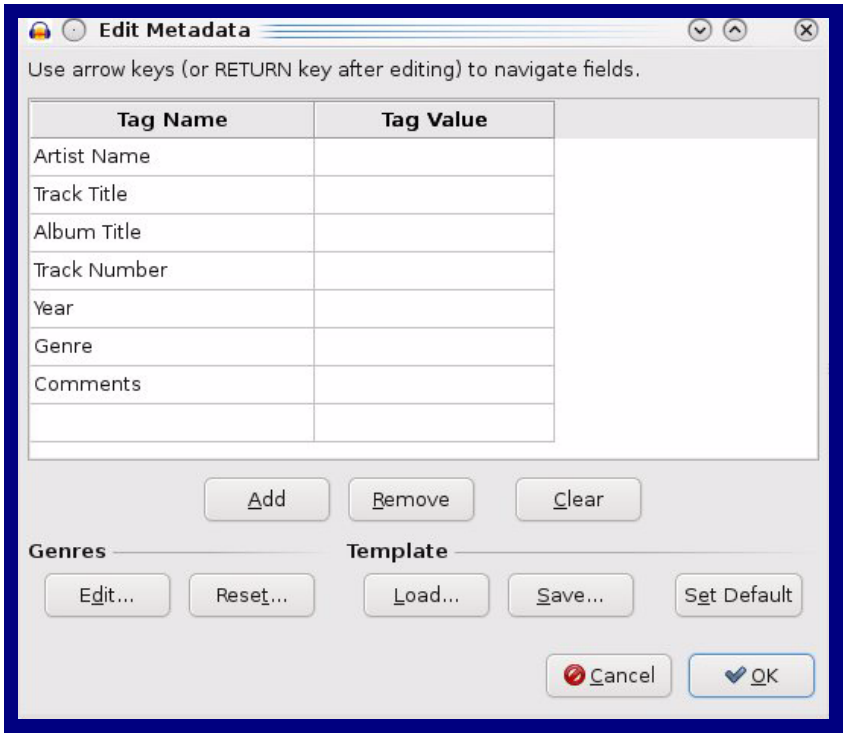


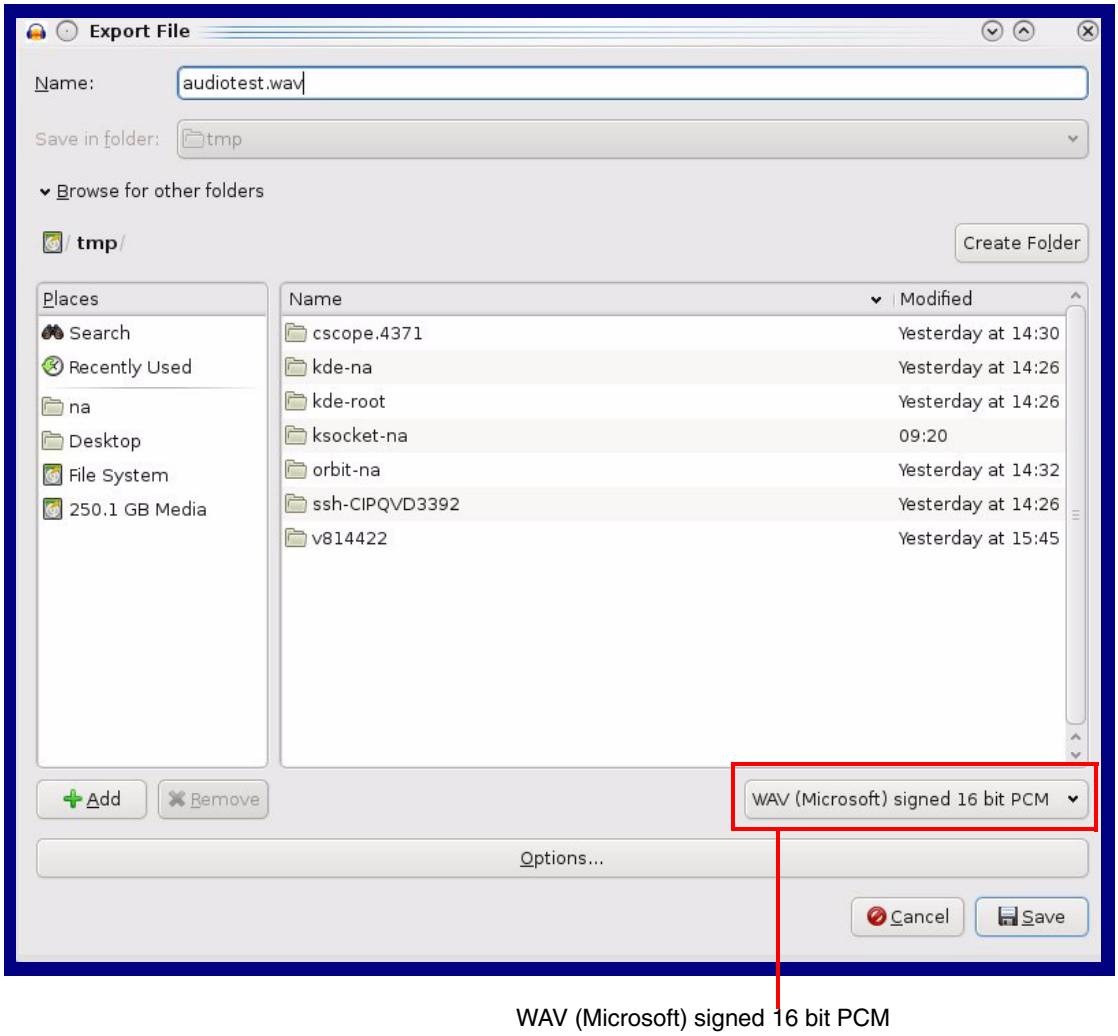
Figure 2-34. Audacity 2



When you export an audio file with Audacity, save the output as:

- **WAV (Microsoft) signed 16 bit PCM**.

Figure 2-35. WAV (Microsoft) signed 16 bit PCM



2.6.13 Configure the Events Parameters

The **Events** page specifies a remote server that can be used to receive HTTP POST events when actions take place on the board.

1. Click on the **Events** menu button to open the **Events** page (Figure 2-36).

Figure 2-36. Event Configuration Page

2. On the **Events** page, enter values for the parameters indicated in Table 2-23.

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-23. Events Configuration Parameters

Web Page Item	Description
Enable Event Generation ?	The device will send HTTP POST events to the specified remote server and port number whenever a certain action takes place. Select an event type below to generate an HTTP POST event.
Events	
Enable Button Events ?	When selected, the device will report Call button presses.
Enable Call Start Events ?	When selected, the device will report the start of a SIP call.
Enable Call Terminated Events ?	When selected, the device will report the end of a SIP call.
Enable Relay Activated Events ?	When selected, the device will report relay activation.
Enable Relay Deactivated Events ?	When selected, the device will report relay deactivation.
Enable Ring Events ?	When selected, the device will report when it starts ringing upon an incoming SIP call. A Ring Event will not be generated when **Auto-Answer Incoming Calls** is enabled on the **Device** page.
Enable Night Ring Events ?	When selected, the device will report when it starts ringing upon an incoming SIP call to the Nightringer extension. As a reminder, the Nightringer extension always rings upon an incoming SIP call and it is not possible to alter this behavior.
Enable Multicast Start Events ?	When selected, the device will report when the device starts playing a multicast audio stream.
Enable Multicast Stop Events ?	When selected, the device will report when the device stops playing a multicast audio stream.
Enable Power On Events ?	When selected, the device will report when it boots.
Enable Sensor Events ?	When selected, the device will report when the on-board sensor is activated.
Enable Remote Relay Events ?	When selected, the device will report when the remote relay (DSR) is activated.
Enable Security Events ?	When enabled, the device will report when the intrusion sensor is activated.
Enable 60 Second Heartbeat ?	When enabled, the device will report a Heartbeat event every 60 seconds. SIP registration is not required to generate Heartbeat events.
Enable Singlewire Start Events ?	When selected, the device will report when a Start event has been received from the Singlewire server.
Enable Singlewire Stop Events ?	When selected, the device will report when a Stop event has been received from the Singlewire server.
Check All	Click on **Check All** to select all of the events on the page.
Uncheck All	Click on **Uncheck All** to de-select all of the events on the page.

Table 2-23. Events Configuration Parameters(continued)

Web Page Item	Description
Event Server	
Server IP Address	The IPv4 address of the event server in dotted decimal notation.
Server Port	Specify the event server port number. The supported range is 0-65536. Enter up to 5 digits.
Server URL	Generally, the destination URL is the name of the application that receives the events and the string in the HTTP POST command. It can be a script used to parse and process the HTTP POST events. Enter up to 127 characters.
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.
Toggle Help	Click on the **Toggle Help** button to see a short description of some of the web page items. First click on the **Toggle Help** button, and you will see a question mark ( ) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

Note You must click on the **Save** button for the changes to take effect.

Note Enabling Event Generation or changing an **Event Server** setting requires a reboot for the changes to take effect.

Note Selecting particular events, **Check All**, or **Uncheck All** does not require a reboot for the changes to take effect.

2.6.13.1 Example Packets for Events

The server and port are used to point to the listening server and the 'Remote Event Server URL' is the destination URL (typically the script running on the remote server that's used to parse and process the POST events).

Note The XML is URL-encoded before transmission so the following examples are not completely accurate.

Here are example packets for every event:

```
POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 197
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>POWERON</event>
</cyberdata>


POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 199
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>HEARTBEAT</event>
</cyberdata>


POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 196
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>BUTTON</event>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 201
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>CALL_ACTIVE</event>
</cyberdata>
POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
```

```
User-Agent: CyberData/1.0.0
Content-Length: 205
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>CALL_TERMINATED</event>
</cyberdata>


POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 197
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>RINGING</event>
</cyberdata>


POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>MULTICAST_START</event>
<index>8</index>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 233
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>MULTICAST_STOP</event>
<index>8</index>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>RELAY_ACTIVATED</event>
</cyberdata>
POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
```

```
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>RELAY_DEACTIVATED</event>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>NIGHTRINGING</event>
</cyberdata>
```

2.6.14 Configure the Door Strike Relay

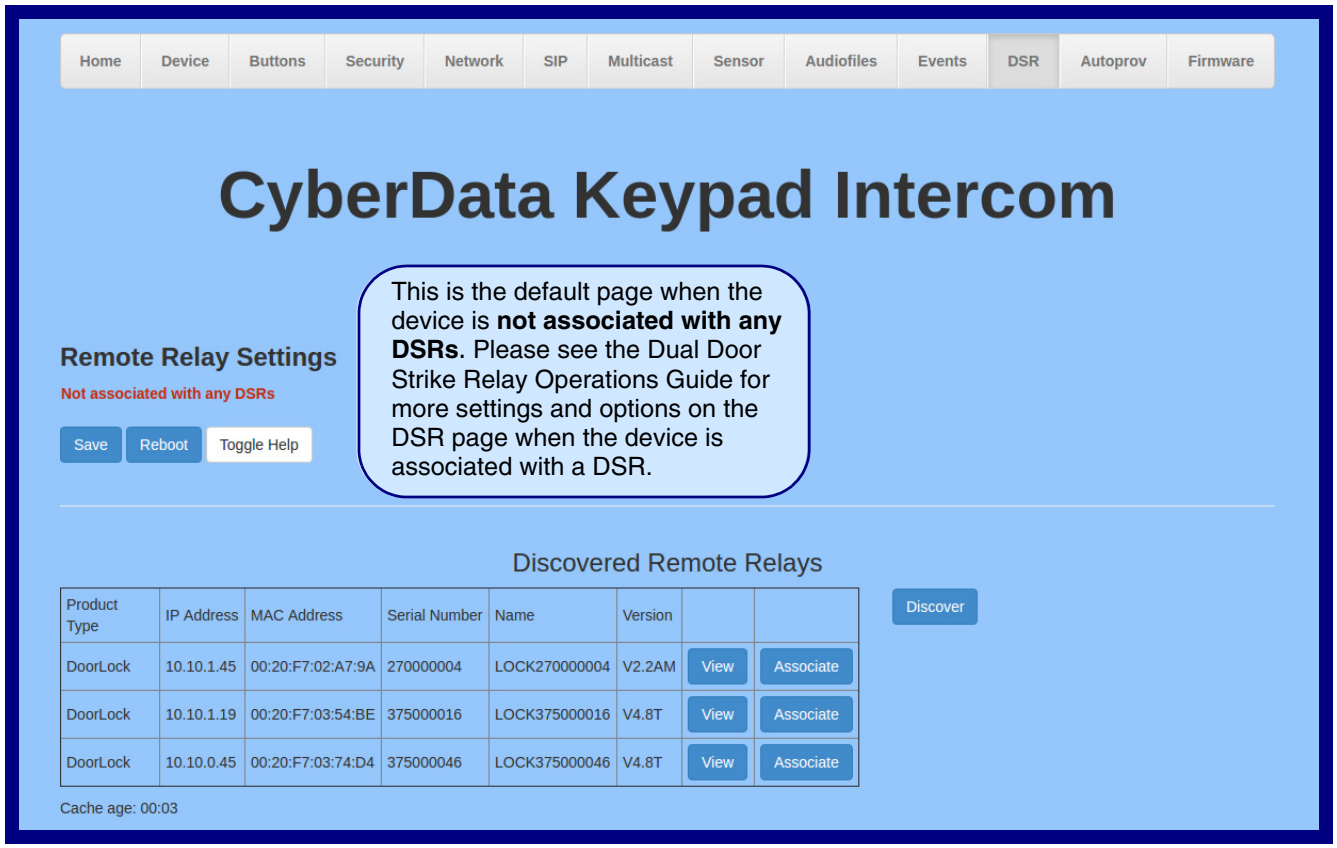
The Door Strike Relay (DSR) is a network device designed to control an electronic door strike. The DSR is meant to be used as a replacement for (or an addition to) the on-board relay. In addition to being a drop-in 12 Amp relay, the DSR can monitor and record when the door is open or closed.

The DSR can be configured to trigger in the following ways: on the entry of a DTMF code, manually through the web interface, or by using a Windows application.

The DSR must be running firmware version 4.8 or later to work with this CyberData device. If you have an older version of the firmware, then please contact CyberData Technical Support. The version number appears in the **Discovered Remote Relays** section on the **DSR** page (Figure 2-37).

1. Click on the **DSR** menu button to open the **DSR** page (Figure 2-37).

Figure 2-37. DSR Page (not associated with any DSRs)



2. On the **DSR** page, enter values for the parameters indicated in Table 2-24.

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-24. DSR Configuration Parameters (not associated with any DSRs)

Web Page Item	Description
Remote Relay Settings	The settings in this section will activate an associated door strike relay.
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.
Toggle Help	Click on the **Toggle Help** button to see a short description of some of the web page items. First click on the **Toggle Help** button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.
Discovered Remote Relays	The **Discovered Remote Relays** section lists all of the networked door strike relays on the network. To associate your device with a door strike relay, click on the **Associate** button. This action allows the user to configure the door strike relay. Keep in mind that a device may only be associated with one door strike relay.
Product Type	Displays the product type of the remote relay.
IP Address	Displays the IP address of the remote relay.
MAC Address	Displays the MAC address of the remote relay.
Serial Number	Displays the serial number of the remote relay.
Name	Displays the name of the remote relay.
Version	Displays the version of the remote relay.
Discover	Use this button to search for and find any remote relays that are available on the network.
View	Use this button to view the settings of a remote relay that has been “discovered” after pressing the **Discover** button.
Associate	Use this button to associate the remote relay with the device. Only one relay may be associated with a device.
Disassociate	Use this button to disassociate the remote relay from the device. Only one relay may be associated with a device. This button is only available when a relay is associated with a device.

Note You must click on the **Save** button and then the **Reboot** button for the changes to take effect.

Note Associating a DSR does not require a reboot. However, you should reboot the device after disassociating a DSR.

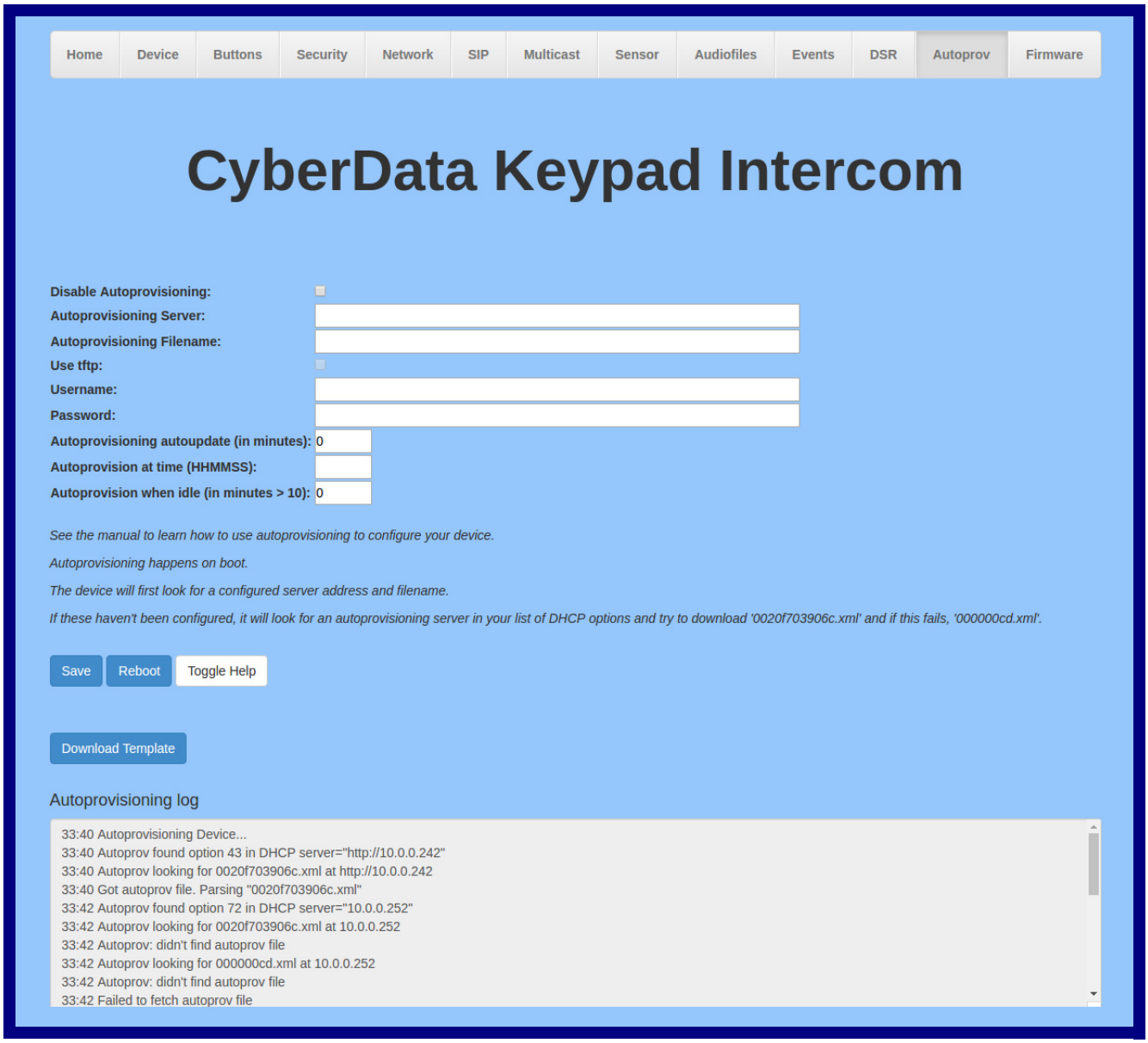
2.6.15 Configure the Autoprovisioning Parameters

Autoprovisioning can be used to automatically configure your device. The autoprovisioning file is an xml file with the device configuration. Values found in this file will override values stored in on-board memory.

Note By default, the device will try to set up its configuration with autoprovisioning.

1. Click the **Autoprov** menu button to open the **Autoprovisioning** page. See Figure 2-38.

Figure 2-38. Autoprovisioning Page



2. On the **Autoprovisioning** page, you may enter values for the parameters indicated in Table 2-25.

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-25. Autoprovisioning Configuration Parameters

Web Page Item	Description
Disable Autoprovisioning ?	Prevent the device from automatically trying to download a configuration file. See Section 2.6.15.1, "Autoprovisioning" for more information.
Autoprovisioning Server ?	Enter the IPv4 address of the provisioning server in dotted decimal notation.
Autoprovisioning Filename ?	The autoprovisioning filename is the configuration filename. The default autoprovisioning filename is in the format of **<mac address>.xml**. Supported filename extensions are .txt, and .xml. The current filename is denoted by an asterisk at the bottom of the **Autoprovisioning Page**. Enter up to 256 characters. A file may have any name with an xml extension. If a file name is entered, the device will look for the specified file name, and only that file.
Use tftp ?	The device will use TFTP (instead of http) to download autoprovisioning files.
Username ?	The username used to authenticate with an autoprovisioning server. Leave this field blank to disable authentication.
Password ?	The password used to authenticate with an autoprovisioning server. Leave this field blank to disable authentication.
Autoprovisioning Autoupdate (in minutes) ?	The reoccurring time (in minutes) the device will wait before checking for new autoprovisioning files. Enter up to 6 digits. A value of 0 will disable this option. **Note**: To use the auto update options, enable the **Set Time with NTP Server on boot** setting on the **Device Configuration Page** page (see Table 2-8).
Autoprovision at time (HHMMSS) ?	The time of day the device will check for a new autoprovisioning file. The time must be 6 characters in length and in HHMMSS format. An empty value will disable this option. **Note**: To use the auto update options, enable the **Set Time with NTP Server on boot** setting on the **Device Configuration Page** page (see Table 2-8).
Autoprovision when idle (in minutes > 10) ?	The idle time (in minutes greater than 10) after which the device will check for a new autoprovisioning file. Enter up to 6 digits. A value of 0 will disable this option. **Note**: To use the auto update options, enable the **Set Time with NTP Server on boot** setting on the **Device Configuration Page** page (see Table 2-8).
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.

Table 2-25. Autoprovisioning Configuration Parameters (continued)

Web Page Item	Description
Reboot	Click on the **Reboot** button to reboot the system.
Toggle Help	Click on the **Toggle Help** button to see a short description of some of the web page items. First click on the **Toggle Help** button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.
Download Template	Press the **Download Template** button to create an autoprovisioning file for the device. See Section 2.6.15.3, "Download Template Button"
Autoprovisioning log	The autoprovisioning log provides information about the latest autoprovisioning attempt (i.e. dhcp options and server accessed and files parsed or not found).

Note You must click on the **Save** button and then the **Reboot** button for the changes to take effect.

2.6.15.1 Autoprovisioning

On boot, the device will look for an autoprovisioning server configured on the Autoprovisioning Page or specified as a DHCP option. When it finds a server, it will try to download the following (in order of preference):

1. The file configured on the autoprovisioning page.
2. A file named according to it's mac address (for example: 0020f7350058.xml).
3. The file 000000cd.xml

The file can be hosted using a standard web server (like apache, IIS, or nginx), and the device can download over SSL. The file server can be an ipv4 address in dotted decimal notation or a fully qualified domain name.

By default, the device will get its autoprovisioning server from the DHCP options. See Section 2.6.15.2, "Sample dhcpd.conf" for an example of how to configure dhcpd to offer autoprovisioning server addresses. If multiple options are set, the device will attempt to download autoprovisioning files from every server.

The DHCP option determines the protocol used to download the autoprovisioning file. The device looks for DHCP options in the following order:

1. Option 43 - a FQDN or an IP address to an http server
2. Option 72 - an IP address to an http server
3. Option 150 - an IP address to a tftp server
4. Option 66 - an IP address to a tftp server or if the entry starts with 'http', a FQDN to a http server.

You can download an autoprovisioning template file from the Autoprovisioning Page using the **Download Template** button (see Table 2-25). This file contains every configuration option that can be set on the board.

Autoprovisioning files can contain the whole configuration or a subset of this file. The first autoprovisioning file can also contain links to other autoprovisioning files.

The <MiscSettings> section contains some examples of additional autoprovisioning files:

```
    <MiscSettings>
        <DeviceName>CyberData VoIP Intercom</DeviceName>
<!--    <AutoprovFile>common.xml</AutoprovFile>-->
<!--    <AutoprovFile>sip_reg[macaddress].xml</AutoprovFile>-->
<!--    <AutoprovFile>audio[macaddress]</AutoprovFile>-->
<!--    <AutoprovFile>device[macaddress].xml</AutoprovFile>-->
    </MiscSettings>
```

After downloading the first autoprovisioning file, the device will step through up to twenty additional <AutoprovFile> entries and try to download these files from the same server.

When the device finds a filename with the string **[macaddress]**, it will replace this string with the mac address.

As an example, the user has configured option 43 on their DHCP server to “http://example.com,” and on their server, they have a file named **0020f7123456.xml** (the same as the mac address of the device).

The file 0020f7123456.xml contains:

```
<?xml version="1.0" encoding="utf-8" ?>
<specific>
         <MiscSettings>
                <DeviceName>Newname</DeviceName>
                <AutoprovFile>common.xml</AutoprovFile>
                <AutoprovFile>sip_reg[macaddress].xml</AutoprovFile>
                <AutoprovFile>audio[macaddress]</AutoprovFile>
                <AutoprovFile>device.xml</AutoprovFile>
         </MiscSettings>
</specific>
```

1. The device will first set it's name to 'Newname'.
2. It will try to download http://example.com/common.xml.
3. It will try to download http://example.com/sip_reg0020f7123456.xml.
4. It will try to download http://example.com/audio0020f7123456.
5. It will try to download http://example.com/device.xml.

The device is reconfigured every time it downloads a new file so if two files configure the same option the last one will be the one that is saved.

It is possible to autoprovision autoprovisioning values (for example, to disable autoprovisioning or to configure a time to check for new files).

Checking for New Autoprovisioning Files after Boot

The device will always check for an autoprovisioning files on boot but it can be configured to also check after a periodic delay, when idle, or at a specified time. When one of these options is set, the device will download its autoprovisioning files again, and if it finds any differences from the files it downloaded on boot, it will force a reboot and reconfigure.

The Autoprovisioning Filename

The autoprovisioning filename can contain a file, a file path, or a directory.

Table 2-26. Autoprovisioning File Name

Autoprovisioning Filename	Autoprovisioning Server	File Downloaded
config.xml	10.0.1.3	10.0.1.3/config.xml
/path/to/config.xml	10.0.1.3	10.0.1.3/path/to/config.xml
subdirectory/path/	10.0.1.3	10.0.1.3/subdirectory/path/0020f7020002.xml

TFTP options may not support subdirectories. If a directory is set in the filename field, firmware and audio files will also be downloaded from this subdirectory.

If the filename ends with a forward slash "/," the device will treat it as a subdirectory.

For example:

The autoprovisioning server is set to "https://www.example.com"

The autoprovisioning filename is set to "cyberdata/"

On boot, the device will try to download:

https://www.example.com/cyberdata/0020f7123456.xml

...and if this fails:

https://www.example.com/cyberdata/000000cd.xml

Audio files and firmware files will also add "cyberdata" to the URL before downloading.

Autoprovisioning Firmware Updates

```
<FirmwareSettings>
  <FirmwareFile>505-uImage-ceilingspeaker</FirmwareFile>
  <FirmwareServer>10.0.1.3</FirmwareServer>
  <OutdoorIntercom30>firmware_file_v9.3.0</OutdoorIntercom30>
  <OutdoorIntercom31>firmware_file_v10.3.0</OutdoorIntercom31>
  <CallButton31>firmware_file_v10.3.0</CallButton31>
</FirmwareSettings>
```

In the <FirmwareSettings> section, the <FirmwareServer> element can be used to specify a different server for hosting firmware files. When this element is not available, the device will try to download the file from the autoprovisioning server.

The device will use the filename to determine when to autoprovision firmware updates. The default configuration is blank, so the first time you set a value in your autoprovisioning file, it may force a firmware update even if the firmware version has not changed.

The <FirmwareFile> name can contain path elements (i.e. /path/to/firmware/10.3.0-uImage-[device_file_name]).

The device also supports product strings for downloading firmware. If the <FirmwareFile> option is not set, the device will look for its particular product string for a firmware filename. In this way, a generic autoprovisioning file can specify unique firmware for a range of products.

The list of valid product strings:

```
<ProductString>CallButton31</ProductString>
<ProductString>EmergencyIntercom31</ProductString>
<ProductString>EmergencyIntercom31SW</ProductString>
<ProductString>IndoorIntercom31</ProductString>
<ProductString>IndoorIntercom31SW</ProductString>
<ProductString>IndoorKeypad31</ProductString>
<ProductString>IndoorKeypad31SW</ProductString>
<ProductString>OfficeRinger31</ProductString>
<ProductString>OfficeRinger31SW</ProductString>
<ProductString>OutdoorIntercom31</ProductString>
<ProductString>OutdoorIntercom31SW</ProductString>
<ProductString>OutdoorKeypad31</ProductString>
<ProductString>OutdoorKeypad31SW</ProductString>
<ProductString>Strobe31</ProductString>
<ProductString>Strobe31SW</ProductString>
```

Autoprovisioning Example 1

Here's a simple example using four autoprovisioning files to configure two devices:

We boot up two devices with mac addresses **00:20:f7:02:00:01** and **00:20:f7:02:00:02** (Device1 and Device2).

The devices are set to use DHCP and that server provides an autoprovisioning server address with option 43. The address is “https://autoprovtest.server.net.” The files on this server are as follows:

000000cd.xml

```
<MiscSettings>
<DeviceName>CyberData Autoprovisioned</DeviceName>
<AutoprovFile>sip_common.xml</AutoprovFile>
<AutoprovFile>sip_[macaddress].xml</AutoprovFile>
</MiscSettings>
```

sip_common.xml

```
<SIPSettings>
<SIPServer>10.0.0.253</SIPServer>
<RemoteSIPPort>5060</RemoteSIPPort>
</SIPSettings>
```

sip_0020f7020001.xml

```
<SIPSettings>
<SIPUserID>198</SIPUserID>
<SIPAuthPassword>ext198</SIPAuthPassword>
<DialoutExtension0>204</DialoutExtension0>
</SIPSettings>
```

sip_0020f7020002.xml

```
<SIPSettings>
<SIPUserID>500</SIPUserID>
<SIPAuthPassword>ext500</SIPAuthPassword>
<DialoutExtension0>555</DialoutExtension0>
</SIPSettings>
```

On boot, Device1 tries to fetch the file **0020f7023614.xml** from “https://autoprovtest.server.net”. This file is not available, so device1 then tries to fetch the file **000000cd.xml**. This file exists, and Device1 parses the three elements.

1. Device1 changes its device name to **CyberData Autoprovisioned**.
2. Device1 finds an AutoprovFile element containing the filename **sip_common.xml**. The device downloads **sip_common.xml** from “https://autoprovtest.server.net,” and imports this configuration, setting the sip server to **10.0.0.253** and the remote port to **5060.3**.
3. Device1 finds another AutoprovFile element containing the filename **sip_[macaddress].xml**. The device replaces the **[macaddress]** with its own mac address value creating **sip_0020f7020001.xml**, downloads this file from “https://autoprovtest.server.net,” and imports this configuration. This sets the user ID to **198**, the password to **ext198**, and the dialout extension to **204**. Device1 is now finished with autoprovisioning.

Device2 goes through the same steps by setting its device name to **CyberData Autoprovisioned**, its SIP server to **10.0.0.253**, and its port to **5060**. When Device2 "sees" **sip_[macaddress].xml**, Device2 replaces it with its own mac address and downloads **sip_0020f7020002.xml** from "https://autoprovtest.server.net." Device2 sets the SIP User ID to **500**, the password to **ext500**, and the dialout extension to **555**.

Autoprovisioning Example 2

Here is another example of setting up your autoprovisioning files:

We boot up two devices with mac addresses **00:20:f7:02:00:01** and **00:20:f7:02:00:02** (Device1 and Device2) and boot them on a network with a DHCP server configured with an autoprovisioning server at **10.0.1.3** on option **150**. Our TFTP server has three files:

0020f7020001.xml

```
<MiscSettings>
<AutoprovFile>common_settings.xml</AutoprovFile>
</MiscSettings>
<SIPSettings>
<SIPUserID>198</SIPUserID>
<SIPAuthPassword>ext198</SIPAuthPassword>
<DialoutExtension0>204</DialoutExtension0>
</SIPSettings>
```

0020f7020002.xml

```
<MiscSettings>
<AutoprovFile>common_settings.xml</AutoprovFile>
</MiscSettings>
<SIPSettings>
<SIPUserID>500</SIPUserID>
<SIPAuthPassword>ext500</SIPAuthPassword>
<DialoutExtension0>555</DialoutExtension0>
</SIPSettings>
```

common_settings.xml

```
<MiscSettings>
<DeviceName>CyberData Autoprovisioned</DeviceName>
</MiscSettings>
<SIPSettings> <SIPServer>10.0.0.253</SIPServer>
<RemoteSIPPort>5060</RemoteSIPPort>
</SIPSettings>
```

1. On boot, Device1 downloads **0020f7020001.xml** from **10.0.1.3** and imports these values. The SIP User ID is **198**, the password is **ext198**, and the dialout extension is **204**.

2. Device1 then gets the filename **common_settings.xml** from the AutoprovFile element and downloads this file from the TFTP server at **10.0.1.3**. and imports these settings. The device name is set to **CyberData Autoprovisioned**, the SIP server is set to **10.0.0.253**, and the port is set to **5060**.

Device2 does the same except it downloads **0020f7020002.xml** on boot and imports these values instead. The Sip User ID is **500**, password is **ext500**, and dialout extension is **555**. Device2 then downloads the **common_settings.xml** file and imports those values. The device name is set to **CyberData Autoprovisioned**, the SIP server is set to **10.0.0.253**, and the port is set to **5060**.

XML Files

XML files can contain <AutoprovFile> elements. If multiple DHCP options are specified, the device will try to download autoprovisioning files from each in turn. The device will only look for <AutoprovFile> elements in the first file downloaded from each server. You can specify up to 20 <AutoprovFile> elements in the first autoprovisioning file.

There are numerous ways to change an element of the **configuration(xml)** file. Using **sip ext** as an example, the extension can be changed:

Within the device-specific xml, i.e. **[macaddress].xml**, via the AutoprovFile element:<SIPSettings>/<SIPExt>

From the device specific xml, a pointer to a sip_common file

From the device specific xml, a pointer to the device specific sip_[macaddress].xml

From the common file, a pointer to sip_common.xml

From the common file, a pointer to the device specific (sip_[macaddress].xml)

Autoprovisioned Audio Files

Audio files are stored in non-volatile memory and an autoprovisioned audio file will only have to be downloaded once for each device. Loading many audio files to the device from the web page could cause it to appear unresponsive. If this happens, wait until the transfer is complete and then refresh the page.

The device uses the file name to determine when to download a new audio file. This means that if you used autoprovisioning to upload a file and then changed the contents of this file at the TFTP server, the device will not recognize that the file has changed (because the file name is the same).

Since audio files are stored in non-volatile memory, if autoprovisioning is disabled after they have been loaded to the board, the audio file settings will not change. You can force a change to the audio files on the board by clicking **Restore Default** on the **Audio Configuration** page or by changing the autoprovisioning file with “**default**” set as the file name.

2.6.15.2 Sample dhcpd.conf

```
#
# Sample configuration file for ISC dhcpd for Debian
#

ddns-update-style none;

option domain-name "voiplab";
option domain-name-servers 10.0.0.252;
option option-150 code 150 = ip-address;
option ntp-servers north-america.pool.ntp.org;
option space VendorInfo;
option VendorInfo.text code 10 = { text };
authoritative;
log-facility local7;

subnet 10.0.0.0 netmask 255.0.0.0 {
    max-lease-time 3600;
    default-lease-time 3600;

    option routers                  10.0.0.1;
    option subnet-mask              255.0.0.0;

    option domain-name              "voiplab";
    option domain-name-servers      10.0.0.252;

    option time-offset              -8;             # Pacific Standard Time

#     option www-server               99.99.99.99;                    # OPTION 72

#     option tftp-server-name          "10.0.1.52";                   # OPTION 66
#     option tftp-server-name          "http://test.cyberdata.net";   # OPTION 66

#     option option-150                10.0.0.252;                    # OPTION 150

# These two lines are needed for option 43
#     vendor-option-space VendorInfo;                                 # OPTION 43
#     option VendorInfo.text "http://test.cyberdata.net";             # OPTION 43

    range 10.10.0.1 10.10.2.1; }
```

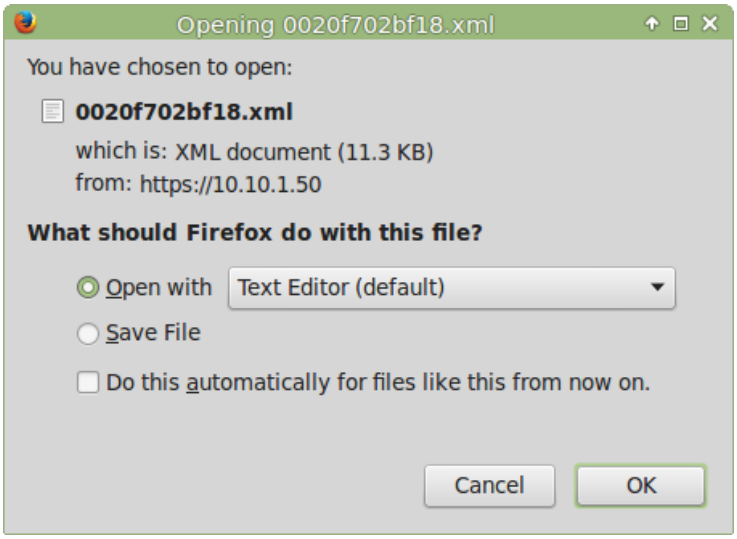
2.6.15.3 Download Template Button

The **Download Template** button allows the user to generate, download, edit, and then store an autoprovisioning template on the server that serves the autoprovisioning files for devices.

To generate an autoprovisioning template directly from the device, complete the following steps:

1. On the **Autoprovisioning** page, click on the **Download Template** button.
2. You will see a window prompting you to save a configuration file (**.xml**) to a location on your computer (Figure 2-39). The configuration file is the basis for the default configuration settings for your unit).
3. Choose a location to save the configuration file and click on **OK**. See Figure 2-39.

Figure 2-39. Configuration File



4. At this point, you can open and edit the autoprovisioning template to change the configuration settings in the template for the unit.
5. You can then upload the autoprovisioning file to a TFTP or HTTP server where the file can be loaded onto other devices.

2.7 Upgrade the Firmware and Reboot the Intercom

Caution

Equipment Hazard: Devices with a serial number that begins with 3081xxxxx can only run firmware versions 10.0.0 or later.

2.7.1 Downloading the Firmware

To download the firmware to your computer:

1. Download the latest firmware file from the **Downloads** tab at the following webpage:

   http://www.cyberdata.net/voip/011308/

2. Unzip the firmware version file. This file may contain the following:

- Firmware file
- Release notes

3. Log in to the Intercom home page as instructed in Section 2.6.4, "Log in to the Configuration Home Page".

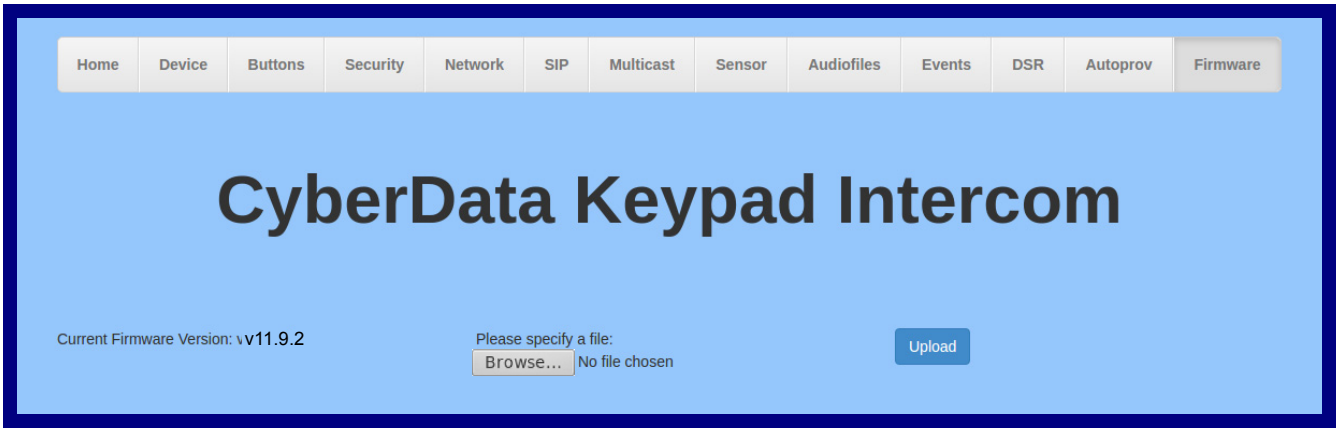
4. Click on the **Firmware** menu button to open the **Firmware** page. See Figure 2-40.

GENERAL ALERT

Caution

Equipment Hazard: CyberData strongly recommends that you first reboot the device before attempting to upgrade the firmware of the device. See Section 2.7.2, "Reboot the Device".

Figure 2-40. Firmware Page



5. Click on the **Browse** button, and then navigate to the location of the firmware file.
6. Select the firmware file.
7. Click on the **Upload** button.

Note Do not reboot the device after clicking on the **Upload** button.

Note This starts the upgrade process. Once the Intercom has uploaded the file, the **Uploading Firmware** countdown page appears, indicating that the firmware is being written to flash. The Intercom will automatically reboot when the upload is complete. When the countdown finishes, the **Firmware** page will refresh. The uploaded firmware filename should be displayed in the system configuration (indicating successful upload and reboot).

GENERAL ALERT

Caution

Equipment Hazard: Restore the factory defaults after upgrading the firmware. See Section 2.7.2, "Reboot the Device".

8. Table 2-27 shows the web page items on the **Firmware** page.

Table 2-27. Firmware Parameters

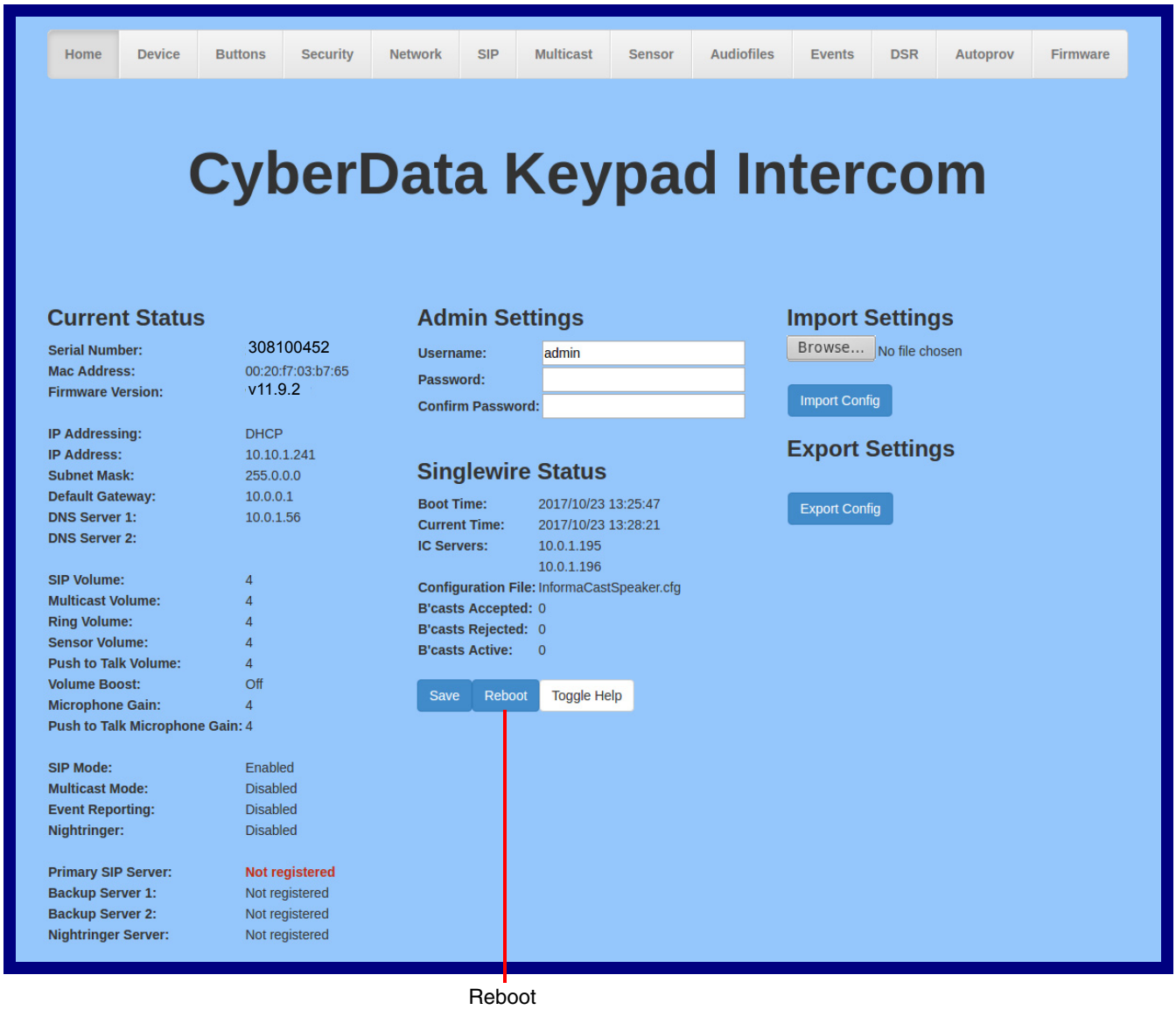
Web Page Item	Description
Current Firmware Version	Shows the current firmware version.
Browse...	Use the **Browse** button to navigate to the location of the Intercom firmware file that you want to upload.
Upload	Click on the **Upload** button to automatically upload the selected firmware and reboot the system.

2.7.2 Reboot the Device

To reboot a Intercom, log in to the web page as instructed in Section 2.6.4, "Log in to the Configuration Home Page".

1. Click on the **Reboot** button on the **Home** page (Figure 2-41). A normal restart will occur.

Figure 2-41. Home Page



2.8 Command Interface

Some functions on the device can be activated using simple POST commands to the web interface. The examples in Table 2-28 use the free unix utility, **wget commands**. However, any program that can send HTTP POST commands to the device should work.

2.8.1 Command Interface Post Commands

Note These commands require an authenticated session (a valid username and password to work).

Table 2-28. Command Interface Post Commands

Device Action	HTTP Post Command[a]
Trigger relay (for configured delay)	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/command.cgi" --post-data "test_relay=yes"
Place call to extension (example: extension 130)	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/command.cgi" --post-data "call=130"
Place point-to-point call[b] (example: IP phone address = 10.0.3.72)	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/command.cgi" --post-data "call=10.0.3.72"
Terminate active call	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/command.cgi" --post-data "terminate=yes"
Force reboot	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/command.cgi" --post-data "reboot=yes"
Test Audio button	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/command.cgi" --post-data "test_audio=yes"
Announce IP address	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/command.cgi" --post-data "speak_ip_address=yes"
Play the "0" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_0=yes"
Play the "1" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_1=yes"
Play the "2" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_2=yes"
Play the "3" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_3=yes"

Table 2-28. Command Interface Post Commands (continued)

Device Action	HTTP Post Command[a]
Play the "4" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_4=yes"
Play the "5" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_5=yes"
Play the "6" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_6=yes"
Play the "7" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_7=yes"
Play the "8" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_8=yes"
Play the "9" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_9=yes"
Play the "Dot" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_d=yes"
Play the "Audio Test" audio file (from Audio Config)	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_audiotest=yes"
Play the "Page Tone" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_pagetone=yes"
Play the "Your IP Address Is" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_youripaddressis=yes"
Play the "Rebooting" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_rebooting=yes"
Play the "Restoring Default" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_restoringdefault=yes"
Play the "Ringback tone" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_ringback=yes"
Play the "Ring tone" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_ringtone=yes"
Play the "Intrusion Sensor Triggered" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_intrusionsensortriggered=yes"
Play the "Door Ajar" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_doorajar=yes"

Table 2-28. Command Interface Post Commands (continued)

Device Action	HTTP Post Command[a]
Play the "Night Ring" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_nightring=yes"
Delete the "0" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_0=yes"
Delete the "1" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_1=yes"
Delete the "2" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_2=yes"
Delete the "3" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_3=yes"
Delete the "4" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_4=yes"
Delete the "5" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_5=yes"
Delete the "6" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_6=yes"
Delete the "7" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_7=yes"
Delete the "8" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_8=yes"
Delete the "9" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_9=yes"
Delete the "Audio Test" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_audiotest=yes"
Delete the "Page Tone" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_pagetone=yes"
Delete the "Your IP Address Is" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_youripaddressis=yes"
Delete the "Rebooting" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_rebooting=yes"
Delete the "Restoring Default" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_restoringdefault=yes"

Table 2-28. Command Interface Post Commands (continued)

Device Action	HTTP Post Command[a]
Delete the "Ringback tone" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_ringback=yes"
Delete the "Ring tone" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_ringtone=yes"
Delete the "Intrusion Sensor Triggered" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_intrusionsensortriggered=yes"
Delete the "Door Ajar" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_doorajar=yes"
Delete the "Night Ring" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_nightring=yes"
Trigger the Door Sensor Test (Sensor Config page)	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/sensor.cgi" --post-data "doortest=yes"
Trigger the Intrusion Sensor Test (Sensor Config page)	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/sensor.cgi" --post-data "intrusiontest=yes"

a.Type and enter all of each http POST command on one line.
b. Must be in point-to-point mode see Section 2.6.9.1, "Point-to-Point Configuration"

Appendix A: Mounting the Singlewire InformaCast Indoor Intercom with Keypad, Flush Mount

A.1 Mount the Intercom

Before you mount the Intercom, make sure that you have received all the parts for each Intercom. Refer to Table A-1.

Table A-1. Mounting Components (Part of the Accessory Kit)

Quantity	Part Name	Illustration
4	#6 X 3/8-inch,100 Deg., Flat Head, Self-Tapping Screw	
4	#6 X 3/8-inch,100 Deg., Flat Head T15 Security Pin Torx Screw	
1	T15 Security Pin Torx Key	

A.2 Dimensions

Figure A-1. Unit Dimensions

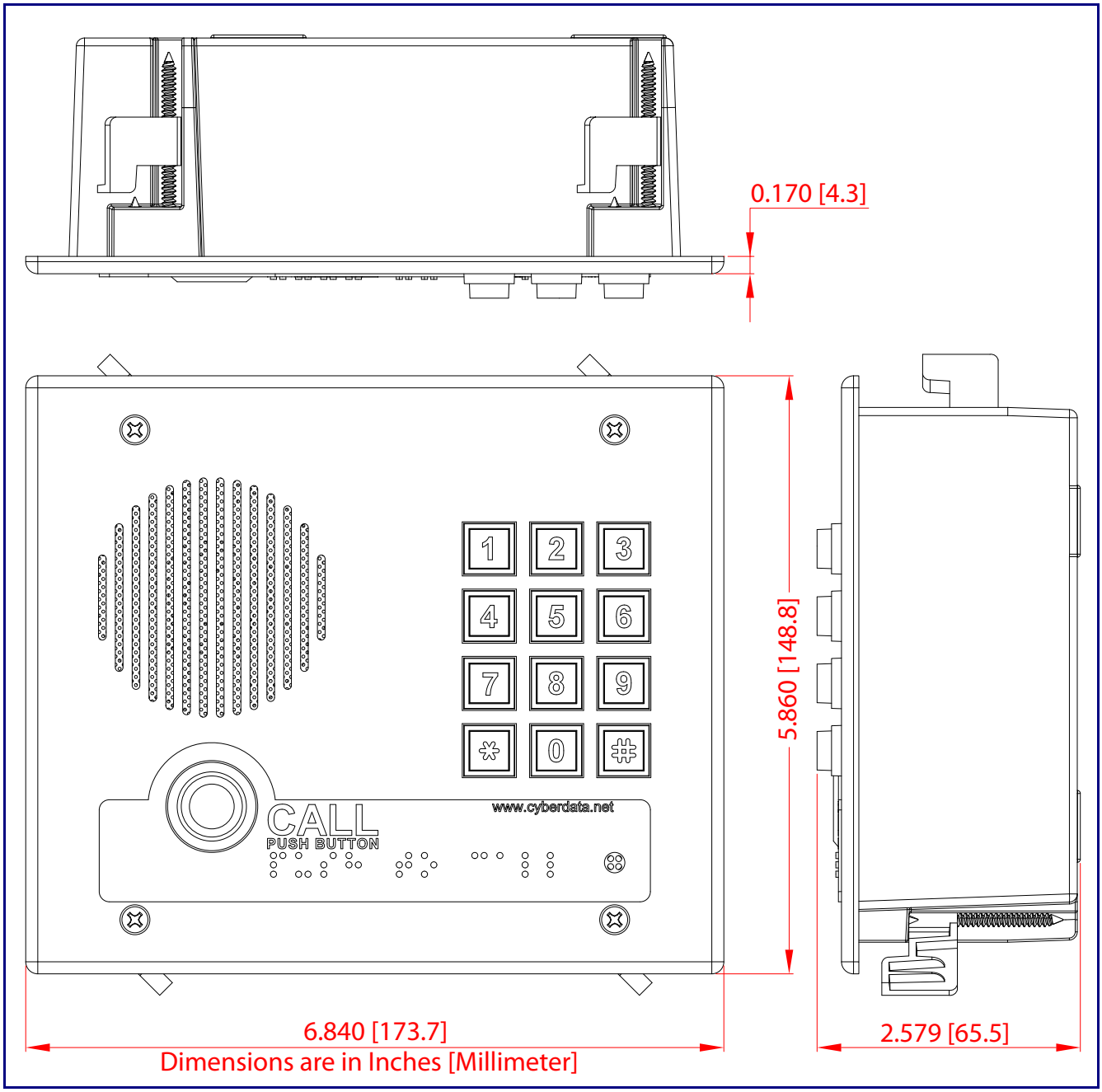
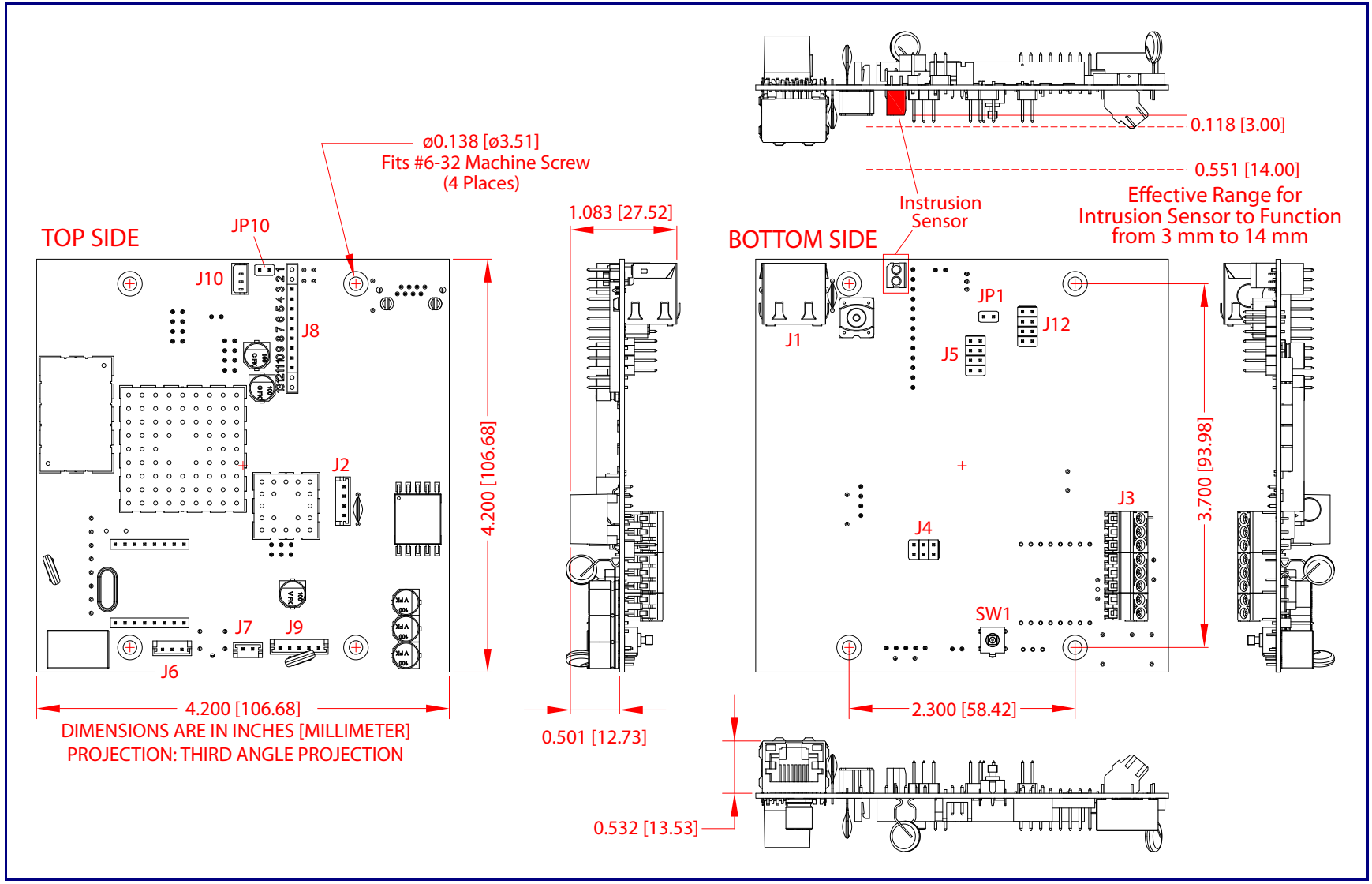


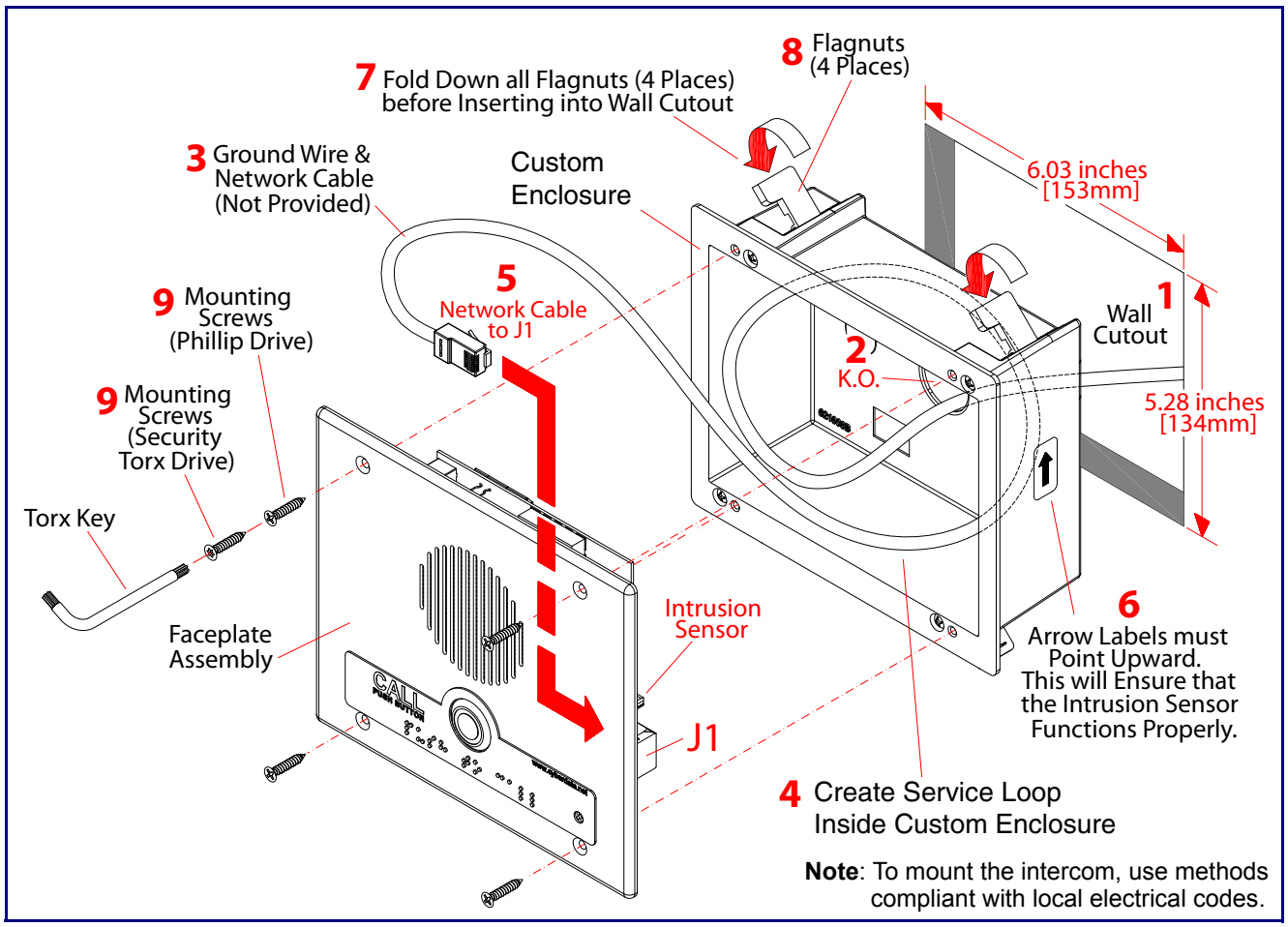
Figure A-2. PCB Dimensions and Intrusion Sensor Range



A.3 Wall Mounting

Figure A-3 illustrates a wall mounting option for the Singlewire InformaCast Indoor Intercom with Keypad, Flush Mount.

Figure A-3. Wall Mounting



To mount the Intercom:

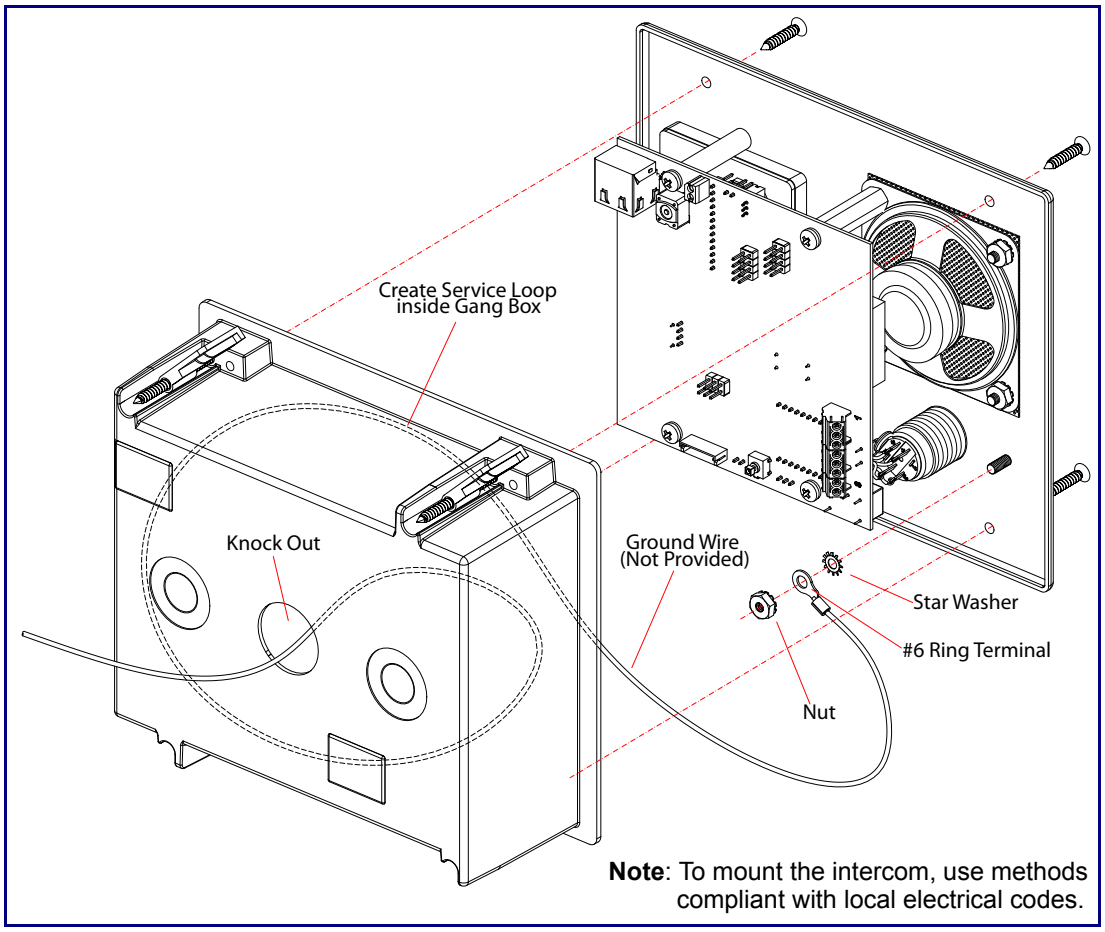
1. Make a wall cutout as shown in the picture.
2. Use a flat blade screwdriver to remove the knockout (KO) of the gang box.
3. Feed the ground wire (shown in Section A.4, "Ground Cable Installation") and the network cable from the wall cutout through the knockout hole of the gang box.
4. Create a service loop for both the ground wire and network cable.
5. Plug the network cable into the J1 connector.
6. Make sure that the arrow labels are pointing up. This will ensure that the intrusion sensor functions properly.

7. Fold down all of the flagnuts, and then insert the gang box into the wall cutout.
8. Tighten the flagnuts with a Phillips screwdriver.
9. Secure the Intercom faceplate assembly to the gang box with either Phillips screws or security Torx screws.

A.4 Ground Cable Installation

Figure A-4 illustrates how to connect a ground cable to the Singlewire InformaCast Indoor Intercom with Keypad, Flush Mount.

Figure A-4. Ground Cable Installation



Appendix B: Setting up a TFTP Server

B.1 Set up a TFTP Server

Autoprovisioning requires a TFTP server for hosting the configuration file.

B.1.1 In a LINUX Environment

To set up a TFTP server on LINUX:

1. Create a directory dedicated to the TFTP server, and move the files to be uploaded to that directory.
2. Run the following command where `/tftpboot/` is the path to the directory you created in Step 1: the directory that contains the files to be uploaded. For example:

   ```
   in.tftpd -l -s /tftpboot/your_directory_name
   ```

B.1.2 In a Windows Environment

You can find several options online for setting up a Windows TFTP server. This example explains how to use the Solarwinds freeware TFTP server, which you can download at:

http://www.cyberdata.net/assets/common/Solarwinds.zip

To set up a TFTP server on Windows:

1. Install and start the software.
2. Select **File**/**Configure**/**Security** tab/**Transmit Only**.
3. Make a note of the default directory name, and then move the firmware files to be uploaded to that directory.

Appendix C: Troubleshooting/Technical Support

C.1 Frequently Asked Questions (FAQ)

To see a list of frequently asked questions for your product, click on the **FAQs** tab at the following webpage:

http://www.cyberdata.net/voip/011308/

C.2 Documentation

The documentation for this product is released in an English language version only.

To download PDF copies of CyberData product documentation, click on the **Downloads** tab at the following webpage:

http://www.cyberdata.net/voip/011308/

C.3 Contact Information

Contact

CyberData Corporation
3 Justin Court
Monterey, CA 93940 USA
www.CyberData.net
Phone: 800-CYBERDATA (800-292-3732)
Fax: 831-373-4193

Sales

Sales 831-373-2601, Extension 334

Technical Support

The fastest way to get technical support for your VoIP product is to submit a VoIP Technical Support form at the following website:

http://support.cyberdata.net/

The Support Form initiates a ticket which CyberData uses for tracking customer requests. Most importantly, the Support Form tells us which PBX system and software version that you are using, the make and model of the switch, and other important information. This information is essential for troubleshooting. Please also include as much detail as possible in the **Comments** section of the Support Form.

Phone: (831) 373-2601, Extension 333

C.4 Warranty and RMA Information

The most recent warranty and RMA information is available at the following website address:

http://support.cyberdata.net/

Index

Numerics

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W