



VoIP Outdoor Intercom with Keypad Operations Guide

Part #011214

Document Part #930809T
for Firmware Version 11.6.2

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

PoE VoIP Intercom Operations Guide 930809T
Part # 011214

COPYRIGHT NOTICE:

© 2016, CyberData Corporation, ALL RIGHTS RESERVED.

This manual and related materials are the copyrighted property of CyberData Corporation. No part of this manual or related materials may be reproduced or transmitted, in any form or by any means (except for internal use by licensed customers), without prior express written permission of CyberData Corporation. This manual, and the products, software, firmware, and/or hardware described in this manual are the property of CyberData Corporation, provided under the terms of an agreement between CyberData Corporation and recipient of this manual, and their use is subject to that agreement and its terms.

DISCLAIMER: Except as expressly and specifically stated in a written agreement executed by CyberData Corporation, CyberData Corporation makes no representation or warranty, express or implied, including any warranty or merchantability or fitness for any purpose, with respect to this manual or the products, software, firmware, and/or hardware described herein, and CyberData Corporation assumes no liability for damages or claims resulting from any use of this manual or such products, software, firmware, and/or hardware. CyberData Corporation reserves the right to make changes, without notice, to this manual and to any such product, software, firmware, and/or hardware.

OPEN SOURCE STATEMENT: Certain software components included in CyberData products are subject to the GNU General Public License (GPL) and Lesser GNU General Public License (LGPL) “open source” or “free software” licenses. Some of this Open Source Software may be owned by third parties. Open Source Software is not subject to the terms and conditions of the CyberData COPYRIGHT NOTICE or software licenses. Your right to copy, modify, and distribute any Open Source Software is determined by the terms of the GPL, LGPL, or third party, according to who licenses that software.

Software or firmware developed by CyberData that is unrelated to Open Source Software is copyrighted by CyberData, subject to the terms of CyberData licenses, and may not be copied, modified, reverse-engineered, or otherwise altered without explicit written permission from CyberData Corporation.

TRADEMARK NOTICE: CyberData Corporation and the CyberData Corporation logos are trademarks of CyberData Corporation. Other product names, trademarks, and service marks may be the trademarks or registered trademarks of their respective owners.



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.

Pictorial Alert Icons

 <p>GENERAL ALERT</p>	<p>General Alert</p> <p><i>This pictorial alert indicates a potentially hazardous situation. This alert will be followed by a hazard level heading and more specific information about the hazard.</i></p>
	<p>Ground</p> <p><i>This pictorial alert indicates the Earth grounding connection point.</i></p>

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.
14. **WARNING: The VoIP Outdoor Intercom with Keypad enclosure is not rated for any AC voltages!**

 <p>GENERAL ALERT</p>	<p>Warning</p> <p><i>Electrical Hazard:</i> This product should be installed by a licensed electrician according to all local electrical and building codes.</p>
 <p>GENERAL ALERT</p>	<p>Warning</p> <p><i>Electrical Hazard:</i> To prevent injury, this apparatus must be securely attached to the floor/wall in accordance with the installation instructions.</p>
 <p>GENERAL ALERT</p>	<p>Warning</p> <p>The PoE connector is intended for intra-building connections only and does not route to the outside plant.</p>

Revision Information

Revision 930809T, which corresponds to firmware version 11.6.2, was released on November 15, 2016, and has the following changes:

- Updates [Figure 1-2](#), "Typical Installation"
- Updates [Figure 2-3](#), "Connections and Alternate Power Input"
- Updates [Figure 2-9](#), "Connector Locations"
- Updates [Figure 2-10](#), "Connector Locations"
- Updates [Figure 2-11](#), "Activity and Link LED"
- Updates [Figure 2-12](#), "RTFM Button"
- Updates [Figure 2-13](#), "RTFM Button"
- Updates [Figure 2-14](#), "RTFM Button"
- Adds [Section 2.3.1.1](#), "Remote Switch Connection"
- Adds [Section 2.3.3.2](#), "Connecting the Networked Dual Door Strike Intermediate Relay"
- Adds [Section 2.3.3.3](#), "Connecting the Networked Dual Door Strike Intermediate Relay—12V Out"
- Updates [Figure 2-18](#), "Home Page"
- Updates [Figure 2-19](#), "Device Configuration Page"
- Updates [Figure 2-21](#), "Button Configuration Page"
- Updates [Figure 2-23](#), "SIP Configuration Page"
- Updates [Figure 2-24](#), "SIP Page Set to Point-to-Point Mode"
- Updates [Figure 2-25](#), "Multicast Configuration Page"
- Updates [Figure 2-33](#), "DSR Page"
- Updates [Figure 2-34](#), "Relay Status Section"
- Updates [Figure 2-35](#), "Configure Device Page"
- Updates [Figure 2-38](#), "Firmware Page"
- Updates [Figure 2-39](#), "Home Page"
- Updates [Table 2-7](#), "Home Page Overview"
- Updates [Table 2-8](#), "Device Configuration Parameters"
- Updates [Table 2-13](#), "Button Configuration Parameters"
- Updates [Table 2-17](#), "SIP Configuration Parameters"
- Updates [Table 2-18](#), "Multicast Configuration Parameters"
- Updates [Table 2-22](#), "DSR Configuration Parameters"
- Updates [Table 2-23](#), "DSR Page Configure Device Parameters"

Browsers Supported

The following browsers have been tested against firmware version 11.6.2:

- Internet Explorer (version: 10)
- Firefox (also called Mozilla Firefox) (version: 23.0.1 and 25.0)
- Chrome (version: 29.0.1547.66 m)
- Safari (version: 5.1.7)

Chapter 1 Product Overview	1
1.1 How to Identify This Product	1
1.2 Typical System Installation	2
1.3 Product Features	3
1.4 Supported Protocols	4
1.5 Supported SIP Servers	4
1.6 Specifications	5
2.1 Parts List	6
Chapter 2 Installing the VoIP Outdoor Intercom with Keypad	6
2.2 Intercom Components	7
2.2.1 Call Button and Indicator Light	8
2.2.2 Dialing from the Keypad	8
2.3 Intercom Setup	9
2.3.1 Intercom Connections	9
2.3.2 Using the On-Board Relay	11
2.3.3 Wiring the Circuit	12
2.3.4 Intercom Connectors	16
2.3.5 Activity and Link LEDs	18
2.3.6 RTFM Button	19
2.3.7 Adjust the Volume	21
2.4 Configure the Intercom Parameters	22
2.4.1 Factory Default Settings	22
2.4.2 Intercom Web Page Navigation	23
2.4.3 Using the Toggle Help Button	24
2.4.4 Log in to the Configuration Home Page	26
2.4.5 Configure the Device	30
2.4.6 Configure the Button Parameters	38
2.4.7 Configure the Network Parameters	42
2.4.8 Configure the SIP Parameters	45
2.4.9 Configure the Multicast Parameters	51
2.4.10 Configure the Sensor Configuration Parameters	54
2.4.11 Configure the Audio Configuration Parameters	58
2.4.12 Configure the Events Parameters	64
2.4.13 Configure the Door Strike Relay	70
2.4.14 Configure the Device (on the DSR page)	74
2.4.15 Configure the Autoprovisioning Parameters	78
2.5 Upgrade the Firmware and Reboot the Intercom	89
2.5.1 Downloading the Firmware	89
2.5.2 Reboot the Device	91
2.6 Command Interface	92
2.6.1 Command Interface Post Commands	92
Appendix A Mounting the VoIP Outdoor Intercom with Keypad	96
A.1 Mount the Intercom	96
A.2 Dimensions	97
A.3 Overview of Installation Types	100
A.4 Network Cable Entry Restrictions	101
A.4.1 Rear Conduit Network Cable Entry Restrictions (without Shroud)	101
A.4.2 Rear Conduit Network Cable Entry Restrictions (with Shroud)	101
A.5 Service Loop Cable Routing	102
A.6 Securing the Intercom	103
A.7 Additional Mounting Options	104
A.7.1 Rear Conduit Mounting Option (Not Provided)	104
A.7.2 Concrete Wall Mounting Option (Not Provided)	105
A.7.3 Goose Neck Mounting Option (Not Provided)	106

Appendix B Setting up a TFTP Server	107
B.1 Set up a TFTP Server	107
B.1.1 In a LINUX Environment	107
B.1.2 In a Windows Environment	107
Appendix C Troubleshooting/Technical Support	108
C.1 Frequently Asked Questions (FAQ)	108
C.2 Documentation	108
C.3 Contact Information	109
C.4 Warranty and RMA Information	109
Index	110

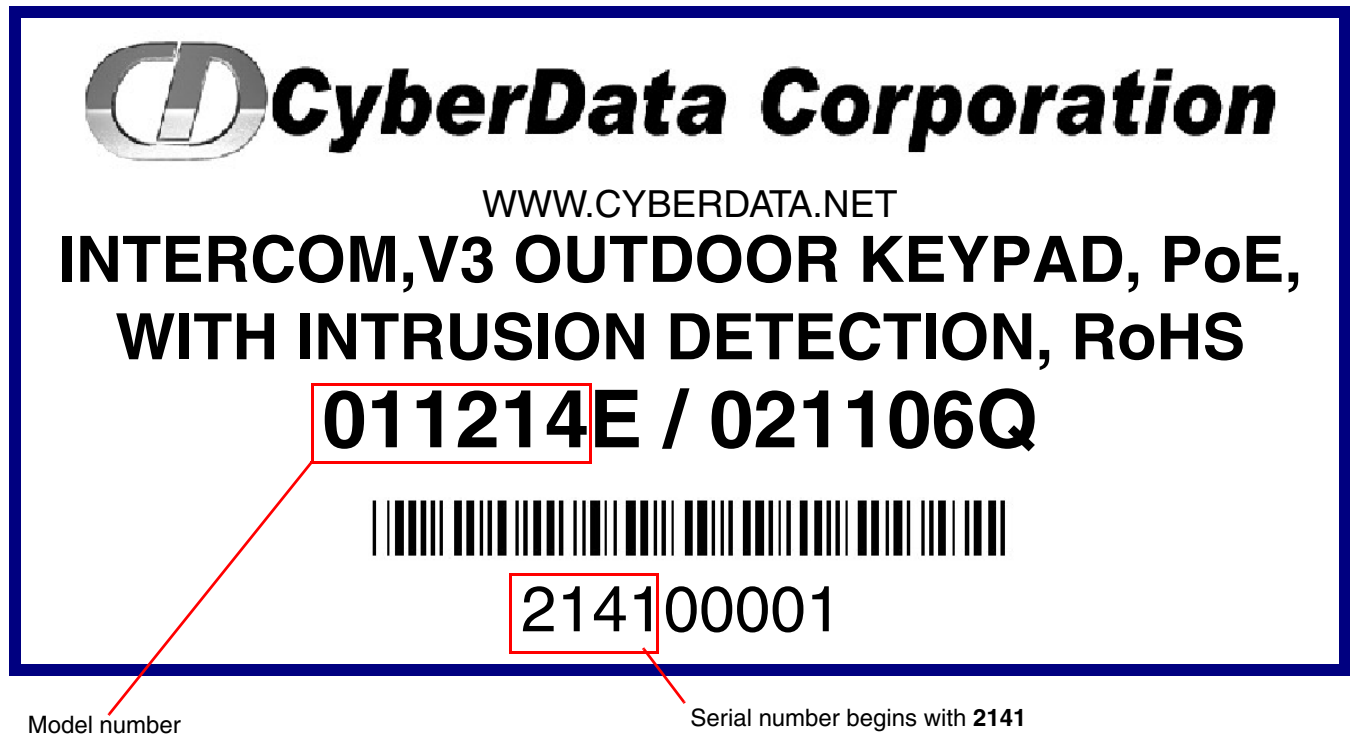
1 Product Overview

1.1 How to Identify This Product

To identify the VoIP Outdoor Intercom with Keypad, 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 **011214**.
- The serial number on the label should begin with **2141**.

Figure 1-1. Model Number Label



1.2 Typical System Installation

The Voice-over-IP (VoIP) Intercom is a Power-over-Ethernet (PoE 802.3af) and Voice-over-IP (VoIP) two-way communications device that easily connects into existing local area networks (LANs) with a single cable connection. The intercom is compatible with most SIP-based IP PBX servers that comply with SIP RFC 3261.

The following figures illustrate how the VoIP Outdoor Intercom with Keypad can be installed as part of a VoIP phone system.

Figure 1-2. Typical Installation

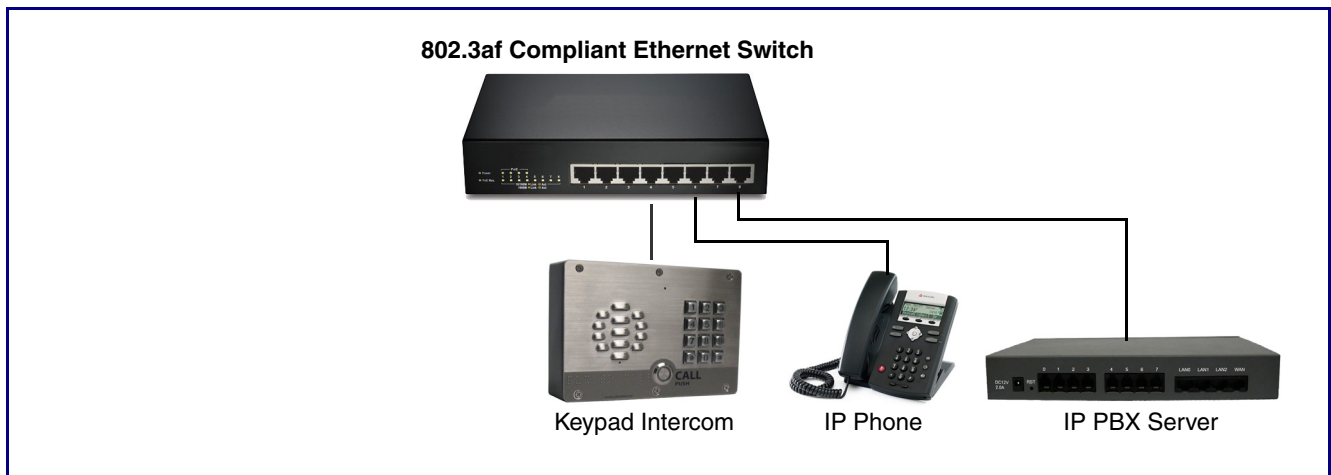
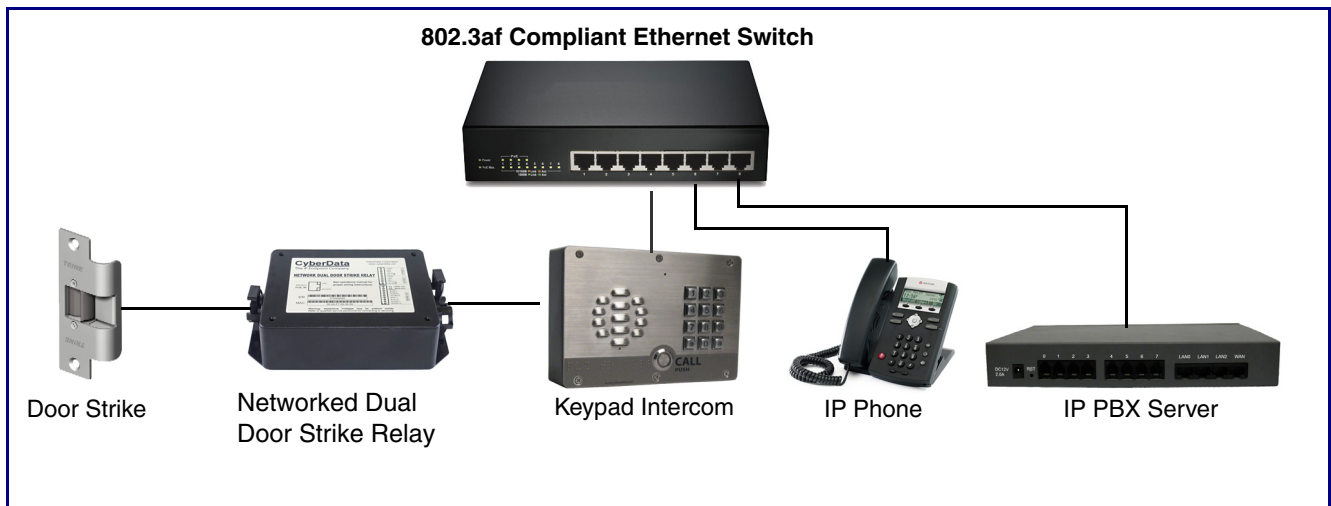


Figure 1-3. Installation with Networked Dual Door Strike Relay



1.3 Product Features

The VoIP Outdoor Intercom with Keypad has the following features:

- 12-key keypad with backlight
- Programmable speed dial
- Optional Weather Shroud for even greater weather protection
- Supports SRST (Survivable Remote Site Telephony) in a Cisco environment. SRST parameters are entered statically into the CyberData product's internal webpage.
- SIP
- Dual speeds of 10 Mbps and 100 Mbps
- 802.3af compliant
- 2 gang outlet box size
- Adaptive full duplex voice operation
- Network/Web management
- Network adjustable speaker volume adjustment
- Network configurable door or intrusion sensor settings
- Network configurable relay activation settings
- Dial Out Extension supports the addition of comma delimited pauses before sending additional DTMF tones
- Network configurable microphone input sensitivity adjustment
- Network downloadable product firmware
- Doubles as a paging speaker
- Call button
- Call activity indicator (light)
- Tamper proof design
- One dry contact relay for auxiliary control
- Autoprovisioning
- Configurable audio files
- Night Ringer
- Peer-to-peer capable
- Door closure and tamper alert signal
- Optional Torx screws with driver kit
- An active call is indicated by the Call Button LED blinking at one second intervals.

1.4 Supported Protocols

The Intercom supports:

- SIP
- 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
- RTP/AVP - Audio Video Profile
- Audio Encodings
 - PCMU (G.711 mu-law)
 - PCMA (G.711 A-law)
 - 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
Power Input	PoE 802.3af compliant or +8 to +12VDC @ 1000mA Regulated Power Supply ^a
Speaker Output	1 Watt Peak Power
On-Board Relay	1A at 30 VDC
Operating Temperature	-10° C to 50° C [14° F to 122° F]
Payload Types	G711, A-law and μ -law
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]
Part Number	011214 011215 Weather Shroud (sold separately)

a. Contacts 1 and 2 on the J3 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.

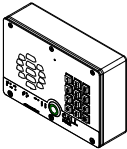


2 Installing the VoIP Outdoor Intercom with Keypad

2.1 Parts List

Table 2-2 illustrates the parts for the VoIP Outdoor Intercom with Keypad.

Note See Appendix A, "Mounting the VoIP Outdoor Intercom with Keypad" for physical mounting information.

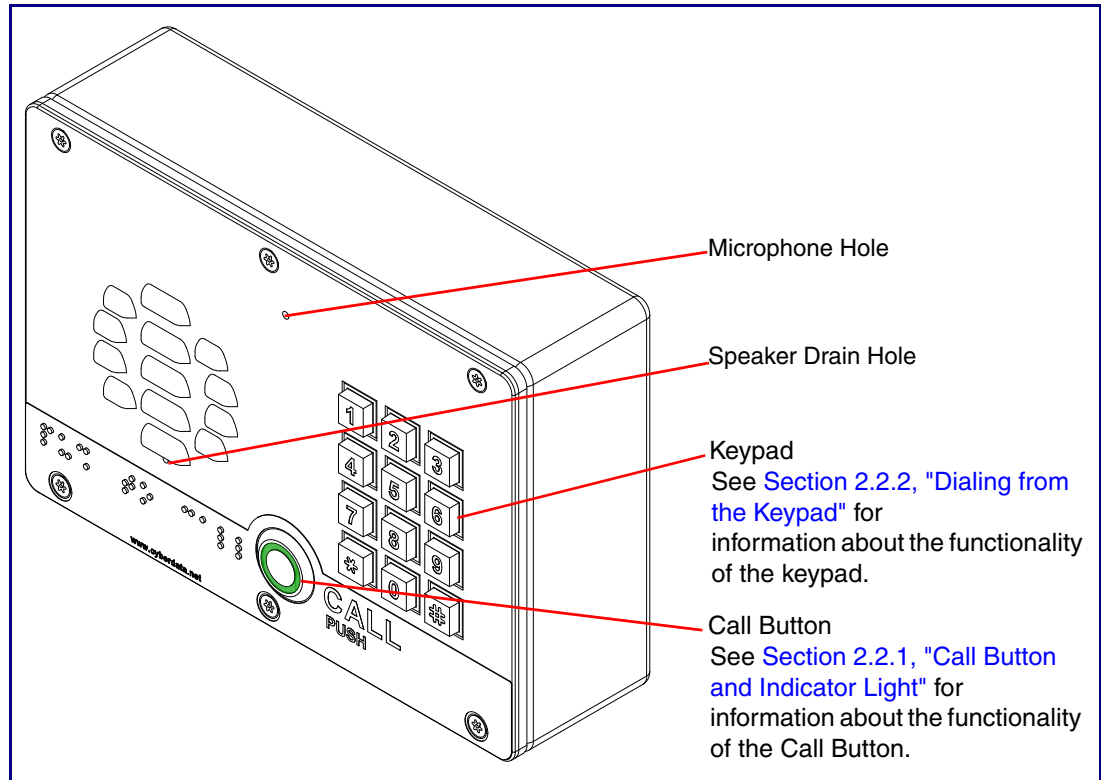
Table 2-2. Parts List

Quantity	Part Name	Illustration
1	VoIP Outdoor Intercom with Keypad 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

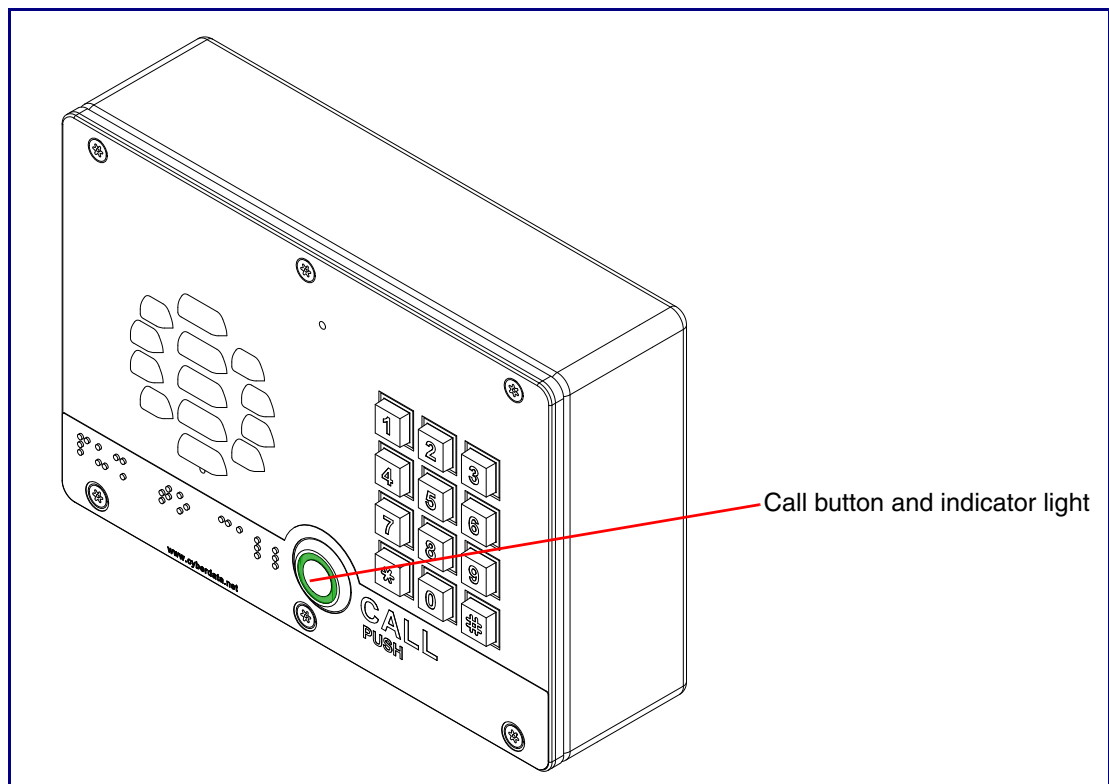


2.2.1 Call Button and Indicator Light

2.2.1.1 Indicator Light 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.
- 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 indicator light. The indicator light will still blink during initialization and calls.
- The indicator light flashes briefly at the beginning of RTFM mode.

Figure 2-2. Call Button and Indicator Light



2.2.2 Dialing from the Keypad

- See the [Enable Telephone Operation](#) setting in [Section 2.4.6, "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.


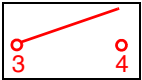
 <small>GENERAL ALERT</small>	<p>Caution</p> <p><i>Equipment Hazard:</i> Contacts 1 and 2 on the terminal block are only for powering the device from a non-PoE 12 VDC power source as an alternative to Network PoE power. Use of these contacts for any other purpose will damage the device and void the product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

Figure 2-3. Connections and Alternate Power Input

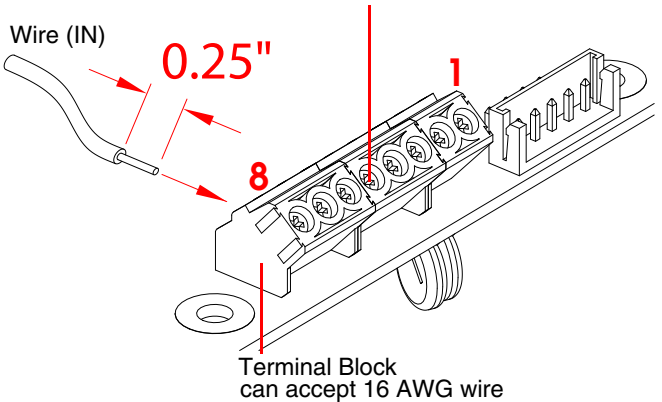
Alternate Power Input:
 1 = +8 to +12VDC @ 1000mA Regulated Power Supply*
 2 = Power Ground*



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.

Use a 3.17 mm (1/8-inch) flat blade screwdriver for the terminal block screws

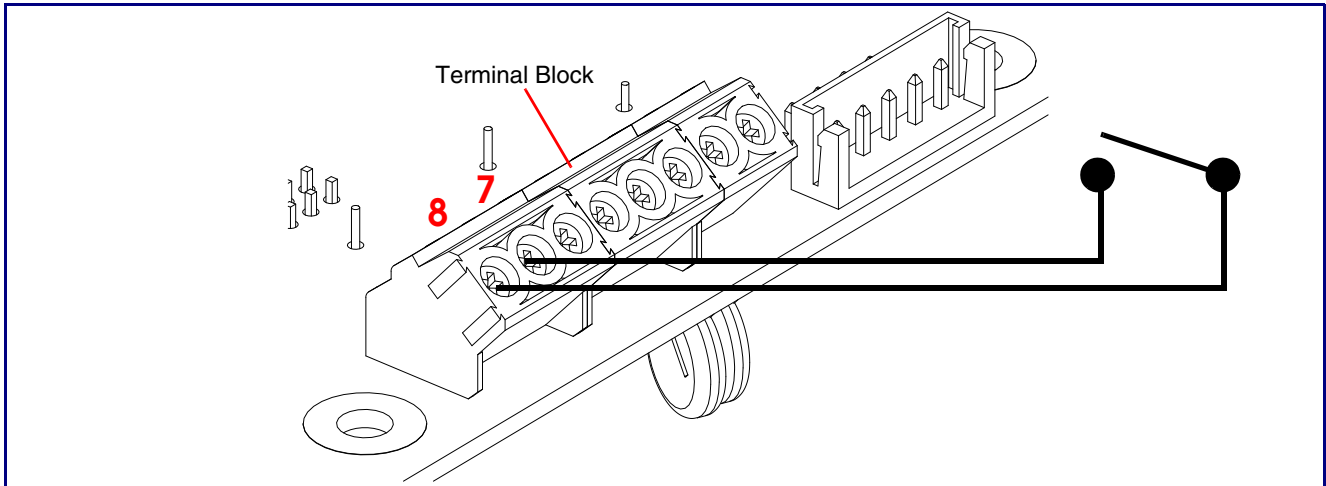


Terminal Block can accept 16 AWG wire




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

 GENERAL ALERT	Warning <i>Electrical Hazard:</i> This product should be installed by a licensed electrician according to all local electrical and building codes.
 GENERAL ALERT	Warning <i>Electrical Hazard:</i> 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.
 GENERAL ALERT	Warning <i>Electrical Hazard:</i> 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, "Connecting the Networked Dual Door Strike Intermediate Relay"](#)).

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.

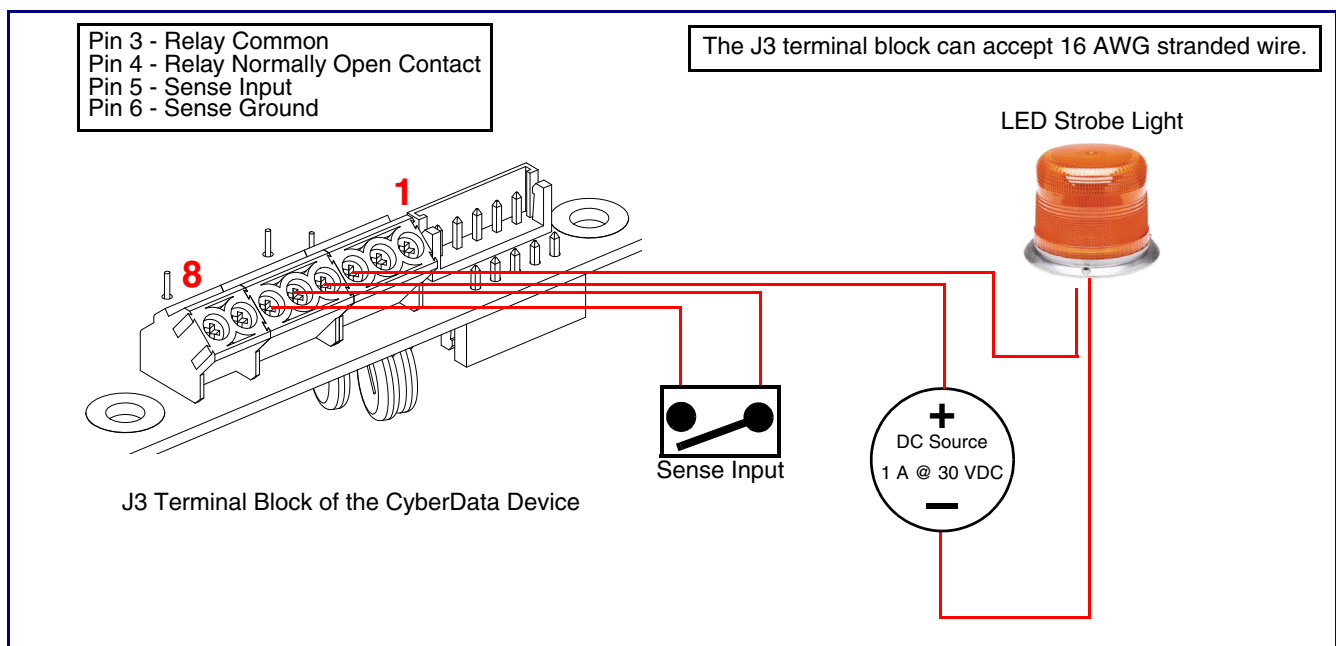
2.3.3 Wiring the Circuit

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 Networked Dual Door Strike Intermediate Relay Module (CD# 011375) (see [Section 2.3.3.2, "Connecting the Networked Dual Door Strike Intermediate Relay"](#)).

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



2.3.3.2 Connecting the Networked Dual Door Strike Intermediate Relay

For wiring an electronic door strike to work over a network, we recommend the use of our external Networked Dual Door Strike Intermediate 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 12V Out) for the wiring diagrams.


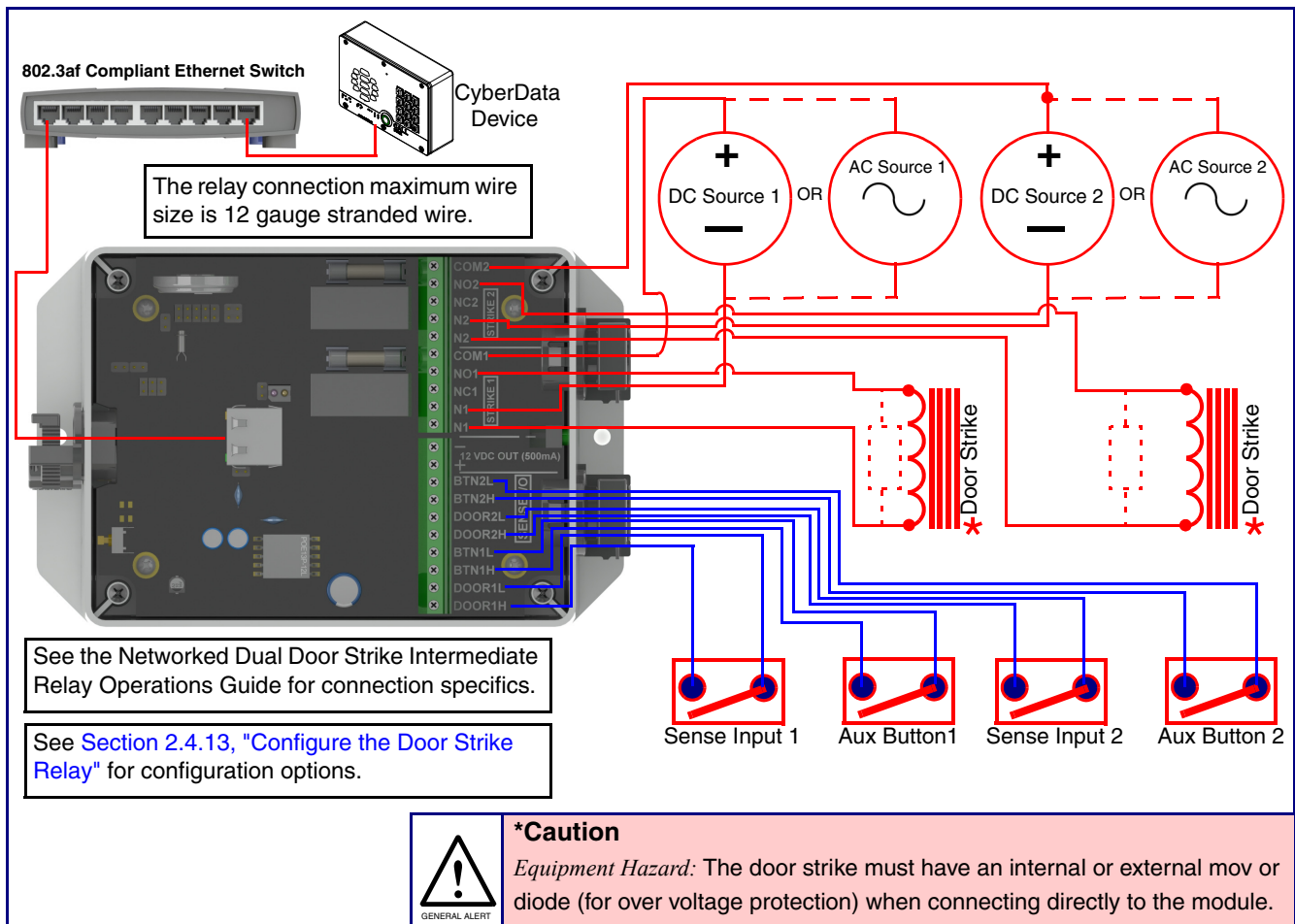
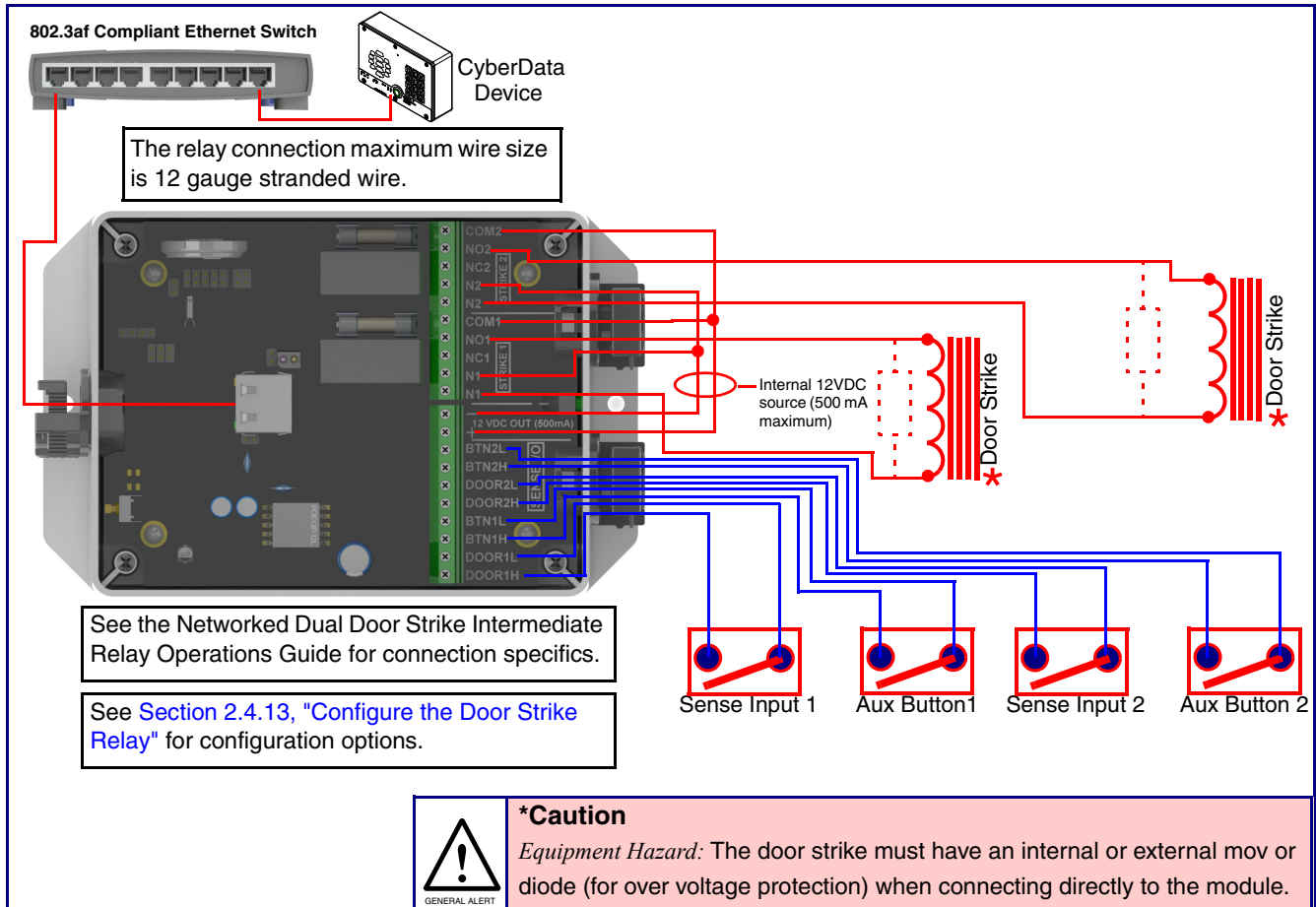
 GENERAL ALERT	<p>Warning</p> <p><i>Electrical Hazard:</i> Hazardous voltages may be present. No user serviceable part inside. Refer to qualified service personnel for connecting or servicing.</p>
--	--

Figure 2-6. Networked Dual Door Strike Intermediate Relay Wiring Diagram



2.3.3.3 Connecting the Networked Dual Door Strike Intermediate Relay—12V Out

Figure 2-7. Networked Dual Door Strike Intermediate Relay Wiring Diagram—12V Out



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

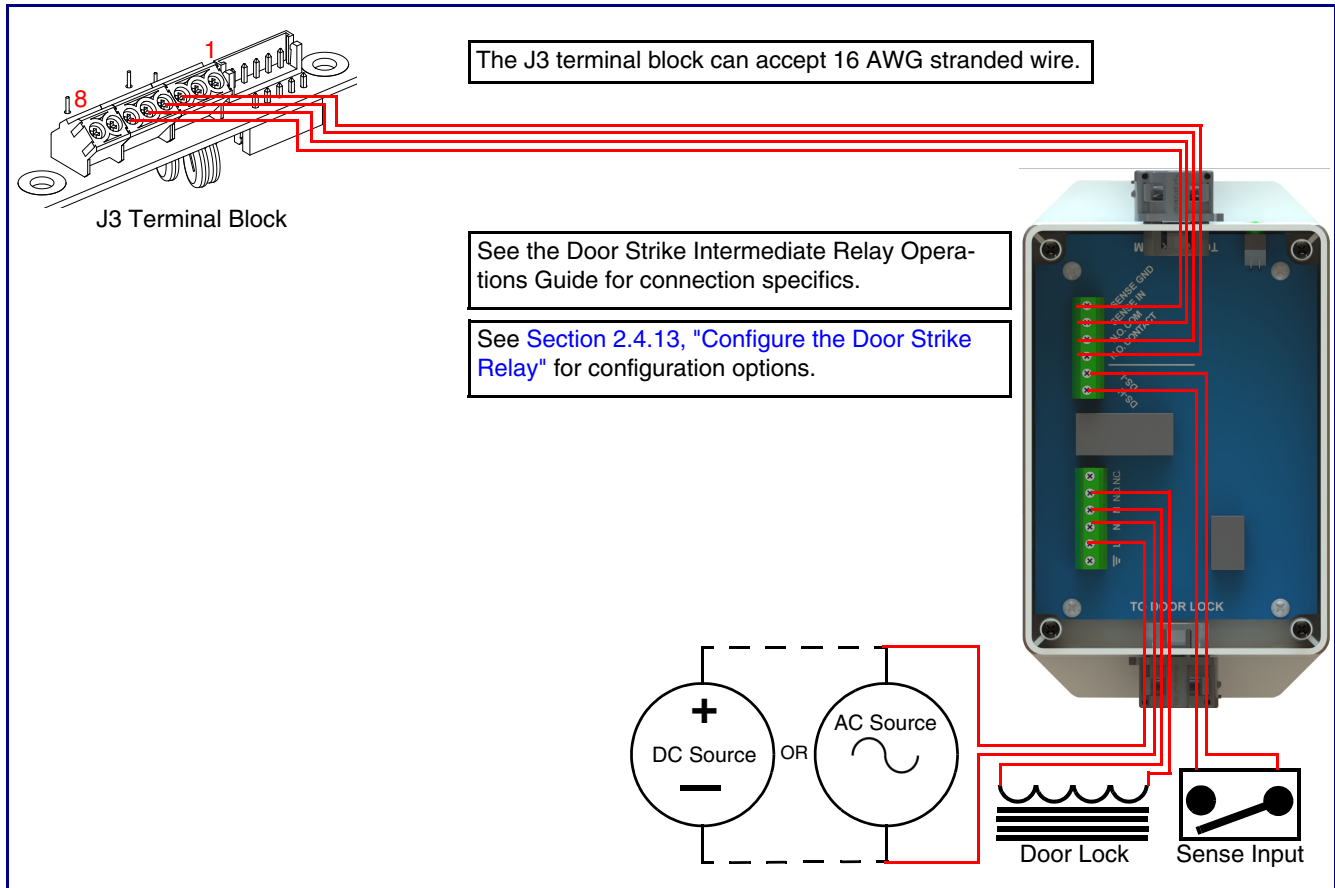
<http://support.cyberdata.net/>

2.3.3.4 Connecting the Door Strike Intermediate Relay Module

For wiring an electronic door strike, we recommend the use of our external Door Strike Intermediate Relay (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 Intermediate Relay Wiring Diagram



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/>

2.3.4 Intercom Connectors

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

Figure 2-9. Connector Locations

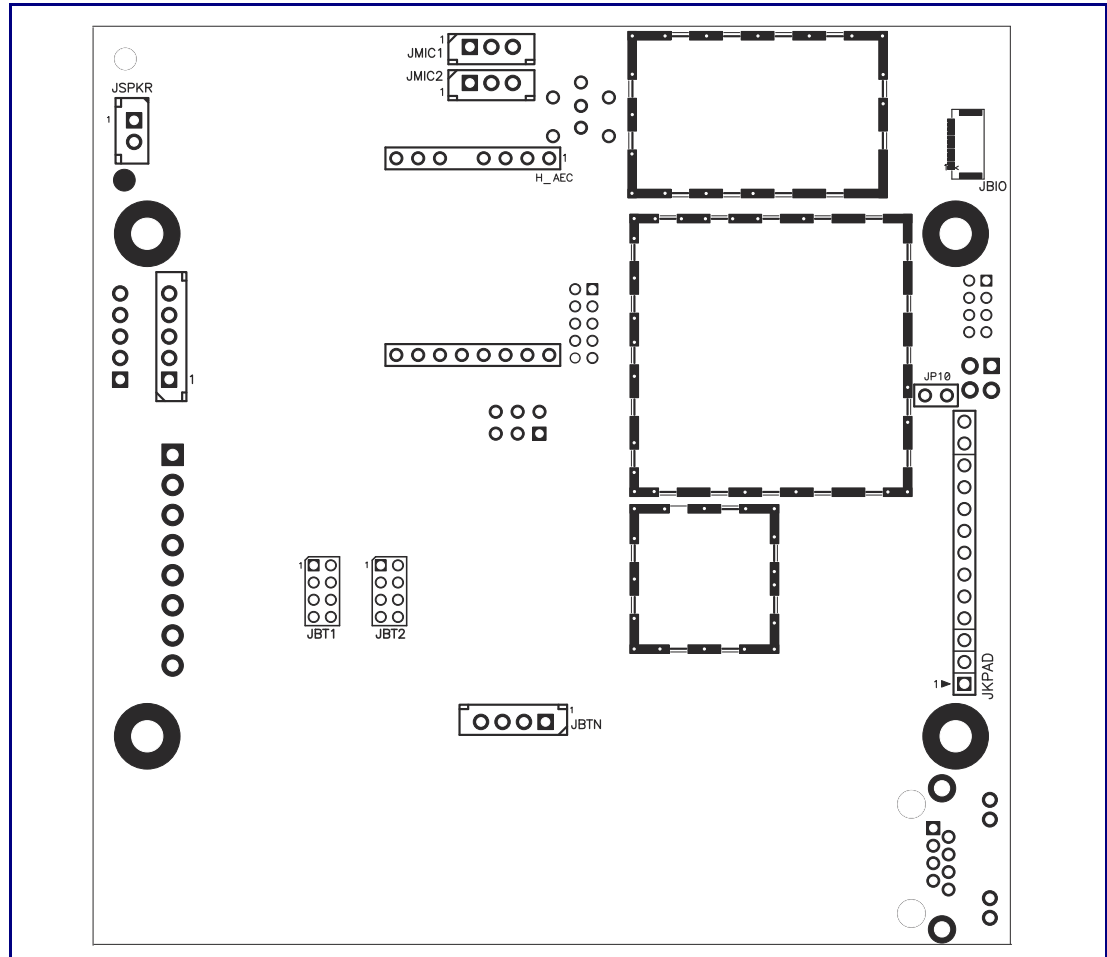


Table 2-3. Connector Functions

Connector	Function
JBTN	Call Button LED Interface
JMIC1	Microphone Interface
JSPKR	Speaker Interface
JKPAD	Keypad Interface — Not Used
JX	Auxiliary Strobe Connector
JY	Proximity Sensor Interface — Not Used
JP10	Disables the intrusion sensor when installed.
JBT1	Touch Button -1 Interface — Not Used
JBT2	Touch Button -2 Interface — Not Used

Figure 2-10. Connector Locations

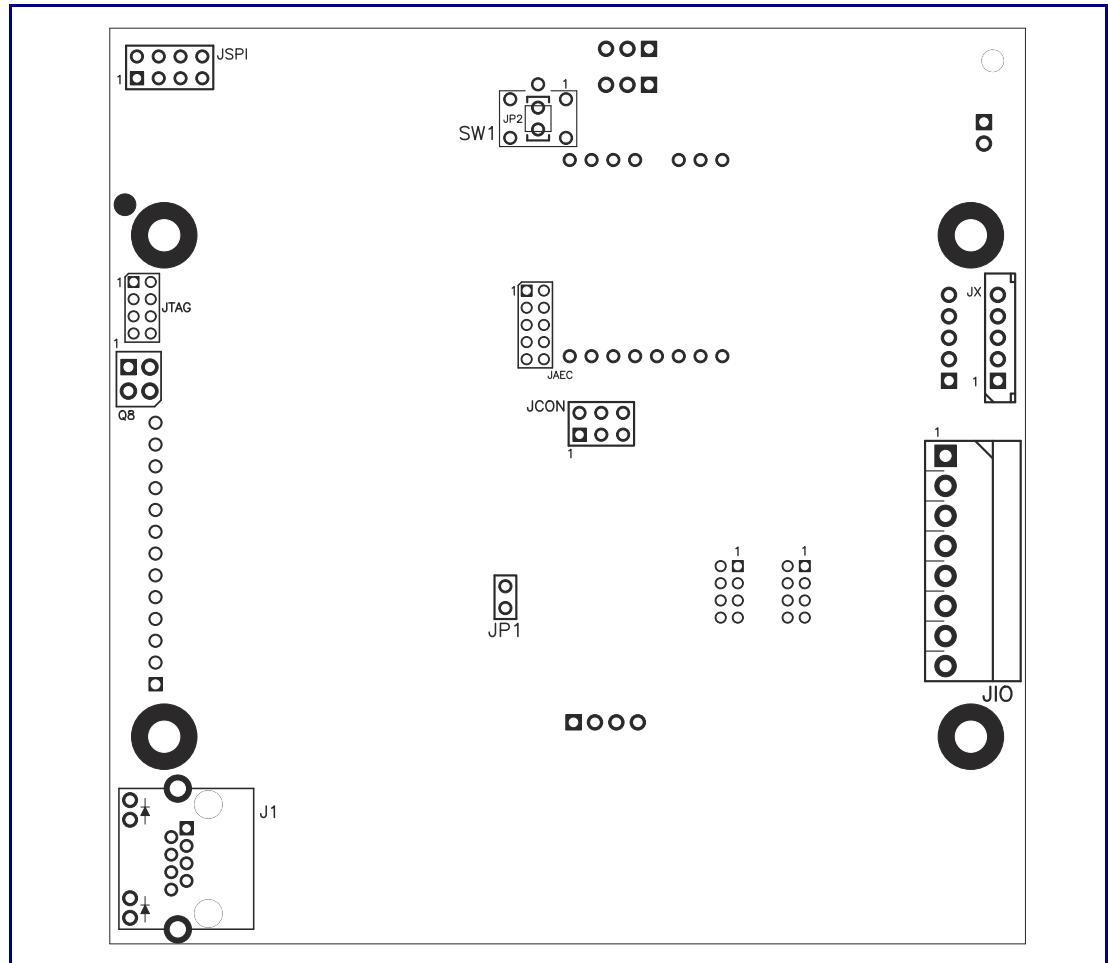


Table 2-4. Connector Functions

Connector	Function
JP1	Reset jumper ^a
J1	PoE Network Connection (RJ-45 ethernet)
JAE	AEC Configuration Interface (Factory Use Only)
JIO	Terminal Block (see Figure 2-3)
JCON	Console Port (Factory Use Only)
JTAG	JTAG (Factory Use Only)
JSPI	Reserved (Factory Use Only)
SW1	See Section 2.3.6, "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.

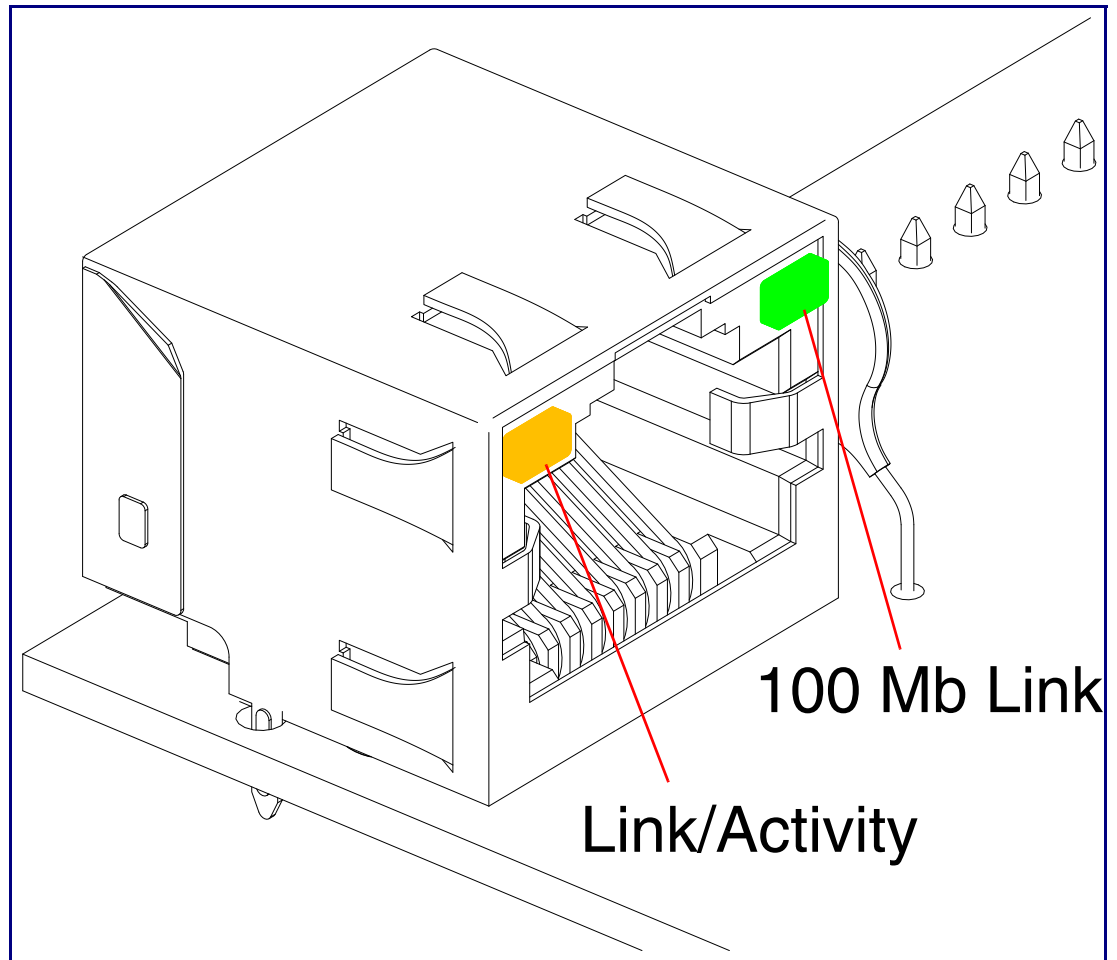
2.3.5 Activity and Link LEDs

2.3.5.1 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, **YELLOW Link/Activity** LED blinks when there is network activity (see [Figure 2-11](#)).
- The square, **GREEN 100Mb Link** LED above the Ethernet port indicates that the network connection has been established (see [Figure 2-11](#)).

Figure 2-11. Activity and Link LED

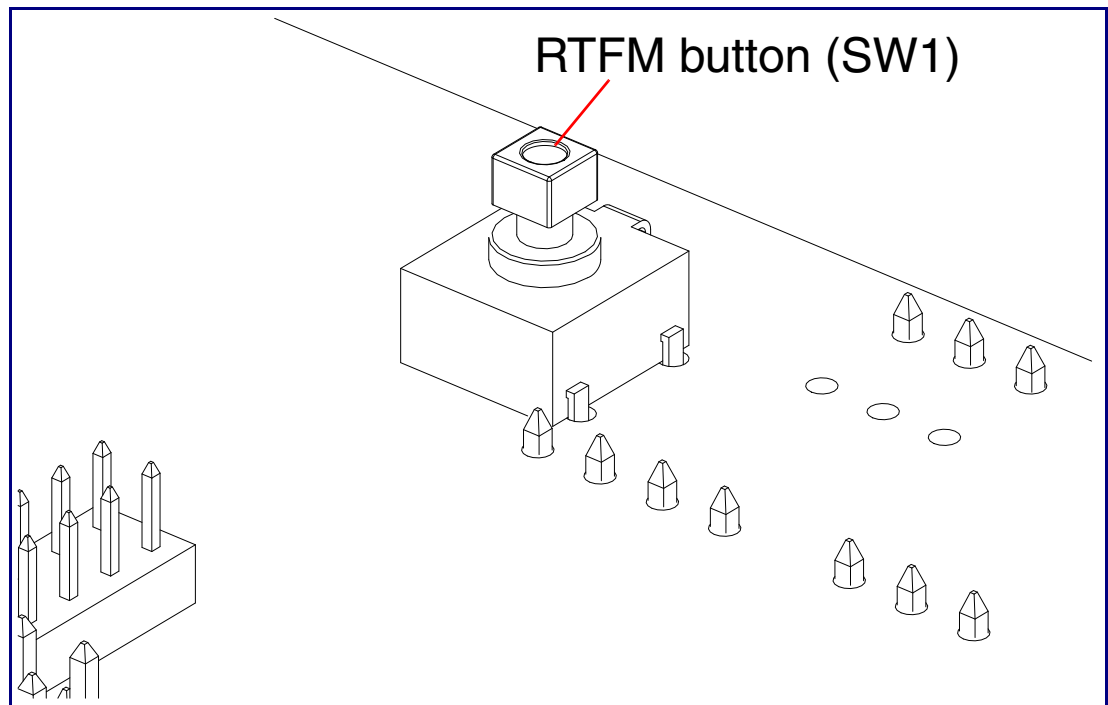


2.3.6 RTFM Button

When the Intercom is operational and linked to the network, you can use the Reset Test Function Management (**RTFM**) button (see **SW1** in [Figure 2-12](#)) 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 2-12. RTFM Button



2.3.6.1 Announcing the IP Address

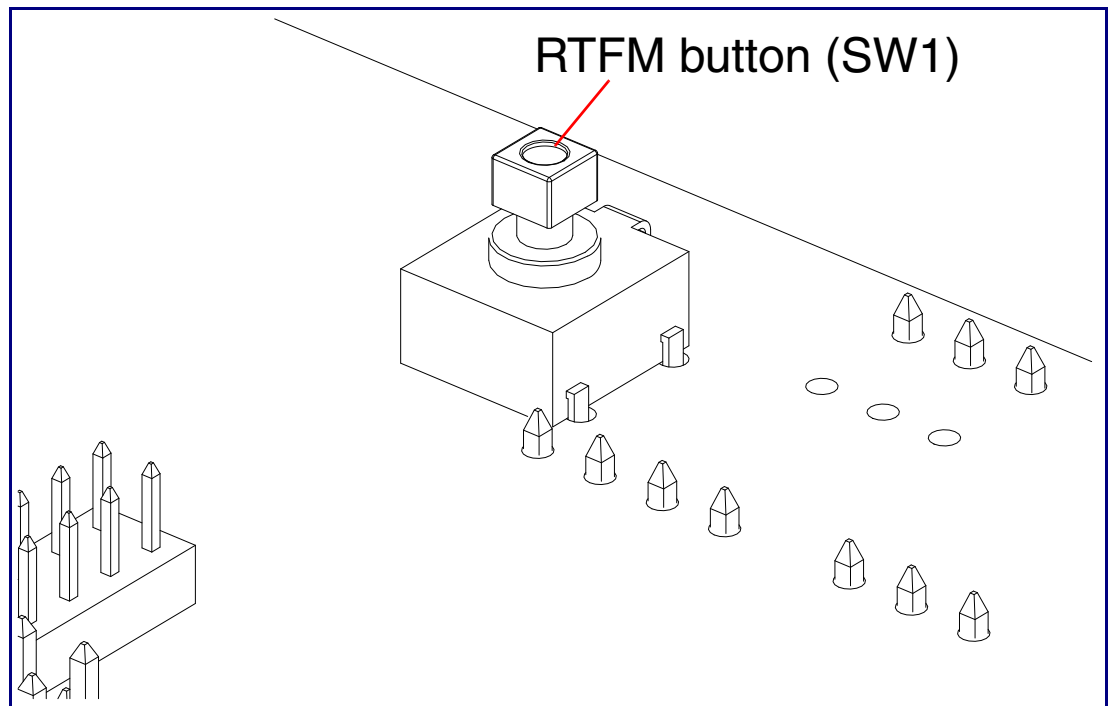
To announce a device's current IP address:

1. Press and release the RTFM button (see **SW1** in [Figure 2-13](#)) 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 2-13. RTFM Button



2.3.6.2 Restoring the Factory Default Settings

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

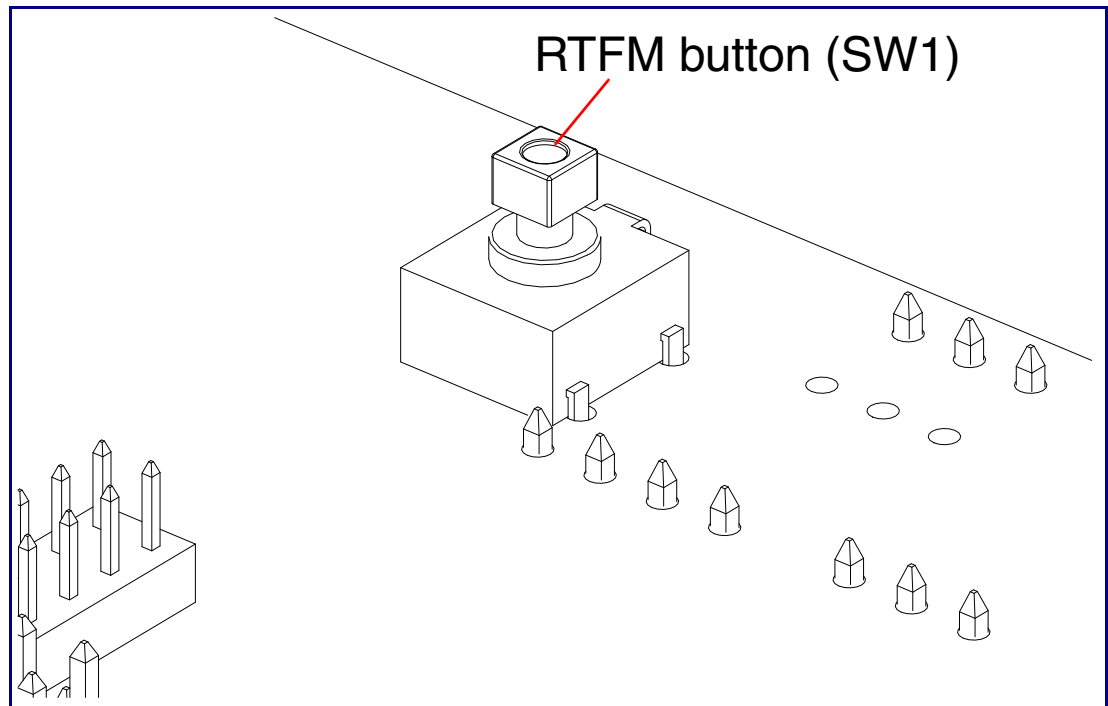
Note Each Intercom is delivered with factory set default values.

To restore the factory default settings:

1. Press and hold the **RTFM button** (see **SW1** in [Figure 2-14](#)) 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 2-14. RTFM Button



2.3.7 Adjust the Volume

You can adjust the volume through the [Device Configuration Page](#).

2.4 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 VoIP Outdoor Intercom with Keypad"](#) for instructions.

2.4.1 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

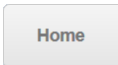

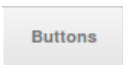



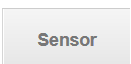
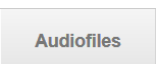
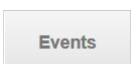



Parameter	Factory Default Setting
IP Addressing	DHCP
IP Address ^a	10.10.10.10
Web Access Username	admin
Web Access Password	admin
Subnet Mask ^a	255.0.0.0
Default Gateway ^a	10.0.0.1

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

2.4.2 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

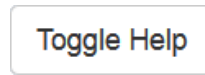
Web Page Item	Description
	Link to the Home page.
	Link to the Device page.
	Link to the Buttons page.
	Link to the Network page.
	Link to go to the SIP page.
	Link to the Multicast page.
	Link to the Sensor page.
	Link to the Audiofiles page.
	Link to the Events page.
	Link to the Door Strike Relay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

2.4.3 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:

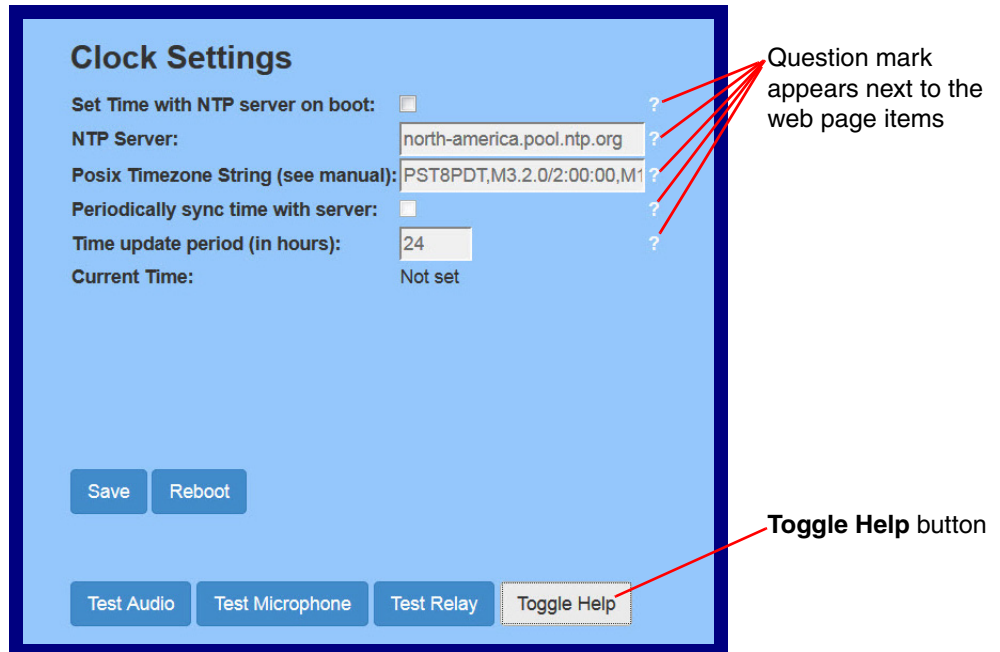
1. Click on the **Toggle Help** button that is on the UI webpage. See [Figure 2-15](#) and [Figure 2-16](#).

Figure 2-15. Toggle/Help Button



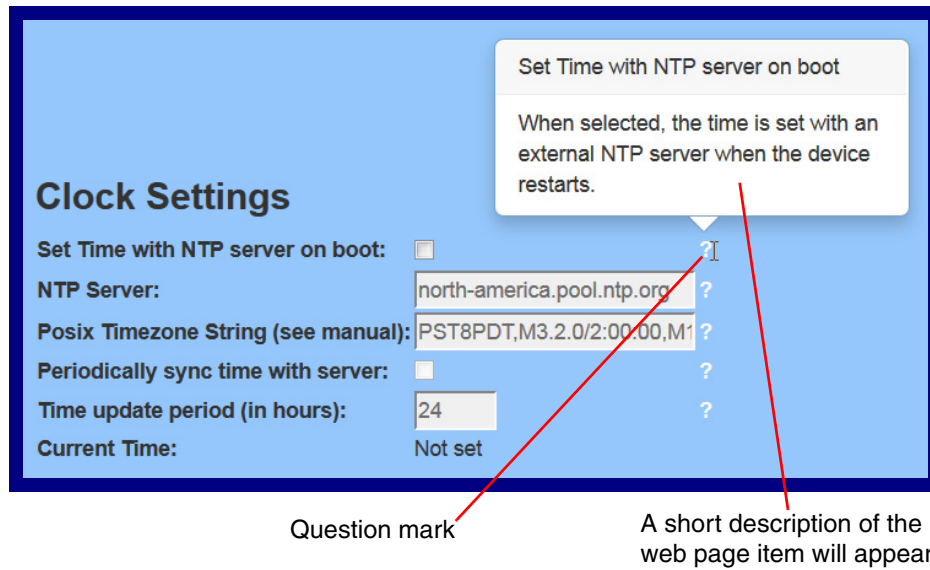
2. You will see a question mark (?) appear next to each web page item that has been provided with a short description by the Help feature. See [Figure 2-16](#).

Figure 2-16. 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 2-17](#).

Figure 2-17. Short Description Provided by the Help Feature



2.4.4 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 2-18):

Web Access Username: **admin**

Web Access Password: **admin**

Figure 2-18. Home Page

The screenshot displays the home page of the CyberData Keypad Intercom web interface. At the top, there is a navigation bar with tabs for Home, Device, Buttons, Network, SIP, Multicast, Sensor, Audiofiles, Events, DSR, Autoprov, and Firmware. The main title is "CyberData Keypad Intercom".

The page is divided into three main sections:

- Current Status:** A list of system parameters including Serial Number (214100452), Mac Address (00:20:f7:03:4e:59), Firmware Version (v11.6.2), IP Addressing (DHCP), IP Address (10.10.1.54), Subnet Mask (255.0.0.0), Default Gateway (10.0.0.1), DNS Server 1 (10.0.1.56), DNS Server 2, SIP Volume (4), Multicast Volume (1), Ring Volume (4), Sensor Volume (4), Push to Talk Volume (0), Volume Boost (Off), Microphone Gain (4), Push to Talk Microphone Gain (0), SIP Mode (Disabled), Multicast Mode (Enabled), Event Reporting (Enabled), Nightringer (Enabled), Primary SIP Server (Not registered), Backup Server 1 (Not registered), Backup Server 2 (Not registered), and Nightringer Server (Registered).
- Admin Settings:** Fields for Username (admin), Password, and Confirm Password. Below these are buttons for Save, Reboot, and Toggle Help.
- Import Settings:** A "Browse..." button with the text "No file chosen" and an "Import Config" button.
- Export Settings:** An "Export Config" button.

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

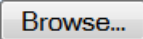





Web Page Item	Description
Admin Settings	
Username ?	The username to access the web interface. Enter up to 25 characters.
Password ?	The password to access the web interface. Enter up to 25 characters.
Confirm Password ?	Confirm the web interface password.
Current Status	
Serial Number	Shows the device 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.
Import Settings	
	Use this button to select a configuration file to import.

Table 2-7. Home Page Overview (continued)

Web Page Item	Description
	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.

2.4.5 Configure the Device

1. Click the **Device** menu button to open the **Device** page. See [Figure 2-19](#).

Figure 2-19. Device Configuration Page

The screenshot shows the 'Device' configuration page for a CyberData Keypad Intercom. The page features a navigation menu at the top with the following tabs: Home, Device, Buttons, Network, SIP, Multicast, Sensor, Audiofiles, Events, DSR, Autoprovisioning, and Firmware. The main heading is 'CyberData Keypad Intercom'. The configuration is organized into four primary sections:

- Volume Settings (0-9):** Includes sliders for SIP Volume (4), Multicast Volume (1), Ring Volume (4), Sensor Volume (4), and Push to Talk Volume (0). A 'No Volume Boost' dropdown menu is also present.
- Microphone Settings (0-9):** Includes sliders for Microphone Gain (4) and Push to Talk Microphone Gain (0).
- Clock Settings:** Includes a checked checkbox for 'Set Time with NTP server on boot', an NTP Server field (north-america.pool.ntp.org), a Posix Timezone String field (PST8PDT,M3.2.0/2:00:00,M11...), a checked checkbox for 'Periodically sync time with server', a Time update period field (24 hours), and a Current Time display (09:48:55).
- Relay Settings:** Includes a checked checkbox for 'Activate Relay with DTMF code', Relay Pulse Code (000), Relay Pulse Duration (2 seconds), Relay Activation Code (987), Relay Deactivation Code (789), and several checkboxes for 'Play tone during DTMF Activation', 'Activate Relay During Ring', 'Activate Relay During Night Ring', 'Activate Relay While Call Active', and 'Activate Relay On Button Press'. A Relay On Button Press Duration field is set to 3.

At the bottom of the page, there are 'Save' and 'Reboot' buttons. Below these, there is a row of buttons for 'Test Audio', 'Test Microphone', 'Test Relay', and 'Toggle Help'. The 'Device Name' field is set to 'power test'.

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.
Multicast Volume ?	Set the speaker volume for multicast audio streams. A value of 0 will mute the speaker during multicasts.
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.
Sensor Volume ?	Set the speaker volume for playing sensor activated audio. A value of 0 will mute the speaker during sensor activated audio.
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.
Volume Boost: ? No Volume Boost Volume Boost 1 Volume Boost 2 Volume Boost 3	<p>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.</p> <p>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.</p> <p>The volume boost options increase the output of the speaker by:</p> <p>3db for Boost level 1 6db for Boost level 2 9db for Boost level 3</p> <p>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.</p> <p>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.</p> <p>Contact CyberData support for additional information if needed.</p>
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.
Posix Timezone String ?	See Section 2.4.5.1, "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.
Current Time	Allows you to input the current time. (6 character limit)
Relay Settings	
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.
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.

Table 2-8. Device Configuration Parameters (continued)
















Web Page Item	Description
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.
	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.
	Click on the Test Microphone button to do a microphone test. When the Test Microphone button is pressed, the following occurs: <ul style="list-style-type: none"> 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.
	Click on the Test Relay button to do a relay test.

Table 2-8. Device Configuration Parameters (continued)

Web Page Item	Description
	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 can change the **SIP Volume**, **Multicast Volume**, **Ring Volume**, **Sensor Volume**, and **Push to Talk Volume** without rebooting the device. You must save and reboot the device for other changes to take effect.

2.4.5.1 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 2-20. 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

2.4.6 Configure the Button Parameters

1. Click the **Button Config** button to open the **Button Configuration** page. See [Figure 2-21](#).

Figure 2-21. Button Configuration Page

Dial Mode

- Enable Telephone Operation:
- Enable Cell Phone Operation:
- Enable Speed Dial Operation:
- Enable Security Operation:

Security Mode Settings

Security Code 0:	1234560	Activate DSR:	<input type="checkbox"/>
Security Code 1:	1234561	Activate DSR:	<input type="checkbox"/>
Security Code 2:	1234562	Activate DSR:	<input type="checkbox"/>
Security Code 3:	1234563	Activate DSR:	<input type="checkbox"/>
Security Code 4:	1234564	Activate DSR:	<input type="checkbox"/>
Security Code 5:	1234565	Activate DSR:	<input type="checkbox"/>
Security Code 6:	1234566	Activate DSR:	<input type="checkbox"/>
Security Code 7:	1234567	Activate DSR:	<input type="checkbox"/>
Security Code 8:	1234568	Activate DSR:	<input type="checkbox"/>
Security Code 9:	1234569	Activate DSR:	<input type="checkbox"/>
Relay Activation Code:	666666	Activate DSR:	<input type="checkbox"/>
Relay Deactivation Code:	999999		

Relay Activation Timeout:

Play Tone While Relay Active:

Allow Telephone Dialout:

Call Button: ID:

Speed Dial Settings

Speed Dial Timeout:

Keypad 1:	241	ID:	id241
Keypad 2:	242	ID:	id242
Keypad 3:	243	ID:	id243
Keypad 4:	244	ID:	id244
Keypad 5:	245	ID:	id245
Keypad 6:	246	ID:	id246
Keypad 7:	247	ID:	id247
Keypad 8:	248	ID:	id248
Keypad 9:	249	ID:	id249
Keypad 0:	2411	ID:	id2411
Keypad *:	2410	ID:	id2410
Keypad #:	2412	ID:	id2412
Call Button:	600	ID:	id204

Button Tones

Play Button Tones:

Save Reboot

Start Button Test Toggle Help

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	
Activate DSR	Activate a network attached relay instead of the relay on the device.
Security Code 0	Up to eight digits using characters 0 through 9 and *.
Security Code 1	Up to eight digits using characters 0 through 9 and *.
Security Code 2	Up to eight digits using characters 0 through 9 and *.
Security Code 3	Up to eight digits using characters 0 through 9 and *.
Security Code 4	Up to eight digits using characters 0 through 9 and *.
Security Code 5	Up to eight digits using characters 0 through 9 and *.
Security Code 6	Up to eight digits using characters 0 through 9 and *.
Security Code 7	Up to eight digits using characters 0 through 9 and *.
Security Code 8	Up to eight digits using characters 0 through 9 and *.
Security Code 9	Up to eight digits using characters 0 through 9 and *.
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).
Relay Activation Timeout	The time in seconds to activate the relay when a security code is entered. Up to five numerical digits.
Play Tone While Relay Active	Play a tone when the relay is activated by a security code.

Table 2-13. Button Configuration Parameters (continued)

Web Page Item	Description
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.
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.
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.
	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 Start button to start a button test.
	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.

2.4.6.1 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.

2.4.6.2 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

All 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.
All 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.

2.4.7 Configure the Network Parameters

1. Click the **Network** menu button to open the **Network** page (Figure 2-22).

Figure 2-22. Network Configuration Page

Home Device Buttons **Network** SIP Multicast Sensor Audiofiles Events DSR Autoprov Firmware

CyberData Keypad Intercom

Stored Network Settings

Addressing Mode: Static DHCP

Hostname:

IP Address:

Subnet Mask:

Default Gateway:

DNS Server 1:

DNS Server 2:

DHCP Timeout in seconds*:

* A value of -1 will retry forever

VLAN Settings

VLAN ID (0-4095):

VLAN Priority (0-7):

Save Reboot Toggle Help

Current Network Settings

IP Address: 10.10.0.247

Subnet Mask: 255.0.0.0

Default Gateway: 10.0.0.1

DNS Server 1: 10.0.0.252

DNS Server 2:




2. On the **Network** page, 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. 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 2.4.1, "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	
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 2-16. Network Configuration Parameters (continued)

Web Page Item	Description
	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 and then the **Reboot** button for the changes to take effect.

2.4.8 Configure the SIP Parameters

1. Click on the **SIP** menu button to open the **SIP** page (Figure 2-23).

Figure 2-23. SIP Configuration Page

The screenshot displays the SIP Configuration Page for a CyberData Keypad Intercom. The page has a blue header with the title "CyberData Keypad Intercom" and a navigation menu at the top with buttons for Home, Device, Buttons, Network, SIP (selected), Multicast, Sensor, Audiofiles, Events, DSR, Autopro, and Firmware.

SIP Settings

- Enable SIP operation:
- Register with a SIP Server:
- Use Cisco SRST:
- Primary SIP Server: 10.0.1.50
- Primary SIP User ID: 613
- Primary SIP Auth ID: 613
- Primary SIP Auth Password: *****
- Backup SIP Server 1: [Empty]
- Backup SIP User ID 1: [Empty]
- Backup SIP Auth ID 1: [Empty]
- Backup SIP Auth Password 1: [Empty]
- Backup SIP Server 2: [Empty]
- Backup SIP User ID 2: [Empty]
- Backup SIP Auth ID 2: [Empty]
- Backup SIP Auth Password 2: [Empty]
- Remote SIP Port: 5060
- Local SIP Port: 5060
- Outbound Proxy: [Empty]
- Outbound Proxy Port: 0
- Disable rport Discovery:
- Re-registration Interval (in seconds): 360
- Unregister on Boot:
- Keep Alive Period: 10000

Nightringer Settings

- Enable Nightringer:
- SIP Server: 10.0.1.50
- Remote SIP Port: 5060
- Local SIP Port: 5061
- Outbound Proxy: [Empty]
- Outbound Proxy Port: 0
- User ID: 614
- Authenticate ID: 614
- Authenticate Password: *****
- Re-registration Interval (in seconds): 360

RTP Settings

- RTP Port (even): 10500

Call Disconnection

- Terminate Call after delay: 30

Codec Selection

- Force Selected Codec:
- Codec: PCMU (G.711, u-law)

Buttons: Save, Reboot, Toggle Help

2. On the **SIP** page, enter values for the parameters indicated in [Table 2-17](#).

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 2-17. 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 2.4.8.1, "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.





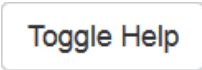

Table 2-17. SIP Configuration Parameters (continued)

Web Page Item	Description
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.
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.
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.

Table 2-17. SIP Configuration Parameters (continued)

Web Page Item	Description
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.
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.
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 2-17. 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).
	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 and then the **Reboot** button 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/>

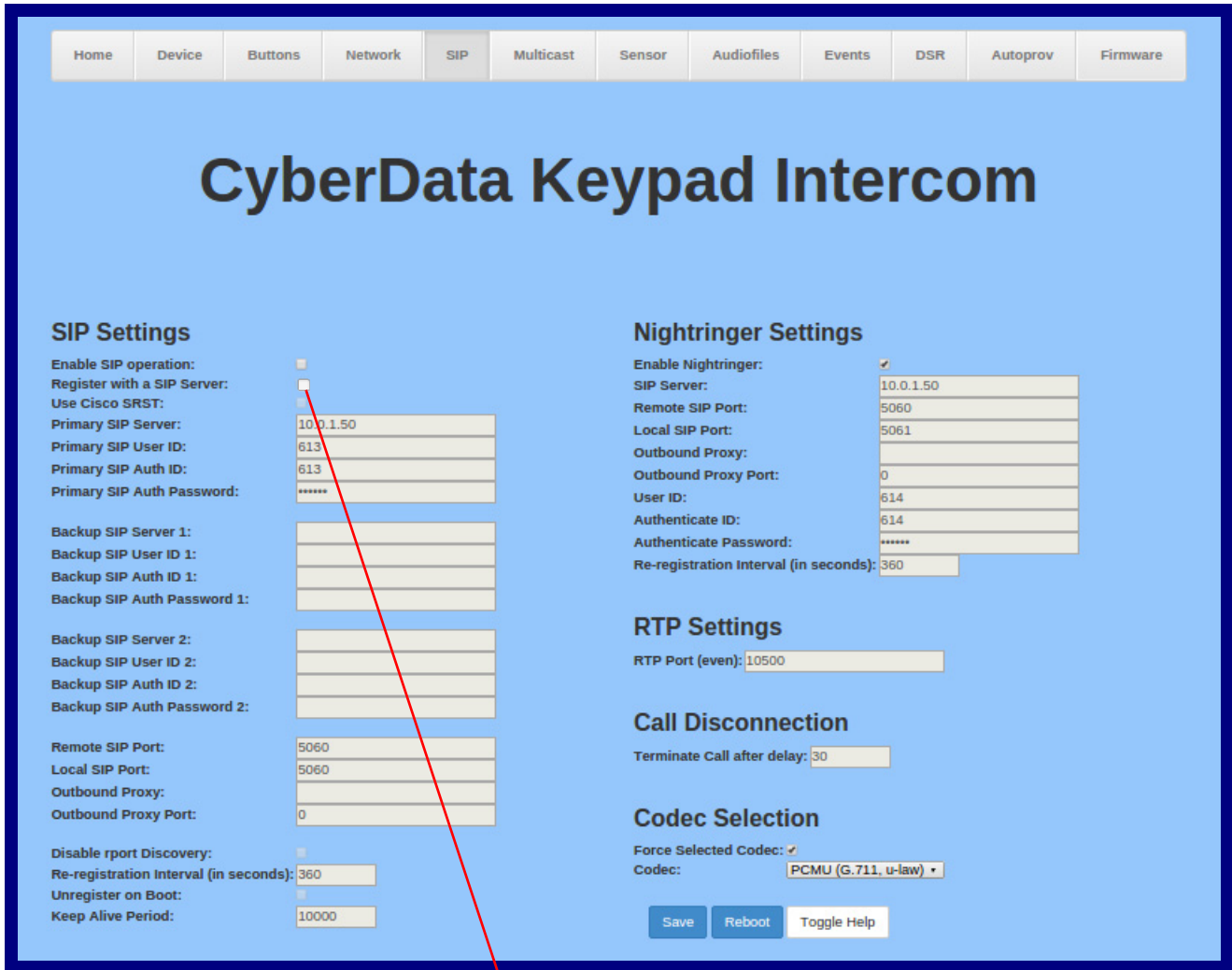
2.4.8.1 Point-to-Point Configuration

When the device is set to not register with a SIP server (see [Figure 2-24](#)), 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 2-24. SIP Page Set to Point-to-Point Mode



Device is set to NOT register with a SIP server

2.4.9 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 2-25](#).

Figure 2-25. Multicast Configuration Page

Home Device Buttons Network SIP **Multicast** Sensor Audiofiles Events DSR Autoprof Firmware

CyberData Keypad Intercom

Multicast Settings

Enable Multicast Operation:

Priority	Address	Port	Name	Beep	Relay
9	239.168.3.10	11022	Emergency	<input type="checkbox"/>	<input checked="" type="checkbox"/>
8	239.168.3.9	10022	MG8	<input type="checkbox"/>	<input checked="" type="checkbox"/>
7	239.168.3.8	9022	MG7	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6	239.168.3.7	8022	MG6	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5	239.168.3.6	7022	MG5	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4	239.168.3.5	6022	MG4	<input type="checkbox"/>	<input type="checkbox"/>
3	239.168.3.4	5022	MG3	<input type="checkbox"/>	<input type="checkbox"/>
2	239.168.3.3	4022	MG2	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1	239.168.3.2	3030	MG1	<input type="checkbox"/>	<input checked="" type="checkbox"/>
0	239.168.3.1	2022	Background Music	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Polycorn Default Channel

Polycorn Priority Channel

Polycorn Emergency Channel

SIP calls are considered priority 4.5

Port range can be from 2000-65535

Priority 9 is the highest and 0 is the lowest

A higher priority audio stream will always supersede a lower one



Priority 9 streams will play at maximum volume

** You need to reboot for changes to take effect*

2. On the **Multicast** 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. Multicast Configuration Parameters

Web Page Item	Description
Enable Multicast Operation	Enables or disables multicast operation.
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 2.4.9.1, "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]).
Name	Assign a descriptive name for this multicast group (25 character limit).
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.
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.
	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.

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

2.4.9.1 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.

2.4.10 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 2-26).

Figure 2-26. Sensor Configuration Page

Home Device Buttons Network SIP Multicast **Sensor** Audiofiles Events DSR Autoprov Firmware

CyberData Keypad Intercom

Door Sensor Settings

Door Sensor Normally Closed: Yes No

Door Open Timeout (in seconds):

Flash Button LED:

Activate Relay:

Play Audio Locally:

Make call to extension:

Dial Out Extension:

Dial Out ID:

Play recorded audio:

Repeat Sensor Message:

Intrusion Sensor Settings

Flash Button LED:

Activate Relay:

Play Audio Locally:

Make call to extension:

Dial Out Extension:

Dial Out ID:

Play recorded audio:

Repeat Intrusion Message:

Save Reboot Toggle Help

Test Door Sensor Test Intrusion Sensor









2. On the **Sensor** 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. 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.
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.

Table 2-19. Sensor Configuration Parameters (continued)

Web Page Item	Description
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.
	Click the Test Door Sensor button to test the door sensor.
	Click the Test Intrusion Sensor button to test the Intrusion sensor.
	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 and then the **Reboot** button for the changes to take effect.

2.4.11 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 2-27).

Figure 2-27. Audiofiles Configuration Page

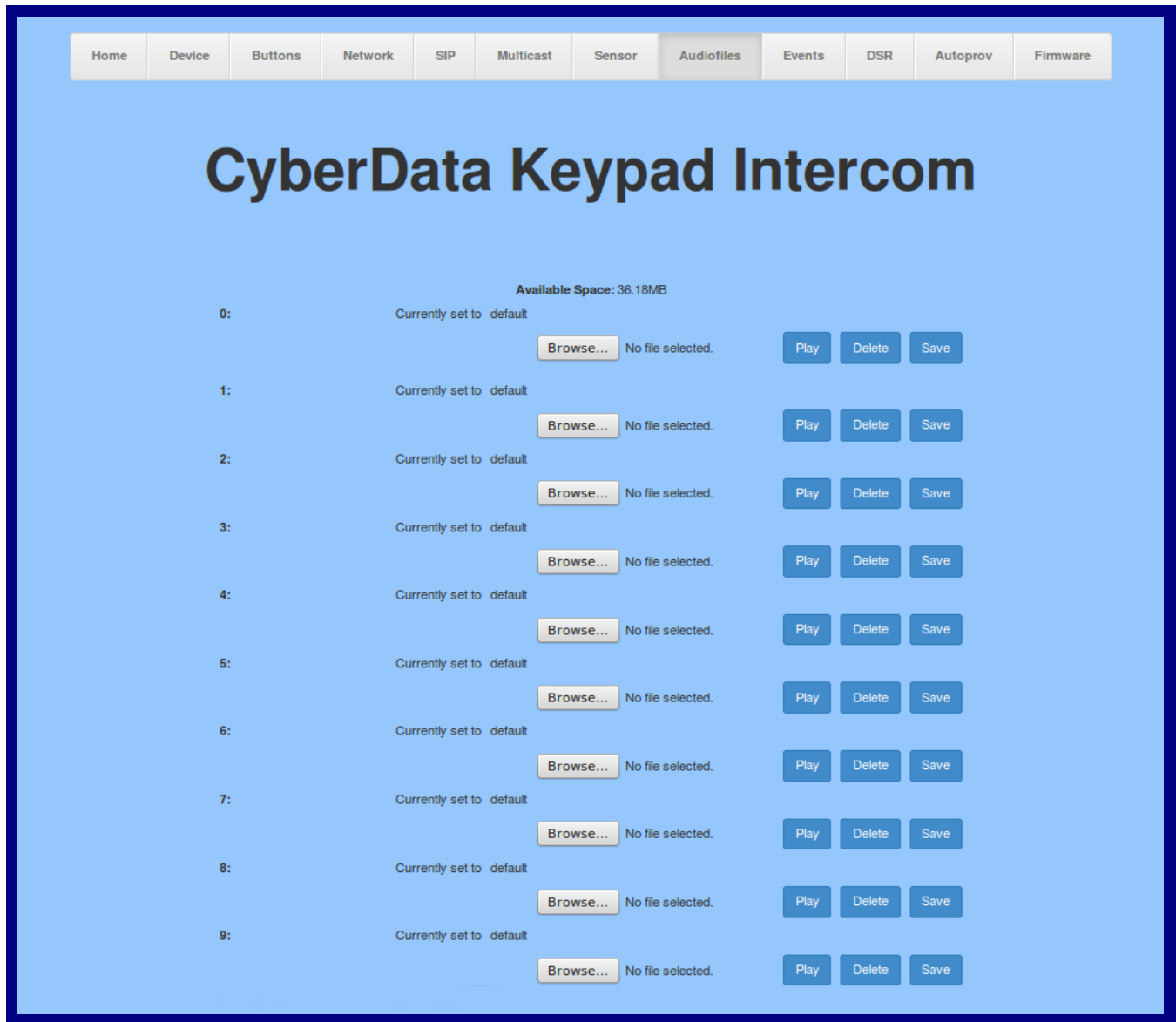


Figure 2-28. Audiofiles Configuration Page (continued)

Dot:	Currently set to default	<input type="button" value="Browse..."/>	No file selected.	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Audio Test:	Currently set to default	<input type="button" value="Browse..."/>	No file selected.	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Page Tone:	Currently set to default	<input type="button" value="Browse..."/>	No file selected.	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Your IP Address Is:	Currently set to default	<input type="button" value="Browse..."/>	No file selected.	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Rebooting:	Currently set to default	<input type="button" value="Browse..."/>	No file selected.	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Restoring Default:	Currently set to default	<input type="button" value="Browse..."/>	No file selected.	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Ringback Tone:	Currently set to default	<input type="button" value="Browse..."/>	No file selected.	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Ring Tone:	Currently set to default	<input type="button" value="Browse..."/>	No file selected.	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Intrusion Sensor Triggered:	Currently set to default	<input type="button" value="Browse..."/>	No file selected.	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Door Ajar:	Currently set to default	<input type="button" value="Browse..."/>	No file selected.	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Night Ring:	Currently set to default	<input type="button" value="Browse..."/>	No file selected.	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>

2. On the **Audiofiles** 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. Audiofiles Configuration Parameters

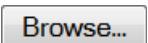

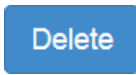

Web Page Item	Description
Available Space	Shows the space available for the user to save custom audio files if they want to change the message when the door or sensor is triggered.
0-9	The name of the audio configuration option is the same as the spoken audio that plays on the board (24 character limit). '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 <i>"This is the CyberData IP speaker test message..."</i> (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.
	Click on the Browse button to navigate to and select an audio file.

Table 2-20. Audiofiles Configuration Parameters (continued)

Web Page Item	Description
	The Play button will play that audio file.
	The Delete button will delete any user uploaded audio and restore the stock audio file.
	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.

2.4.11.1 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 2-29](#) through [Figure 2-31](#).

Figure 2-29. Audacity 1

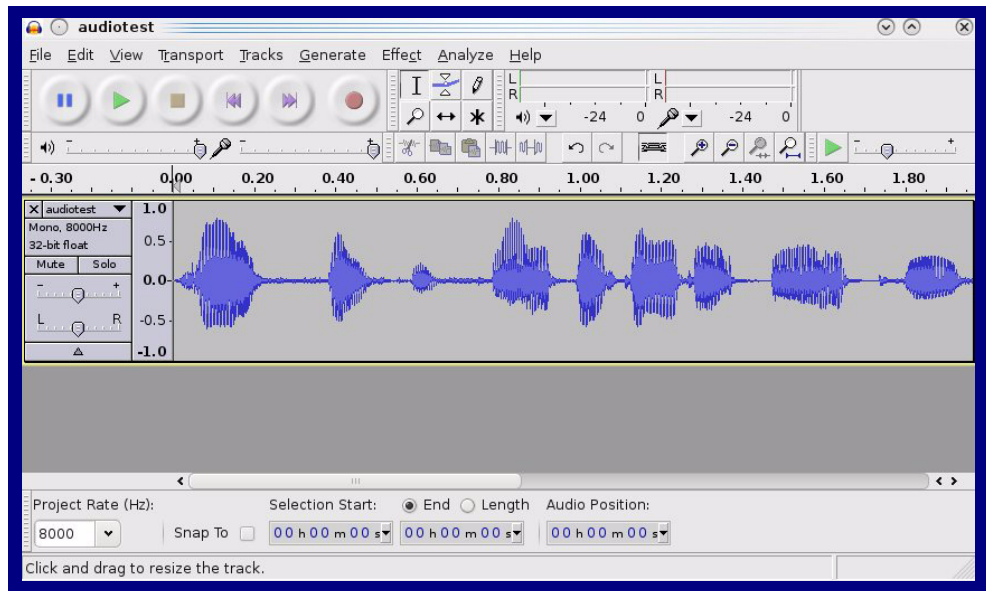
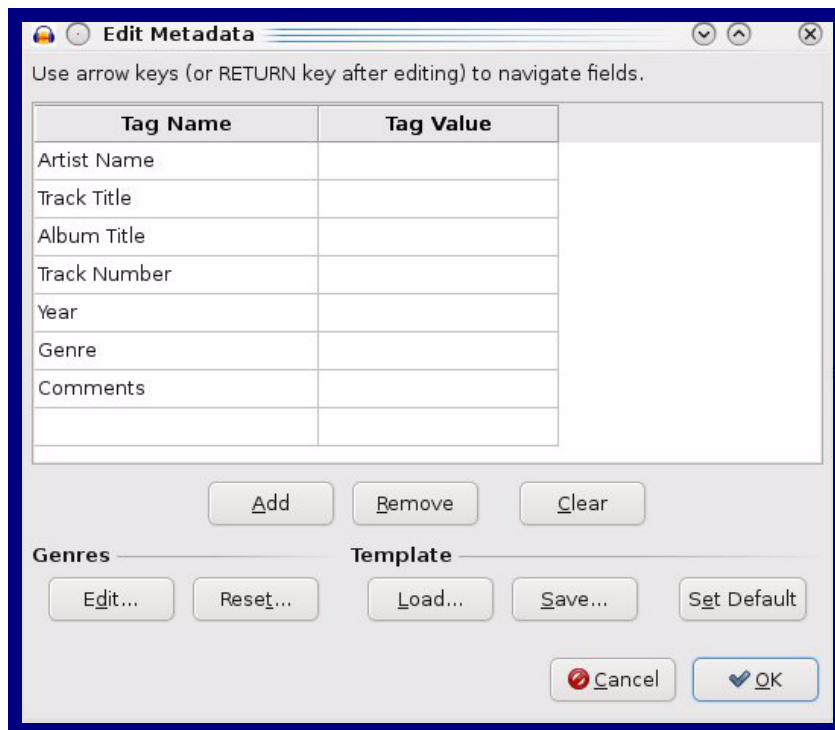


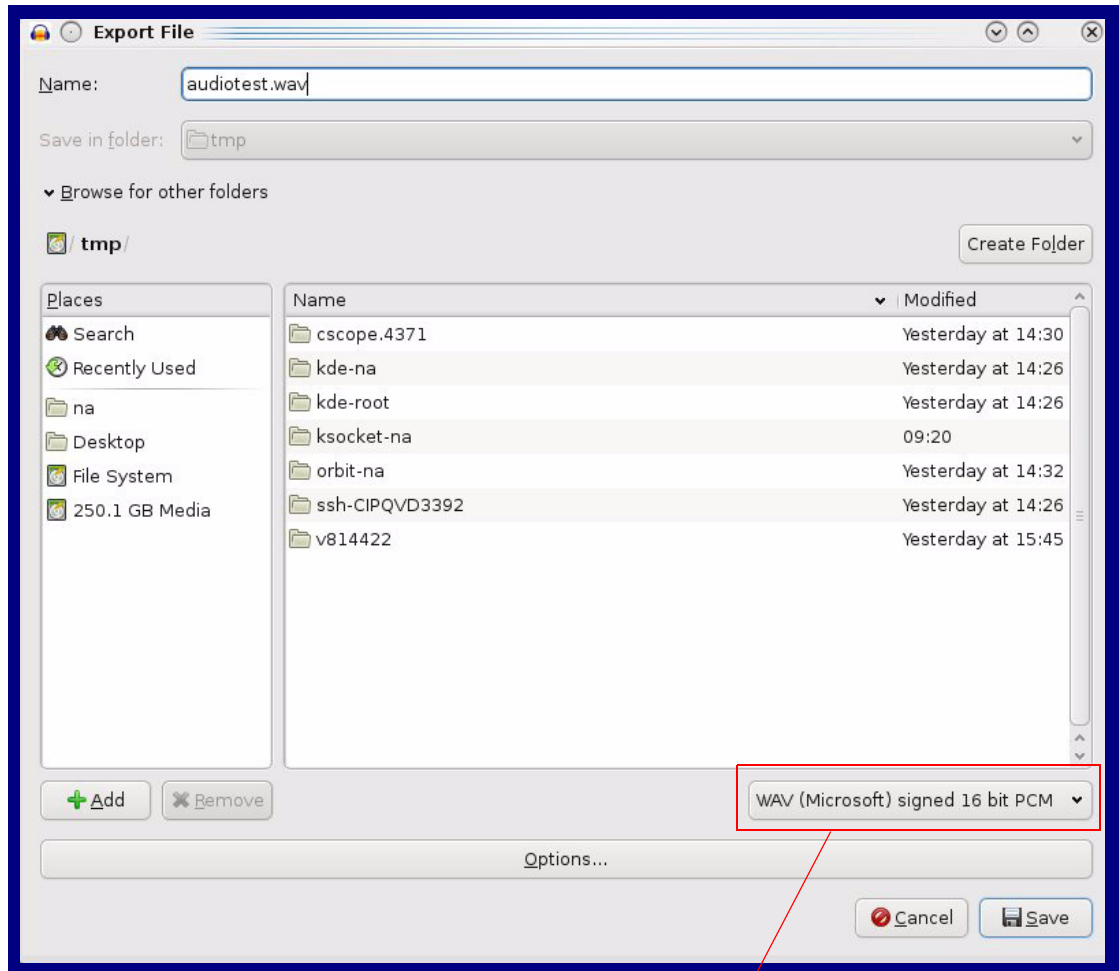
Figure 2-30. Audacity 2



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

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

Figure 2-31. WAV (Microsoft) signed 16 bit PCM



WAV (Microsoft) signed 16 bit PCM

2.4.12 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 2-32).

Figure 2-32. Event Configuration Page

Home Device Buttons Network SIP Multicast Sensor Audiofiles **Events** DSR Autopro Firmware

CyberData Keypad Intercom

Enable Event Generation:

Events

Enable Button Events:

Enable Call Start Events:

Enable Call Terminated Events:

Enable Relay Activated Events:

Enable Relay Deactivated Events:

Enable Ring Events:

Enable Night Ring Events:

Enable Multicast Start Events:

Enable Multicast Stop Events:

Enable Power On Events:

Enable Sensor Events:

Enable Remote Relay Events:

Enable Security Events:

Enable 60 Second Heartbeat:

[Check All](#) [Uncheck All](#)

Event Server

Server IP Address:

Server Port:

Server URL:








2. On the **Events** 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. 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.
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 2-21. 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.
	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 and then the **Reboot** button for the changes to take effect.

2.4.12.1 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>
```

2.4.13 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, during different call events, manually through the web interface, or by using a Windows application.

1. Click on the **DSR** menu button to open the **DSR** page (Figure 2-33).

Figure 2-33. DSR Page

Remote Relay Settings

Not associated with any DSRs

Activate Remote Relay with DTMF code:

DTMF Activation Code:

DTMF Activation Duration (in seconds):

Activate Remote Relay During Ring:

Activate Remote Relay During Night Ring:

Activate Remote Relay While Call Active:

Activate Remote Relay On Button Press:

Remote Relay On Button Press Duration (in seconds):

Listen Port for Remote Relay Status:

Remote Door Sensor Settings

Door Open Timeout (in seconds):

Flash Button LED:

Activate Local Relay:

Play Audio Locally:

Make call to extension:

Play recorded audio:

Dial Out Extension:

Dial Out ID:

Discovered Remote Relays

Product Type	IP Address	MAC Address	Serial Number	Name	Version		
DoorLock	10.10.1.45	00:20:F7:02:A7:9A	270000004	LOCK270000004	V2.2AM	<input type="button" value="View"/>	<input type="button" value="Associate"/>
DoorLock	10.10.1.179	00:20:F7:02:A7:E2	270000078	LOCK270000078	V2.0A	<input type="button" value="View"/>	<input type="button" value="Associate"/>
DoorLock	10.10.1.19	00:20:F7:03:54:BE	375000016	LOCK375000016	V6.6A	<input type="button" value="View"/>	<input type="button" value="Associate"/>

Cache age: 00:20

2. On the **DSR** 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. DSR Configuration Parameters

Web Page Item	Description
Remote Relay Settings	
Activate Relay with DTMF Code ?	Activates the remote relay (DSR) when the DTMF Activation Code is entered on the phone during a SIP call with the device. RFC2833 DTMF payload types are supported.
DTMF Activation Code ?	Activation code used to activate the remote relay (DSR) when entered on a phone during a SIP call with the device. Activate Remote Relay with DTMF Code must be enabled. Enter up to 25 digits. Note: While Enable DTMF Push to Talk is enabled, the *, #, and 0 keys cannot be used in the DTMF activation code.
DTMF Activation Duration (in seconds) ?	The length of time (in seconds) during which the remote relay (DSR) will be activated when the DTMF Activation Code is detected. Enter up to 5 digits.
Activate Remote Relay During Ring ?	When selected, the remote relay (DSR) 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. When selected, the network relay will be activated for as long as the call is active.
Activate Remote Relay During Night Ring ?	When selected, the remote relay (DSR) will be activated as long as the Nightringer extension is ringing.
Activate Remote Relay While Call Active ?	When selected, the remote relay (DSR) will be activated as long as the call is active.
Activate Remote Relay on Button Press ?	When selected, the remote relay (DSR) will be activated when the Call Button is pressed.
Remote Relay on Button Press Duration (in seconds) ?	The length of time (in seconds) during which the remote relay (DSR) will be activated when the Call button is pressed. Enter up to 5 digits. A Remote Relay on Button Press Duration value of 0 will pulse the remote relay (DSR) once when the Call button is pressed.
Listen Port for Remote Relay Status ?	Specify the port to listen for remote relay (DSR) status packets.
Remote Door Sensor Settings	
Door Open Timeout (in seconds) ?	The time (in seconds) the device will wait before it performs an action when the remote (DSR) door sensor is activated. The action(s) performed are based on the configured Remote Door Sensor Settings below.
Flash Button LED ?	When selected, the Call button LED will flash until the remote (DSR) door sensor is deactivated (roughly 10 times/second).
Activate Local Relay ?	When selected, the device's on-board relay will be activated until the remote (DSR) door sensor is deactivated.
Play Audio Locally ?	When selected, the device will loop an audio file out of the speaker until the remote (DSR) door sensor is deactivated.

Table 2-22. DSR Configuration Parameters (continued)


















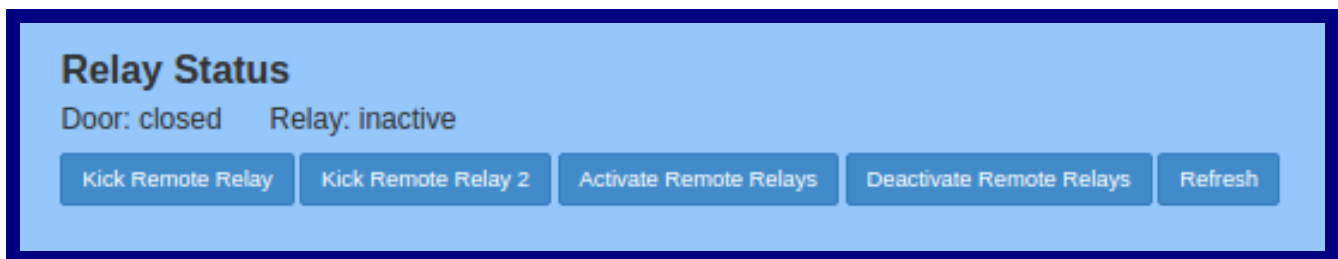
Web Page Item	Description
Make call to extension 	When selected, the device will call an extension when the remote (DSR) door sensor is activated. Use the 'Dial Out Extension' field below to specify the extension the device will call.
Play recorded audio 	When selected, the device will call the Dial Out Extension and play an audio file to the phone answering the SIP call (corresponds to Door Ajar on the Audiofiles page) when the remote (DSR) door sensor is activated.
Dial Out Extension 	Specify the extension the device will call when the remote (DSR) 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.
	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.
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.
	Use this button to search for and find any remote relays that are available on the network.
	Use this button to view the settings of a remote relay that has been "discovered" after pressing the Discover button.
	Use this button to associate the remote relay with the device. Only one relay may be associated with a device.

Table 2-22. DSR Configuration Parameters (continued)

Web Page Item	Description
	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.
Relay Status	Note: The Relay Status section and settings (Figure 2-34) only appear on the webpage when there is an associated door strike relay.
Door	Shows the status of the door.
Relay	Shows the status of the remote relay.
	Click on the Kick Remote Relay button to activate the remote relay for a specified time. The time is equal to the DTMF timeout.
	Click on the Kick Remote Relay button to activate the second remote relay for a specified time. The time is equal to the DTMF timeout.
	Click on the Activate Remote Relay button to activate both remote relays until the Deactivate Remote Relay button is pressed.
	Click on the Deactivate Remote Relay button to deactivate both remote relays.
	Click on the Refresh button to refresh the web page and accurately display the status of the remote relay (active/inactive) and door (open/closed).

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

Figure 2-34. Relay Status Section



2.4.14 Configure the Device (on the DSR page)

1. Click the **View** button on the **DSR** page to open the **Configure Device** page (Figure 2-35).

Figure 2-35. Configure Device Page

Configure Device

Serial Number	<input type="text" value="375000016"/>	<input type="button" value="Refresh"/>
MAC Address	<input type="text" value="00:20:F7:03:54:BE"/>	<input type="button" value="Get Log"/>
Version	<input type="text" value="V6.6A"/>	<input type="button" value="Clear Log"/>
Device Name	<input type="text" value="LOCK375000016"/>	<input type="button" value="Reboot"/>
Addressing Mode	<input type="radio"/> Static <input checked="" type="radio"/> DHCP	<input type="button" value="Set Time"/>
IP Address:	<input type="text" value="10.10.1.19"/>	<input type="button" value="Save Changes"/>
Subnet Mask:	<input type="text" value="255.0.0.0"/>	<input type="button" value="Cancel"/>
Default Gateway:	<input type="text" value="10.0.0.1"/>	
Command Port:	<input type="text" value="59999"/>	
Send Events	<input checked="" type="radio"/> Off <input type="radio"/> On	
Event IP Address:	<input type="text" value="10.255.255.255"/>	
Event Port:	<input type="text" value="49999"/>	
Energize Time:	<input type="text" value="6"/>	
DST	<input checked="" type="radio"/> Off <input type="radio"/> On	
DST Start:	<input type="text" value="M3.2.0/02.00.00"/>	
DST End:	<input type="text" value="M11.1.0/02.00.00"/>	
Current Time:	<input type="text" value="01:53:37 04222014"/>	
Encryption:	<input checked="" type="radio"/> None <input type="radio"/> AES-256	
Password:	<input type="text"/>	
Enable Multicast	<input checked="" type="radio"/> Off <input type="radio"/> On	
Multicast Listen Address:	<input type="text" value="239.168.3.1"/>	
Multicast Listen Port:	<input type="text" value="65535"/>	
Multicast Timeout:	<input type="text" value="255"/>	
Dual DSR Mode:	<input type="text" value="1"/>	

Door State	<input type="text" value="closed"/>	
Relay State	<input type="text" value="inactive"/>	
Button State	<input type="text" value="inactive"/>	
LED	<input type="text" value="red"/>	
Alarm State	<input type="text" value="alarm"/>	
JP4, 6, 9, 10	<input type="text" value="0000"/>	
Door2 State	<input type="text" value="closed"/>	
Relay2 State	<input type="text" value="inactive"/>	
Button2 State	<input type="text" value="inactive"/>	

No file chosen

2. On the **Configure Device** 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.








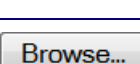

Table 2-23. DSR Page Configure Device Parameters

Web Page Item	Description
Serial Number	Displays the serial number of the door strike relay.
MAC Address	Displays the mac address of the door strike relay.
Version	Displays the firmware version of the door strike relay.
Device Name	Displays the name of the door strike relay. The default name is "LOCK," followed by the 9 digit ASCII serial number. The maximum name length is 13 characters. The unit will always respond to its default name.
Addressing Mode	Determines whether an IP address will be manually assigned through Static mode or dynamically assigned through a DHCP server.
IP Address	Displays the IP address of the door strike relay.
Subnet Mask	Displays the subnet mask of the door strike relay.
Default Gateway	Displays the default gateway of the door strike relay.
Command Port	This shows the port on which the door strike relay sends status packets to the device (defaults to 49999).
Send Events	When enabled, events can be sent to the associated device.
Event IP Address	The IP address of the associated device.
Event Port	This is the port by which the door strike relay receives commands (defaults to 59999).
Energize Time	This is the number of seconds that the relay will be energized.
DST	Allows you to either enable or disable the Daylight Savings Time feature.
DST Start	Sets the Daylight Savings Time starting time in the following format: M3.2.0/02:00:00 M3 is the third month (March). .2 is the second occurrence of the day in the month. .0 is Sunday. /02:00:00 is the time. Note: When the occurrence is set to 5 , the final occurrence of the day in the specified month is used.
DST End	Sets the Daylight Savings Time ending time in the following format: M11.1.0/02:00:00 M11 is the eleventh month (November). .1 is the first occurrence of the day in the month. .0 is Sunday. /02:00:00 is the time. Note: When the occurrence is set to 5 , the final occurrence of the day in the specified month is used.

Table 2-23. DSR Page Configure Device Parameters (continued)

Web Page Item	Description
Current Time	Sets the current time. Note: Be sure to save the current time by clicking on the Set Time button.
Encryption	Encryption can either be set to None or AES-256 .
Password	Sets the AES encryption key. If encryption is currently enabled, the response to this command will be sent using the "old" key. The new key should be sent as 64 ASCII hexadecimal characters.
Enable Multicast	Enables or disables multicast operation.
Multicast Listen Address	Enter the multicast IP Address (15 character limit).
Multicast Listen Port	Enter the port number for this multicast group (5 character limit [range can be from 2000 to 65535]).
Multicast Timeout	Time (in seconds) that the remote relay will remain active after the multicast broadcast has ended.
Mode	Enter the mode of operation (1 - 8): MODE 1 - Close mode After receipt of this command the controller will lock both doors. MODE 2 - Open mode After receipt of this command the controller will unlock both doors. Whenever an open door is detected the both relays will be activated. This command is intended for use during normal business hours. This mode permits entrance and exit from the controlled area whilst enforcing the presence of an 'air lock.' MODE 3 - Enter mode In this mode the outer door is normally unlocked. After the outer door is opened and re-closed the inner door will be unlocked for a single time period (the outer door will always be locked whenever the inner door is open). MODE 4 - Exit mode In this mode the inner door is normally unlocked. After the inner door is opened and re-closed the outer door will be unlocked for a single time period. The inner door will always be locked whenever the outer door is open. MODE 5 - Outer open mode In this mode the outer door is normally unlocked. The outer door will be locked whenever the inner door is open to enforce air lock. MODE 6 - Inner open mode In this mode the inner door is normally unlocked. The inner door will be locked whenever the outer door is open to enforce air lock. MODE 7 - Emergency mode After receipt of this command both doors are unlocked and the air lock procedure is no longer enforced. This mode allows both doors to be simultaneously opened to allow emergency egress from the controlled area.
Mode	MODE 8 - Single door mode In this mode the controller works in single door mode. All commands for the outer door are ignored and the status of its associated button and sense switch are not reported to the host.
Door State	This field displays the current door state and is not configurable.
Relay State	This field displays the current relay state and is not configurable.

Table 2-23. DSR Page Configure Device Parameters (continued)

Web Page Item	Description
Button State	This field displays the current button state and is not configurable.
LED	This field displays the current LED state and is not configurable.
Alarm State	This field displays the current alarm state and is not configurable.
JP4, 6, 9, 10	This shows whether jumpers JP4, JP6, JP9, or JP10 are either enabled or disabled through the four digit sequence (0000). The 0 turns to 1 for an enabled jumper. For example, 0011 would mean jumpers JP9 and JP10 are activated, but JP4 and JP9 are not.
Door2 State	This field displays the current door2 state and is not configurable.
Relay2 State	This field displays the current relay2 state and is not configurable.
Button2 State	This field displays the current button2 state and is not configurable.
	Click on the Refresh button to refresh the Device Configuration page.
	Click on the Get Log button to get a log of the associated door strike relay activity. The door strike relay has 128Kb non-volatile storage for log data, storing an average of 10 days' worth of log data before it is overwritten.
	Click on the Clear Log button to clear the log from the door strike relay
	Click on the Reboot button to reboot any “discovered” remote relays and clear any associated devices.
	Click on the Set Time button to change the time.
	Click on the Save Changes button to save any changes that are made to the Device Configuration page. Note: The time setting must be saved by pressing the Set Time button.
	Click on the Cancel button to cancel any changes that were made to the Configure Device page and return to the DSR page.
	Click on the Browse button to navigate through your computer and find firmware files.
	Click on the Upgrade button to upgrade the firmware of the door strike relay.

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

2.4.15 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 2-36](#).

Figure 2-36. Autoprovisioning Page

Home Device Buttons Network SIP Multicast Sensor Audiofiles Events DSR Autoprov Firmware

CyberData Keypad Intercom

Disable Autoprovisioning:

Autoprovisioning Server:

Autoprovisioning Filename:

Use tftp:

Username:

Password:

Autoprovisioning autoupdate (in minutes):

Autoprovision at time (HHMMSS):

Autoprovision when idle (in minutes > 10):

See the manual to learn how to use autoprovisioning to configure your device.

Autoprovisioning happens on boot.

The device will first look for a configured server address and filename.

If these haven't been configured, it will look for an autoprovisioning server in your list of DHCP options and try to download '0020f702ea13.xml' and if this fails, '000000cd.xml'.

Save Reboot Toggle Help

Download Template

Autoprovisioning log

```

00:00 Autoprovisioning Device...
00:00 Autoprov found option 43 in DHCP server="http://chalmers.cyberdata.net"
00:00 Autoprov looking for 0020f702ea13.xml at http://chalmers.cyberdata.net
00:00 Got autoprov file. Parsing "0020f702ea13.xml"
00:00 Autoprov found option 72 in DHCP server="10.0.0.252"
00:00 Autoprov looking for 0020f702ea13.xml at 10.0.0.252
00:00 Got autoprov file. Parsing "0020f702ea13.xml"
00:00 Autoprov found option 150 in DHCP server="10.0.0.252"
00:00 Autoprov looking for 0020f702ea13.xml at 10.0.0.252
00:01 Got autoprov file. Parsing "0020f702ea13.xml"
00:01 Autoprov found option 66 in DHCP server="http://chalmers.cyberdata.net"
    
```

- On the **Autoprovisioning** page, you may 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. Autoprovisioning Configuration Parameters





Web Page Item	Description
Disable Autoprovisioning ?	Prevent the device from automatically trying to download a configuration file. See Section 2.4.15.1, "Autoprovisioning" for more information.
Autoprovisioning Server ?	Enter the IPv4 address of the provisioning server in dotted decimal notation.
Autoprovisioning Filename ?	<p>The autoprovisioning filename is the configuration filename. The default autoprovisioning filename is in the format of <mac address>.xml.</p> <p>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.</p> <p>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.</p>
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) ?	<p>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.</p> <p>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).</p>
Autoprovision at time (HHMMSS) ?	<p>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.</p> <p>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).</p>
Autoprovision when idle (in minutes > 10) ?	<p>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.</p> <p>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).</p>
	<p>Click the Save button to save your configuration settings.</p> <p>Note: You need to reboot for changes to take effect.</p>

Table 2-24. Autoprovisioning Configuration Parameters (continued)

Web Page Item	Description
	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.
	Press the Download Template button to create an autoprovisioning file for the device. See Section 2.4.15.3, "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.

2.4.15.1 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 2.4.15.2, "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 auto provisioning template file from the [Auto provisioning Page](#) using the **Download Template** button (see [Table 2-24](#)). This file contains every configuration option that can be set on the board.

Auto provisioning files can contain the whole configuration or a subset of this file. The first auto provisioning file can also contain links to other auto provisioning files.

The `<MiscSettings>` section contains some examples of additional auto provisioning 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 auto provisioning 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 its 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 auto provision auto provisioning values (for example, to disable auto provisioning or to configure a time to check for new files).

Checking for New Auto provisioning Files after Boot

The device will always check for an auto provisioning 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 auto provisioning 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 2-25. 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 <FirmwareSettings>
Firmware Updates <FirmwareFile>505-uImage-ceiling-speaker</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-ulmage-[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 auto provisioning 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 auto provisioning 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 auto provisioned 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 auto provisioning 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 auto provisioning 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 auto provisioning file with “**default**” set as the file name.

2.4.15.2 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; }
}
```

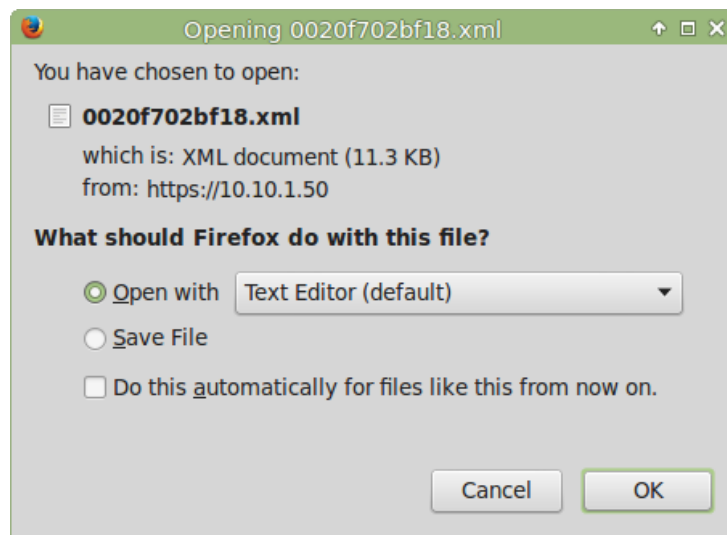
2.4.15.3 Download Template Button

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

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

1. On the **Auto provisioning** 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 2-37). 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 2-37.

Figure 2-37. Configuration File



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

2.5 Upgrade the Firmware and Reboot the Intercom



Caution

Equipment Hazard: Devices with a serial number that begins with 2141xxxxx can only run firmware versions 10.0.0 or later.

2.5.1 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/011214/>
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 2.4.4, "Log in to the Configuration Home Page"](#).

- Click on the **Firmware** menu button to open the **Firmware** page. See [Figure 2-38](#).


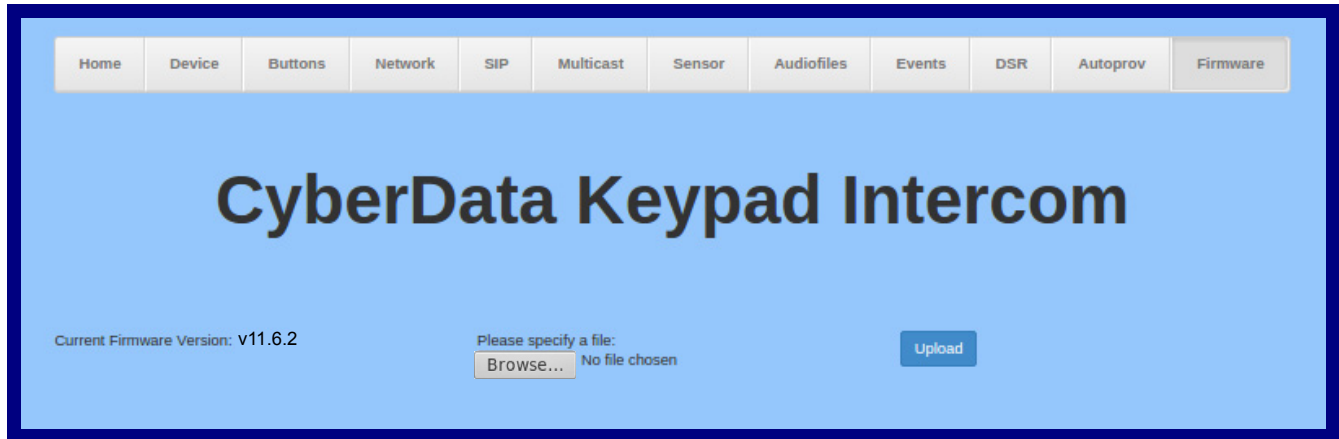
 <small>GENERAL ALERT</small>	<p>Caution</p> <p>Equipment Hazard: CyberData strongly recommends that you first reboot the device before attempting to upgrade the firmware of the device. See Section 2.5.2, "Reboot the Device".</p>
---	---

Figure 2-38. Firmware Page





- Click on the **Browse** button, and then navigate to the location of the firmware file.
- Select the firmware file.
- 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).

- [Table 2-26](#) shows the web page items on the **Firmware** page.

Table 2-26. Firmware Parameters

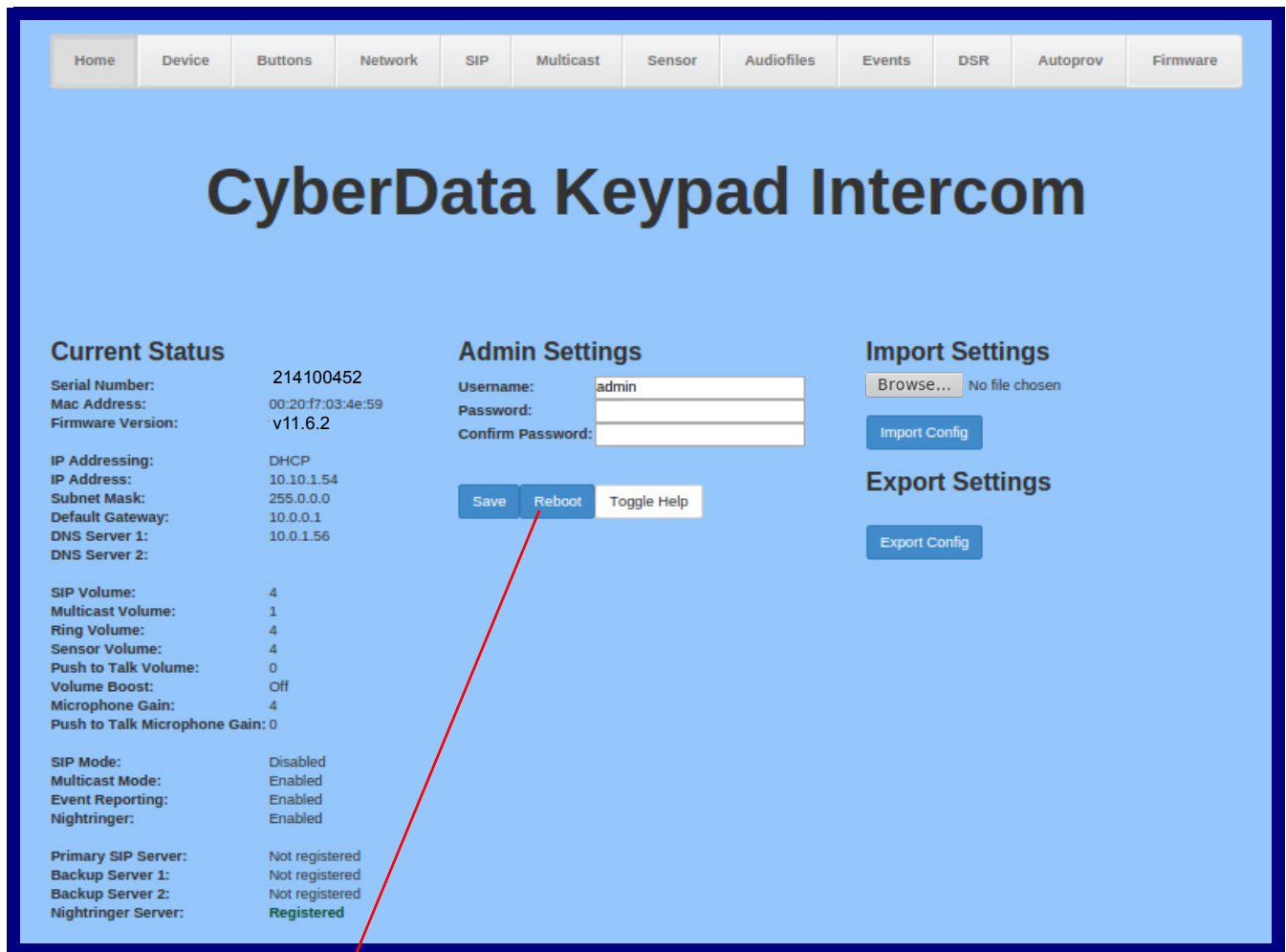
Web Page Item	Description
Current Firmware Version	Shows the current firmware version.
	Use the Browse button to navigate to the location of the Intercom firmware file that you want to upload.
	Click on the Upload button to automatically upload the selected firmware and reboot the system.

2.5.2 Reboot the Device

To reboot a Intercom, log in to the web page as instructed in [Section 2.4.4, "Log in to the Configuration Home Page"](#).

1. Click on the **Reboot** button on the **Home** page ([Figure 2-39](#)). A normal restart will occur.

Figure 2-39. Home Page



Reboot

2.6 Command Interface

Some functions on the device can be activated using simple POST commands to the web interface. The examples in [Table 2-27](#) use the free unix utility, **wget commands**. However, any program that can send HTTP POST commands to the device should work.

2.6.1 Command Interface Post Commands

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

Table 2-27. 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 2-27. 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 2-27. Command Interface Post Commands (continued)

Device Action	HTTP Post Command^a
Play the "Night Ring" audio file	<code>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"</code>
Delete the "0" audio file	<code>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"</code>
Delete the "1" audio file	<code>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"</code>
Delete the "2" audio file	<code>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"</code>
Delete the "3" audio file	<code>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"</code>
Delete the "4" audio file	<code>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"</code>
Delete the "5" audio file	<code>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"</code>
Delete the "6" audio file	<code>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"</code>
Delete the "7" audio file	<code>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"</code>
Delete the "8" audio file	<code>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"</code>
Delete the "9" audio file	<code>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"</code>
Delete the "Audio Test" audio file	<code>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"</code>
Delete the "Page Tone" audio file	<code>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"</code>
Delete the "Your IP Address Is" audio file	<code>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"</code>
Delete the "Rebooting" audio file	<code>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"</code>
Delete the "Restoring Default" audio file	<code>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"</code>

Table 2-27. 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 2.4.8.1, "Point-to-Point Configuration"](#)

Appendix A: Mounting the VoIP Outdoor Intercom with Keypad

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](#). See [Table A-2](#) and [Table A-3](#) for optional accessories.

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

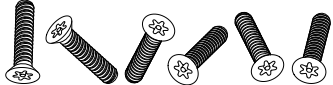

Quantity	Part Name	Illustration
6	Accessory Kit Security Torx MS	
1	Mounting Component Security Torx Key	

Table A-2. Optional Accessories (for gooseneck mounting)

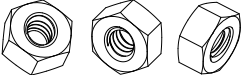



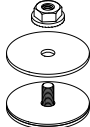
Quantity	Part Name	Illustration
3	Carriage bolt nuts	
3	Carriage bolts	
3	Carriage bolt washers	

Table A-3. Optional Accessories

Quantity	Part Name	Illustration
1	Spacer for Half-inch Set Screw Connector	
1	531085B Hole Plug Assembly	

A.2 Dimensions

Figure A-1. Unit Dimensions—Front and Side View

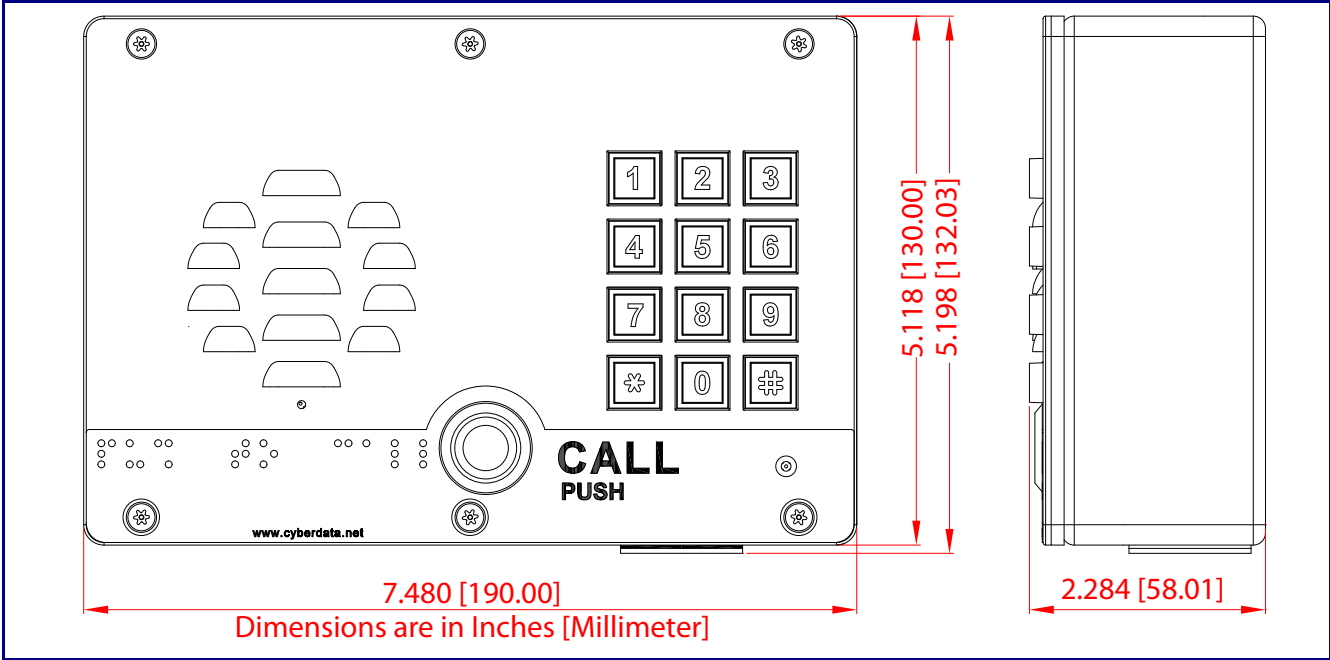


Figure A-1. Unit Dimensions—Rear View with Mounting Hole Locations

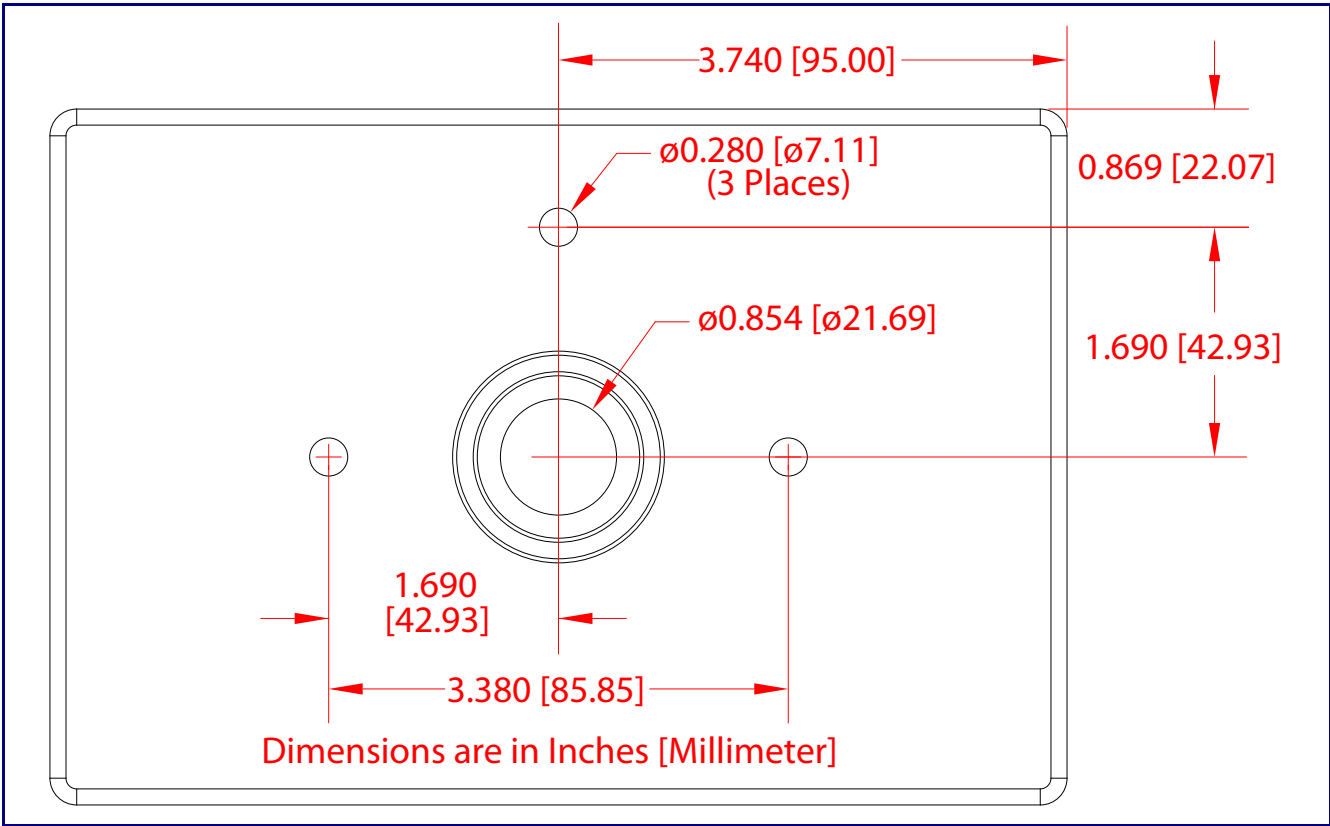


Figure A-2. Shroud Dimensions and Mounting Hole Locations

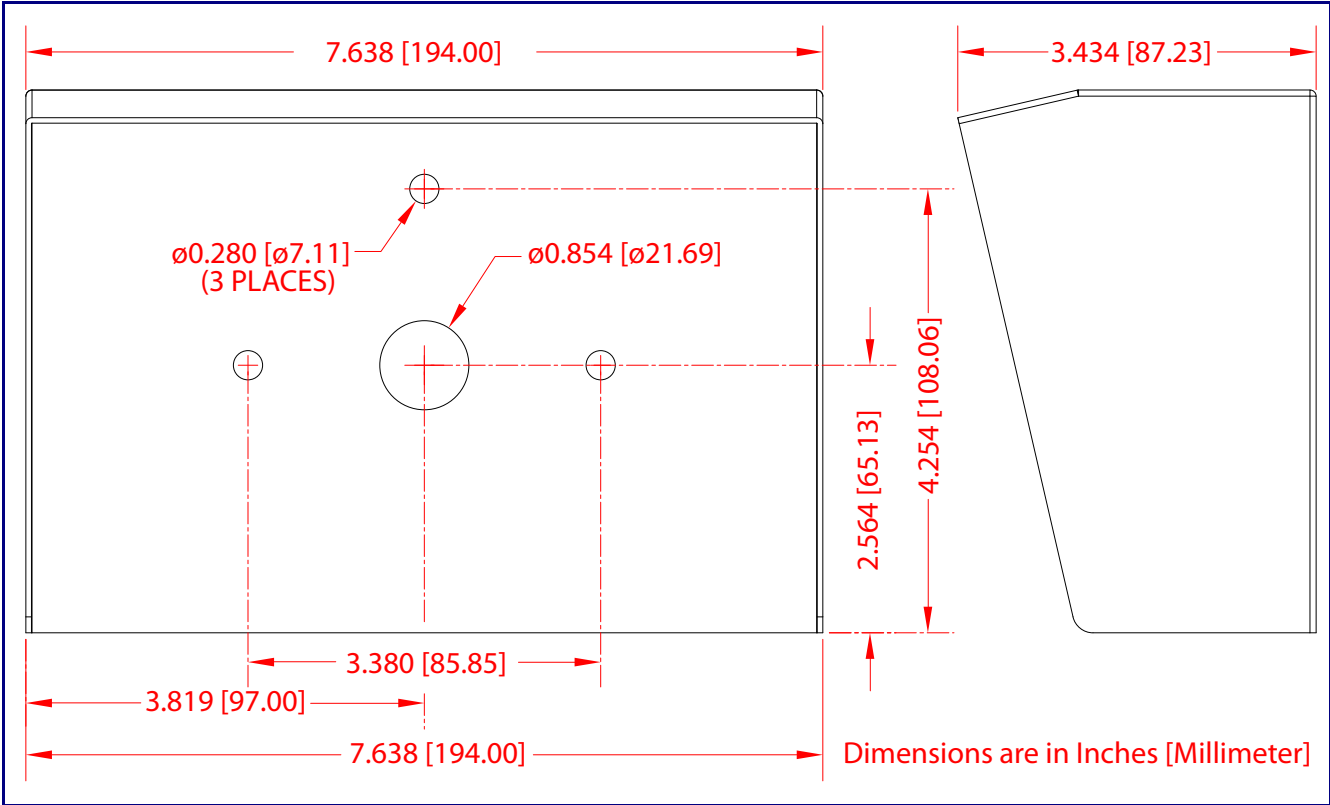
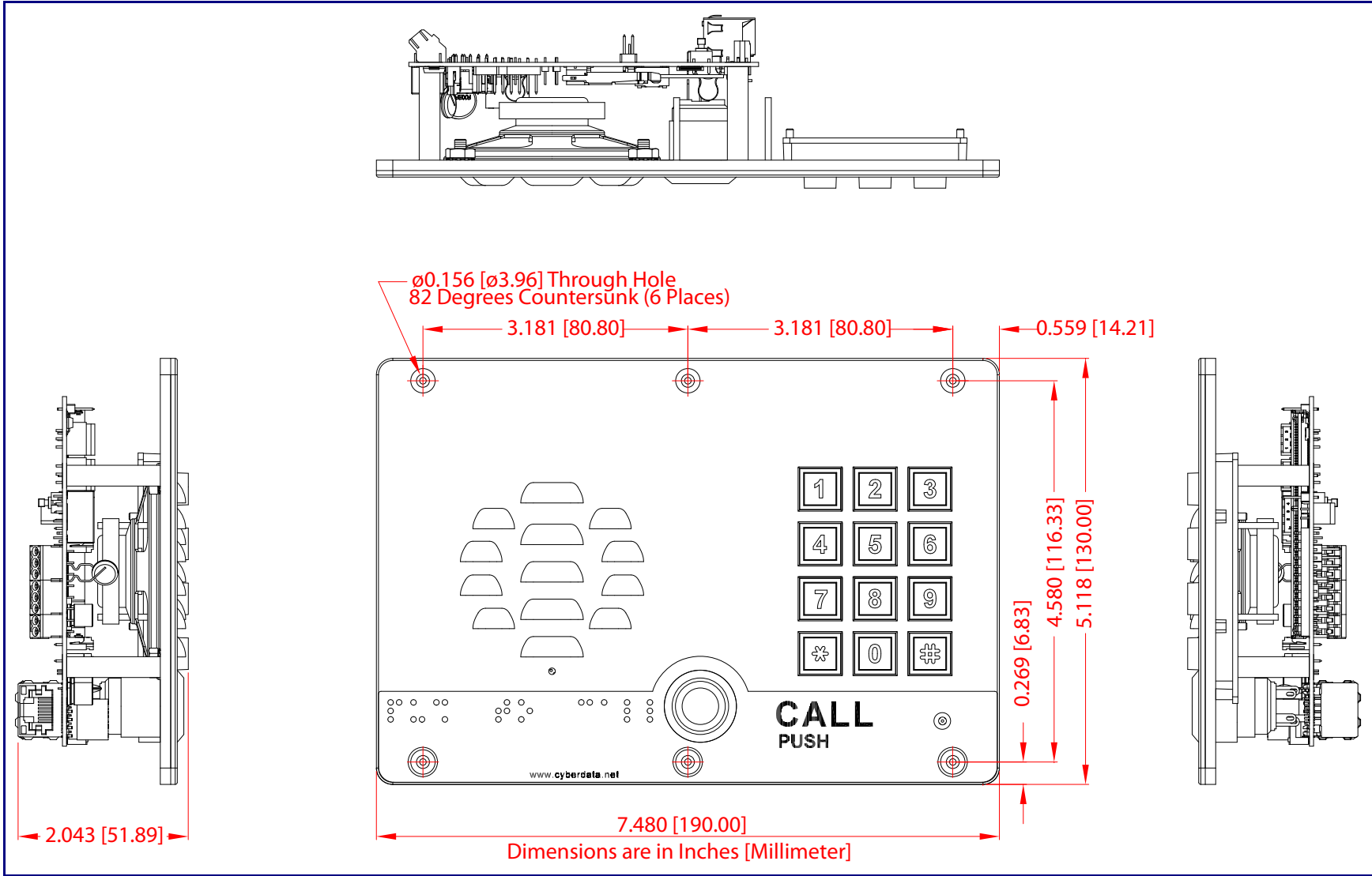


Figure A-3. Unit Dimensions—Faceplate and Board Assembled

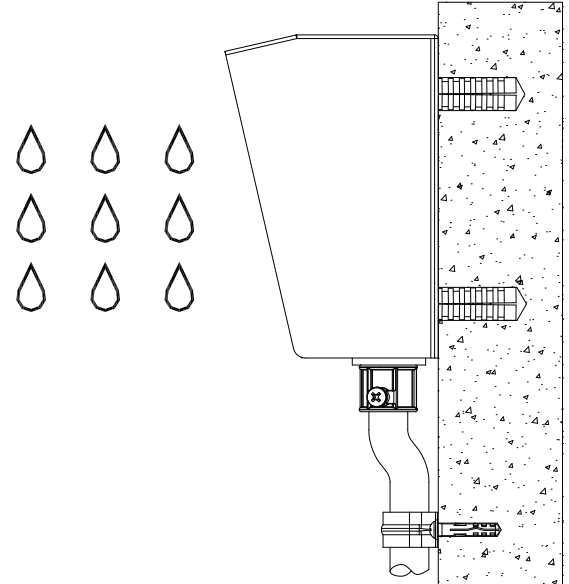
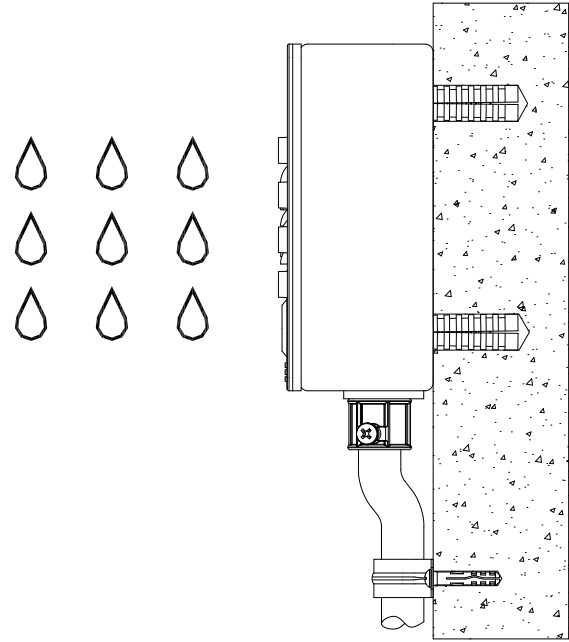


A.3 Overview of Installation Types

An overview of the installation types and the required components are provided in [Table A-4](#).

Table A-4. Overview of Installation Types

Installation Type	What You Need
Outdoor, on surface	011214 Intercom only
Outdoor, on surface with shroud (increased resistance)	011214 Intercom 011215 Weather Shroud (sold separately)

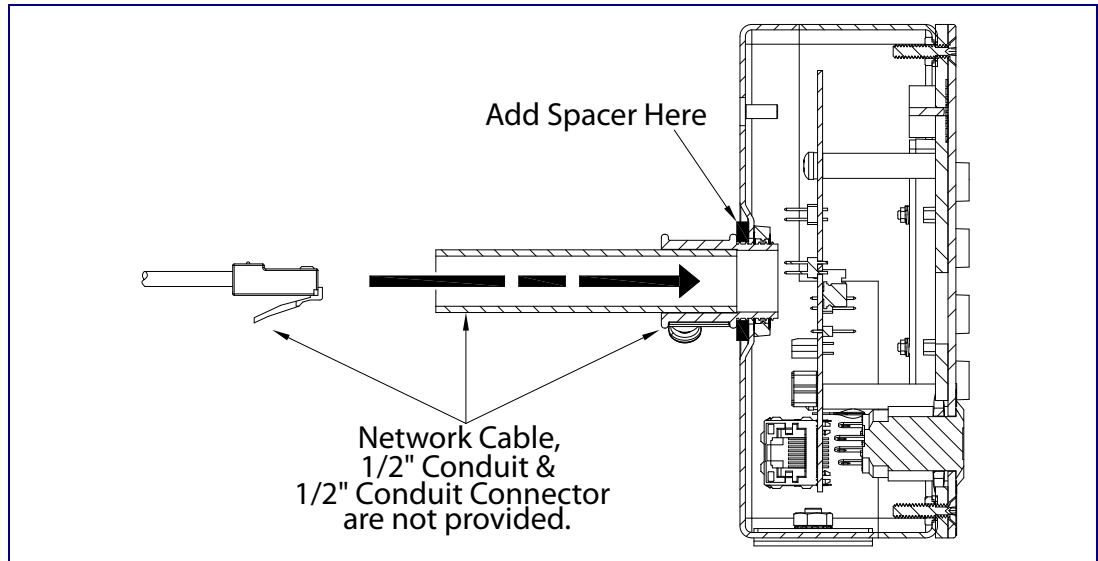


A.4 Network Cable Entry Restrictions

A.4.1 Rear Conduit Network Cable Entry Restrictions (without Shroud)

See [Figure A-4](#) for the rear conduit cable entry restrictions (without Shroud).

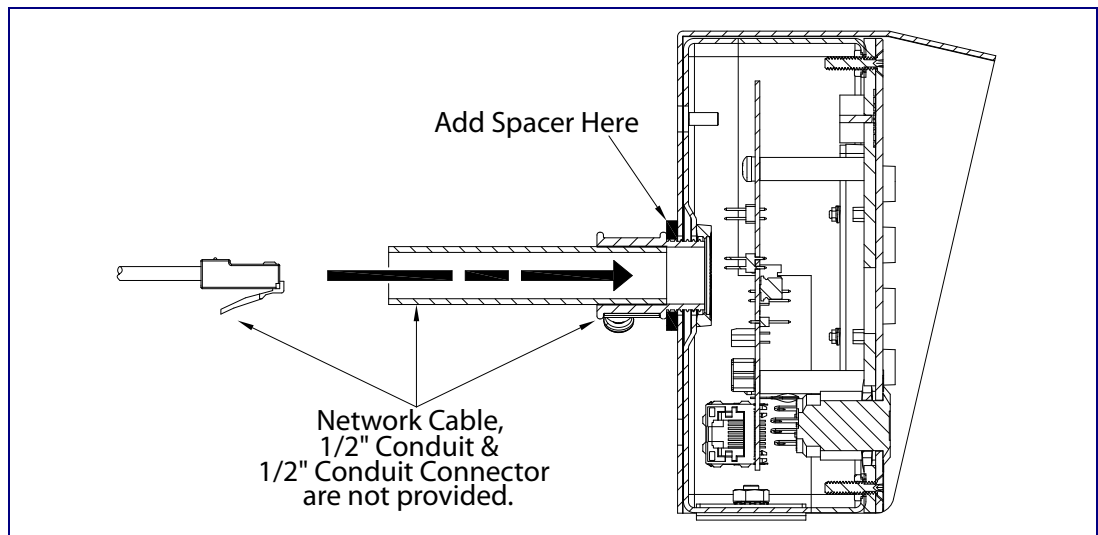
Figure A-4. Rear Conduit Network Cable Entry Restrictions—Without Shroud



A.4.2 Rear Conduit Network Cable Entry Restrictions (with Shroud)

See [Figure A-5](#) for the rear conduit cable entry restrictions (with shroud).

Figure A-5. Rear Conduit Network Cable Entry Restrictions—With Shroud



A.5 Service Loop Cable Routing

Figure A-6 and Figure A-7 illustrate how to route the cables to the Intercom to create a service loop.

Figure A-6. Ground Cable Service Loop Routing

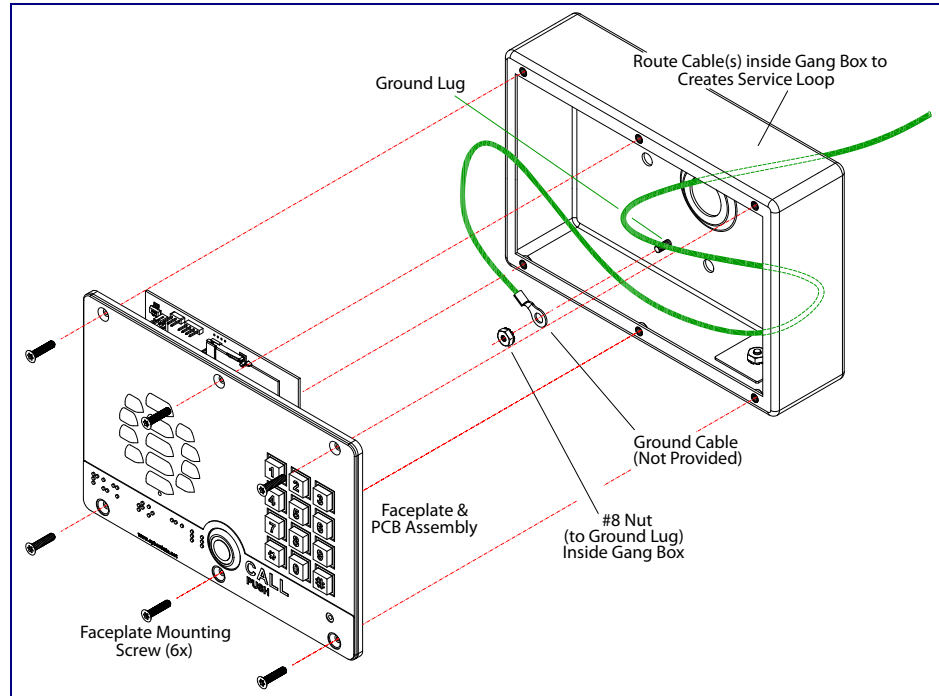
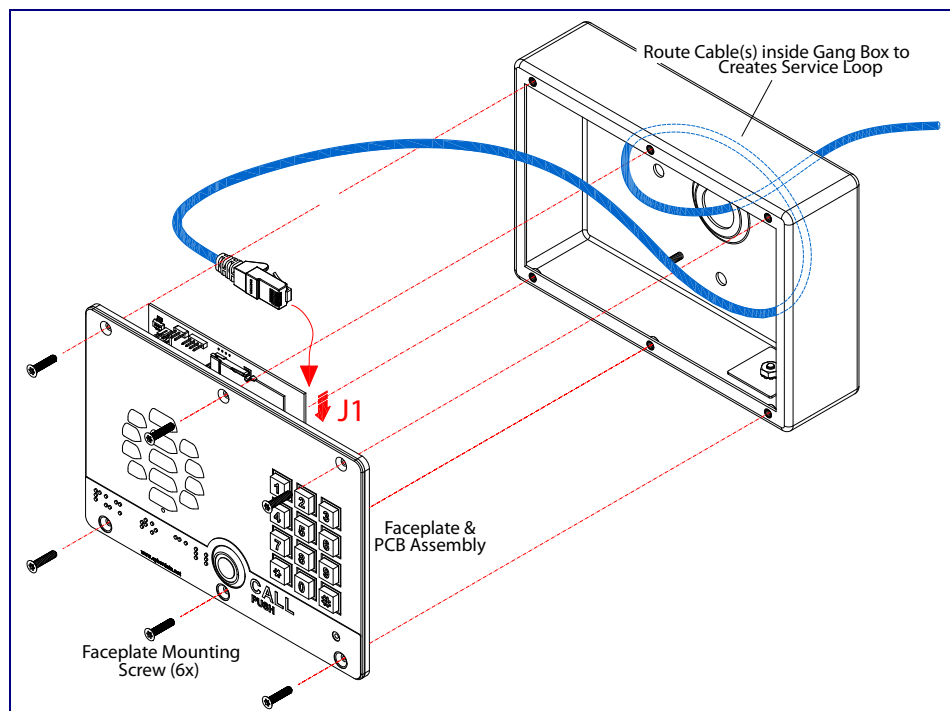


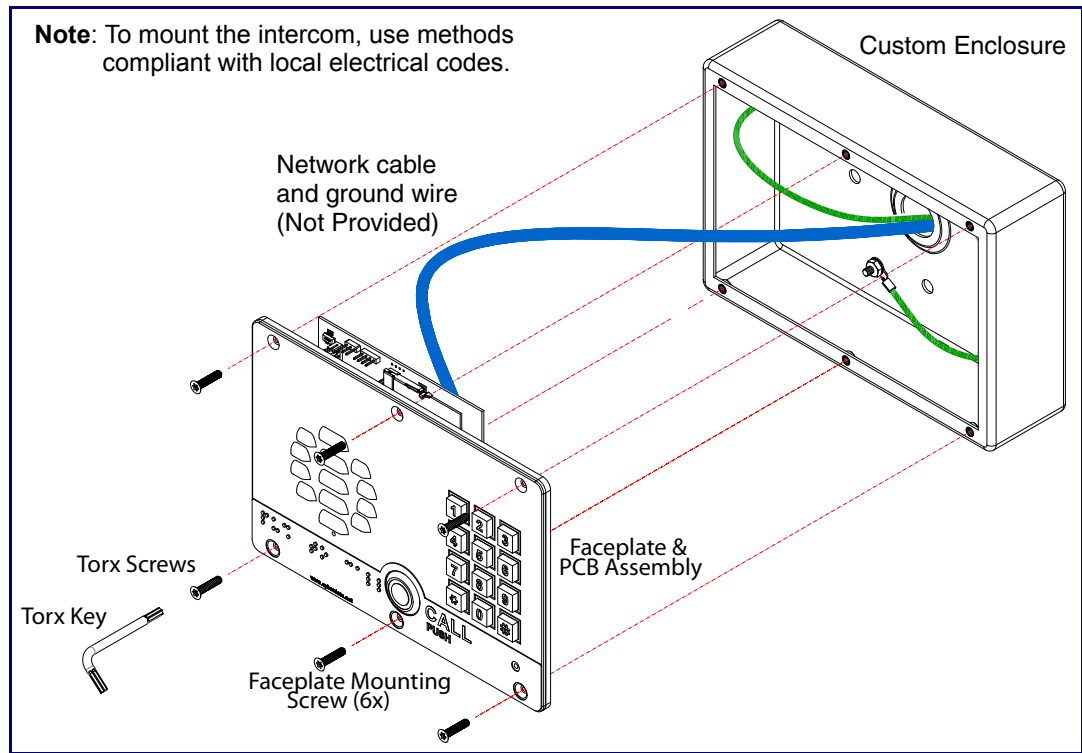
Figure A-7. Network Cable Service Loop Routing



A.6 Securing the Intercom

Use the four Security Torx screws to secure the Intercom. See [Figure A-8](#).

Figure A-8. Securing the Intercom



GENERAL ALERT

Caution

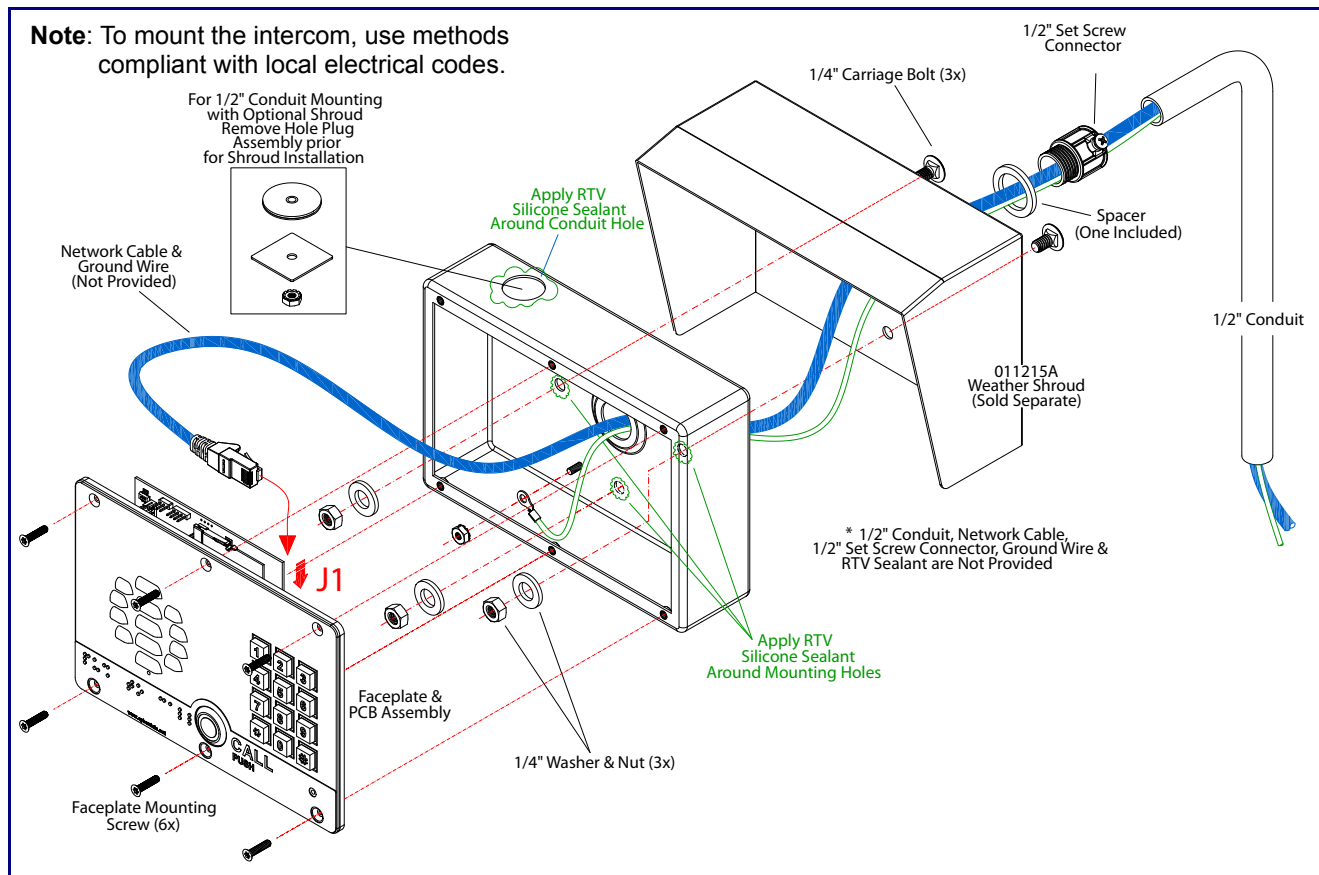
Equipment Hazard: Do not use an electric or power screwdriver to fasten the face plate and PCB assembly to the gang box. To prevent over-torque damage to the gasket, do not apply more than 10 inch-pounds force. Over-torquing will cause the gasket to tear, risk moisture intrusion, and effectively void the manufacturer's warranty.

A.7 Additional Mounting Options

A.7.1 Rear Conduit Mounting Option (Not Provided)

Figure A-9 illustrates a rear conduit mounting option for the VoIP Outdoor Intercom with Keypad.

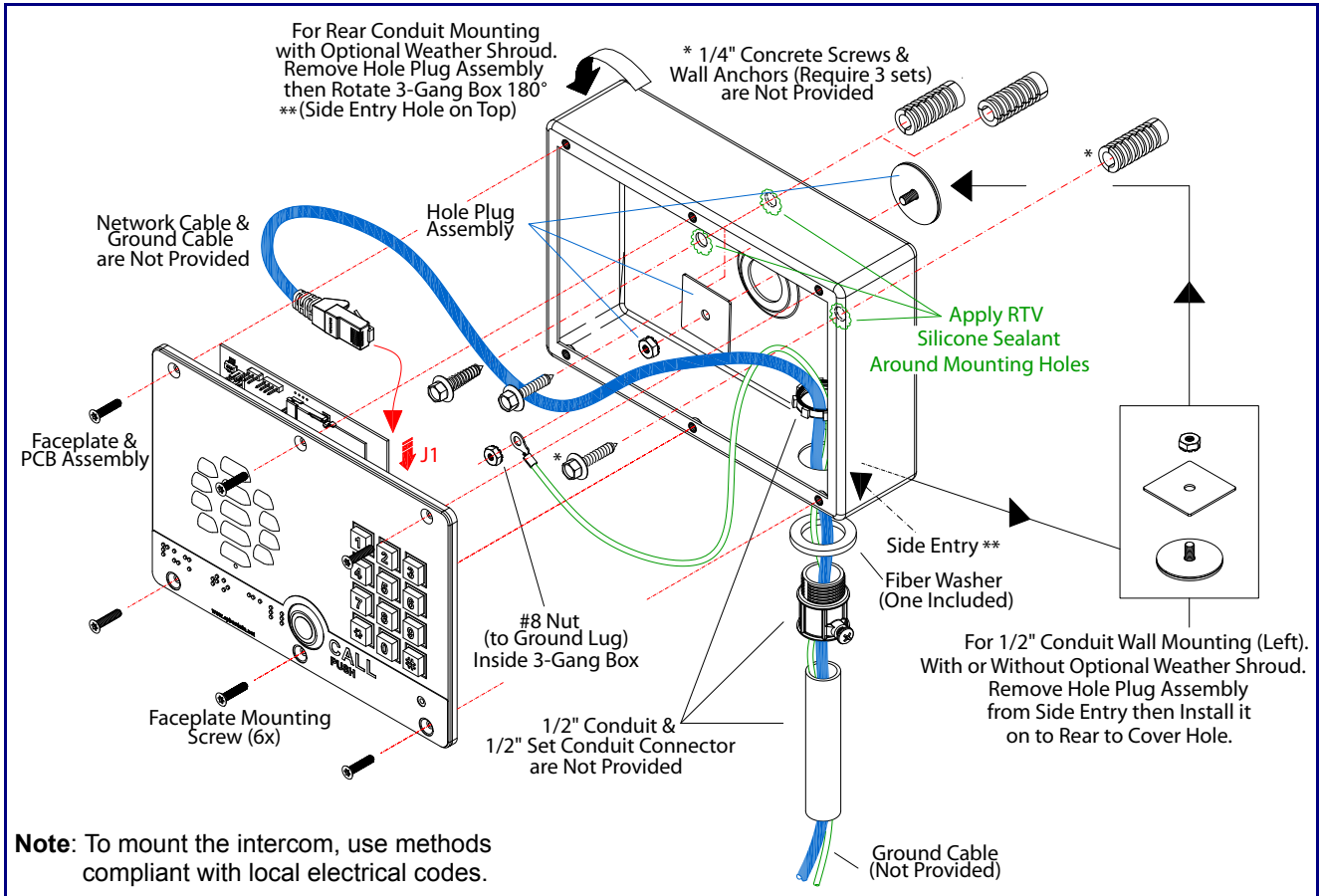
Figure A-9. Optional Rear Conduit Mounting



A.7.2 Concrete Wall Mounting Option (Not Provided)

Figure A-10 illustrates a concrete wall mounting option for the VoIP Outdoor Intercom with Keypad.

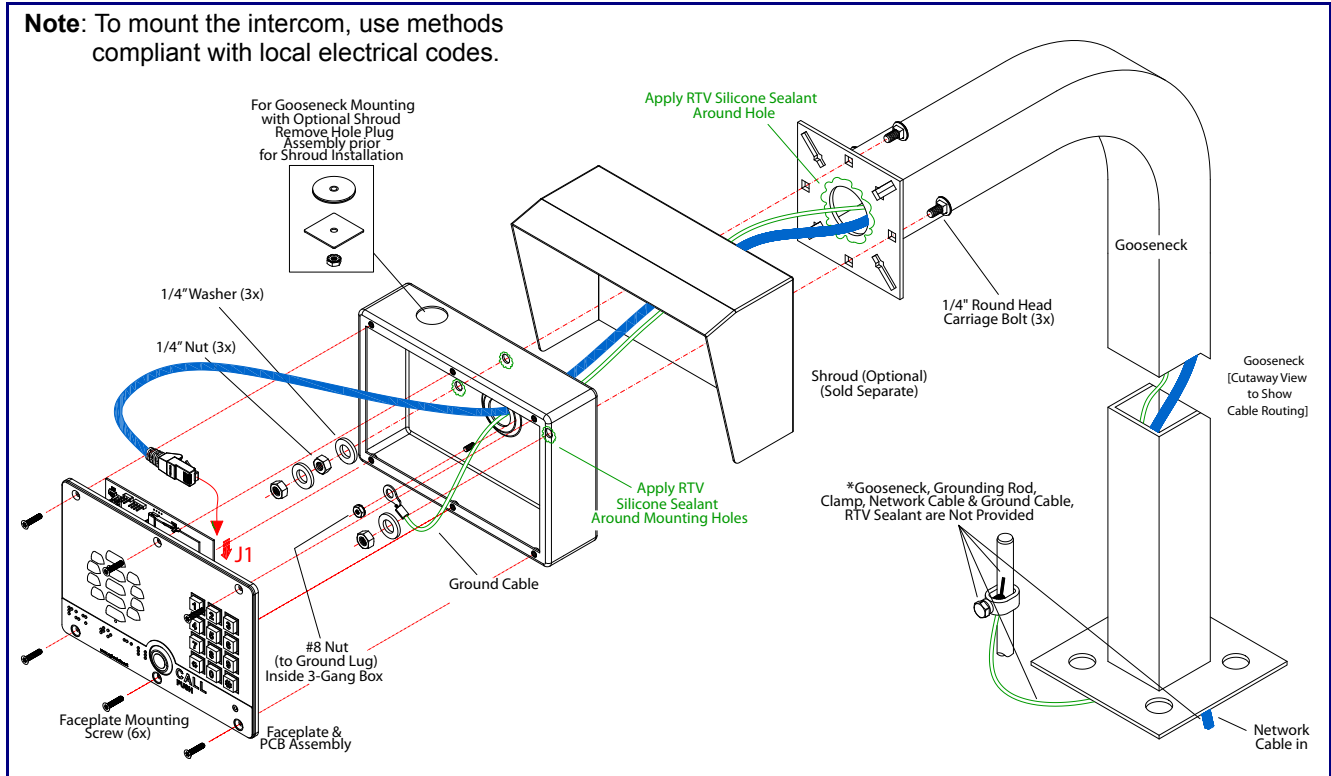
Figure A-10. Optional Concrete Wall Mounting



A.7.3 Goose Neck Mounting Option (Not Provided)

Figure A-11 illustrates a gooseneck mounting option for the VoIP Outdoor Intercom with Keypad.

Figure A-11. Optional Goose Neck Mounting



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/support/voip/solarwinds.html>

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/011214/>

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/011214/>

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 The fastest way to get technical support for your VoIP product is to submit a VoIP Technical
Support 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

16 AWG gauge wire 9

A

activate local relay (door sensor) 71
 activate relay (door sensor) 56
 activate relay (intrusion sensor) 56
 activity LED 18
 address, configuration login 26
 alternative power input 5
 announcing a device's IP address 20
 audio configuration 58
 night ring tone parameter 60
 audio configuration page 58
 audio encodings 4
 audio files, user-created 62
 autoprovision at time (HHMMSS) 79
 autoprovision when idle (in minutes > 10) 79
 autoprovisioning 80
 download template button 80
 autoprovisioning autoupdate (in minutes) 79
 autoprovisioning configuration 78, 79
 autoprovisioning filename 79
 autoprovisioning server (IP Address) 79

B

backup SIP server 1 46
 backup SIP server 2 46
 backup SIP servers, SIP server
 backups 46
 boost (volume) 31

C

call button
 indicator light 8
 call termination 33
 changing
 the web access password 30
 Cisco SRST 46
 command interface 92
 commands 92
 concrete wall mounting option (not provided) 105

conduit mounting option (not provided) 104
 configurable parameters 31, 43, 46, 75
 configuration
 audio 58
 default IP settings 22
 door sensor 54
 intrusion sensor 54
 network 42
 SIP 45
 using Web interface 22
 configuration home page 26
 configuration page
 configurable parameters 31, 43, 75
 contact information 109
 contact information for CyberData 109
 current network settings 43
 CyberData contact information 109

D

default
 gateway 22
 intercom settings 110
 IP address 22
 subnet mask 22
 username and password 22
 web login username and password 26
 default gateway 22, 43
 default intercom settings 21
 default IP settings 22
 default login address 26
 device configuration 30
 device configuration parameters 79
 the device configuration page 78
 device configuration page 30, 38, 39
 device configuration parameters 31
 device configuration password
 changing for web configuration access 30
 DHCP Client 4
 dial mode 39
 dial out call 41
 dial out extension (door sensor) 56, 72
 dial out extension (intrusion sensor) 56
 dial out extension strings 41, 50
 dimensions 5, 97
 shroud dimensions and mounting hole locations 98
 unit dimensions and intrusion sensor range without
 the gang box 99
 unit dimensions—front and side view 97
 unit dimensions—rear view and mounting hole

- locations 97
- discovery utility program 26
- DNS server 43
- door sensor 54, 56, 71
 - activate local relay 71
 - activate relay 56
 - dial out extension 56, 72
 - door open timeout 56, 71
 - door sensor normally closed 56
 - flash button LED 56, 71
 - play audio locally 56, 71
- door strike intermediate relay 13, 15
- download autoprovisioning template button 80
- DTMF
 - play tone during DTMF activation 32
- DTMF push to talk 33
- DTMF tones 41
- DTMF tones (using rfc2833) 41, 50

E

- electric screwdriver 103
- enable night ring events 65
- enable security operation 39
- ethernet I/F 5
- event configuration
 - enable night ring events 65
- expiration time for SIP server lease 47, 48
- export settings 28, 29

F

- factory default settings 21
- fastening, gang box 103
- firmware
 - where to get the latest firmware 89
- flash button LED (door sensor) 56, 71
- flash button LED (intrusion sensor) 56

G

- gang box, fastening 103
- gasket, avoid over-torque damage 103
- get autoprovisioning template 80
- GMT table 36
- GMT time 36
- goose neck mounting option (not provided) 106

H

- home page 26
- http POST command 92
- http web-based configuration 4

I

- identifier names (PST, EDT, IST, MUT) 36
- identifying your product 1
- import settings 28, 29
- import/export settings 28, 29
- indicator light 8
- installation, typical intercom system 2
- intercom configuration
 - default IP settings 22
- intercom configuration page
 - configurable parameters 46
- intrusion sensor 54, 56
 - activate relay 56
 - dial out extension 56
 - flash button LED 56
 - play audio locally 56
- intrusion sensor range 99
- IP address 22, 43
- IP addressing
 - default
 - IP addressing setting 22

J

- J3 terminal block, 16 AWG gauge wire 9

K

- keypad configuration page 38

L

- lease, SIP server expiration time 47, 48
- LED
 - green link LED 18
 - yellow activity LED 18
- lengthy pages 53
- link LED 18
- Linux, setting up a TFTP server on 107
- local SIP port 47
- log in address 26

M

MGROUP

MGROUP Name 52

mounting 96

- additional mounting options 104
- concrete wall mounting option (not provided) 105
- conduit mounting option (not provided) 104
- goose neck mounting option (not provided) 106
- illustration of intercom mounting process 96
- mounting an intercom 96
- mounting components (part of the accessory kit) 96
- network cable entry restrictions 101
- overview of installation types 100
- rear conduit network cable entry restrictions (with shroud) 101
- rear conduit network cable entry restrictions (without shroud) 101
- securing the intercom 103
- service loop cable routing 102

mounting components (part of the accessory kit) 96

multicast configuration 58

Multicast IP Address 52

N

navigation (web page) 23

navigation table 23

network cable entry restrictions 101

network configuration of intercom 42

Network Setup 42

nightring tones 53

Nightringer 9, 88

nightringer settings 47

NTP server 31, 32

O

on-board relay 11

on-board relay, 1A at 30 VDC 5

operating temperature 5

output 5

overview of installation types 100

P

packet time 4

pages (lengthy) 53

part number 5

parts list 6

password

- for SIP server login 46

- login 26

- restoring the default 22

payload types 5

play audio locally (door sensor) 56, 71

play audio locally (intrusion sensor) 56

play tone during DTMF activation 32

point-to-point configuration 50

polycom default channel 52

polycom emergency channel 52

polycom priority channel 52

port

- local SIP 47

- remote SIP 47

posix timezone string

- timezone string 32

POST command 92

power input 5

- alternative 5

power screwdriver 103

priority

- assigning 53

product

- configuring 22

- parts list 6

product features 3

product overview

- product features 3

- product specifications 5

- supported protocols 4

- supported SIP servers 4

- typical system installation 2

product specifications 5

protocol 5

protocols supported 4

push to talk, DTMF 33

R

rear conduit network cable entry restrictions (with shroud) 101

rear conduit network cable entry restrictions (without shroud) 101

reboot 90, 91

remote SIP port 47

reset test function management button 19

resetting the IP address to the default 96

restoring factory default settings 21, 110

ringtones 53

- lengthy pages 53

RJ-45 17

rport discovery setting, disabling 47

RTFM button 19

RTFM jumper 19, 20, 21
RTP/AVP 4

S

sales 109
securing the intercom 103
security code 41
security mode settings 39
sensor setup page 55, 70
sensor setup parameters 54
sensors 56, 71
server address, SIP 46
service 109
service loop cable routing 102
set time with external NTP server on boot 31
setting up the device 9
settings, default 21
shroud dimensions and mounting hole locations 98
SIP
 enable SIP operation 46
 local SIP port 47
 user ID 46
SIP (session initiation protocol) 4
SIP configuration 45
 SIP Server 46
SIP configuration parameters
 outbound proxy 47, 48
 registration and expiration, SIP server lease 47, 48
 unregister on reboot 47
 user ID, SIP 46
SIP registration 46
SIP remote SIP port 47
SIP server 46
 password for login 46
 SIP servers supported 4
 unregister from 47
 user ID for login 46
SIP volume 31
speaker output 5
SRST 46
subnet mask 22, 43
supported protocols 4

T

tech support 109
technical support, contact information 109
terminal block, 16 AWG gauge wire 9
TFTP server 4, 107
time zone string examples 36
triggering a dial out call or security code 41

U

unit dimensions and intrusion sensor range without the
 gang box 99
unit dimensions—front and side view 97
unit dimensions—rear view and mounting hole
 locations 97
upgrading to firmware 6.x.x from 5.x.x 103
user ID
 for SIP server login 46
username
 changing for web configuration access 30
 default for web configuration access 26
 restoring the default 22

V

VLAN ID 43
VLAN Priority 43
VLAN tagging support 43
VLAN tags 43
volume
 microphone gain 31
 multicast volume 31
 push to talk volume 31
 ring volume 31
 sensor volume 31
 SIP volume 31
volume boost 31

W

warranty policy at CyberData 109
web access password 22
web access username 22
web configuration log in address 26
web page
 navigation 23
web page navigation 23
web-based intercom configuration 22
weight 5
wget, free unix utility 92
Windows, setting up a TFTP server on 107
wiring the circuit 12
 devices less than 1A at 30 VDC 12