



SIP-enabled h.264 Video Outdoor Intercom Operations Guide

Part #011410
Document Part #931334B
for Firmware Version 1.0.0

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

SIP-enabled h.264 Video Outdoor Intercom Operations Guide 931334B
Part # 011410

COPYRIGHT NOTICE:

© 2017, 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.

Revision Information

Revision 931334B, which corresponds to firmware version 1.0.0, was released on May 1, 2017, and has the following changes:



- Updates [Section 1.3, "Product Features"](#)
- Updates [Figure 2-5, "Field of View"](#)
- Updates [Section 2.6, "Upgrade the Firmware"](#)
- Adds [Section 2.7, "Reboot the Device"](#)

Browsers Supported

The following browsers have been tested against firmware version 1.0.0:

- Internet Explorer (version: 10)
- Firefox (also called Mozilla Firefox) (version: 52.02)
- Chrome (version 570.2987.98)
- Opera (version 12.16)
- Safari (version: 5.1.7)

Pictorial Alert Icons

 <p>GENERAL ALERT</p>	General Alert 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.
	Ground This pictorial alert indicates the Earth grounding connection point.

Hazard Levels

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

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

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


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


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


Important Safety Instructions

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

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

 <p>GENERAL ALERT</p>	<p>Warning <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 <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 The PoE connector is intended for intra-building connections only and does not route to the outside plant.</p>
--	--

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
Chapter 2 Installing the SIP-enabled h.264 Video Outdoor Intercom	6
2.1 Parts List	6
2.2 Intercom Components	7
2.3 Intercom Setup	8
2.3.1 Mechanical Adjustment	8
2.3.2 Field of View	11
2.3.3 Intercom Connections	12
2.3.4 Using the On-Board Relay	14
2.3.5 Wiring the Circuit	15
2.3.6 Intercom Connectors	16
2.3.7 Activity and Link LEDs	20
2.3.8 RTFM Button	21
2.3.9 Adjusting the Intercom Volume	23
2.3.10 Call Button and the Call Button LED	24
2.4 Configure the Intercom Parameters	25
2.4.1 Factory Default Settings	25
2.4.2 Intercom Web Page Navigation	26
2.4.3 Using the Toggle Help Button	27
2.4.4 Log in to the Home Page	29
2.4.5 Configure the Device	33
2.4.6 Configure the Video Parameters	38
2.4.7 Configure the Network Parameters	41
2.4.8 Configure the SIP (Session Initiation Protocol) Parameters	44
2.4.9 Configure the Multicast Parameters	50
2.4.10 Configure the Sensor Parameters	54
2.4.11 Configure the Audio Parameters	58
2.4.12 Configure the Events Parameters	64
2.4.13 Configure the Autoprovisioning Parameters	70
2.5 Upgrade the Firmware and Reboot the Intercom	82
2.5.1 Downloading the Firmware	82
2.6 Upgrade the Firmware	84
2.7 Reboot the Device	87
2.8 Command Interface	88
2.8.1 Command Interface Post Commands	88
Appendix A Mounting the Intercom	92
A.1 Mounting Components	92
A.2 Dimensions	93
A.3 Overview of Installation Types	95
A.4 Network Cable Entry Restrictions	96
A.4.1 Conduit Mounting Restrictions (Side Entry)	96
A.4.2 Conduit Mounting Restrictions (Rear Entry without Shroud)	97
A.4.3 Conduit Mounting Restrictions (Rear Entry with Shroud)	97
A.5 Service Loop Cable Routing	98
A.6 Securing the Intercom	99
A.7 Additional Mounting Options	100
A.7.1 Conduit Mounting Option (Not Provided)	100
A.7.2 Conduit to Gang Box Installation	101
A.7.3 Gooseneck Mounting Option (Not Provided)	102
A.7.4 Ground Cable Installation for Gooseneck Mounting Option	103

Appendix B Setting up a TFTP Server	104
B.1 Set up a TFTP Server	104
B.1.1 In a LINUX Environment	104
B.1.2 In a Windows Environment	104
Appendix C Troubleshooting/Technical Support	105
C.1 Frequently Asked Questions (FAQ)	105
C.2 Documentation	105
C.3 Contact Information	106
C.4 Warranty and RMA Information	106
Index	107

1 Product Overview

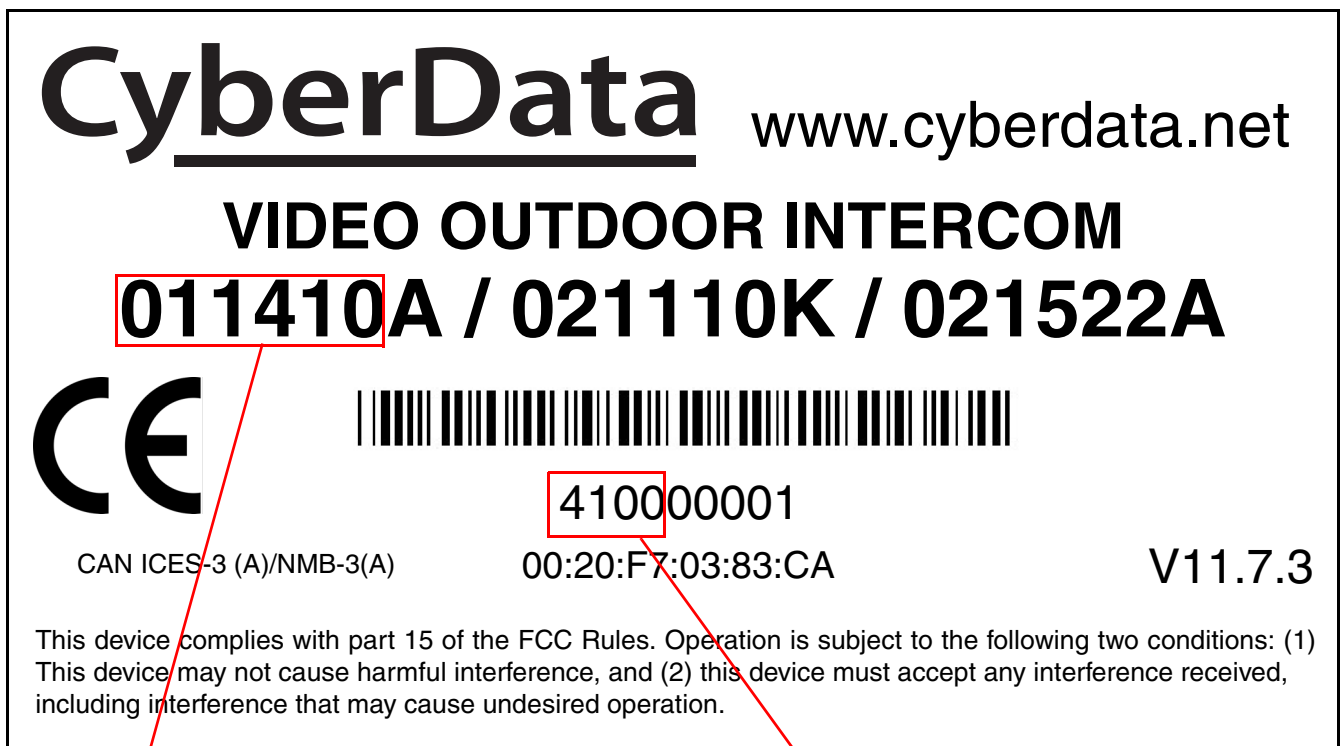
1.1 How to Identify This Product

To identify the SIP-enabled h.264 Video Outdoor Intercom, 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 **011410**.
- The serial number on the label should begin with **410**.

Figure 1-1. Model Number Label



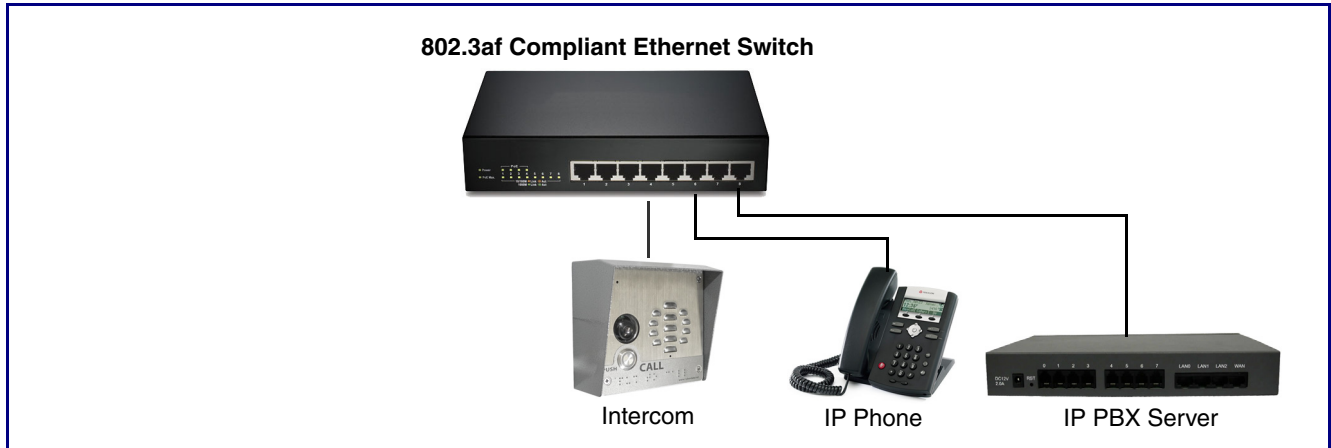
Model number

Serial number begins with **410**

1.2 Typical System Installation

The following figures illustrate how the SIP-enabled h.264 Video Outdoor Intercom can be installed as part of a VoIP phone system.

Figure 1-2. Typical Installation



1.3 Product Features

The SIP-enabled h.264 Video Outdoor Intercom has the following features:

- PoE 802.3af enabled (Powered-over-Ethernet)
- SIP compliant
- Adjustable camera angle
- Full-duplex voice operation
- Supports SRST (Survivable Remote Site Telephony) in a Cisco environment
- Network web management
- Network adjustable speaker volume and microphone sensitivity
- Network downloadable firmware
- Doubles as a paging speaker
- Dry relay contact for auxiliary control (controls external power)
- Door closure and tamper alert signal
- Optional Weather Shroud for even greater weather protection
- IP65 rated enclosure
- Conformal coated PCBA
- Optional Security Torx screws with driver kit
- Downloadable alert, ringtones and callout messages

1.4 Supported Protocols

The Intercom supports the following protocols:

- SIP (session initiation protocol)
- 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
- Facilitates autoprovisioning configuration values on boot
- 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

Specifications	
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
SIP Video Payload	Baseline profile @ 320x240
Video Lens Angle	72 degrees
Dimensions ^b	5.118 inches [130 mm] Length 2.252 inches [57.21 mm] Width 5.118 inches [130 mm] Height
Weight	2.0 lbs. (0.90 kg)
Boxed Weight	3.0 lbs. (1.36 kg)
Part Number	011410 011188 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.

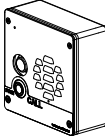


2 Installing the SIP-enabled h.264 Video Outdoor Intercom

2.1 Parts List

Table 2-1 illustrates the SIP-enabled h.264 Video Outdoor Intercom parts.

Note See Appendix A, "Mounting the Intercom" for physical mounting information.

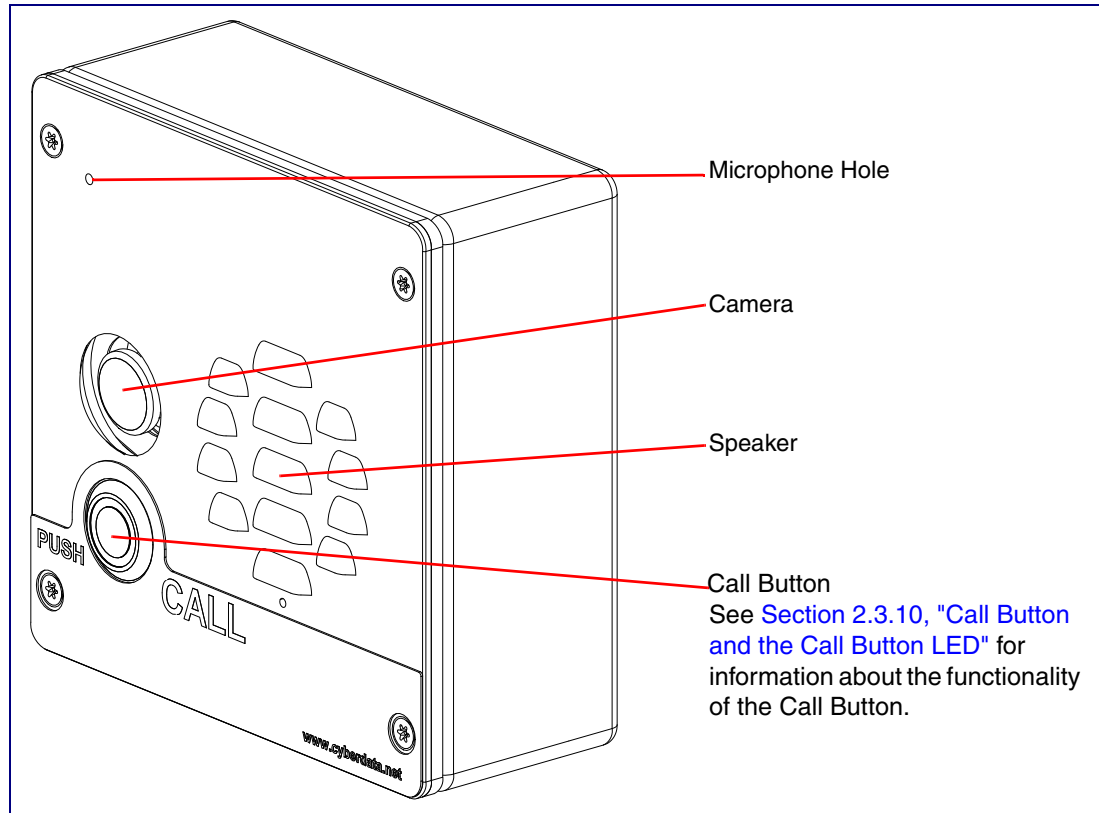
Table 2-1. Parts List

Quantity	Part Name	Illustration
1	Intercom Assembly	
1	Installation Quick Reference Guide	
1	Intercom Mounting Accessory Kit	

2.2 Intercom Components

Figure 2-1 shows the components of the Intercom.

Figure 2-1. Intercom Components



2.3 Intercom Setup

2.3.1 Mechanical Adjustment

The SIP-enabled h.264 Video Outdoor Intercom has a mechanical adjustment that ships in the default position of 0 degrees horizontal (Figure 2-2), but it allows you to tilt it 15 degrees down or 15 degrees up as shown in Figure 2-3 and Figure 2-4.

Figure 2-2. Mechanical Adjustment at 0 degrees horizontal

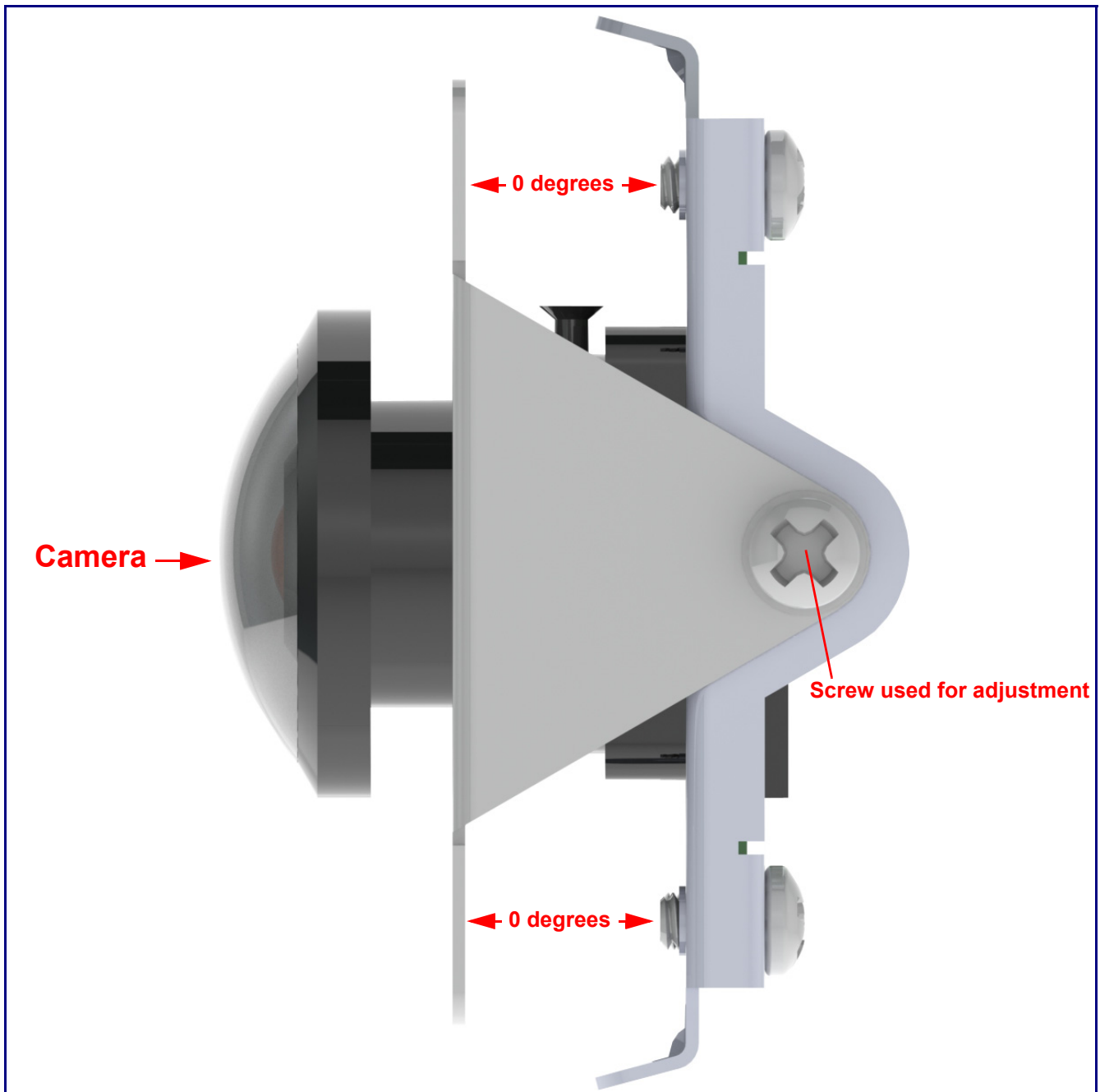


Figure 2-3. Mechanical Adjustment at 15 Degree Angle

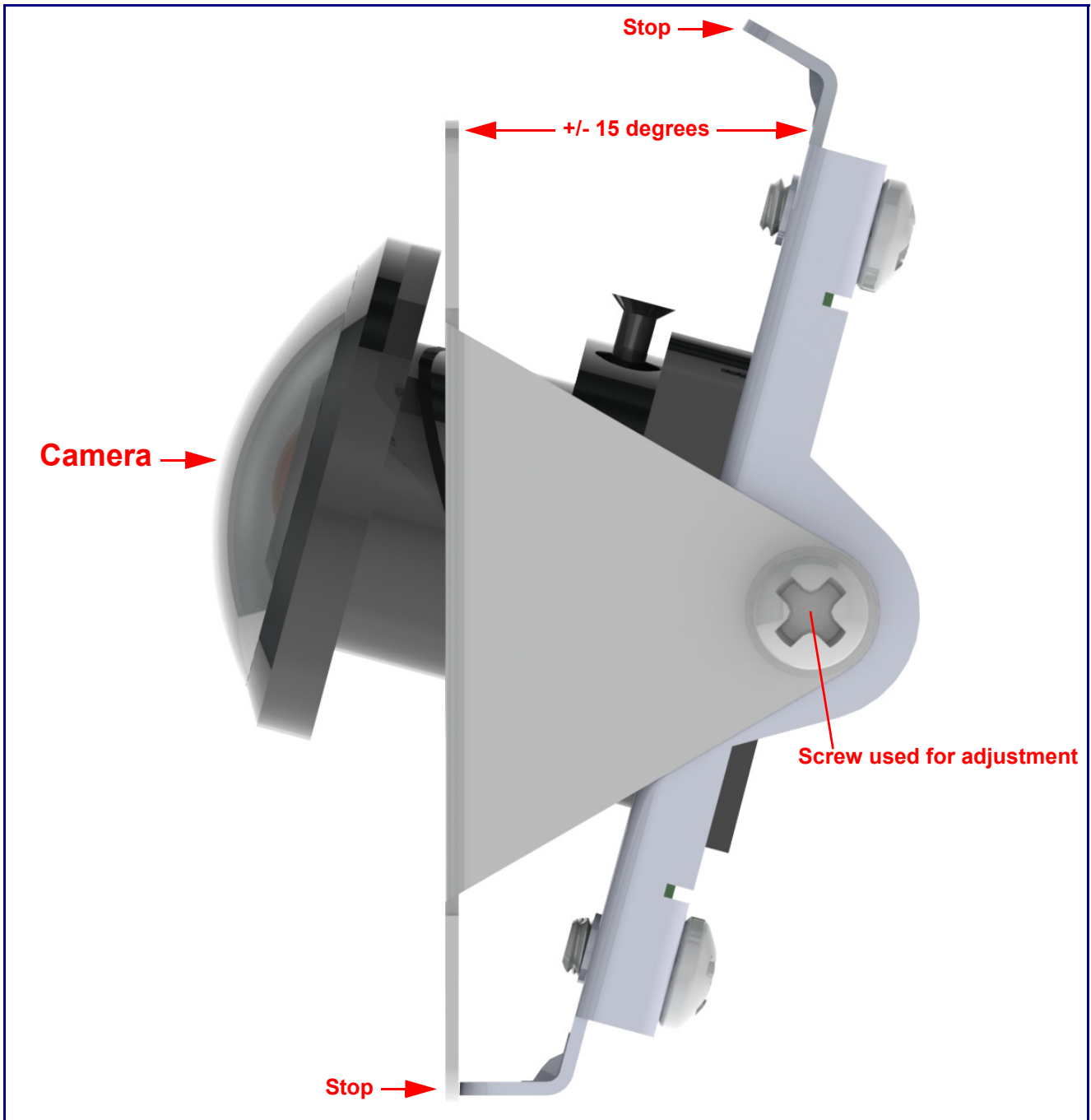
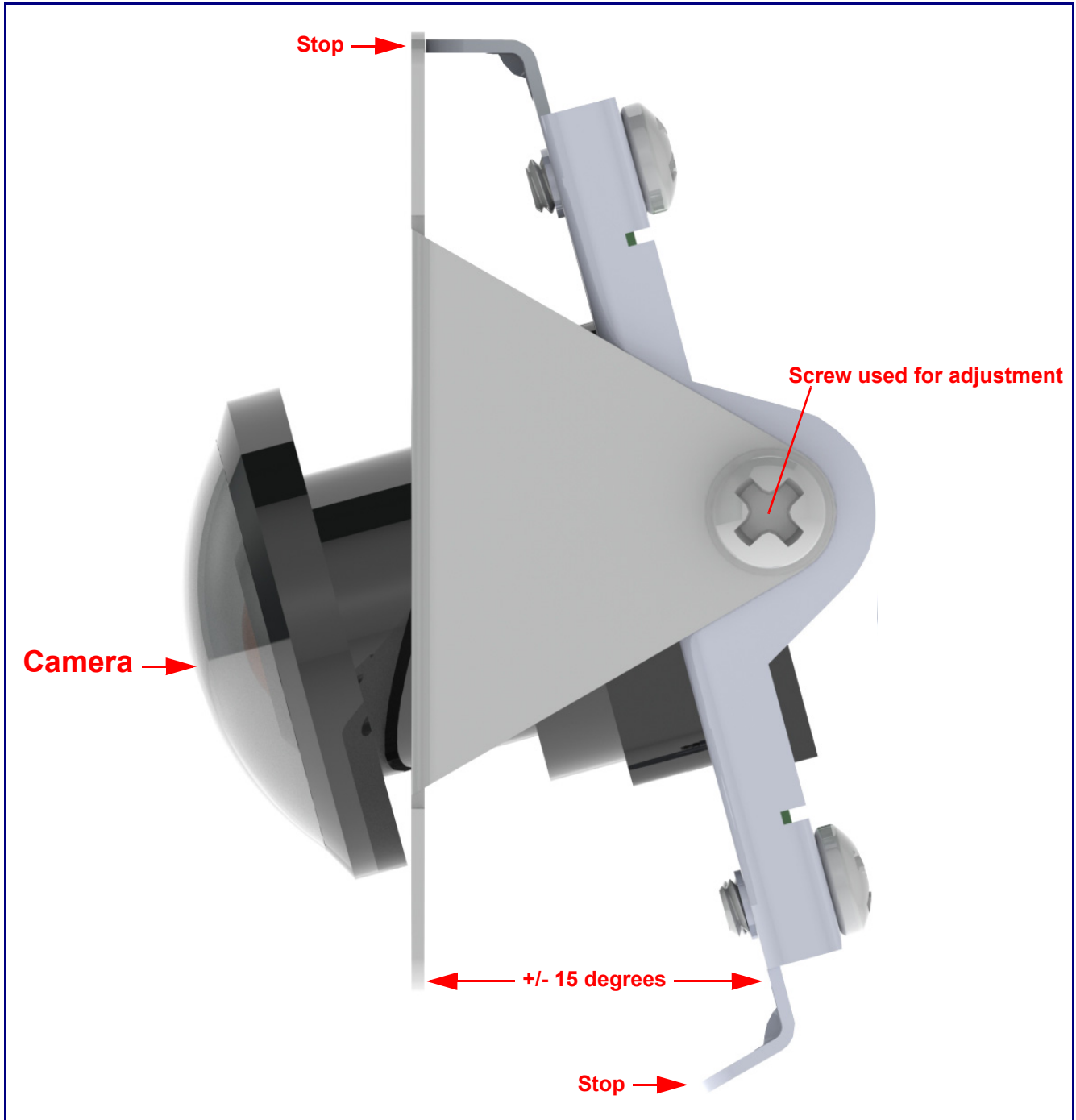


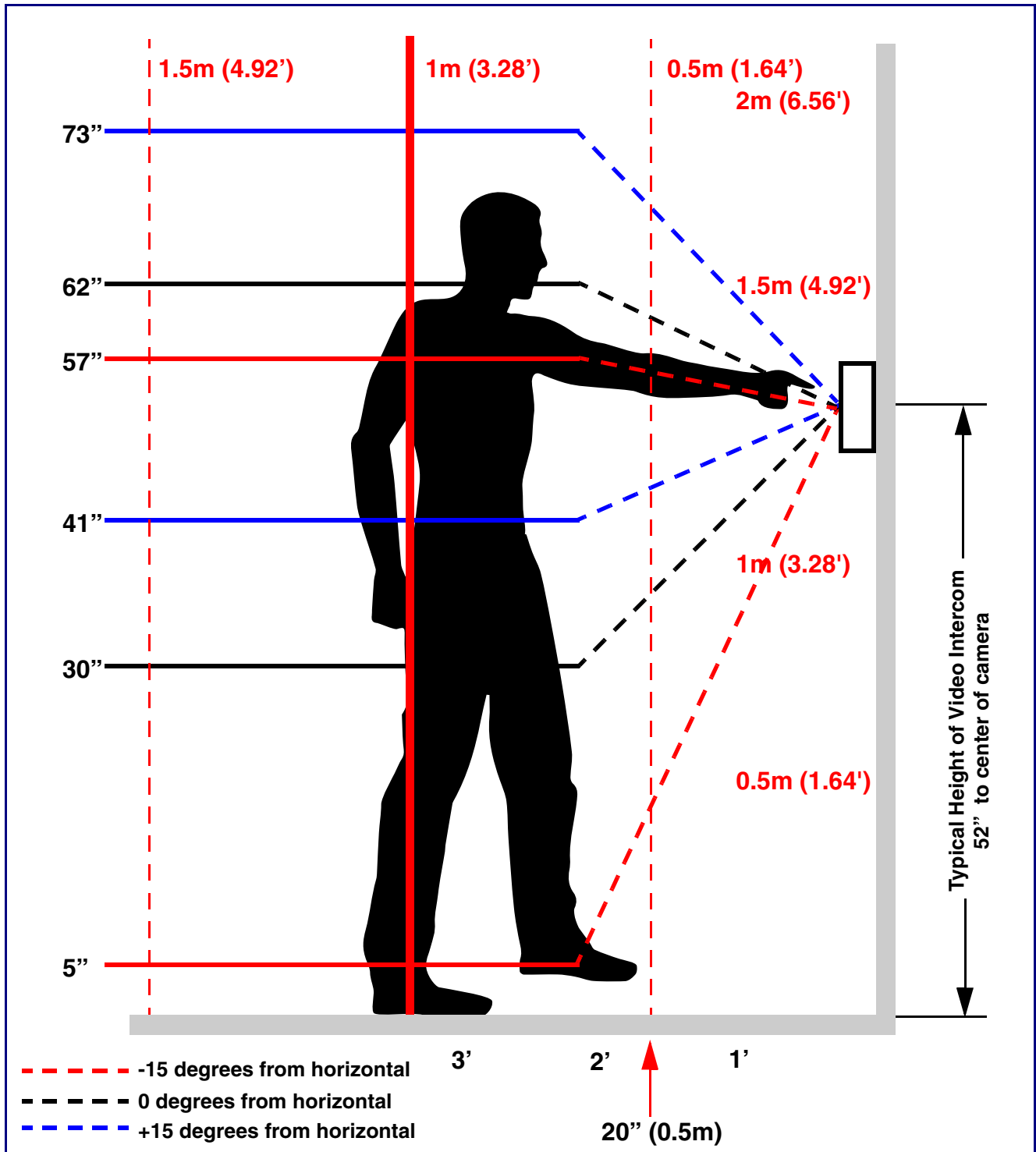
Figure 2-4. Mechanical Adjustment at 15 Degree Angle



2.3.2 Field of View

Figure 2-5 shows the field of view of the SIP-enabled h.264 Video Outdoor Intercom when it is mounted at the recommended 48 to 52 inches above the ground.

Figure 2-5. Field of View



2.3.3 Intercom Connections

Figure 2-6 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.



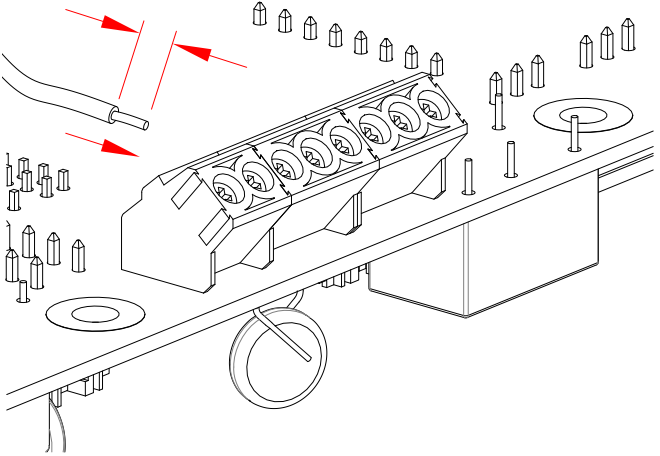
	<p>Caution</p> <p><i>Equipment Hazard:</i> Contacts 1 and 2 on the terminal block are only for powering the device from a non-PoE 12 VDC power source as an alternative to Network PoE power. Use of these contacts for any other purpose will damage the device and void the product warranty.</p>
---	--

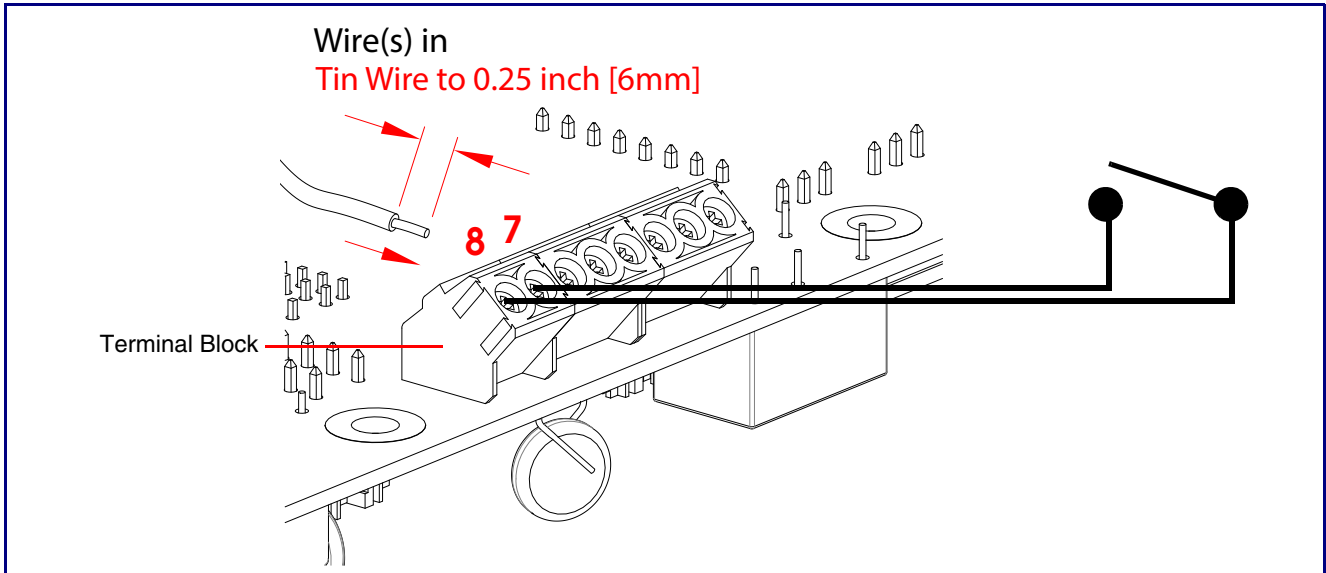
Figure 2-6. Intercom Connections

<p>Alternate Power Input: 1 = +8 to +12VDC @ 1000mA Regulated Power Supply* 2 = Power Ground*</p>	<p>Terminal block can accept up to 16 AWG wire. Tool required for terminal block screw: Size #00 Phillip Drive Screwdriver</p>
	<p>Wire(s) in Tin Wire to 0.25 inch [6mm]</p>
<p>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"</p>	
<p>*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.</p>	




2.3.3.1 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 2-7. Remote Switch Connection



2.3.4 Using the On-Board Relay

 <p>GENERAL ALERT</p>	<p>Warning <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 <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.</p>
 <p>GENERAL ALERT</p>	<p>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.</p>

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 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# 011269) (see [Section](#) , "If you have questions about connecting door strikes or setting up the web configurable options, please contact our support department at the following [website](#):").

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 Page](#) on the web interface.

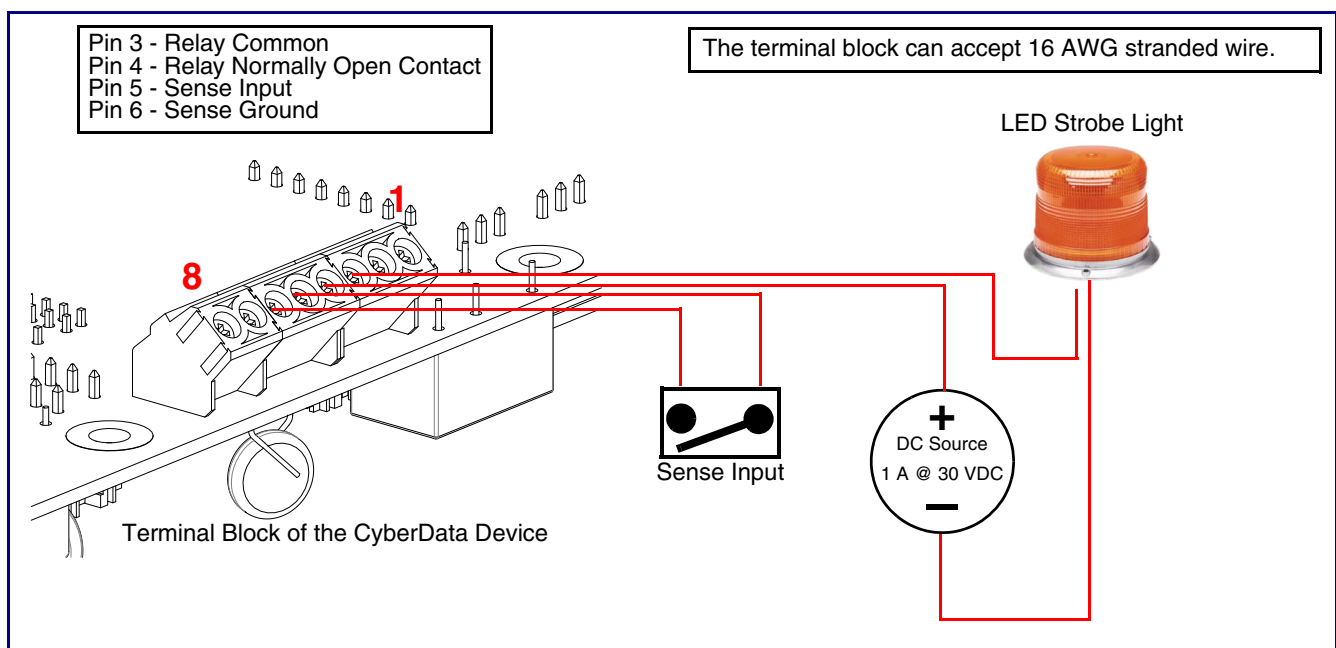
2.3.5 Wiring the Circuit

2.3.5.1 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 2-8](#) 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](#) , "If you have questions about connecting door strikes or setting up the web configurable options, please contact our support department at the following [website](#):").

Figure 2-8. Devices Less than 1A at 30 VDC



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/>

2.3.6 Intercom Connectors

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

Figure 2-9. Connector Locations

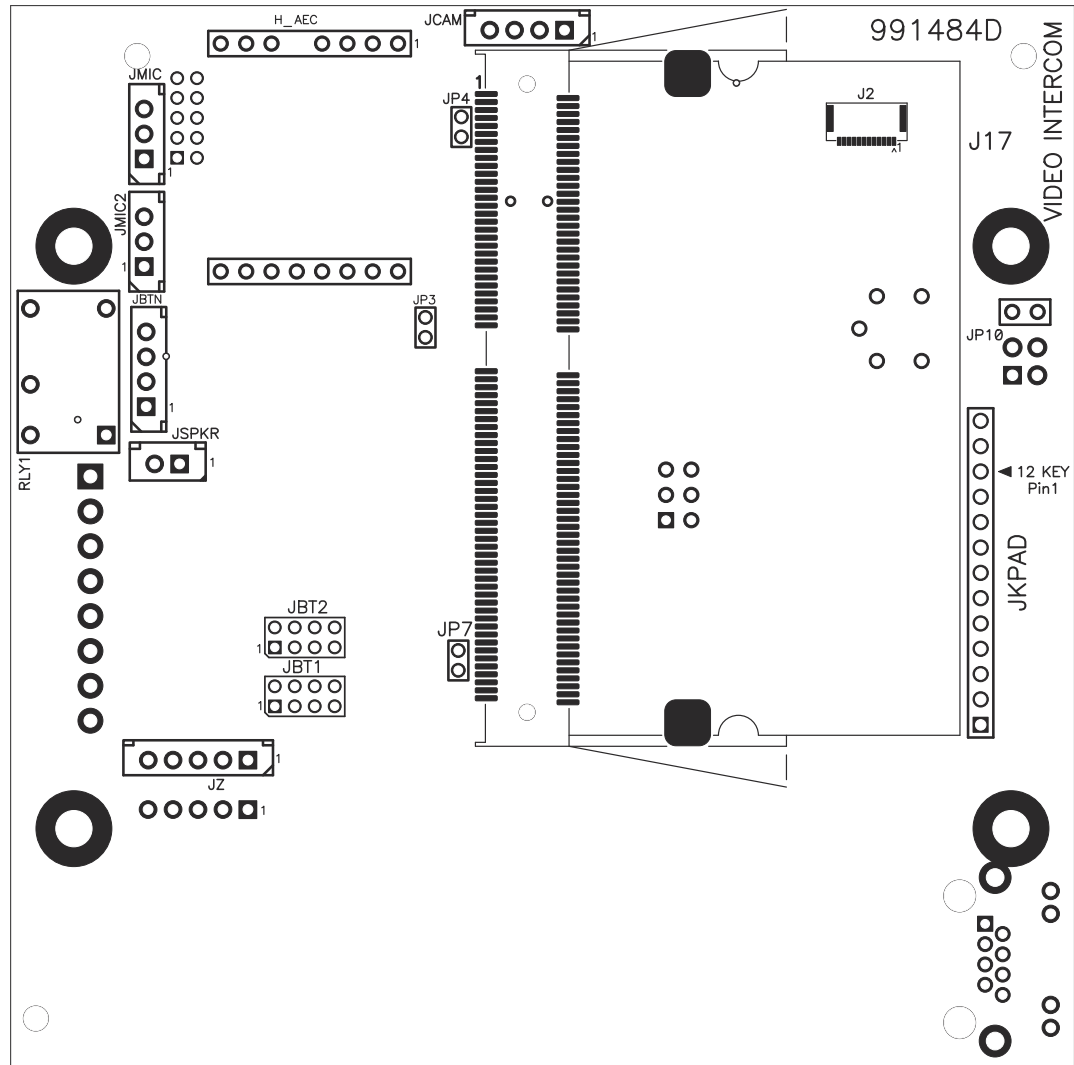


Table 2-2. Connector Functions

Connector	Function
JCAM	Camera Interface
H_AEC	Echo Cancellation Interface
JBTN	Call Button LED Interface
JMIC	Microphone Interface
JMIC2	Second Microphone Interface — Not Used
JSPKR	Speaker Interface
JKPAD	Keypad Interface — Not Used
JY	Sensor Interface — Not Used
JP3	Audio Mute — Factory Use Only
JP4	Boot from mSD Card — Factory Use Only
JP7	EPROM Write Protect — Factory Use Only
JP10	Disables the intrusion sensor when installed.
J17	Sitara Card Interface — Factory Use Only
JBT1	Touch Button -1 Interface — Not Used
JBT2	Touch Button -2 Interface — Not Used

Figure 2-10. Connector Locations

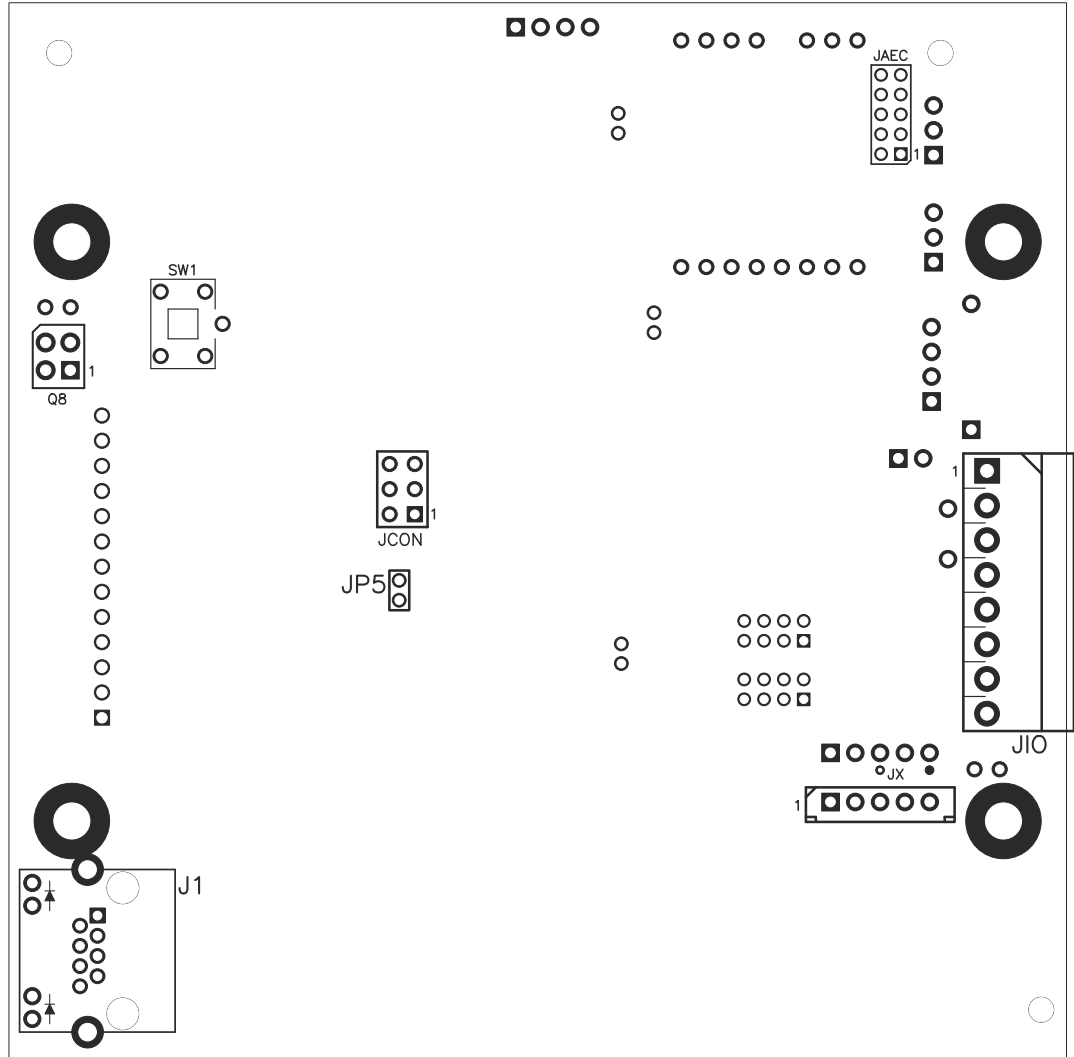


Table 2-3. Connector Functions

Connector	Function
J1	PoE Network Connection (RJ-45 ethernet)
JP5	Reset jumper ^a
JX	Auxiliary Strobe Interface
Q8	Intrusion Detector
JAEC	AEC Configuration Interface — Factory Use Only
JIO	Terminal Block (see Figure 2-6)
JCON	Console Port — Factory Use Only
JSPI	Reserved — Factory Use Only
SW1	See Section 2.3.8, "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.

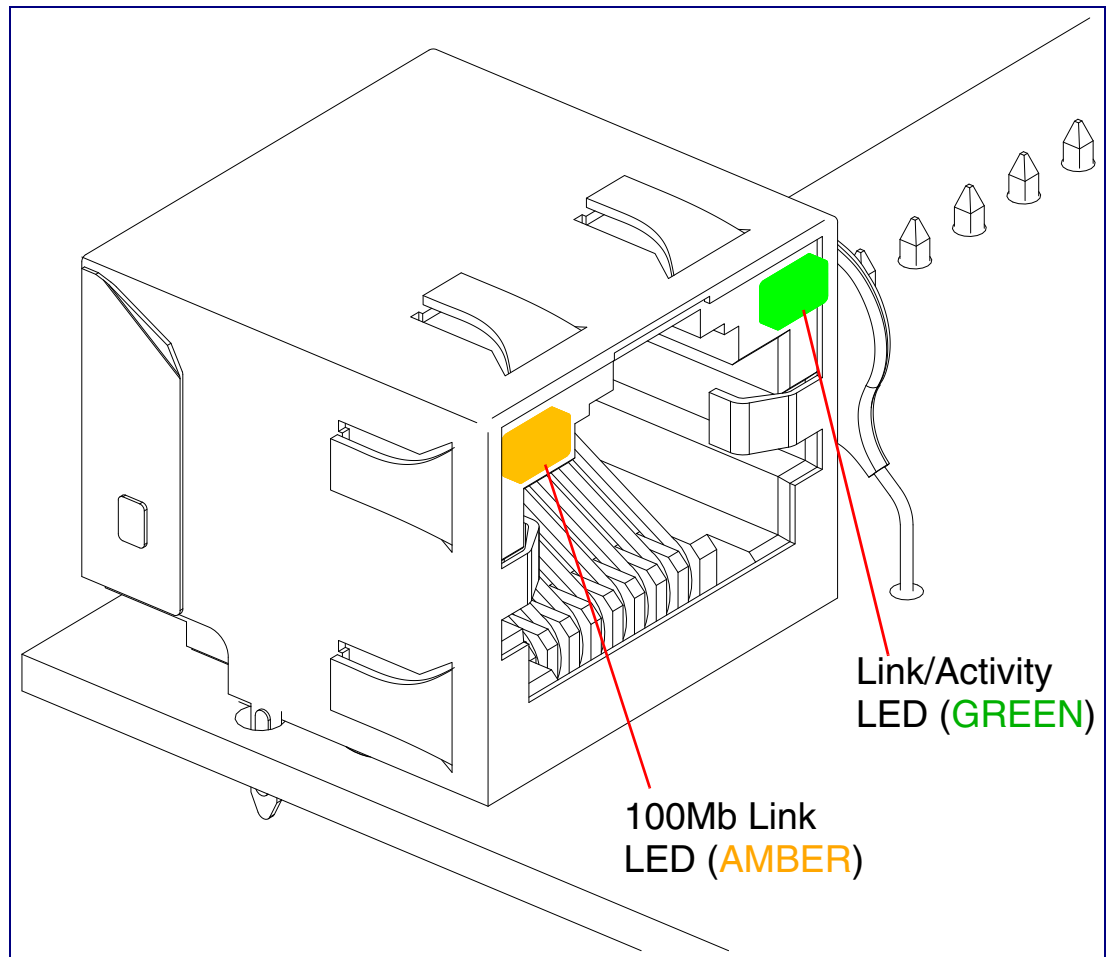
2.3.7 Activity and Link LEDs

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

Figure 2-11. Activity and Link LED

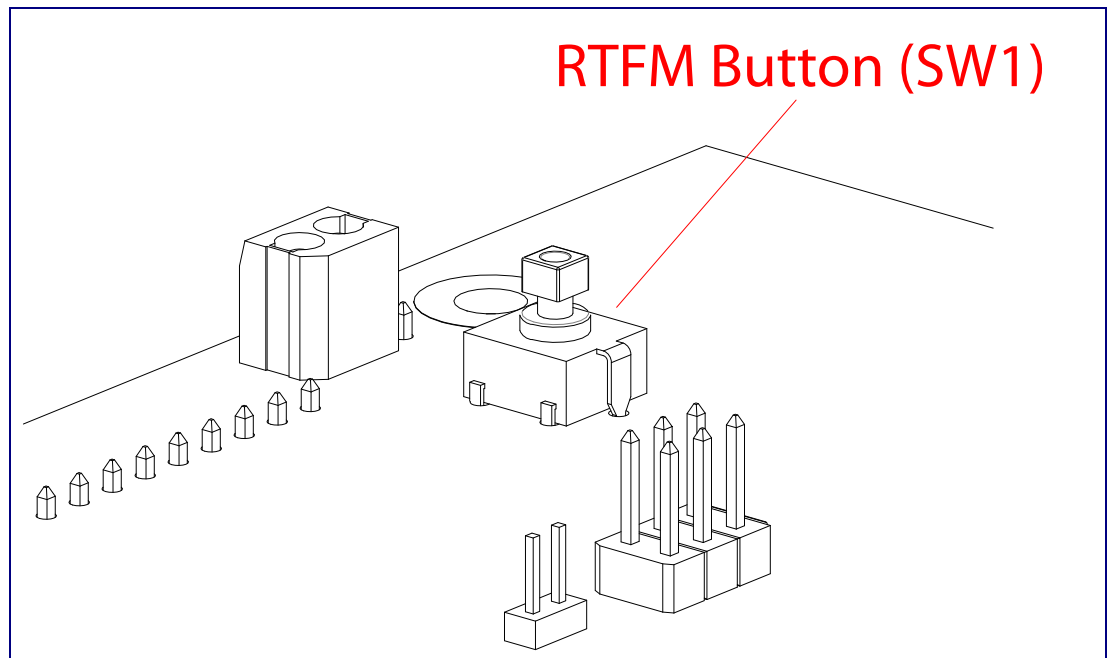


2.3.8 RTFM Button

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



2.3.8.1 Announcing the IP Address

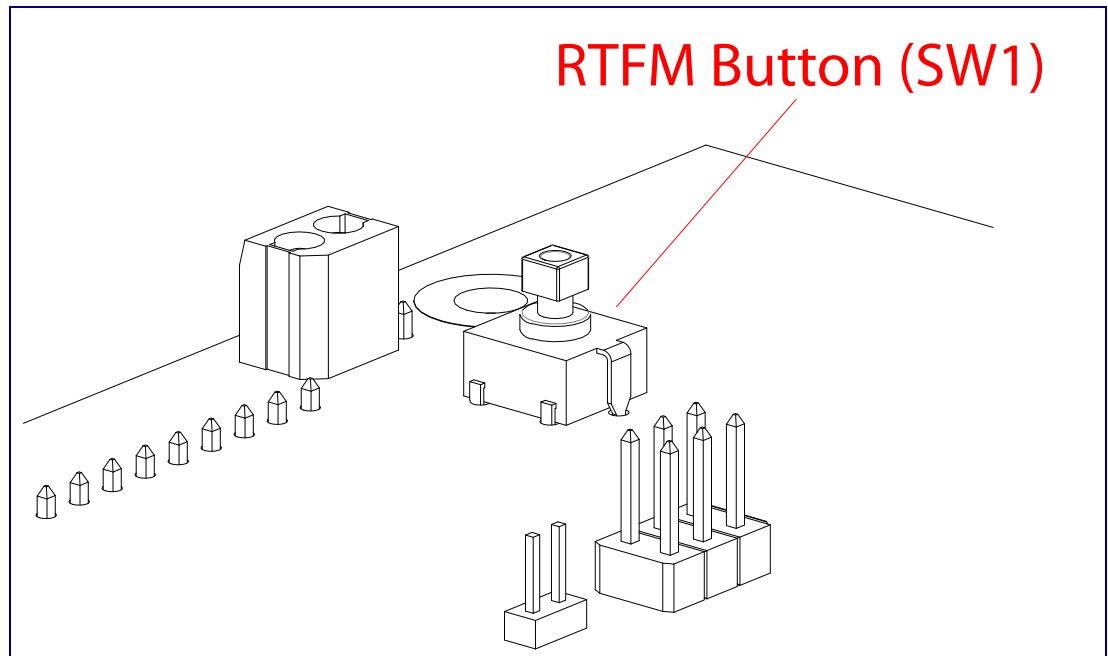
To announce a device's current IP address:

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



2.3.8.2 Restoring the Factory Default Settings

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

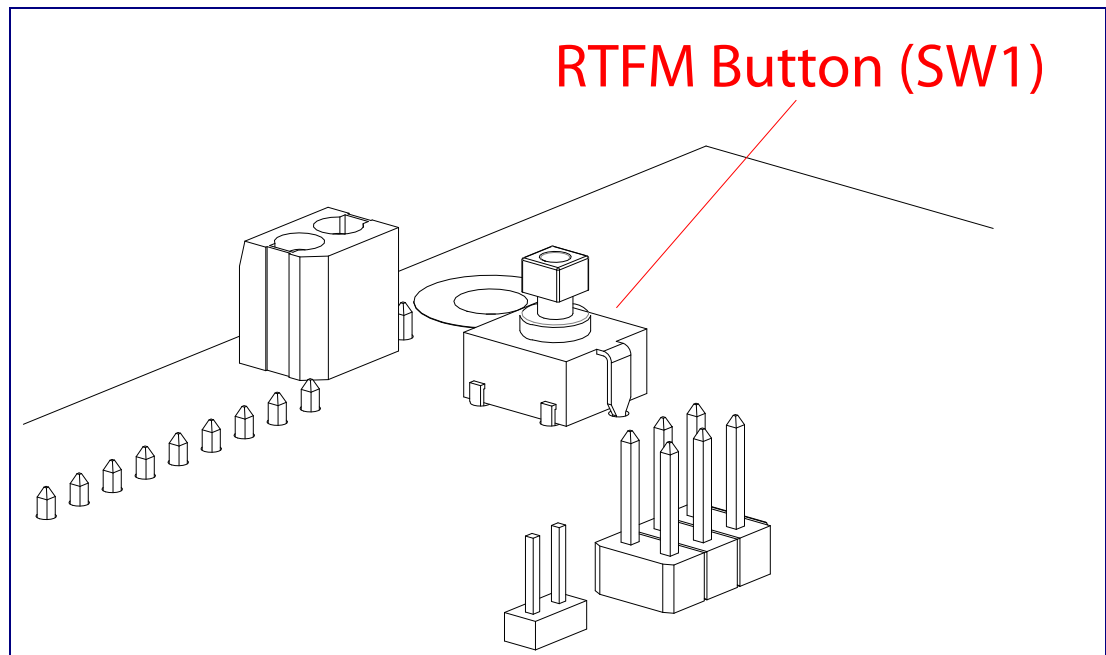
Note Each Intercom is delivered with factory set default values.

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



2.3.9 Adjusting the Intercom Volume

You can adjust the Intercom volume through the [SIP Volume](#), [Multicast Volume](#), [Ring Volume](#), and [Sensor Volume](#) settings on the [Device Page](#).

2.3.10 Call Button and the Call Button LED

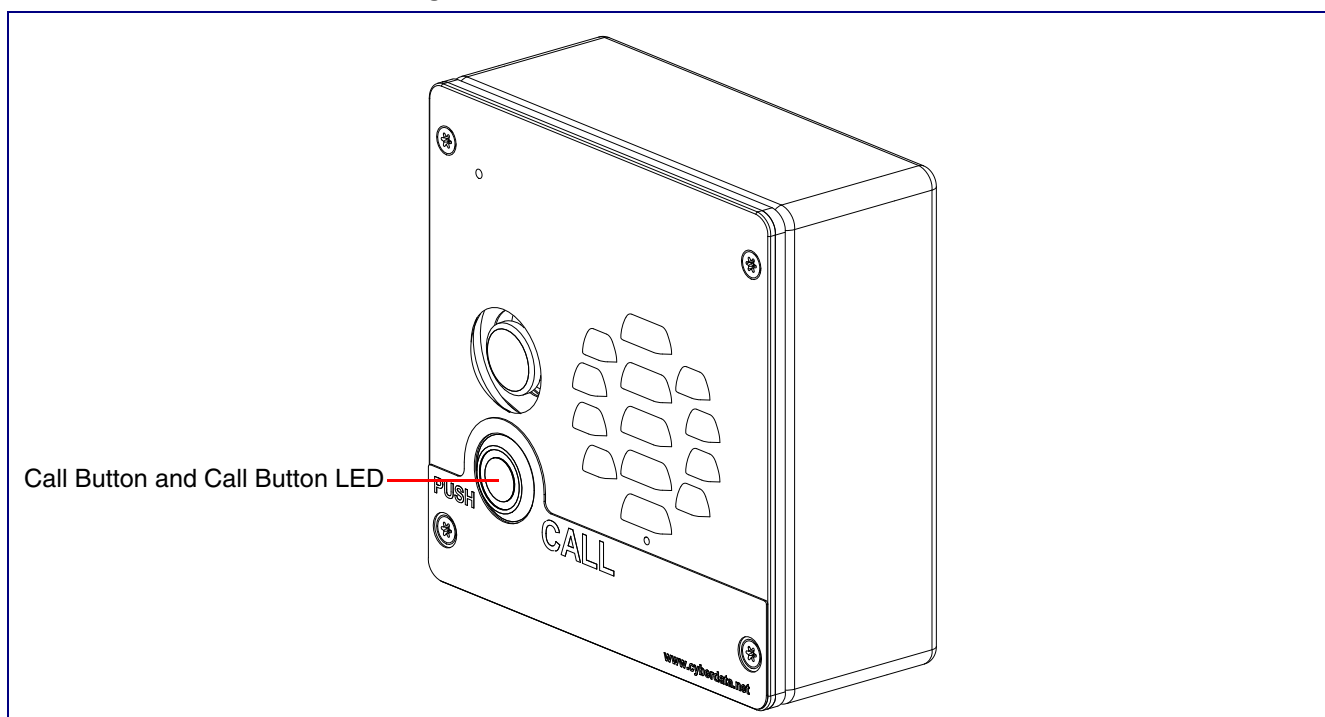
2.3.10.1 Calling with the The Call Button

- You may initiate a call by pressing the **Call** button.
- An active call is indicated by the Call Button LED blinking at one second intervals.
- The Intercom can automatically answer an incoming call.
- You can press the Call Button to terminate an active call.

2.3.10.2 Call Button LED Function

- Upon initial power or reset, the Call Button LED will illuminate.
- On boot, the Call Button LED will flash ten times a second while setting up the network and downloading autoprovisioning files.
- The device “autoprovisions” by default, and the initial process may take several minutes as the device searches for and downloads updates. The Call Button LED will blink during this process. During the initial provisioning, or after the factory defaults have been reset, the device may download firmware twice. The device will blink, remain solid for 10 to 20 seconds, and then resume blinking. This process will take longer if there are many audio files downloading.
- When the software has finished initialization, the Call Button LED will blink twice.
- When a call is established (not just ringing), the Call Button LED will blink.
- On the **Device Page** (see [Section 2.4.5, "Configure the Device"](#)), there is an option called **Button Lit When Idle**. This option sets the normal state for the indicator LED. The Call Button LED will still blink during initialization and calls.
- The Call Button LED flashes briefly at the beginning of RTFM mode.

Figure 2-15. Call Button and Call Button LED



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 Intercom"](#) 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 2-4. Factory Default Settings

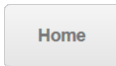
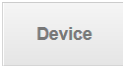

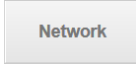



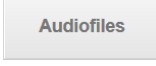
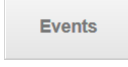
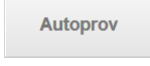
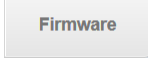
Parameter	Factory Default Setting
IP Addressing	DHCP
IP Address ^a	10.10.10.10
Web Access Username	admin
Web Access Password	admin
Subnet Mask ^a	255.0.0.0
Default Gateway ^a	10.0.0.1

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

2.4.2 Intercom Web Page Navigation

Table 2-5 shows the navigation buttons that you will see on every Intercom web page.

Table 2-5. Web Page Navigation

Web Page Item	Description
	Link to the Home page.
	Link to the Device page.
	Link to the Video 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 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:

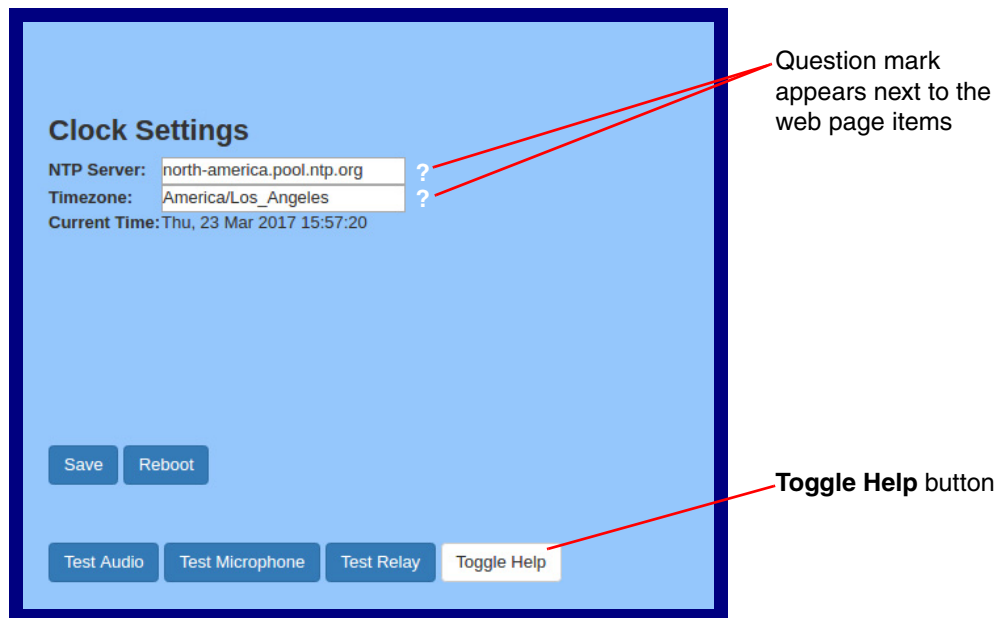
1. Click on the **Toggle Help** button that is on the UI webpage. See [Figure 2-16](#) and [Figure 2-17](#).

Figure 2-16. Toggle/Help Button



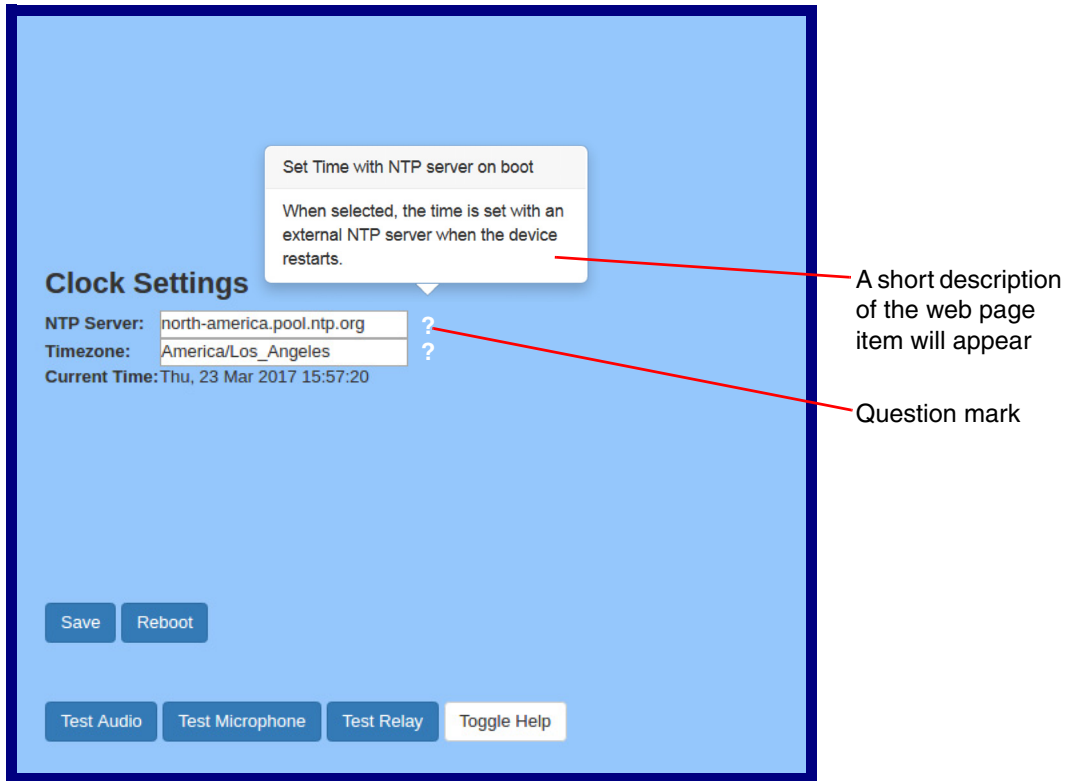
2. You will see a question mark (?) appear next to each web page item that has been provided with a short description by the Help feature. See [Figure 2-17](#).

Figure 2-17. 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 2-18](#).

Figure 2-18. Short Description Provided by the Help Feature



2.4.4 Log in to the 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 website address:

<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 2-19):

Web Access Username: **admin**

Web Access Password: **admin**

Figure 2-19. Home Page

The screenshot displays the home page of the CyberData Outdoor Intercom web interface. At the top, there is a navigation bar with tabs for Home, Device, Video, Network, SIP, Multicast, Sensor, Audiofiles, Events, Autopro, and Firmware. The main heading is "CyberData Outdoor Intercom".

The page is divided into three main sections:

- Current Status:** Displays device information such as Serial Number (410000001), Mac Address (00:20:f7:03:87:07), Firmware Version (v1.0.0), and Partition information. It includes a "Boot From Other Partition" button.
- Admin Settings:** Contains login fields for Username (admin), Password (masked with dots), and Confirm Password (masked with dots). It features "Save", "Reboot", and "Toggle Help" buttons.
- Import Settings:** Includes a "Choose File" button (No file chosen) and an "Import Config" button.
- Export Settings:** Includes an "Export Config" button.

Below the Admin Settings, there are sections for IP Addressing (DHCP, 10.10.1.127), SIP Volume (4), Multicast Volume (4), Ring Volume (4), Sensor Volume (4), and Microphone Gain (4). There are also sections for SIP Mode, Multicast Mode, Event Reporting, and Nightringer, all currently set to Disabled. At the bottom, it shows SIP server registration status: Primary SIP Server (Not registered), Backup Server 1 (Not registered), Backup Server 2 (Not registered), and Nightringer Server (Not registered).

3. On the **Home** page, review the setup details and navigation buttons described in [Table 2-6](#).

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 2-6. 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.
Partition 2	Contains a complete copy of bootable software.
Partition 3	Contains an alternate, complete copy of bootable software.
Booting From	Indicates the partition currently used for boot.
	Allows the user to boot from the alternate partition.
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.
Microphone Gain	Shows the current 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.

Table 2-6. Home Page Overview (continued)

Web Page Item	Description
Import Settings	
	Use this button to select a configuration file to import.
	After selecting a configuration file, click Import to import the configuration from the selected file. Then, click Save and Reboot to store changes.
Export Settings	
	Click Export to export the current configuration to a file.
	Click the Save button to save your configuration settings. Note: You need to reboot for changes to take effect.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

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

2.4.5 Configure the Device

1. Click the **Device** menu button to open the **Device** page. See [Figure 2-20](#).

Figure 2-20. Device Page

The screenshot shows the 'Device' configuration page for a CyberData Outdoor Intercom. The page has a blue background and a navigation bar at the top with tabs for Home, Device, Video, Network, SIP, Multicast, Sensor, Audiofiles, Events, Autoprov, and Firmware. The main title is 'CyberData Outdoor Intercom'. The page is divided into four sections: Volume Settings (0-9), Relay Settings, Clock Settings, and Misc Settings. At the bottom, there are buttons for Save, Reboot, Test Audio, Test Microphone, Test Relay, and Toggle Help.

Section	Setting	Value
Volume Settings (0-9)	SIP Volume:	4
	Multicast Volume:	4
	Ring Volume:	4
	Sensor Volume:	4
	Microphone Gain:	4
Relay Settings	Activate Relay with DTMF code:	<input checked="" type="checkbox"/>
	Relay Pulse Code:	123
	Relay Pulse Duration (in seconds):	2
	Relay Activation Code:	456
	Relay Deactivation Code:	654
	Play tone during DTMF Activation:	<input type="checkbox"/>
	Activate Relay During Ring:	<input type="checkbox"/>
	Activate Relay During Night Ring:	<input type="checkbox"/>
	Activate Relay While Call Active:	<input type="checkbox"/>
	Activate Relay On Button Press:	<input type="checkbox"/>
Relay On Button Press Duration:	3	
Clock Settings	NTP Server:	north-america.pool.ntp.org
	Timezone:	America/Los_Angeles
	Current Time:	Thu, 23 Mar 2017 15:57:20
Misc Settings	Device Name:	Outdoor Intercom
	Auto-Answer Incoming Calls:	<input checked="" type="checkbox"/>
	Button Lit when Idle:	<input checked="" type="checkbox"/>
	Button Brightness (0-255):	255
	Play Ringback Tone:	<input type="checkbox"/>
	Enable Push to Talk:	<input type="checkbox"/>
	Enable DTMF Push to Talk:	<input type="checkbox"/>
	Prevent Call Termination:	<input type="checkbox"/>
Disable HTTPS (NOT recommended):	<input type="checkbox"/>	

2. On the **Device** page, you may enter values for the parameters indicated 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. Device Page 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.
Microphone Gain ?	Set the microphone gain level.

Table 2-7. Device Page Parameters (continued)













Web Page Item	Description
Clock Settings	
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.
Timezone	Enter the tz database string of your timezone. Examples: America/Los_Angeles America/New_York Europe/London America/Toronto See https://en.wikipedia.org/wiki/List_of_tz_database_time_zones for a full list of valid strings.
Current Time	Displays the current time.
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 2-7. Device Page 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: <ol 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.
	Click the Save button to save your configuration settings. Note: You need to reboot for changes to take effect.

Table 2-7. Device Page Parameters (continued)

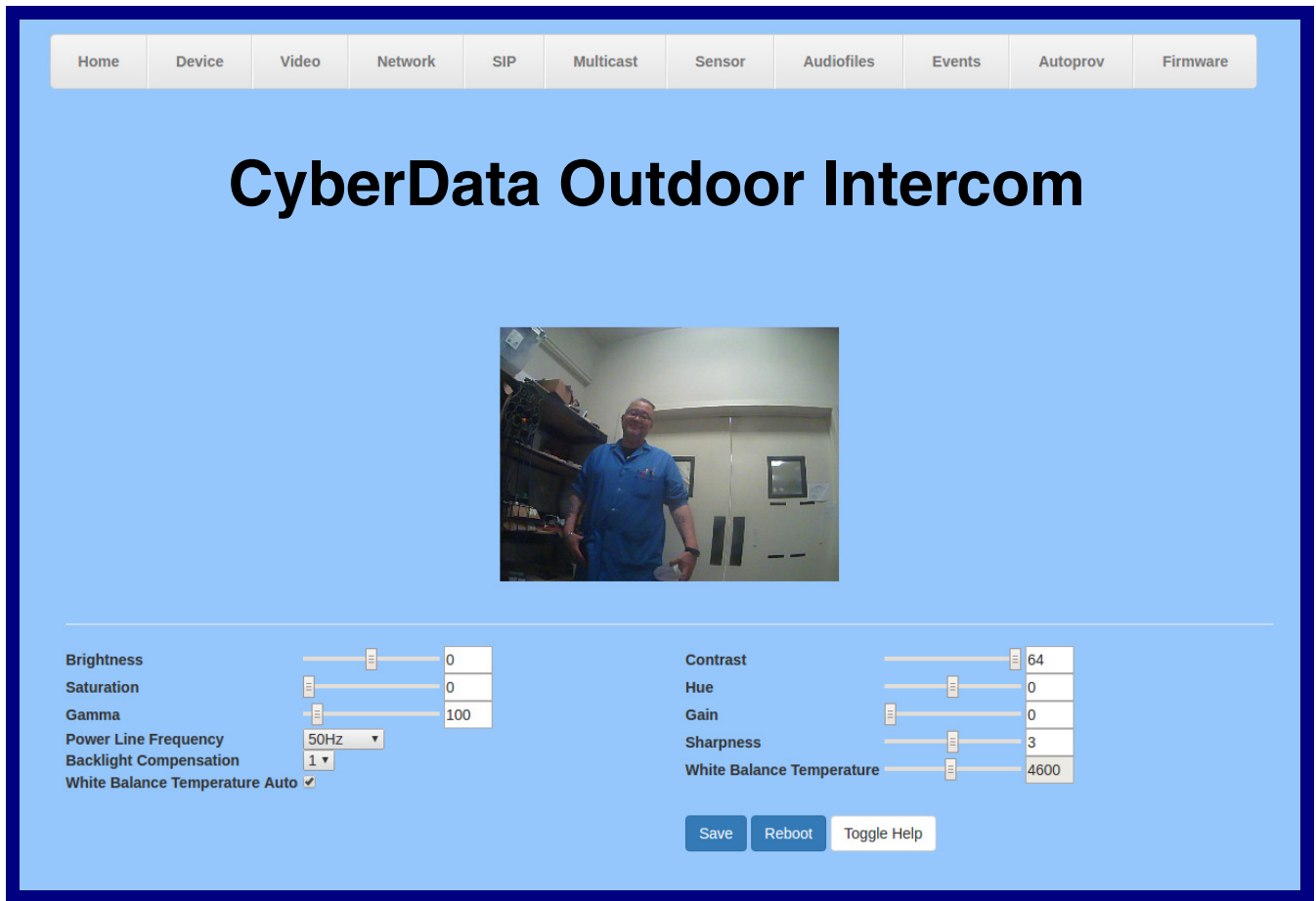
Web Page Item	Description
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

- Note** You must click on the **Save** button and then the **Reboot** button for the changes to take effect.
- Note** The **SIP Volume**, **Multicast Volume**, **Ring Volume**, and **Sensor Volume** settings do not require a reboot for the changes to take effect.
- Note** None of the **Relay Settings** require a reboot for the changes to take effect.
- Note** The **Disable HTTPS (NOT recommended)** setting requires a reboot for the changes to take effect.

2.4.6 Configure the Video Parameters

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

Figure 2-21. Video Page



2. On the **Video** page, enter values for the parameters indicated in [Table 2-9](#).

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. Video Page Parameters



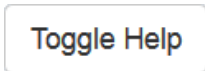
Web Page Item	Description
Brightness ?	The Brightness parameter brightens the entire image equally. Enter a value between -64 and 64. The default value is 0.
Saturation ?	Saturation increases the separation between colors, and has a more noticeable effect on vibrant colors, less on neutral colors, and no effect on black and white images. Enter a value between 0 and 128. The default value is 64.
Gamma ?	Gamma controls the image's grayscale. Increasing gamma can make the image look brighter, because it increases the brightness of the shadows and midtones without affecting the highlights. Enter a value between 72 and 500. The default value is 100.
Power Line Frequency ?	The Power line Frequency option allows the user to select 50Hz, 60Hz, or disabled for the frequency of the power line. Adjust this value if you're seeing flickering from fluorescent light sources. The default value is 50Hz.
Backlight Compensation ?	Backlight Compensation allows the camera to adjust the exposure of the entire image to properly expose the subject in the foreground, to avoid silhouettes where there is a bright light source. Select 0, 1, or 2. The default value is 1.
White Balance Temperature Auto ?	White balance temperature auto allows the device to automatically compensate for cast in lighting. Select "On" or "Off." The default value is "On."
Contrast ?	Contrast is the separation between the darkest and brightest areas of the image. Increasing contrast will make an image look more vibrant; decreasing can make it look duller. Enter a value between 0 and 64. The default value is 32.
Hue ?	Also referred to as "tint," hue affects the red/green balance of the image. Enter a value between -40 and 40. The default value is 0.
Gain ?	Gain controls the amplification of the signal from the camera, including background noise. Enter a value between 0 and 100. The default value is 0.
Sharpness ?	Sharpness controls the contrast along and near the edges in the image. Enter a value between 0 and 6. The default value is 3.
White Balance Temperature ?	White balance temperature compensates for cast in lighting, keeping white and gray neutral. This setting is only applicable if "White Balance Temperature Auto" is set to "off." Enter a value between 2800 and 6500. The default value is 4600.
	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.

Table 2-8. Video Page Parameters (continued)

Web Page Item	Description
	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.

2.4.7 Configure the Network Parameters

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

Figure 2-22. Network Page

Home Device Video Network SIP Multicast Sensor Audiofiles Events Autoprov Firmware

CyberData Outdoor Intercom

Stored Network Settings

Addressing Mode: Static DHCP ?

Hostname: ?

IP Address: ?

Subnet Mask: ?

Default Gateway: ?

DNS Server 1: ?

DNS Server 2: ?

VLAN Settings

VLAN ID (0-4095): ?

VLAN Priority (0-7): ?

Save Reboot Toggle Help

Current Network Settings

IP Address: 10.10.1.47
Subnet Mask: 255.0.0.0
Default Gateway: 10.0.0.1
DNS Server 1: 10.0.1.56
DNS Server 2:

2. On the **Network** page, enter values for the parameters indicated in [Table 2-9](#).

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 2-9. Network Page Parameters



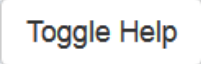
Web Page Item	Description
Stored Network Settings	
Addressing Mode ?	Select either DHCP IP Addressing or Static Addressing by marking the appropriate radio button. DHCP Addressing mode is enabled on default and the device will attempt to resolve network addressing with the local DHCP server upon boot. 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.
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. Note: CISCO requires Priority 5 for SIP operation.
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.
	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.

Table 2-9. Network Page Parameters (continued)

Web Page Item	Description
	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 (Session Initiation Protocol) Parameters

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

Figure 2-23. SIP Page

The screenshot shows the SIP configuration page for a CyberData Outdoor Intercom. The page features a navigation bar at the top with buttons for Home, Device, Video, Network, SIP, Multicast, Sensor, Audiofiles, Events, Autopro, and Firmware. The main title is "CyberData Outdoor Intercom".

SIP Settings

- Enable SIP operation:
- Primary SIP Server: 10.0.0.253
- Primary SIP User ID: 199
- Primary SIP Auth ID: 199
- Primary SIP Auth Password: *****
- Re-registration Interval (in seconds): 360
- Backup SIP Server 1: [Empty]
- Backup SIP User ID: [Empty]
- Backup SIP Auth ID: [Empty]
- Backup SIP Auth Password: [Empty]
- Re-registration Interval (in seconds): 360
- Backup SIP Server 2: [Empty]
- Backup SIP User ID: [Empty]
- Backup SIP Auth ID: [Empty]
- Backup SIP Auth Password: [Empty]
- Re-registration Interval (in seconds): 360
- Remote SIP Port: 5060
- Local SIP Port: 5060
- Outbound Proxy: [Empty]
- Outbound Proxy Port: 0
- Register with a SIP Server:
- Disable rport Discovery:
- Unregister on Boot:
- Keep Alive Period: 10000

Nightringer Settings

- SIP Server: [Empty]
- SIP User ID: [Empty]
- SIP Auth ID: [Empty]
- SIP Auth Password: [Empty]
- Re-registration Interval (in seconds): 360

Dial Out Settings

- Dial out Extension: 204
- Extension ID: id204

Call Disconnection

- Terminate Call after delay: 0

RTP Settings

- RTP Port (even): 10500
- Jitter Buffer: 50

Buttons: Save, Reboot, Toggle Help

2. On the **SIP** page, enter values for the parameters indicated in [Table 2-10](#).

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 2-10. SIP Page 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.
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.
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.
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.
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.
Backup SIP Server 2 ?	Enter a second backup SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the second backup SIP server. This field can accept entries of up to 255 characters in length.
Backup SIP User ID 2 ?	Specify the SIP User ID for the second backup SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the second backup SIP server. Enter up to 64 alphanumeric characters.
Backup SIP Auth ID 2 ?	Specify the Authenticate ID for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
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.

Table 2-10. SIP Page Parameters (continued)

Web Page Item	Description
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.
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.
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 2.4.8.2, "Delayed DTMF").
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	
SIP Server ?	Enter the SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's Nightringer extension on the SIP server. This field can accept entries of up to 255 characters in length.
Remote SIP Port ?	The Remote SIP Port is the port number the device will use as the destination port when sending SIP messages for the Nightringer extension. The default Remote SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
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.
SIP 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.
SIP Auth ID ?	Specify the Authenticate ID for the SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.

Table 2-10. SIP Page Parameters (continued)

Web Page Item	Description
SIP Auth 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.
Dial Out Settings	
Dial Out Extension 	Specify the extension the device will call when someone presses the Call button. Enter up to 64 alphanumeric characters. Note: For information about dial-out extension strings and DTMF tones, see Section 2.4.8.1, "Dial Out Extension Strings and DTMF Tones (using rfc2833)" .
Extension ID 	A Caller identification string added to outbound calls. Enter up to 64 alphanumeric characters.
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.
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.
Jitter Buffer 	Specify the size of the jitter buffer (in milliseconds) used for SIP calls. Valid values are 50-1000. Note: It may be necessary to adjust the jitter buffer on the device receiving the video.
	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 The **Terminate Call After Delay** setting does not require a reboot for the changes to take effect.

Note For specific server configurations, go to the following website address:
<http://www.cyberdata.net/connecting-to-ip-pbx-servers/>

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

On the **SIP 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 2-11. 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 64.

2.4.8.2 Delayed DTMF

On the **SIP** page the dial out extension supports 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 2-12. 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.

2.4.9 Configure the Multicast Parameters

The **Multicast** 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 2-24](#).

Figure 2-24. Multicast Page

Home Device Video Network SIP Multicast Sensor Audiofiles Events Autoprov Firmware

CyberData Outdoor Intercom

Multicast Settings

Enable Multicast Operation:

Priority	Address	Port	Name	Beep	Relay
9	239.168.3.10	11000	Emergency	<input type="checkbox"/>	<input type="checkbox"/>
8	239.168.3.9	10000	MG8	<input type="checkbox"/>	<input type="checkbox"/>
7	239.168.3.8	9000	MG7	<input type="checkbox"/>	<input type="checkbox"/>
6	239.168.3.7	8000	MG6	<input type="checkbox"/>	<input type="checkbox"/>
5	239.168.3.6	7000	MG5	<input type="checkbox"/>	<input type="checkbox"/>
4	239.168.3.5	6000	MG4	<input type="checkbox"/>	<input type="checkbox"/>
3	239.168.3.4	5000	MG3	<input type="checkbox"/>	<input type="checkbox"/>
2	239.168.3.3	4000	MG2	<input type="checkbox"/>	<input type="checkbox"/>
1	239.168.3.2	3000	MG1	<input type="checkbox"/>	<input type="checkbox"/>
0	239.168.3.1	2000	Background Music	<input type="checkbox"/>	<input type="checkbox"/>



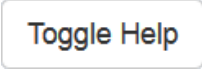
SIP calls are considered priority 4.5
Port range can be from 2000-65535
Priority 9 is the highest and 0 is the lowest
A higher priority audio stream will always supersede a lower one
Priority 9 streams will play at maximum volume
** You need to reboot for changes to take effect*

Save Reboot

2. On the **Multicast** page, enter values for the parameters indicated in [Table 2-13](#).

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 2-13. Multicast Page 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]). Note: The multicast ports have to be even values. The webpage will enforce this restriction.
Name	Assign a descriptive name for this multicast group (25 character limit).
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.
	Click the Save button to save your configuration settings. Note: You need to reboot for changes to take effect.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

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

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

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

2.4.9.1 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 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 2-25](#)).

Figure 2-25. Sensor Page

The screenshot shows the 'Sensor' configuration page for a CyberData Outdoor Intercom. At the top, a navigation bar includes links for Home, Device, Video, Network, SIP, Multicast, Sensor, Audiofiles, Events, Autopro, and Firmware. The main heading is 'CyberData Outdoor Intercom'. The page is divided into two sections: 'Door Sensor Settings' and 'Intrusion Sensor Settings'. The 'Door Sensor Settings' section includes: 'Door Sensor Normally Closed' (radio buttons for Yes and No), 'Door Open Timeout (in seconds):' (input field with '0'), 'Flash Button LED:' (checkbox), 'Activate Relay:' (checkbox), 'Play Audio Locally:' (checkbox), 'Make call to extension:' (checkbox), 'Dial Out Extension:' (input field with '204'), 'Dial Out ID:' (input field with 'id204'), 'Play recorded audio:' (checkbox), and 'Repeat Sensor Message:' (input field with '0'). The 'Intrusion Sensor Settings' section includes: 'Flash Button LED:' (checkbox), 'Activate Relay:' (checkbox), 'Play Audio Locally:' (checkbox), 'Make call to extension:' (checkbox), 'Dial Out Extension:' (input field with '204'), 'Dial Out ID:' (input field with 'id204'), 'Play recorded audio:' (checkbox), and 'Repeat Intrusion Message:' (input field with '0'). At the bottom, there are buttons for 'Save', 'Reboot', 'Toggle Help', 'Test Door Sensor', and 'Test Intrusion Sensor'.









2. On the **Sensor** page, enter values for the parameters indicated in [Table 2-14](#).

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 2-14. Sensor Page 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 2-14. Sensor Page 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 for the changes to take effect.

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

2.4.11 Configure the Audio 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 2-26).

Figure 2-26. Audiofiles Page

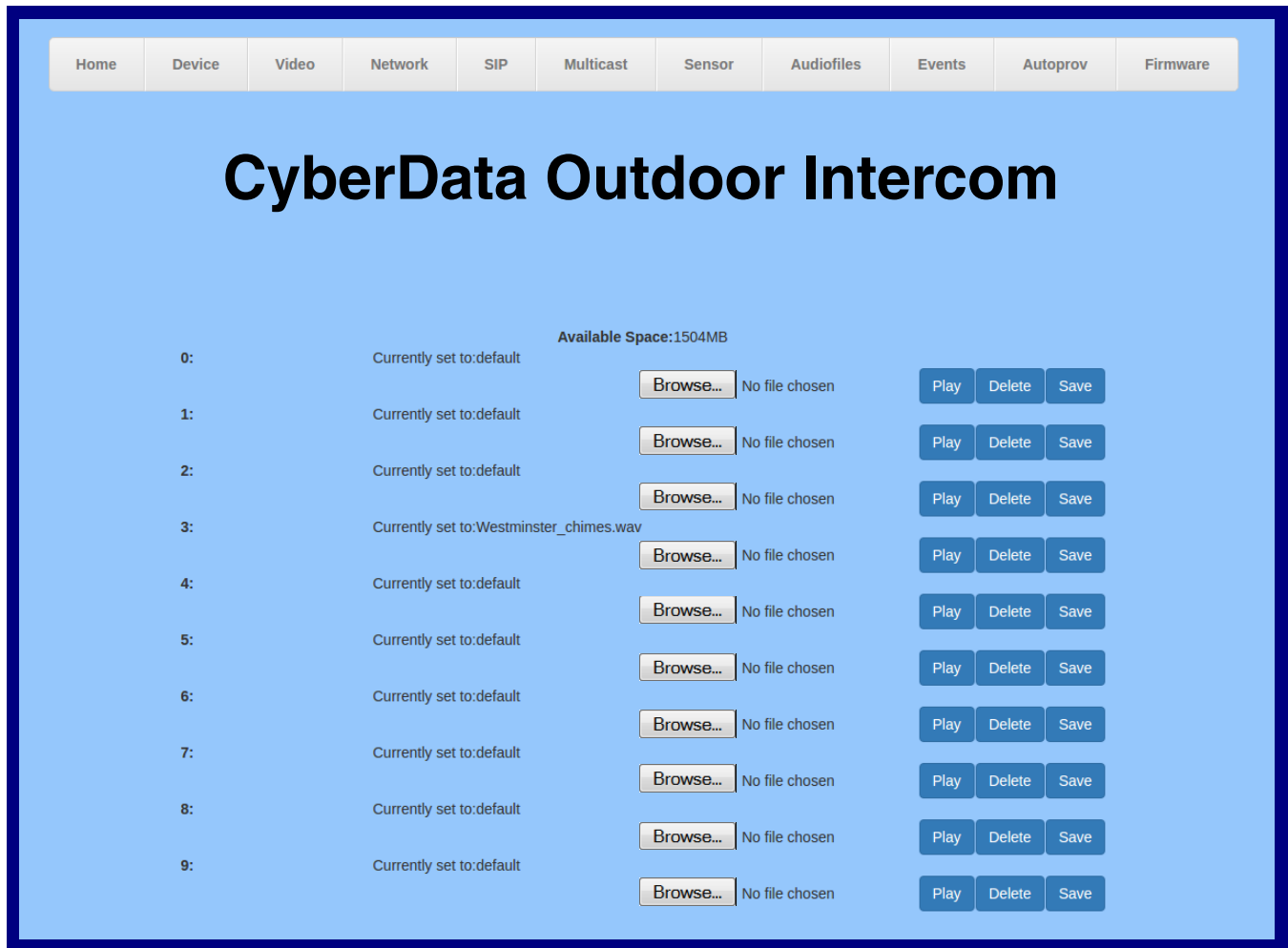


Figure 2-27. Audiofiles Page

Dot:	Currently set to:default	<input type="button" value="Browse..."/> No file chosen	<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 chosen	<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 chosen	<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 chosen	<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 chosen	<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 chosen	<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 chosen	<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 chosen	<input type="button" value="Play"/> <input type="button" value="Delete"/> <input type="button" value="Save"/>
Intrusion Sensor Triggered:	Currently set to:Gong.wav	<input type="button" value="Browse..."/> No file chosen	<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 chosen	<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 chosen	<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 2-15](#).

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 2-15. Audiofiles Page Parameters

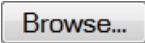



Web Page Item	Description
Available Space	Shows the space available for the user to save custom audio files if they want to change the message when the door or sensor is triggered.
0-9	The name of the audio configuration option is the same as the spoken audio that plays on the board (24 character limit).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

Table 2-15. Audiofiles Page Parameters (continued)

Web Page Item	Description
	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 2-28](#) through [Figure 2-30](#).

Figure 2-28. Audacity 1

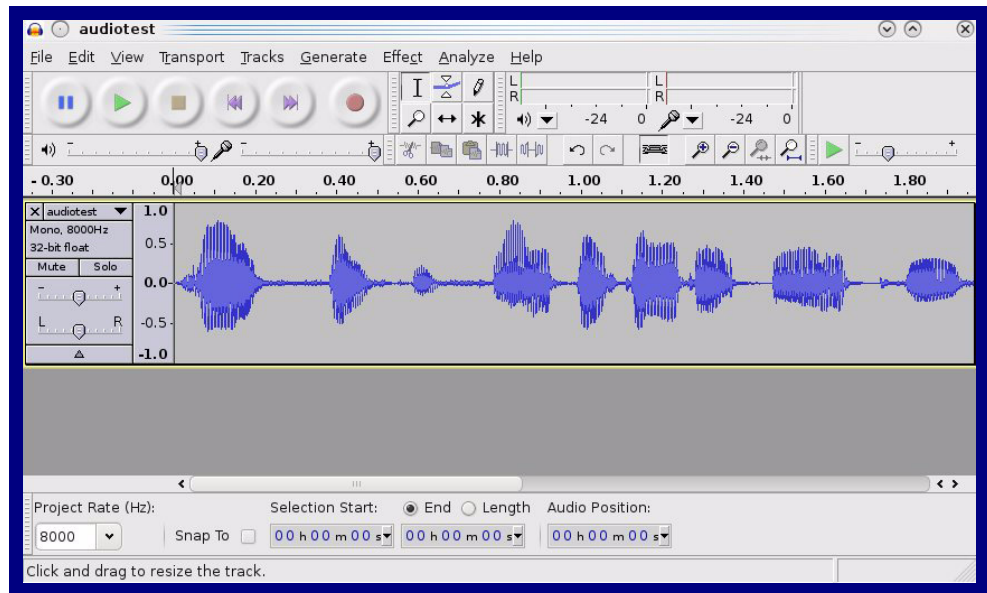
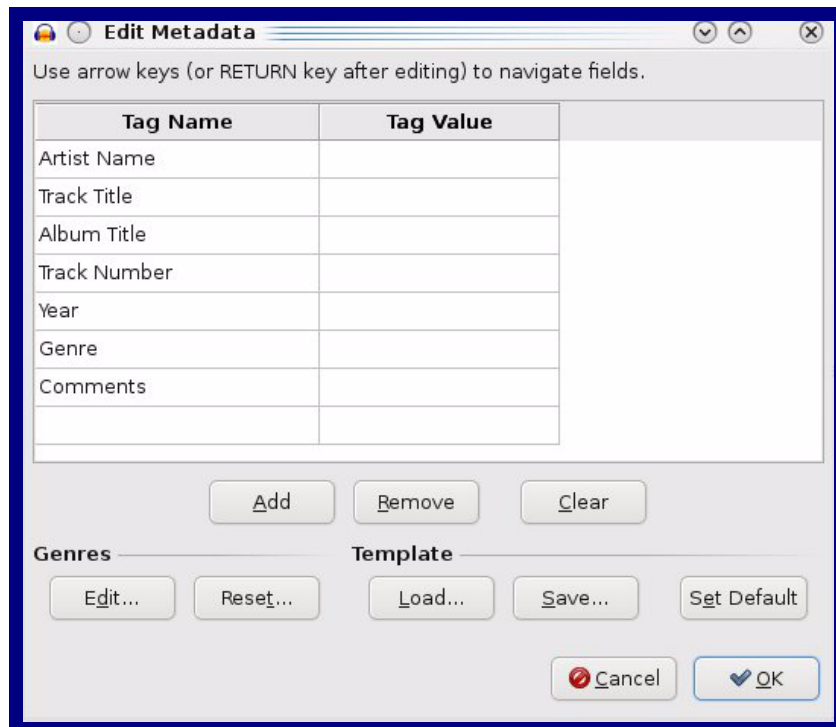


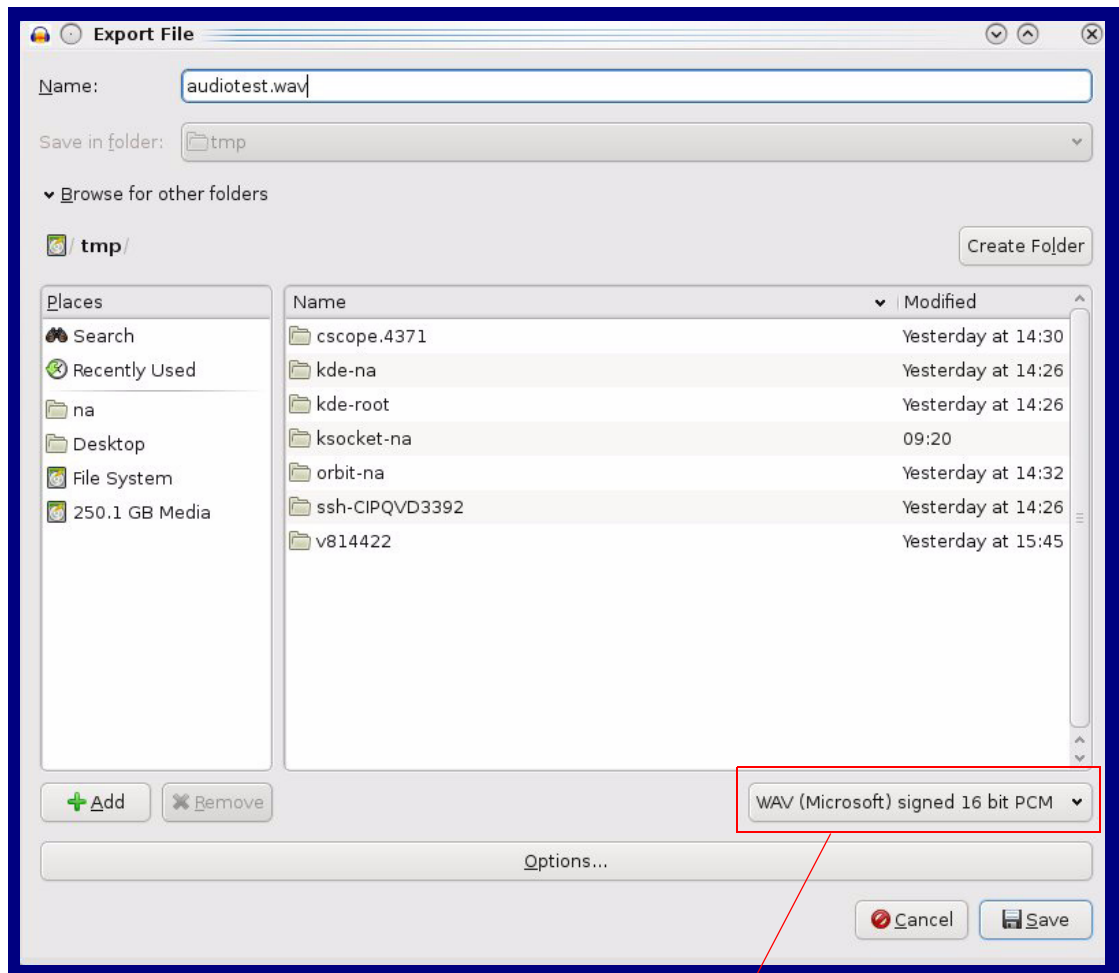
Figure 2-29. Audacity 2



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

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

Figure 2-30. 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 2-31).

Figure 2-31. Events Page

Home Device Video Network SIP Multicast Sensor Audiofiles Events Autopro Firmware

CyberData Outdoor 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: 10.0.0.250

Server Port: 8080

Server URL: xmlparse_engine

[Save](#) [Reboot](#) [Toggle Help](#)






2. On the **Events** 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. Events Page 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 Events ?	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.
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.

Table 2-16. Events Page Parameters(continued)

Web Page Item	Description
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 for the changes to take effect.

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

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

2.4.12.1 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 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 2-32](#).

Figure 2-32. Autoprovisioning Page

The screenshot shows the 'Autoprov' configuration page for a CyberData Outdoor Intercom. At the top, there is a navigation menu with buttons for Home, Device, Video, Network, SIP, Multicast, Sensor, Audiofiles, Events, Autoprov (selected), and Firmware. The main heading is 'CyberData Outdoor Intercom'. Below this, there are several configuration options:

- Disable Autoprovisioning:** A checkbox that is currently unchecked.
- Autoprovisioning Server:** A text input field.
- Autoprovisioning Filename:** A text input field.
- Use tftp:** A checkbox that is currently unchecked.
- Username:** A text input field.
- Password:** A text input field.
- Autoprovisioning autoupdate (in minutes):** A numeric input field with the value '0'.
- Autoprovision at time (HHMMSS):** A text input field.
- Autoprovision when idle (in minutes > 10):** A numeric input field with the value '0'.

Below the input fields, there are three lines of instructional text:

- 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.*

Below the text, there are three buttons: 'Save', 'Reboot', and 'Toggle Help'. Further down, there is a 'Download Template' button. At the bottom, there is a section titled 'Autoprovisioning log' with a large, empty text area for displaying logs.

2. On the **Autoprovisioning** page, you may 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. Autoprovisioning Page Parameters





Web Page Item	Description
Disable Autoprovisioning ?	Prevent the device from automatically trying to download a configuration file. See Section 2.4.13.1, "Autoprovisioning" for more information.
Autoprovisioning Server ?	Enter the IPv4 address of the provisioning server in dotted decimal notation.
Autoprovisioning Filename ?	The autoprovisioning filename is the configuration filename. The default autoprovisioning filename is in the format of <mac address>.xml . Supported filename extensions are .txt, and .xml. The current filename is denoted by an asterisk at the bottom of the Autoprovisioning Page . Enter up to 256 characters. A file may have any name with an xml extension. If a file name is entered, the device will look for the specified file name, and only that file.
Use tftp ?	The device will use TFTP (instead of http) to download autoprovisioning files.
Username ?	The username used to authenticate with an autoprovisioning server. Leave this field blank to disable authentication.
Password ?	The password used to authenticate with an autoprovisioning server. Leave this field blank to disable authentication.
Autoprovisioning Autoupdate (in minutes) ?	The reoccurring time (in minutes) the device will wait before checking for new autoprovisioning files. Enter up to 6 digits. A value of 0 will disable this option.
Autoprovision at time (HHMMSS) ?	The time of day the device will check for a new autoprovisioning file. The time must be 6 characters in length and in HHMMSS format. An empty value will disable this option.
Autoprovision when idle (in minutes > 10) ?	The idle time (in minutes greater than 10) after which the device will check for a new autoprovisioning file. Enter up to 6 digits. A value of 0 will disable this option.
	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.

Table 2-17. Autoprovisioning Page Parameters (continued)

Web Page Item	Description
	Press the Download Template button to create an autoprovisioning file for the device. See Section 2.4.13.3, "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.

2.4.13.1 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 2.4.13.2, "Sample dhcpd.conf"](#) for an example of how to configure dhcpd to offer autoprovisioning server addresses. If multiple options are set, the device will attempt to download autoprovisioning files from every server.

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

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

You can download an autoprovisioning template file from the [Autoprovisioning Page](#) using the **Download Template** button (see [Table 2-17](#)). This file contains every configuration option that can be set on the board.

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

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

```
<MiscSettings>
    <DeviceName>CyberData VoIP Intercom</DeviceName>
<!--    <AutoprovFile>common.xml</AutoprovFile>-->
```

```
<!-- <AutprovFile>sip_reg[macaddress].xml</AutprovFile>-->  
<!-- <AutprovFile>audio[macaddress]</AutprovFile>-->  
<!-- <AutprovFile>device[macaddress].xml</AutprovFile>-->  
    </MiscSettings>
```

After downloading the first autoprovisioning file, the device will step through up to twenty additional <AutprovFile> 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 autoprovision autoprovisioning values (for example, to disable autoprovisioning or to configure a time to check for new files).

Checking for New
Autoprovisioning
Files after Boot

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

The Autoprovisioning Filename

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

Table 2-18. 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-ceilingsspeaker</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://autoprovttest.server.net.” Device2 sets the SIP User ID to **500**, the password to **ext500**, and the dialout extension to **555**.

Autoprovisioning
 Example 2

Here is another example of setting up your autoprovisioning files:

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

0020f7020001.xml

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

0020f7020002.xml

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

common_settings.xml

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

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

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

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

XML Files

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

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

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

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

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

From the common file, a pointer to sip_common.xml

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

Autoprovisioned Audio Files

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

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

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

2.4.13.2 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; }
}
```

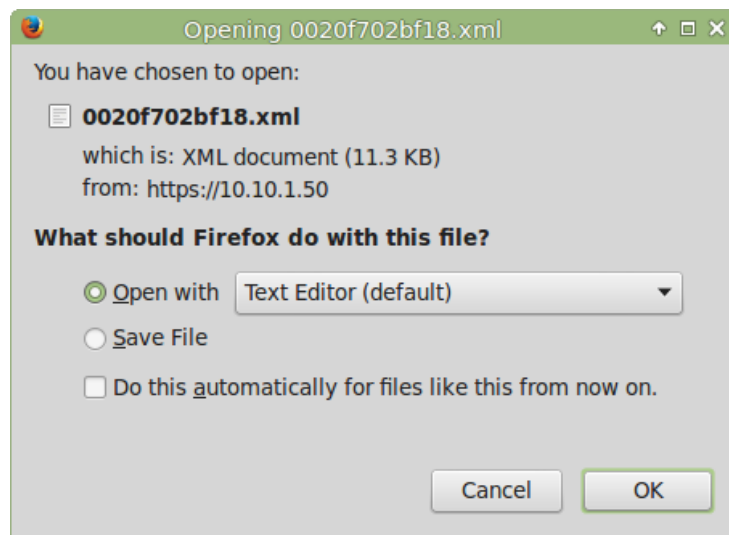
2.4.13.3 Download Template Button

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

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

1. On the **Autoprovisioning** page, click on the **Download Template** button.
2. You will see a window prompting you to save a configuration file (**.xml**) to a location on your computer ([Figure 2-33](#)). 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 2-33](#).

Figure 2-33. Configuration File



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

2.5 Upgrade the Firmware and Reboot the Intercom



Caution

Equipment Hazard: Devices with a serial number that begins with 4100xxxxx 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/011410/>
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 Home Page"](#).

4. Click on the **Firmware** menu button to open the **Firmware** page. See [Figure 2-34](#).


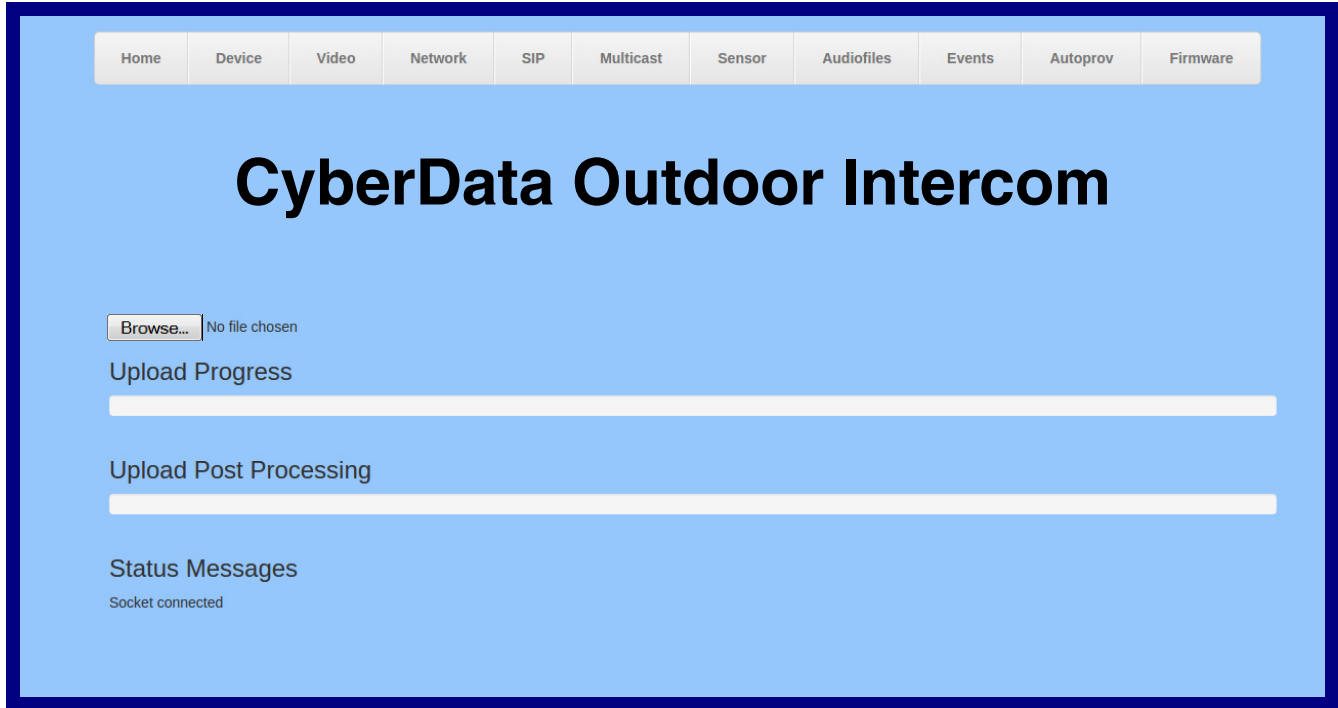
 <p>GENERAL ALERT</p>	<p>Caution</p> <p>Equipment Hazard: CyberData strongly recommends that you first reboot the device before attempting to upgrade the firmware of the device. See Section 2.7, "Reboot the Device".</p>
--	---

Figure 2-34. Firmware Page



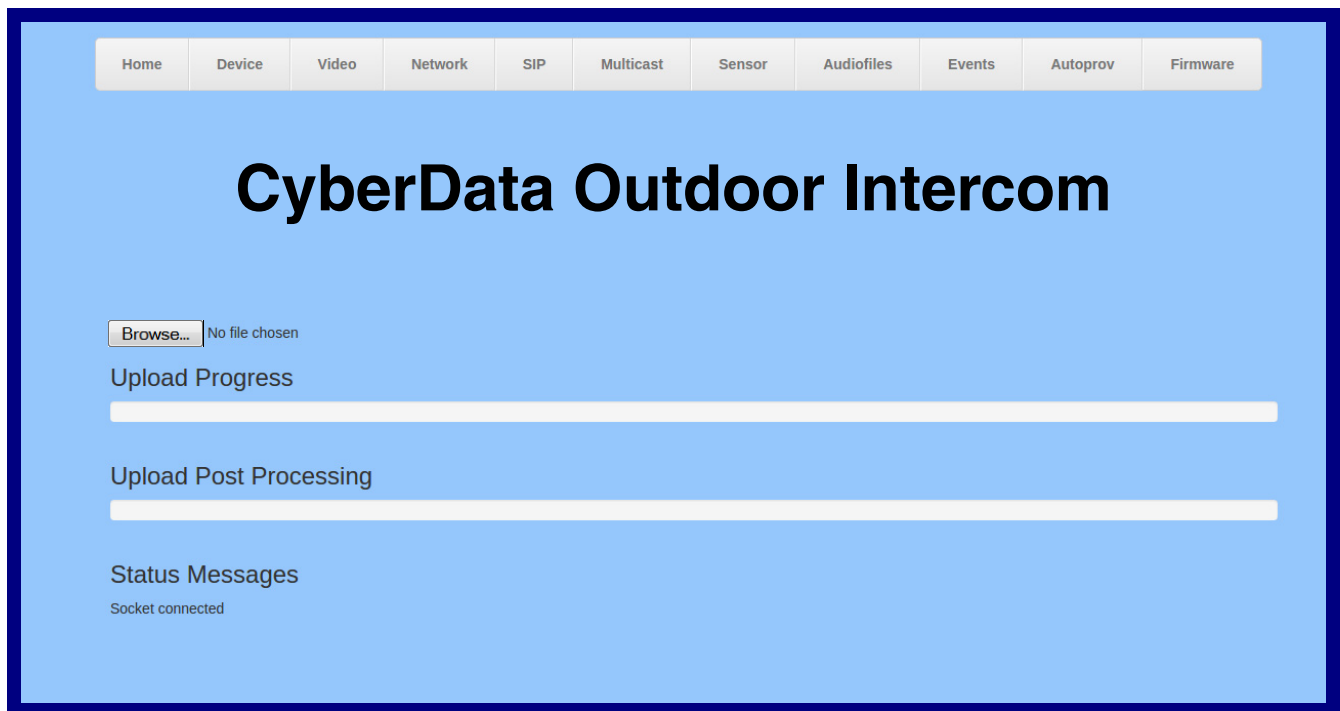
2.6 Upgrade the Firmware

Note CyberData strongly recommends that you do not upgrade the firmware when the device is likely to be in use.

To upgrade the firmware of your device:

1. Download the latest firmware file from the **Downloads** tab at the following webpage:
<http://www.cyberdata.net/voip/011410/>
2. Unzip the firmware version file. This file may contain the following:
 - Firmware file
 - Release notes
 - Autoprovisioning template
3. Log in to the **Home** page as instructed in [Section 2.4.4, "Log in to the Home Page"](#).
4. Click on the **Firmware** menu button to open the **Firmware** page ([Figure 2-34](#)).

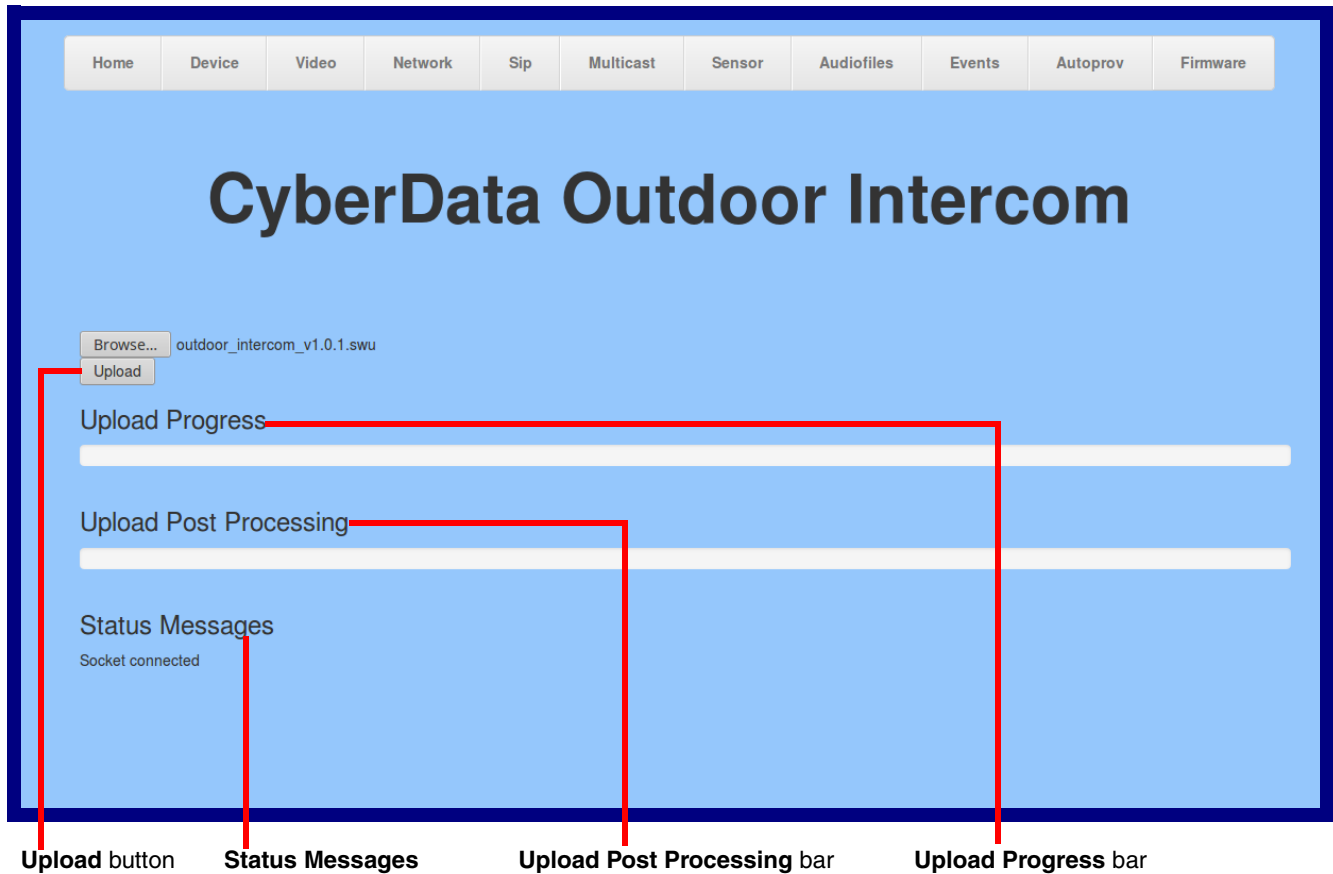
Figure 2-35. Firmware Page



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

6. Select the firmware file. This reveals the **Upload** button (Figure 2-36).

Figure 2-36. Upload Button



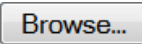
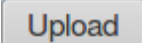
7. Click on the **Upload** button. After selecting the **Upload** button, you will see the progress of the upload in the **Upload Progress** bar.
8. When the upload is complete, you will see the words **Upload finished** under **Status Messages**.
9. At this point, you will see the progress of the upload's post processing in the **Upload Post Processing** bar.

Note Do not reboot the device before the upgrading process is complete.

10. When the process is complete, you will see the words **SWUPDATE Successful** under **Status Messages**.
11. The device will reboot automatically.
12. The **Home** page will display the version number of the firmware and indicate which boot partition is active.

Table 2-19 shows the web page items on the **Firmware** page.

Table 2-19. Firmware Page Parameters

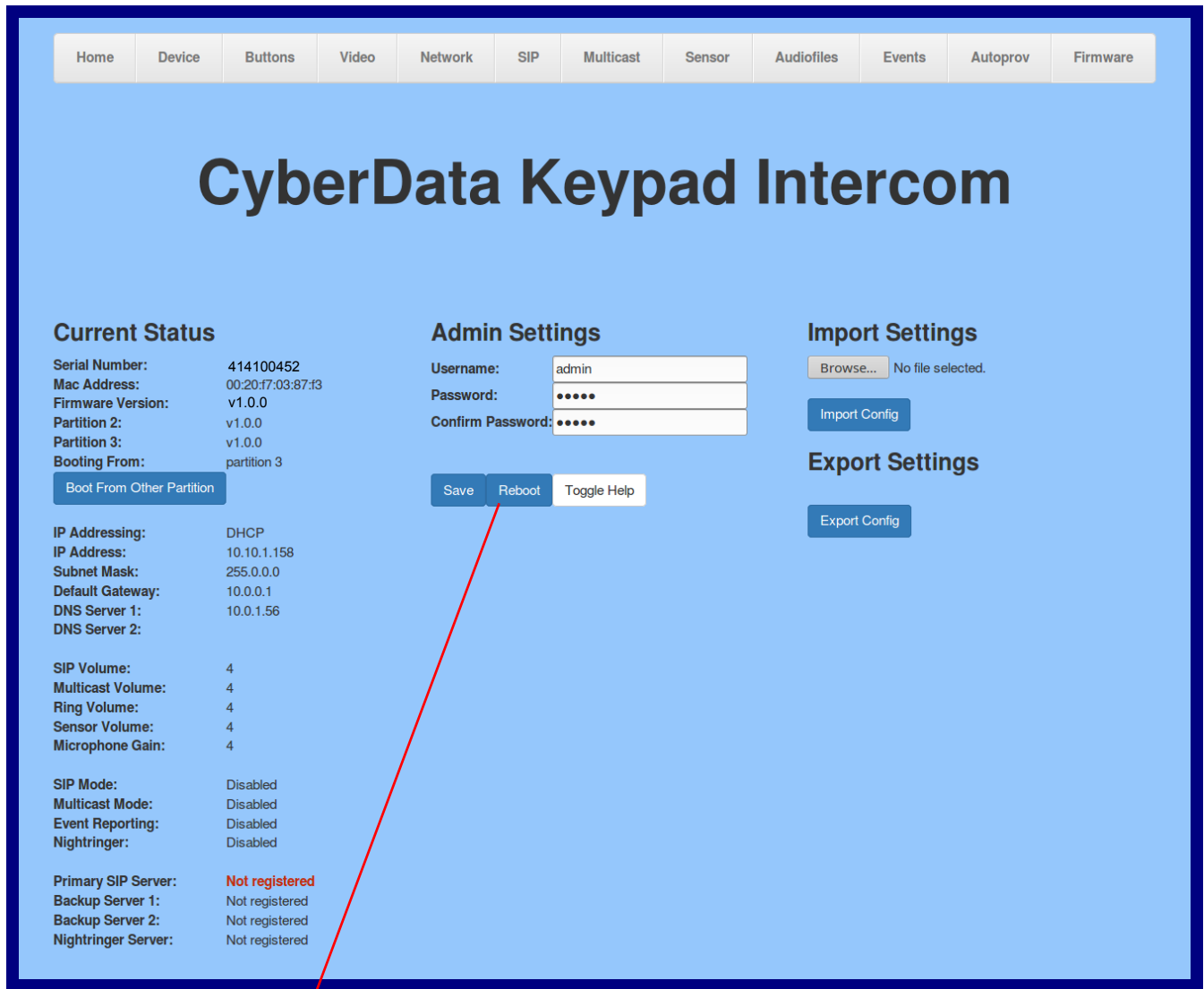
Web Page Item	Description
	Use the Browse button to navigate to the location of the Intercom firmware file that you want to upload.
	Click on the Upload button to automatically upload the selected firmware and reboot the system. Note: This button only appears after the user has selected a firmware file.
Upload progress	Status bar indicates the progress in uploading the file.
Upload Post Processing	Status bar indicates the progress of the software installation.
Status Messages	Messages relevant to the firmware update process appear here.

2.7 Reboot the Device

To reboot the device, complete the following steps:

1. Log in to the **Home** page as instructed in [Section 2.4.4, "Log in to the Home Page"](#).
2. Click on the **Reboot** button on the **Home** page ([Figure 2-37](#)). A normal restart will occur.

Figure 2-37. Home Page



Reboot

2.8 Command Interface

Some functions on the device can be activated using simple POST commands to the web interface. The examples in [Table 2-20](#) use the free unix utility, **wget** commands. However, any program that can send HTTP POST commands to the device should work.

2.8.1 Command Interface Post Commands

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

Table 2-20. 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 2-20. Command Interface Post Commands (continued)

Device Action	HTTP Post Command^a
Play 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 "play_4=yes"</code>
Play 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 "play_5=yes"</code>
Play 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 "play_6=yes"</code>
Play 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 "play_7=yes"</code>
Play 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 "play_8=yes"</code>
Play 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 "play_9=yes"</code>
Play the "Dot" 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_d=yes"</code>
Play the "Audio Test" audio file (from Audio Config)	<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_audiotest=yes"</code>
Play 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 "play_pagetone=yes"</code>
Play 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 "play_youripaddressis=yes"</code>
Play 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 "play_rebooting=yes"</code>
Play 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 "play_restoringdefault=yes"</code>
Play the "Ringback 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 "play_ringback=yes"</code>
Play the "Ring 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 "play_ringtones=yes"</code>
Play the "Intrusion Sensor Triggered" 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_intrusionsensortriggered=yes"</code>
Play the "Door Ajar" 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_doorajar=yes"</code>

Table 2-20. 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 2-20. 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_ringtones=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 2.4.8.2, "Delayed DTMF"](#)

Appendix A: Mounting the Intercom

A.1 Mounting Components

Before you mount the Intercom, make sure that you have received all the parts for each Intercom. Refer to the following tables.

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

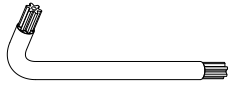
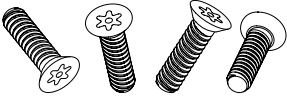
Quantity	Part Name	Illustration
1	T-15H Torx Key	
4	Security Torx Screw	

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


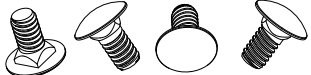


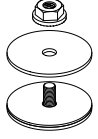
Quantity	Part Name	Illustration
4	Carriage bolt nuts	
4	Carriage bolts	
4	Carriage bolt washers	

Table A-3. Optional Accessories

Quantity	Part Name	Illustration
1	Spacer for half-inch set conduit connector	
1	531085B hole plug assembly	

A.2 Dimensions

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

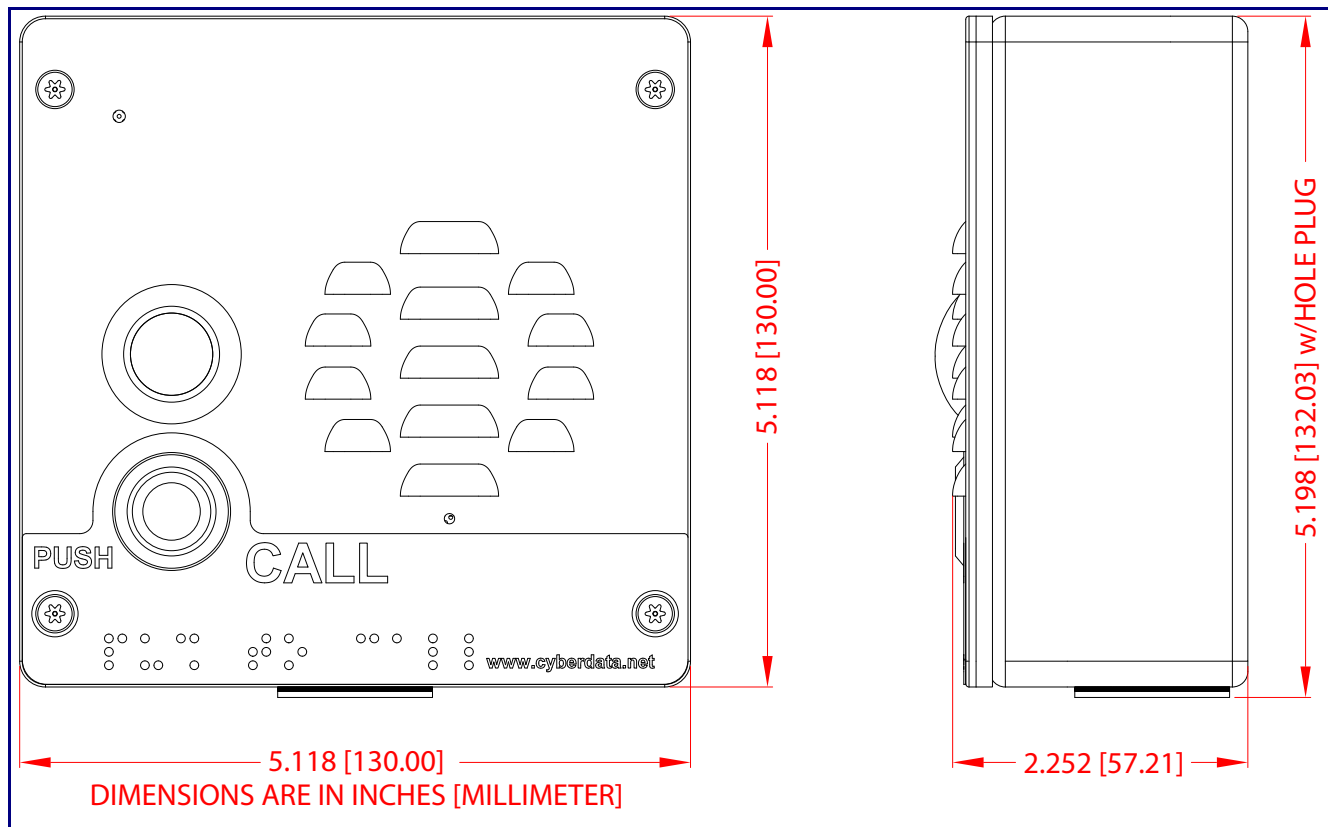


Figure A-2. Unit Dimensions—Rear View with Mounting Hole Locations

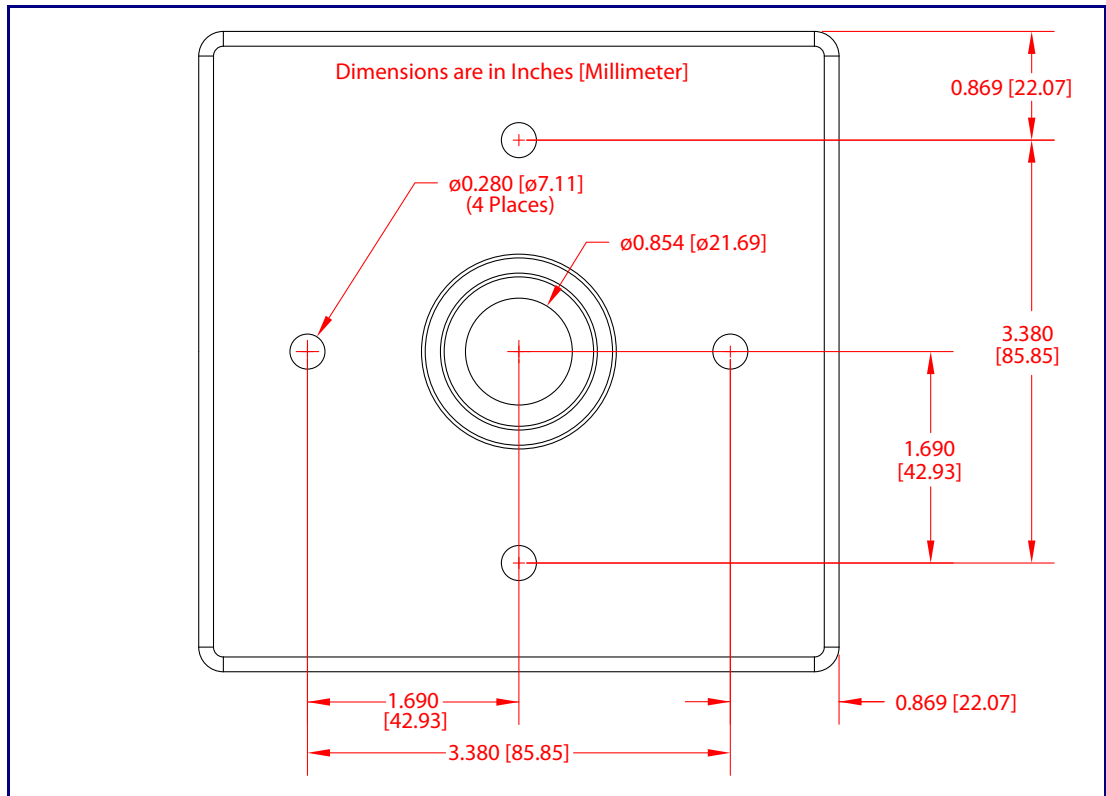
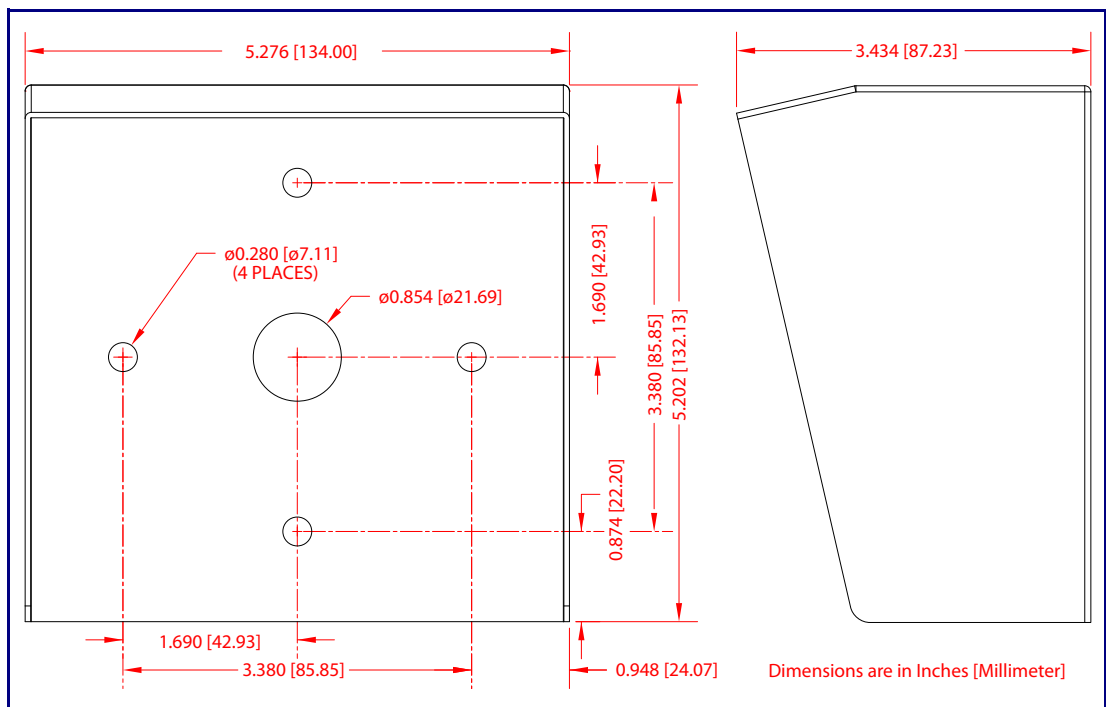


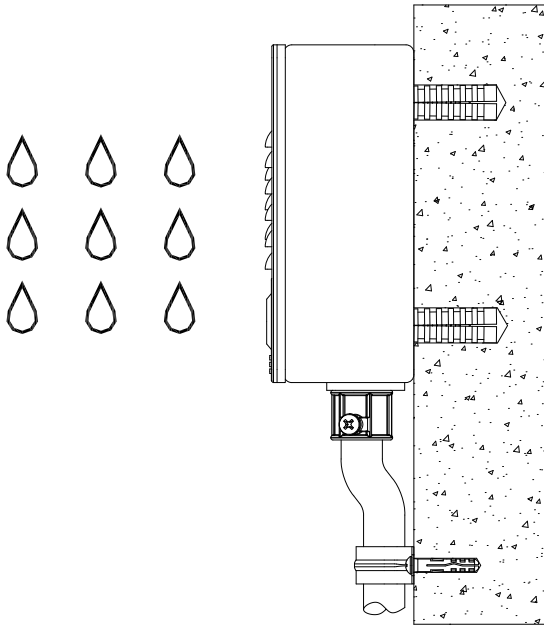
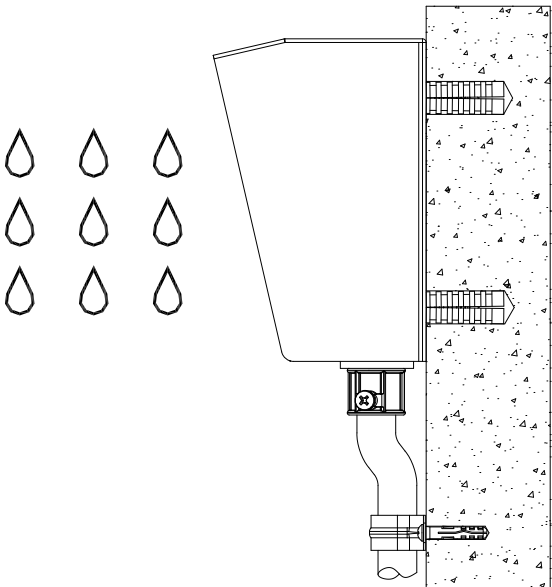
Figure A-3. Shroud Dimensions—Front and Side View with Mounting Hole Locations



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

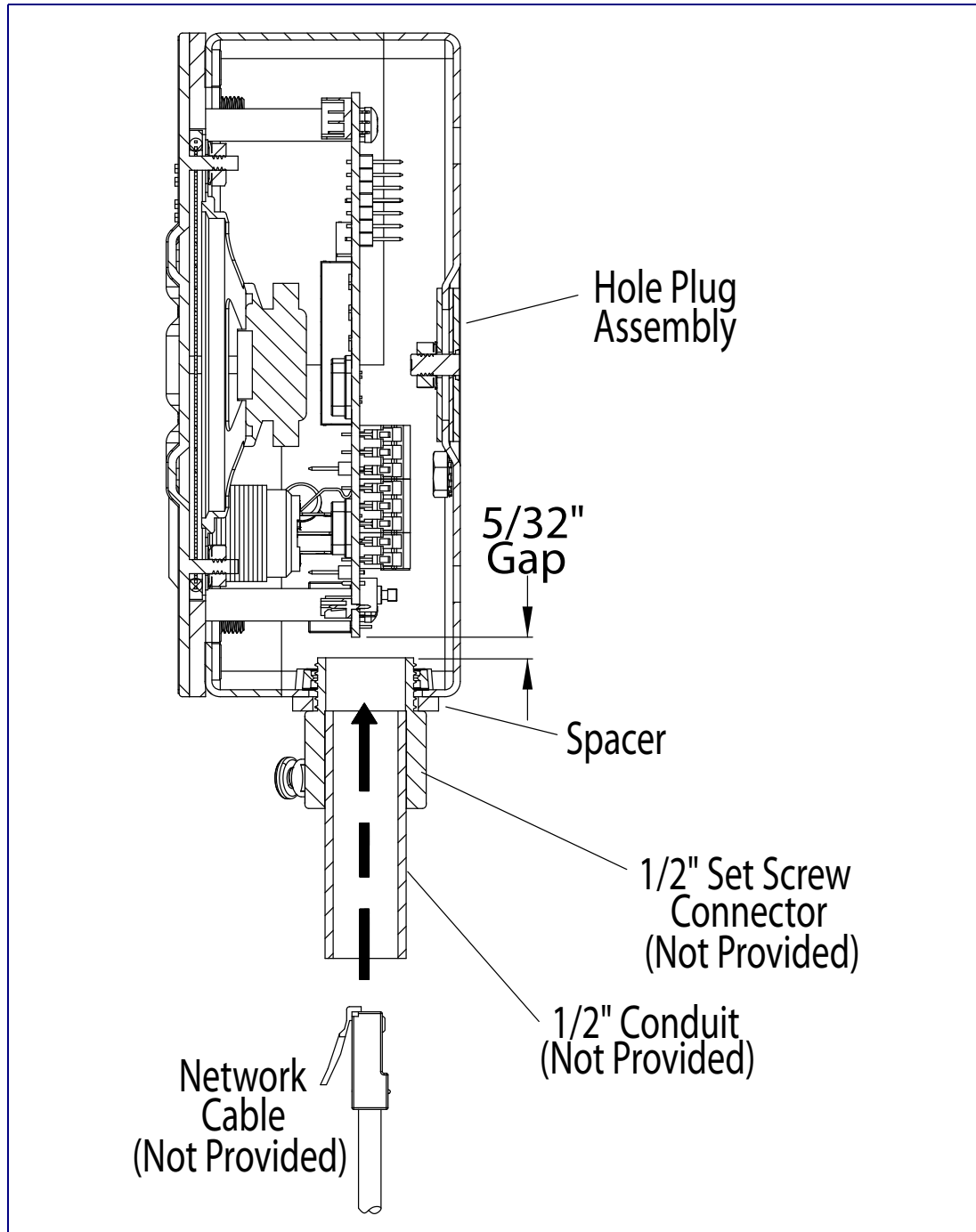
Installation Type	What You Need
Outdoor, on surface  <p>The diagram shows a rectangular intercom unit mounted on a textured surface. To the left of the unit are nine teardrop-shaped water droplets arranged in a 3x3 grid, representing rain. The intercom unit is secured to the surface with two screws along its top edge and one screw at the bottom. A cable is connected to the bottom of the unit.</p>	011410 Intercom only
Outdoor, on surface with shroud (increased resistance)  <p>The diagram shows the same intercom unit as in the first diagram, but with a large, curved, protective shroud mounted over the top and sides of the unit. To the left of the shrouded unit are nine teardrop-shaped water droplets arranged in a 3x3 grid, representing rain. The intercom unit is secured to the surface with two screws along its top edge and one screw at the bottom. A cable is connected to the bottom of the unit.</p>	011410 Intercom 011188 Weather Shroud (sold separately)

A.4 Network Cable Entry Restrictions

A.4.1 Conduit Mounting Restrictions (Side Entry)

See [Figure A-4](#) for the conduit mounting restrictions (side entry).

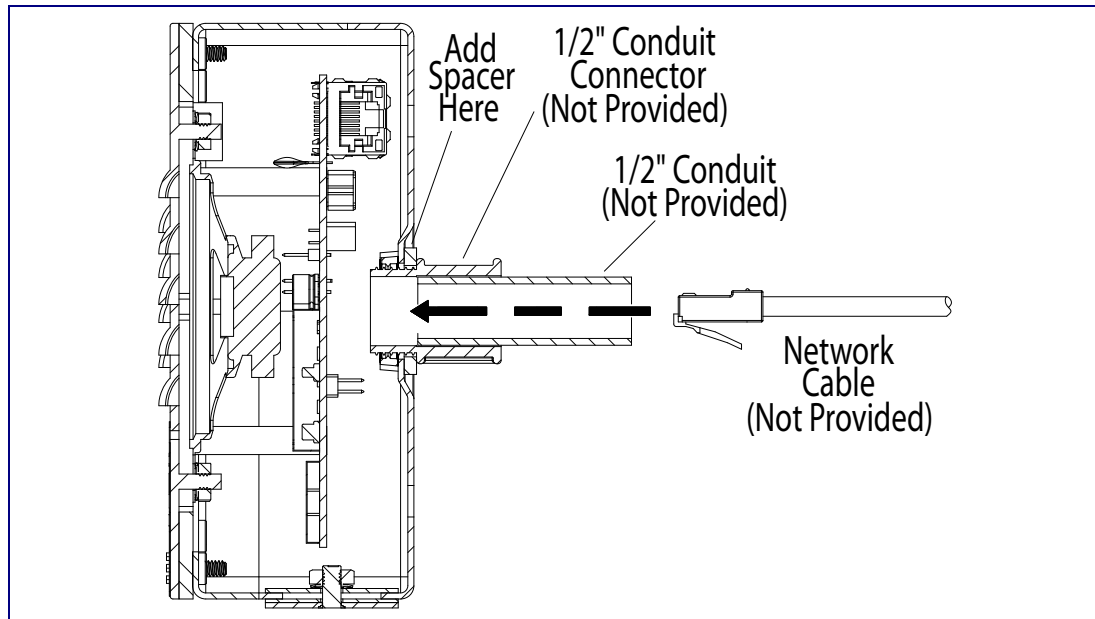
Figure A-4. Conduit Mounting Restrictions (Side Entry)



A.4.2 Conduit Mounting Restrictions (Rear Entry without Shroud)

See [Figure A-5](#) for the conduit mounting restrictions (rear entry without shroud).

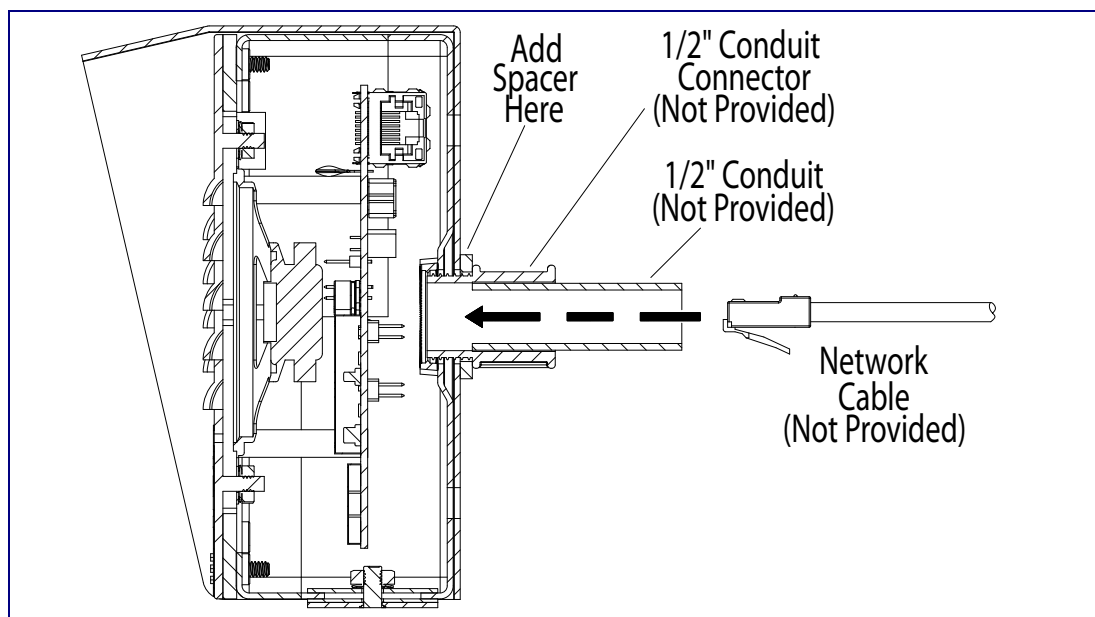
Figure A-5. Conduit Mounting Restrictions (Rear Entry without Shroud)



A.4.3 Conduit Mounting Restrictions (Rear Entry with Shroud)

See [Figure A-6](#) for the conduit mounting restrictions (rear entry with shroud).

Figure A-6. Conduit Mounting Restrictions (Rear Entry with Shroud)



A.5 Service Loop Cable Routing

Figure A-7 and Figure A-8 illustrate a service loop cable routing option for the SIP-enabled h.264 Video Outdoor Intercom.

Figure A-7. Ground Cable Service Loop Routing

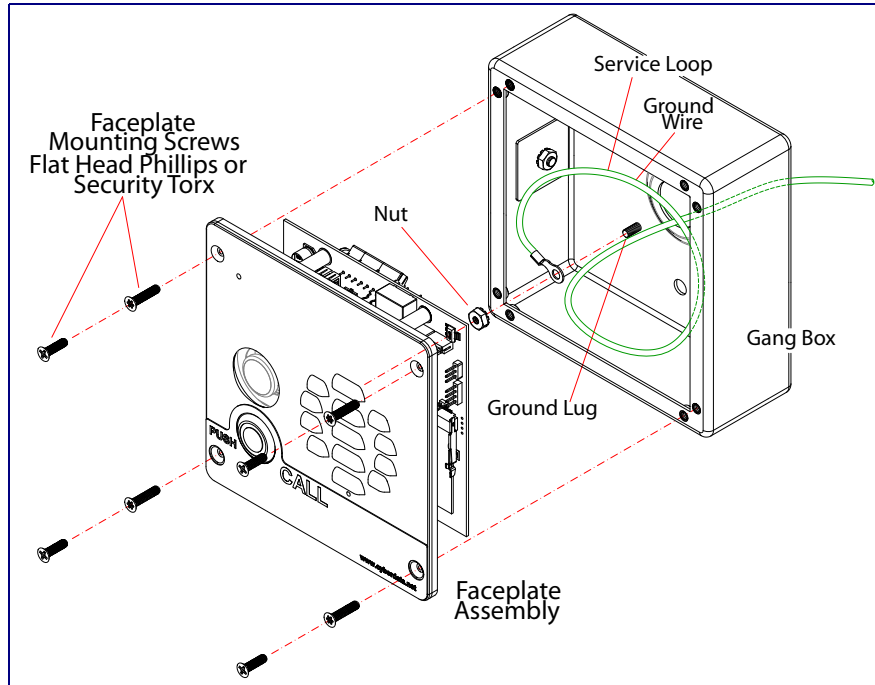
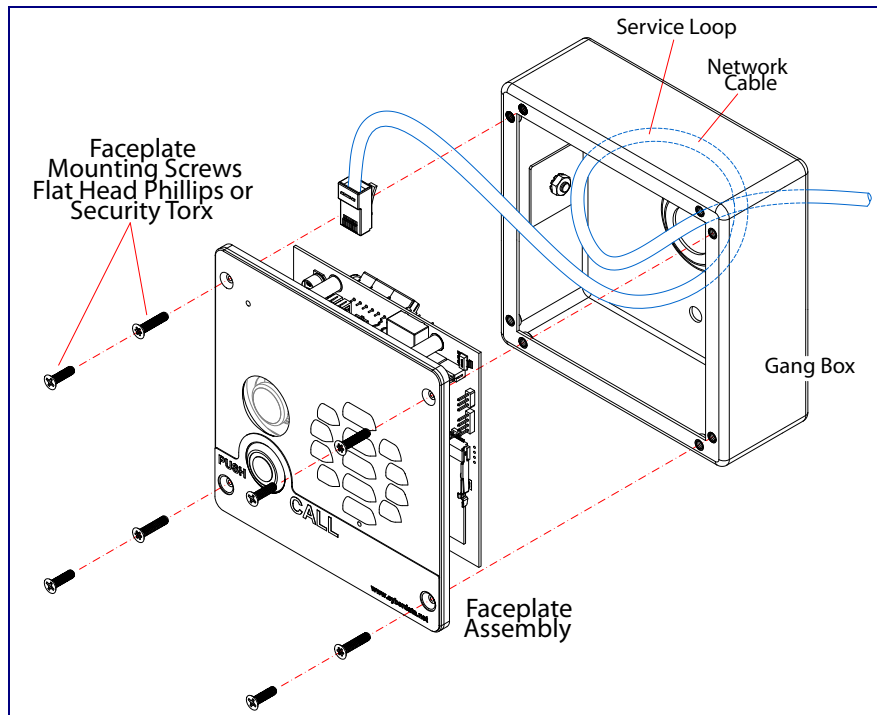


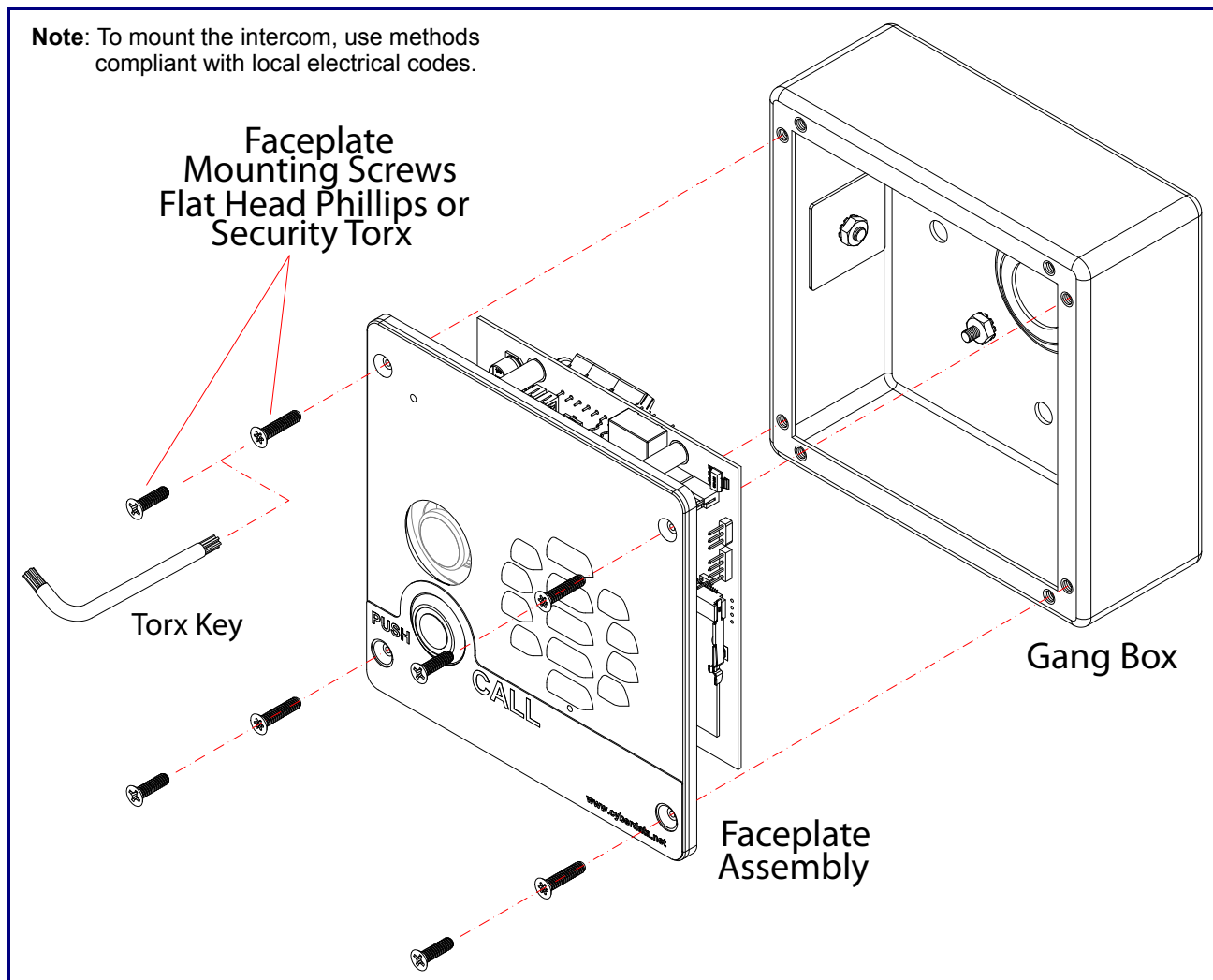
Figure A-8. Network Cable Service Loop Routing



A.6 Securing the Intercom

Figure A-9 illustrates how to secure the SIP-enabled h.264 Video Outdoor Intercom with Torx screws.

Figure A-9. Securing the Intercom



GENERAL ALERT

Caution

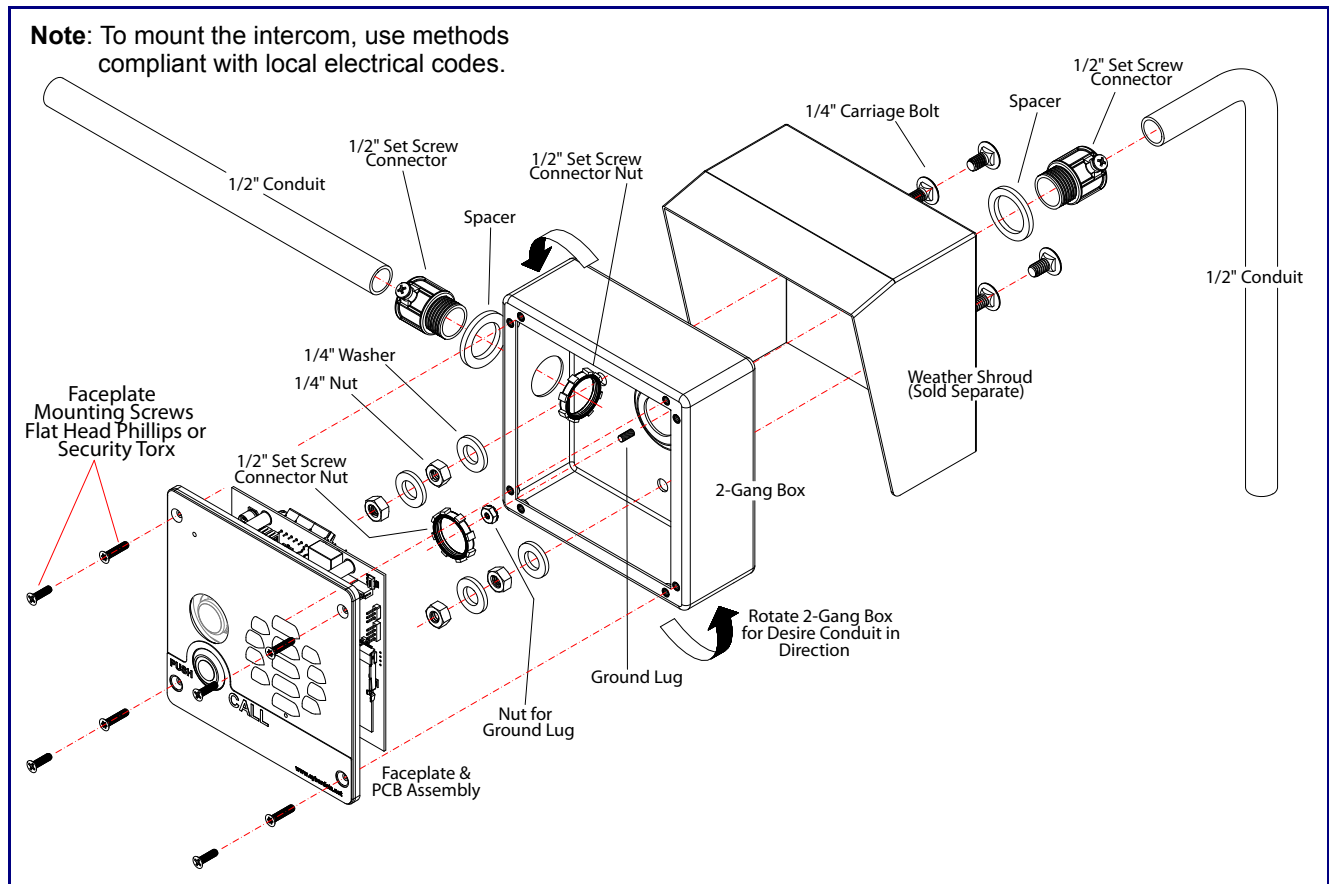
Equipment Hazard: Do not use an electric or power screwdriver to fasten the face plate and PCB assembly to the gang box. To prevent over-torque damage to the gasket, do not apply more than 10 inch-pounds force. Over-torquing will cause the gasket to tear, risk moisture intrusion, and effectively void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

A.7 Additional Mounting Options

A.7.1 Conduit Mounting Option (Not Provided)

Figure A-10 illustrates a side and rear conduit mounting option for the SIP-enabled h.264 Video Outdoor Intercom.

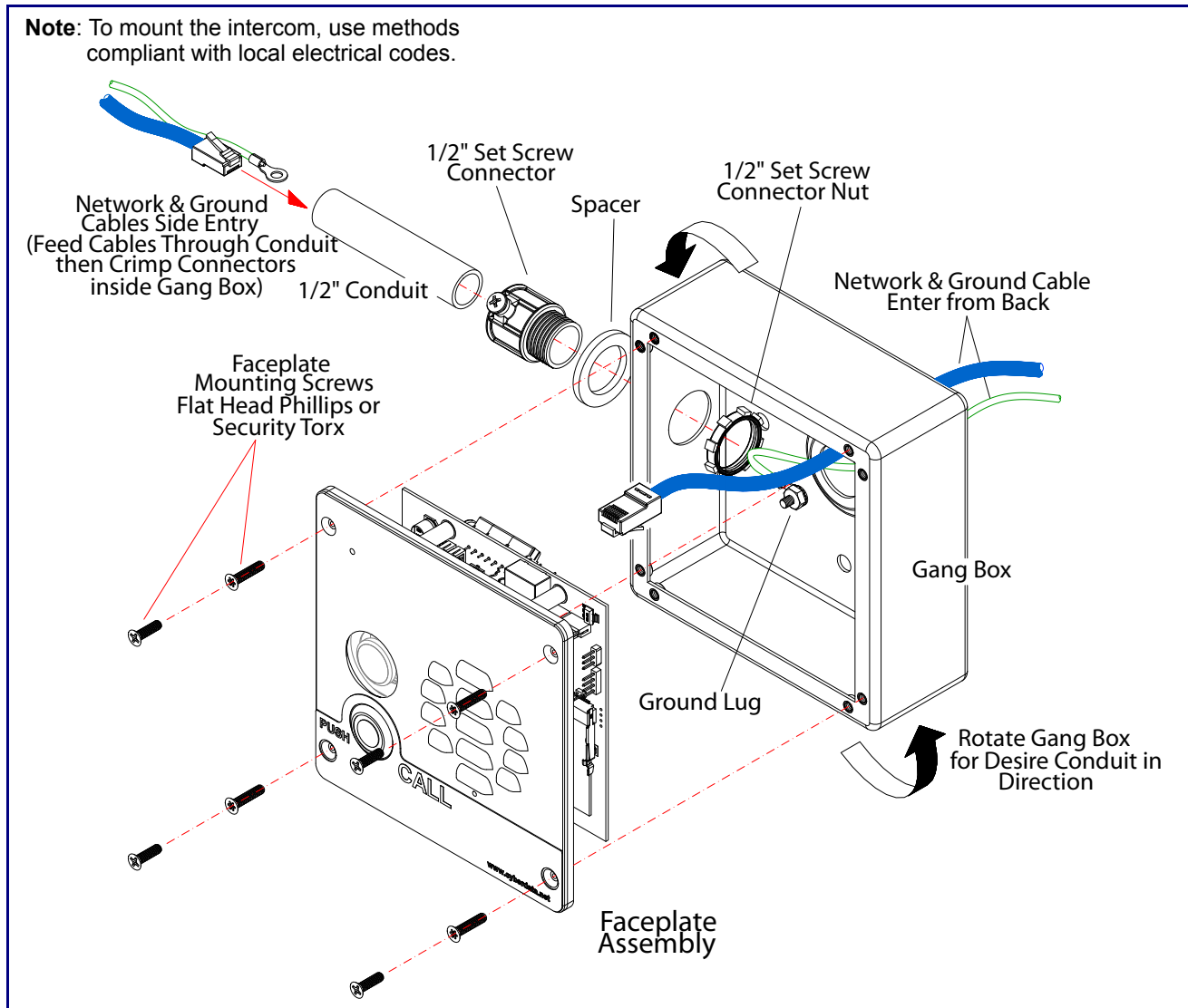
Figure A-10. Optional Conduit Mounting



A.7.2 Conduit to Gang Box Installation

Figure A-11 illustrates a conduit to gang box installation option for the SIP-enabled h.264 Video Outdoor Intercom.

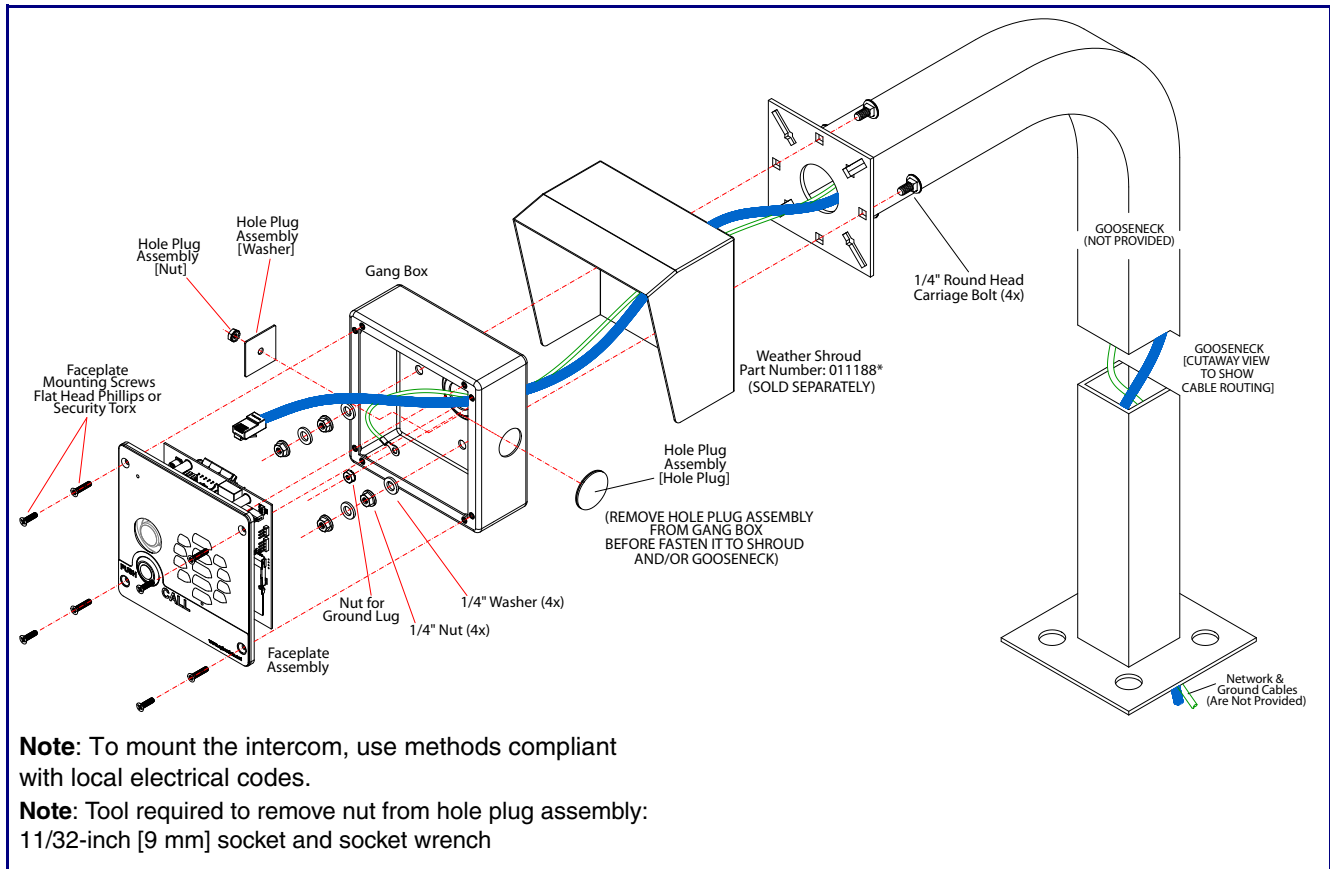
Figure A-11. Optional Conduit to Gang Box Installation



A.7.3 Gooseneck Mounting Option (Not Provided)

Figure A-12 illustrates a gooseneck mounting option for the SIP-enabled h.264 Video Outdoor Intercom.

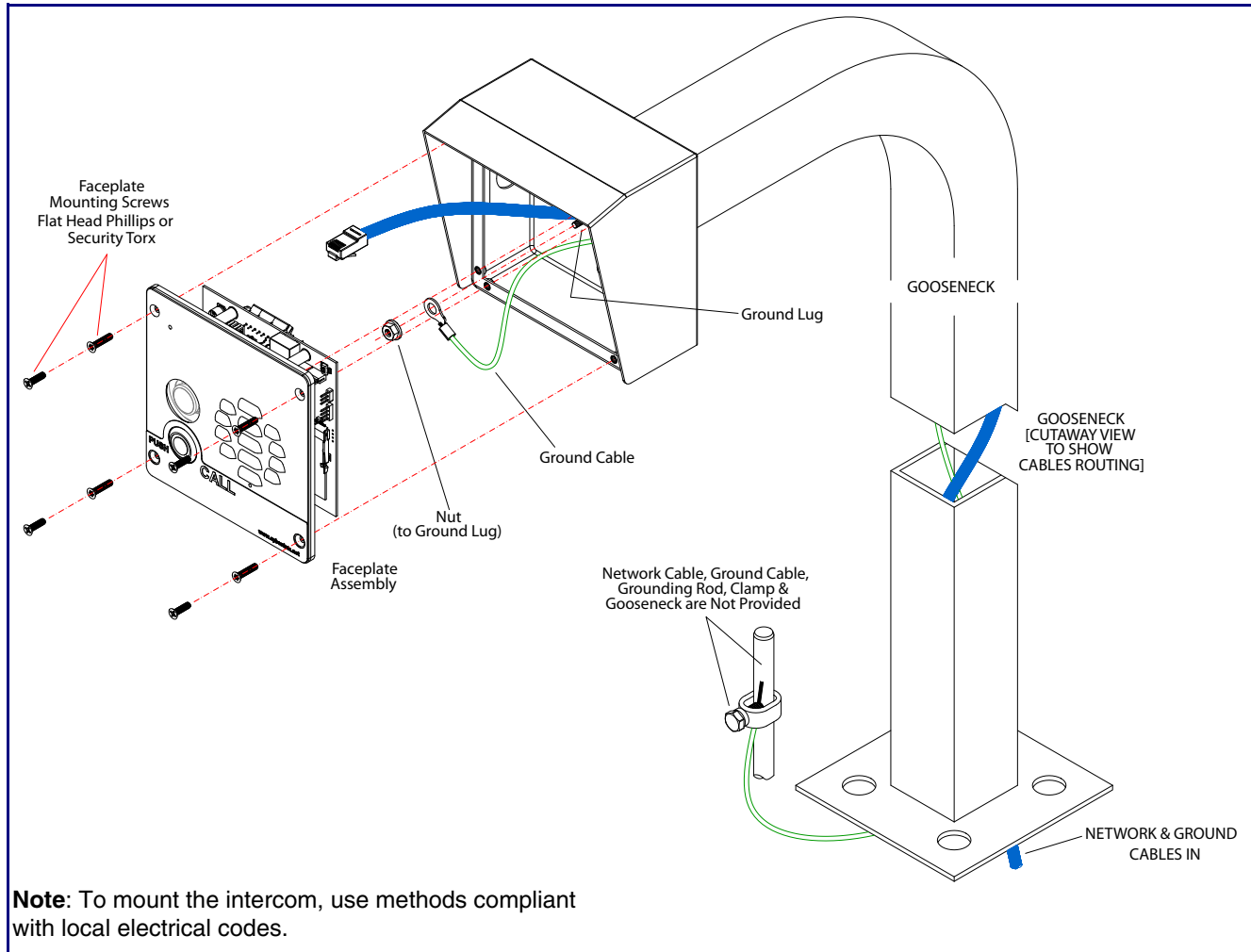
Figure A-12. Optional Gooseneck Mounting



A.7.4 Ground Cable Installation for Gooseneck Mounting Option

Figure A-13 illustrates the correct ground cable installation for the gooseneck mounting option.

Figure A-13. Ground Cable Installation for 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 from the following website address:

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

To set up a TFTP server on Windows:

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

Appendix C: Troubleshooting/Technical Support

C.1 Frequently Asked Questions (FAQ)

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

<http://www.cyberdata.net/voip/011410/>

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/011410/>

C.3 Contact Information

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

Sales Sales 831-373-2601, Extension 334

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

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

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

Phone: (831) 373-2601, Extension 333

C.4 Warranty and RMA Information

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

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

Index

Numerics

16 AWG gauge wire 12

A

activate relay (door sensor) 56
 activate relay (intrusion sensor) 56
 activity LED 20
 address, configuration login 29
 alternative power input 5
 announcing a device's IP address 22
 audio configuration 58
 night ring tone parameter 60
 audio configuration page 58
 audio encodings 4
 audio files, user-created 62
 autoprovision at time (HHMMSS) 71
 autoprovision when idle (in minutes > 10) 71
 autoprovisioning 72
 download template button 72
 setting up a TFTP server 104
 autoprovisioning autoupdate (in minutes) 71
 autoprovisioning configuration 70, 71
 autoprovisioning filename 71
 autoprovisioning server (IP Address) 71

B

backup SIP server 1 45
 backup SIP server 2 45
 backup SIP servers, SIP server
 backups 45

C

call button 24
 call button LED 24
 call termination 36
 changing
 the web access password 33
 command interface 88
 commands 88
 concrete wall mounting option (not provided) 101
 conduit mounting option (not provided) 100
 configurable parameters 34, 39, 42, 45

configuration
 audio 58
 default IP settings 25
 door sensor 54
 intrusion sensor 54
 network 38, 41
 SIP 44
 configuration home page 29
 configuration page
 configurable parameters 34, 39, 42
 contact information 106
 contact information for CyberData 106
 current network settings 42
 CyberData contact information 106

D

default
 gateway 25
 intercom settings 107
 IP address 25
 subnet mask 25
 username and password 25
 web login username and password 29
 default gateway 25, 42
 default intercom settings 23
 default IP settings 25
 default login address 29
 device configuration 33
 device configuration parameters 71
 the device configuration page 70
 device configuration page 33
 device configuration parameters 34
 device configuration password
 changing for web configuration access 33
 DHCP Client 4
 dial out extension (door sensor) 56
 dial out extension (intrusion sensor) 56
 dial out extension strings 48
 dial-out extension strings 49
 dimensions 5, 93
 shroud dimensions and mounting hole locations 94
 unit dimensions—front and side view 93
 unit dimensions—rear view and mounting hole
 locations 94
 discovery utility program 29
 DNS server 42
 door sensor 54, 56
 activate relay 56
 dial out extension 56

- door open timeout 56
- door sensor normally closed 56
- flash button LED 56
- play audio locally 56
- download autoprovisioning template button 72
- DTMF push to talk 36
- DTMF tones 48, 49
- DTMF tones (using rfc2833) 48

E

- electric screwdriver 99
- enable night ring events 65
- ethernet I/F 5
- event configuration
 - enable night ring events 65
- expiration time for SIP server lease 45, 46, 47
- export settings 32

F

- factory default settings 23
- fastening, gang box 99
- firmware
 - where to get the latest firmware 82, 84
- flash button LED (door sensor) 56
- flash button LED (intrusion sensor) 56

G

- gang box, fastening 99
- gasket, avoid over-torque damage 99
- get autoprovisioning template 72
- goose neck mounting option (not provided) 102
- ground cable installation 98
- ground cable installation for goose neck mounting
 - option 103

H

- home page 29
- http POST command 88
- http web-based configuration 4

I

- identifying your product 1

- import settings 32
- import/export settings 32
- installation, typical intercom system 2
- intercom configuration
 - default IP settings 25
- intercom configuration page
 - configurable parameters 45
- intrusion sensor 54, 56
 - activate relay 56
 - dial out extension 56
 - flash button LED 56
 - play audio locally 56
- IP address 25, 42
- IP addressing
 - default
 - IP addressing setting 25

J

- J3 terminal block, 16 AWG gauge wire 12

L

- lease, SIP server expiration time 45, 46, 47
- LED
 - green link LED 20
 - yellow activity LED 20
- lengthy pages 53
- link LED 20
- Linux, setting up a TFTP server on 104
- local SIP port 46
- log in address 29

M

- MGROUP
 - MGROUP Name 52
- mounting 92
 - additional mounting options 100
 - concrete wall mounting option (not provided) 101
 - conduit mounting option (not provided) 100
 - goose neck mounting option (not provided) 102
 - ground cable installation 98
 - ground cable installation for goose neck mounting
 - option 103
 - network cable entry restrictions 96
 - optional accessories 92
 - overview of installation types 92, 95
 - rear conduit network cable entry restrictions (with shroud) 97
 - rear conduit network cable entry restrictions (without

- shroud) 97
- securing the intercom 99
- service loop cable routing 98
- side conduit network cable entry restrictions 96
- mounting components 92
- multicast configuration 58
- Multicast IP Address 52

N

- navigation (web page) 26
- navigation table 26
- network cable entry restrictions 96
- network configuration 38, 41
- nightring tones 53
- Nightringer 12, 81
- nightringer settings 46
- NTP server 35

O

- on-board relay 5, 14
- operating temperature 5
- overview of installation types 95

P

- packet time 4
- pages (lengthy) 53
- part number 5
- parts list 6
- password
 - for SIP server login 45
 - login 29
 - restoring the default 25
- payload types 5
- play audio locally (door sensor) 56
- play audio locally (intrusion sensor) 56
- point-to-point configuration 49
- port
 - local SIP 46
 - remote SIP 46
- POST command 88
- power input 5
 - alternative 5
- power screwdriver 99
- priority
 - assigning 53
- 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 36

R

- rear conduit network cable entry restrictions (with shroud) 97
- rear conduit network cable entry restrictions (without shroud) 97
- reboot 86
- remote SIP port 46
- reset test function management button 21
- resetting the IP address to the default 92, 105
- restoring factory default settings 23, 107
- ringtones 53
 - lengthy pages 53
- RJ-45 19
- rport discovery setting, disabling 46
- RTFM button 21
- RTFM jumper 21, 22, 23
- RTP/AVP 4

S

- sales 106
- securing the device 99
- sensor setup page 55
- sensor setup parameters 54
- sensors 56
- server address, SIP 45
- service 106
- service loop cable routing 98
- setting up the device 8
- settings, default 23
- shroud dimensions and mounting hole locations 94
- side conduit network cable entry restrictions 96
- SIP
 - enable SIP operation 45
 - local SIP port 46
 - user ID 45
- SIP configuration 44
- SIP configuration parameters
 - outbound proxy 46
 - registration and expiration, SIP server lease 45, 46, 47
 - unregister on reboot 46

- user ID, SIP 45
- SIP registration 46
- SIP remote SIP port 46
- SIP server 45
 - password for login 45
 - SIP servers supported 4
 - unregister from 46
 - user ID for login 45
- SIP server configuration 45
- SIP volume 34
- speaker output 5
- subnet mask 25, 42
- supported protocols 4

T

- tech support 106
- technical support, contact information 106
- terminal block, 16 AWG gauge wire 12
- TFTP server 4, 104

U

- unit dimensions—front and side view 93
- unit dimensions—rear view and mounting hole
 - locations 94
- user ID
 - for SIP server login 45
- username
 - changing for web configuration access 33
 - default for web configuration access 29
 - restoring the default 25

V

- video parameters 38
- video, field of view 11
- video, mechanical adjustment 8
- VLAN ID 42
- VLAN tagging support 42
- VLAN tags 42
- volume
 - microphone gain 34
 - multicast volume 34
 - ring volume 34
 - sensor volume 34
 - SIP volume 34

W

- warranty policy at CyberData 106
- web access password 25
- web access username 25
- web configuration log in address 29
- web page
 - navigation 26
- web page navigation 26
- wget, free unix utility 88
- Windows, setting up a TFTP server on 104
- wiring the circuit 15
 - devices less than 1A at 30 VDC 15