

VoIP V3 Emergency Intercom Operations Guide

Part #011209*, RAL 9003, Signal White Color

*Replaces #011035

*Document Part #930504E
for Firmware Version 7.1.6*

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

VoIP V3 Emergency Intercom Operations Guide 930504E
Part # 011209*
***Replaces 011035.**

COPYRIGHT NOTICE:

© 2013, 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://www.cyberdata.net/support/contactsupportvoip.html>

Phone: (831) 373-2601, Ext. 333



Email: support@cyberdata.net

Fax: (831) 373-4193



Company and product information is at www.cyberdata.net.

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.

| | |
|--|--|
|  <p>GENERAL ALERT</p> | <p>Warning</p> <p><i>Electrical Hazard:</i> This product should be installed by a licensed electrician according to all local electrical and building codes.</p> |
|  <p>GENERAL ALERT</p> | <p>Warning</p> <p><i>Electrical Hazard:</i> To prevent injury, this apparatus must be securely attached to the floor/wall in accordance with the installation instructions.</p> |

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.

Revision Information

Revision 930504E, which was released on February 15, 2013 and corresponds to firmware version 7.1.6, has the following changes:

- Updates [Section 1.6, "Product Specifications"](#).

Contents

| | |
|---|-----------|
| 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 Product Specifications | 5 |
| 1.7 Dimensions | 6 |
| | |
| Chapter 2 Installing the VoIP V3 Emergency Intercom | 9 |
| 2.8 Parts List | 9 |
| 2.9 Intercom Components | 10 |
| 2.9.1 Call Button and the Call Button LED | 10 |
| 2.10 Intercom Setup | 12 |
| 2.10.1 Intercom Connections | 12 |
| 2.10.2 Connecting the Intercom to the Auxiliary Relay | 13 |
| 2.10.3 Identifying the VoIP Intercom Connectors | 15 |
| 2.10.4 Network Connectivity, and Data Rate | 17 |
| 2.10.5 RTFM Button | 19 |
| 2.10.6 Adjust the Volume | 20 |
| 2.11 Configure the Intercom Parameters | 21 |
| 2.11.1 Factory Default Settings | 21 |
| 2.11.2 Intercom Web Page Navigation | 22 |
| 2.11.3 Log in to the Configuration Home Page | 23 |
| 2.11.4 Configure the Device | 26 |
| 2.11.5 Configure the Network Parameters | 29 |
| 2.11.6 Configure the SIP Parameters | 31 |
| 2.11.7 Configure the Nightringer Parameters | 36 |
| 2.11.8 Configure the Sensor Configuration Parameters | 38 |
| 2.11.9 Configure the Multicast Parameters | 41 |
| 2.11.10 Configure the Audio Configuration Parameters | 43 |
| 2.11.11 Configure the Event Parameters | 48 |
| 2.11.12 Configure the Autoprovisioning Parameters | 53 |
| 2.12 Upgrade the Firmware and Reboot the Intercom | 58 |
| 2.12.1 Uploading the Firmware | 58 |
| 2.12.2 Reboot the Intercom | 60 |
| 2.13 Command Interface | 61 |
| 2.13.1 Command Interface Post Commands | 61 |
| | |
| Appendix A Mounting the Indoor Intercom | 65 |
| A.1 Wall Mounting Components | 65 |
| A.2 PCB Dimensions | 70 |
| | |
| Appendix B Setting up a TFTP Server | 71 |
| B.1 Set up a TFTP Server | 71 |
| B.1.1 In a LINUX Environment | 71 |
| B.1.2 In a Windows Environment | 71 |
| | |
| Appendix C Troubleshooting/Technical Support | 72 |
| C.1 Frequently Asked Questions (FAQ) | 72 |

C.2 Documentation72
C.3 Contact Information73
C.4 Warranty74
 C.4.1 Warranty & RMA Returns within the United States74
 C.4.2 Warranty & RMA Returns Outside of the United States74
 C.4.3 Spare in the Air Policy74
 C.4.4 Return and Restocking Policy75
 C.4.5 Warranty and RMA Returns Page75

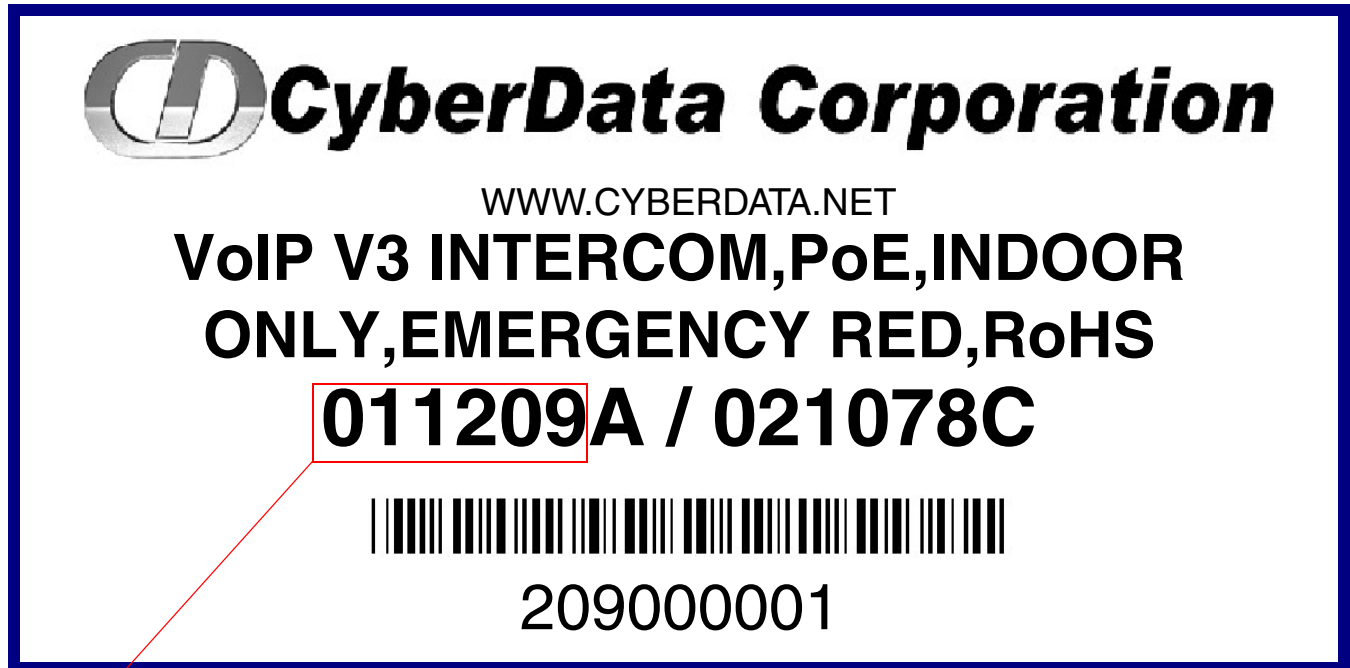
Index **76**

1 Product Overview

1.1 How to Identify This Product

To identify the VoIP V3 Emergency Intercom, look for a model number label similar to the one shown in [Figure 1-1](#). The model number on the label should be **011209**.

Figure 1-1. Model Number Label



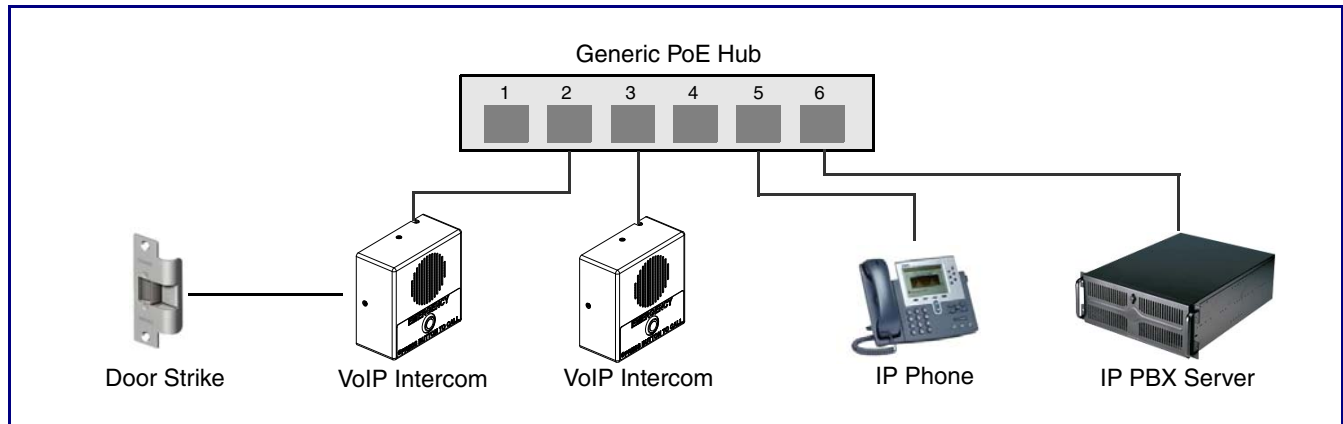
Model number




1.2 Typical System Installation

The Voice-over-IP (VoIP) VoIP V3 Emergency Intercom is a SIP endpoint designed to provide VoIP phone connectivity in a tamper proof and secure package.

Figure 1-2 illustrates how the VoIP V3 Emergency Intercom can be installed as part of a VoIP phone system.

Figure 1-2. Typical Installation—Door Entry/Access Control



| | |
|--|--|
|  GENERAL ALERT | <p>Warning Electrical Hazard: The VoIP Intercom enclosure is not rated for any AC voltages.</p> |
|  GENERAL ALERT | <p>Warning Electrical Hazard: This product should be installed by a licensed electrician according to all local electrical and building codes.</p> |
|  GENERAL ALERT | <p>Warning Electrical Hazard: To prevent injury, this apparatus must be securely attached to the floor/wall in accordance with the installation instructions.</p> |

1.3 Product Features

The VoIP V3 Emergency Intercom has the following features:

- Supports SRST (Survivable Remote Site Telephony) in a Cisco environment. SRST parameters are entered statically into the CyberData product's internal webpage.
- SIP compliant
- Dual speeds of 10 Mbps and 100 Mbps
- PoE 802.3af-enabled (Powered-over-Ethernet)
- Adaptive full duplex voice operation
- Network/Web management
- Network configurable speaker volume
- Network configurable door or intrusion sensor settings
- Network configurable relay activation settings
- Dial out extension supports the addition of comma delimited pauses before sending additional DTMF tones
- Network configurable microphone input sensitivity adjustment
- Network downloadable product firmware
- Doubles as a paging speaker
- Call button
- Call activity indicator (Call Button LED)

Note An active call is indicated by the Call Button LED blinking at one second intervals.

- Tamper proof design
- Concurrent SIP and multicast paging
- Dry contact relay for auxiliary control

Note 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.

- Autoprovisioning
- Configurable audio files
- Night Ringer
- Three year warranty
- Door closure and tamper alert signal
- Peer-to-peer capable

1.4 Supported Protocols

The Intercom supports:

- SIP
- HTTP Web-based configuration
Provides an intuitive user interface for easy system configuration and verification of Intercom operations.
- DHCP Client
Dynamically assigns IP addresses in addition to the option to use static addressing.
- TFTP Client
Facilitates hosting for the Autoprovisioning configuration file.
- RTP
- RTP/AVP - Audio Video Profile
- Facilitates autoprovisioning configuration values on boot
- Packet Time 20 ms
- Audio Encodings
PCMU (G.711 mu-law)
PCMA (G.711 A-law)

1.5 Supported SIP Servers

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

<http://www.cyberdata.net/support/voip/server.html>

1.6 Product Specifications

Table 1-1. Specifications

| Category | Specification |
|-----------------------|--|
| Speaker Output | 1 Watt Peak Power |
| Ethernet I/F | 10/100 Mbps |
| Protocol | SIP RFC 3261 Compatible |
| Power Input | PoE 802.3af compliant or +12 to 24 VDC at 1000 mA (500 mA minimum) |
| Operating Temperature | -10° C to 50° C (14° F to 122° F) |
| Payload Types | G711, A-law and μ -law |
| Auxiliary Relay | 1A at 30 VDC |
| Dimensions | 5.118" x 5.118" x 2.25" (H x W x D) |
| Weight | 0.71 lbs./shipping weight of 1.1 lbs. (0.32 kg/shipping weight of 0.5 kg) |
| Part Number | 011209 ^a |

a. This number replaces the 011035 number.

1.7 Dimensions

Figure 1-3. Dimensions—Unit Dimensions

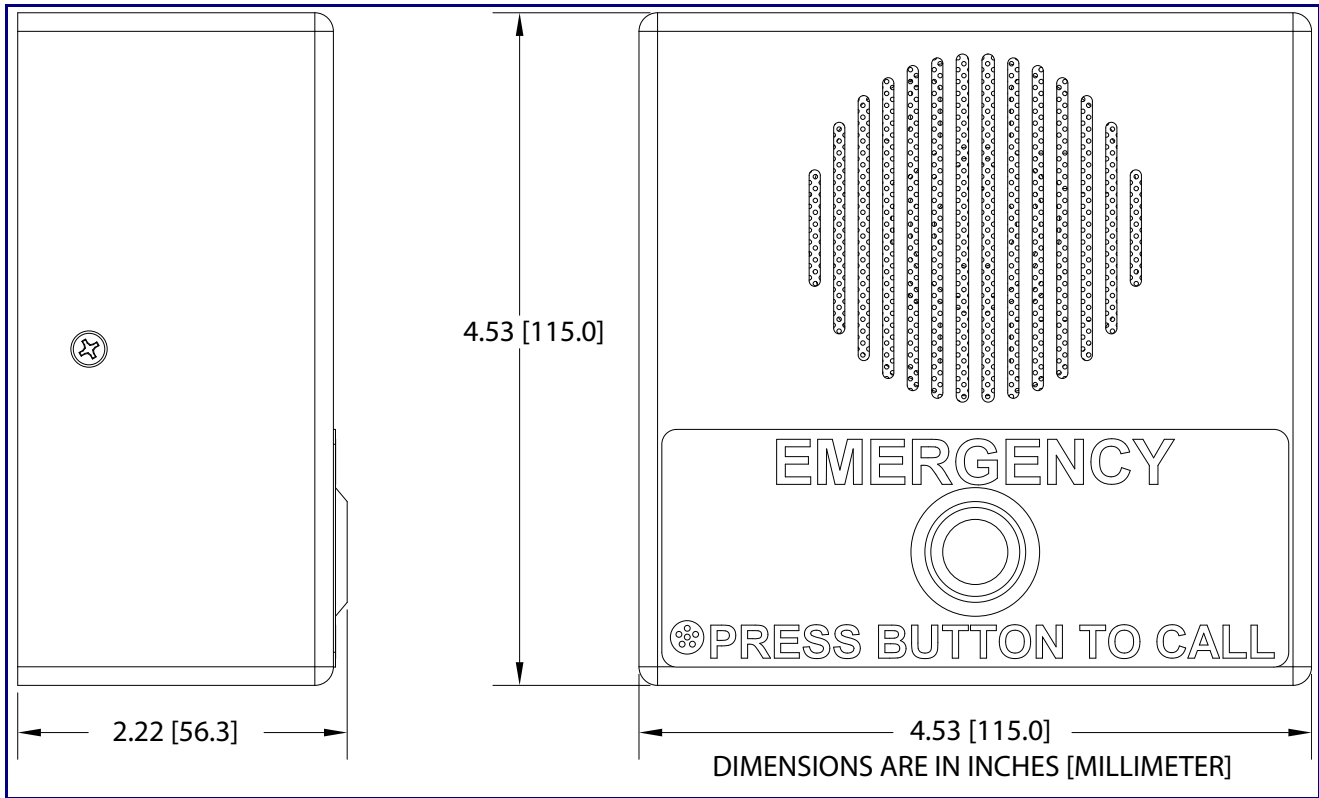


Figure 1-4. Label Dimensions

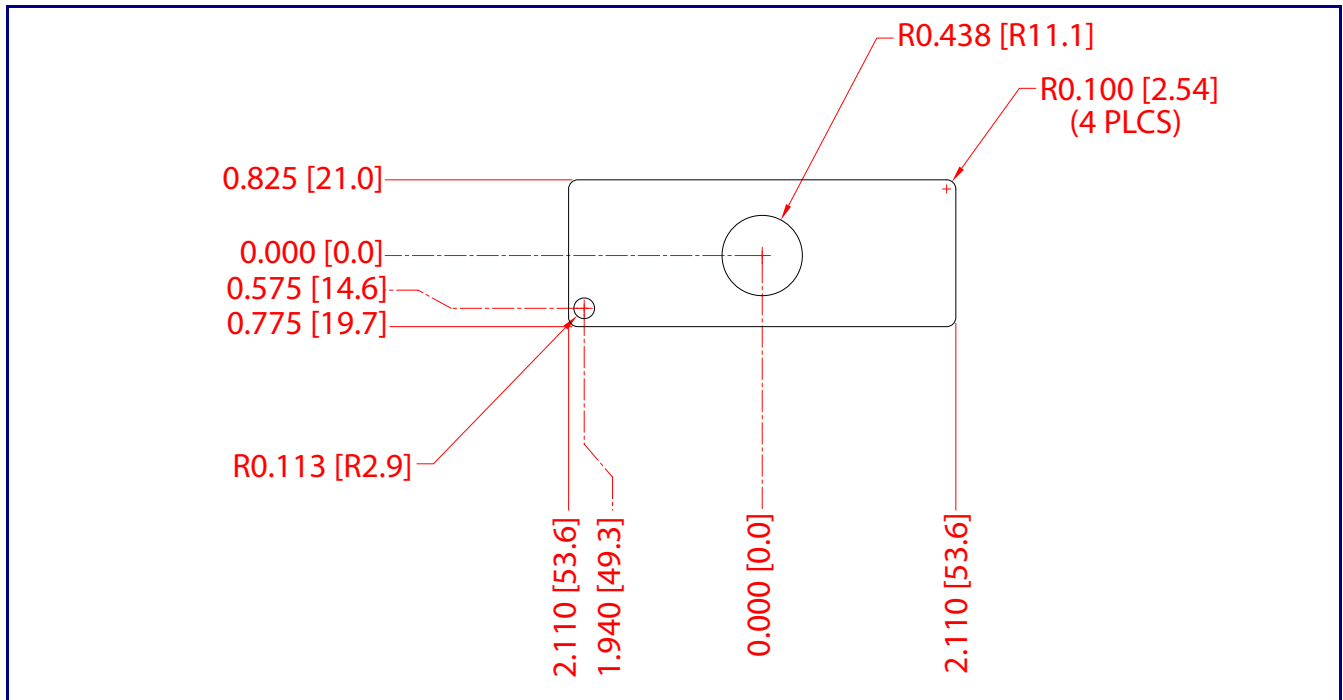


Figure 1-5. Label Alignment

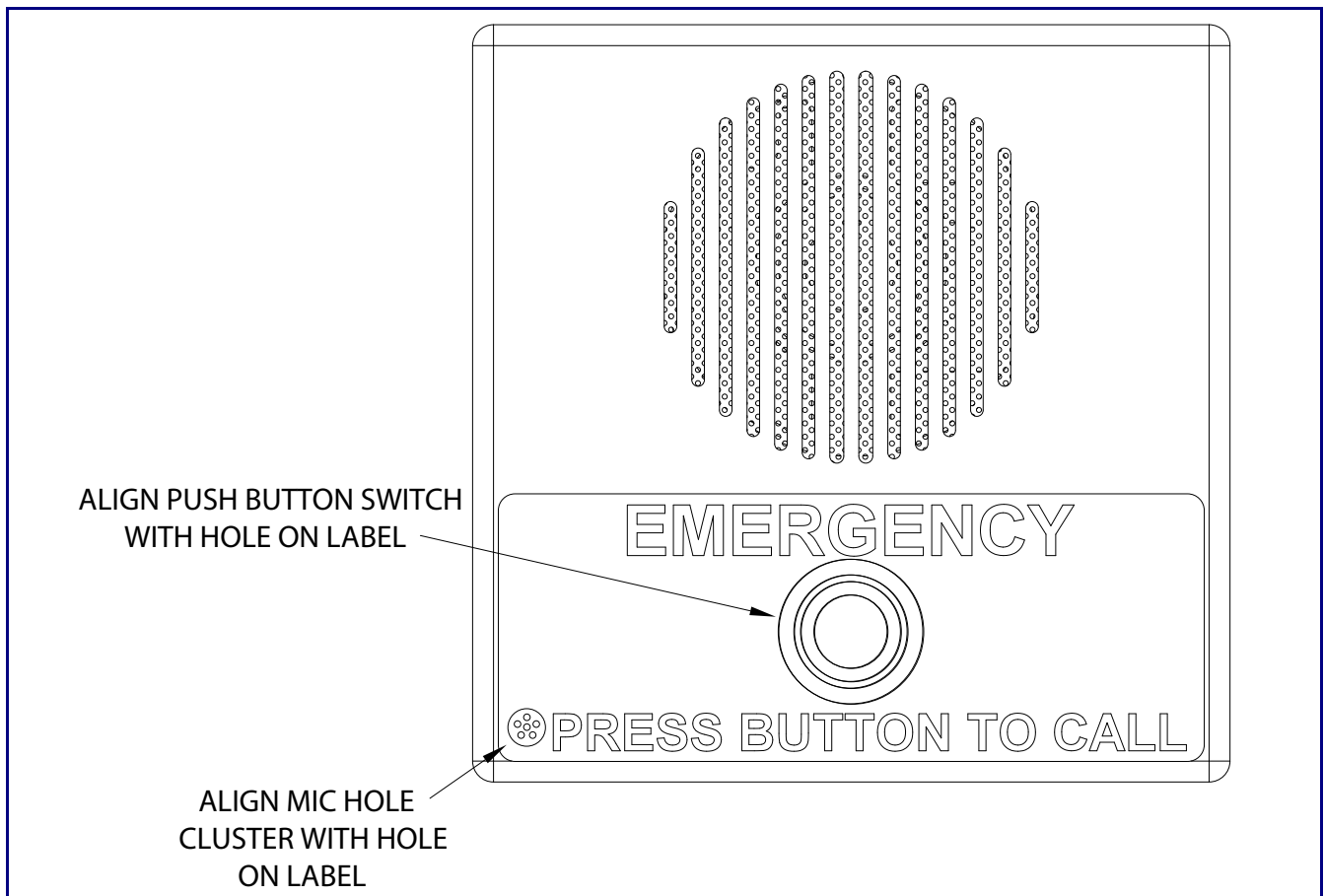
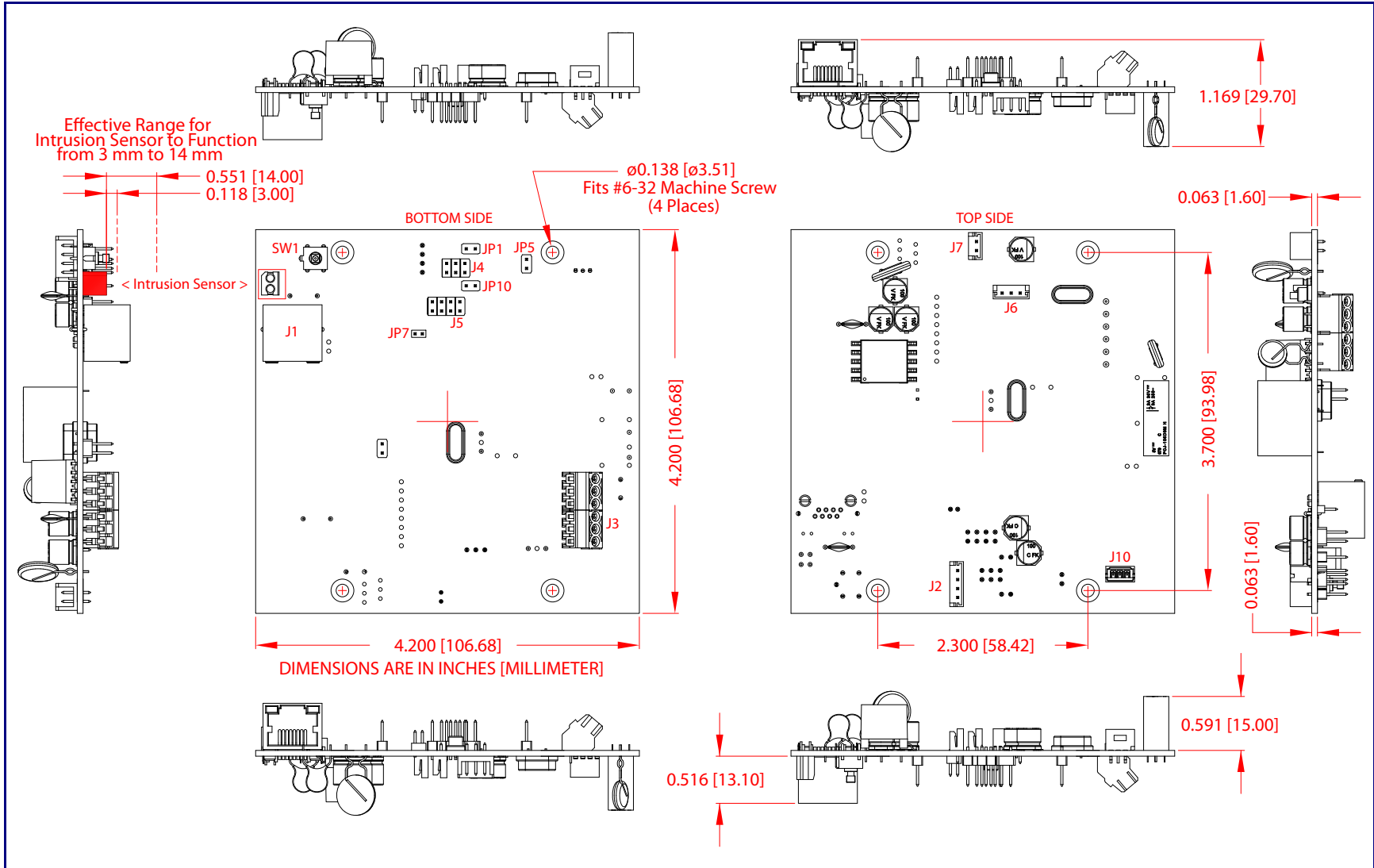


Figure 1-6. PCB Dimensions and Intrusion Sensor Range

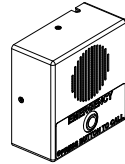




2 Installing the VoIP V3 Emergency Intercom

2.8 Parts List

Table 2-2 illustrates the VoIP V3 Emergency Intercom parts.

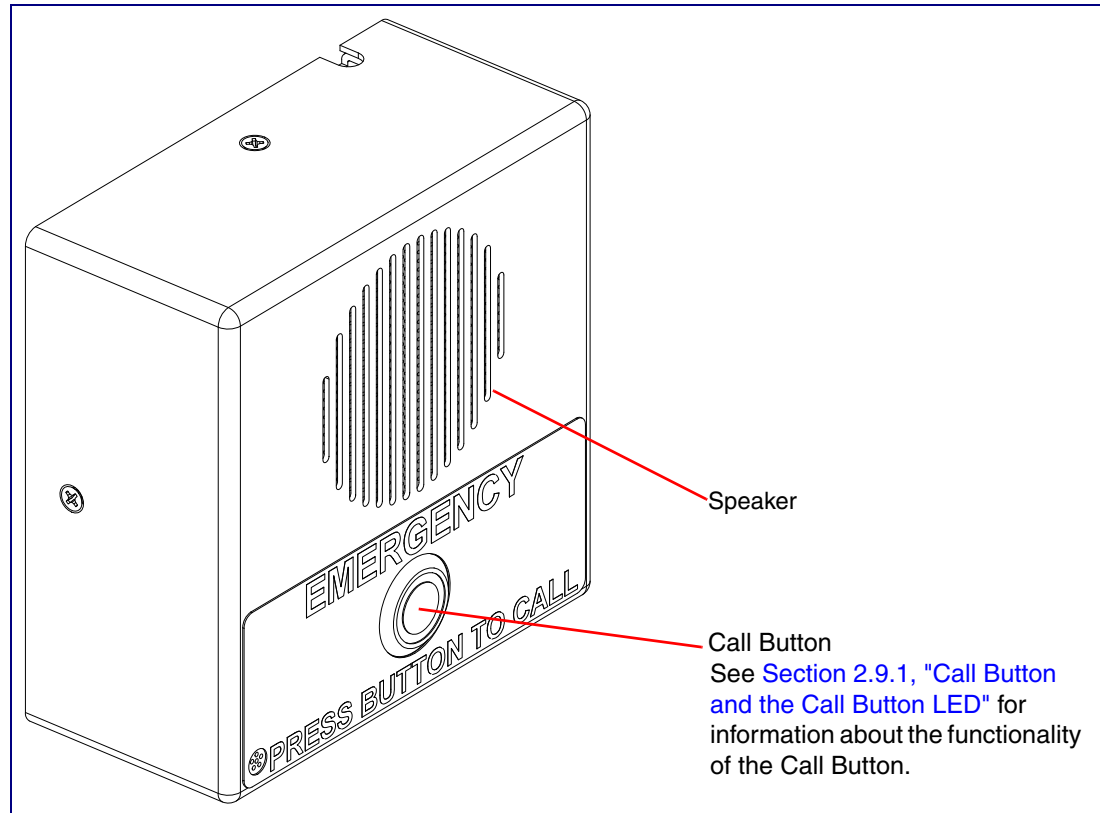
Table 2-2. Parts List

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

2.9 Intercom Components

Figure 2-7 shows the components of the Intercom .

Figure 2-7. Intercom Components



2.9.1 Call Button and the Call Button LED

2.9.1.1 Calling with the The Call Button

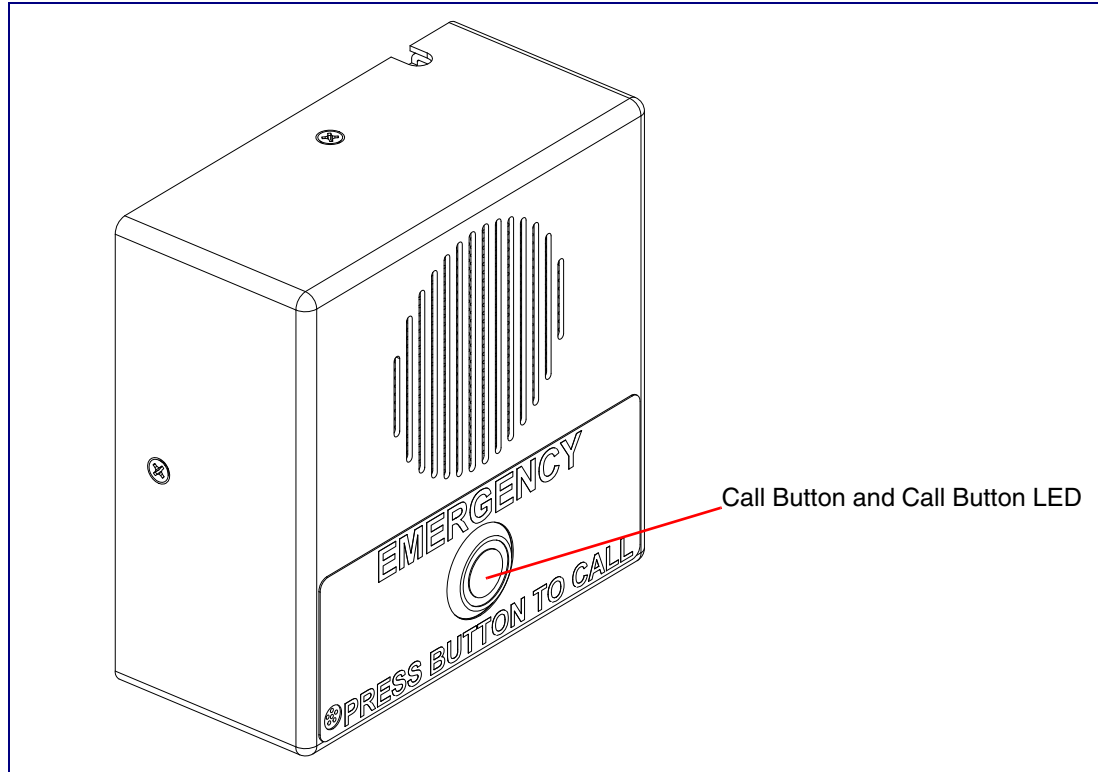
- You may initiate a call by pressing the **Call** button.
- An active call is indicated by the Call Button LED blinking at one second intervals.
- The Intercom can automatically answer an incoming call.
- You can press the **Call** button to terminate an active call whether the call was an incoming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

2.9.1.2 Call Button LED Function

- Upon initial power or reset, the Call Button LED will illuminate.
- When the software has finished initialization, the Call Button LED will blink twice.
- When a call is established (not just ringing), the Call Button LED will blink.

- On the **Device Configuration Page**, there is an option called **Button Lit When Idle**. This option sets the normal state for the indicator light. The Call Button LED will still blink during initialization and calls.
- The Call Button LED flashes briefly at the beginning of RTFM mode.

Figure 2-8. Call Button and Call Button LED



2.10 Intercom Setup

2.10.1 Intercom Connections

Figure 2-9 shows the pin connections on the J3 (terminal block). This terminal block can accept 16 AWG gauge wire.

Note As an alternative to using PoE power, you can supply +12 to 24 VDC at 1000 mA (500 mA minimum) into the terminal block.


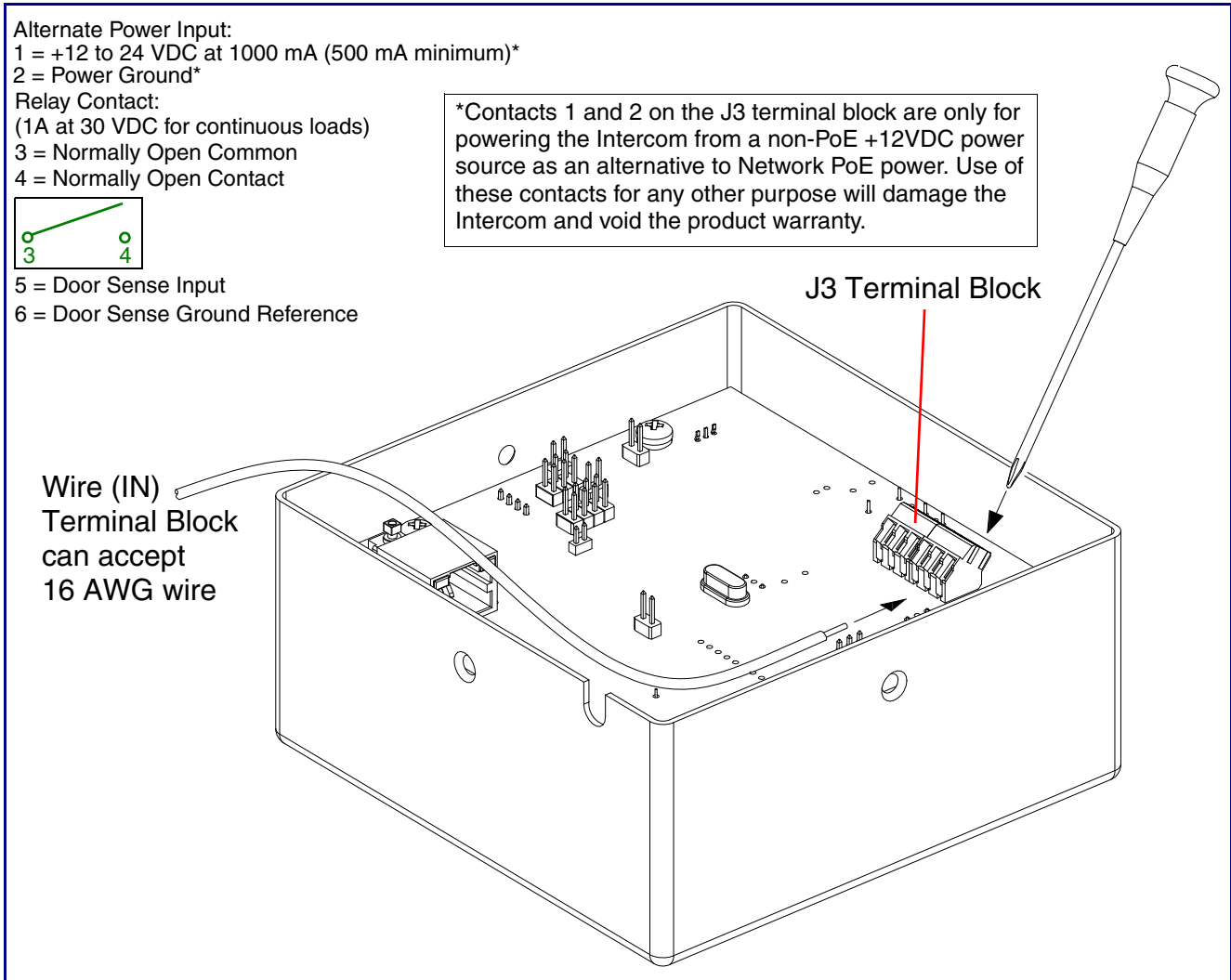




| | |
|---|---|
|  | <p>Caution</p> <p>Equipment Hazard: Contacts 1 and 2 on the J3 terminal block are only for powering the Intercom from a non-PoE +12VDC power source as an alternative to Network PoE power. Use of these contacts for any other purpose will damage the Intercom and void the product warranty.</p> |
|---|---|

Figure 2-9. Intercom Connections



2.10.2 Connecting the Intercom to the Auxiliary Relay

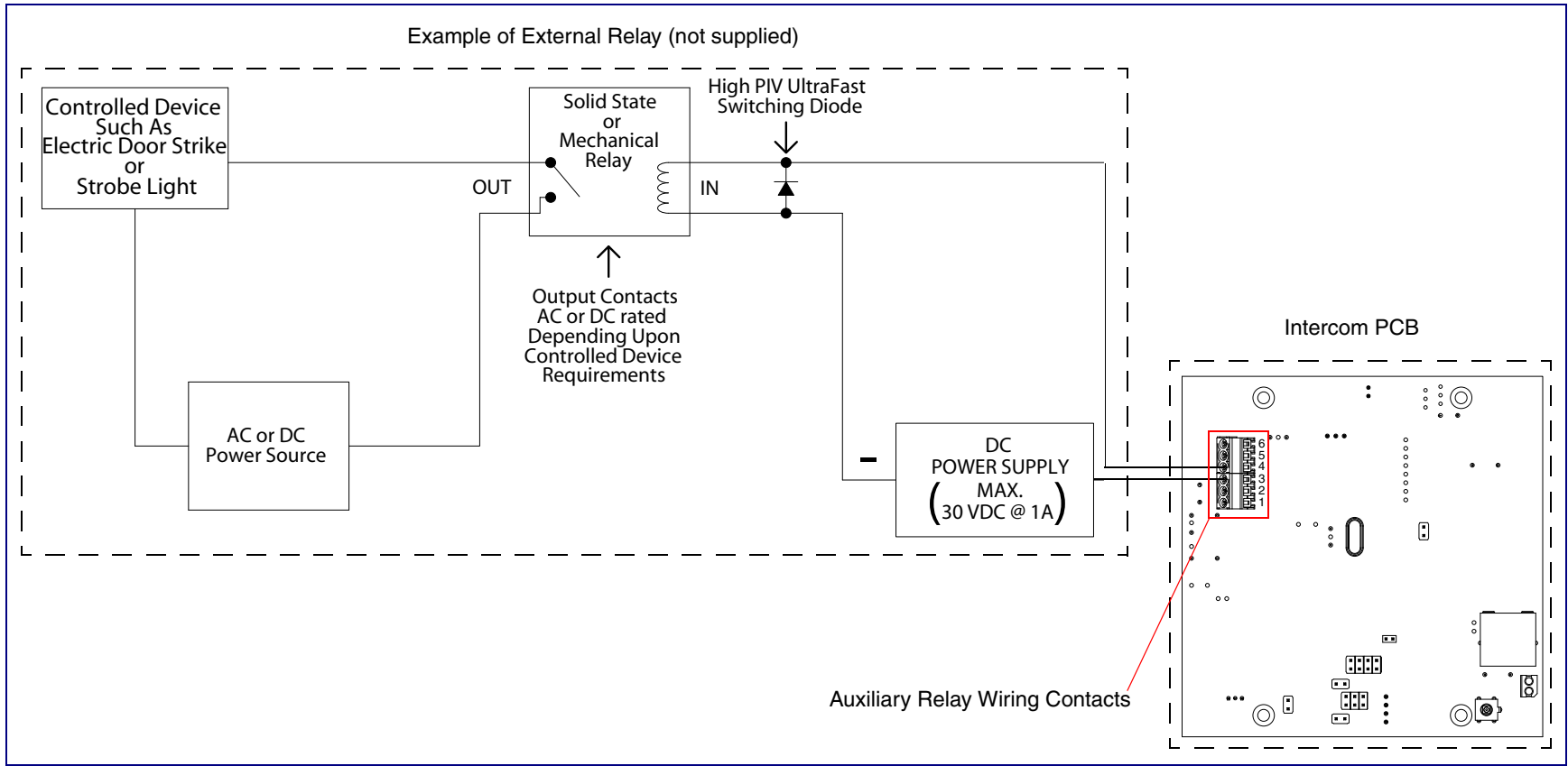
| | |
|--|---|
|  | <p>Warning <i>Electrical Hazard:</i> The VoIP Intercom enclosure is not rated for any AC voltages.</p> |
|  | <p>Warning <i>Electrical Hazard:</i> This product should be installed by a licensed electrician according to all local electrical and building codes.</p> |
|  | <p>Warning <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>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> |

The VoIP Intercom incorporates an on-board relay which enables users to control an external relay for activating an auxiliary device such as an electric door strike (see [Figure 2-10, "Auxiliary Relay Wiring Diagram"](#)).

The Intercom relay contacts are limited to 1A at 30 VDC. The Intercom relay activation time is selectable through the web interface and is controlled by DTMF tones generated from the phone being called. The DTMF tones are selectable from the web interface as well.

Note The three digit code for the auxiliary relay must be sent in conformance with RFC2833 DTMF generation.

Figure 2-10. Auxiliary Relay Wiring Diagram



2.10.3 Identifying the VoIP Intercom Connectors

See the following Figures and Tables to identify the connectors and functions.

Figure 2-11. Connector Locations

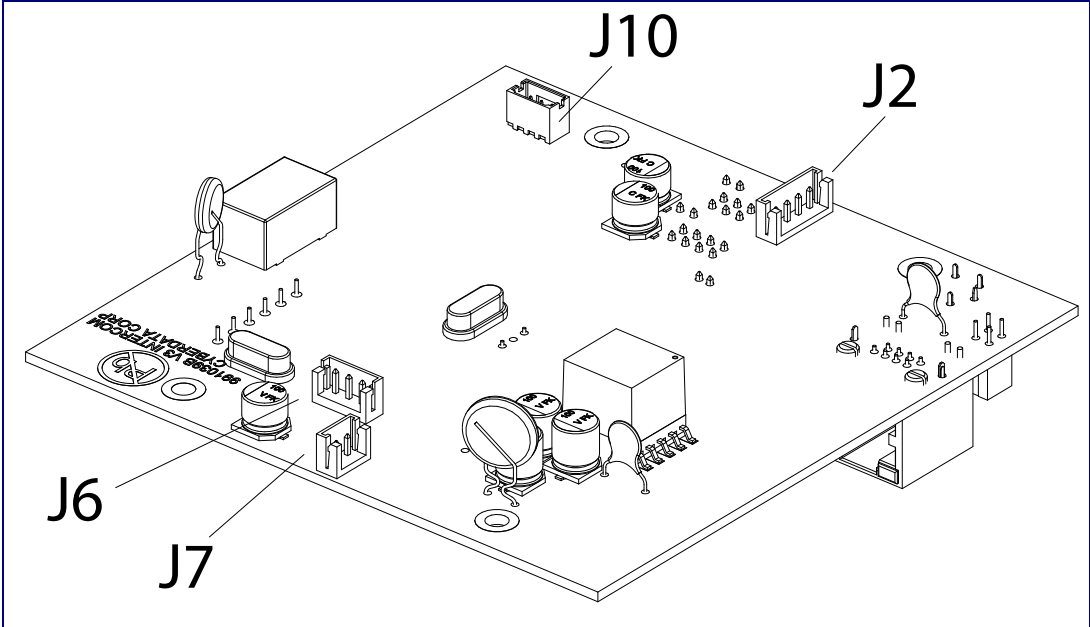


Table 2-3. Connector Functions

| Connector | Function |
|-----------|----------------------------------|
| J2 | Call Button. LED Interface |
| J6 | Microphone Interface |
| J7 | Speaker Interface |
| J10 | Proximity Sensor Interface - N/A |

Figure 2-12. Connector Locations

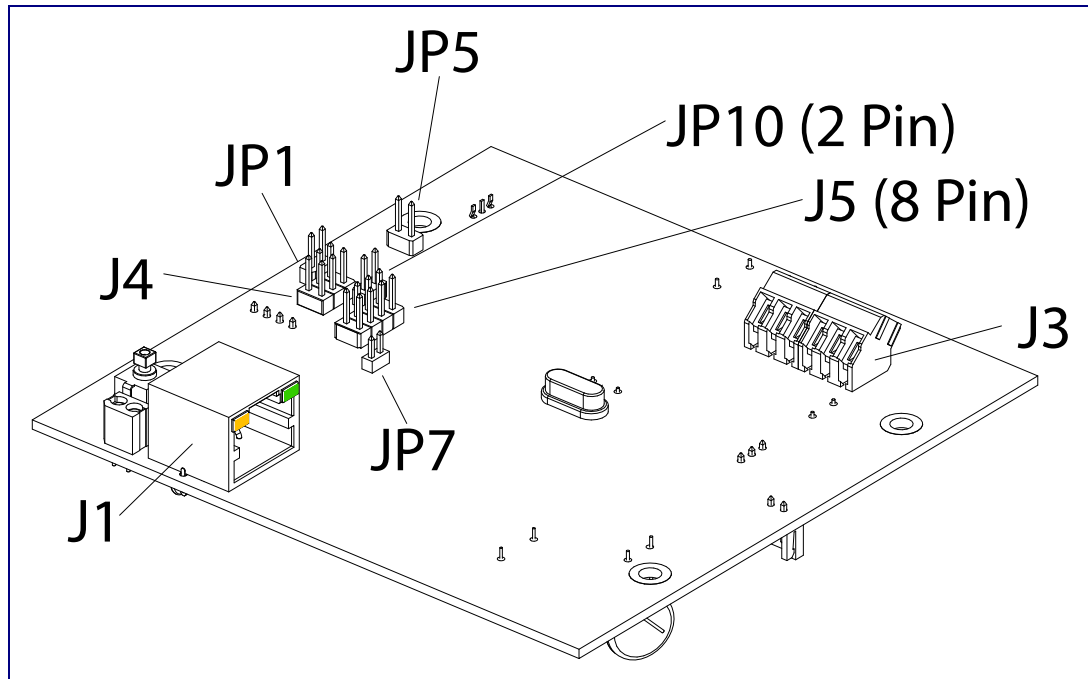


Table 2-4. Connector Functions

| Connector | Function |
|-----------|--|
| J1 | PoE Network Connection (RJ-45 ethernet) |
| J3 | Terminal Block (see Figure 2-9) |
| J4 | Factory Only—Console Port |
| J5 | Factory Only—JTAG |
| JP1 | Factory Only—Reset |
| JP5 | Factory Only—Watch Dog |
| JP7 | Factory Only—Boot Mode |
| JP10 | Disables the intrusion sensor when installed. |

2.10.4 Network Connectivity, and Data Rate

When you connect the Ethernet cable or power supply (Figure 2-13) to the Intercom, the following occurs:

- The square, **GREEN Link** LED above the Ethernet port (Figure 2-14) indicates that the network connection has been established. The **Link** LED changes color to confirm the auto-negotiated connection speed rate:
- The **Link** LED is **YELLOW** at 10 Mbps.
- The **Link** LED is **ORANGE** at 100 Mbps.

Figure 2-13. Network Connector Prior to Installation

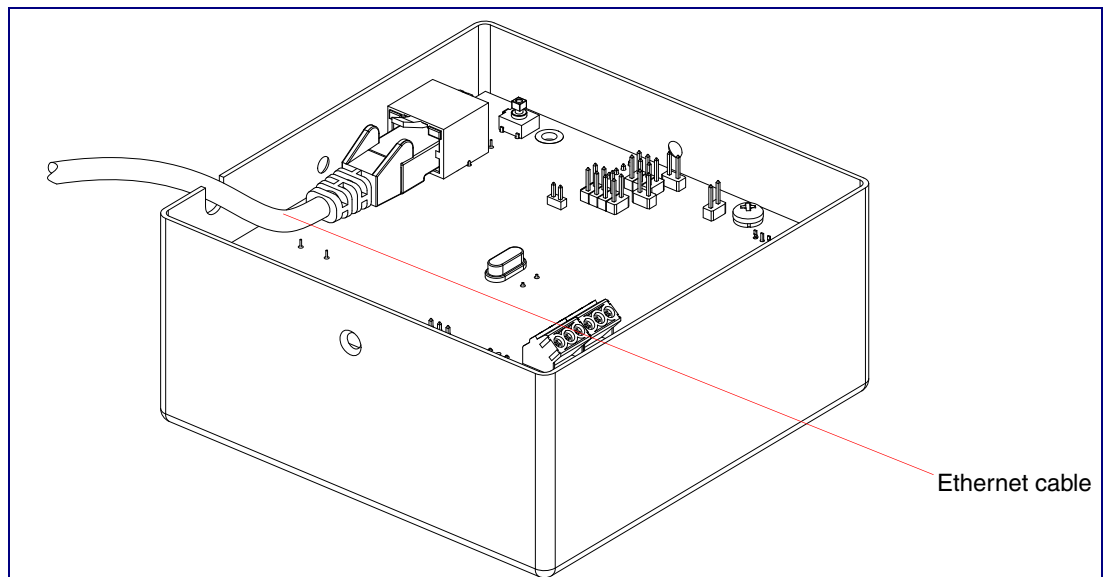
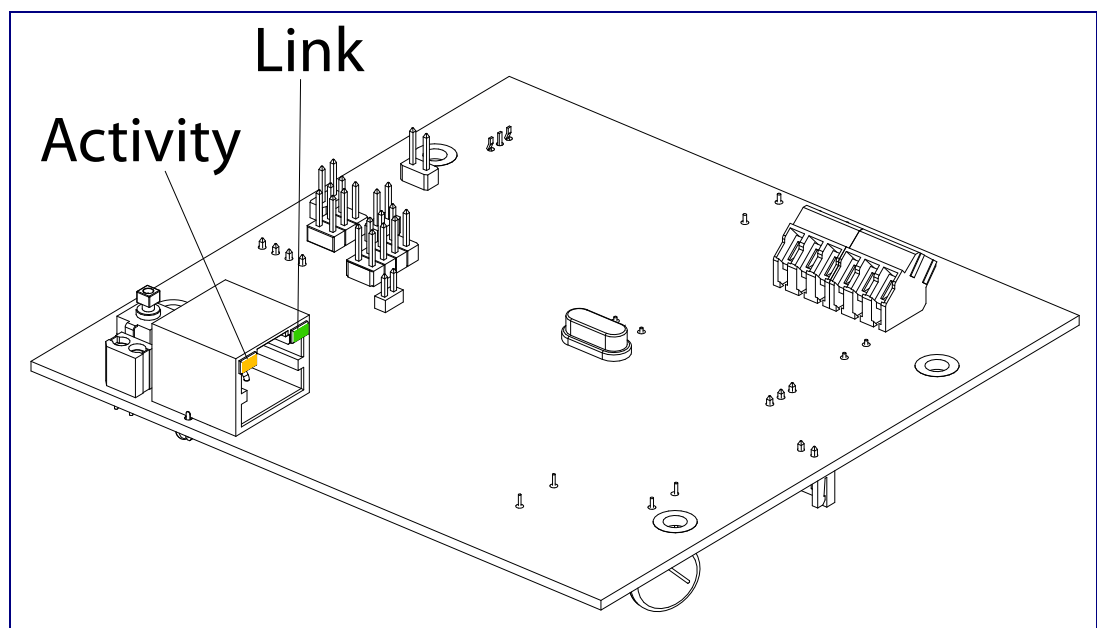


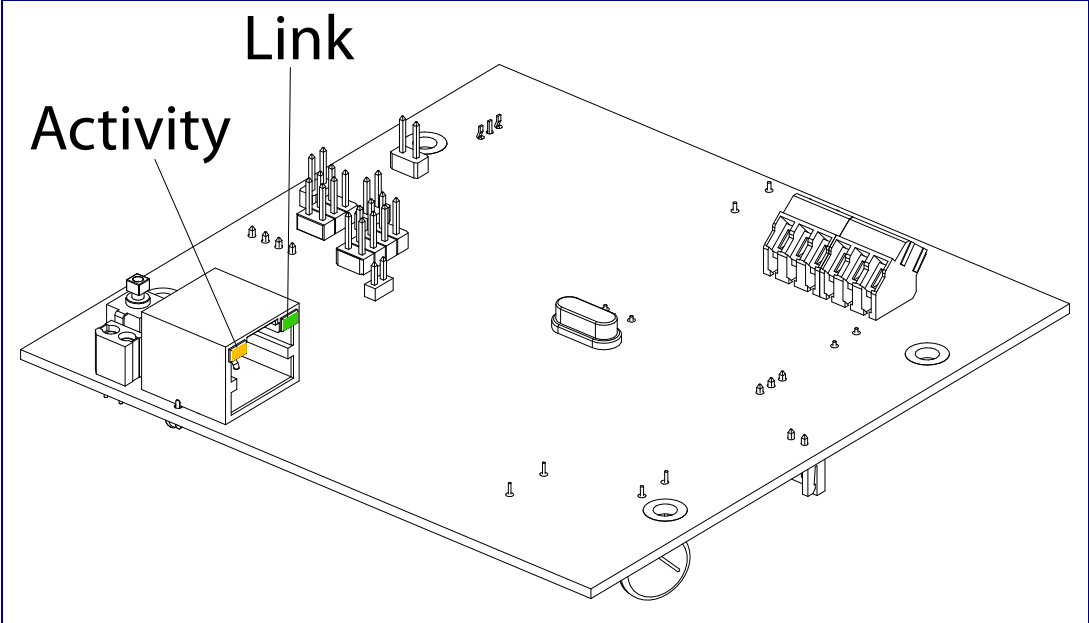
Figure 2-14. Network LEDs



2.10.4.1 Verify Network Activity

The square, **YELLOW Activity** LED (see [Figure 2-15](#)) blinks when there is network activity.

Figure 2-15. Network Connector

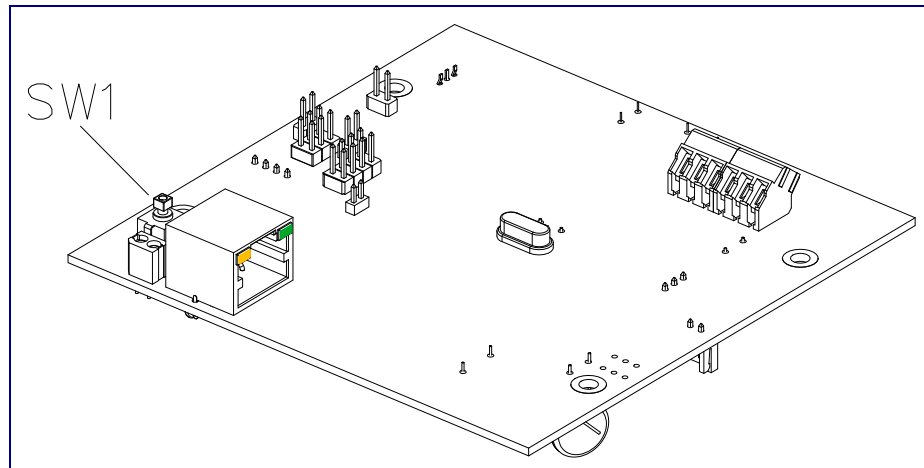


2.10.5 RTFM Button

When the Intercom is operational and linked to the network, use the Reset Test Function Management (**RTFM**) button (see **SW1** in [Figure 2-16](#)) on the Intercom board to announce and confirm the Intercom's IP Address and test that the audio is working.

Note You must do these tests prior to final assembly.

Figure 2-16. RTFM Button (SW1)



2.10.5.1 Announcing the IP Address

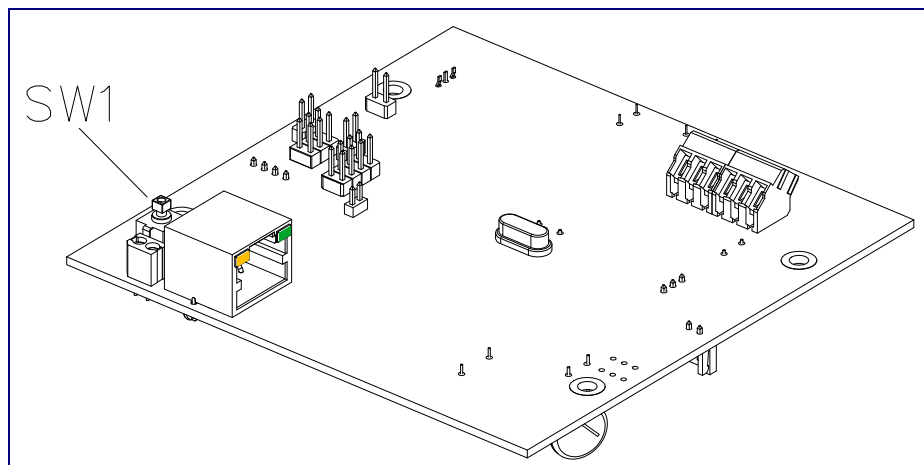
To announce a device's current IP address:

1. Press and release the RTFM button (see **SW1** in [Figure 2-17](#)) 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 2-17. RTFM Button (SW1)



2.10.5.2 Restoring the Factory Default Settings

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

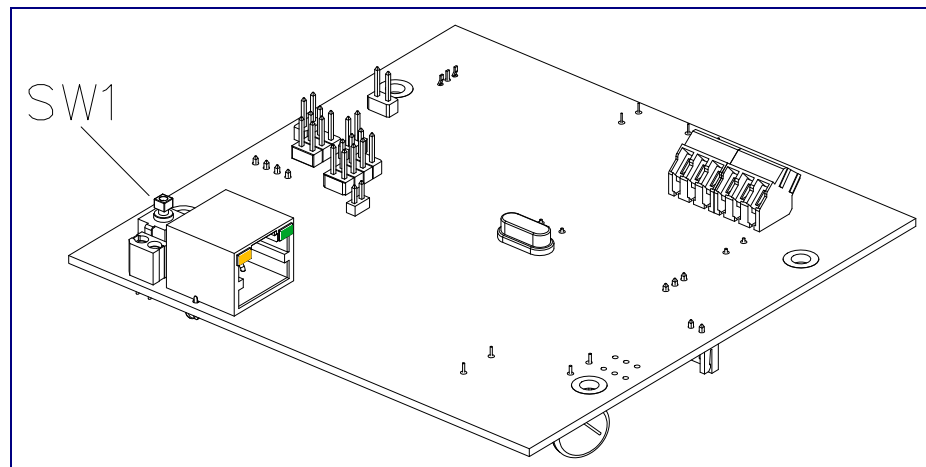
Note Each Intercom is delivered with factory set default values.

To restore the factory default settings:

1. Press and hold the **RTFM button** (see **SW1** in [Figure 2-18](#)) 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 2-18. RTFM Button



2.10.6 Adjust the Volume

You can adjust the volume through the [Speaker Volume](#) setting on the [Device Configuration Page](#).

2.11 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 Indoor Intercom"](#) for instructions.

2.11.1 Factory Default Settings

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

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

Table 2-5. Factory Default Settings









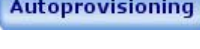

| Parameter | Factory Default Setting |
|------------------------------|--------------------------------|
| IP Addressing | DHCP |
| IP Address ^a | 10.10.10.10 |
| Web Access Username | admin |
| Web Access Password | admin |
| Subnet Mask ^a | 255.0.0.0 |
| Default Gateway ^a | 10.0.0.1 |

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

2.11.2 Intercom Web Page Navigation

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

Table 2-6. Web Page Navigation

| Web Page Item | Description |
|---|---|
|  | Link to the Home page. |
|  | Link to the Device Configuration page. |
|  | Link to the Networking page. |
|  | Link to go to the SIP Configuration page. |
|  | Link to go to the Nightringer page. |
|  | Link to the Sensor Configuration page. |
|  | Link to the Multicast Configuration page. |
|  | Link to the Audio Configuration page. |
|  | Link to the Event Configuration page. |
|  | Link to the Autoprovisioning Configuration page. |
|  | Link to the Update Firmware page. |

2.11.3 Log in to the Configuration Home Page

1. Open your browser to the Intercom IP address.

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

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

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

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

http://www.cyberdata.net/support/voip/discovery_utility.html

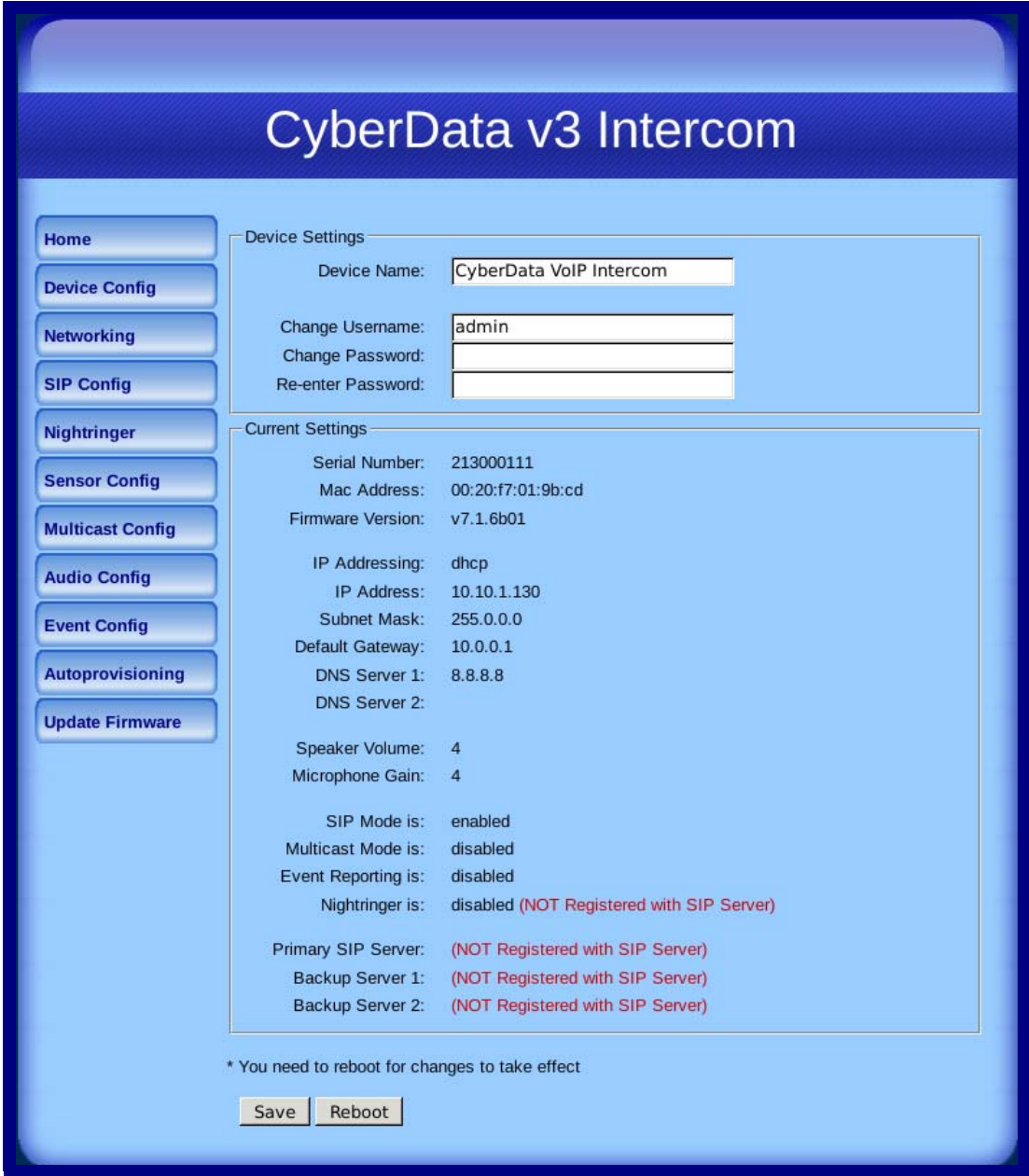
Note The Intercom ships in DHCP mode. To get to the **Home** page, use the discovery utility to scan for the device on the network and open your browser from there.

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**

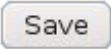

Web Access Password: **admin**

Figure 2-19. Home Page



3. On the **Home Page**, review the setup details and navigation buttons described in [Table 2-7](#).

Table 2-7. Home Page Overview

| Web Page Item | Description |
|---|--|
| Device Settings | |
| Device Name | Shows the device name. |
| Change Username | Type in this field to change the username. |
| Change Password | Type in this field to change the password. |
| Re-enter Password | Type the password again in this field to confirm the new password. |
| Current Settings | |
| Serial Number | Shows the device serial number. |
| Mac Address | Shows the device Mac address. |
| Firmware Version | Shows the current firmware version. |
| IP Addressing | Shows the current IP addressing setting (DHCP or static). |
| IP Address | Shows the current IP address. |
| Subnet Mask | Shows the current subnet mask address. |
| Default Gateway | Shows the current default gateway address. |
| DNS Server 1 | Shows the current DNS Server 1 address. |
| DNS Server 2 | Shows the current DNS Server 2 address. |
| Speaker Volume | Shows the current speaker volume level. |
| Microphone Gain | Shows the current microphone gain level. |
| SIP Mode is | Shows the current status of the SIP mode. |
| Multicast Mode is | Shows the current status of the Multicast mode. |
| Event Reporting is | Shows the current status of the Event Reporting mode. |
| Nightringer is | 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. |
|  | 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. |

2.11.4 Configure the Device

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

Figure 2-20. Device Configuration Page

CyberData v3 Intercom

Device Configuration

Home
Device Config
Networking
SIP Config
Nightringer
Sensor Config
Multicast Config
Audio Config
Event Config
Autoprovisioning
Update Firmware

Volume Settings

Speaker Volume: 4
Microphone Gain: 4

Relay Settings

Activate Relay with DTMF code:
DTMF Activation Code: 321
DTMF Activation Duration (in seconds): 2

Activate Relay During Ring:
Activate Relay During Night Ring:
Activate Relay While Call Active:

Activate Relay on Button Press:
Relay on Button Press Timeout (in seconds): 3

Miscellaneous Settings

Auto-Answer Incoming Calls:
Button Lit when Idle:
Play Ringback Tone:
Enable Push to Talk:

* You need to reboot for changes to take effect


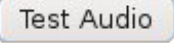


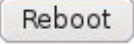
Save Test Audio Test Microphone Test Relay Reboot

2. On the **Device Configuration** page, you may enter values for the parameters indicated in [Table 2-8](#).

Table 2-8. Device Configuration Parameters

| Web Page Item | Description |
|--|---|
| Volume Settings | |
| Speaker Volume | Type the desired Intercom volume level into this field. |
| Microphone Gain | Type the desired microphone gain level into this field. |
| Relay Settings | |
| Activate Relay with DTMF Code | When selected, the relay can be activated with a DTMF code. |
| DTMF Activation Code | Type the desired DTMF activation code (25 character limit). |
| DTMF Activation Duration (in seconds) | Type the desired DTMF activation duration (in seconds) (2 character limit [activation times now go up to 99 seconds]). NOTE: A DTMF activation duration of 0 will toggle the relay indefinitely or until the activation code is sent again |
| Activate Relay During Ring | When selected, the relay will be activated for as long as the call is active. NOTE: When the phone is set to Auto Answer , it will not ring and this option does nothing. |
| Activate Relay During Night Ring | Check this box to activate the relay for as long as a Night Ring tone is ringing. |
| Activate Relay While Call Active | When selected, the relay will be activated for as long as the 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 Timeout (in seconds) | Type the desired time (in seconds) that you want the relay to activate after the Call Button is pressed (1 character limit). |
| Miscellaneous Settings | |
| Auto-Answer Incoming Calls | When selected, the device will automatically answer incoming calls. When Auto Answer is Off, the device will play a ringtone through the Intercom speaker until someone presses the button. |
| Button Lit When Idle | When selected, the Call Button remains lit when idle. |
| Play Ringback Tone | When selected, you will hear a ringback tone while making a call. |

Table 2-8. Device Configuration Parameters (continued)

| Web Page Item | Description |
|---|---|
| Enable Push to Talk | <p>This option is for noisy environments. When enabled, the microphone will be muted normally. When the button is pressed and held, it will unmute the microphone and allow the operator to send audio back.</p> <p>NOTE: When Enable Push to Talk is enabled, you cannot stop an active call with the call button. The device on the other end will need to end the call.</p> <p>NOTE: Enable Push to Talk will not work on some older hardware.</p> |
|  | <p>Click the Save button to save your configuration settings.</p> <p>Note: You need to reboot for changes to take effect.</p> |
|  | <p>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.</p> |
|  | <p>Click on the Test Microphone button to do a microphone test. When the Test Microphone button is pressed, the following occurs:</p> <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. |
|  | <p>Click on the Test Relay button to do a relay test.</p> |
|  | <p>Click on the Reboot button to reboot the system.</p> |

3. After changing the parameters, click the **Save** button.

2.11.5 Configure the Network Parameters

1. Click the **Networking** button to open the **Network Configuration** page (Figure 2-21).

Figure 2-21. Network Configuration Page

CyberData v3 Intercom

Network Configuration

Home
Device Config
Networking
SIP Config
Nightringer
Sensor Config
Multicast Config
Audio Config
Event Config
Autoprovisioning
Update Firmware

Stored Network Settings

IP Addressing: Static DHCP

IP Address: 10.10.10.10

Subnet Mask: 255.0.0.0

Default Gateway: 10.0.0.1

DNS Server 1: 10.0.0.1

DNS Server 2: 10.0.0.1

DHCP Timeout

DHCP Timeout in seconds*: 60

* A value of -1 will retry forever

Current Network Settings

IP Address: 10.10.1.130

Subnet Mask: 255.0.0.0

Default Gateway: 10.0.0.1

DNS Server 1: 8.8.8.8



DNS Server 2:

* You need to reboot for changes to take effect

Save Reboot

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

Table 2-9. Network Configuration Parameters

| Web Page Item | Description |
|---|---|
| Stored Network Settings | |
| IP Addressing | Select either DHCP IP Addressing or Static IP Addressing by marking the appropriate radio button. If you select Static , configure the remaining parameters indicated in Table 2-9 . If you select DHCP , go to Step 3 . |
| IP Address | Enter the Static IP address. |
| Subnet Mask | Enter the Subnet Mask address. |
| Default Gateway | Enter the Default Gateway address. |
| DNS Server 1 | Enter the DNS Server 1 address. |
| DNS Server 2 | Enter the DNS Server 2 address. |
| DHCP Timeout | |
| DHCP Timeout in seconds | Enter the desired timeout duration (in seconds) that the device will wait for a response from the DHCP server before defaulting back to the stored static IP address. Note: A value of -1 will cause the device to retry indefinitely and a value of 0 will cause the device to reset to a default of 60 seconds. |
| 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. |

3. After changing the parameters, click **Save Settings**. This updates the changed parameters and reboots the Intercom if appropriate.
4. Connect the Intercom to the target network.
5. From a system on the same network as the Intercom, open a browser with the new IP address of the Intercom.

2.11.6 Configure the SIP Parameters

1. Click **SIP Config** to open the **SIP Configuration** page (Figure 2-22).

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

<http://www.cyberdata.net/support/server/index.html>

Figure 2-22. SIP Configuration Page

CyberData v3 Intercom

SIP Configuration

Enable SIP operation:

SIP Settings

Primary SIP Server (Registered): 10.0.1.17
 Primary SIP User ID: 231
 Primary SIP Auth ID: 231
 Primary SIP Auth Password: ext231

Backup SIP Server 1 (NOT Registered):
 Backup SIP User ID 1: 230
 Backup SIP Auth ID 1: 230
 Backup SIP Auth Password 1: ext230

Backup SIP Server 2 (NOT Registered):
 Backup SIP User ID 2: 230
 Backup SIP Auth ID 2: 230
 Backup SIP Auth Password 2: ext230

Use Cisco SRST:

Remote SIP Port: 5060
 Local SIP Port: 5060
 Outbound Proxy:
 Outbound Proxy Port: 0

Register with a SIP Server:
 Re-registration Interval (in seconds): 100

Call disconnection

Terminate call after delay (in seconds): 0
 Note: A value of 0 will disable this function

RTP Settings

RTP Port (even): 10500

Dial Out Settings

Dial out Extension: 130
 Extension ID: id204a

* You need to reboot for changes to take effect



Save Reboot

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

Table 2-10. SIP Configuration Parameters

| Web Page Item | Description |
|--|---|
| Enable SIP Operation | Enables or disables SIP operation. |
| SIP Settings | |
| Primary SIP Server | Use this field to set the address (in dotted decimal notation or as a canonical name) for the Primary SIP Server. This field can accept canonical names of up to 255 characters in length. |
| Primary SIP User ID | Type the SIP User ID for the Primary SIP Server (up to 64 alphanumeric characters). |
| Primary Auth ID | Type the Authenticate ID for the Primary SIP Server (up to 64 alphanumeric characters). |
| Primary Auth Password | Type the Authenticate Password for the Primary SIP Server (up to 64 alphanumeric characters). |
| Backup SIP Server 1 Backup SIP Server 2 | <ul style="list-style-type: none"> • If all of the Primary SIP Server and Backup SIP Server fields are populated, the device will attempt to stay registered with all three servers all of the time. You can leave the Backup SIP Server 1 and Backup SIP Server 2 fields blank if they are not needed. • In the event of a registration failure on the Primary SIP Server, the device will use the next highest priority server for outbound calls (Backup SIP Server 1). If Backup SIP Server 1 fails, the device will use Backup SIP Server 2. • If a higher priority SIP Server comes back online, the device will switch back to this server. |
| Backup SIP User ID 1 Backup SIP User ID 2 | Type the SIP User ID for the Backup SIP Server (up to 64 alphanumeric characters). |
| Backup SIP Auth ID 1 Backup SIP Auth ID 2 | Type the SIP Authenticate ID for the Backup SIP Server (up to 64 alphanumeric characters). |
| Backup SIP Auth Password 1 Backup SIP Auth Password 2 | Type the SIP Authenticate Password for the Backup SIP Server (up to 64 alphanumeric characters). |
| Use Cisco SRST | When selected, the backup servers are handled according to Cisco SRST (Survivable Remote Site Telephony). |
| Remote SIP Port | Type the Remote SIP Port number (default 5060) (8 character limit). |
| Local SIP Port* | Type the Local SIP Port number (default 5060) (8 character limit). |
| Outbound Proxy | Type the Outbound Proxy as either a numeric IP address in dotted decimal notation or the fully qualified host name (255 character limit [FQDN]). |
| Outbound Proxy Port | Type the Outbound Proxy Port number (8 character limit). |
| Register with a SIP Server | <p>Check this box to enable SIP Registration.</p> <p>For information about Point-to-Point Configuration, see Section 2.11.6.2, "Point-to-Point Configuration".</p> |
| Re-registration Interval (in seconds) | Type the SIP Registration lease time (in seconds) |

Table 2-10. SIP Configuration Parameters (continued)

| Web Page Item | Description |
|---|---|
| Call Disconnection | |
| Terminate call after delay (in seconds) | Type the desired number of seconds that you want to transpire after a connection delay before a call is terminated. Note: A value of 0 will disable this function. |
| RTP Settings | |
| RTP Port (even) | Specify the port number used for the RTP stream after establishing a SIP call. This port number has to be an even number and defaults to 10500. |
| Dial Out Settings | |
| Dial Out Extension | Type the dial out extension number (64 character limit). Note: For information about dial-out extension strings and DTMF tones, see Section 2.11.6.1, "Dial Out Extension Strings and DTMF Tones (using rfc2833)" . |
| Extension ID | Type the desired Extension ID (64 character limit). |
|  | 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. |

3. After changing the parameters, click **Save Settings**.

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

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

Table 2-11. 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.

2.11.6.2 Point-to-Point Configuration

When the board is set to not register with a SIP server (see [Figure 2-23](#)), it's possible to set the intercom to dial out to a single endpoint.

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

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

Figure 2-23. SIP Configuration Page Set to Point-to-Point Mode

Intercom is set to NOT register with a SIP server

2.11.6.3 Delayed DTMF

On the **SIP Configuration** 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.

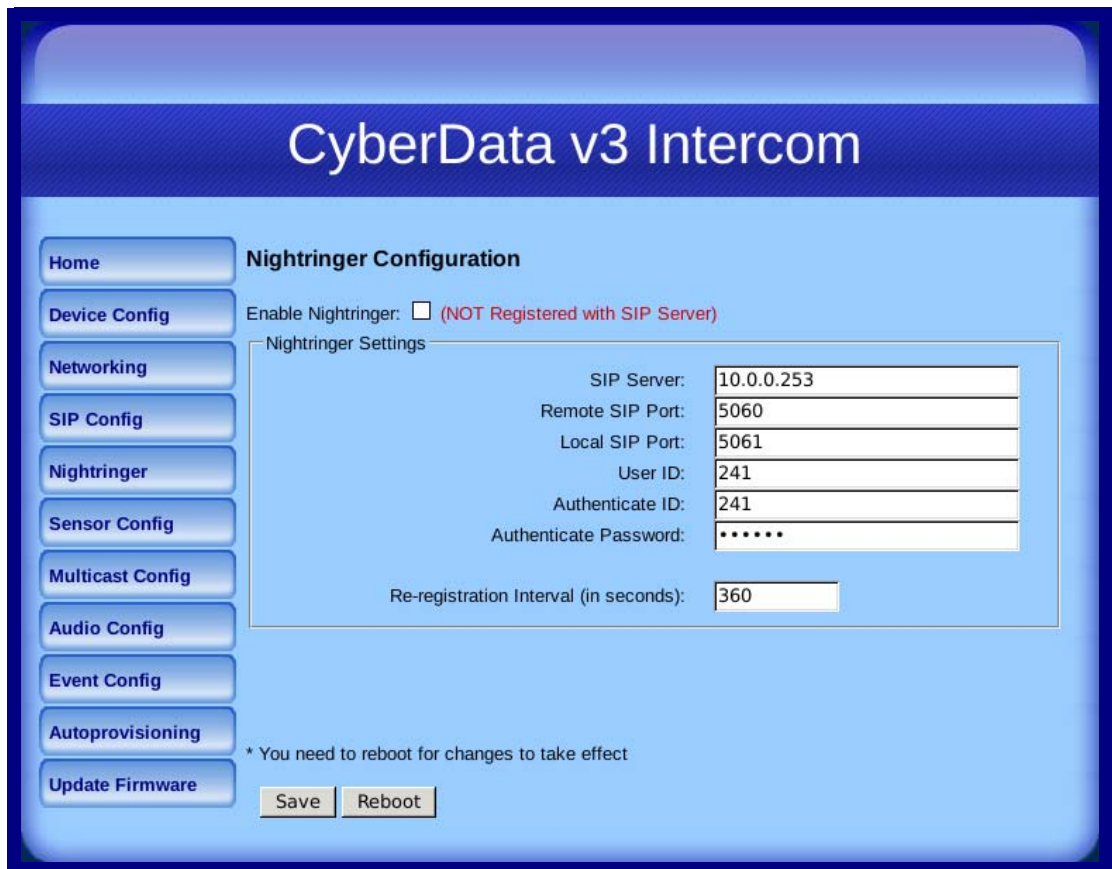
2.11.7 Configure the Nightringer Parameters

When the Nightringer is enabled, the Intercom will register as a second SIP extension. Registration does not have to be to the same server as the primary SIP registration. Any calls made to the Nightringer extension will cause the Intercom to play a ring tone. There is no way to answer this call. The Nightringer is designed to be used in buildings where calls made after hours are directed to a ring group.

| | |
|---|--|
|  | <p>Caution</p> <p>Nightringer requires SIP Registration. Nightringer cannot be used in peer to peer mode.</p> |
|---|--|

1. Click on the **Nightringer** button to open the **Nightringer Configuration** page. See [Figure 2-24](#).

Figure 2-24. Nightringer Configuration Setup



CyberData v3 Intercom

Nightringer Configuration

Enable Nightringer: (NOT Registered with SIP Server)

Nightringer Settings



| | |
|--|------------|
| SIP Server: | 10.0.0.253 |
| Remote SIP Port: | 5060 |
| Local SIP Port: | 5061 |
| User ID: | 241 |
| Authenticate ID: | 241 |
| Authenticate Password: | ***** |
| Re-registration Interval (in seconds): | 360 |

* You need to reboot for changes to take effect

Save Reboot

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

Table 2-13. Nightringer Configuration Parameters

| Web Page Item | Description |
|---|--|
| Enable Nightringer | When the nightringer is enabled, the unit will attempt to register a second extension with the SIP server. Any calls made to this extension will play a ringtone. |
| Nightringer Settings | |
| SIP Server | Type the SIP server represented as either a numeric IP address in dotted decimal notation. |
| Remote SIP Port | Type the Remote SIP Port number (default 5060) (8 character limit). |
| Local SIP Port | Type the Local SIP Port number (default 5060) (8 character limit). Note: This value cannot be the same as the Local SIP Port* found on the SIP Configuration Page . |
| User ID | Type the User ID (up to 64 alphanumeric characters). |
| Authenticate ID | Type the Authenticate ID (up to 64 alphanumeric characters). |
| Authenticate Password | Type the Authenticate Password (up to 64 alphanumeric characters). |
| Re-registration Interval (in seconds) | Type the SIP Registration lease time in minutes (default is 60 minutes) (8 character limit). Re-registration Interval (in seconds)* |
|  | 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. |

3. After changing the parameters, click on the **Save** button.

2.11.8 Configure the Sensor Configuration Parameters

The door sensor (pins 5 and 6) on the header can be used to monitor a door's open or closed state. There is an option on the **Sensor Configuration** 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.

For each sensor there are four actions the Intercom can take:

- 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 a preset extension and play a pre-recorded audio file (once)

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 Config** to open the **Sensor Configuration** page (Figure 2-25).

Figure 2-25. Sensor Configuration Page

CyberData v3 Intercom

Sensor Configuration

Home
Device Config
Networking
SIP Config
Nightringer
Sensor Config
Multicast Config
Audio Config
Event Config
Autoprovisioning
Update Firmware

Door Sensor Settings

Door Sensor Normally Closed: Yes No
Door Open Timeout (in seconds):

Flash Button LED:
Activate Relay:
Play Audio Locally:

Make call to extension:
Play recorded audio:
Dial Out Extension:
Dial Out ID:

Intrusion Sensor Settings

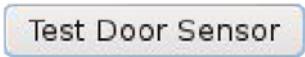



Flash Button LED:
Activate Relay:
Play Audio Locally:

Make call to extension:
Play recorded audio:
Dial Out Extension:
Dial Out ID:

* You need to reboot for changes to take effect

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

Table 2-14. Sensor Configuration Parameters

| Web Page Item | Description |
|---|--|
| Door Sensor Settings | |
| Door Sensor Normally Closed | Select the inactive state of the door sensors. |
| Door Open Timeout (in seconds) | Select the number of seconds that you want to pass before the door sensor is activated. |
| Flash Button LED | Check this box to flash the LED until the sensor is deactivated (roughly 10 times/second). |
| Activate Relay | Check this box to activate the relay until the sensor is deactivated. |
| Play Audio Locally | Check this box to loop an audio file out of the Intercom speaker until the sensor is deactivated. |
| Make call to extension | Check this box to call a preset extension (once). |
| Play recorded audio | Check this box to play a pre-recorded audio file (once). |
| Dial Out Extension | Enter the desired dial-out extension number. |
| Dial Out ID | Type the desired Extension ID (64 character limit). |
|  | Use this button to test the door sensor. |
| Intrusion Sensor Settings | |
| Flash Button LED* | Check this box to flash the LED until the sensor is deactivated (roughly 10 times/second). |
| Activate Relay | Check this box to activate the relay until the sensor is deactivated. |
| Play Audio Locally | Check this box to loop an audio file out of the Intercom speaker until the sensor is deactivated. |
| Make call to extension | Check this box to call a preset extension (once). |
| Play recorded audio | Check this box to play a pre-recorded audio file (once). |
| Dial Out Extension | Enter the desired dial-out extension number. |
| Dial Out ID | Type the desired Extension ID (64 character limit). |
|  | Use this 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. |

3. After changing the parameters, click **Save Settings**.

2.11.9 Configure the Multicast Parameters

Multicast groups use multicasting to create public address paging zones. Multicasting is based on the concept of a group. Multicast addresses specify an arbitrary group of IP hosts that have joined the group and want to receive traffic sent to the group. Group members send IGMP messages to their local multicast routers, allowing the group traffic traversal from the source.

The **Multicast Configuration** page allows the Intercom to join up to 10 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 devices 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 three. The Intercom supports simultaneous SIP and Multicast.

1. Click on the **Multicast Configuration** button to open the **Multicast Configuration** page. See [Figure 2-26](#).

Figure 2-26. Multicast Configuration Page

CyberData v3 Intercom

Multicast Configuration

Enable Multicast operation:

Device Settings

| priority | Address | port | Multicast Group Name |
|---------------------------------------|--------------|-------|----------------------|
| 9 | 239.168.3.10 | 11000 | Emergency |
| 8 | 239.168.3.9 | 10000 | MG8 |
| 7 | 239.168.3.8 | 9000 | MG7 |
| 6 | 239.168.3.7 | 8000 | MG6 |
| 5 | 239.168.3.6 | 7000 | MG5 |
| SIP calls are considered priority 4.5 | | | |
| 4 | 239.168.3.5 | 6000 | MG4 |
| 3 | 239.168.3.4 | 5000 | MG3 |
| 2 | 239.168.3.3 | 4000 | MG2 |
| 1 | 239.168.3.2 | 3000 | MG1 |
| 0 | 239.168.3.1 | 2000 | Background Music |

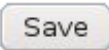

Port range can be from 2000-65535
 Ports must be even numbers
 Priority 9 is the highest and 0 is the lowest
 A higher priority audio stream will always supercede a lower one
 Priority 9 streams will play at maximum volume

* You need to reboot for changes to take effect

Save Reboot

2. On the **Multicast Configuration** page, enter values for the parameters indicated in [Table 2-15](#).

Table 2-15. Multicast Configuration Parameters

| Web Page Item | Description |
|--|--|
| Enable Multicast Operation | Enables or disables multicast operation. |
| Device Settings | |
| Priority | Indicates the priority for the multicast group. Priority 9 is the highest (emergency streams). 0 is the lowest (background music). SIP calls are considered priority 4.5 . See Section 2.11.9.1, "Assigning Priority" for more details. |
| Address | Enter the multicast IP Address for this multicast group (15 character limit). |
| Port (range can be from 2000 to 65535) | Enter the port number for this multicast group (5 character limit). Note: The multicast ports have to be even values. The webpage will enforce this restriction. |
| Multicast Group Name | Assign a descriptive name for this multicast group (25 character limit). |
|  | 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. |

3. After changing the parameters, click on the **Save** button.

2.11.9.1 Assigning Priority

When playing multicast streams, audio on different streams will preempt each other according to their priority in the list. An audio stream with a higher priority will interrupt a stream with a lower priority.

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 level 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.

2.11.10 Configure the Audio Configuration Parameters

The **Audio Configuration** 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 **Audio Config** to open the **Audio Configuration** page (Figure 2-27).

Figure 2-27. Audio Configuration Page

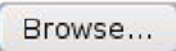


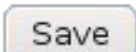
The screenshot displays the 'Audio Configuration' page for the 'CyberData v3 Intercom'. On the left is a vertical sidebar with buttons for: Home, Device Config, Networking, SIP Config, Nightringer, Sensor Config, Multicast Config, Audio Config (highlighted), Event Config, Autoprovisioning, and Update Firmware. The main content area is titled 'Audio Configuration' and shows 'Available Space = 14.82MB'. Below this, there is a section for 'Audio Files' with 9 numbered entries (0-8). Each entry consists of a status line (e.g., '0: Currently set to default'), a 'New File:' text input field, a 'Browse...' button, and three buttons: 'Play', 'Delete', and 'Save'.

Figure 2-28. Audio Configuration Page (continued)



2. On the **Audio Configuration** page, enter values for the parameters indicated in [Table 2-16](#).

Table 2-16. Audio Configuration Parameters

| Web Page Item | Description |
|---|--|
| Audio Files | |
| 0-9 | The name of the audio configuration option is the same as the spoken audio that plays on the board (24 character limit). '0' corresponds to the spoken word "zero." '1' corresponds to the spoken word "one." '2' corresponds to the spoken word "two." '3' corresponds to the spoken word "three." '4' corresponds to the spoken word "four." '5' corresponds to the spoken word "five." '6' corresponds to the spoken word "six." '7' corresponds to the spoken word "seven." '8' corresponds to the spoken word "eight." '9' corresponds to the spoken word "nine." |
| Dot | Corresponds to the spoken word "dot." (24 character limit) |
| Audiotest | Corresponds to the message <i>"This is the CyberData IP speaker test message..."</i> (24 character limit) |
| Page tone | Corresponds to a simple tone used for beep on initialization and beep on page (24 character limit). |
| Your IP Address is | Corresponds to the message "Your IP address is..." (24 character limit). |
| Rebooting | Corresponds to the spoken word "Rebooting" (24 character limit). |
| Restoring default | Corresponds to the message "Restoring default" (24 character limit). |
| Ringback tone | This is the ringback tone that plays when calling a remote extension (24 character limit). |
| Ring tone | This is the tone that plays when set to ring when receiving a call (24 character limit). |
| Intrusion Sensor Triggered | Corresponds to the message "Intrusion Sensor Triggered" (24 character limit). |
| Door Ajar | Corresponds to the message "Door Ajar" (24 character limit). |
| Night Ring | Specifies the ringtone for nightring. By default this parameter uses the same audio file that is selected for the Ring Tone parameter. |
|  | The Browse button will allow you to navigate to and select an audio file. |
|  | The Play button will play that audio file. |
|  | The Delete button will delete any user uploaded audio and restore the stock audio file. |
|  | The Save button will download a new user audio file to the board once you've selected the file by using the Browse button. The Save button will delete any pre-existing user-uploaded audio files. |

2.11.10.1 User-created Audio Files

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

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

You can use the free utility *Audacity* to convert audio files into this format. See [Figure 2-29](#) through [Figure 2-31](#).

Figure 2-29. Audacity 1

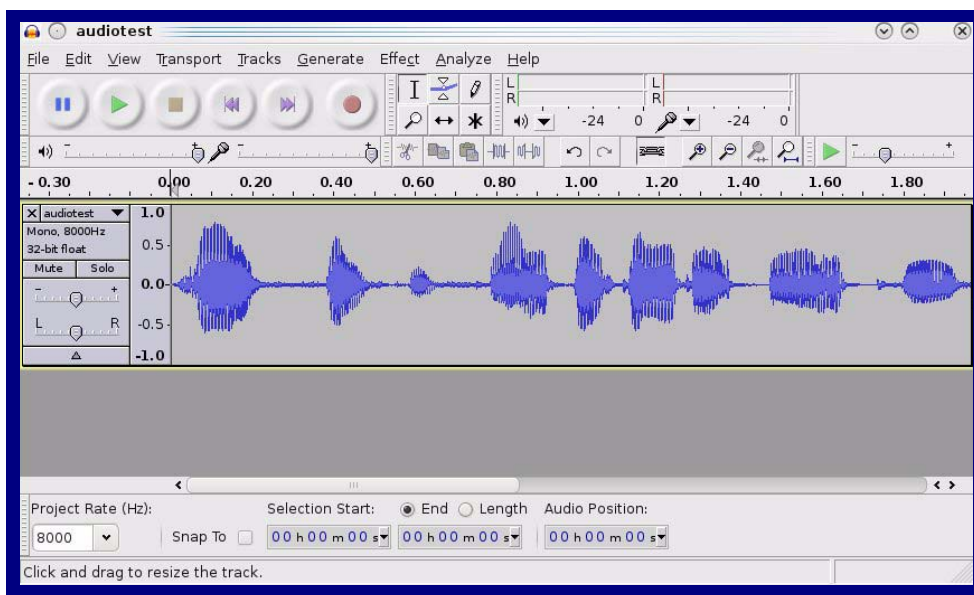
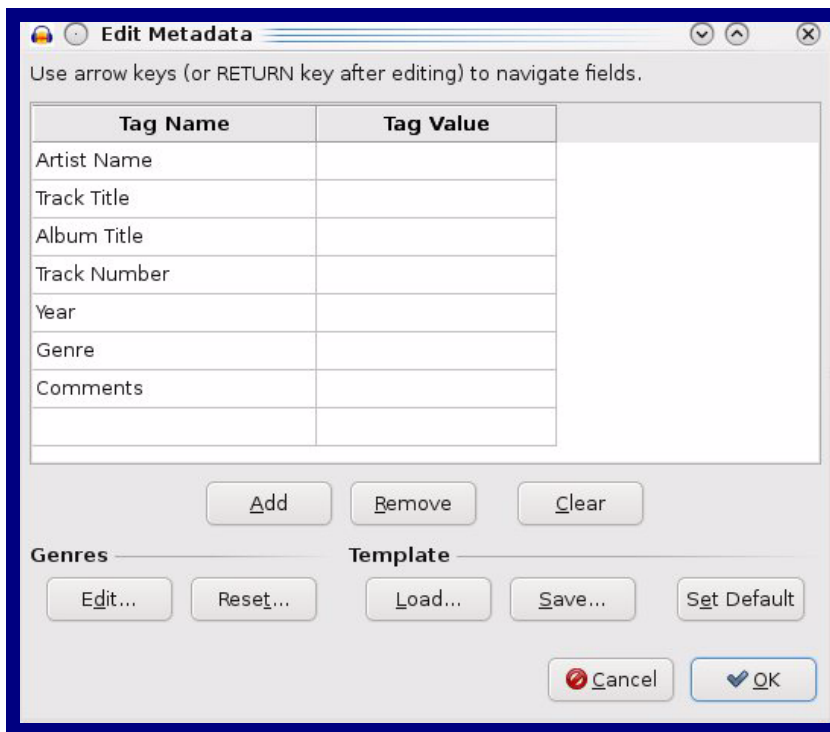


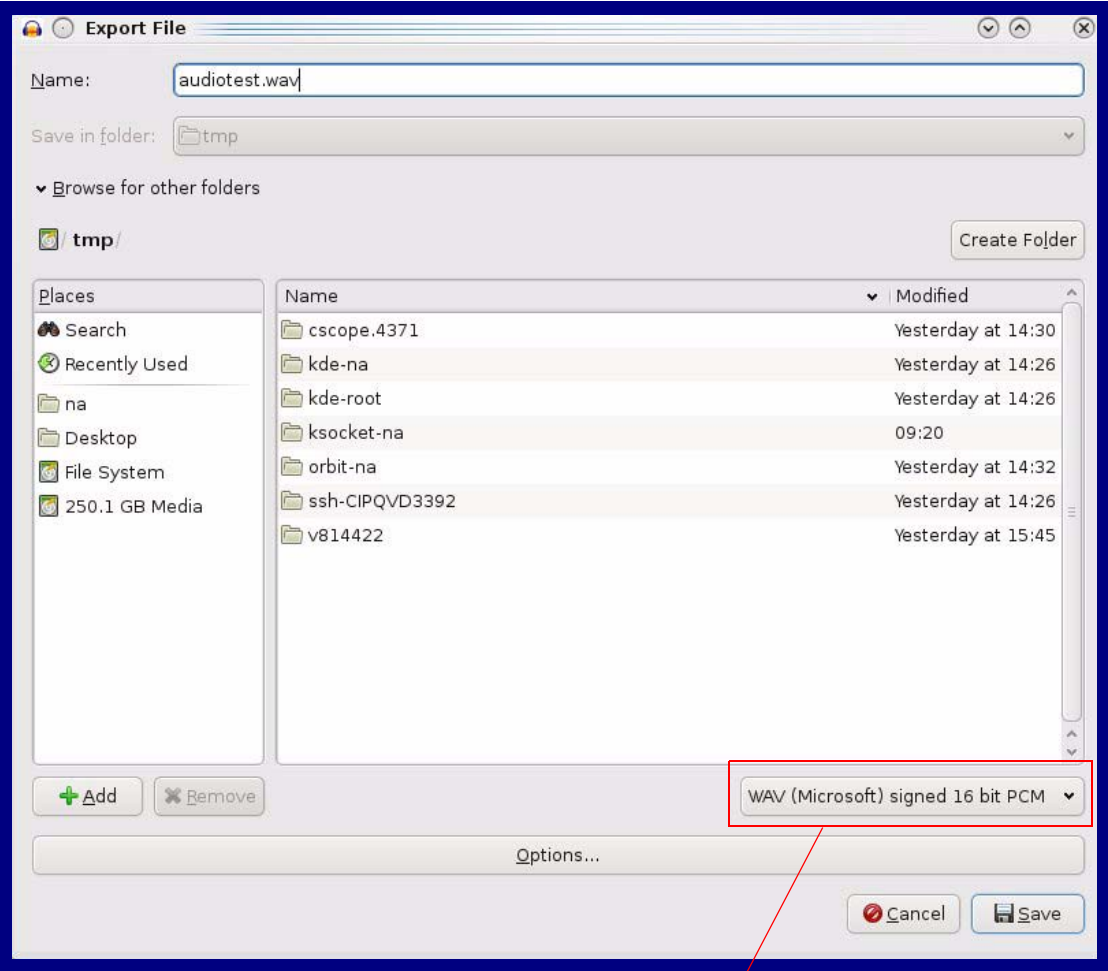
Figure 2-30. Audacity 2



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

- WAV (Microsoft) signed 16 bit PCM.

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



WAV (Microsoft) signed 16 bit PCM

2.11.11 Configure the Event Parameters

Click the **Event Config** button to open the **Event Configuration** page (Figure 2-32). The **Event Configuration** page specifies a remote server that can be used to receive HTTP POST events when actions take place on the board.

Figure 2-32. Event Configuration Page

CyberData v3 Intercom

Event Configuration

Enable Event Generation:

Remote Event Server

Remote Event Server IP: 10.0.0.250

Remote Event Server Port: 8080

Remote Event Server URL: xmlparse_engine

Events

Enable Button Events:

Enable Call Active 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 Security Events:

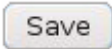


Enable 60 second Heartbeat Events:

* You need to reboot for changes to take effect

Save Test Event Reboot

Table 2-17 shows the web page items on the **Event Configuration** page.

Table 2-17. Event Configuration

| Web Page Item | Description |
|---|--|
| Enable Event Generation | When selected, Event Generation is enabled. |
| Remote Event Server | |
| Remote Event Server IP | Type the Remote Event Server IP address. (64 character limit) |
| Remote Event Server Port | Type the Remote Event Server port number. (8 character limit) |
| Remote Event Server URL | Type the Remote Event Server URL. (127 character limit) |
| Events | |
| Enable Button Events | When selected, Button Events are enabled. |
| Enable Call Active Events | When selected, Call Active Events are enabled. |
| Enable Call Terminated Events | When selected, Call Terminated Events are enabled. |
| Enable Relay Activated Events | When selected, Relay Activated Events are enabled. |
| Enable Relay Deactivated Events | When selected, Relay Deactivated Events are enabled. |
| Enable Ring Events | When selected, Ring Events are enabled. |
| Enable Night Ring Events | When selected, there is a notification when the unit receives a night ring. |
| Enable Multicast Start Events | When selected, Multicast Start Events are enabled. |
| Enable Multicast Stop Events | When selected, Multicast Stop Events are enabled. |
| Enable Power On Events | When selected, Power On Events are enabled. |
| Enable Security Events | When selected, Security Events are enabled. |
| Enable 60 Second Heartbeat Events | When selected, 60 Second Heartbeat Events are enabled. |
|  | Click the Save button to save your configuration settings. Note: You need to reboot for changes to take effect. |
|  | Click on the Test Event button to test an event. |
|  | Click on the Reboot button to reboot the system. |

2.11.11.1 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>
```

2.11.12 Configure the Autoprovisioning Parameters

1. Click the **Autoprovisioning** button to open the **Autoprovisioning Configuration** page.
See [Figure 2-33](#).

Figure 2-33. Autoprovisioning Configuration Page

CyberData v3 Intercom

Autoprovisioning

Autoprovisioning

Enable Autoprovisioning:

Get Autoprovisioning from DHCP:

Autoprovisioning Server (IP Address): 10.0.0.254

Autoprovisioning autoupdate (in minutes): 1440



* Autoprovisioning file name: 0020f7019bcd.config

* You need to reboot for changes to take effect

Save Reboot

2. On the **Autoprovisioning Configuration** page, you may enter values for the parameters indicated in [Table 2-18](#).

Table 2-18. Autoprovisioning Configuration Parameters

| Web Page Item | Description |
|---|--|
| Autoprovisioning | |
| Enable Autoprovisioning | See Section 2.11.12.1, "Autoprovisioning" . |
| Get Autoprovisioning from DHCP | See Section 2.11.12.1, "Autoprovisioning" . |
| Autoprovisioning Server (IP Address) | See Section 2.11.12.1, "Autoprovisioning" (15 character limit). |
| Autoprovisioning Autoupdate (in minutes) | Type the desired time (in minutes) that you want the Autoprovisioning feature to update (6 character limit). |
|  | 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. |

3. After changing the parameters, click the **Save** button.

2.11.12.1 Autoprovisioning

Enable Autoprovisioning Option With autoprovisioning enabled, the board will get its configuration from a remote TFTP server on startup or periodically on a scheduled delay. Autoprovisioned values will override values stored in on-board memory and will be visible on the web page. The board gets its autoprovisioning information from an XML-formatted file hosted from a TFTP server. CyberData will provide a template for this XML file and the user can modify it for their own use.

To use autoprovisioning, create a copy of the autoprovisioning template with the desired settings and name this file with the mac address of the device to configure (for example: **0020f7350058.config**). Put this file into your TFTP server directory and manually set the TFTP server address on the board.

It is not necessary to set every option found in the autoprovisioning template. As long as the XML is valid, the file can contain any subset. Options not autoprovisioned will default to the values stored in the on board memory. For example if you only wanted to modify the device name, the following would be a valid autoprovisioning file:

```
<?xml version="1.0" encoding="utf-8" ?>
<specific>
  <MiscSettings>
    <DeviceName>auto Intercom</DeviceName>
  </MiscSettings>
</specific>
```

Networking The board will only apply networking settings or firmware upgrades after a reboot.

Get Autoprovisioning from DHCP When this option is checked, the device will automatically fetch its autoprovisioning server address from the DHCP server. The device will use the address specified in **OPTION 150** (TFTP-server-name) or **OPTION 66**. If both options are set, the device will use **OPTION 150**.

Refer to the documentation of your DHCP server for setting up **OPTION 150**.

To set up a Linux DHCPD server to serve autoprovisioning information (in this case using both option 66 and 150), here's an example dhcpd.conf:

```
# dhcpd.conf
#
# Configuration file for ISC dhcpd (see 'man dhcpd.conf')
#
ddns-update-style ad-hoc;

option option-150 code 150 = ip-address;

subnet 10.0.0.0 netmask 255.0.0.0 {
    max-lease-time 120;
    default-lease-time 120;

    option routers                10.0.0.1;
    option subnet-mask            255.0.0.0;

    option domain-name            "voiplab";
    option domain-name-servers    10.0.0.1;

    option time-offset             -8;      # Pacific Standard Time

    option tftp-server-name        "10.0.0.254";

    option option-150              10.0.0.254;

    range 10.10.0.1 10.10.2.1;}
```

Autoprovisioning Server (IP Address) Instead of using DHCP to provide the autoprovisioning tftp server address, you can specify an address manually.

Autoprovisioning Autoupdate If **Autoprovisioning** is enabled and the **Autoprovisioning Autoupdate** value is something other than **0** minutes, a service is started on startup that will wait the configured number of minutes and then try to re-download its autoprovisioning file. It will compare its previously autoprovisioned file with this new file and if there are differences, it will reboot the board.

Autoprovisioned Firmware Upgrades An Autoprovisioned firmware upgrade only happens after a reboot, will take roughly three minutes, and the web page will be unresponsive during this time.

The '**FirmwareVersion**' value in the xml file *must* match the version stored in the '**FirmwareFile**'.

```
<FirmwareVersion>v6.3.0</FirmwareVersion>
<FirmwareFile>630-intercom-uImage</FirmwareFile>
```

If these values are mismatched, the board can get stuck in a loop where it goes through the following sequence of actions:

1. The board downloads and writes a new firmware file.
2. After the next reboot, the board recognizes that the firmware version does not match.
3. The board downloads and writes the firmware file again.

CyberData has timed a firmware upgrade at 140 seconds. Therefore, if you suspect the board is stuck in a loop, either remove or comment out the **FirmwareVersion** line in the XML file and let the board boot as it normally does.

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 the **Delete** button on the **Audio Configuration** page which will restore the default audio file. You can also change the autoprovisioning file with the word **default** set as the file name.

2.12 Upgrade the Firmware and Reboot the Intercom



Caution

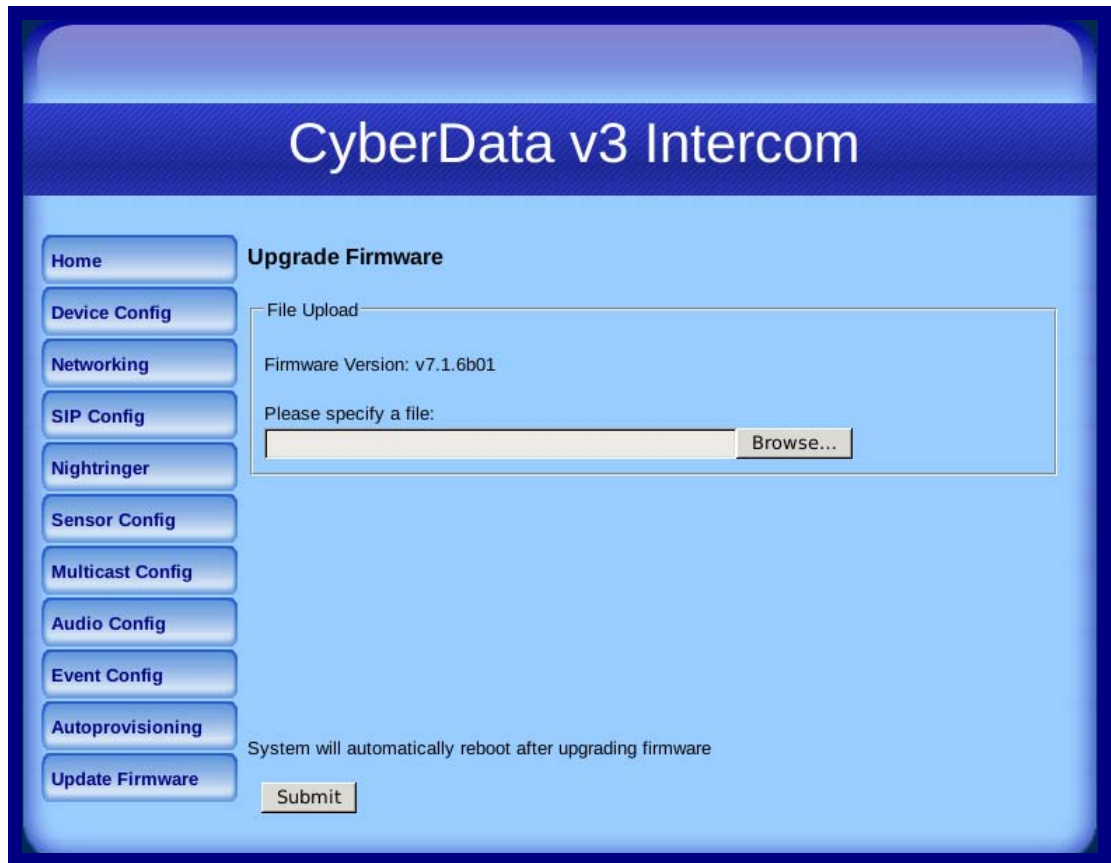
Equipment Hazard: V3 devices like the VoIP V3 Emergency Intercom cannot use firmware 6.x.x or earlier, and older V1 and V2 devices cannot use firmware 7.x.x or later.

2.12.1 Uploading the Firmware

To upload the firmware from your computer:

1. Retrieve the latest Intercom firmware file from the VoIP V3 Emergency Intercom **Downloads** page at:
<http://www.cyberdata.net/products/voip/digitalanalog/intercomindoorv3/downloads.html>
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 2.11.3, "Log in to the Configuration Home Page"](#).
4. Click the **Update Firmware** button to open the **Upgrade Firmware** page. See [Figure 2-34](#).

Figure 2-34. Upgrade Firmware Page



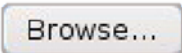

5. Select **Browse**, and then navigate to the location of the Intercom firmware file.
6. Click **Submit**.

Note Do not reboot the board after pressing the **Submit** button.

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

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

Table 2-19. Firmware Upgrade Parameters

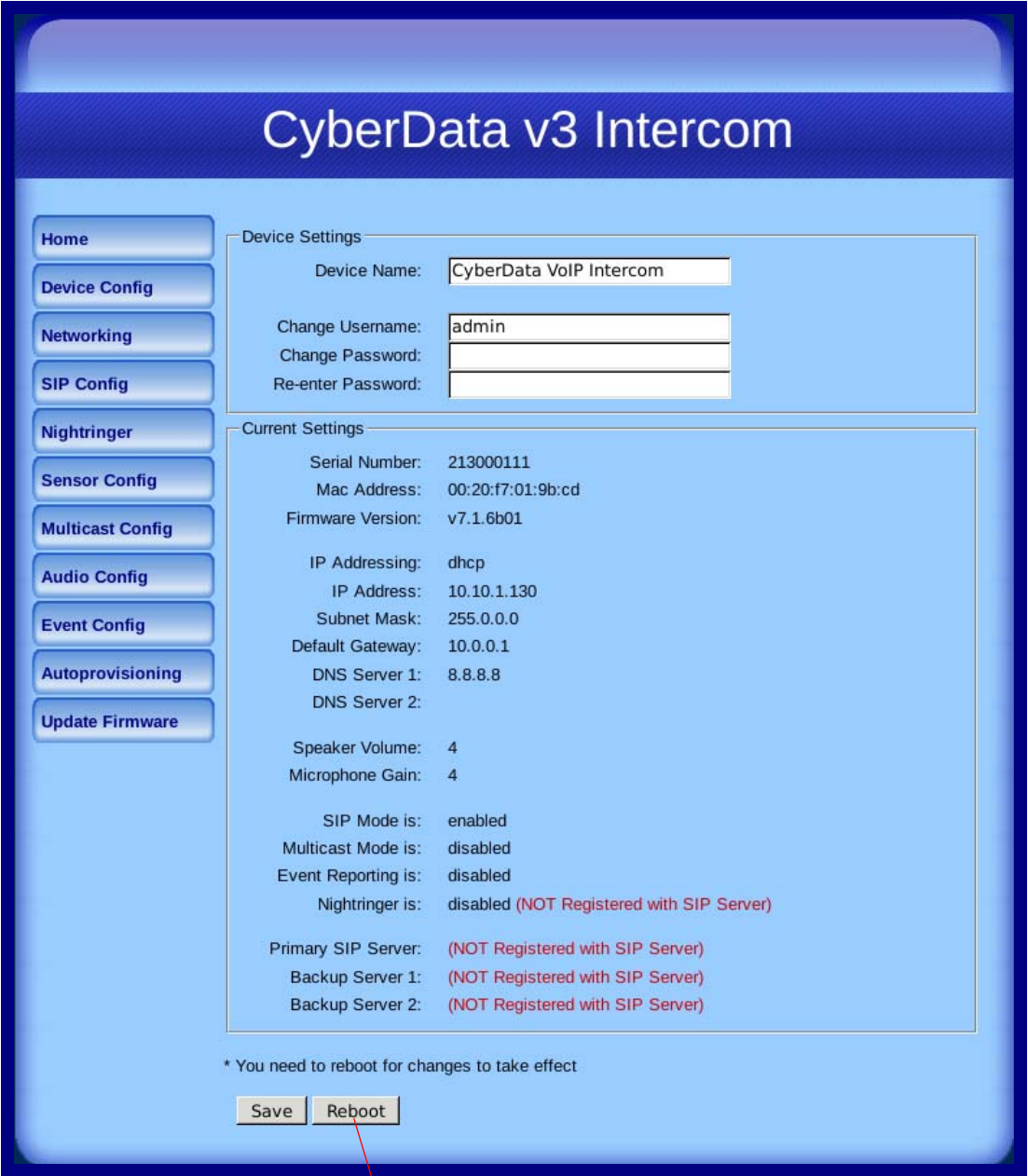
| Web Page Item | Description |
|---|---|
| File Upload | |
| Firmware Version | Shows the current firmware version. |
|  | Use the Browse button to navigate to the location of the Intercom firmware file that you want to upload. |
|  | Click on the Submit button to automatically upload the selected firmware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

2.12.2 Reboot the Intercom

To reboot a Intercom, log in to the web page as instructed in [Section 2.11.3, "Log in to the Configuration Home Page"](#).

1. Click **Reboot** ([Figure 2-35](#)). A normal restart will occur.

Figure 2-35. Reboot System Section



Reboot

2.13 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.

2.13.1 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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://10.0.3.71/cgi-bin/command.cgi" --post-data "terminate=yes" |
| Force reboot | wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/command.cgi" --post-data "reboot=yes" |
| Test Audio button | wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/command.cgi" --post-data "test_audio=yes" |
| Announce IP address | wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_0=yes" |
| Play the "1" audio file | wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_1=yes" |
| Play the "2" audio file | wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_2=yes" |
| Play the "3" audio file | wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.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 | wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_4=yes" |
| Play the "5" audio file | wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_5=yes" |
| Play the "6" audio file | wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_6=yes" |
| Play the "7" audio file | wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_7=yes" |
| Play the "8" audio file | wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_8=yes" |
| Play the "9" audio file | wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_9=yes" |
| Play the "Dot" audio file | wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_d=yes" |
| Play the "Audio Test" audio file (from Audio Config) | wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_audiotest=yes" |
| Play the "Page Tone" audio file | wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_pagetone=yes" |
| Play the "Your IP Address Is" audio file | wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_youripaddressis=yes" |
| Play the "Rebooting" audio file | wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_rebooting=yes" |
| Play the "Restoring Default" audio file | wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_restoringdefault=yes" |
| Play the "Ringback tone" audio file | wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_ringback=yes" |
| Play the "Ring tone" audio file | wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_ringtone=yes" |
| Play the "Intrusion Sensor Triggered" audio file | wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_intrusionsensortriggered=yes" |
| Play the "Door Ajar" audio file | wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_doorajar=yes" |

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

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

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 --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_ringback=yes" |
| Delete the "Ring tone" audio file | wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_ringtone=yes" |
| Delete the "Intrusion Sensor Triggered" audio file | wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_intrusionsensortriggered=yes" |
| Delete the "Door Ajar" audio file | wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_doorajar=yes" |
| Delete the "Night Ring" audio file | wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_nightring=yes" |
| Trigger the Door Sensor Test (Sensor Config page) | wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/sensorconfig.cgi" --post-data "doortest=yes" |
| Trigger the Intrusion Sensor Test (Sensor Config page) | wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/sensorconfig.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 2.11.6.2, "Point-to-Point Configuration"](#)

Appendix A: Mounting the Indoor Intercom

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


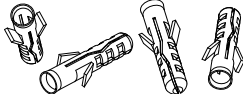
| Quantity | Part Name | Illustration |
|----------|-----------------------|---|
| 4 | Sheet Metal Screw |  |
| 4 | Plastic Ribbed Anchor |  |

Table A-2. Gang Box Mounting Components


| Quantity | Part Name | Illustration |
|----------|--|---|
| 4 | #6-32 FlatHead Countersunk Machine Screw |  |

Figure A-1 shows how to properly connect the VoIP Intercom.

Figure A-1. Cable Connections

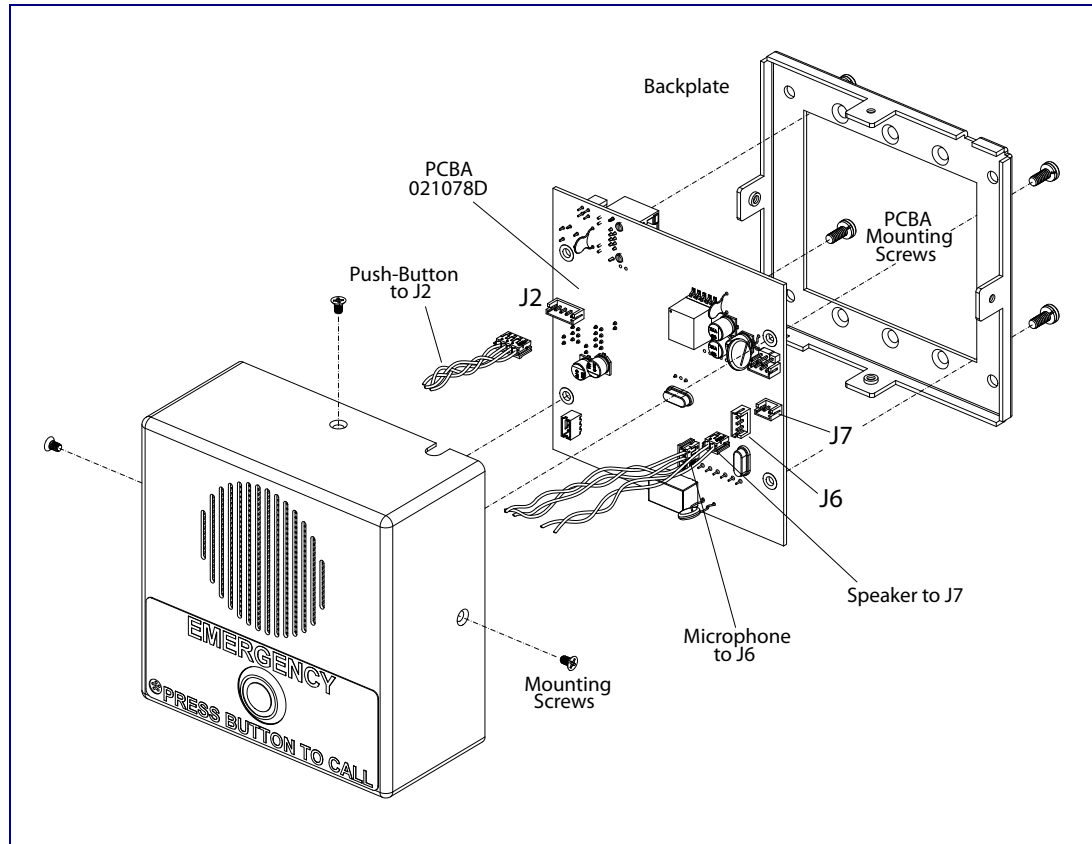


Figure A-2 shows a wall mounting option.

Figure A-2. Wall Mounting Option

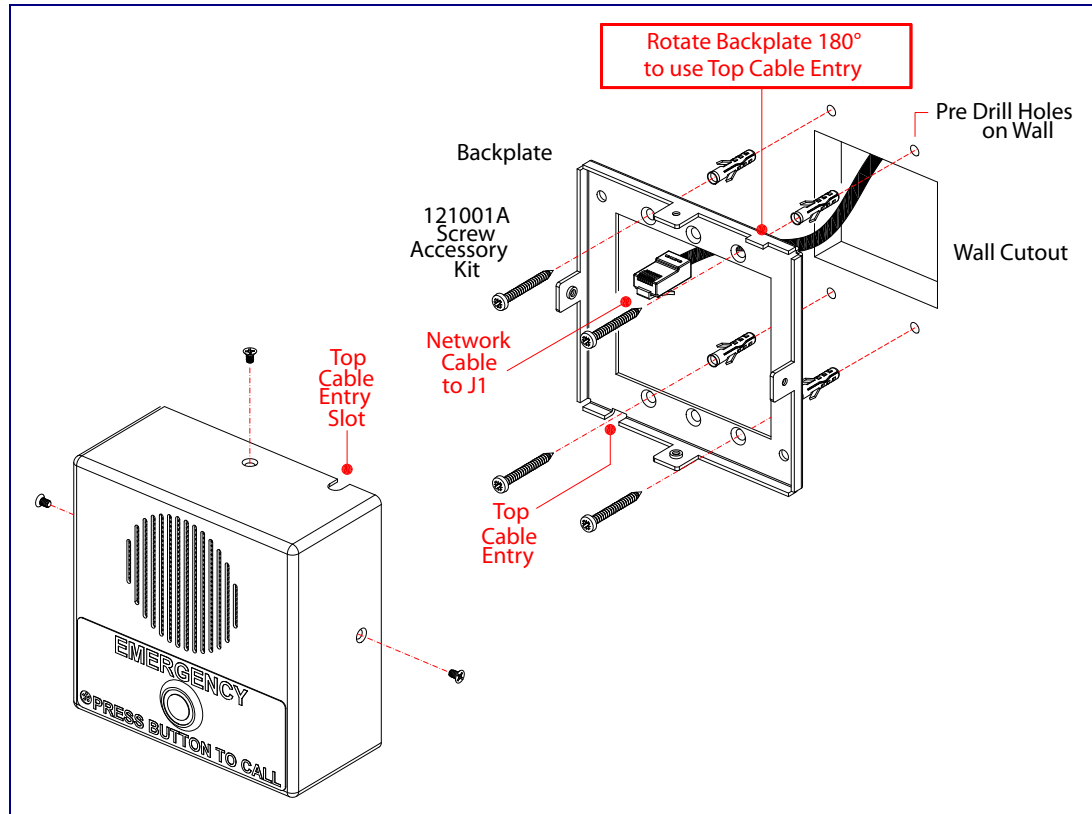


Figure A-3 shows a 1-Gang Box and a 2-Gang Box mounting option.

Figure A-3. Gang Box Mounting

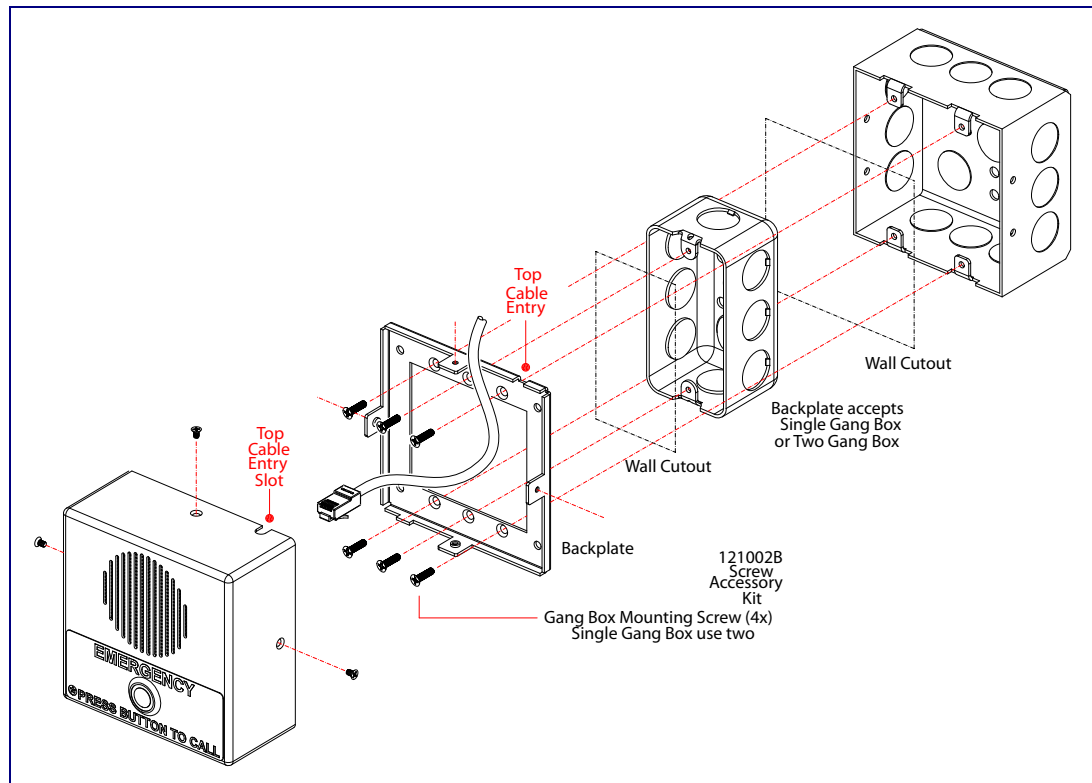
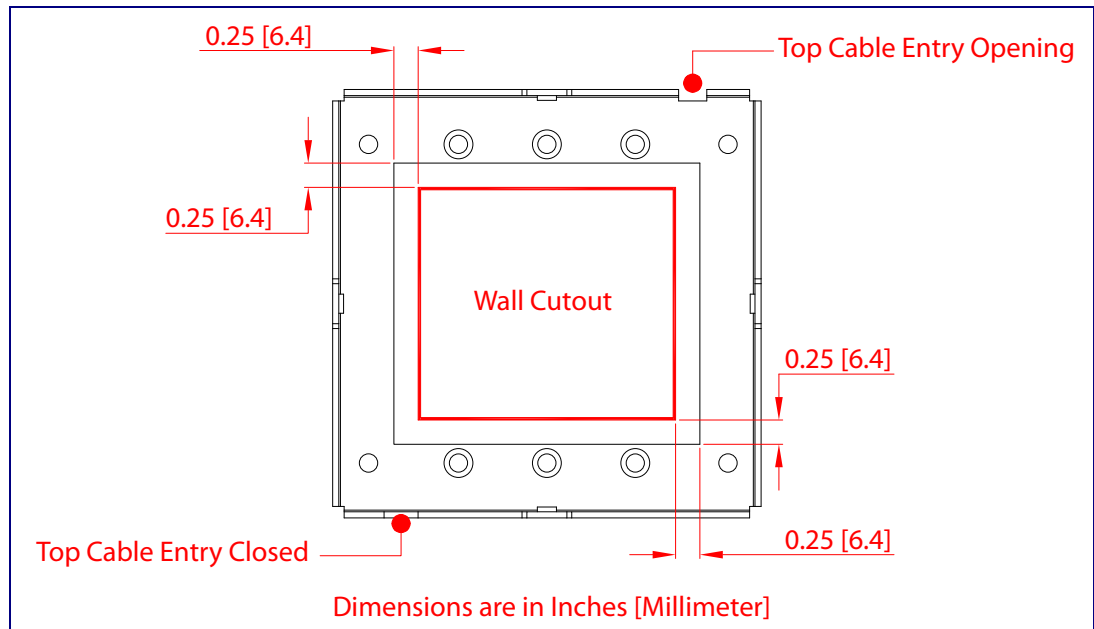


Figure A-4 shows the maximum recommended wall cutout dimensions.

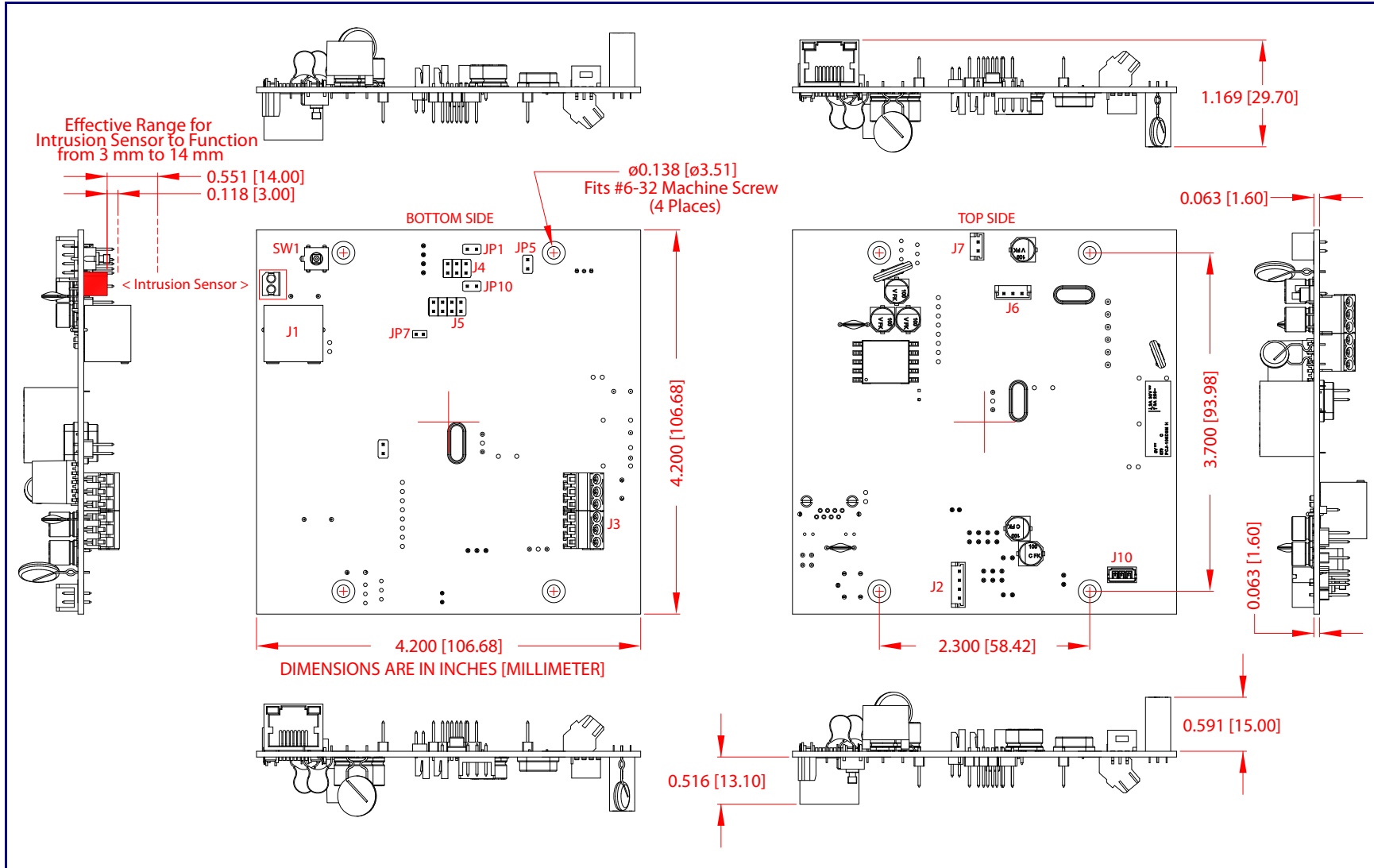
Figure A-4. Maximum Recommended Wall Cutout Dimensions



A.2 PCB Dimensions

Figure A-5 shows the PCB dimensions and the intrusion sensor range.

Figure A-5. PCB Dimensions and Intrusion Sensor Range



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/support/voip/solarwinds.html>

To set up a TFTP server on Windows:

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

Appendix C: Troubleshooting/Technical Support

C.1 Frequently Asked Questions (FAQ)

A list of frequently asked questions (FAQs) are available on the VoIP V3 Emergency Intercom product page at:

<http://www.cyberdata.net/products/voip/digitalanalog/intercomemergencyv3/faqs.html>

Select the support page for your product to see a list of frequently asked questions for the CyberData product:

C.2 Documentation

The documentation for this product is released in an English language version only. You can download PDF copies of CyberData product documentation from the VoIP V3 Emergency Intercom product page at:

<http://www.cyberdata.net/products/voip/digitalanalog/intercomemergencyv3/docs.html>

C.3 Contact Information

| | |
|----------------------------------|---|
| Contact | <p>CyberData Corporation 3 Justin Court Monterey, CA 93940 USA www.CyberData.net Phone: 800-CYBERDATA (800-292-3732) Fax: 831-373-4193</p> |
| Sales | <p>Sales 831-373-2601 Extension 334</p> |
| Technical Support | <p>The fastest way to get technical support for your VoIP product is to submit a VoIP Technical Support form at the following website:</p> <p>http://www.cyberdata.net/support/contactsupportvoip.html</p> <p>Phone: (831) 373-2601, Ext. 333 Email: support@cyberdata.net</p> |
| Returned Materials Authorization | <p>To return the product, contact the Returned Materials Authorization (RMA) department:</p> <p>Phone: 831-373-2601, Extension 136 Email: RMA@CyberData.net</p> <p>When returning a product to CyberData, an approved CyberData RMA number must be printed on the outside of the original shipping package. No product will be accepted for return without an approved RMA number. Send the product, in its original package, to the following address:</p> <p>CyberData Corporation 3 Justin Court Monterey, CA 93940 Attention: RMA "your RMA number"</p> |
| RMA Status Form | <p>If you need to inquire about the repair status of your product(s), please use the CyberData RMA Status form at the following web address:</p> <p>http://www.cyberdata.net/support/rmastatus.html</p> |

C.4 Warranty

CyberData warrants its product against defects in material or workmanship for a period of two years from the date of purchase. Should the product fail within the warranty period, CyberData will repair or replace the product free of charge. This warranty includes all parts and labor.

Should the product fail out-of-warranty, a flat rate repair charge of one half of the purchase price of the product will be assessed. Repairs that are in warranty but are damaged by improper modifications or abuse, will be charged at the out-of-warranty rate. Products shipped to CyberData, both in and out-of-warranty, are shipped at the expense of the customer. Shipping charges for repaired products shipped back to the customer by CyberData, will be paid by CyberData.

CyberData shall not under any circumstances be liable to any person for any special, incidental, indirect or consequential damages, including without limitation, damages resulting from use or malfunction of the products, loss of profits or revenues or costs of replacement goods, even if CyberData is informed in advance of the possibility of such damages.

C.4.1 Warranty & RMA Returns within the United States

If service is required, you must contact CyberData Technical Support prior to returning any products to CyberData. Our Technical Support staff will determine if your product should be returned to us for further inspection. If Technical Support determines that your product needs to be returned to CyberData, an RMA number will be issued to you at this point.

Your issued RMA number must be printed on the outside of the shipping box. No product will be accepted for return without an approved RMA number. The product in its original package should be sent to the following address:

CyberData Corporation
3 Justin Court.
Monterey, CA 93940
Attn: RMA "xxxxxx"

C.4.2 Warranty & RMA Returns Outside of the United States

If you purchased your equipment through an authorized international distributor or reseller, please contact them directly for product repairs.

C.4.3 Spare in the Air Policy

CyberData now offers a *Spare in the Air* no wait policy for warranty returns within the United States and Canada. More information about the *Spare in the Air* policy is available at the following web address:

<http://www.cyberdata.net/support/warranty/spareintheair.html>

C.4.4 Return and Restocking Policy

For our authorized distributors and resellers, please refer to your CyberData Service Agreement for information on our return guidelines and procedures.

For End Users, please contact the company that you purchased your equipment from for their return policy.

C.4.5 Warranty and RMA Returns Page

The most recent warranty and RMA information is available at the CyberData Warranty and RMA Returns Page at the following web address:

<http://www.cyberdata.net/support/warranty/index.html>

Index

Numerics

100 Mbps indicator light 17
16 AWG gauge wire 12

A

AC voltages, intercom enclosure is not rated 13
AC voltages, intercom enclosure not rated for 2
act light 18
activate relay (door sensor) 40
activate relay (intrusion sensor) 40
address, configuration login 23
announcing a device's IP address 19
audio configuration 43
 night ring tone parameter 45
audio configuration page 43
audio encodings 4
audio files, user-created 46
autoprovisioning 55
 autoprovisioned audio files 57
 autoprovisioned firmware upgrades 56
 autoprovisioning autoupdate 56
 autoprovisioning enabled option 55
 autoprovisioning from DHCP 55
 autoprovisioning server (IP address) 56
 networking 55
 setting up a TFTP server 71
autoprovisioning configuration 53, 54
auxiliary relay 5, 13
auxiliary relay wiring diagram 14

B

backup SIP server 1 32
backup SIP server 2 32
backup SIP servers, SIP server
 backups 32

C

cable connections 66
call button 10
 LED 10
call button LED 10
changing

 the web access password 26
Cisco SRST 32
command interface 61
commands 61
configurable parameters 27, 30, 32
configuration
 audio 43
 default IP settings 21
 door sensor 38
 intrusion sensor 38
 network 29
 SIP 31
 using Web interface 21
configuration home page 23
configuration page
 configurable parameters 27, 30
contact information 73
contact information for CyberData 73
Current Network Settings 30
current network settings 30
cutout dimensions, maximum recommended 69
CyberData contact information 73

D

default
 gateway 21
 intercom settings 76
 IP address 21
 subnet mask 21
 username and password 21
 web login username and password 23
default gateway 21, 30
default intercom settings 20
default IP settings 21
default login address 23
device configuration 26
 device configuration parameters 54
 the device configuration page 53
device configuration page 26
device configuration parameters 27
device configuration password
 changing for web configuration access 26
DHCP Client 4
DHCP IP addressing 30
dial out extension (door sensor) 40
dial out extension (intrusion sensor) 40
dial out extension strings 33
dial-out extension strings 35
dimensions 5

- label 7
 - pcb dimensions and intrusion sensor range 8, 70
 - unit dimensions 6
- discovery utility program 23
- DNS server 30
- door sensor 38, 40, 45
 - activate relay 40
 - dial out extension 40
 - door open timeout 40
 - door sensor normally closed 40
 - flash button LED 40
 - play audio locally 40
- door strike
 - cannot be powered by alternate power input nor PoE power 3, 12
- DTMF tones 33, 35
- DTMF tones (using rfc2833) 33
- dual speeds 17

E

- enable night ring events 49
- event configuration
 - enable night ring events 49
- expiration time for SIP server lease 32, 37

F

- factory default settings 20
 - how to set 20
- firmware
 - where to get the latest firmware 58
- flash button LED (door sensor) 40
- flash button LED (intrusion sensor) 40

G

- green link light 17

H

- home page 23
- http POST command 61
- http web-based configuration 4

I

- identifying your product 1
- illustration of intercom mounting process 65
- installation, typical intercom system 2
- intercom configuration
 - default IP settings 21
- intercom configuration page
 - configurable parameters 32
- intrusion sensor 38, 40
 - activate relay 40
 - dial out extension 40
 - flash button LED 40
 - play audio locally 40
- IP address 21, 30
- IP addressing 30
 - default IP addressing setting 21

J

- J3 terminal block, 16 AWG gauge wire 12

L

- label alignment 7
- label dimensions 7
- lease, SIP server expiration time 32, 37
- lengthy pages 42
- link light 17
- Linux, setting up a TFTP server on 71
- local SIP port 32
- log in address 23

M

- MGROUP
 - MGROUP Name 42
- mounting
 - gang box mounting 68
 - maximum recommended wall cutout dimensions 69
 - wall cutout dimensions 70
 - wall mounting 67
 - wall mounting components 65
- mounting an intercom 65
- multicast configuration 41
- Multicast IP Address 42

N

- navigation (web page) 22
- navigation table 22
- network activity, verifying 18
- network configuration of intercom 29
- network rate 5
- Network Setup 29
- nightring tones 42
- Nightringer 12, 36
- Nightringer in peer to peer mode (cannot be used) 36
- nightringer settings 37
- Nightringer, SIP registration required 36

O

- operating temperature 5
- orange link light 17

P

- packet time 4
- pages (lengthy) 42
- part number 5
- password
 - for SIP server login 32
 - login 23
 - restoring the default 21
- payload types 5
- pcb dimensions and intrusion sensor range 8, 70
- play audio locally (door sensor) 40
- play audio locally (intrusion sensor) 40
- point-to-point configuration 34
- port
 - local SIP 32
 - remote SIP 32
- POST command 61
- power requirement 5
- priority
 - assigning 42
- product
 - configuring 21
 - mounting 65
 - parts list 9
- 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

R

- reboot 59, 60
- regulatory compliance 5
- remote SIP port 32
- reset test function management button 19
- resetting the IP address to the default 65, 72
- restoring factory default settings 20, 76
- restoring the factory default settings 20
- return and restocking policy 75
- ringtones 42
 - lengthy pages 42
- RJ-45 16
- RMA returned materials authorization 73
- RMA status 73
- RTFM button 19
- RTFM jumper 19, 20
- RTP/AVP 4

S

- sales 73
- sensor setup page 39
- sensor setup parameters 38
- sensors 40
- server address, SIP 32
- service 73
- setting up an intercom 12
- settings, default 20
- SIP
 - enable SIP operation 32
 - local SIP port 32
 - user ID 32
- SIP (session initiation protocol) 4
- SIP configuration 31
 - SIP Server 32
- SIP configuration parameters
 - outbound proxy 32
 - registration and expiration, SIP server lease 32, 37
 - user ID, SIP 32
- SIP registration 32
- SIP remote SIP port 32
- SIP server 32
 - password for login 32
 - SIP servers supported 4
 - user ID for login 32
- SIP settings 33
- Spare in the Air Policy 74
- speaker output 5

SRST 32
 static IP addressing 30
 subnet mask 21, 30
 supported protocols 4

T

tech support 73
 technical support, contact information 73
 terminal block, 16 AWG gauge wire 12
 TFTP server 4, 71

U

unit dimensions 6
 user ID
 for SIP server login 32
 username
 changing for web configuration access 26
 default for web configuration access 23
 restoring the default 21

V

verifying
 network activity 18

W

wall cutout dimensions 70
 wall cutout dimensions, maximum recommended 69
 wall mounting option 67
 warranty 74
 warranty & RMA returns outside of the United States 74
 warranty & RMA returns within the United States 74
 warranty and RMA returns page 75
 warranty policy at CyberData 74
 web access password 21
 web access username 21
 web configuration log in address 23
 web page
 navigation 22
 web page navigation 22
 web-based intercom configuration 21
 weight 5
 wget, free unix utility 61
 Windows, setting up a TFTP server on 71

Y

yellow act light 18
 yellow link light 17