



# *VoIP Intercom Operations Guide*

Part #010935  
Document Part #930242A-D  
for Firmware Version 6.5.1

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

---

---

**PoE VoIP Intercom Operations Guide 930242A-D**  
**Part # 010935**

**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](mailto:support@cyberdata.net)

Fax: (831) 373-4193

Company and product information is at [www.cyberdata.net](http://www.cyberdata.net).

---

## Revision Information

Revision 930242A-D, which was released on October 3, 2014 and corresponds to firmware version 6.5.1, has the following changes:

- Updates [Figure 2-1, "VoIP Intercom Connections"](#).

---

## Browsers Supported



The following browsers have been tested against firmware version 6.5.1:

- Internet Explorer (version: 10)
- Firefox (also called Mozilla Firefox) (version: 23.0.1)
- Chrome (version: 29.0.154.66 m)
- Safari (version: 5.1.7)

---



# Important Safety Instructions

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

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

---

## Hazard Levels

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

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

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

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

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

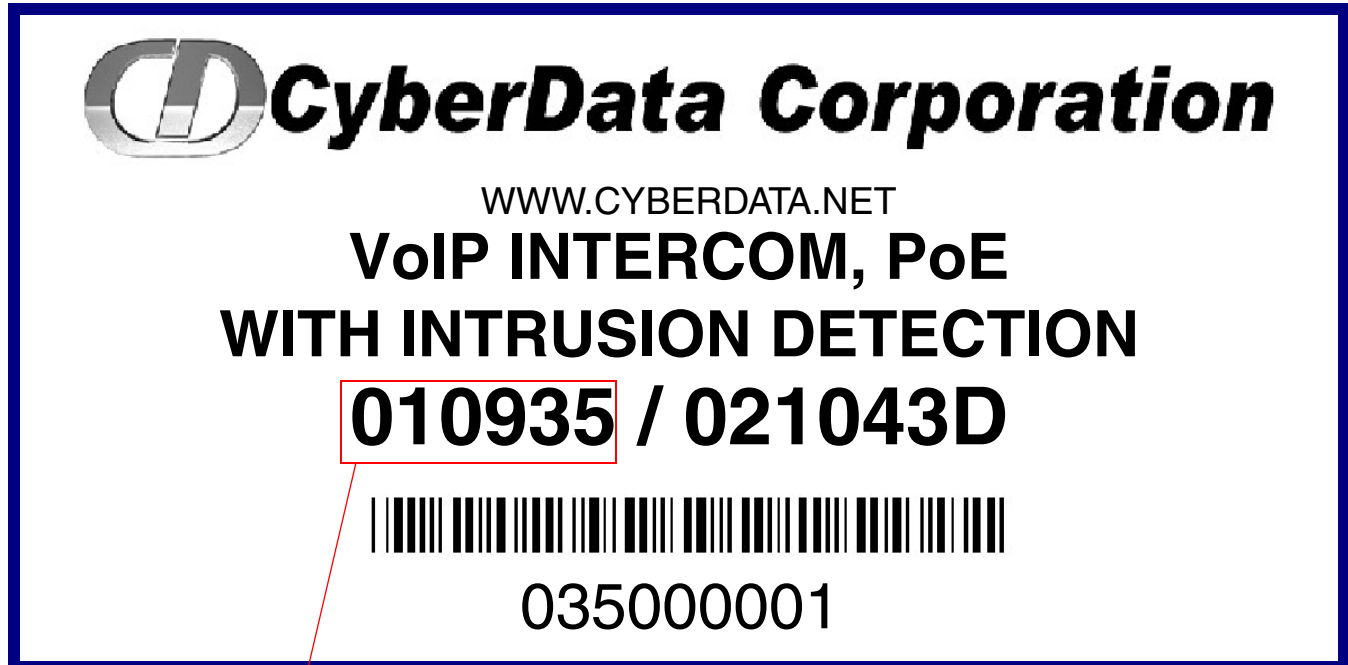
<b>Chapter 1 Product Overview</b>	<b>1</b>
1.1 How to Identify This Product .....	1
1.2 Typical System Installation .....	2
1.3 Product Features .....	4
1.4 Supported Protocols .....	5
1.5 Supported SIP Servers .....	5
1.6 Product Specifications .....	6
1.7 Dimensions .....	7
<b>Chapter 2 Installing the VoIP Intercom</b>	<b>9</b>
2.1 Parts List .....	9
2.1 Intercom Setup .....	10
2.1.1 VoIP Intercom Connections .....	10
2.1.2 Connecting the Intercom to the Auxiliary Relay .....	11
2.1.3 Identifying the VoIP Intercom Connectors .....	13
2.1.4 Call Button and the Call Button LED .....	15
2.1.5 Network Connectivity, and Data Rate .....	16
2.1.6 RTFM Button .....	18
2.1.7 Announcing the IP Address .....	20
2.1.8 Restore the Factory Default Settings .....	21
2.1.9 Adjust the Volume .....	25
2.2 Configure the Intercom Parameters .....	25
2.2.1 Intercom Web Page Navigation .....	26
2.2.2 Log in to the Configuration Home Page .....	27
2.2.3 Configure the Device .....	30
2.2.4 Configure the Network Parameters .....	33
2.2.5 Configure the SIP Parameters .....	35
2.2.6 Configure the Nightringer Parameters .....	40
2.2.7 Configure the Sensor Configuration Parameters .....	42
2.2.8 Configure the Multicast Parameters .....	45
2.2.9 Configure the Audio Configuration Parameters .....	47
2.2.10 Configure the Event Parameters .....	52
2.2.11 Configure the Autoprovisioning Parameters .....	57
2.3 Upgrade the Firmware and Reboot the Intercom .....	65
2.3.1 Reboot the Intercom .....	67
2.4 Command Interface .....	68
2.4.1 Command Interface Post Commands .....	68
<b>Appendix A Mounting the Intercom</b>	<b>74</b>
A.1 Mount the Intercom .....	74
A.1.1 Custom Flush Mounting .....	79
<b>Appendix B Setting up a TFTP Server</b>	<b>80</b>
B.1 Set up a TFTP Server .....	80
B.1.1 In a LINUX Environment .....	80
B.1.2 In a Windows Environment .....	80
<b>Appendix C Troubleshooting/Technical Support</b>	<b>81</b>
C.1 Frequently Asked Questions (FAQ) .....	81
C.2 Documentation .....	81
C.3 Contact Information .....	82
C.4 Warranty .....	83
C.4.1 Warranty & RMA Returns within the United States .....	83
C.4.2 Warranty & RMA Returns outside of the United States .....	83
C.4.3 Spare in the Air Policy .....	84
C.4.4 Return and Restocking Policy .....	84
C.4.5 Warranty and RMA Returns Page .....	84
<b>Index</b>	<b>85</b>

# 1 Product Overview

## 1.1 How to Identify This Product

To identify the VoIP Intercom, look for a model number label similar to the one shown in [Figure 1-1](#). The model number on the label should be **010935**.

Figure 1-1. Model Number Label



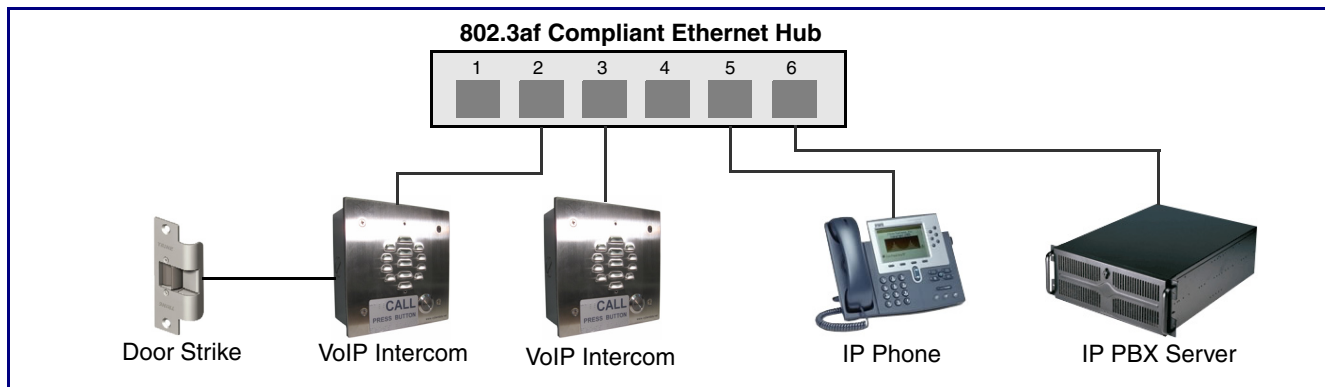
Model number

## 1.2 Typical System Installation

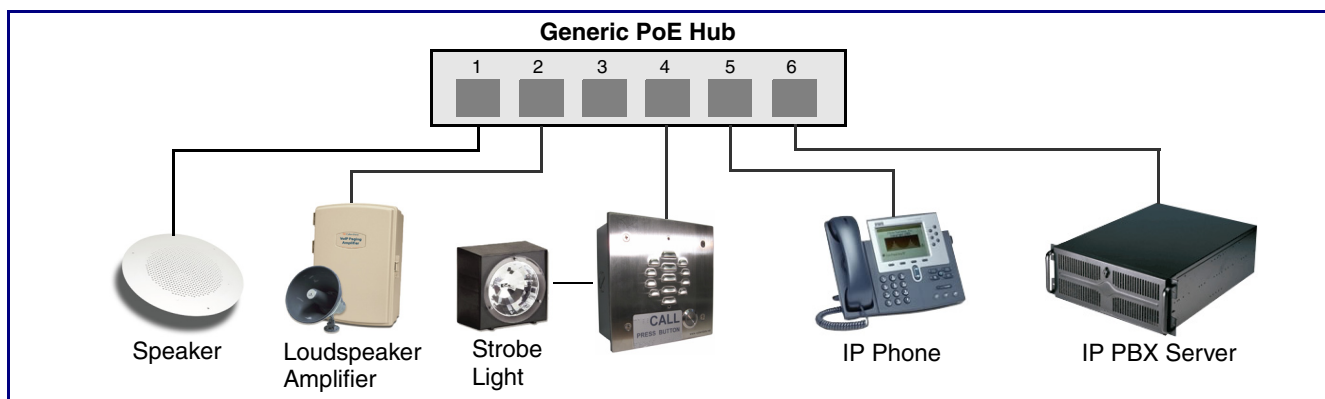
The Voice-over-IP (VoIP) Intercom is a SIP endpoint designed to provide VoIP phone connectivity in a tamper proof and secure package.

Figure 1-2, Figure 1-3, and Figure 1-4 illustrate how the VoIP Intercoms can be installed as part of a VoIP phone system.

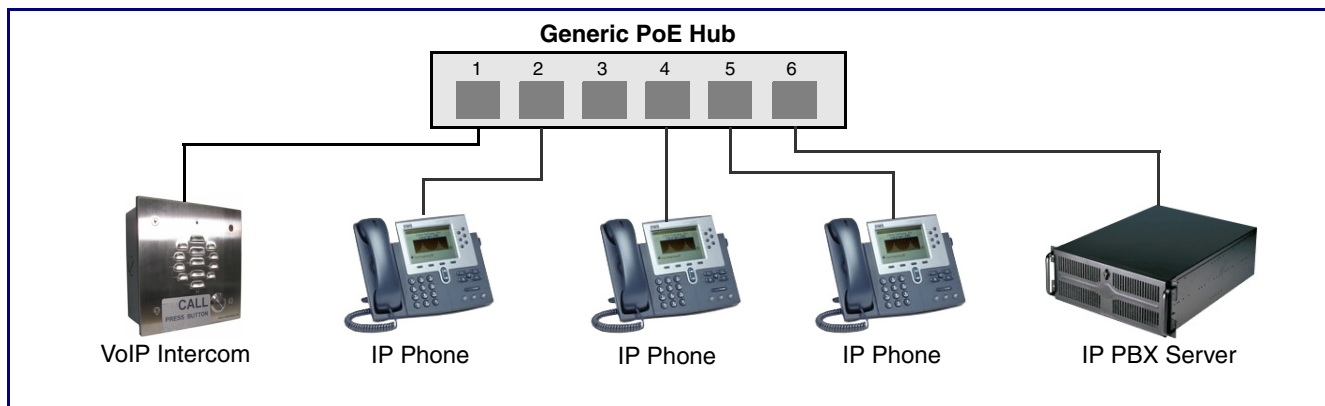
**Figure 1-2. Typical Installation—Door Entry/Access Control**






**Figure 1-3. Typical Installation—Mass Notification**



**Figure 1-4. Typical Installation—Emergency Phone**





 <p>GENERAL ALERT</p>	<p><b>Warning</b> <i>Electrical Hazard:</i> The VoIP Intercom enclosure is not rated for any AC voltages.</p>
 <p>GENERAL ALERT</p>	<p><b>Warning</b> <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><b>Warning</b> <i>Electrical Hazard:</i> To prevent injury, this apparatus must be securely attached to the floor/wall in accordance with the installation instructions.</p>

## 1.3 Product Features



- SIP
- Dual speeds of 10 Mbps and 100 Mbps
- 802.3af compliant
- 2 gang outlet box size
- Adaptive full duplex voice operation
- Network/Web management
- Network adjustable speaker volume adjustment
- Network configurable door or intrusion sensor settings
- Network configurable relay activation settings
- Dial Out Extension supports the addition of comma delimited pauses before sending additional DTMF tones
- Network configurable microphone input sensitivity adjustment
- Network downloadable product firmware
- Doubles as a paging speaker
- Call button
- Call activity indicator (light)
- Tamper proof design
- One dry contact relay for auxiliary control
- Autoprovisioning
- Configurable audio files
- Night Ringer
- Three year warranty
- Peer-to-peer capable
- Door closure and tamper alert signal
- Optional Torx screws with driver kit

## 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
- Audio Encodings
  - PCMU (G.711 mu-law)
  - PCMA (G.711 A-law)
  - Packet Time 20 ms

---

## 1.5 Supported SIP Servers

Go to the following link to find the VoIP Intercom product page which will have information on how to configure the VoIP Intercom for various supported SIP servers:

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

---

## 1.6 Product Specifications

<b>Category</b>	<b>Specification</b>
Speaker Output	1 Watt Peak Power
Ethernet I/F	10/100 Mbps
Protocol	SIP RFC 3261 Compatible
Power Input	PoE 802.3af compliant or +5 volts at 1000m
Operating Temperature	-10° C to 50° C (14° F to 122° F)
Payload Types	G711, A-law and $\mu$ -law
Part Number	010935
Dimensions	5" x 5" x 2.5"
Weight	1.6 lbs./shipping weight of 2.2 lbs. (0.7 kg/shipping weight of 1.0kg)
Auxiliary Relay	1A at 30 VDC

## 1.7 Dimensions

Figure 1-5. Dimensions—Size of Unit With Case

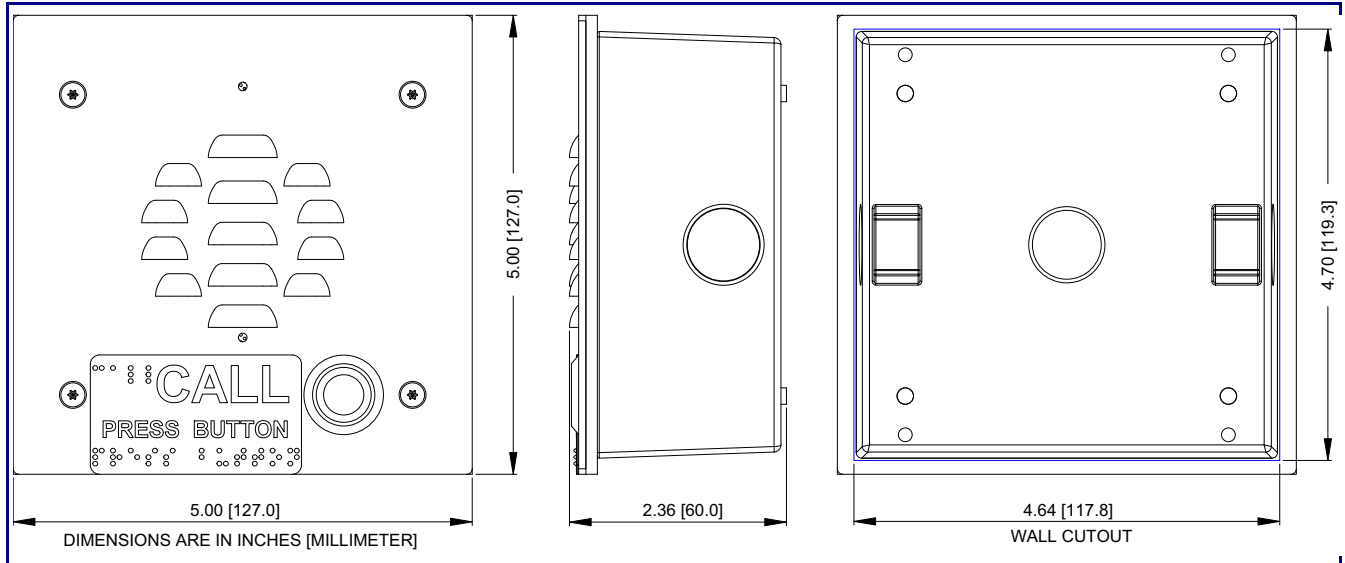
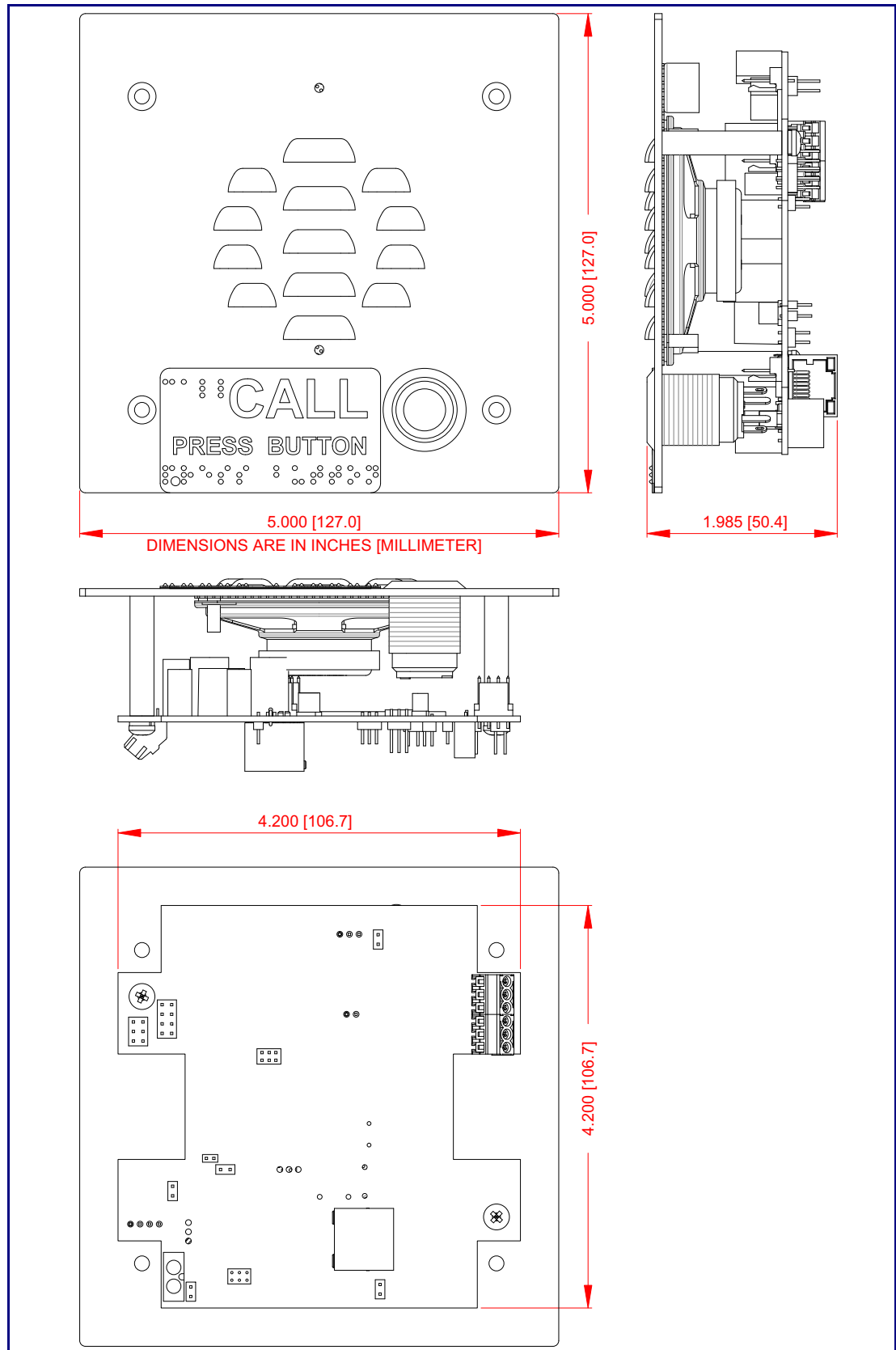


Figure 1-6. Dimensions—Size of Unit Without Gang Box






## 2 Installing the VoIP Intercom

### 2.1 Parts List

Table 2-1 illustrates the SiP VoIP and PoE Speaker parts.

**Table 2-1. Parts List**

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

## 2.1 Intercom Setup

### 2.1.1 VoIP Intercom Connections

Figure 2-1 shows the pin connections on the J7 (terminal block). This terminal block can accept 16 AWG gauge wire.

**Note** As an alternative to using PoE power, you can supply 5 VDC at 1000 mA into the terminal block.


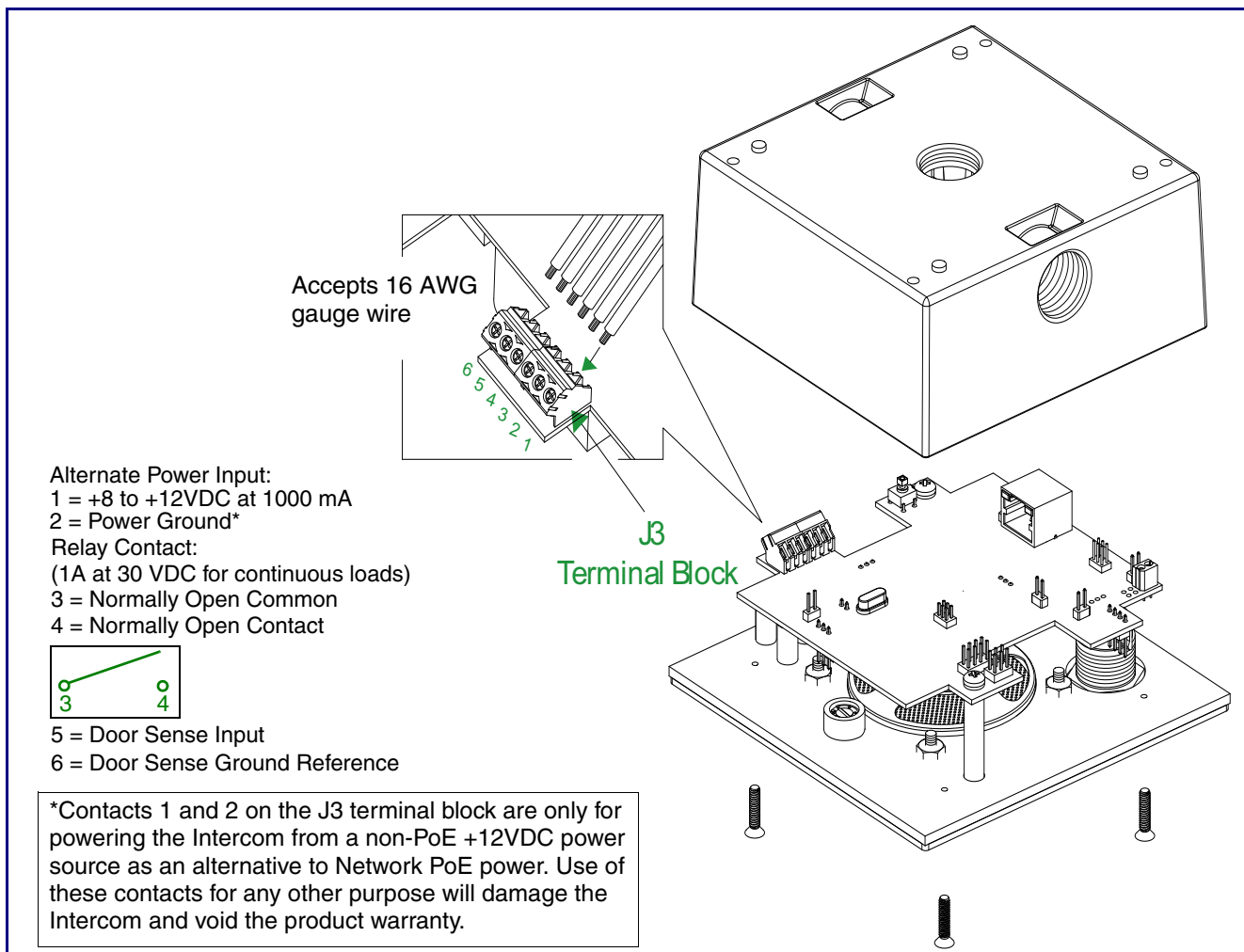




 <small>GENERAL ALERT</small>	<p><b>Caution</b></p> <p><b>Equipment Hazard:</b> Contacts 1 and 2 on the J3 terminal block are only for powering the Intercom from a non-PoE +12VDC power source as an alternative to Network PoE power. Use of these contacts for any other purpose will damage the Intercom and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

Figure 2-1. VoIP Intercom Connections





## 2.1.2 Connecting the Intercom to the Auxiliary Relay

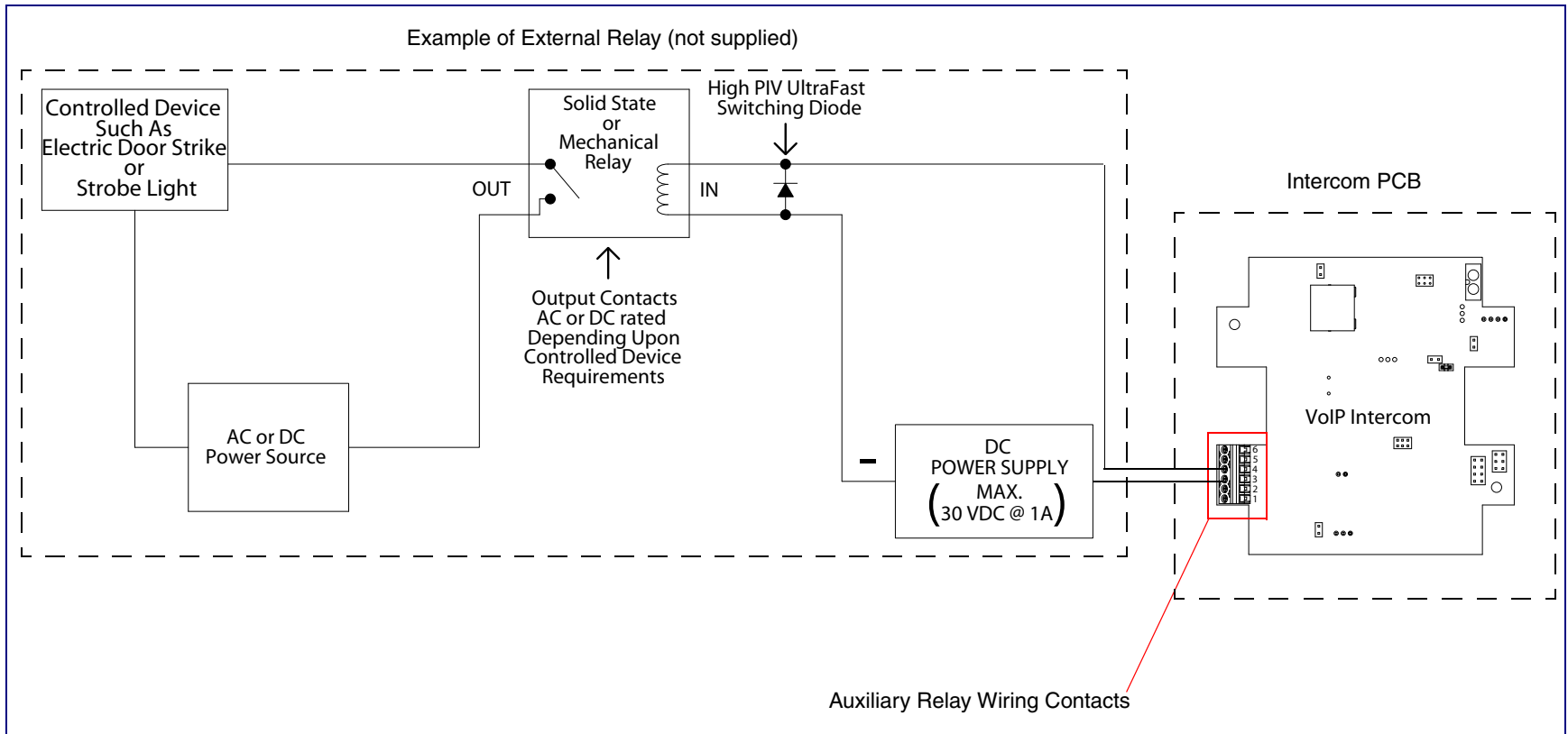
	<p><b>Warning</b> <i>Electrical Hazard:</i> The VoIP Intercom enclosure is not rated for any AC voltages.</p>
	<p><b>Warning</b> <i>Electrical Hazard:</i> This product should be installed by a licensed electrician according to all local electrical and building codes.</p>
	<p><b>Warning</b> <i>Electrical Hazard:</i> To prevent injury, this apparatus must be securely attached to the floor/wall in accordance with the installation instructions.</p>
	<p><b>Warning</b> <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 2.1.2, "Connecting the Intercom to the Auxiliary Relay"](#)).

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.

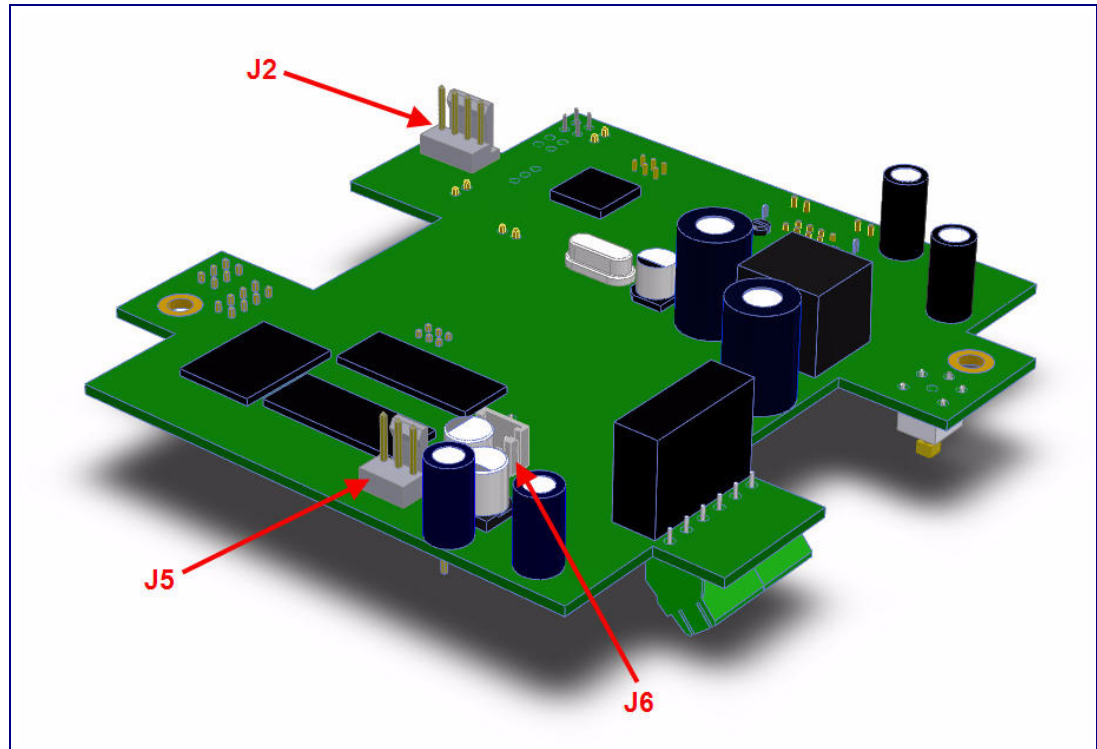
Figure 2-2. Auxiliary Relay Wiring Diagram



## 2.1.3 Identifying the VoIP Intercom Connectors

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

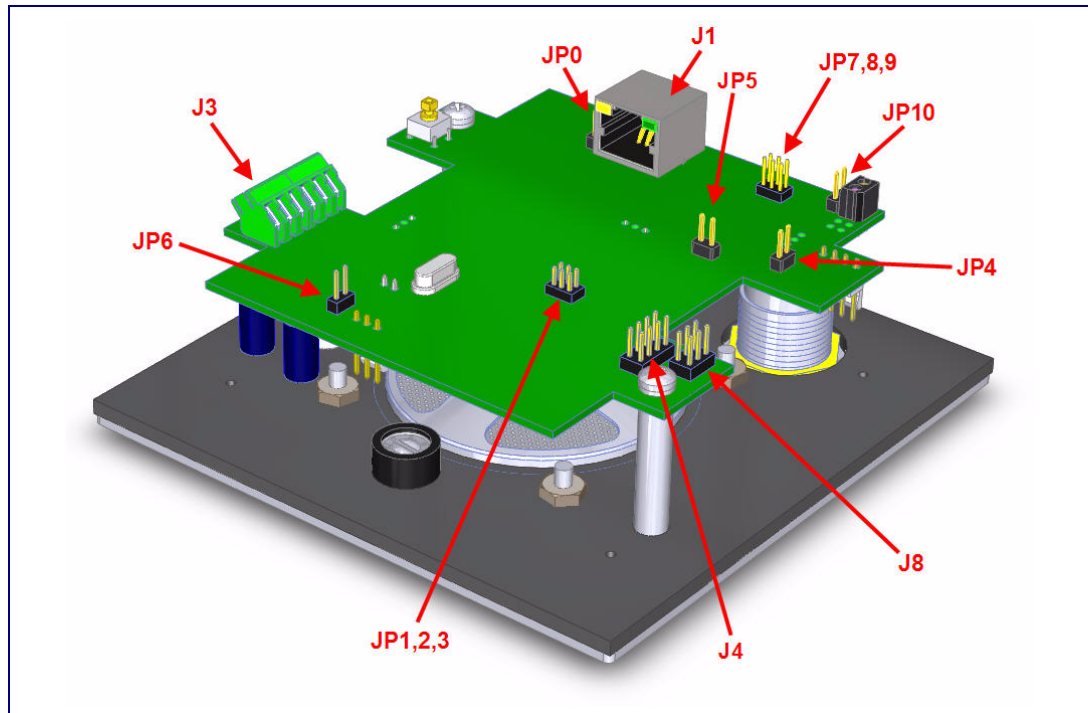
**Figure 2-3. J2, J5, and J6 Connector Locations**



**Table 2-2. Connector Functions**

Connector	Function
J2	Call Button. LED Interface
J5	Microphone Interface
J6	Speaker Interface

**Figure 2-4. Connector Locations**



**Table 2-3. Connector Functions**

Connector	Function
J1	PoE Network Connection (RJ-45 ethernet)
J3	Terminal Block (see <a href="#">Figure 2-1</a> )
J4	Factory Only
J8	Factory Only
JP0	Factory Only
JP1	Factory Only
JP2	Factory Only
JP3	Factory Only
JP4	Factory Only
JP5	Factory Only
JP6	Factory Only
JP7	Factory Only
JP8	Factory Only
JP9	Factory Only
JP10	Disables the intrusion sensor when installed.
SW1	RTFM (see <a href="#">Section 2.1.6, "RTFM Button"</a> )

---

## 2.1.4 Call Button and the Call Button LED

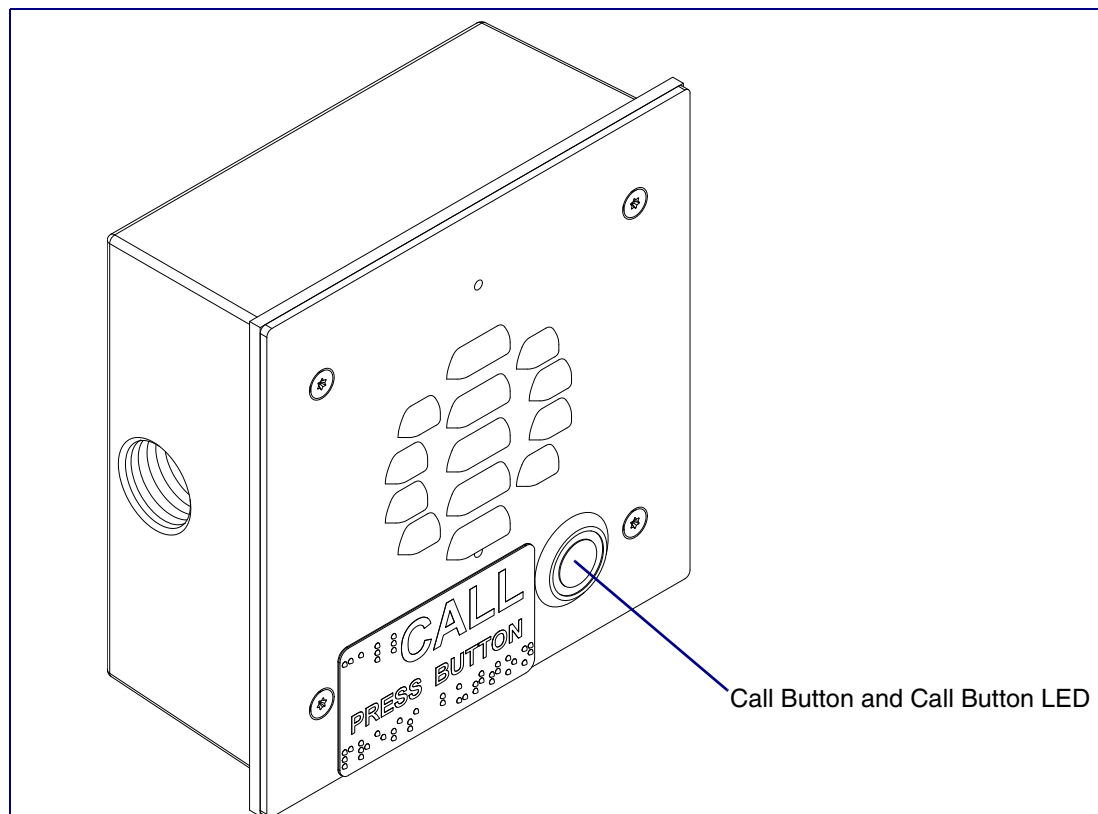
### 2.1.4.1 Calling with the The Call Button

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

### 2.1.4.2 Call Button LED Function

- Upon initial power or reset, the call button LED will illuminate.
- While the software is setting up the network, the call button led will blink rapidly (10 times/second).
- 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 call button led. The Call Button LED will still blink during initialization and calls.
- The Call Button LED will flash briefly at the beginning of RTFM mode.

**Figure 2-5. Call Button and Call Button LED**



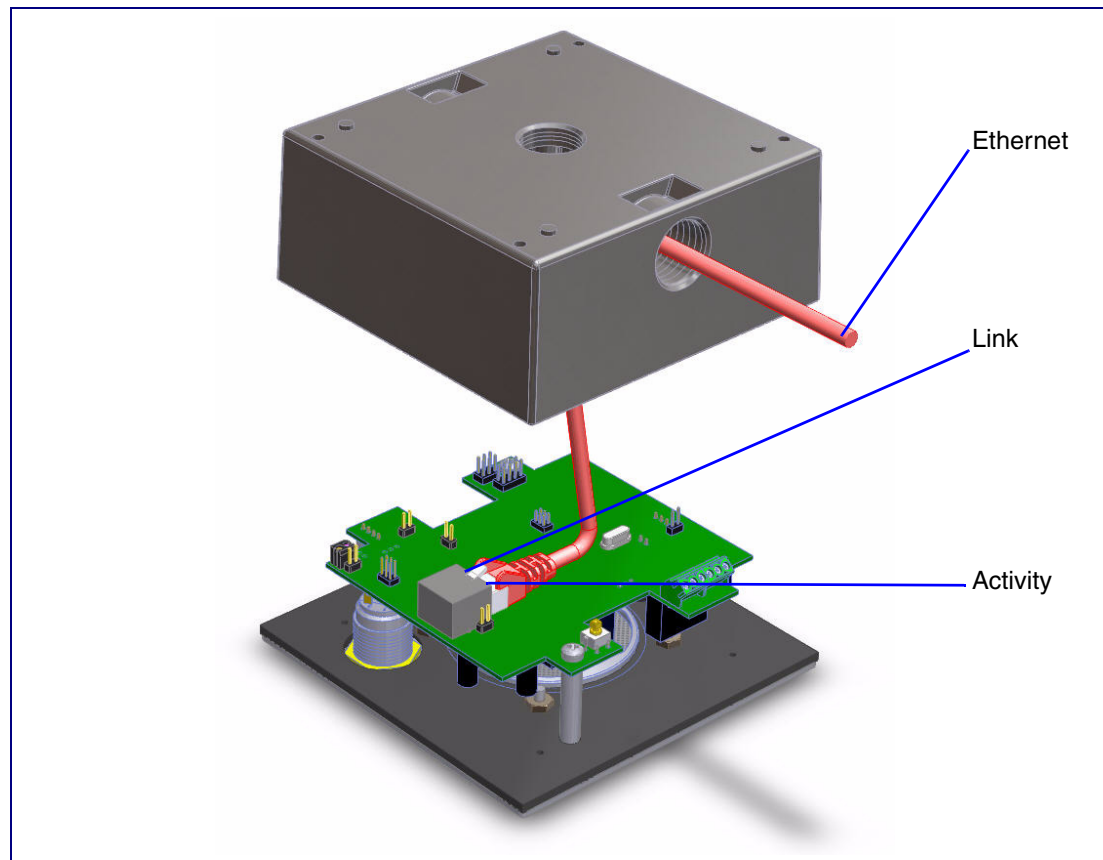
---

## 2.1.5 Network Connectivity, and Data Rate

When you plug in the Ethernet cable or power supply:

- The square, green **Link** light above the Ethernet port indicates that the network connection has been established (see [Figure 2-6](#) and [Figure 2-7](#)). The Link light changes color to confirm the auto-negotiated baud rate:
- This light is yellow at 10 Mbps.
- It is orange at 100 Mbps.

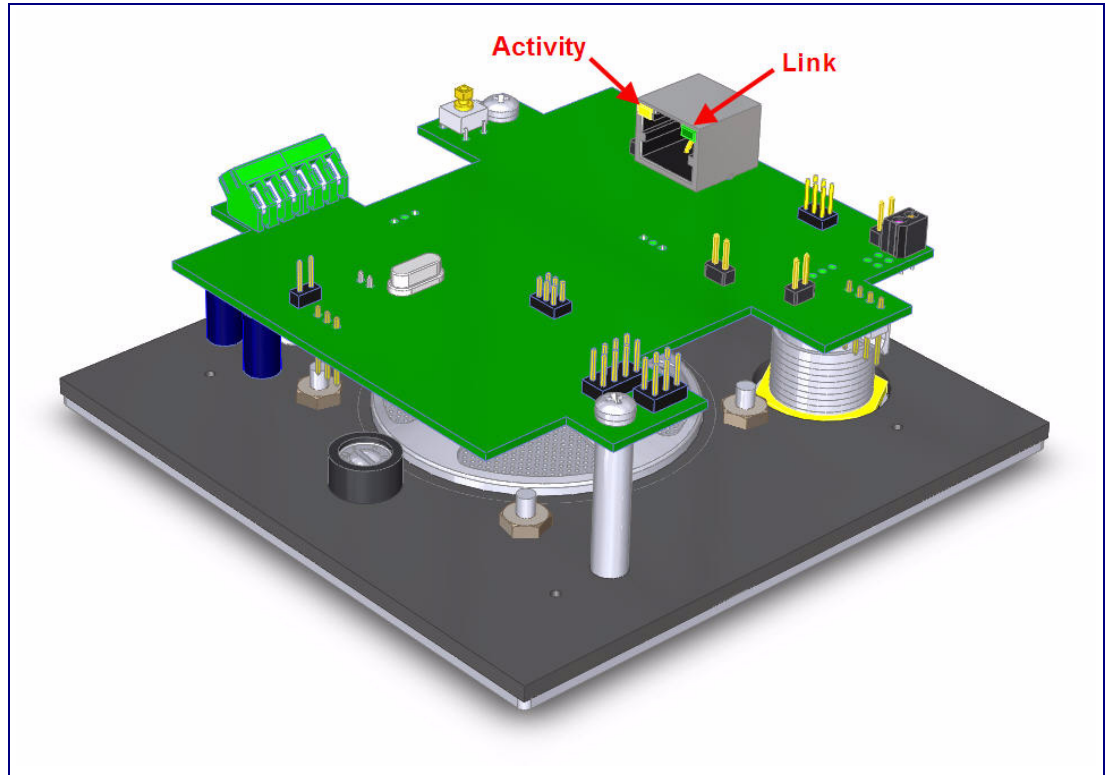
**Figure 2-6. Network Connector Prior to Installation**



### 2.1.5.1 Verify Network Activity

The square, yellow **Activity** light blinks when there is network activity.

**Figure 2-7. Network Connector**



## 2.1.6 RTFM Button



### Caution

Your intercom will have either an RTFM button or two jumper pins labeled JP11 on the circuit board. If your intercom does not have an RTFM button, use JP11 for IP address announcement and factory reset functions. Intercoms with JP11 jumper pins instead of an SW1 switch correspond to part numbers 010935A, 010935B, 010935C, 010935D, and 010935E. You will need a jumper shunt to place over the JP11 jumper pins per the instructions below. Intercoms with an RTFM button correspond to part number 010935F.

When the Intercom is operational and linked to the network, use the Reset Test Function Management (RTFM) button (see **SW1** in [Figure 2-8](#)) or place a jumper shunt on the JP11 jumper pins (see **JP11** in [Figure 2-9](#)) on the Intercom board to announce and confirm the Intercom's IP Address and test the audio is working. Your intercom will have an RTMF button or a JP11 jumper but not both.

**Note** You must do these tests prior to final assembly.

**Figure 2-8. RTFM Button (SW1)**

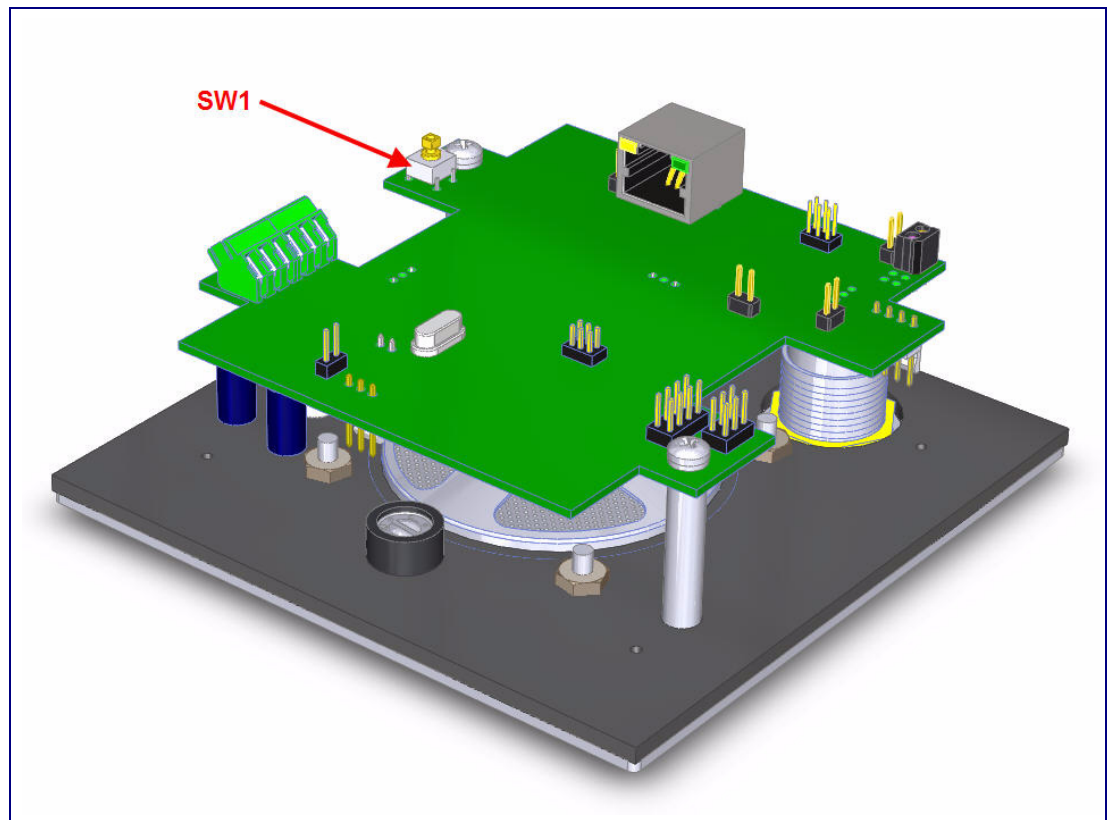
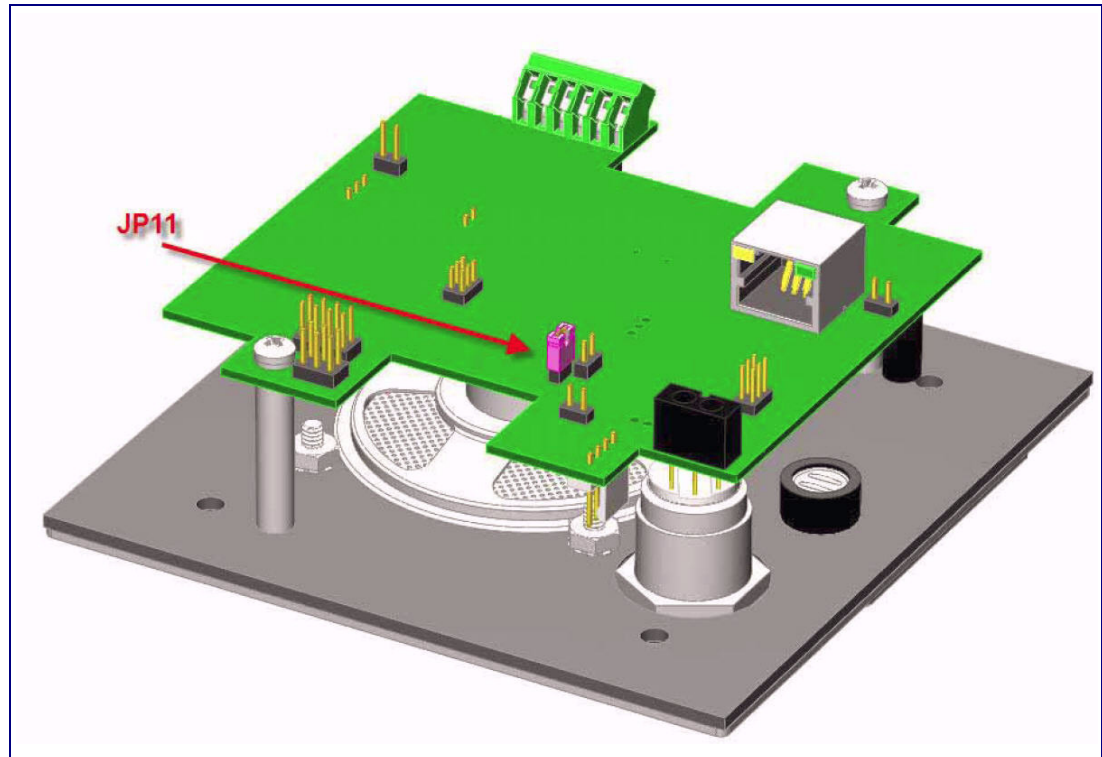




Figure 2-9. Jumper on JP11



---

## 2.1.7 Announcing the IP Address

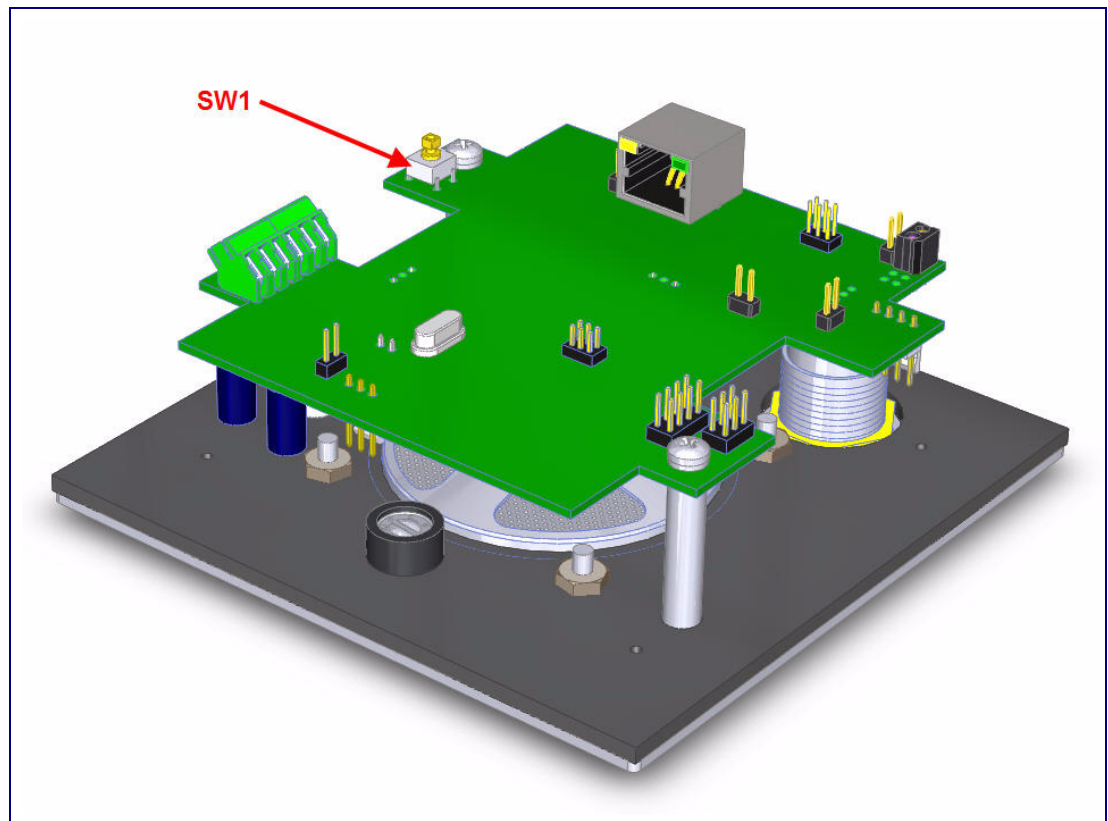
To announce a device's current IP address, first determine if you have an Intercom with an RTFM button (see **SW1** in [Figure 2-10](#)), and then do one of the following:

- If you have an Intercom that has an RTFM button, then see [Section 2.1.7.1, "Intercom with an RTFM Button"](#).
- If you have an Intercom that has a jumper and does not have an RTFM button, then see [Section 2.1.7.2, "Intercom with a Jumper and No RTFM Button"](#).

### 2.1.7.1 Intercom with an RTFM Button

1. If you have an Intercom with an RTFM button, then press and hold the RTFM button (see **SW1** in [Figure 2-10](#)) until the IP address is announced.
2. Release the Call Button after the IP address is announced.

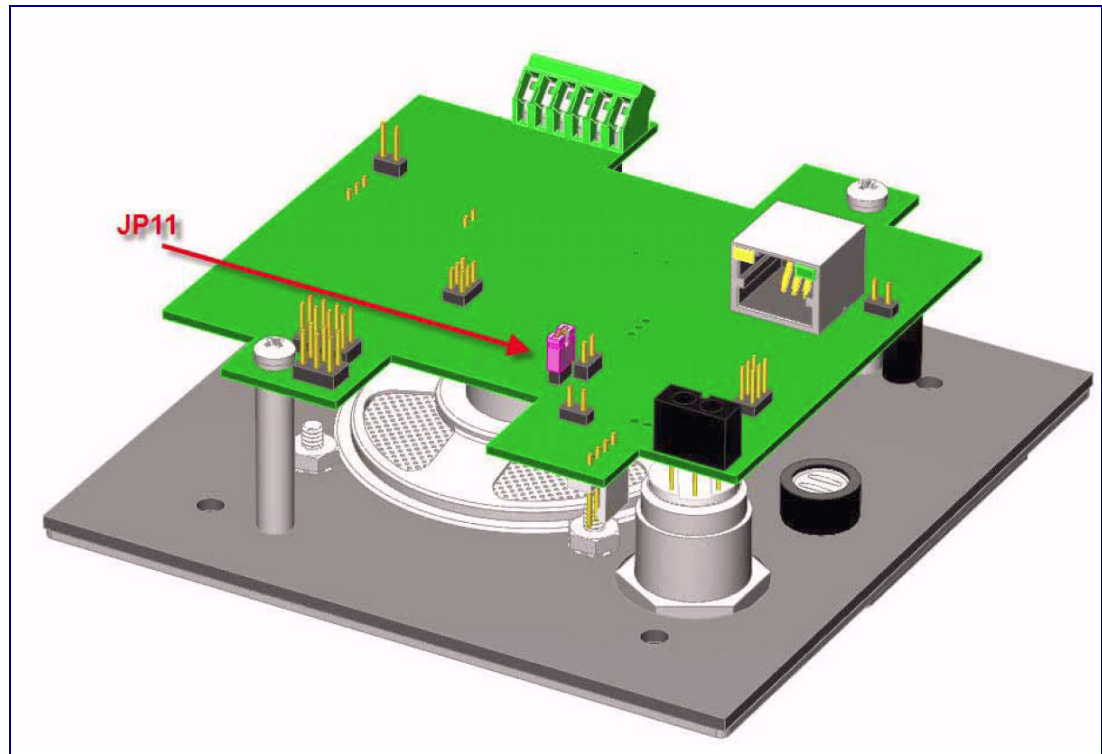
**Figure 2-10. RTFM Button (SW1 Button)**



### 2.1.7.2 Intercom with a Jumper and No RTFM Button

1. If you have an Intercom with a jumper and no RTFM button, then install a jumper on JP11. See **JP11** in [Figure 2-11](#).
2. Wait until the IP address is announced.
3. Remove the jumper and restart the unit.

**Figure 2-11. Jumper on JP11**



---

### 2.1.8 Restore the Factory Default Settings

When troubleshooting configuration problems, it is sometimes convenient to restore the device to a known state. To restore the factory default settings on your device, do one of the following:

- If you have an Intercom that has an RTFM Button, then see [Section 2.1.8.1, "Intercom with an RTFM Button"](#).
- If you have an Intercom that has a jumper and does not have an RTFM button, then see [Section 2.1.8.2, "Intercom with a Jumper"](#).

**Note** Each Intercom is delivered with factory set default values.

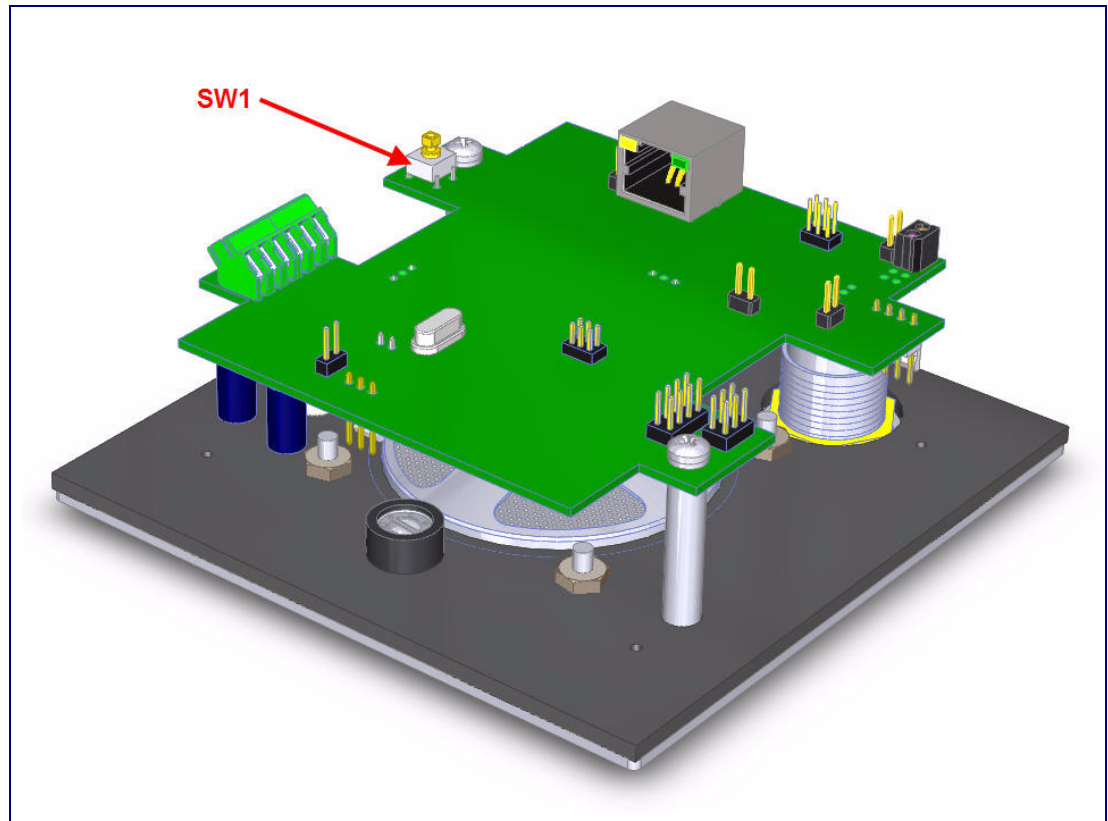
**Note** The device will use DHCP to obtain the new IP address (DHCP-assigned address or default to 10.10.10.10 if a DHCP server is not present).

### 2.1.8.1 Intercom with an RTFM Button

Complete the following steps to restore defaults on an Intercom that has an RTFM button:

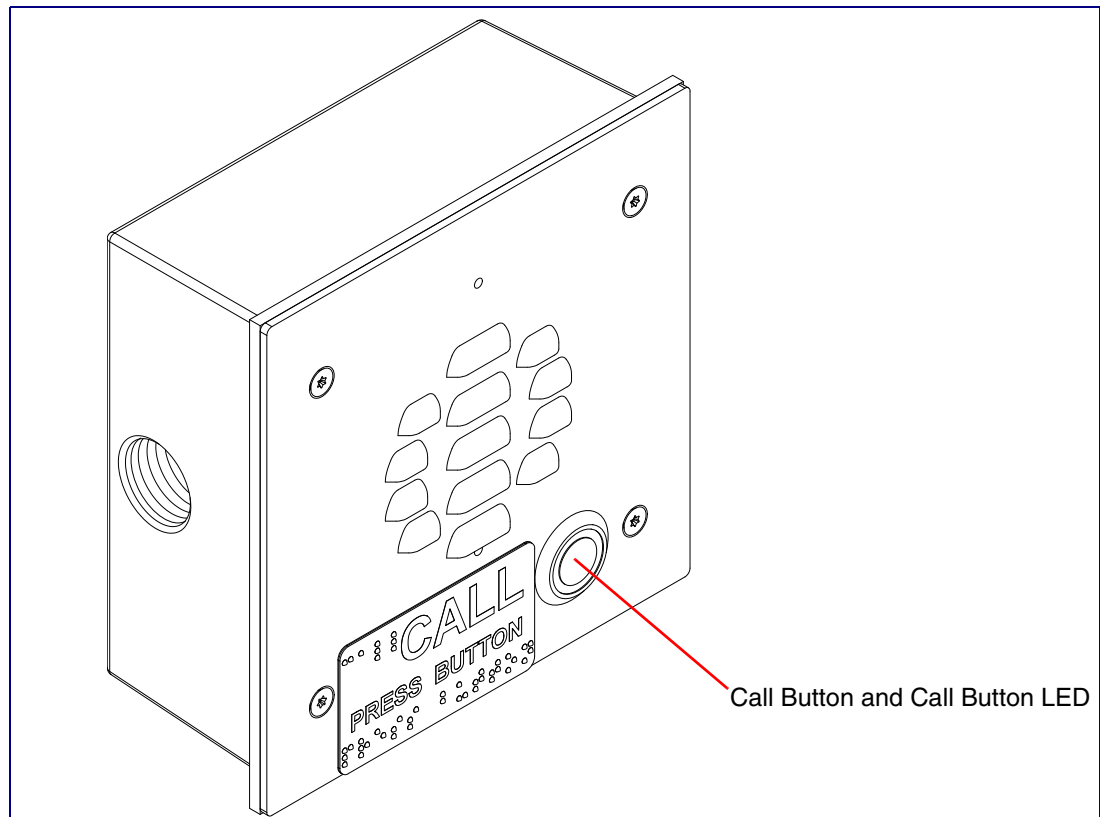
1. Press and hold the RTFM button (**SW1** in [Figure 2-12](#)) until the Intercom announces the IP address.

**Figure 2-12. RTFM Button (SW1 Button)**



2. The Call Button LED (see [Figure 2-13](#)) on the front will blink quickly.
3. Press and hold the Call Button until "**restoring defaults**" is announced.

**Figure 2-13. Call Button and Call Button LED**



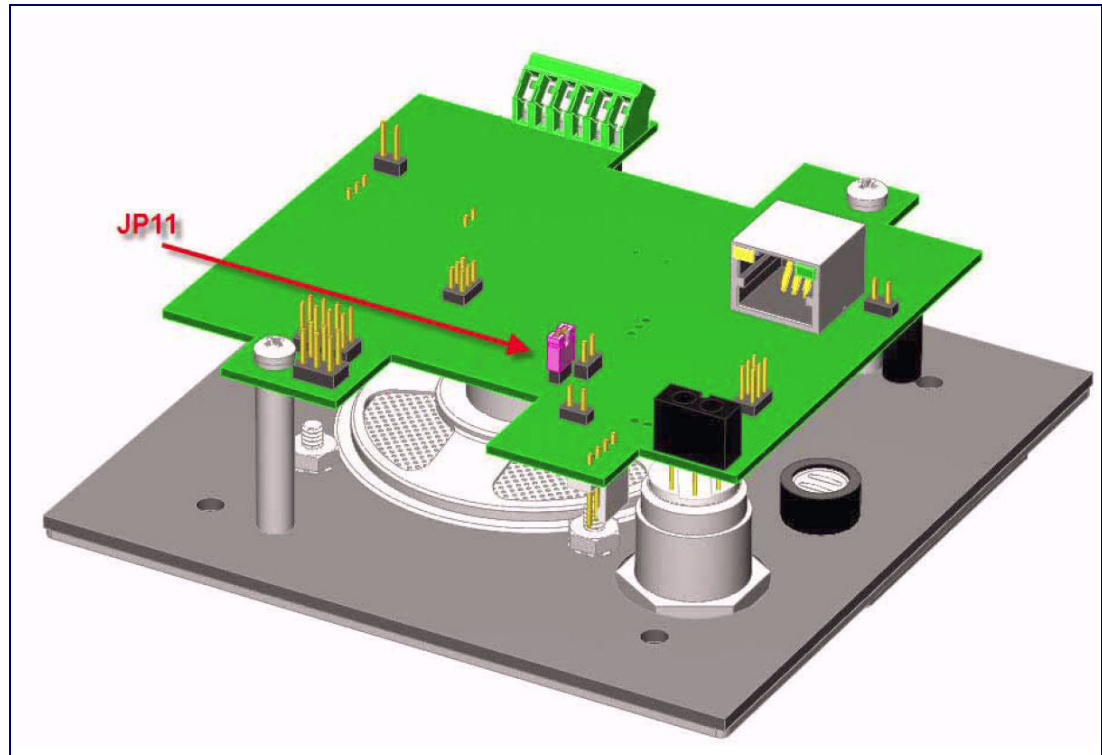
4. Release the Call Button and wait for the Intercom to reboot.

## 2.1.8.2 Intercom with a Jumper

Complete the following steps to restore defaults on an Intercom that has a jumper and no RTFM button:

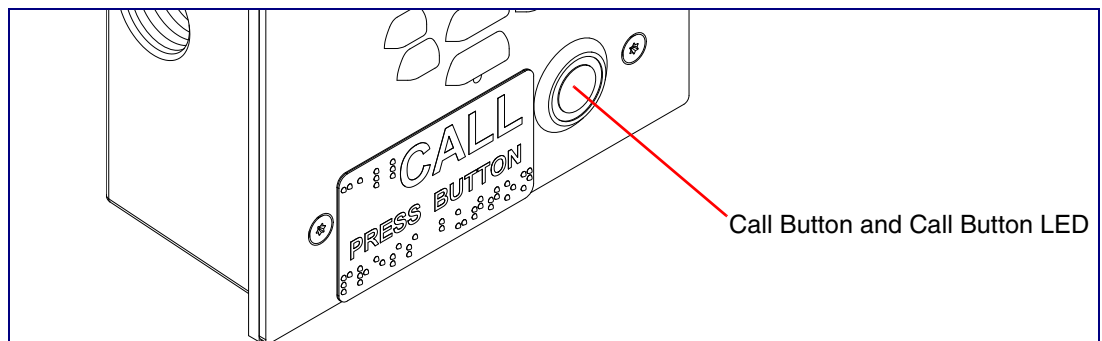
1. Put a jumper on JP11. See [Figure 2-14](#).

**Figure 2-14. Jumper on JP11**



2. Wait for the Intercom to announce the IP address.
3. Press and hold the Call Button (see [Figure 2-15](#)) until "**restoring defaults**" is announced.
4. Release the Call Button and wait for the Intercom to reboot.
5. Remove the jumper and cycle power by unplugging Intercom and plugging it back in.

**Figure 2-15. Call Button and Call Button LED**



---

## 2.1.9 Adjust the Volume

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

---

## 2.2 Configure the Intercom Parameters

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

Configure each Intercom and verify its operation *before* you mount it. When you are ready to mount an Intercom, refer to [Appendix A, "Mounting the Intercom"](#) for instructions.

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

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

**Table 2-4. Factory Default Settings**

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












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

---

## 2.2.1 Intercom Web Page Navigation

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

**Table 2-5. Web Page Navigation**

Web Page Item	Description
	Link to the <b>Home</b> page.
	Link to the <b>Device Configuration</b> page.
	Link to the <b>Networking</b> page.
	Link to go to the <b>SIP Configuration</b> page.
	Link to go to the <b>Nightringer</b> page.
	Link to the <b>Sensor Configuration</b> page.
	Link to the <b>Multicast Configuration</b> page.
	Link to the <b>Audio Configuration</b> page.
	Link to the <b>Event Configuration</b> page.
	Link to the <b>Autoprovisioning Configuration</b> page.
	Link to the <b>Update Firmware</b> page.



---

## 2.2.2 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](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 2-16):

Web Access Username: **admin**

Web Access Password: **admin**

Figure 2-16. Home Page

The screenshot shows the 'Home Page' of the CyberData Intercom configuration interface. The page has a blue header with the title 'CyberData Intercom'. On the left side, there is a vertical menu of buttons: Home, Device Config, Networking, SIP Config, Nightringer, Sensor Config, Multicast Config, Audio Config, Event Config, Autoprovisioning, and Update Firmware. The main content area is divided into two sections: 'Device Settings' and 'Current Settings'. The 'Device Settings' section contains fields for 'Device Name' (CyberData VoIP Intercom), 'Change Username' (admin), 'Change Password', and 'Re-enter Password'. The 'Current Settings' section displays various system parameters: Serial Number (113000017), Mac Address (00:20:f7:00:8f:e6), Firmware Version (v6.5.1), IP Addressing (dhcp), IP Address (10.10.1.110), Subnet Mask (255.0.0.0), Default Gateway (10.0.0.1), DNS Server 1 (10.0.0.1), DNS Server 2, Speaker Volume (4), and Microphone Gain (4). Below these are status indicators for SIP Mode (enabled), Multicast Mode (disabled), Event Reporting (disabled), Nightringer (disabled), and three SIP Servers (Primary, Backup 1, and Backup 2), all of which are currently '(NOT Registered with SIP Server)'. A note at the bottom states '\* You need to reboot for changes to take effect', followed by 'Save' and 'Reboot' buttons.

## CyberData Intercom

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

**Device Settings**

Device Name: CyberData VoIP Intercom

Change Username: admin

Change Password:

Re-enter Password:

**Current Settings**

Serial Number: 113000017  
Mac Address: 00:20:f7:00:8f:e6  
Firmware Version: v6.5.1

IP Addressing: dhcp  
IP Address: 10.10.1.110  
Subnet Mask: 255.0.0.0  
Default Gateway: 10.0.0.1  
DNS Server 1: 10.0.0.1  
DNS Server 2:

Speaker Volume: 4  
Microphone Gain: 4

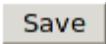
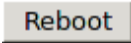
SIP Mode is: enabled  
Multicast Mode is: disabled  
Event Reporting is: disabled  
Nightringer is: disabled (NOT Registered with SIP Server)

Primary SIP Server: (NOT Registered with SIP Server)  
Backup Server 1: (NOT Registered with SIP Server)  
Backup Server 2: (NOT Registered with SIP Server)

\* You need to reboot for changes to take effect

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

**Table 2-6. Home Page Overview**

Web Page Item	Description
<b>Device Settings</b>	
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.
<b>Current Settings</b>	
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 ( <b>DHCP</b> or <b>static</b> ).
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 <b>Save</b> button to save your configuration settings. <b>Note:</b> You need to reboot for changes to take effect.
	Click on the <b>Reboot</b> button to reboot the system.

## 2.2.3 Configure the Device

1. Click the **Device Configuration** button to open the **Device Configuration** page. See [Figure 2-17](#).

Figure 2-17. Device Configuration Page

**CyberData 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:   
Volume Boost:

\* You need to reboot for changes to take effect

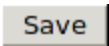
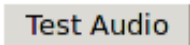
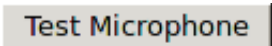
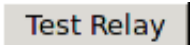
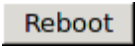
Save Test Audio Test Microphone Test Relay Reboot

2. On the **Device Configuration** page, you may enter values for the parameters indicated in [Table 2-7](#).

**Table 2-7. Device Configuration Parameters**

Web Page Item	Description
<b>Volume Settings</b>	
Speaker Volume	Type the desired Intercom volume level into this field.
Microphone Gain	Type the desired microphone gain level into this field.
<b>Relay Settings</b>	
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]). <b>NOTE:</b> A DTMF activation duration of <b>0</b> 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. <b>NOTE:</b> When the phone is set to <b>Auto Answer</b> , 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).
<b>Miscellaneous Settings</b>	
Auto-Answer Incoming Calls	When selected, the device will automatically answer incoming calls.  When <b>Auto Answer</b> 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 2-7. 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><b>NOTE:</b> When <b>Enable Push to Talk</b> 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><b>NOTE:</b> <b>Enable Push to Talk</b> will not work on some older hardware.</p>
Volume Boost	When <b>Volume Boost</b> is enabled, the device will play at a higher volume at the risk of having the audio clip at very high levels.
	Click the <b>Save</b> button to save your configuration settings. <b>Note:</b> You need to reboot for changes to take effect.
	Click on the <b>Test Audio</b> button to do an audio test. When the <b>Test Audio</b> button is pressed, you will hear a voice message for testing the device audio quality and volume.
	Click on the <b>Test Relay</b> button to do a relay test.
	Click on the <b>Test Microphone</b> button to do a microphone test. When the <b>Test Microphone</b> button is pressed, the following occurs: <ol style="list-style-type: none"> <li>1. The device will immediately start recording 3 seconds of audio.</li> <li>2. The device will beep (indicating the end of recording).</li> <li>3. The device will play back the recorded audio.</li> </ol>
	Click on the <b>Reboot</b> button to reboot the system.

**Note** You can change the **Speaker Volume** and **Microphone Gain** without rebooting the device. You must save and reboot the device for other changes to take effect.

## 2.2.4 Configure the Network Parameters

1. Click the **Networking** button to open the **Network Configuration** page (Figure 2-18).

Figure 2-18. Network Configuration Page

**CyberData 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

VLAN ID (0-4095): 0

VLAN Priority (0-7): 0

DHCP Timeout

DHCP Timeout in seconds\*: 60

\* A value of -1 will retry forever

Current Network Settings

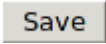
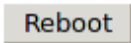
IP Address: 10.10.1.110  
Subnet Mask: 255.0.0.0  
Default Gateway: 10.0.0.1  
DNS Server 1: 10.0.0.1  
DNS Server 2:

\* 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 2-8](#).

**Table 2-8. Network Configuration Parameters**

Web Page Item	Description
<b>Stored Network Settings</b>	
IP Addressing	Select either <b>DHCP IP Addressing</b> or <b>Static IP Addressing</b> by marking the appropriate radio button. If you select <b>Static</b> , configure the remaining parameters indicated in <a href="#">Table 2-8</a> . If you select <b>DHCP</b> , go to <a href="#">Step 3</a> .
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.
VLAN ID (0-4095)	Enter the VLAN ID number.  <b>Note:</b> The device supports 802.11Q VLAN tagging support. The switch port connected to the device will need to be in “trunking mode” for the VLAN tags to propagate.
VLAN Priority (0-7)	Enter the VLAN priority number.
<b>DHCP Timeout</b>	
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.  <b>Note:</b> A value of <b>-1</b> will cause the device to retry indefinitely and a value of <b>0</b> will cause the device to reset to a default of 60 seconds.
<b>Current Network Settings</b>	
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 <b>Save</b> button to save your configuration settings.  <b>Note:</b> You need to reboot for changes to take effect.
	Click on the <b>Reboot</b> button to reboot the system.

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



## 2.2.5 Configure the SIP Parameters

1. Click **SIP Config** to open the **SIP Configuration** page (Figure 2-19).

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

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

**Figure 2-19. SIP Configuration Page**

**CyberData Intercom**

**SIP Configuration**

Enable SIP operation:  (NOT Registered with SIP Server)

**SIP Settings**

SIP Server: 10.0.0.253

Backup SIP Server 1:

Backup SIP Server 2:

Use Cisco SRST:

Remote SIP Port: 5060

Local SIP Port: 5060

Outbound Proxy:

Outbound Proxy Port: 0

SIP User ID: 199

Authenticate ID: 199

Authenticate Password: ●●●●●●

Register with a SIP Server:

Re-registration Interval (in seconds): 360

Unregister on Reboot:

Disable rport Discovery:

**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: 204

Extension ID: id204

\* You need to reboot for changes to take effect

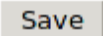
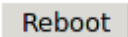
Save Reboot

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

**Table 2-9. SIP Configuration Parameters**

Web Page Item	Description
Enable SIP Operation	Enables or disables SIP operation.
<b>SIP Settings</b>	
SIP Server	Use this field to set the address (in dotted decimal notation or as a canonical name) of the SIP registrar. This field can accept canonical names of up to 255 characters in length.
Backup SIP Server 1 Backup SIP Server 2	<p>When the primary SIP Server goes offline and the device fails to register after the normal re-registration interval, the controller will fall back to using Backup SIP Server 1.</p> <p>If Backup SIP Server 1 fails, the device will use Backup SIP Server 2.</p> <p>If a higher priority SIP Server comes back online, the device will switch back to this server.</p> <p>You can leave the <b>Backup SIP Server 1</b> and <b>Backup SIP Server 2</b> fields blank.</p>
Use Cisco SRST	When selected, the backup servers are handled according to Cisco SRST (Survivable Remote Site Telephony).
Remote SIP Port	Type the <b>Remote SIP Port</b> number (default 5060) (8 character limit).
Local SIP Port	Type the <b>Local SIP Port</b> 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).
SIP User ID	Type the <b>SIP User ID</b> (up to 64 alphanumeric characters).
Authenticate ID	Type the <b>Authenticate ID</b> (up to 64 alphanumeric characters).
Authenticate Password	Type the <b>Authenticate Password</b> (up to 64 alphanumeric characters).
Register with a SIP Server	<p>Check this box to enable SIP Registration.</p> <p>For information about Point-to-Point Configuration, see <a href="#">Section 2.2.5.2, "Point-to-Point Configuration"</a>.</p>
Re-registration Interval (in seconds)	The SIP Registration lease time in seconds.
Unregister on Reboot	When selected, on boot, the device will first register with a SIP server with a expiration delay of 0 seconds. This has the effect of unregistering any current devices on this extension.
Disable rport discovery	When selected, the device is prevented from including the public WAN IP address in the contact information sent to remote SIP servers. This setting will generally only need to be enabled when using an SBC in conjunction with a remote SIP server.

**Table 2-9. SIP Configuration Parameters (continued)**

Web Page Item	Description
<b>Call Disconnection</b>	
Terminate call after delay (in seconds)	Type the desired number of seconds that you want to transpire before a call is terminated.  Note: A value of <b>0</b> will disable this function.
<b>RTP Settings</b>	
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.
<b>Dial Out Settings</b>	
Dial Out Extension	Type the dial out extension number (64 character limit).  <b>Note:</b> For information about dial-out extension strings and DTMF tones, see <a href="#">Section 2.2.5.1, "Dial Out Extension Strings and DTMF Tones (using rfc2833)"</a> .
Extension ID	Type the desired Extension ID (64 character limit).
	Click the <b>Save</b> button to save your configuration settings.  <b>Note:</b> You need to reboot for changes to take effect.
	Click on the <b>Reboot</b> button to reboot the system.

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

### 2.2.5.1 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 2-10. 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.

## 2.2.5.2 Point-to-Point Configuration

When the board is set to not register with a SIP server (see [Figure 2-20](#)), 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 2-20. SIP Configuration Page Set to Point-to-Point Mode**

Intercom is set to NOT register with a SIP server

### 2.2.5.3 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 2-11. Examples of Dial-Out Extension Strings**

<b>Extension String</b>	<b>Resulting Action</b>
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.

## 2.2.6 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.

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

**Figure 2-21. Nightringer Configuration Setup**

**CyberData 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
Outbound Proxy:	
Outbound Proxy Port:	0
User ID:	241
Authenticate ID:	241
Authenticate Password:	●●●●●●

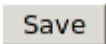
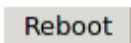
Re-registration Interval (in seconds): 360

\* 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 2-12](#).

**Table 2-12. 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.
<b>Nightringer Settings</b>	
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). <b>Note:</b> This value cannot be the same as the <a href="#">Local SIP Port</a> found on the <a href="#">SIP Configuration Page</a> .
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 (5 character limit [values from 1 to 65535]).
User ID	Type the <b>User ID</b> (up to 64 alphanumeric characters).
Authenticate ID	Type the <b>Authenticate ID</b> (up to 64 alphanumeric characters).
Authenticate Password	Type the <b>Authenticate Password</b> (up to 64 alphanumeric characters).
Re-registration Interval (in seconds)	The SIP Registration lease time in seconds.
	Click the <b>Save</b> button to save your configuration settings. <b>Note:</b> You need to reboot for changes to take effect.
	Click on the <b>Reboot</b> button to reboot the system.

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

---

## 2.2.7 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.

Each sensor can trigger up to five different actions:

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

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



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

Figure 2-22. Sensor Configuration Page

**CyberData 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:


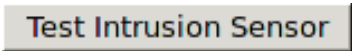
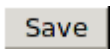
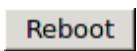
**Intrusion Sensor Settings**

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 2-13](#).

**Table 2-13. Sensor Configuration Parameters**

Web Page Item	Description
<b>Door Sensor Settings</b>	
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.
<b>Intrusion Sensor Settings</b>	
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 <b>Save</b> button to save your configuration settings. <b>Note:</b> You need to reboot for changes to take effect.
	Click on the <b>Reboot</b> button to reboot the system.

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

## 2.2.8 Configure the Multicast Parameters

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

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

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

1. Click on the **Multicast Configuration** button to open the **Multicast Configuration** page. See [Figure 2-23](#).

**Figure 2-23. Multicast Configuration Page**

**CyberData Intercom**

**Multicast Configuration**

Enable Multicast operation:

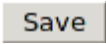
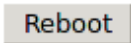
Priority	Address	Port	Name	Beep
9	239.168.3.10	11000	Emergency	<input type="checkbox"/>
8	239.168.3.9	10000	MG8	<input type="checkbox"/>
7	239.168.3.8	9000	MG7	<input type="checkbox"/>
6	239.168.3.7	8000	MG6	<input type="checkbox"/>
5	239.168.3.6	7000	MG5	<input type="checkbox"/>
SIP calls are considered priority 4.5				
4	239.168.3.5	6000	MG4	<input type="checkbox"/>
3	239.168.3.4	5000	MG3	<input type="checkbox"/>
2	239.168.3.3	4000	MG2	<input type="checkbox"/>
1	239.168.3.2	3000	MG1	<input type="checkbox"/>
0	239.168.3.1	2000	Background Music	<input type="checkbox"/>

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

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

**Table 2-14. Multicast Configuration Parameters**

Web Page Item	Description
Enable Multicast Operation	Enables or disables multicast operation.
<b>Device Settings</b>	
Priority	Indicates the priority for the multicast group. Priority <b>9</b> is the highest (emergency streams). <b>0</b> is the lowest (background music). SIP calls are considered priority <b>4.5</b> . See <a href="#">Section 2.2.8.1, "Assigning Priority"</a> 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).  <b>Note:</b> The multicast ports have to be even values. The webpage will enforce this restriction.
Name	Assign a descriptive name for this multicast group (25 character limit).
Beep	When selected, the device will play a beep before multicast audio is sent.
	Click the <b>Save</b> button to save your configuration settings.  <b>Note:</b> You need to reboot for changes to take effect.
	Click on the <b>Reboot</b> button to reboot the system.

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

### 2.2.8.1 Assigning Priority

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

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

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

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

Ringtones and  
Nightringtones

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

## 2.2.9 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 2-24).

Figure 2-24. Audio Configuration Page

The screenshot displays the 'Audio Configuration' page for CyberData Intercom. The page features a blue header with the product name and a left-hand navigation menu. The main content area shows the current audio configuration status, including available space and a list of audio files. Each file entry includes a 'New File:' field with a 'Browse...' button and 'Play', 'Delete', and 'Save' controls.

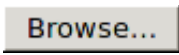


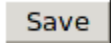
Figure 2-25. Audio Configuration Page (continued)

The screenshot displays a series of audio configuration options, each with a label, a status indicator, a file input field, and control buttons. The options are:

- 9:** Currently set to default. New File: [input field] Browse... [Play] [Delete] [Save]
- Dot:** Currently set to default. New File: [input field] Browse... [Play] [Delete] [Save]
- Audio test:** Currently set to default. New File: [input field] Browse... [Play] [Delete] [Save]
- Page tone:** Currently set to default. New File: [input field] Browse... [Play] [Delete] [Save]
- Your IP Address Is:** Currently set to default. New File: [input field] Browse... [Play] [Delete] [Save]
- Rebooting:** Currently set to default. New File: [input field] Browse... [Play] [Delete] [Save]
- Restoring Default:** Currently set to default. New File: [input field] Browse... [Play] [Delete] [Save]
- Ringback tone:** Currently set to default. New File: [input field] Browse... [Play] [Delete] [Save]
- Ring tone:** Currently set to default. New File: [input field] Browse... [Play] [Delete] [Save]
- Intrusion Sensor Triggered:** Currently set to default. New File: [input field] Browse... [Play] [Delete] [Save]
- Door Ajar:** Currently set to default. New File: [input field] Browse... [Play] [Delete] [Save]
- Night Ring:** Currently set to default. New File: [input field] Browse... [Play] [Delete] [Save]

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

**Table 2-15. Audio Configuration Parameters**

Web Page Item	Description
<b>Audio Files</b>	
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 <b><i>"This is the CyberData IP speaker test message..."</i></b> (24 character limit)
Pagetone	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 <b>Ring Tone</b> parameter.
	The <b>Browse</b> button will allow you to navigate to and select an audio file.
	The <b>Play</b> button will play that audio file.
	The <b>Delete</b> button will delete any user uploaded audio and restore the stock audio file.
	The <b>Save</b> button will download a new user audio file to the board once you've selected the file by using the <b>Browse</b> button. The <b>Save</b> button will delete any pre-existing user-uploaded audio files.

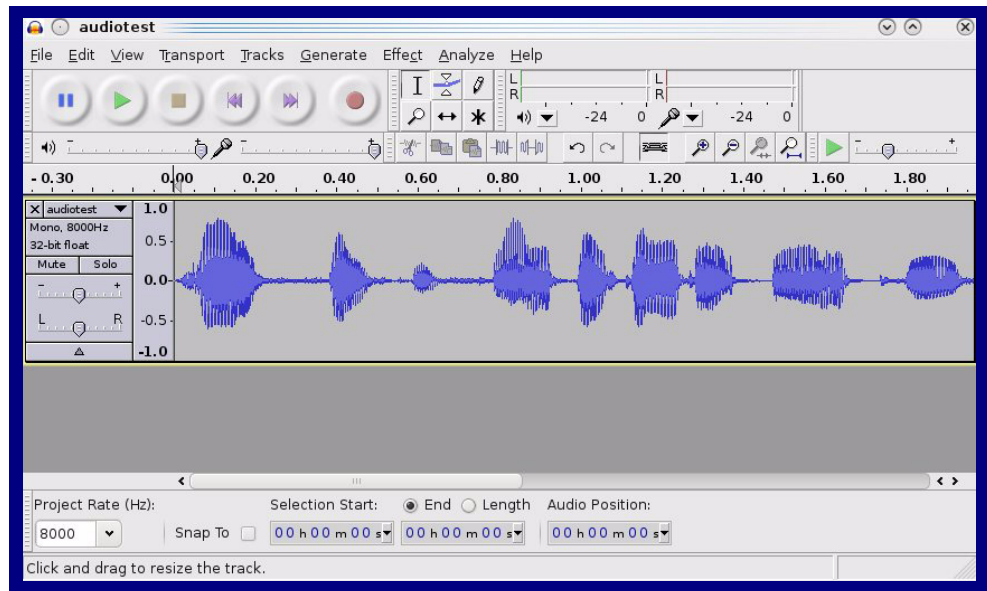
### 2.2.9.1 User-created Audio Files

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

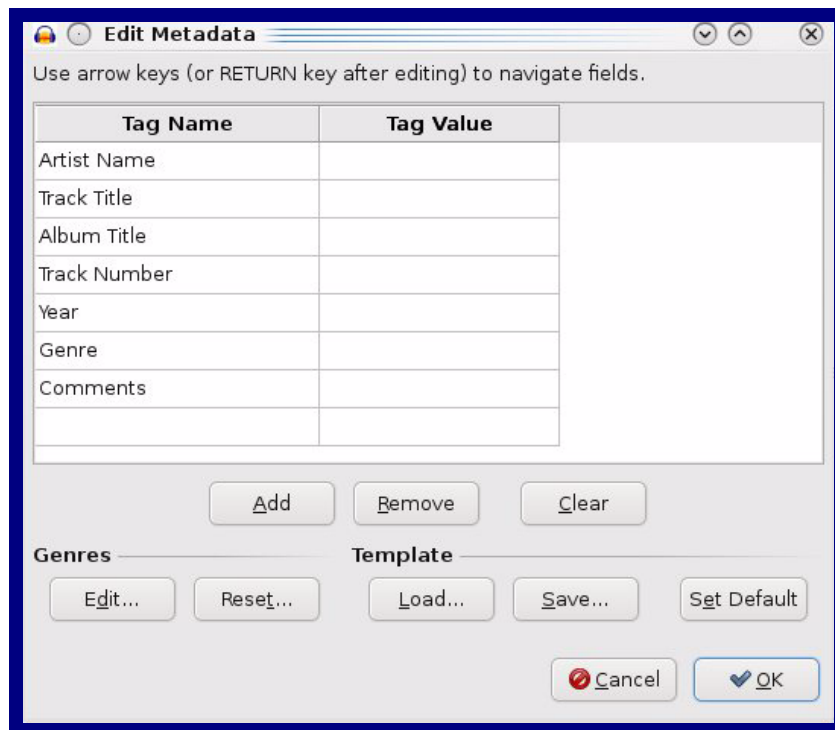
RIFF (little-endian) data, WAVE audio, Microsoft PCM, 16 bit, mono 8000 Hz

You can use the free utility *Audacity* to convert audio files into this format. See [Figure 2-26](#) through [Figure 2-28](#).

**Figure 2-26. Audacity 1**



**Figure 2-27. Audacity 2**

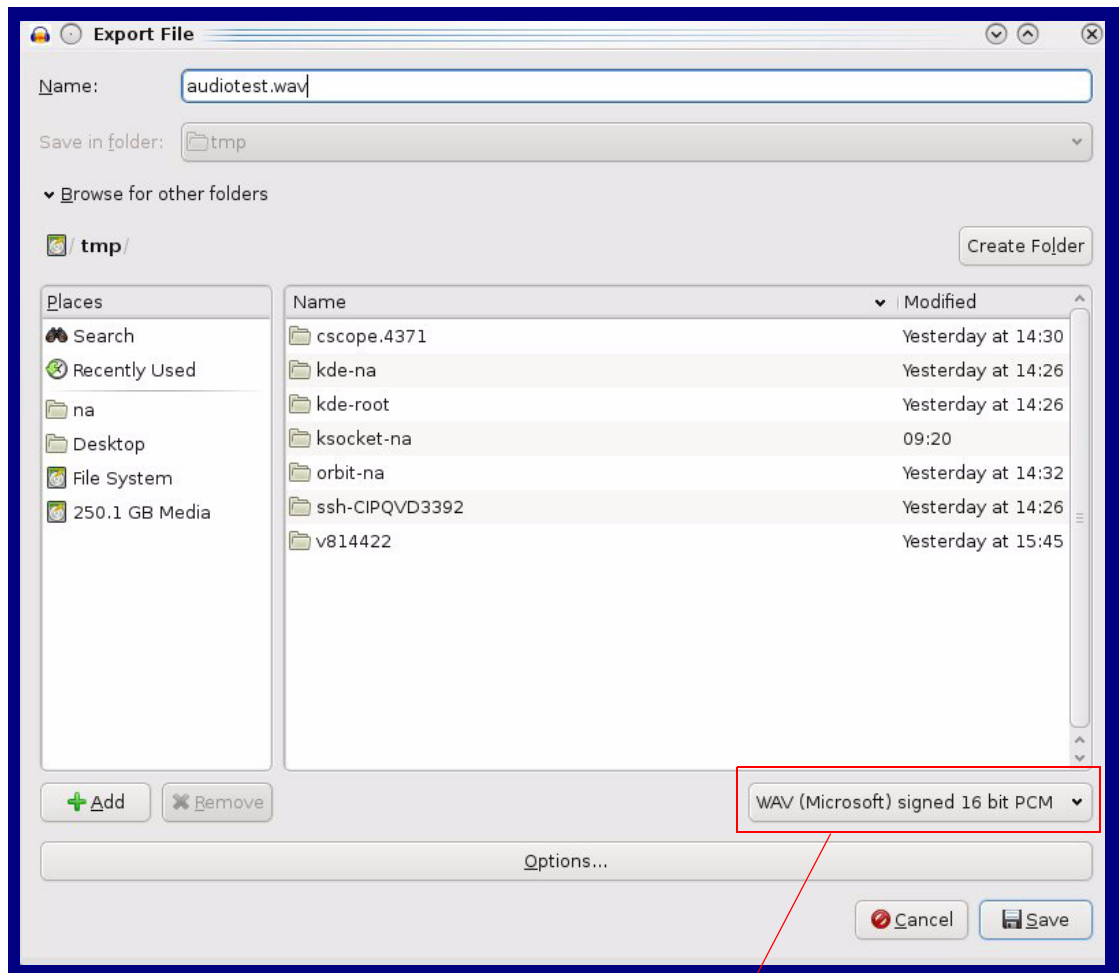




When you export an audio file with Audacity, save the output as:

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

**Figure 2-28. WAV (Microsoft) signed 16 bit PCM**



WAV (Microsoft) signed 16 bit PCM

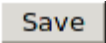
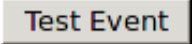
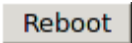
## 2.2.10 Configure the Event Parameters

Click the **Event Config** button to open the **Event Configuration** page (Figure 2-29). 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 2-29. Event Configuration Page

Table 2-16 shows the web page items on the **Event Configuration** page.

**Table 2-16. Event Configuration**

<b>Web Page Item</b>	<b>Description</b>
Enable Event Generation	When selected, Event Generation is enabled.
<b>Remote Event Server</b>	
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)
<b>Events</b>	
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 Door Sensor Events	When selected, Door Sensor Events are enabled.
Enable Intrusion Sensor Events	When selected, Intrusion Sensor Events are enabled.
Enable 60 Second Heartbeat Events	When selected, 60 Second Heartbeat Events are enabled.
	Click the <b>Save</b> button to save your configuration settings. <b>Note:</b> You need to reboot for changes to take effect.
	Click on the <b>Test Event</b> button to test an event.
	Click on the <b>Reboot</b> button to reboot the system.

## 2.2.10.1 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>
```

## 2.2.11 Configure the Autoprovisioning Parameters

Autoprovisioning can be used to configure your device automatically on boot, after a periodic delay, after sitting idle for a period of time, or at a specified time.

The autoprovisioning file contains the board configuration in xml format. Autoprovisioned values in this file will override values stored in on-board memory.

The autoprovisioning file can be hosted with a tftp or a web server and by default is named according to the MAC address of the device (for example: 0020f7350058.config). The autoprovisioning filename can also be specified.

The device does not have a real time clock but can sync with a network time server on boot.

1. Click the **Autoprovisioning** button to open the **Autoprovisioning Configuration** page. See [Figure 2-30](#).

**Figure 2-30. Autoprovisioning Configuration Page**

**CyberData Intercom**

**Autoprovisioning**

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

**Autoprovisioning**

Enable Autoprovisioning:

Get Autoprovisioning from DHCP:

Download Protocol:  HTTP  TFTP

Autoprovisioning Server (IP Address): 10.0.0.254

Autoprovisioning Filename: \_\_\_\_\_

Autoprovisioning autoupdate (in minutes): 0

Autoprovision at time (HHMMSS): \_\_\_\_\_

Autoprovision when idle (in minutes > 10): 0

**Clock**

NTP Server: north-america.pool.ntp.org

Posix Timezone String (see manual): PST8PDT,M3.2.0/2:00:00,M11.1.0/2:00:01

Set Time with external NTP server on boot:

Periodically update with time server:

Time update period (in hours): 24

**Set time from NTP Server**

**Current Time**

Current Time in 24 hour format (HHMMSS): 180015

**Set Time**

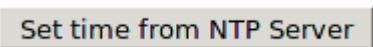
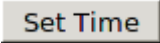
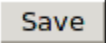
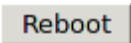
\* Autoprovisioning file name: 0020f7008fe6.config

\* You need to reboot for changes to take effect

**Save** **Reboot**

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

**Table 2-17. Autoprovisioning Configuration Parameters**

Web Page Item	Description
<b>Autoprovisioning</b>	
Enable Autoprovisioning	See <a href="#">Section 2.2.11.1, "Autoprovisioning"</a> .
Get Autoprovisioning from DHCP	See <a href="#">Section 2.2.11.1, "Autoprovisioning"</a> .
Download Protocol	Allows you to select whether the autoprovisioning file is acquired via <b>TFTP</b> or <b>HTTP</b> .
Autoprovisioning Server (IP Address)	See <a href="#">Section 2.2.11.1, "Autoprovisioning"</a> (15 character limit).
Autoprovisioning Filename	Type the desired name for the autoprovisioning file.
Autoprovisioning Autoupdate (in minutes)	Type the desired time (in minutes) that you want the Autoprovisioning feature to update (6 character limit). <b>Note:</b> A value of <b>0</b> will disable this option.
Autoprovision at time (HHMMSS)	Type the desired time of day that you want the Autoprovisioning feature to update (must be 6 characters). <b>Note:</b> An empty value will disable this option.
Autoprovision when idle (in minutes > 10)	Type the desired time (in minutes greater than 10) that you want the Autoprovisioning feature to update after a certain amount of idle time (6 character limit). <b>Note:</b> A value of <b>0</b> will disable this option.
<b>Clock</b>	
NTP Server	Allows you to select the NTP server (64 character limit).
Posix Timezone String	See <a href="#">Section 2.2.11.2, "Time Zone Strings"</a> (43 character limit).
Set Time with External NTP Server on boot	When selected, the time is set with an external NTP server when the device restarts.
Periodically update with time server	When selected, the time is periodically updated with a time server.
Time update period (in hours)	Allows you to select the time updated period (in hours) (4 character limit).
	Allows you to set the time from the NTP server.
<b>Current Time</b>	
Current Time (UTC) in 24 hour format (HHMMSS)	Allows you to input the current time in the 24 hour format. (6 character limit)
	Click on this button to set the clock after entering the current time.
	Click the <b>Save</b> button to save your configuration settings. <b>Note:</b> You need to reboot for changes to take effect.
	Click on the <b>Reboot</b> button to reboot the system.

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



### 2.2.11.1 Autoprovisioning

Autoprovisioning File 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>
```

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** When the device is set to autoprovision either after a period of time, or when idle, or at a time of day, the device will do the following:

- Re-download the autoprovisioning file.
- Compare this new file to the one downloaded on boot, and if it finds differences, force a system reset.
- After rebooting, the board will configure itself according to this new file.

**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>v6.5.1</FirmwareVersion>
<FirmwareFile>651-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 **Restore Default** on the **Audio Configuration** page or by changing the autoprovisioning file with “**default**” set as the file name.

## 2.2.11.2 Time Zone Strings

The posix time zone string tells the internal date and time utilities how to handle daylight savings time for different time zones. [Table 2-18](#) shows some common strings.

**Table 2-18. Common Time Zone Strings**

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

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

[Table 2-19](#) shows a breakdown of the parts that constitute the following time zone string:

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

**Table 2-19. Time Zone String Parts**

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

Time Zone String Examples **Table 2-20** has some more examples of time zone strings.

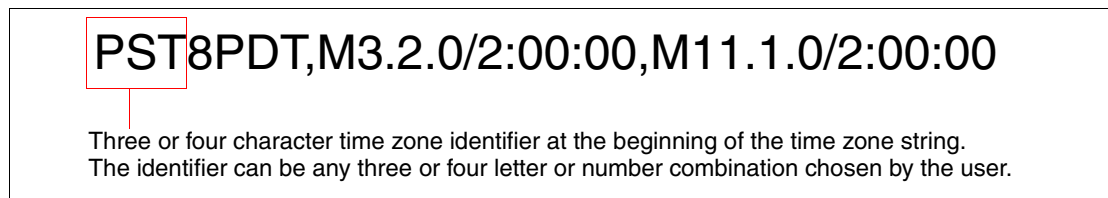
**Table 2-20. Time Zone String Examples**

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

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

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

**Figure 2-31. Three or Four Character Time Zone Identifier**



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

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

World GMT Table **Table 2-21** has information about the GMT time in various time zones.

**Table 2-21. World GMT Table**

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

**Table 2-21. World GMT Table (continued)**

<b>Time Zone</b>	<b>City or Area Zone Crosses</b>
GMT+1	Berlin, Rome
GMT+2	Israel, Cairo
GMT+3	Moscow, Kuwait
GMT+4	Abu Dhabi, Muscat
GMT+5	Islamabad, Karachi
GMT+6	Almaty, Dhaka
GMT+7	Bangkok, Jakarta
GMT+8	Hong Kong, Beijing
GMT+9	Tokyo, Osaka
GMT+10	Sydney, Melbourne, Guam
GMT+11	Magadan, Soloman Is.
GMT+12	Fiji, Wellington, Auckland

---

## 2.3 Upgrade the Firmware and Reboot the Intercom

**Note** To guard against failed firmware upgrades, units shipped from CyberData with firmware version 5.1.2 and later feature a built-in "fail safe" mechanism. Note that field upgrading earlier units with v5.x.x will not allow for this feature.

**Note** Any units that have shipped with firmware version 6.0.0 or later will not be able to run firmware that is version 5.1.2 or earlier.



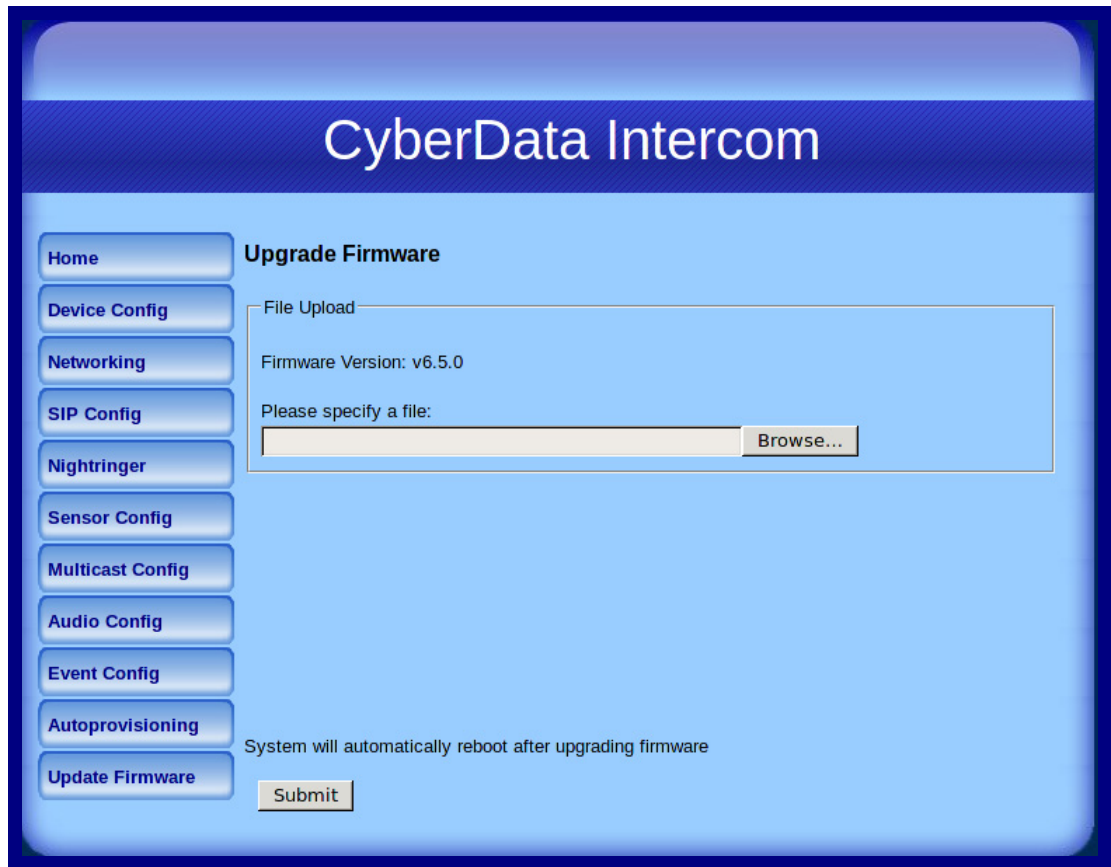
### Caution

When upgrading to firmware version 6.x.x from version 5.x.x or earlier, your device configuration settings will be lost because the way that the device stores the configuration settings is different in version 6.x.x.

To upload the firmware from your computer:

1. Retrieve the latest Intercom firmware file from the VoIP Intercom **Downloads** page at:  
<http://www.cyberdata.net/products/voip/digitalanalog/intercom/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 2.2.2, "Log in to the Configuration Home Page"](#).
4. Click the **Update Firmware** button to open the **Upgrade Firmware** page. See [Figure 2-32](#).

Figure 2-32. Upgrade Firmware Page

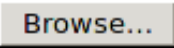
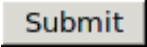


5. Select **Browse**, and then navigate to the location of the Intercom firmware file.
6. Click **Submit**.

**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 2-22 shows the web page items on the **Upgrade Firmware** page.

Table 2-22. Firmware Upgrade Parameters

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

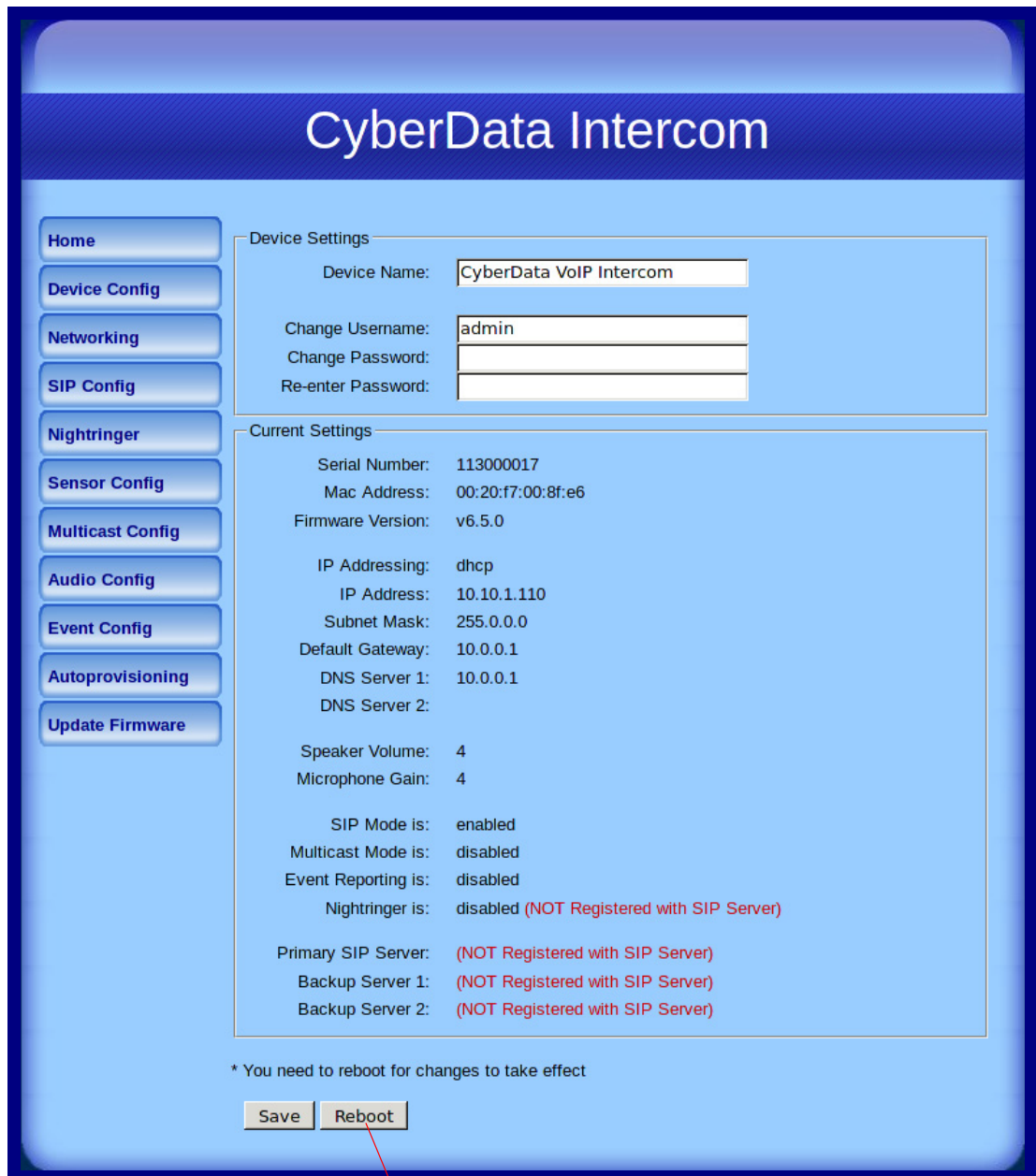


## 2.3.1 Reboot the Intercom

To reboot a Intercom, log in to the web page as instructed in [Section 2.2.2, "Log in to the Configuration Home Page"](#).

1. Click **Reboot** ([Figure 2-33](#)). A normal restart will occur.

**Figure 2-33. Reboot System Section**



Reboot

## 2.4 Command Interface

Some functions on the device can be activated using simple POST commands to the web interface. The examples in [Table 2-23](#) use the free unix utility, **wget commands**. However, any program that can send HTTP POST commands to the device should work.

### 2.4.1 Command Interface Post Commands

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

**Table 2-23. Command Interface Post Commands**

Device Action	HTTP Post Command <sup>a</sup>
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 <sup>b</sup> (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 2-23. Command Interface Post Commands (continued)**

<b>Device Action</b>	<b>HTTP Post Command<sup>a</sup></b>
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 2-23. Command Interface Post Commands (continued)**

<b>Device Action</b>	<b>HTTP Post Command<sup>a</sup></b>
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 2-23. Command Interface Post Commands (continued)**

<b>Device Action</b>	<b>HTTP Post Command<sup>a</sup></b>
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 2-23. Command Interface Post Commands (continued)**

<b>Device Action</b>	<b>HTTP Post Command<sup>a</sup></b>
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 2-23. Command Interface Post Commands (continued)**

Device Action	HTTP Post Command <sup>a</sup>
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.

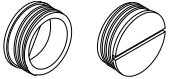
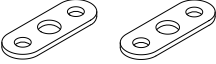




b. Must be in point-to-point mode see [Section 2.2.5.2, "Point-to-Point Configuration"](#)

# Appendix A: Mounting the Intercom

## A.1 Mount the Intercom

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

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

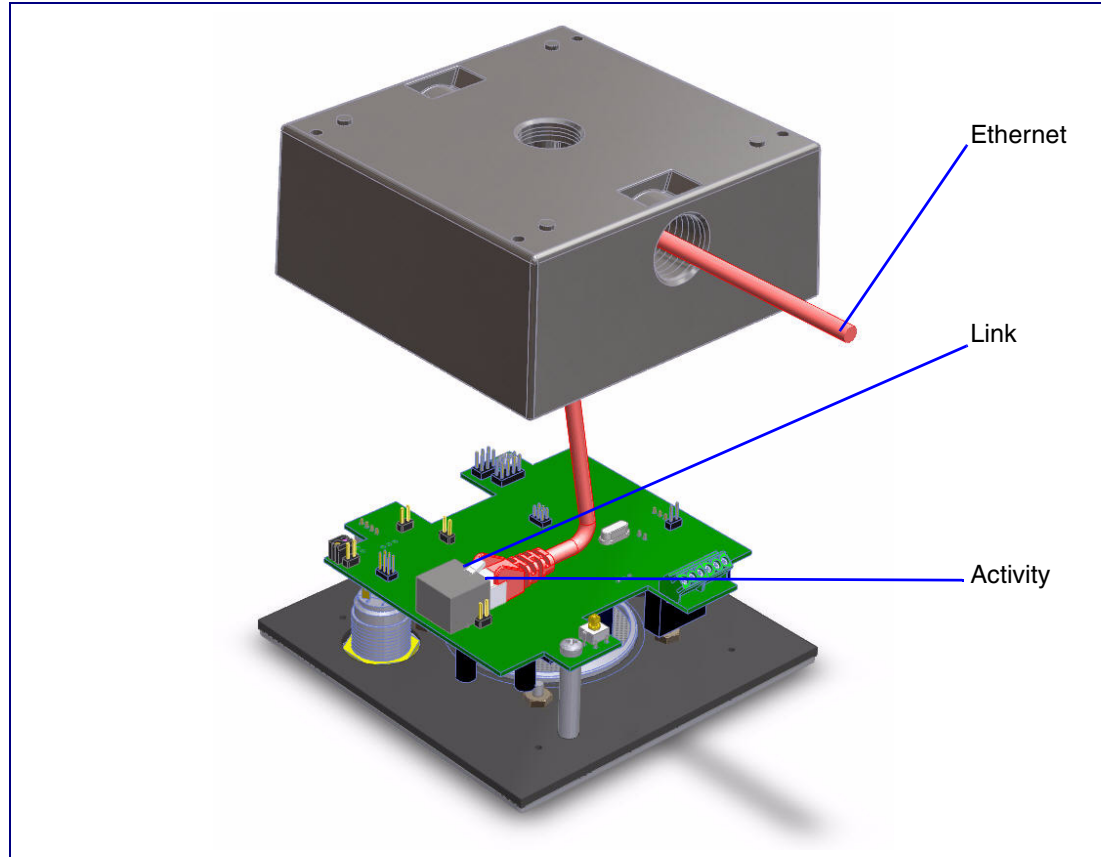
Quantity	Part Name	Illustration
2	Outlet Box Plugs	
2	Flush Mounting Plate	
2	8-32 x 1/4" Flat Head Phillips Machine Screw	
1	10-24 x 5/16" Pan Head Phillips Machine Screw	
1	T-15H Torx Key	
4	Security Torx Screw	



To mount the Intercom:

1. Plug the Ethernet cable into the Intercom Assembly (see [Figure A-1](#)). [Section 2.1.5, "Network Connectivity, and Data Rate"](#) explains how the **Link** and **Status** LEDs work.

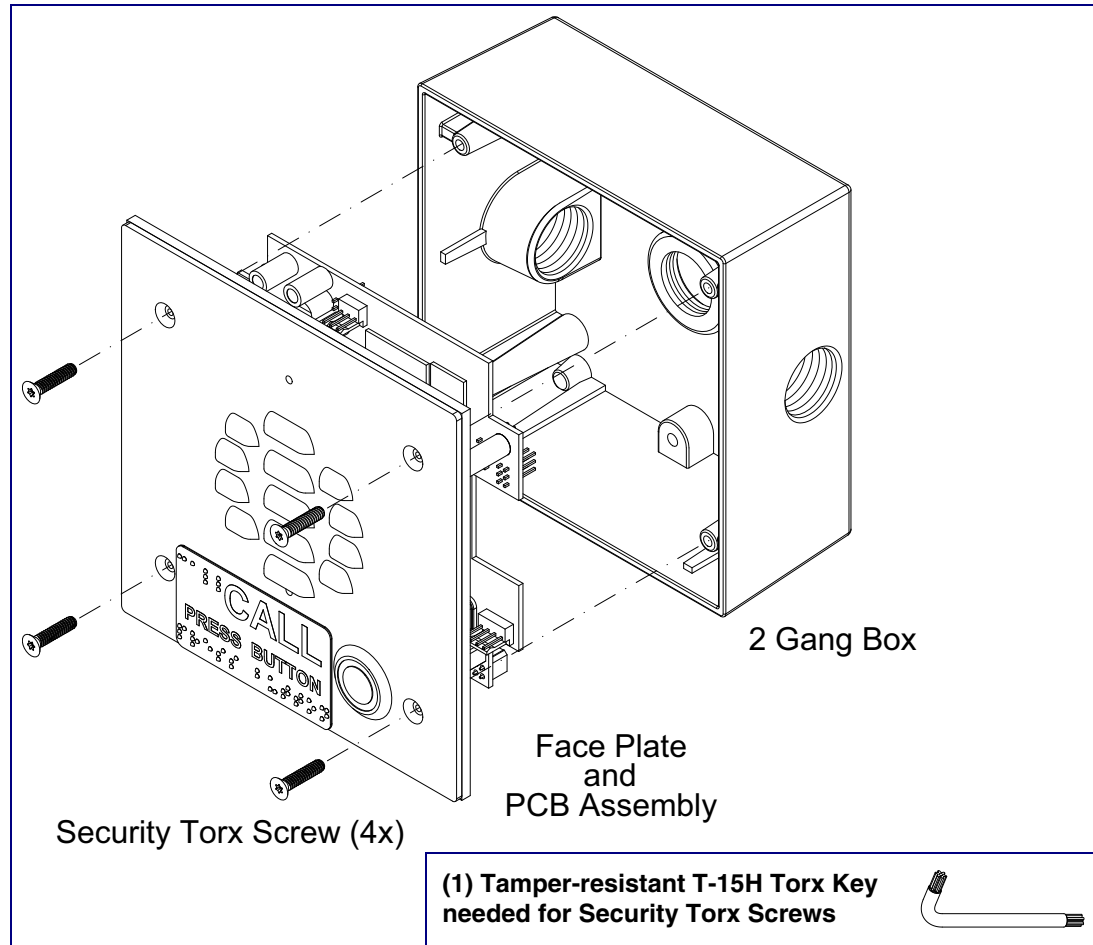
**Figure A-1. Network Connector Prior to Installation**



2. To fasten the Intercom:

- For wall mounting, use the two **8-32 X 1/4" FLAT HEAD PHILLIPS MACHINE SCREW** and the one **10-24 X 5/16" PAN HEAD PHILLIPS MACHINE SCREW** to secure the Intercom.

Figure A-2. VoIP Intercom Assembly



**Caution**

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

If the thread on the conduit is longer than 3/8 inch, then a **stop nut** (not supplied) is required. Otherwise, use the **outlet box plug** to plug the exit hole.

**Note** Apply good quality waterproof sealant to all threads.

**Figure A-3. Mounting the VoIP Intercom Assembly**

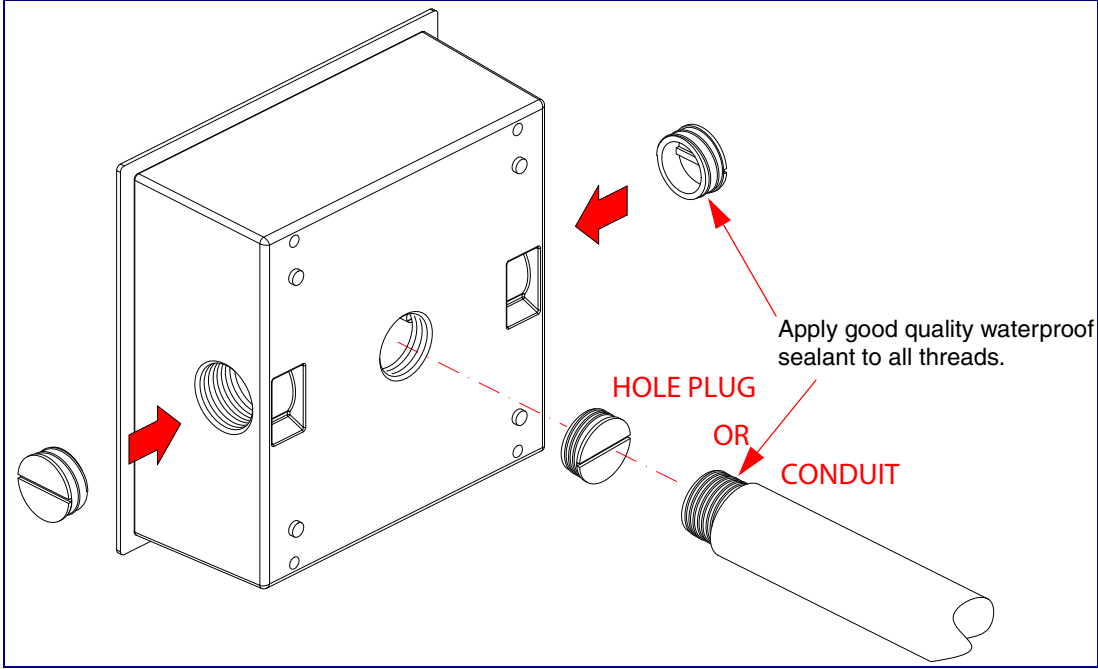


Figure A-4 shows the restrictions of the conduit going into the box.

**Figure A-4. Conduit Restrictions**

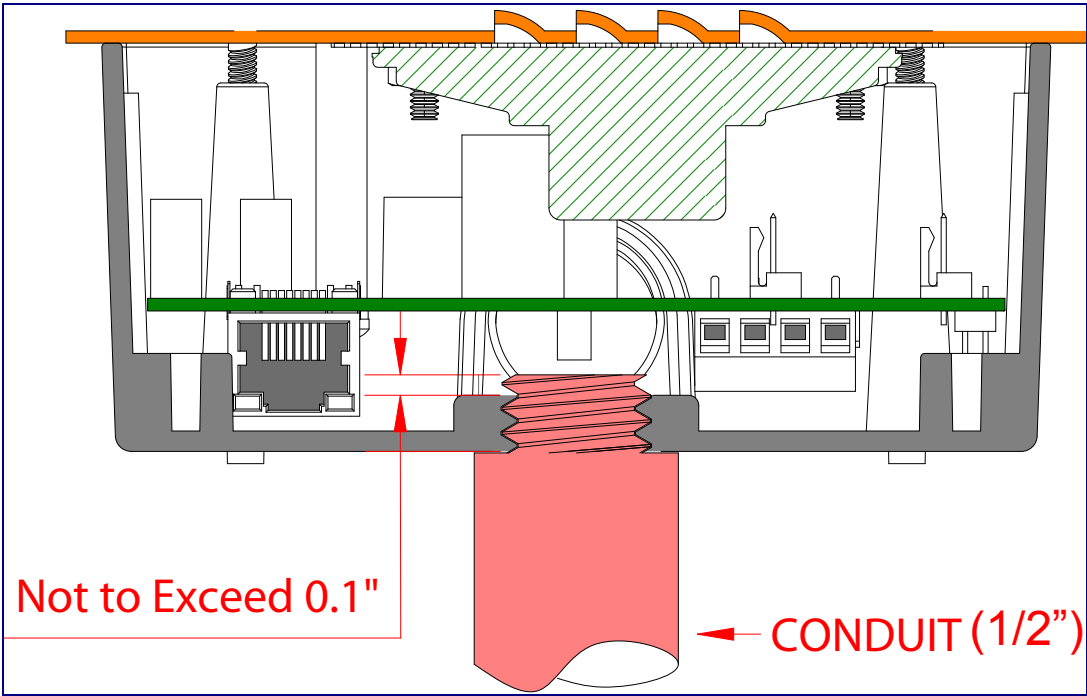
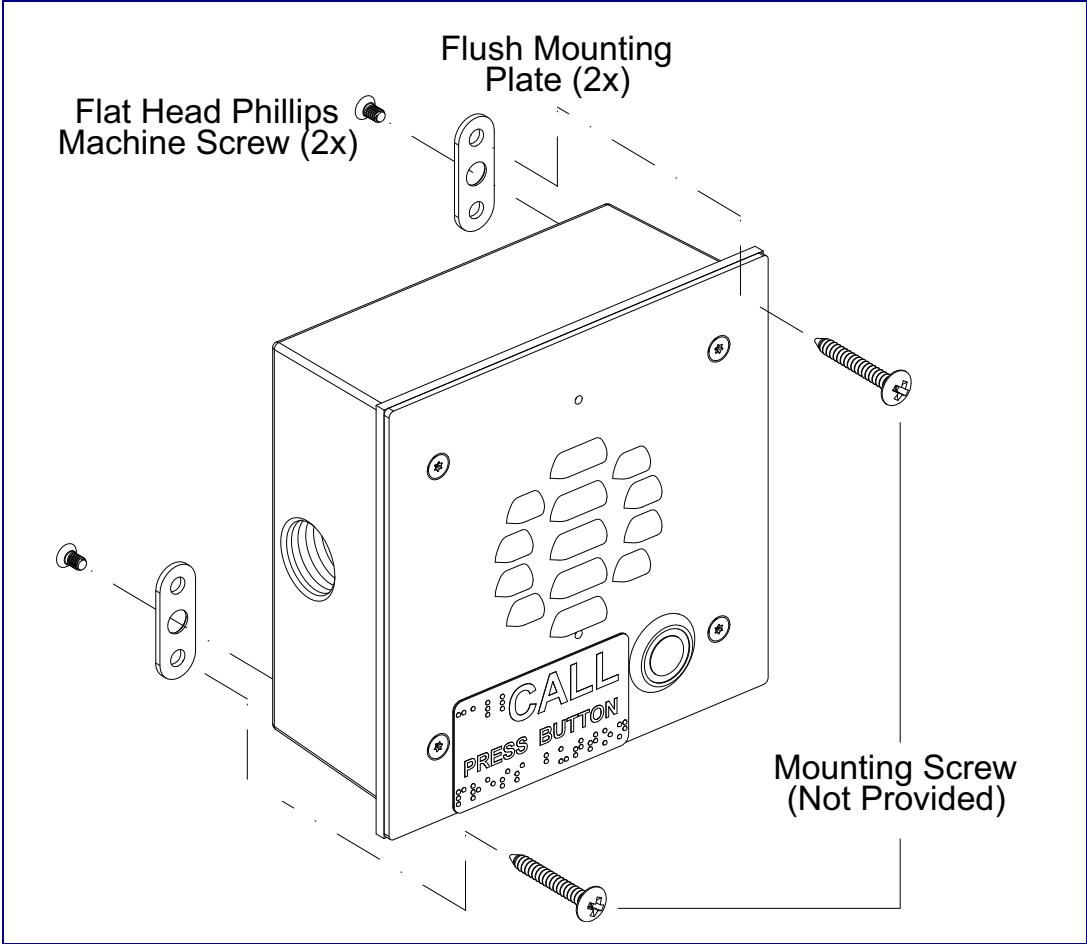


Figure A-5 shows how to properly mount the VoIP Intercom.

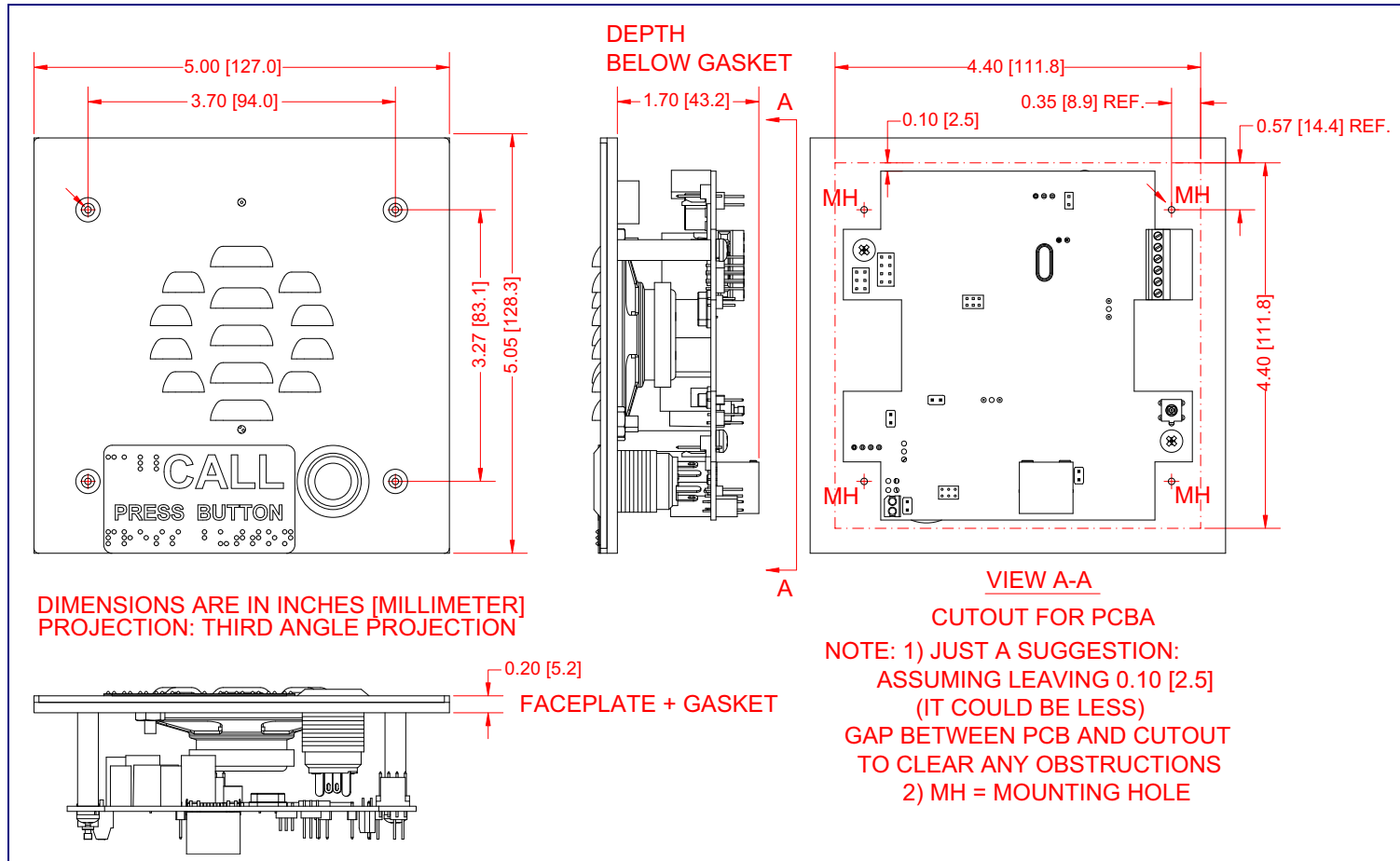
**Figure A-5. Mounting**



## A.1.1 Custom Flush Mounting

Figure A-6 shows how to do a custom flush mounting for the VoIP Intercom.

**Figure A-6. Custom Flush Mounting**



# Appendix B: Setting up a TFTP Server

---

## B.1 Set up a TFTP Server

Autoprovisioning requires a TFTP server for hosting the configuration file.

---

### B.1.1 In a LINUX Environment

To set up a TFTP server on LINUX:

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

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

---

### B.1.2 In a Windows Environment

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

<http://www.cyberdata.net/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 Intercom product page at:

<http://www.cyberdata.net/products/voip/digitalanalog/intercom/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 Intercom product page at:

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

---

## C.3 Contact Information

Contact	<p>CyberData Corporation 3 Justin Court Monterey, CA 93940 USA <a href="http://www.CyberData.net">www.CyberData.net</a> 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><a href="http://www.cyberdata.net/support/contactsupportvoip.php">http://www.cyberdata.net/support/contactsupportvoip.php</a></p> <p>The Support Form initiates a ticket which CyberData uses for tracking customer requests. Most importantly, the Support Form tells us which PBX system and software version that you are using, the make and model of the switch, and other important information. This information is essential for troubleshooting. Please also include as much detail as possible in the <b>Comments</b> section of the Support Form.</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. Also, RMA numbers require an active VoIP Technical Support ticket number. A product will not 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><a href="http://www.cyberdata.net/support/rmastatus.html">http://www.cyberdata.net/support/rmastatus.html</a></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 Warranty, CyberData will repair or replace the product free of charge. This warranty includes all parts and labor.

Should the product fail Out of the Warranty period, a flat rate repair charge of one half of the purchase price of the product will be assessed. Repairs that are Within Warranty period but are damaged by improper installation, modification, or abuse are deemed Out of Warranty and will be charged at the Out of Warranty rate. A device is deemed Out of Warranty when its purchase date is longer than two years or when the device has been damaged due to human error during installation, modification, or abuse. A replacement unit will be offered at full cost if the device cannot be repaired.

**End of Life Devices** are included under this policy. End of Life devices are devices that are no longer produced or sold. Technical support is still available for these devices. However, no firmware revisions or updates will be provided. If an End of Life device cannot be repaired, the replacement offered may be the current version of the device.

Products shipped to CyberData, both within and out of warranty, are shipped at the expense of the customer. CyberData will pay return shipping charges for repaired products.

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 16  
16 AWG gauge wire 10

## A

AC voltages 3  
AC voltages, intercom enclosure is not rated 11  
act light 17  
activate relay (door sensor) 44  
activate relay (intrusion sensor) 44  
address, configuration login 27  
audio configuration 47  
    night ring tone parameter 49  
audio configuration page 47  
audio encodings 5  
audio files, user-created 50  
Autoprovision at time (HHMMSS) 58  
autoprovision at time (HHMMSS) 58  
autoprovision when idle (in minutes > 10) 58  
autoprovisioning 59  
    autoprovisioned audio files 61  
    autoprovisioned firmware upgrades 60  
    autoprovisioning autoupdate 60  
    autoprovisioning from DHCP 59  
    autoprovisioning server (IP address) 60  
    setting up a TFTP server 80  
autoprovisioning autoupdate (in minutes) 58  
autoprovisioning configuration 57, 58  
autoprovisioning filename 58  
auxiliary relay 11  
auxiliary relay wiring diagram 12  
auxiliary relay, 1A at 30 VDC 6

## B

backup SIP server 1 36  
backup SIP server 2 36  
backup SIP servers, SIP server  
    backups 36  
baud rate  
    verifying 16

## C

call button 15  
    LED 15  
call button LED 15  
changing  
    the web access password 30  
Chrome (web browser) 3  
Cisco SRST 36  
command interface 68  
commands 68  
conduit restrictions 77  
configurable parameters 29, 31, 34, 36, 66  
configuration  
    audio 47  
    default IP settings 25  
    door sensor 42  
    intrusion sensor 42  
    network 33  
    SIP 35  
    using Web interface 25  
configuration home page 27  
configuration page  
    configurable parameters 29, 31, 34  
contact information 82  
contact information for CyberData 82  
Current Network Settings 34  
current network settings 34  
CyberData contact information 82

## D

default  
    gateway 25  
    intercom settings 85  
    IP address 25  
    subnet mask 25  
    username and password 25  
    web login username and password 27  
default gateway 25, 34  
default intercom settings 21  
default IP settings 25  
default login address 27  
device configuration 30  
    device configuration parameters 58  
    the device configuration page 57  
device configuration page 30  
device configuration parameters 31  
device configuration password  
    changing for web configuration access 30

- DHCP Client 5
- DHCP IP addressing 34
- dial out extension (door sensor) 44
- dial out extension (intrusion sensor) 44
- dial out extension strings 37
- dial-out extension strings 39
- dimensions 6, 7
- disable rport discovery 36
- discovery utility program 27
- DNS server 34
- door sensor 42, 44, 49
  - activate relay 44
  - dial out extension 44
  - door open timeout 44
  - door sensor normally closed 44
  - flash button LED 44
  - play audio locally 44
- door strike
  - cannot be powered by alternate power input nor PoE power 10
- download protocol, HTTP or TFTP 58
- DTMF tones 37, 39
- DTMF tones (using rfc2833) 37
- dual speeds 16

## E

- electric screwdriver 76
- enable night ring events 53
- ethernet cable 75
- event configuration
  - enable night ring events 53
- expiration time for SIP server lease 36, 41

## F

- factory default settings 21
- fastening, gang box 76
- Firefox (web browser) 3
- firmware
  - where to get the latest firmware 65
- flash button LED (door sensor) 44
- flash button LED (intrusion sensor) 44
- flush mounting, custom 79

## G

- gang box, fastening 76
- gasket, avoid over-torque damage 76
- GMT table 63
- GMT time 63

- green link light 16

## H

- home page 27
- http POST command 68
- http web-based configuration 5

## I

- identifier names (PST, EDT, IST, MUT) 63
- identifying your product 1
- illustration of intercom mounting process 74
- installation, typical intercom system 2
- intercom configuration
  - default IP settings 25
- intercom configuration page
  - configurable parameters 36, 66
- Internet Explorer (web browser) 3
- intrusion sensor 42, 44
  - activate relay 44
  - dial out extension 44
  - flash button LED 44
  - play audio locally 44
- IP address 25, 34
- IP addressing 34
  - default
    - IP addressing setting 25

## J

- J3 terminal block, 16 AWG gauge wire 10

## L

- lease, SIP server expiration time 36, 41
- lengthy pages 46
- link LED 75
- link light 16
- Linux, setting up a TFTP server on 80
- local SIP port 36
- log in address 27

## M

- MGROUP
  - MGROUP Name 46

- mounting an intercom 74
- Mozilla Firefox (web browser) 3
- multicast configuration 45
- Multicast IP Address 46

## N

- navigation (web page) 26
- navigation table 26
- network activity, verifying 17
- network configuration of intercom 33
- Network Setup 33
- nightring tones 46
- Nightringer 10
- nightringer settings 41
- NTP server 58

## O

- operating temperature 6
- orange link light 16

## P

- packet time 5
- pages (lengthy) 46
- part number 6
- parts list 9
- password
  - for SIP server login 36
  - login 27
  - restoring the default 25
- payload types 6
- play audio locally (door sensor) 44
- play audio locally (intrusion sensor) 44
- point-to-point configuration 38
- port
  - local SIP 36
  - remote SIP 36
- posix timezone string
  - timezone string 58
- POST command 68
- power input 6
- power screwdriver 76
- priority
  - assigning 46
- product
  - configuring 25
  - mounting 74
  - parts list 9
- product features 4

- product overview
  - product features 4
  - product specifications 6
  - supported protocols 5
  - supported SIP servers 5
  - typical system installation 2
- product specifications 6
- protocol 6
- protocols supported 5

## R

- reboot 66, 67
- remote SIP port 36
- reset test function management button 18
- resetting the IP address to the default 74, 81
- restoring factory default settings 21, 85
- return and restocking policy 84
- ringtones 46
  - lengthy pages 46
- RJ-45 14
- RMA returned materials authorization 82
- RMA status 82
- rport discovery 36
- RTFM button 18
- RTFM jumper 18, 20, 21, 22, 24
- RTP/AVP 5

## S

- Safari (web browser) 3
- sales 82
- sensor setup page 43
- sensor setup parameters 42
- sensors 44
- server address, SIP 36
- service 82
- set the time from the NTP server 58
- set time with external NTP server on boot 58
- setting up an intercom 10
- settings, default 21
- SIP
  - enable SIP operation 36
  - local SIP port 36
  - user ID 36
- SIP (session initiation protocol) 5
- SIP configuration 35
  - SIP Server 36
- SIP configuration parameters
  - outbound proxy 36, 41
  - registration and expiration, SIP server lease 36, 41
  - unregister on reboot 36

- user ID, SIP 36
- SIP registration 36
- SIP remote SIP port 36
- SIP server 36
  - password for login 36
  - SIP servers supported 5
  - unregister from 36
  - user ID for login 36
- SIP settings 37
- Spare in the Air Policy 84
- speaker output 6
- SRST 36
- static IP addressing 34
- status LED 75
- subnet mask 25, 34
- supported protocols 5

## T

- tech support 82
- technical support, contact information 82
- terminal block, 16 AWG gauge wire 10
- TFTP server 5, 80
- time zone string examples 63

## U

- upgrading to firmware 6.x.x from 5.x.x 65, 76
- user ID
  - for SIP server login 36
- username
  - changing for web configuration access 30
  - default for web configuration access 27
  - restoring the default 25

## V

- verifying
  - baud rate 16
  - network activity 17
  - network connectivity 16
- VLAN ID 34
- VLAN Priority 34
- VLAN tagging support 34
- VLAN tags 34
- volume boost 32

## W

- warranty 83
- warranty & RMA returns outside of the United States 83
- warranty and RMA returns page 84
- warranty policy at CyberData 83
- web access password 25
- web access username 25
- web configuration log in address 27
- web page
  - navigation 26
- web page navigation 26
- web-based intercom configuration 25
- weight 6
- wget, free unix utility 68
- Windows, setting up a TFTP server on 80

## Y

- yellow act light 17
- yellow link light 16