



# *SIP Indoor Intercom Operations Guide*

Part #011211\*, RAL 9003, Signal White Color

\*Replaces #011111

*Document Part #931604B  
for Firmware Version 20.4.1*

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

---

---

**SIP Indoor Intercom Operations Guide 931604B**  
**Part # 011211\***  
**\*Replaces 011111.**

**COPYRIGHT NOTICE:**

© 2022, 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:  
<https://support.cyberdata.net/>

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 931604B, which was released on March 1, 2022, corresponds to firmware version 20.4.1, and has the following changes:

- Updates [Figure 1-2, "Typical Installation"](#)
- Updates [Section 1.3, "Features"](#)
- Updates [Table 1-1, "Specifications"](#)
- Updates [Figure 2-19, "Home Page"](#)
- Updates [Table 2-6, "Home Page Overview"](#)
- Updates [Figure 2-22, "SIP Configuration Page"](#)
- Updates [Figure 2-23, "SIP Configuration Page"](#)
- Updates [Figure 2-24, "SIP Page Set to Point-to-Point Mode"](#)
- Updates [Table 2-9, "SIP Configuration Parameters"](#) to add the [Asymmetric RTP](#) setting
- Updates [Figure 2-25, "SSL Configuration Page"](#)
- Updates [Figure 2-26, "SSL Configuration Page"](#)
- Updates [Table 2-12, "SSL Configuration Parameters"](#)
- Updates [Figure 2-42, "Home Page"](#)

---

# Important Safety Instructions

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



## Warning

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





## Warning

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

---

## Pictorial Alert Icons

|   |   |
|---|---|
|  | <b>General Alert</b><br>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. |
|  | <b>Ground</b><br>This pictorial alert indicates the Earth grounding connection point.   |

---

## Hazard Levels

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

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

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

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

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

---

## Abbreviations and Terms

| Abbreviation or Term | Definition  |
|----------------------|---|
| A-law                | A standard companding algorithm, used in European digital communications systems to optimize, i.e., modify, the dynamic range of an analog signal for digitizing. |
| AVP                  | Audio Video Profile   |
| Cat 5                | TIA/EIA-568-B Category 5  |
| DHCP                 | Dynamic Host Configuration Protocol   |
| LAN                  | Local Area Network  |
| LED                  | Light Emitting Diode  |
| Mbps                 | Megabits per Second.  |
| NTP                  | Network Time Protocol   |
| PBX                  | Private Branch Exchange   |
| PoE                  | Power over Ethernet (as per IEEE 802.3af standard)  |
| RTFM                 | Reset Test Function Management  |
| SIP                  | Session Initiated Protocol  |
| SRTP                 | Secure Real Time Protocol   |
| u-law                | A companding algorithm, primarily used in the digital telecommunication   |
| UC                   | Unified Communications  |
| VoIP                 | Voice over Internet Protocol  |

# Contents

---

|  |               |
|--|---------------|
| <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 Features .....   | 3             |
| 1.4 Supported Protocols .....  | 4             |
| 1.5 Supported SIP Servers .....  | 4             |
| 1.6 Specifications .....   | 5             |
| 1.7 Compliance .....   | 6             |
| 1.7.1 CE Statement .....   | 6             |
| 1.7.2 FCC Statement .....  | 6             |
| 1.7.3 Industry Canada (IC) Compliance Statement .....                          | 6             |
| <br><b>Chapter 2 Installing the SIP Indoor Intercom</b>                        | <br><b>7</b>  |
| 2.1 Parts List .....   | 7             |
| 2.2 Intercom Components .....  | 8             |
| 2.3 Intercom Setup .....   | 9             |
| 2.3.1 Intercom Connections .....   | 9             |
| 2.3.2 Using the On-Board Relay .....   | 11            |
| 2.3.3 Wiring the Circuit .....   | 12            |
| 2.3.4 Connecting an Auxiliary RGB (Multi-Color) Strobe Kit to the Device ..... | 16            |
| 2.3.5 Intercom Connectors .....  | 17            |
| 2.3.6 Activity and Link LEDs .....   | 21            |
| 2.3.7 RTFM Button .....  | 22            |
| 2.3.8 Adjusting the Intercom Volume .....                                      | 24            |
| 2.3.9 Call Button and the Call Button LED .....                                | 25            |
| 2.4 Configure the Intercom Parameters .....                                    | 26            |
| 2.4.1 Factory Default Settings .....   | 26            |
| 2.4.2 Intercom Web Page Navigation .....                                       | 27            |
| 2.4.3 Using the Toggle Help Button .....                                       | 28            |
| 2.4.4 Log in to the Configuration Home Page .....                              | 30            |
| 2.4.5 Configure the Device .....   | 34            |
| 2.4.6 Configure the Network Parameters .....                                   | 38            |
| 2.4.7 Configure the SIP (Session Initiation Protocol) Parameters .....         | 40            |
| 2.4.8 Configure the SSL Parameters .....                                       | 49            |
| 2.4.9 Configure the Multicast Parameters .....                                 | 55            |
| 2.4.10 Configure the Sensor Configuration Parameters .....                     | 59            |
| 2.4.11 Configure the Audio Configuration Parameters .....                      | 63            |
| 2.4.12 Configure the Events Parameters .....                                   | 69            |
| 2.4.13 Configure the Door Strike Relay .....                                   | 75            |
| 2.4.14 Configure the Autoprovisioning Parameters .....                         | 77            |
| 2.5 Upgrade the Firmware .....   | 88            |
| 2.6 Reboot the Device .....  | 91            |
| 2.7 Command Interface .....  | 92            |
| 2.7.1 Command Interface Post Commands .....                                    | 92            |
| <br><b>Appendix A Mounting the Indoor Intercom</b>                             | <br><b>96</b> |
| A.1 Wall Mounting Components .....   | 96            |
| A.2 Cable Connections .....  | 97            |
| A.3 Wall Mounting Option .....   | 98            |
| A.4 Gang Box Option .....  | 99            |
| A.5 Wall Cutout Dimensions .....   | 100           |

|   |            |
|---|------------|
| A.6 PCB Dimensions .....                            | 101        |
| <b>Appendix B Setting up a TFTP Server</b>          | <b>102</b> |
| B.1 Set up a TFTP Server .....                      | 102        |
| B.1.1 In a LINUX Environment .....                  | 102        |
| B.1.2 In a Windows Environment .....                | 102        |
| <b>Appendix C Troubleshooting/Technical Support</b> | <b>103</b> |
| C.1 Frequently Asked Questions (FAQ) .....          | 103        |
| C.2 Documentation .....                             | 103        |
| C.3 Contact Information .....                       | 104        |
| C.4 Warranty and RMA Information .....              | 104        |
| <b>Index</b>  | <b>105</b> |



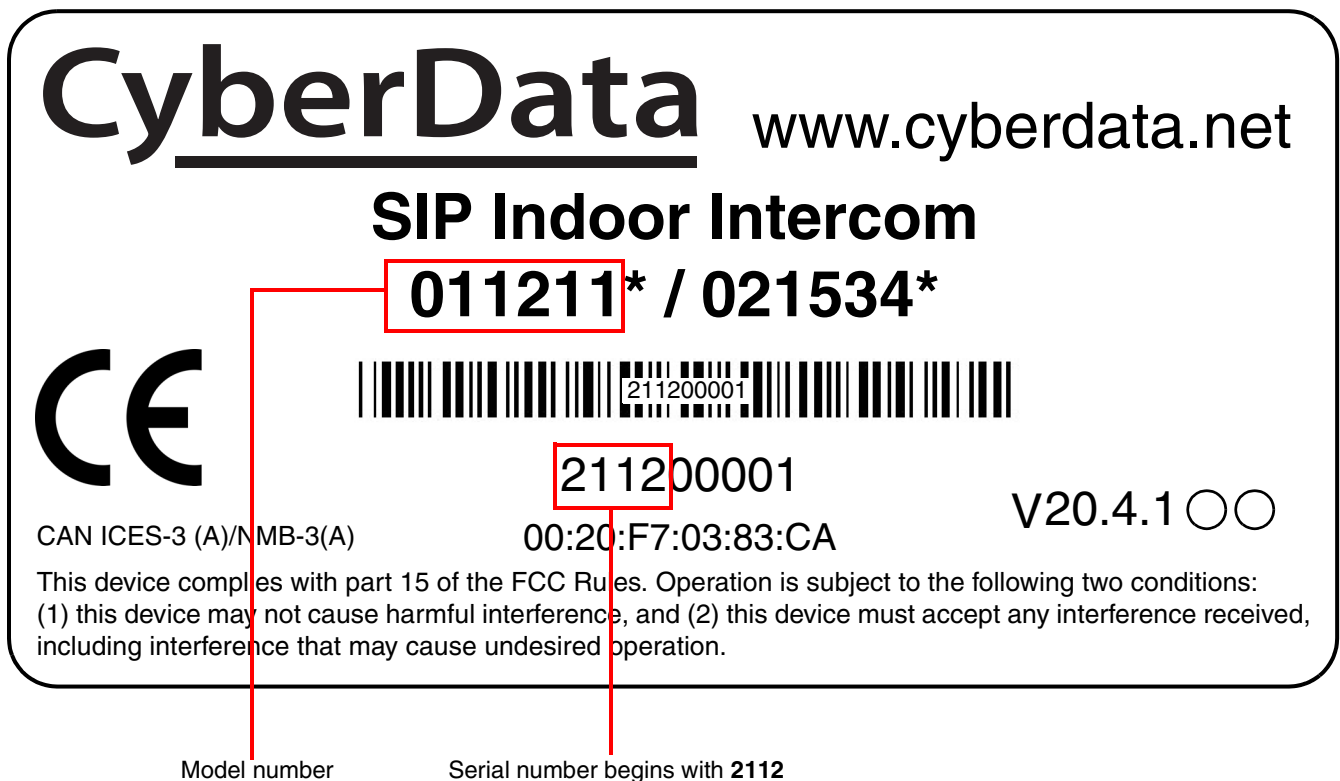
# 1 Product Overview

## 1.1 How to Identify This Product

To identify the SIP Indoor Intercom, look for a model number label similar to the one shown in [Figure 1-1](#). Confirm the following:

- The model number on the label should be **011211**.
- The serial number on the label should begin with **2112**.

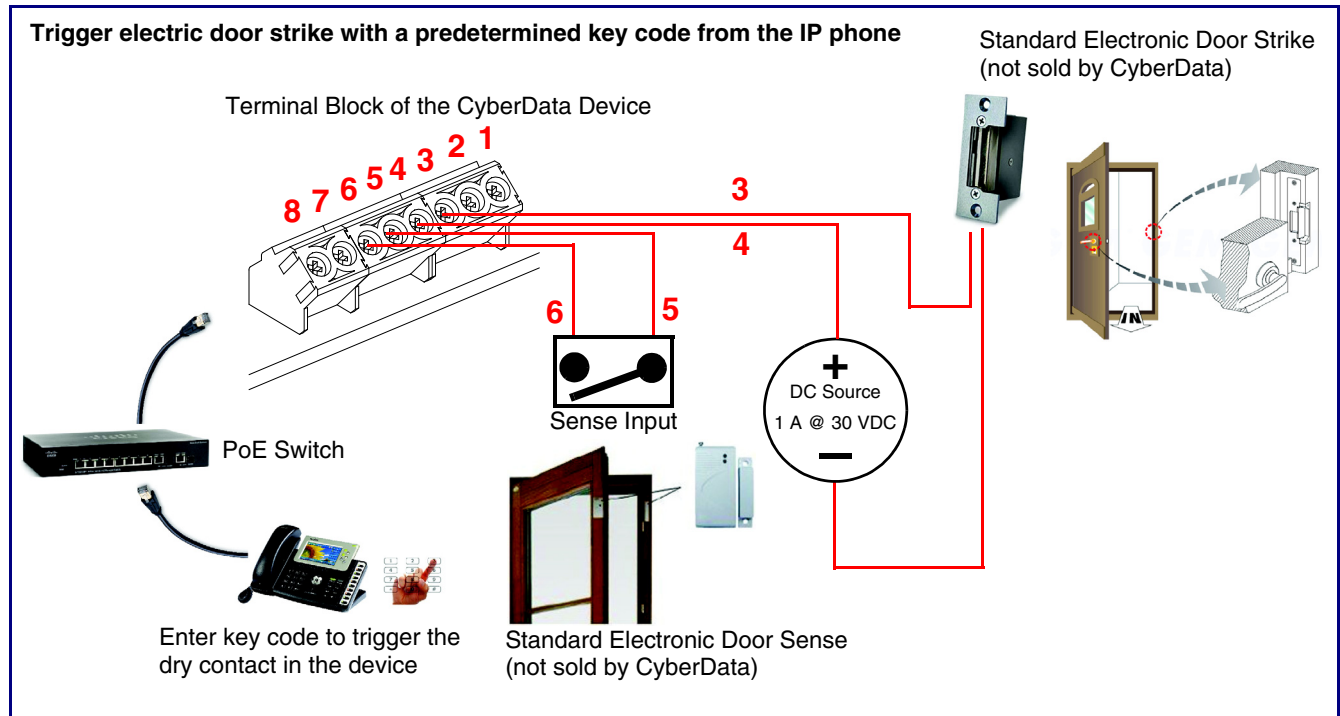
**Figure 1-1. Model Number Label**



## 1.2 Typical System Installation

The following figures illustrate how the SIP Indoor Intercom can be installed as part of a VoIP phone system.

**Figure 1-2. Typical Installation**



---

## 1.3 Features

The SIP Indoor Intercom has the following features:

- Full duplex audio with enhanced acoustic echo cancelling
  - Half duplex push-to-talk audio from the phone side using the phone's keypad or from the intercom side using the call button
  - Simultaneous SIP and multicast
  - Supports user-uploadable ring and alert tones
  - Loud/Night Ringer function - second SIP extension
  - Can receive pages directly from Poly phones as well as other devices that send standard multicast
- 
- DTMF-controlled dry relay contact for auxiliary control
  - Door closure and tamper alert signal
  - Network volume control
  - Supports Auxiliary Strobe Kit for visual notification
- 
- TLS 1.2 and SRTP enhanced security for IP endpoints in a local or cloud-based environment
  - Autoprovisioning via HTTP, HTTPS, or TFTP
  - HTTPS or HTTP web based configuration. HTTPS is enabled by default
  - Configurable event generation for device health and status monitoring
  - 802.11q VLAN tagging
  - Web-based upgradeable firmware
  - Support for Cisco SRST resiliency

---

## 1.4 Supported Protocols

The Intercom supports the following protocols:

- SIP (session initiation protocol)
- HTTP Web-based configuration

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

- DHCP Client

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

- TFTP Client

Facilitates hosting for the Autoprovisioning configuration file.

- RTP

- RTP/AVP - Audio Video Profile

- Facilitates autoprovisioning configuration values on boot

- Audio Encodings

PCMU (G.711 mu-law)

PCMA (G.711 A-law)

G.722

G.729

Packet Time 20 ms

---

## 1.5 Supported SIP Servers

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

<https://www.cyberdata.net/pages/connecting-to-ip-pbx-servers>

## 1.6 Specifications

**Table 1-1. Specifications**

| Specifications          |   |
|-------------------------|---|
| Ethernet I/F            | 10/100 Mbps   |
| Protocol                | SIP RFC 3261 Compatible   |
| Power Input             | PoE 802.3af compliant or +8 to +12VDC @ 1000mA Regulated Power Supply (not included) <sup>a</sup>   |
| Speaker Output          | 2 Watts Peak Power  |
| On-Board Relay          | 1A at 30 VDC  |
| Payload Types           | G.711 a-law, G.711 $\mu$ -law, G.722, and G.729   |
| Network Security        | TLS 1.2, SRTP, HTTPS  |
| Operating Range         | Temperature: -40° C to 55° C (-40° F to 131° F)<br>Humidity: 5-95%, non-condensing  |
| Storage Temperature     | -40° C to 70° C (-40° F to 158° F)  |
| Storage Altitude        | Up to 15,000 ft. (4573 m)   |
| Dimensions <sup>b</sup> | 4.53 inches [115 mm] Length<br>2.22 inches [56.3 mm] Width<br>4.53 inches [115 mm] Height   |
| Weight                  | 1.0 lbs. [0.45 kg]  |
| Boxed Weight            | 2.0 lbs. [0.90 kg]  |
| Compliance              | CE: EMC Directive – Class A EN 55032 & EN 55024, LV Safety Directive EN 62368-1; RoHS Compliant; FCC Part 15 Class; Industry Canada ICES-3 Class A; IEEE 802.3 Compliant; TAA Compliant |
| Warranty                | 2 Years Limited   |
| Part Number             | 011211  |

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

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

---

## 1.7 Compliance

---

### 1.7.1 CE Statement



As of the date of manufacture, the Paging Series has been tested and found to comply with the specifications for CE marking and standards per EMC and Radio communications Compliance. This applies to the following products: 011145, 011146, 011233, 011280, 011295, 011314, 011368, and 011372.

EMC Directive - Class A Emissions, Immunity, and LV Safety Directive, RoHS Compliant.  
Flammability rating on all components is 94V-0.

---

### 1.7.2 FCC Statement



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

**CAUTION:** Changes or modifications not expressly approved by the manufacturer responsible for compliance could void the user's authority to operate the equipment.

---

### 1.7.3 Industry Canada (IC) Compliance Statement

Operation is subject to the following two conditions:

1. This device may not cause interference, and
2. This device must accept any interference, including interference that may cause undesired operations of the device.

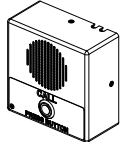


ICES-3 Class A

## 2 Installing the SIP Indoor Intercom

### 2.1 Parts List

Table 2-1 illustrates the SIP Indoor Intercom parts.

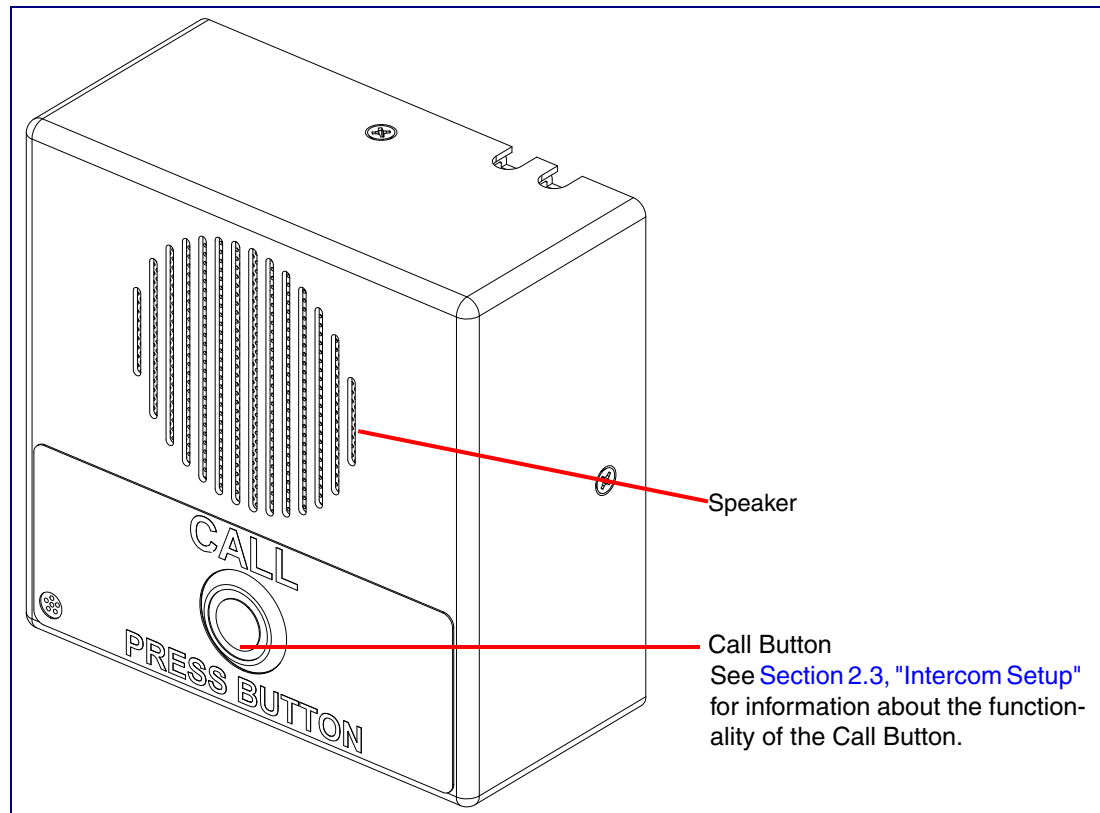
**Table 2-1. Parts List**

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

## 2.2 Intercom Components

Figure 2-1 shows the components of the Intercom.

**Figure 2-1. Intercom Components**






## 2.3 Intercom Setup


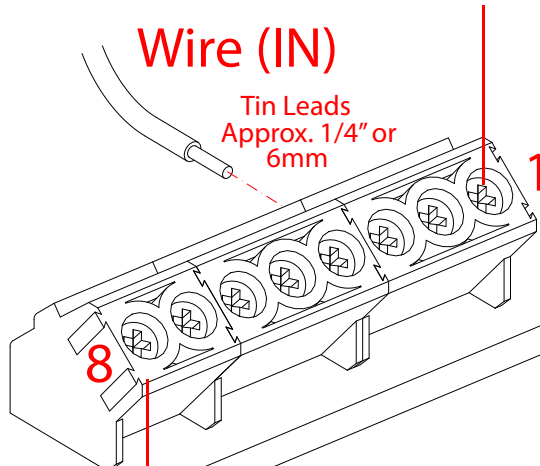
### 2.3.1 Intercom Connections

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

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

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

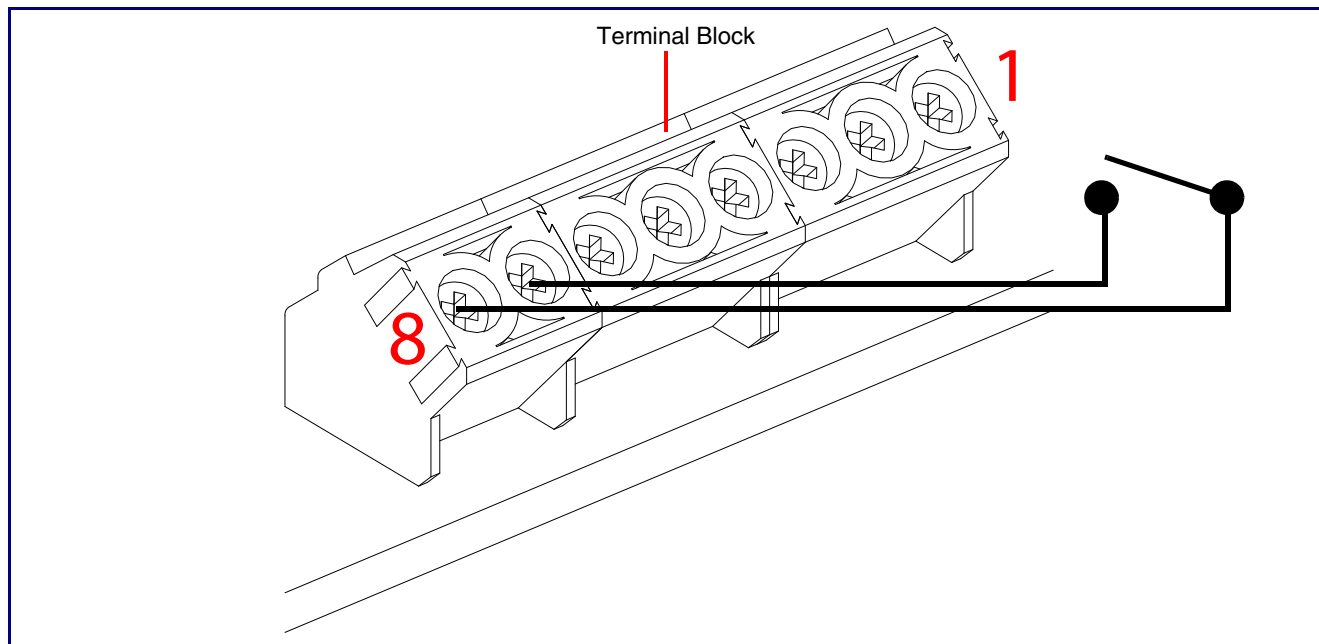
**Figure 2-2. Connections and Alternate Power Input**

|   |  |
|---|--|
| <p>Alternate Power Input:<br/>1 = +8 to +12VDC @ 1000mA Regulated Power Supply*<br/>2 = Power Ground*</p>  <p>Relay Contact:<br/>(1 A at 30 VDC for continuous loads)<br/>3 = Relay Common<br/>4 = Relay Normally Open Contact<br/>5 = Sense Input<br/>6 = Sense Ground<br/>7 = Remote Switch "A"<br/>8 = Remote Switch "B"</p> <p>*Contacts 1 and 2 on the terminal block are only for powering the device from a non-PoE 12VDC power source as an alternative to Network PoE power. Use of these contacts for any other purpose will damage the device and void the product warranty.</p> | <p>Use a 3.17 mm (1/8-inch) flat blade screwdriver for the terminal block screws</p> <p><b>Wire (IN)</b></p> <p>Tin Leads<br/>Approx. 1/4" or<br/>6mm</p>  <p>Terminal Block<br/>can accept 16 AWG wire</p> |
|---|--|




### 2.3.1.1 Remote Switch Connection

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

**Figure 2-3. Remote Switch Connection**



## 2.3.2 Using the On-Board Relay

|  |  |
|--|--|
| <br>GENERAL ALERT | <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>  |
| <br>GENERAL ALERT | <p><b>Warning</b></p> <p><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>     |
| <br>GENERAL ALERT | <p><b>Warning</b></p> <p><i>Electrical Hazard:</i> The relay does not support AC powered door strikes. Any use of this relay beyond its normal operating range can cause damage to the product and is not covered under our warranty policy.</p> |

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

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

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

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

For more information on the sensor options, see the [Sensor Configuration Page](#) on the web interface.

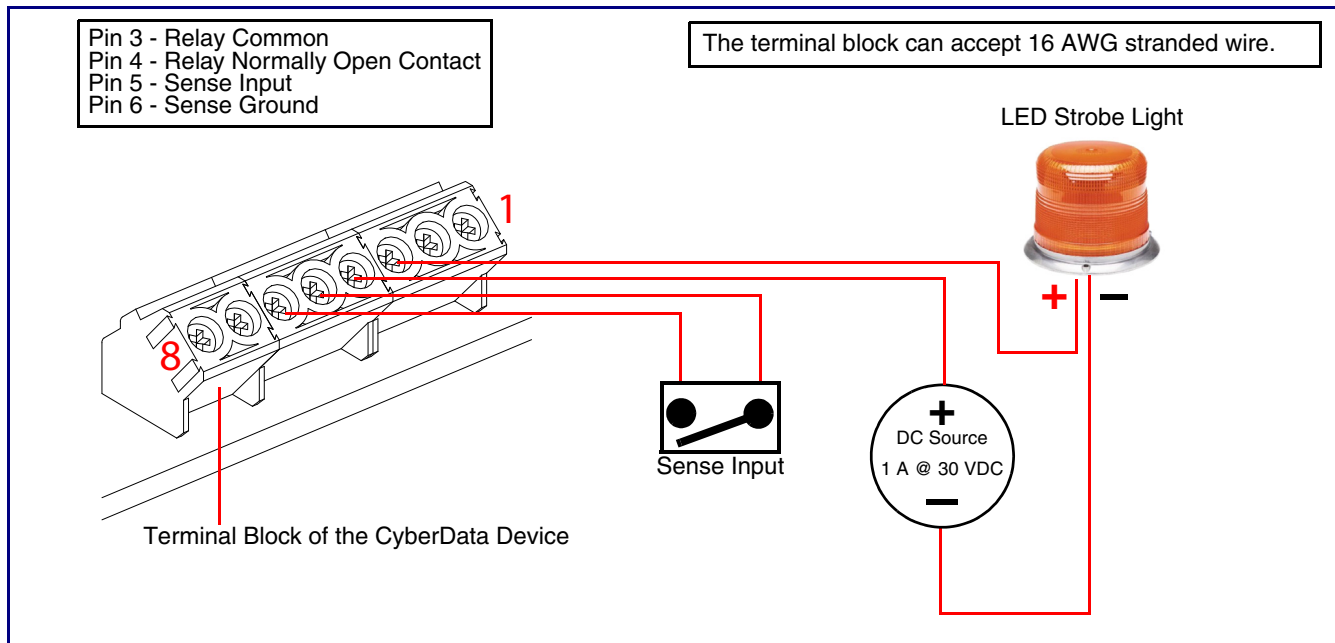
## 2.3.3 Wiring the Circuit

### 2.3.3.1 Devices Less than 1A at 30 VDC

If the power for the device is less than 1A at 30 VDC and is not an inductive load, then see [Figure 2-4](#) for the wiring diagram.

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


**Figure 2-4. Devices Less than 1A at 30 VDC**



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

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

This product provides an easier method of connecting standard door strikes as well as AC and higher voltage devices. See [Figure 2-5](#) and [Figure 2-6](#) for the wiring diagrams.

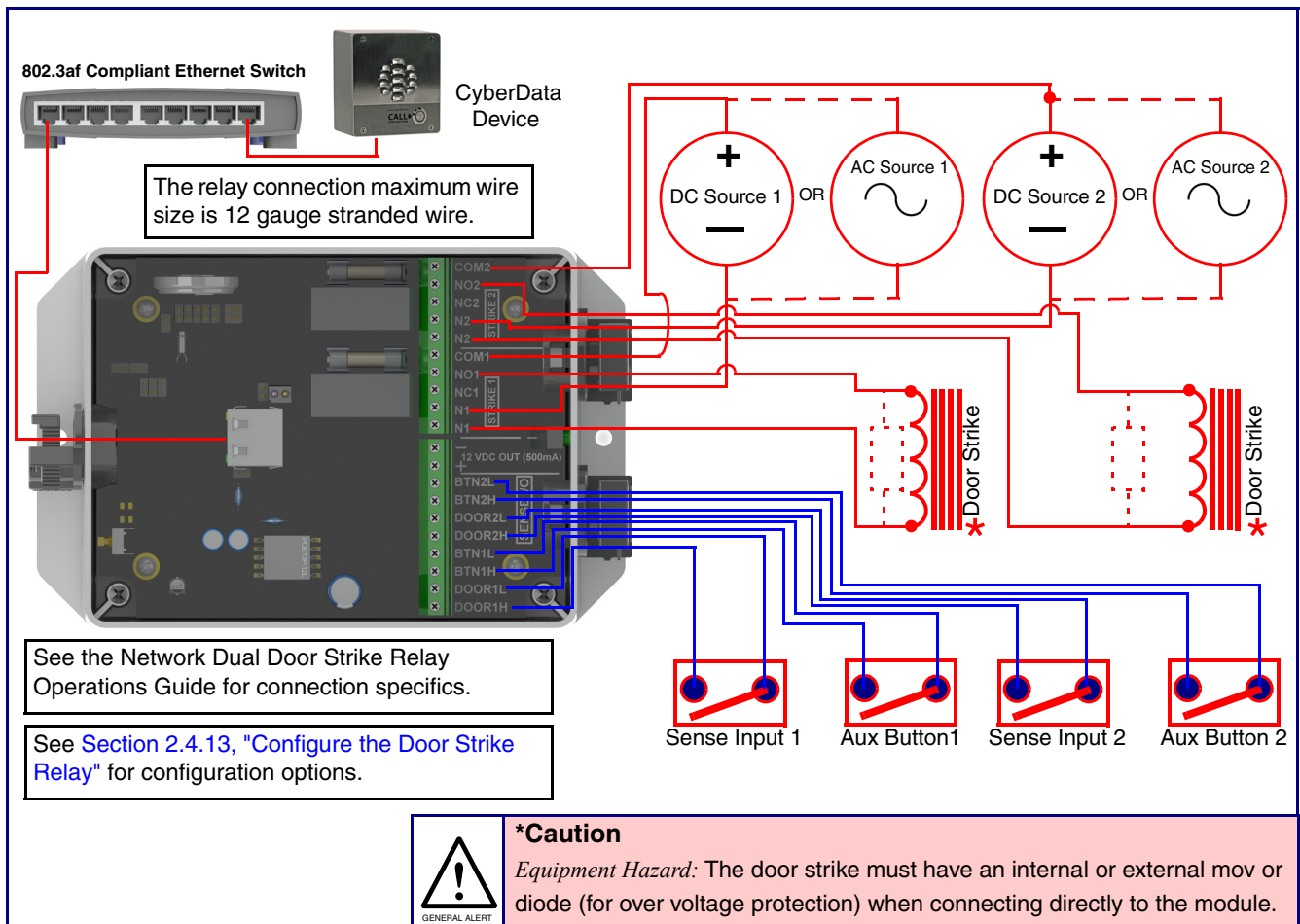


GENERAL ALERT

**Warning**

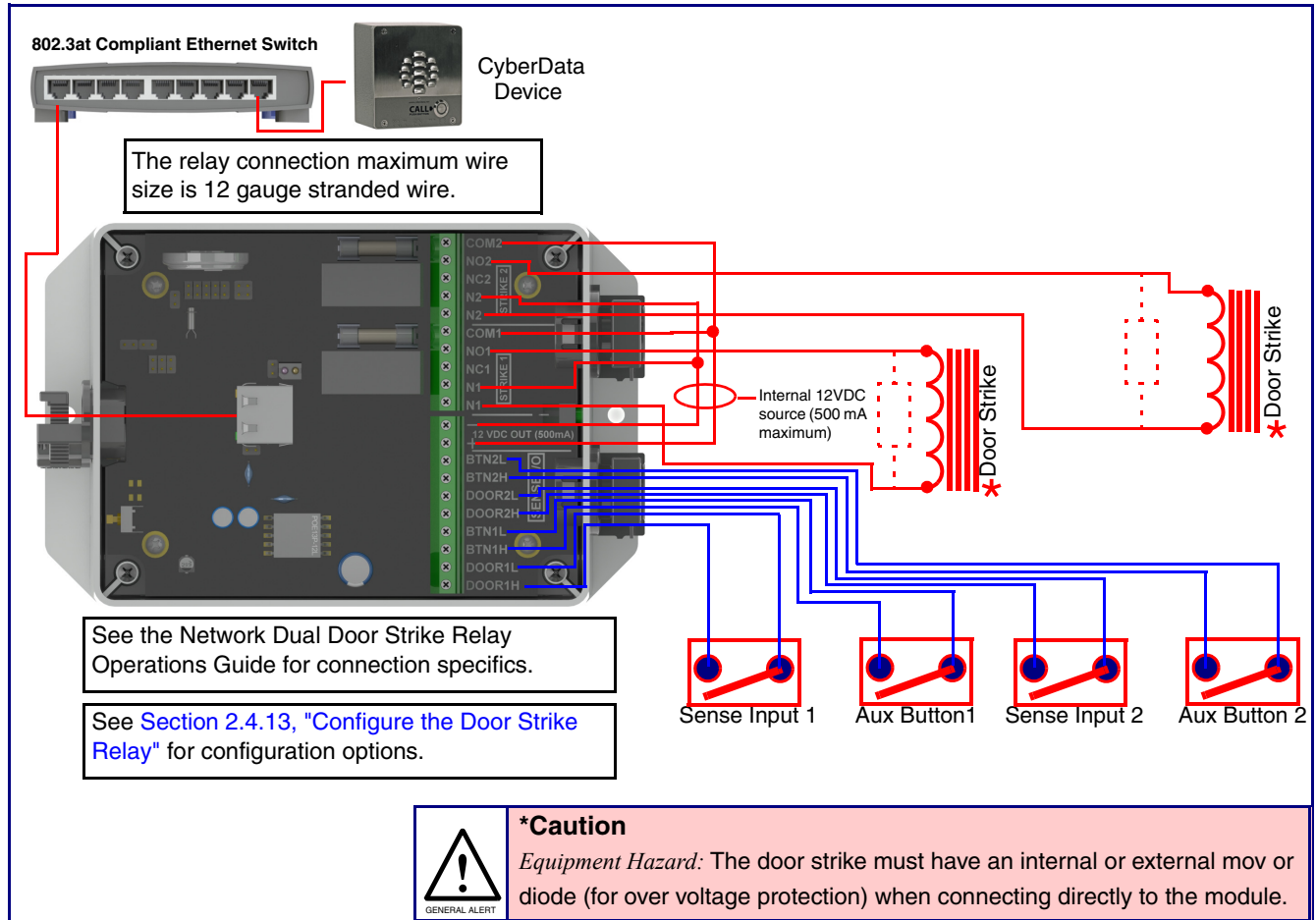
*Electrical Hazard:* Hazardous voltages may be present. No user serviceable part inside. Refer to qualified service personnel for connecting or servicing.

**Figure 2-5. Network Dual Door Strike Relay Wiring Diagram with External Power Source**



### 2.3.3.3 Network Dual Door Strike Relay Wiring Diagram Using PoE+

**Figure 2-6. Network Dual Door Strike Relay Wiring Diagram Using PoE+**



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

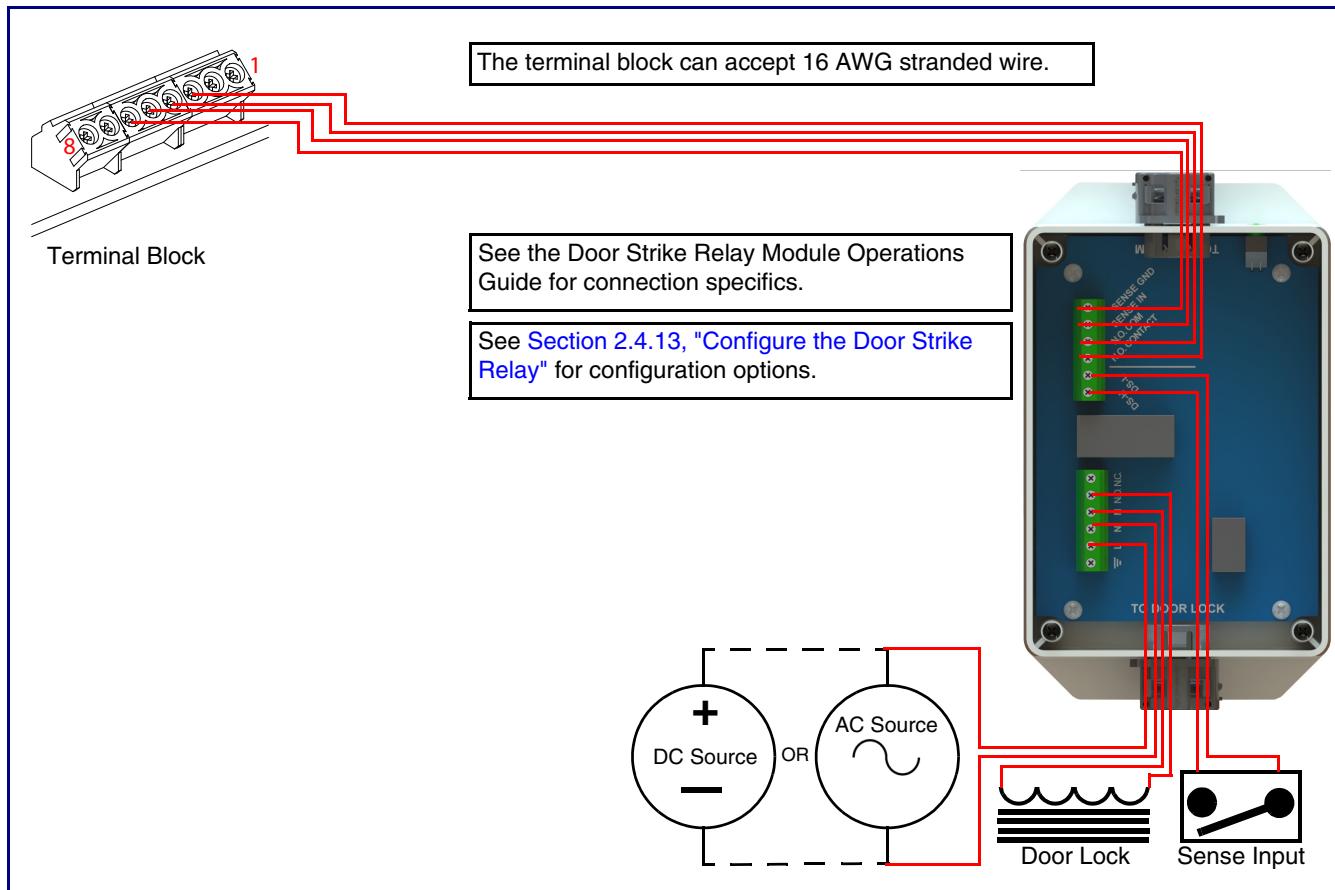
<https://support.cyberdata.net/>

#### 2.3.3.4 Door Strike Relay Module Wiring Diagram from Intercom

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

This product provides an easier method of connecting standard door strikes as well as AC and higher voltage devices. See [Figure 2-7](#) for the wiring diagram.

### Figure 2-7. Door Strike Relay Module Wiring Diagram from Intercom



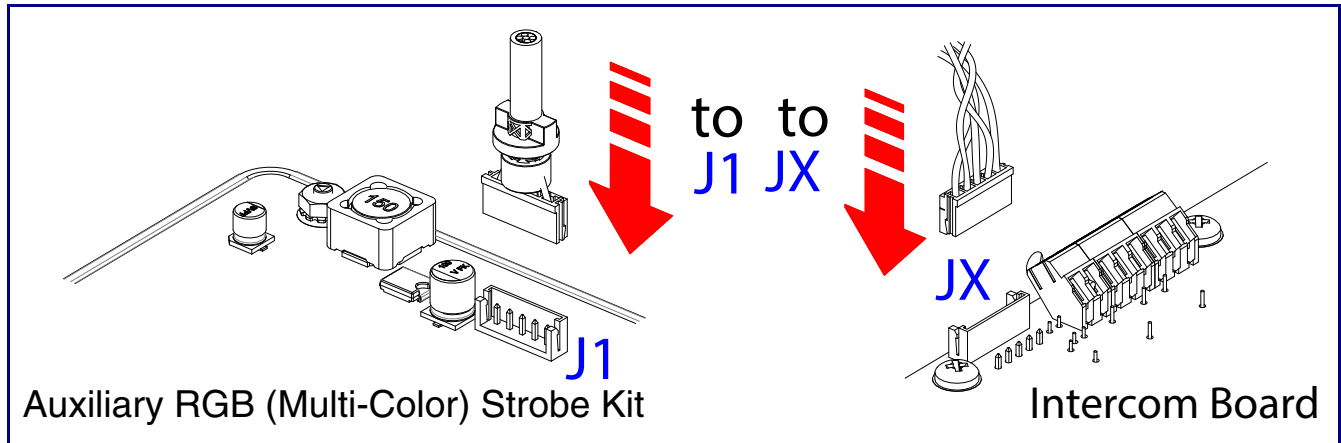
If you have questions about connecting door strikes or setting up the web configurable options, please contact our support department at the following website:

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

### 2.3.4 Connecting an Auxiliary RGB (Multi-Color) Strobe Kit to the Device

1. Connect the strobe cable to the board of the Auxiliary RGB (Multi-Color) Strobe Kit and the board of the Intercom as shown in [Figure 2-8](#). Please see the Auxiliary RGB (Multi-Color) Strobe Kit Operations Guide for more information about this product.

**Figure 2-8. Connecting the Auxiliary RGB (Multi-Color) Strobe Kit to the Intercom**

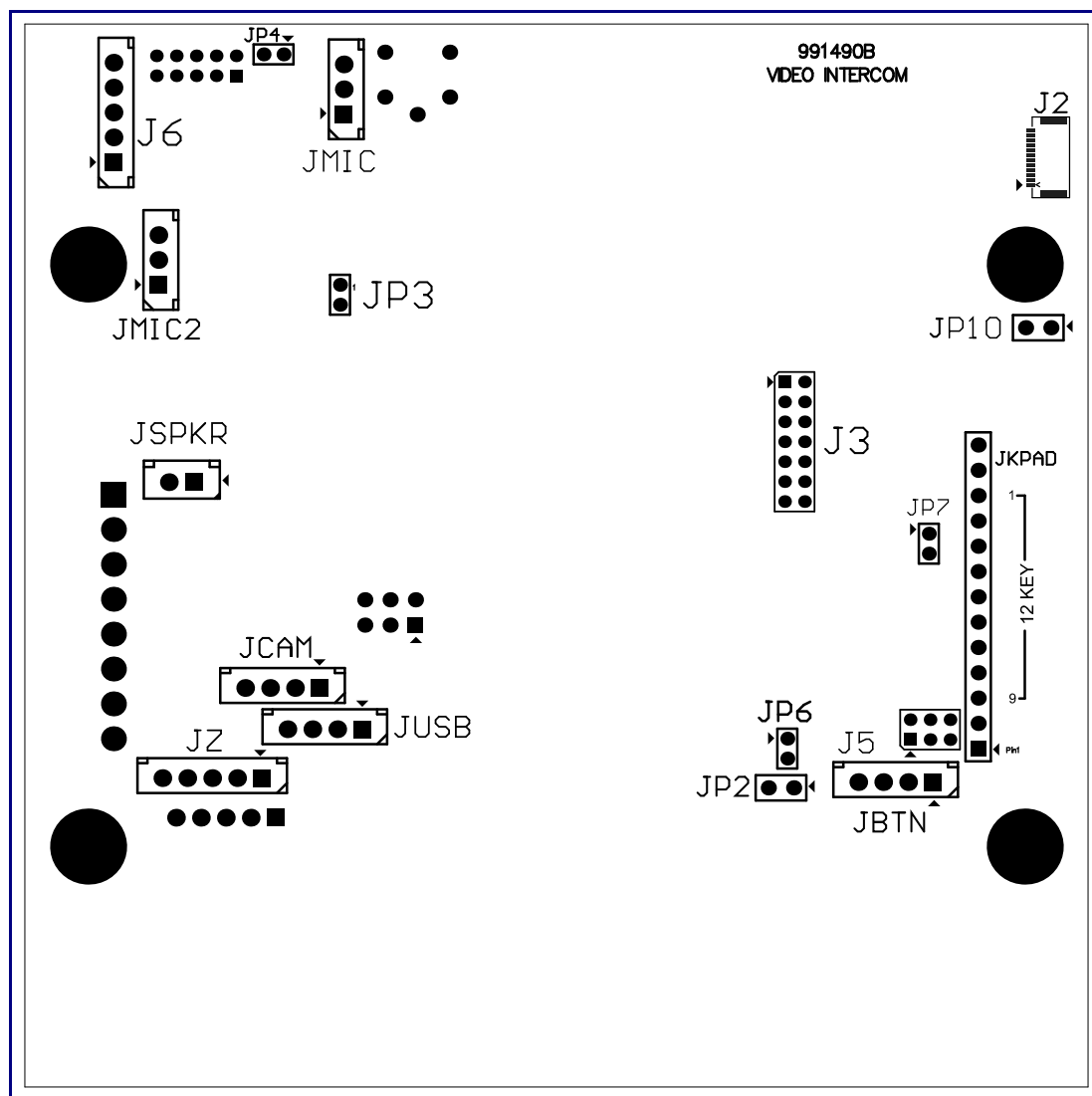




## 2.3.5 Intercom Connectors

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

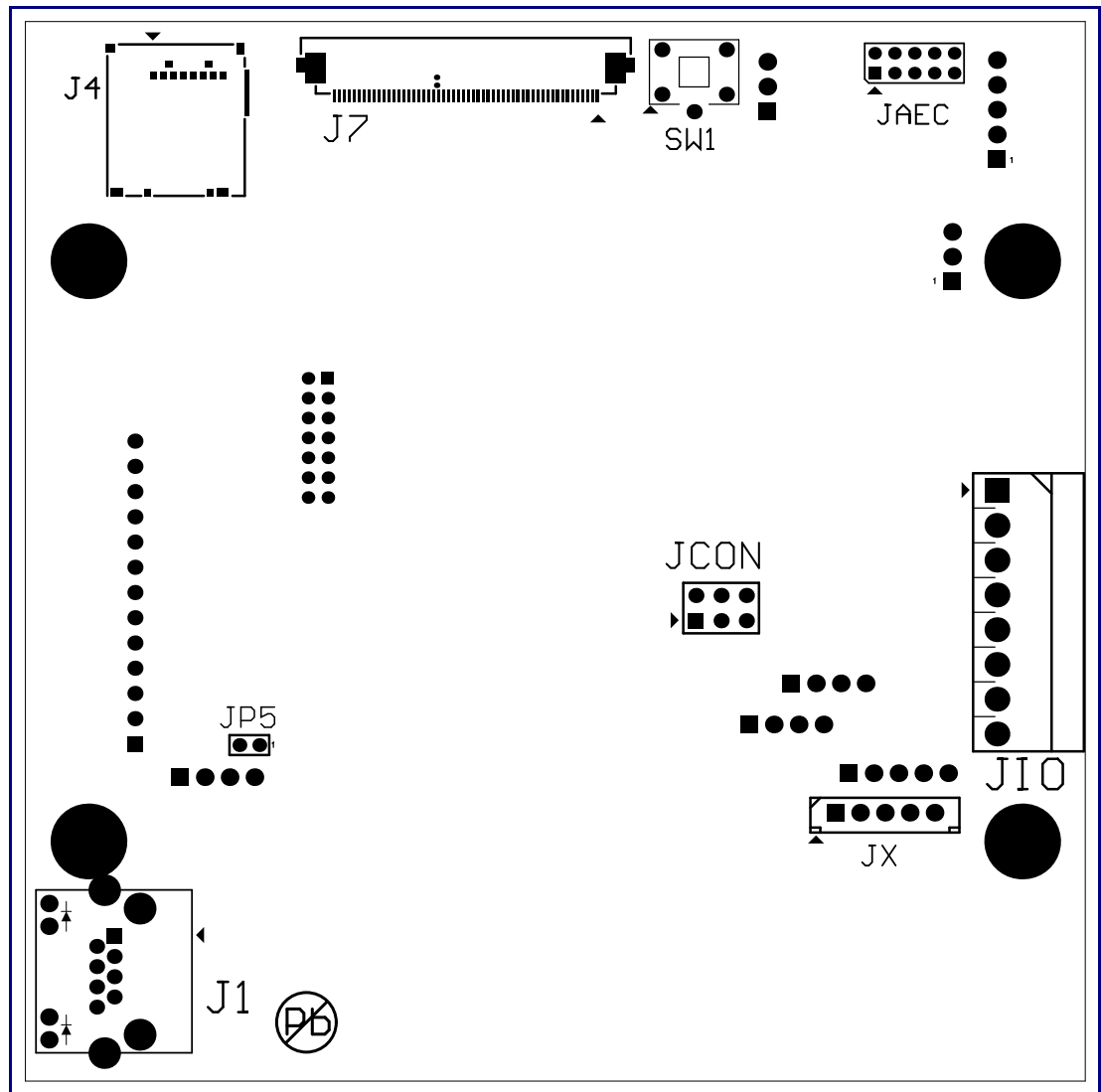
**Figure 2-9. Connector Locations—Board Top**



**Table 2-2. Connector Functions—Board Top**

| <b>Connector</b> | <b>Function</b>                                   |
|------------------|---|
| JBTN             | Call Button LED Interface                         |
| JMIC             | Microphone Interface                              |
| JMIC2            | Second Microphone Interface (Not Used)            |
| JSPKR            | Speaker Interface                                 |
| JKPAD            | Keypad Interface (Not Used)                       |
| JUSB             | USB Interface (Not Used)                          |
| JZ               | I <sup>2</sup> C 5V Peripheral Bus                |
| J2               | Biometric Interface (Not Used)                    |
| J3               | JTAG Interface (Not Used)                         |
| J5               | ISP AT-Tiny Interface (Factory Only)              |
| J6               | Digital Microphone Interface (Not Used)           |
| JP3              | Mute Disable Jumper—Jumper should be removed      |
| JP6              | Enable AT-Tiny—Jumper should be installed         |
| JP7              | Enable Write to EEPROM—Jumper should be installed |
| JP10             | Disables the intrusion sensor when installed.     |

Figure 2-10. Connector Locations—Board Bottom



**Table 2-3. Connector Functions—Board Bottom**

| Connector | Function   |
|-----------|--|
| J1        | PoE Network Connection (RJ-45 ethernet)          |
| J4        | SD Card Slot                                     |
| JAEC      | AEC Configuration Interface (Factory Use Only)   |
| JCON      | Console Port (Factory Use Only)                  |
| JIO       | Terminal Block (see <a href="#">Figure 2-2</a> ) |
| JP5       | Reset jumper <sup>a</sup>                        |
| JX        | Auxiliary Strobe Connector                       |
| SW1       | See <a href="#">Section 2.3.7, "RTFM Button"</a> |

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

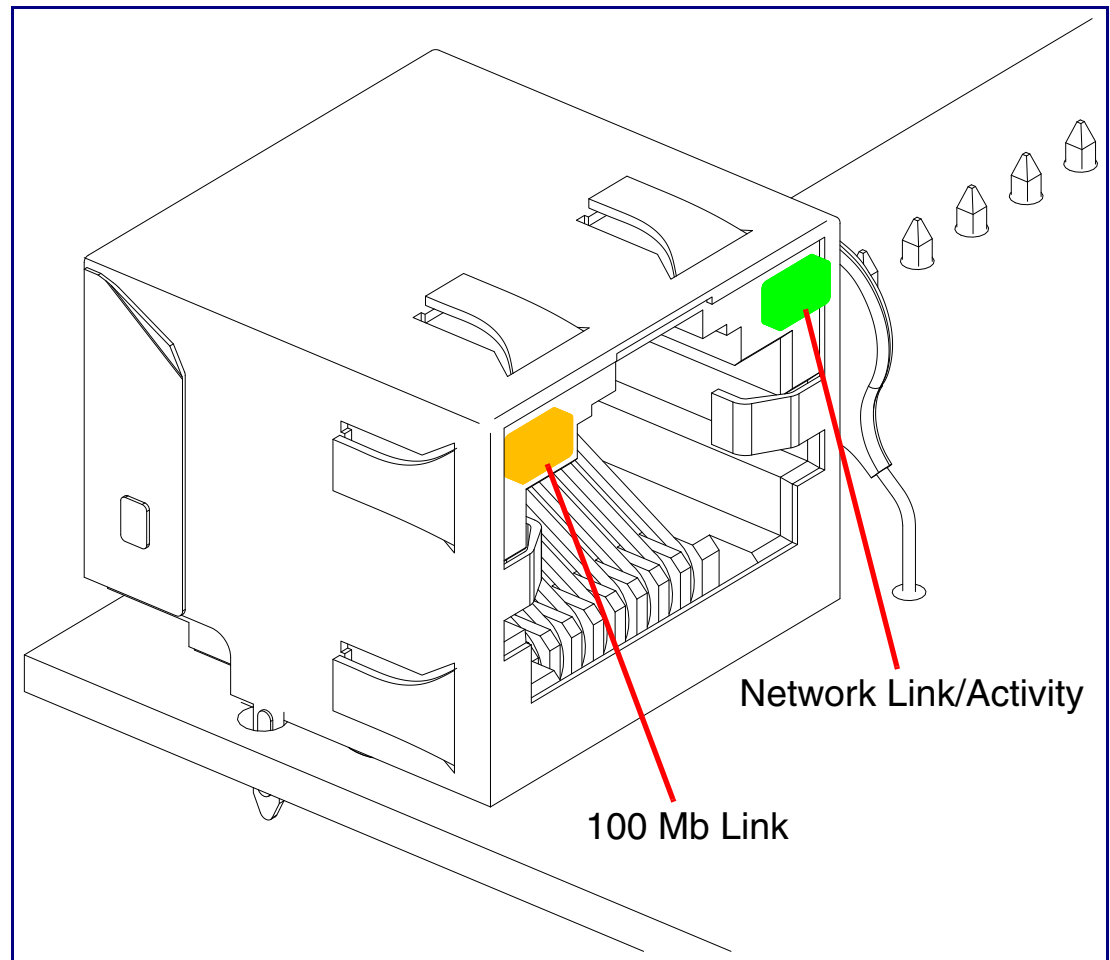
## 2.3.6 Activity and Link LEDs

### 2.3.6.1 Verifying the Network Connectivity and Data Rate

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

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

**Figure 2-11. Activity and Link LED**



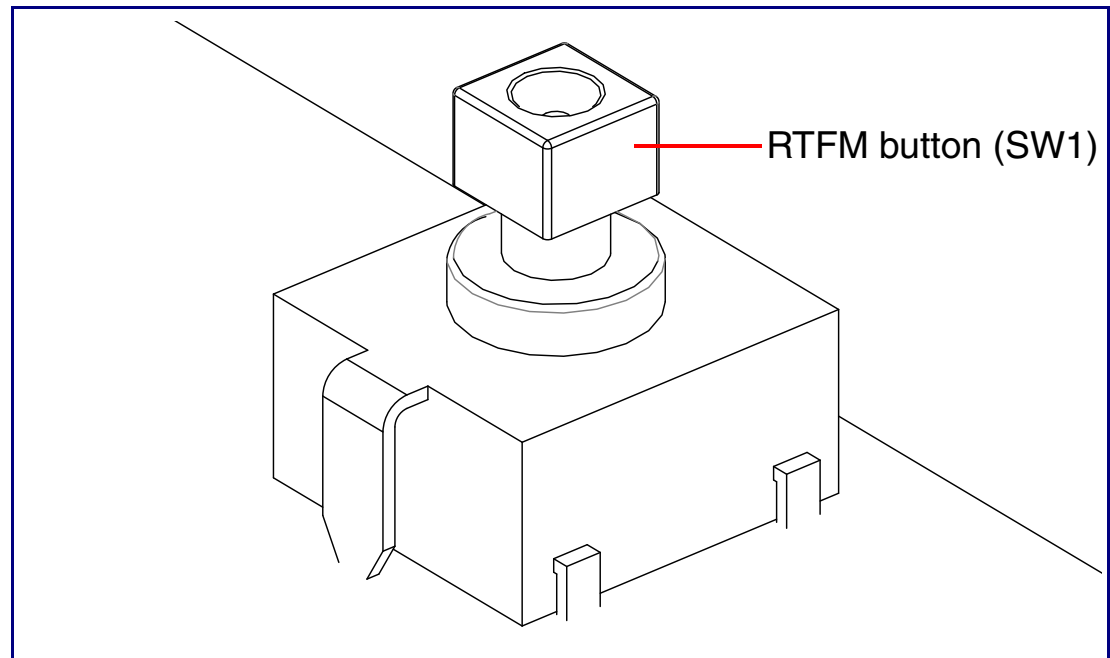
---

## 2.3.7 RTFM Button

When the Intercom is operational and linked to the network, you can use the Reset Test Function Management (**RTFM**) button (see **SW1** in [Figure 2-12](#)) on the Intercom board to announce and confirm the Intercom's IP Address and test to see if the audio is working.

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

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



### 2.3.7.1 Announcing the IP Address

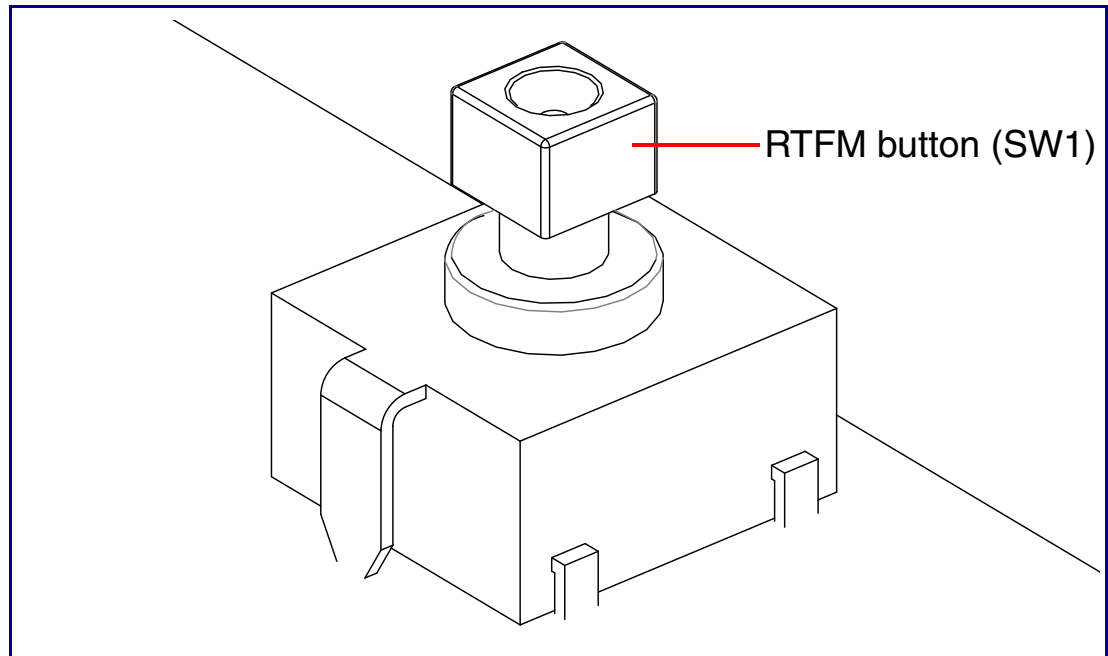
To announce a device's current IP address:

1. Press and release the RTFM button (see **SW1** in [Figure 2-13](#)) within a five second window.

**Note** The device will use DHCP to obtain the new IP address (DHCP-assigned address or default to IPv4 Link Local if a DHCP server is not present).

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

**Figure 2-13. RTFM Button (SW1)**



### 2.3.7.2 Restoring the Factory Default Settings

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

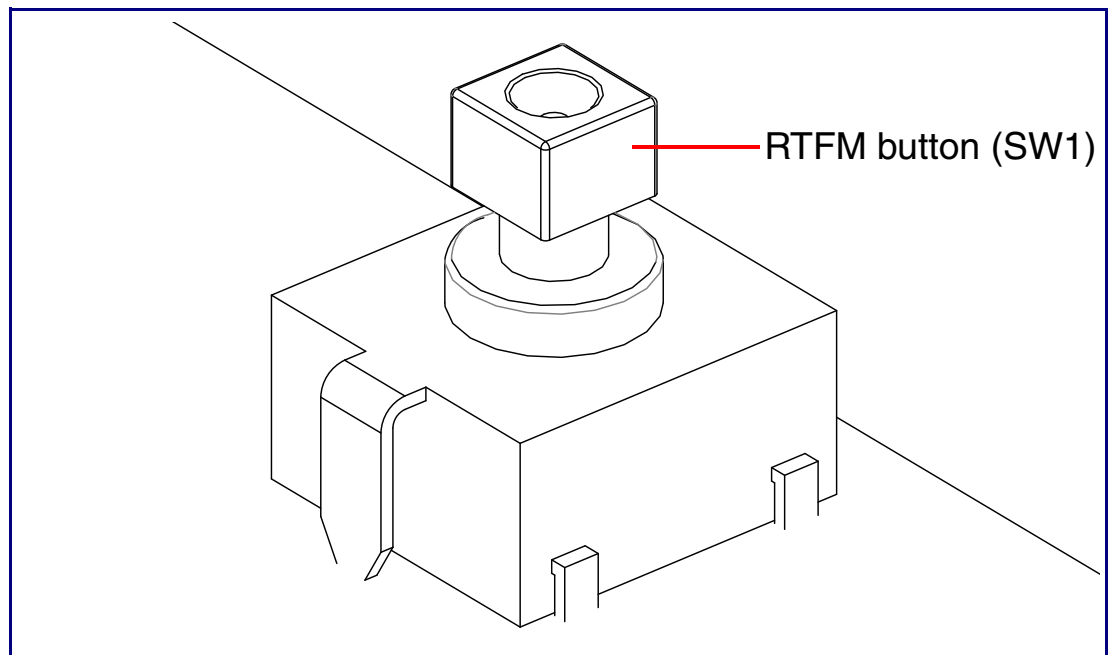
**Note** Each Intercom is delivered with factory set default values.

To restore the factory default settings:

1. Press and hold the **RTFM button** (see **SW1** in [Figure 2-14](#)) for more than five seconds.
2. The device announces that it is restoring the factory default settings.

**Note** The device will use DHCP to obtain the new IP address (DHCP-assigned address or default to IPv4 Link Local if a DHCP server is not present).

**Figure 2-14. RTFM Button (SW1)**



---

### 2.3.8 Adjusting the Intercom Volume

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



## 2.3.9 Call Button and the Call Button LED

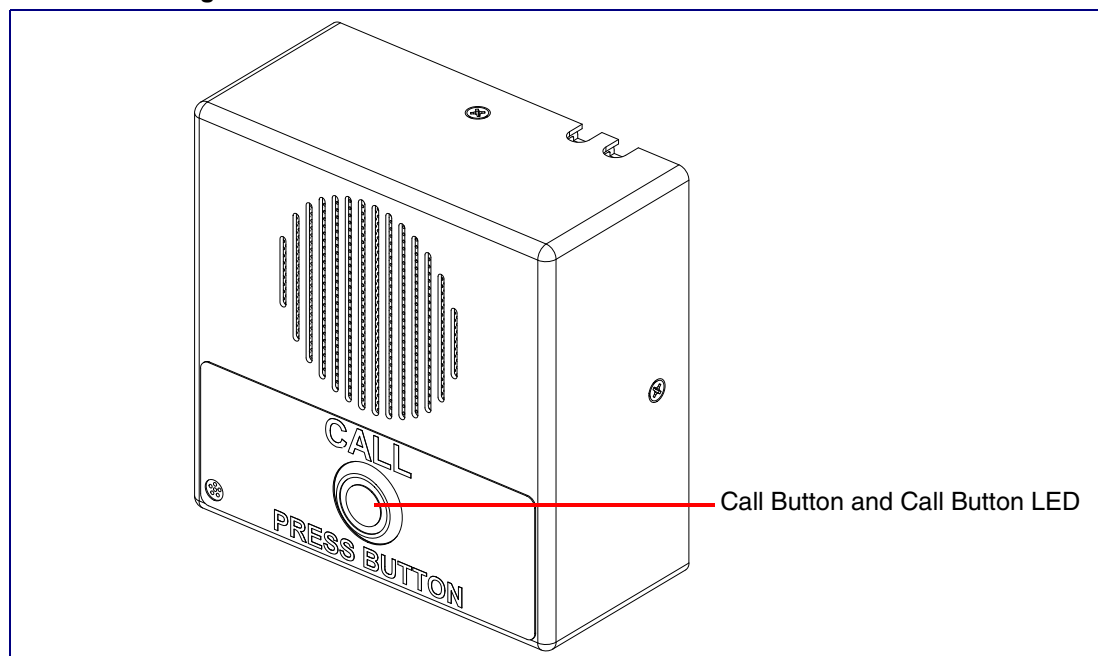
### 2.3.9.1 Calling with the The Call Button

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

### 2.3.9.2 Call Button LED Function

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

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



---

## 2.4 Configure the Intercom Parameters

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

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

---

### 2.4.1 Factory Default Settings

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

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

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

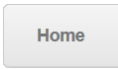
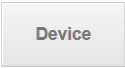
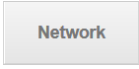



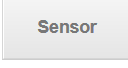
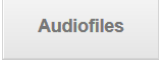
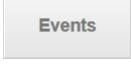

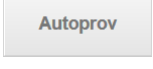
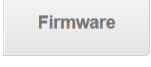
| Parameter                    | Factory Default Setting |
|------------------------------|-------------------------|
| IP Addressing                | DHCP                    |
| IP Address <sup>a</sup>      | IPv4 Link Local         |
| Web Access Username          | admin                   |
| Web Access Password          | admin                   |
| Subnet Mask <sup>a</sup>     | IPv4 Link Local         |
| Default Gateway <sup>a</sup> | IPv4 Link Local         |

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

## 2.4.2 Intercom Web Page Navigation

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

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

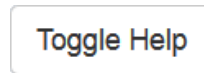
| Web Page Item   | Description                                |
|---|--|
|    | Link to the <b>Home</b> page.              |
|    | Link to the <b>Device</b> page.            |
|    | Link to the <b>Network</b> page.           |
|    | Link to go to the <b>SIP</b> page.         |
|    | Link to the <b>SSL</b> page.               |
|   | Link to the <b>Multicast</b> page.         |
|  | Link to the <b>Sensor</b> page.            |
|  | Link to the <b>Audiofiles</b> page.        |
|  | Link to the <b>Events</b> page.            |
|  | Link to the <b>Door Strike Relay</b> page. |
|  | Link to the <b>Autoprovisioning</b> page.  |
|  | Link to the <b>Firmware</b> page.          |

## 2.4.3 Using the Toggle Help Button

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

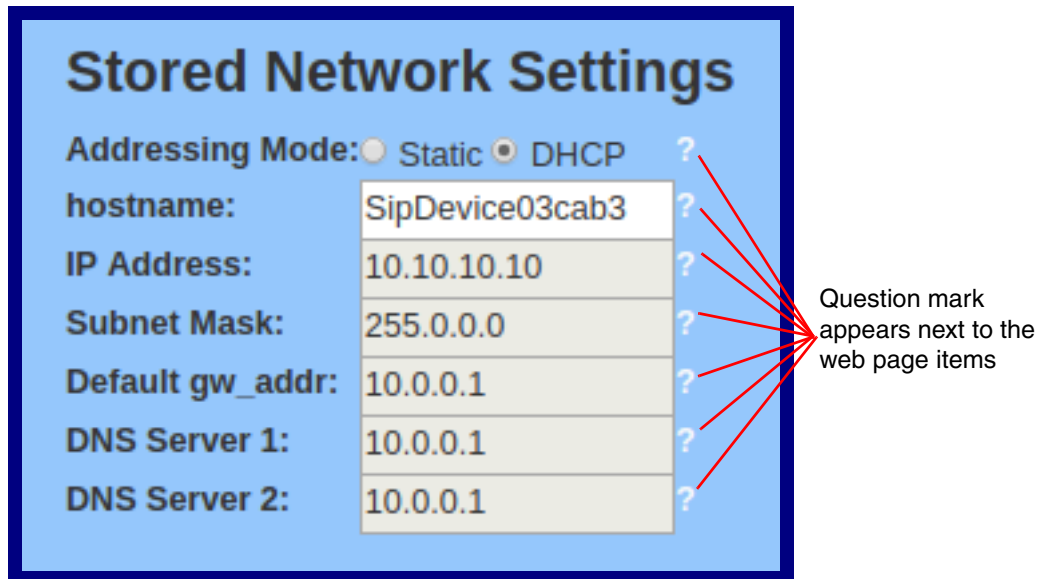
1. Click on the **Toggle Help** button that is on the UI webpage. See [Figure 2-16](#) and [Figure 2-17](#).

**Figure 2-16. Toggle/Help Button**



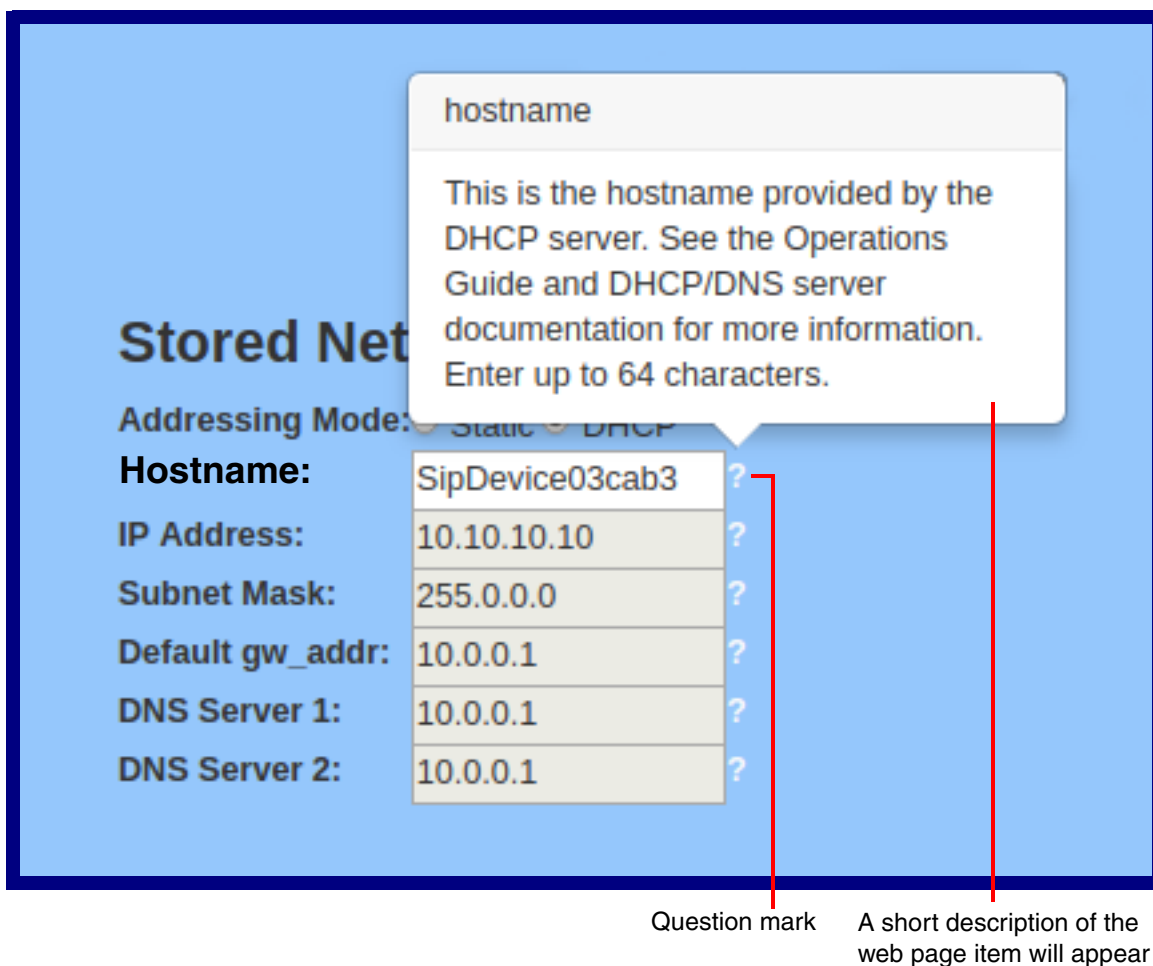
2. You will see a question mark (?) appear next to each web page item that has been provided with a short description by the Help feature. See [Figure 2-17](#).

**Figure 2-17. Toggle Help Button and Question Marks**



3. Move the mouse pointer to hover over the question mark (?), and a short description of the web page item will appear. See [Figure 2-18](#).

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



---

## 2.4.4 Log in to the 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 IPv4 Link Local.

**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:

<https://www.cyberdata.net/pages/discovery>

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

2. When prompted, use the following default **Web Access Username** and **Web Access Password** to access the **Home Page** (Figure 2-19):

Web Access Username: **admin**

Web Access Password: **admin**

Figure 2-19. Home Page

HomeDeviceNetworkSIPSSLMulticastSensorAudiofilesEventsDSRAutoprovFirmware

CyberData Intercom

Device Status

Serial Number:211200001  
Mac Address:00:20:f7:03:fb:79  
Firmware Version:v20.4.1  
Partition 2:v20.4.1  
Partition 3:v20.4.1  
Bootling From:partition 3

Boot From Other Partition

IP Addressing:DHCP  
IP Address:10.10.0.95  
Subnet Mask:255.0.0.0  
Default Gateway:10.0.0.1  
DNS Server 1:10.0.1.56  
DNS Server 2:

SIP Volume:4  
Multicast Volume:4  
Ring Volume:4  
Sensor Volume:4  
Push to Talk Volume:4  
Microphone Gain:4  
Push to Talk Microphone Gain:4

SIP Mode:Enabled  
Multicast Mode:Disabled  
Event Reporting:Disabled

Primary SIP Server:Not registered  
Backup Server 1:Not registered  
Backup Server 2:Not registered  
Nightringer Server:Not registered

Sensor Status

Relay Status:Locked  
Door Status:Closed  
Intrusion:Closed

Admin Settings

Username:admin  
Password:\*\*\*\*\*  
Confirm Password:\*\*\*\*\*

SaveRebootToggle Help

Import Settings

Browse...No file chosen

Import Config

Export Settings

Export Config

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







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

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

| Web Page Item  | Description   |
|--|---|
| <b>Admin Settings</b>  |   |
| Username ?   | The username to access the web interface. Enter up to 25 characters.      |
| Password ?   | The password to access the web interface. Enter up to 25 characters.      |
| Confirm Password ?   | Confirm the web interface password.                                       |
| <b>Device Status</b>   |   |
| Serial Number  | Shows the device serial number.   |
| Mac Address  | Shows the device Mac address.   |
| Firmware Version   | Shows the current firmware version.                                       |
| Partition 2  | Contains a complete copy of bootable software.                            |
| Partition 3  | Contains an alternate, complete copy of bootable software.                |
| Bootting From  | Indicates the partition currently used for boot.                          |
|  | Allows the user to boot from the alternate partition.                     |
| IP Addressing  | Shows the current IP addressing setting ( <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.                                   |
| SIP Volume   | Shows the current SIP volume level.                                       |
| Multicast Volume   | Shows the current Multicast volume level.                                 |
| Ring Volume  | Shows the current Ring volume level.                                      |
| Sensor Volume  | Shows the current Sensor volume level.                                    |
| Push to Talk Volume  | Shows the current push to talk volume                                     |
| Microphone Gain  | Shows the current microphone gain level.                                  |
| Push to Talk Microphone Gain   | Shows the current push to talk microphone gain level.                     |
| SIP Mode   | Shows the current status of the SIP mode.                                 |
| Multicast Mode   | Shows the current status of the Multicast mode.                           |
| Event Reporting  | Shows the current status of the Event Reporting mode.                     |
| Nightringer  | Shows the current status of the Nightringer mode.                         |
| Primary SIP Server   | Shows the current status of the Primary SIP Server.                       |
| Backup Server 1  | Shows the current status of Backup Server 1.                              |
| Backup Server 2  | Shows the current status of Backup Server 2.                              |



**Table 2-6. Home Page Overview (continued)**

| Web Page Item   | Description   |
|---|---|
| Nightringer Server  | Shows the current status of Nightringer Server.   |
| <b>Sensor Status</b>  |   |
| Relay Status  | Shows the current status of the door when the Home Page is refreshed.   |
| Door Status   | Shows the current status of the relay when the Home Page is refreshed.  |
| Intrusion   | Shows the current status of the intrusion sensor when the Home Page is refreshed.   |
| <b>Import Settings</b>  |   |
|    | Use this button to select a configuration file to import.   |
|    | After selecting a configuration file, click Import to import the configuration from the selected file.  |
| <b>Export Settings</b>  |   |
|    | Click Export to export the current configuration to a file.   |
|    | Click the <b>Save</b> button to save your configuration settings.   |
|   | Click on the <b>Reboot</b> button to reboot the system.   |
|  | Click on the <b>Toggle Help</b> button to see a short description of some of the web page items. First click on the <b>Toggle Help</b> button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item. |

## 2.4.5 Configure the Device

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

**Figure 2-20. Device Configuration Page**

**CyberData Intercom**

**Volume Settings (0-9)**

SIP Volume:

Multicast Volume:

Ring Volume:

Sensor Volume:

Push to Talk Volume:

**Microphone Settings (0-9)**

Microphone Gain:

Push to Talk Microphone Gain:

**Relay Settings**

Activate Relay with DTMF code: ☒

Relay Pulse Code:

Relay Pulse Duration (in seconds):

Relay Activation Code:

Relay Deactivation Code:

Play tone during DTMF Activation: ☐

Activate Relay During Ring: ☐

Activate Relay During Night Ring: ☐

Activate Relay While Call Active: ☐

Activate Relay On Button Press: ☐

Relay On Button Press Duration:

**Clock Settings**

Enable NTP: ☒

NTP Server:

Timezone:

Current Time: Fri, 21 Sep 2018 15:01:59

**Misc Settings**

Device Name:

Auto-Answer Incoming Calls: ☒

Button Lit when Idle: ☒

Button Brightness (0-255):

Play Ringback Tone: ☐

Enable Push to Talk: ☐

Enable DTMF Push to Talk: ☐

Prevent Call Termination: ☐

Disable HTTPS (NOT recommended): ☐

**Buttons:** Save, Reboot, Toggle Help, Test Audio, Test Microphone, Test Relay

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

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




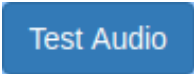






**Table 2-7. Device Configuration Parameters**

| Web Page Item                   | Description   |
|---------------------------------|---|
| <b>Volume Settings (0-9)</b>    |   |
| SIP Volume ?                    | Set the speaker volume for a SIP call. A value of 0 will mute the speaker during SIP calls.   |
| Multicast Volume ?              | Set the speaker volume for multicast audio streams. A value of 0 will mute the speaker during multicasts.   |
| Ring Volume ?                   | Set the ring volume for incoming calls. A value of 0 will mute the speaker instead of playing the ring tone when Auto-Answer Incoming Calls is disabled.  |
| Sensor Volume ?                 | Set the speaker volume for playing sensor activated audio. A value of 0 will mute the speaker during sensor activated audio.  |
| Push to Talk Volume ?           | Set the speaker volume for Push to Talk operation. A value of 0 will mute the speaker in Push to Talk mode.   |
| <b>Microphone Settings</b>      |   |
| Microphone Gain ?               | Set the microphone gain level.  |
| Push to Talk Microphone Gain ?  | Set the microphone gain level for Push to Talk operation.   |
| <b>Clock Settings</b>           |   |
| Enable NTP ?                    | Sync device's local time with the specified NTP Server.   |
| NTP Server ?                    | Use this field to set the address (in IPv4 dotted decimal notation or as a canonical name) for the NTP Server. This field can accept canonical names of up to 64 characters in length.  |
| Timezone                        | Enter the tz database string of your timezone.<br><br>Examples:<br>America/Los_Angeles<br>America/New_York<br>Europe/London<br>America/Toronto<br><br>See <a href="https://en.wikipedia.org/wiki/List_of_tz_database_time_zones">https://en.wikipedia.org/wiki/List_of_tz_database_time_zones</a> for a full list of valid strings. |
| Current Time                    | Displays the current time.  |
| <b>Relay Settings</b>           |   |
| Activate Relay with DTMF Code ? | Activates the relay when the DTMF Activation Code is entered on the phone during a SIP call with the device. RFC2833 DTMF payload types are supported.  |
| Relay Pulse Code ?              | DTMF code used to pulse the relay when entered on a phone during a SIP call with the device. Relay will activate for Relay Pulse Duration seconds then deactivate. Activate Relay with DTMF Code must be enabled. Enter up to 25 digits (* and # are supported).  |

**Table 2-7. Device Configuration Parameters (continued)**

| Web Page Item                       | Description   |
|-------------------------------------|---|
| Relay Pulse Duration (in seconds) ? | The length of time (in seconds) during which the relay will be activated when the DTMF Relay Activation Code is detected. Enter up to 5 digits.   |
| Relay Activation Code ?             | Activation code used to activate the relay when entered on a phone during a SIP call with the device. Relay will be active indefinitely, or until the DTMF Relay Deactivation code is entered. Activate Relay with DTMF Code must be enabled. Enter up to 25 digits (* and # are supported).  |
| Relay Deactivation Code ?           | Code used to deactivate the relay when entered on a phone during a SIP call with the device. Activate Relay with DTMF Code must be enabled. Enter up to 25 digits (* and # are supported).  |
| Play tone during DTMF Activation ?  | When selected, the device will play a tone out of the speaker upon DTMF relay activation. The tone plays for the DTMF Activation Duration (in seconds).   |
| Activate Relay During Ring ?        | When selected, the relay will be activated for as long as the device is ringing. When Auto-Answer Incoming Calls is enabled, the device will not ring and this option does nothing.   |
| Activate Relay During Night Ring ?  | When selected, the relay will be activated as long as the Nightringer extension is ringing.   |
| Activate Relay While Call Active ?  | When selected, the relay will be activated as long as the SIP call is active.   |
| Activate Relay on Button Press ?    | When selected, the relay will be activated when the Call button is pressed.   |
| Relay on Button Press Duration ?    | The length of time (in seconds) during which the relay will be activated when the Call button is pressed. Enter up to 5 digits. A <b>Relay on Button Press Duration</b> value of 0 will pulse the relay once when the Call button is pressed.   |
| <b>Misc Settings</b>                |   |
| Device Name ?                       | Type the device name. Enter up to 25 characters.  |
| Auto-Answer Incoming Calls ?        | When selected, the device will automatically answer incoming calls. When Auto-Answer Incoming Calls is disabled, the device will play a ring tone (corresponds to Ring Tone on the Audiofiles page) out of the speaker until someone presses the Call button to answer the call or the caller disconnects before the call can be answered.                  |
| Button Lit When Idle ?              | When selected, the Call button LED is illuminated while the device is idle (a call is not in progress).   |
| Button Brightness (0-255) ?         | The desired Call button LED brightness level. Acceptable values are 0-255, where 0 is the dimmest and 255 is the brightest. Enter up to three digits.   |
| Play Ringback Tone ?                | When selected, the device will play a ringback tone (corresponds to Ringback Tone on the Audiofiles page) out of the speaker while placing an outbound call. The Ringback Tone will play until the call is answered.  |
| Enable Push to Talk ?               | This option is for noisy environments. When enabled, the microphone will be muted normally. When the Call button is pressed and held, it will unmute the microphone and allow the operator to send audio back. Using Push to Talk prevents the operator from terminating a call by pressing the Call button. The call must be terminated by the phone user. |

**Table 2-7. Device Configuration Parameters (continued)**

| Web Page Item   | Description   |
|---|---|
| Enable DTMF Push to Talk         | <p>This option is for noisy environments. When enabled, in an active call, the remote phone can force receive only audio (setting the mic gain to max and muting the speaker) by pressing the * key.</p> <p>Pressing the # key will force send only audio (setting the max speaker volume and muting the mic). Pressing the 0 key will restore full duplex operation with the normal microphone and speaker volume.</p>         |
| Prevent Call Termination         | When this option is enabled, a call cannot be terminated using the call button.   |
| Disable HTTPS (NOT recommended)  | <p>Disables the encrypted connection to the webpage. We do not recommend disabling HTTPS for security reasons.</p> <p><b>Note</b> This setting requires a reboot for the changes to take effect.</p>  |
|                                  | 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.   |
|                                  | <p>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:</p> <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>Test Relay</b> button to do a relay test.   |
|                                | Click the <b>Save</b> button to save your configuration settings.   |
|                                | Click on the <b>Reboot</b> button to reboot the system.   |
|                                | Click on the <b>Toggle Help</b> button to see a short description of some of the web page items. First click on the <b>Toggle Help</b> button, and you will see a question mark (  ) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item. |

## 2.4.6 Configure the Network Parameters

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

Figure 2-21. Network Configuration Page

HomeDeviceNetworkSIPSSLMulticastSensorAudiofilesEventsDSRAutoprovFirmware

CyberData Intercom

Stored Network Settings

Addressing Mode: ☐ Static ☒ DHCP

hostname:

IP Address:

Subnet Mask:

Default Gateway:

DNS Server 1:

DNS Server 2:

VLAN Settings

VLAN ID (0-4095):

VLAN Priority (0-7):

Current Network Settings

IP Address: 10.10.1.245

Subnet Mask: 255.0.0.0

Default Gateway: 10.0.0.1

DNS Server 1: 10.0.1.56

DNS Server 2:

Save




Reboot

Toggle Help

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

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

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

| Web Page Item   | Description   |
|---|---|
| <b>Stored Network Settings</b>  |   |
| Addressing Mode ?   | Select either DHCP IP Addressing or Static Addressing by marking the appropriate radio button. DHCP Addressing mode is enabled on default and the device will attempt to resolve network addressing with the local DHCP server upon boot. If DHCP Addressing fails, the device will revert to the last known IP address or the factory default address if no prior DHCP lease was established. See <a href="#">Section 2.4.1, "Factory Default Settings"</a> for factory default settings. Be sure to click <b>Save</b> and <b>Reboot</b> to store changes when configuring a Static address. |
| Hostname ?  | This is the hostname provided by the DHCP server. See the DHCP/DNS server documentation for more information. Enter up to 64 characters.  |
| IP Address ?  | Enter the Static IPv4 network address in dotted decimal notation.   |
| Subnet Mask ?   | Enter the Subnet Mask in dotted decimal notation.   |
| Default Gateway ?   | Enter the Default Gateway IPv4 address in dotted decimal notation.  |
| DNS Server 1 ?  | Enter the primary DNS Server IPv4 address in dotted decimal notation.   |
| DNS Server 2 ?  | Enter the secondary DNS Server IPv4 address in dotted decimal notation.   |
| <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.   |
| <b>VLAN Settings</b>  |   |
| VLAN ID (0-4095) ?  | Specify the IEEE 802.1Q VLAN ID number. Enter up to 4 digits. A value of 0 disables vlan.<br><b>Note:</b> The device supports 802.1Q VLAN tagging support. The switch port connected to the device will need to be in "trunking mode" for the VLAN tags to propagate.   |
| VLAN Priority (0-7) ?   | Specify the IEEE 802.1p VLAN priority level. Enter 1 digit. A value of 0 may cause the VLAN ID tag to be ignored.   |
|  | Click the <b>Save</b> button to save your configuration settings.   |
|  | Click on the <b>Reboot</b> button to reboot the system.   |
|  | Click on the <b>Toggle Help</b> button to see a short description of some of the web page items. First click on the <b>Toggle Help</b> button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.   |

## 2.4.7 Configure the SIP (Session Initiation Protocol) Parameters

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

Figure 2-22. SIP Configuration Page

**SIP Settings**

Enable SIP operation: ☒

Register with a SIP Server: ☒

Primary SIP Server:

Primary SIP User ID:

Primary SIP Auth ID:

Primary SIP Auth Password:

Re-registration Interval (in seconds):

Backup SIP Server 1:

Backup SIP User ID:

Backup SIP Auth ID:

Backup SIP Auth Password:

Re-registration Interval (in seconds):

Backup SIP Server 2:

Backup SIP User ID:

Backup SIP Auth ID:

Backup SIP Auth Password:

Re-registration Interval (in seconds):

Remote SIP Port:

Local SIP Port:

SIP Transport Protocol:

TLS Version:

Verify Server Certificate: ☐

Outbound Proxy:

Outbound Proxy Port:

Use Cisco SRST: ☐

Disable rport Discovery: ☐

Unregister on Boot: ☐

Keep Alive Period:

**Nightringer Settings**

SIP Server:

SIP User ID:

SIP Auth ID:

SIP Auth Password:

Re-registration Interval (in seconds):

**SIP Ring Strobe Settings**

Blink Strobe on Ring: ☐

| Scene | Brightness | Color | Red | Green | Blue |
|-------|------------|-------|-----|-------|------|
| ADA   | 255        | Color | 255 | 255   | 255  |

**SIP Call Strobe Settings**

Blink Strobe during Call: ☐

| Scene | Brightness | Color | Red | Green | Blue |
|-------|------------|-------|-----|-------|------|
| ADA   | 255        | Color | 255 | 255   | 255  |

**MWI Strobe Settings**

Blink Strobe on MWI: ☐

| Scene | Brightness | Color | Red | Green | Blue |
|-------|------------|-------|-----|-------|------|
| ADA   | 255        | Color | 255 | 255   | 255  |

**Nightringer Strobe Settings**

Blink Strobe on Nightring: ☐

| Scene | Brightness | Color | Red | Green | Blue |
|-------|------------|-------|-----|-------|------|
| ADA   | 255        | Color | 255 | 255   | 255  |

**Dial Out Settings**

Dial out Extension:

Extension ID:

Send Multicast Audio: ☐

Multicast Address:

Multicast Port:

Repeat Message:

The strobe settings will only appear if a CyberData Strobe product is connected to your device. If a CyberData Strobe product is not connected to your device, you will not see the strobe settings.



Figure 2-23. SIP Configuration Page

Backup SIP Server 2:  
Backup SIP User ID:  
Backup SIP Auth ID:  
Backup SIP Auth Password:  
Re-registration Interval (in seconds):

Remote SIP Port:  
Local SIP Port:

SIP Transport Protocol:  
TLS Version:  
Verify Server Certificate:

☐

Outbound Proxy:  
Outbound Proxy Port:

Use Cisco SRST:  
Disable rport Discovery:  
Unregister on Boot:  
Keep Alive Period:

☐  
☐  
☐

SIP Call Strobe Settings

Blink Strobe during Call:  
Scene BrightnessColor Red Green Blue  
ADA 255 Color 255 255 255 Preview

MWI Strobe Settings

Blink Strobe on MWI:  
Scene BrightnessColor Red Green Blue  
ADA 255 Color 255 255 255 Preview

Nightringer Strobe Settings

Blink Strobe on Nightring:  
Scene BrightnessColor Red Green Blue  
ADA 255 Color 255 255 255 Preview

Dial Out Settings

Dial out Extension: 204  
Extension ID: id204  
Send Multicast Audio:  
Multicast Address: 224.5.5.5  
Multicast Port: 5050  
Repeat Message: 1

Call Disconnection

Terminate Call after delay: 0

Audio Codec Selection

Codec: Auto Select

RTP Settings

RTP Port (even): 10500  
Asymmetric RTP:  
Jitter Buffer: 50  
RTP Encryption (SRTP): Disabled

Save Reboot Toggle Help

The strobe settings will only appear if a CyberData Strobe product is connected to your device.  
If a CyberData Strobe product is not connected to your device, you will not see the strobe settings.

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

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



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

| Web Page Item                           | Description   |
|---|---|
| <b>SIP Settings</b>                     |   |
| Enable SIP Operation ?                  | When enabled, the device will transmit, receive, and process SIP messages according to the configured SIP settings below.   |
| Register with a SIP Server ?            | When enabled, the device will attempt to register to the configured SIP Server(s) on this page. To configure the device to send and receive point-to-point SIP calls, enable <b>SIP Operation</b> and disable <b>Register with a SIP Server</b> (see <a href="#">Section 2.4.7.2, "Point-to-Point Configuration"</a> ). |
| Primary SIP Server ?                    | Enter the SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the primary SIP server. This field can accept entries of up to 255 characters in length.                         |
| Primary SIP User ID ?                   | Specify the SIP User ID for the Primary SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the primary SIP server. Enter up to 64 alphanumeric characters.  |
| Primary SIP Auth ID ?                   | Specify the Authenticate ID for the Primary SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.   |
| Primary SIP Auth Password ?             | Specify the Authenticate Password for the Primary SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.   |
| Re-registration Interval (in seconds) ? | The SIP Re-registration interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.   |
| Backup SIP Server 1 ?                   | Enter the backup SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the backup SIP server. This field can accept entries of up to 255 characters in length.                   |
| Backup SIP User ID 1 ?                  | Specify the SIP User ID for the first backup SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the first backup SIP server. Enter up to 64 alphanumeric characters.  |
| Backup SIP Auth ID ?                    | Specify the Authenticate ID for the first backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.  |
| Backup SIP Auth Password ?              | Specify the Authenticate Password for the first backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.  |
| Re-registration Interval (in seconds) ? | The SIP Re-registration interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.   |
| Backup SIP Server 2 ?                   | Enter a second backup SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the second backup SIP server. This field can accept entries of up to 255 characters in length.       |
| Backup SIP User ID ?                    | Specify the SIP User ID for the second backup SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the second backup SIP server. Enter up to 64 alphanumeric characters.  |
| Backup SIP Auth ID ?                    | Specify the Authenticate ID for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.   |


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

| Web Page Item                           | Description   |
|---|---|
| Backup SIP Auth Password ?              | Specify the Authenticate Password for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.   |
| Re-registration Interval (in seconds) ? | The SIP Re-registration interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.   |
| Remote SIP Port ?                       | The Remote SIP Port is the port number the device will use as the destination port when sending SIP messages. The default Remote SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.  |
| Local SIP Port ?                        | The Local SIP Port is the port number the device will use to receive SIP messages. The default Local SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.  |
| SIP Transport Protocol ?                | Choose the transport protocol for SIP signaling. This will affect all extensions, including the Nightringer. Default is UDP.  |
| TLS Version ?                           | Choose the TLS version for SIP over TLS. Modern security standards strongly recommend using TLS 1.2.  |
| Verify Server Certificate ?             | When enabled, the device will verify the authenticity of the server during the TLS handshake by its certificate and common name. The TLS handshake will be aborted if the server is deemed to be inauthentic and SIP registration will not proceed.   |
| Outbound Proxy ?                        | Enter the Outbound Proxy address as an IPv4 address in dotted decimal notation or a fully qualified domain name (FQDN). When an IP address is configured, the device will send all SIP messages to this IP address. When an FQDN is configured, the device will run DNS NAPTR, SRV, and A queries on the FQDN to resolve an IP address to which it will send all SIP messages. This field can accept entries of up to 255 characters in length. |
| Outbound Proxy Port ?                   | The Outbound Proxy Port is port number used as the destination port when sending SIP messages to the outbound proxy. A value of 0 will default to 5060. The supported range is 0-65536. Enter up to 5 digits.   |
| Use Cisco SRST ?                        | When enabled, the backup servers are handled according to Cisco SRST (Survivable Remote Site Telephony). It is required for use in clustered Cisco Unified Communications Manager topologies.   |
| Disable rport Discovery ?               | Disabling rport Discovery will prevent the device from including the public WAN IP address and port number in the contact information that is sent to the remote SIP servers. This will generally only need to be enabled when using an SBC or SIP ALG in conjunction with a remote SIP server.   |
| Unregister on Boot ?                    | When enabled, the device will send one registration with an expiry of 0 on boot.  |
| Keep Alive Period ?                     | The minimum time in milliseconds between keep-alive packets sent for nat traversal. A value of 0 will disable keep alive packets.   |
| <b>SIP Ring Strobe Settings</b>         | <b>The following strobe settings will only appear if a CyberData Strobe product is connected to your device. If a CyberData Strobe product is not connected to your device, you will not see the strobe settings.</b>   |
| Blink Strobe on Ring ?                  | When selected, the Strobe will blink a scene when ringing.  |
| Scene ?                                 | Select desired scene (only one may be chosen).  |
| ADA Compliant ?                         | Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.   |
| Slow Fade ?                             | Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.  |


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

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




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

| Web Page Item   | Description   |
|---|---|
| Blink Strobe on MWI ?   | When selected, the strobe will blink a scene when a voicemail is waiting for its extension.   |
| Scene ?   | Select desired scene (only one may be chosen).  |
| ADA Compliant ?   | Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.   |
| Slow Fade ?   | Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.  |
| Fast Fade ?   | Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.  |
| Slow Blink ?  | Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.   |
| Fast Blink ?  | Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.   |
| MWI Call Color ?  | Select desired color (only one may be chosen).  |
| Brightness ?  | How bright the strobe will blink when there is a message waiting. This is the maximum brightness for “fade” type scenes.  |
| Red ?   | The red LED value for MWI.  |
| Green ?   | The green LED value for MWI.  |
| Blue ?  | The blue LED value for MWI.   |
|    | Use this button to preview the strobe flashing behavior for the <b>MWI Strobe Settings</b> .  |
| <b>Nightringer Settings</b>   |   |
| SIP Server ?  | Enter the SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's Nightringer extension on the SIP server. This field can accept entries of up to 255 characters in length. |
| SIP User ID ?   | Specify the SIP User ID for the SIP server. This parameter becomes the user portion of the SIP-URI for the device's Nightringer extension. Enter up to 64 alphanumeric characters.  |
| SIP Auth ID ?   | Specify the Authenticate ID for the SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.   |
| SIP Auth Password ?   | Specify the Authenticate Password for the SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.   |
| Re-registration Interval (in seconds) ?   | The SIP Re-registration Interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.   |
| <b>Nightringer Strobe Settings</b>  |   |
| <b>The following strobe settings will only appear if a CyberData Strobe product is connected to your device. If a CyberData Strobe product is not connected to your device, you will not see the strobe settings.</b> |   |
| Blink Strobe on Nightring ?   | When selected, the Strobe will blink a scene when the Nightringer is ringing.   |
| Scene ?   | Select desired scene (only one may be chosen).  |
| ADA Compliant ?   | Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.   |

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

| Web Page Item   | Description  |
|---|--|
| Slow Fade ?   | Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.   |
| Fast Fade ?   | Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.   |
| Slow Blink ?  | Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.  |
| Fast Blink ?  | Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.  |
| Color ?   | Select desired color (only one may be chosen).   |
| Brightness ?  | How bright the strobe will blink when the Nightringer is ringing. This is the maximum brightness for "fade" type scenes.   |
| Red ?   | The red LED value for Nightringer.   |
| Green ?   | The green LED value for Nightringer.   |
| Blue ?  | The blue LED value for Nightringer.  |
|  | Use this button to preview the strobe flashing behavior for the <b>Nightringer Strobe Settings</b> .   |
| <b>Dial Out Settings</b>  |  |
| Dial Out Extension ?  | Specify the extension the device will call when someone presses the Call button. Enter up to 64 alphanumeric characters.<br><br><b>Note:</b> For information about dial-out extension strings and DTMF tones, see <a href="#">Section 2.4.7.1, "Dial Out Extension Strings and DTMF Tones (using rfc2833)"</a> . |
| Extension ID ?  | A Caller identification string added to outbound calls. Enter up to 64 alphanumeric characters.  |
| Send Multicast Audio ?  | When selected, the device will play an audio file to the specified multicast address and port.   |
| Multicast Address ?   | The multicast address used for multicasting an audio file.   |
| Multicast Port ?  | The multicast port used for multicasting an audio file.  |
| Repeat Message ?  | The number of times to repeat the audio message to the remote endpoint. Enter a value from 1-65536.  |
| <b>Call Disconnection</b>   |  |
| Terminate Call After Delay ?  | Automatically terminate an active call after a given delay in seconds. A value of 0 will disable this function. Enter up to 8 digits.  |
| <b>Audio Codec Selection</b>  |  |
| Codec ?   | Select the desired codec (only one may be chosen).   |
| <b>RTP Settings</b>   |  |
| RTP Port (even) ?   | Specify the port number used for the RTP stream after establishing a SIP call. This port number must be an even number and defaults to 10500. The supported range is 0-65536. Enter up to 5 digits.  |

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

| Web Page Item   | Description  |
|---|--|
| Asymmetric RTP ?  | <p>Specify if the remote endpoint will send and receive RTP packets on different ports. If set to false, the device will track the address/port that is sending RTP packets during a SIP call. If the address/port changes mid-stream, the device will disregard the SDP and send all further RTP packets to this new address.</p> <p>If set to true, this device will ignore the sending address/port and send RTP as specified in the SDP. Warning! Enabling asymmetric RTP can cause the RTP stream to be lost.</p> <p>Most installations should not enable asymmetric RTP.</p> |
| Jitter Buffer ?   | Specify the size of the jitter buffer (in milliseconds) used for SIP calls. Valid values are 50-1000.  |
| RTP Encryption (SRTP) ?   | When enabled, a SIP call's audio streams are encrypted using SRTP.   |
|  | Click the <b>Save</b> button to save your configuration settings.  |
|  | Click on the <b>Reboot</b> button to reboot the system.  |
|  | Click on the <b>Toggle Help</b> button to see a short description of some of the web page items. First click on the <b>Toggle Help</b> button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.  |

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

#### 2.4.7.1 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.

## 2.4.7.2 Point-to-Point Configuration

When the device is set to not register with a SIP server (see [Figure 2-24](#)), it is possible to set the device to dial out to a single endpoint.

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

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

**Figure 2-24. SIP Page Set to Point-to-Point Mode**

The screenshot shows the 'SIP' configuration page for a CyberData Intercom. The top navigation bar includes tabs for Home, Device, Network, SIP (selected), SSL, Multicast, Sensor, Audiofiles, Events, DSR, Autoprov, and Firmware. The main header reads 'CyberData Intercom'. Below this, there are three main sections: 'SIP Settings', 'Nightringer Settings', and 'SIP Ring Strobe Settings'. In the 'SIP Settings' section, 'Enable SIP operation' is checked with a blue checkbox, and 'Register with a SIP Server' is unchecked with a white checkbox. Below these are input fields for 'Primary SIP Server' (0.0.0.0.253), 'Primary SIP User ID' (99), 'Primary SIP Auth ID' (99), 'Primary SIP Auth Password' (\*\*\*\*\*), and 'Re-registration Interval (in seconds)' (360). The 'Nightringer Settings' section includes input fields for 'SIP Server' (Host or IP address), 'SIP User ID' (User ID), 'SIP Auth ID' (Auth ID), 'SIP Auth Password' (Password), and 'Re-registration Interval (in seconds)' (360). The 'SIP Ring Strobe Settings' section is currently empty.

Device is set to NOT register with a SIP server

## 2.4.7.3 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**

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

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



## 2.4.8 Configure the SSL Parameters

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

Figure 2-25. SSL Configuration Page

Home Device Network SIP **SSL** Multicast Sensor Audiofiles Events DSR Autoprovision Firmware

# CyberData Intercom

### Web Server Certificate

```

subject=
countryName           = US
stateOrProvinceName   = California
localityName          = Monterey
organizationName       = Cyberdata
commonName             = 0020f703fb79
notBefore=Aug 26 22:36:09 2020 GMT
notAfter=Aug 24 22:36:09 2030 GMT

```

Browse... No file chosen

Import Web Certificate

Restore Web Certificate

### SIP Client Certificate

```

subject=
countryName           = US
stateOrProvinceName   = California
localityName          = Monterey
organizationName       = Cyberdata
commonName             = 0020f703fb79
notBefore=Aug 26 22:36:09 2020 GMT
notAfter=Aug 24 22:36:09 2030 GMT

```

Browse... No file chosen

Import SIP Certificate

Restore SIP Certificate

Password (optional):

### Autoprovisioning Client Certificate

```

subject=
countryName           = US
stateOrProvinceName   = California
localityName          = Monterey
organizationName       = Cyberdata
commonName             = 0020f703fb79
notBefore=Aug 26 22:36:09 2020 GMT
notAfter=Aug 24 22:36:09 2030 GMT

```

Browse... No file chosen

Import Autoprovisioning Certificate

Restore Autoprovisioning Certificate

Password (optional):

Download Cyberdata CA Save Reboot Toggle Help

### Test TLS Connection

Server: 10.0.0.253 Port: 5060 Test SIP Connection Test Autoprovision Connection

### List of Trusted CAs

Upload CA Certificate: Browse... No file chosen Import CA Certificate Remove All Restore Defaults

|   |                                 |      |        |
|---|---------------------------------|------|--------|
| 1 | CyberData_CA.pem                | Info | Remove |
| 2 | DigiCert_Assured_ID_Root_CA.crt | Info | Remove |
| 3 | DigiCert_Assured_ID_Root_G2.crt | Info | Remove |
| 4 | DigiCert_Assured_ID_Root_G3.crt | Info | Remove |
| 5 | DigiCert_Global_Root_CA.crt     | Info | Remove |
| 6 | DigiCert_Global_Root_G2.crt     | Info | Remove |

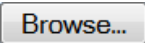


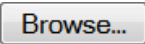


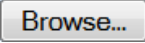
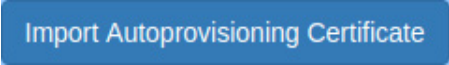
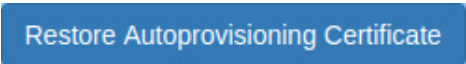
**Figure 2-26. SSL Configuration Page**

|    |  | Info | Remove |
|----|--|------|--------|
| 7  | DigiCert_Global_Root_G3.crt                                      | Info | Remove |
| 8  | DigiCert_High_Assurance_EV_Root_CA.crt                           | Info | Remove |
| 9  | DigiCert_Trusted_Root_G4.crt                                     | Info | Remove |
| 10 | GeoTrust_Global_CA.crt   | Info | Remove |
| 11 | GeoTrust_Primary_Certification_Authority.crt                     | Info | Remove |
| 12 | GeoTrust_Primary_Certification_Authority_-_G2.crt                | Info | Remove |
| 13 | GeoTrust_Primary_Certification_Authority_-_G3.crt                | Info | Remove |
| 14 | GeoTrust_Universal_CA.crt  | Info | Remove |
| 15 | GeoTrust_Universal_CA_2.crt                                      | Info | Remove |
| 16 | Go_Daddy_Class_2_CA.pem  | Info | Remove |
| 17 | Go_Daddy_Root_Certificate_Authority_-_G2.pem                     | Info | Remove |
| 18 | VeriSign_Class_3_Public_Primary_Certification_Authority_-_G4.crt | Info | Remove |
| 19 | VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5.crt | Info | Remove |
| 20 | VeriSign_Universal_Root_Certification_Authority.crt              | Info | Remove |
| 21 | Verisign_Class_1_Public_Primary_Certification_Authority.crt      | Info | Remove |
| 22 | Verisign_Class_1_Public_Primary_Certification_Authority_-_G3.crt | Info | Remove |
| 23 | Verisign_Class_2_Public_Primary_Certification_Authority_-_G2.crt | Info | Remove |
| 24 | Verisign_Class_2_Public_Primary_Certification_Authority_-_G3.crt | Info | Remove |
| 25 | Verisign_Class_3_Public_Primary_Certification_Authority.crt      | Info | Remove |
| 26 | Verisign_Class_3_Public_Primary_Certification_Authority_-_G3.crt | Info | Remove |
| 27 | thawte_Primary_Root_CA.crt                                       | Info | Remove |
| 28 | thawte_Primary_Root_CA_-_G2.crt                                  | Info | Remove |
| 29 | thawte_Primary_Root_CA_-_G3.crt                                  | Info | Remove |









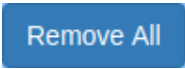

2. On the **SSL** page, enter values for the parameters indicated in [Table 2-12](#).

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

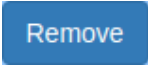
**Table 2-12. SSL Configuration Parameters**

| Web Page Item   | Description   |
|---|---|
| <b>Web Server Certificate</b>   | Certificate used by the web server.   |
|    | Click <b>Browse</b> to select a certificate to import.  |
|    | After selecting a certificate, click <b>Import Web Certificate</b> to import it as the certificate used by this device's web server.  |
|    | Restore the device's default web server certificate. This will remove the user-uploaded Web Server Certificate.(Server CAs and Trusted CAs are unaffected).   |
| <b>SIP Client Certificate</b>   | When doing mutual authentication this device will present a client certificate with these parameters.   |
|    | Click <b>Browse</b> to select a certificate to import.  |
|   | After selecting a certificate, click <b>Import SIP Certificate</b> to import it as the certificate used by the device during SIP transactions.  |
|  | Restore the device's default sip client certificate. This will remove any user-uploaded sip client certificates (Server CAs and Trusted CAs are unaffected).  |
| Optional Password   | Enter the optional password for the SIP certificate's private key.<br><b>Note:</b> When using a password, it must be entered and saved before importing the certificate.                                |
| <b>Autoprovisioning Client Certificate</b>  | When doing mutual authentication this device will present a client certificate with these parameters.   |
|  | Click <b>Browse</b> to select a certificate to import.  |
|  | After selecting a certificate, click <b>Import Autoprovisioning Certificate</b> to import it as this device's certificate. This certificate will be used when requesting files during autoprovisioning. |
|  | Restore the device's default autoprovisioning certificate. This will remove any user-uploaded autoprovisioning certificates. (Server CAs and Trusted CAs are unaffected).                               |
| Optional Password ?   | Enter the optional password for the Autoprovisioning certificate's private key.<br><b>Note:</b> When using a password, it must be entered and saved before importing the certificate.                   |
| Cyberdata CA ?  | Right click and <b>Save Link As...</b> to get the Cyberdata CA used to sign this client certificate.  |

**Table 2-12. SSL Configuration Parameters (continued)**

| Web Page Item   | Description   |
|---|---|
|    | Click the <b>Save</b> button to save your configuration settings.   |
|    | Click on the <b>Reboot</b> button to reboot the system.   |
|    | Click on the <b>Toggle Help</b> button to see a short description of some of the web page items. First click on the <b>Toggle Help</b> button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item. |
| <b>Test TLS Connection</b>  |   |
| Server ?  | The ssl test server address as a fully qualified domain name or in IPv4 dotted decimal notation.  |
| Port ?  | The supported range is 0-65536. SIP connections over TLS to port 5060 are modified to connect to port 5061. This test button will do the same.  |
|    | Use this button to test a TLS connection to a remote server using the sip client key and password. This will attempt to make a socket connection to the configured test server and port and report the success or failure. This can be used to debug TLS connection issues separate from SIP registration issues.                           |
|  | Use this button to test a TLS connection to a remote server using the autoprovisioning client key and password. This will attempt to make a socket connection to the configured test server and port and report the success or failure. This can be used to debug TLS connection issues with secure autoprovisioning.                       |
| <b>List of Trusted CAs</b>  |   |
|  | Use this button to select a configuration file to import.   |
|  | Click <b>Browse</b> to select a CA certificate to import. After selecting a server certificate authority (CA), click <b>Import CA Certificate</b> to import it to the list of trusted CAs. CAs are used to validate the certificate presented by the server when establishing a TLS connection.   |
|  | <b>Restore Defaults</b> will restore the default list of registered CAs and <b>Remove All</b> will remove all registered CAs.   |
|  | <b>Restore Defaults</b> will restore the default list of registered CAs and <b>Remove All</b> will remove all registered CAs.   |
|  | Provides details of the certificate. After clicking on this button, the <b>Certificate Info Window</b> appears. See <a href="#">Section 2.4.8.1, "Certificate Info Window"</a> .  |

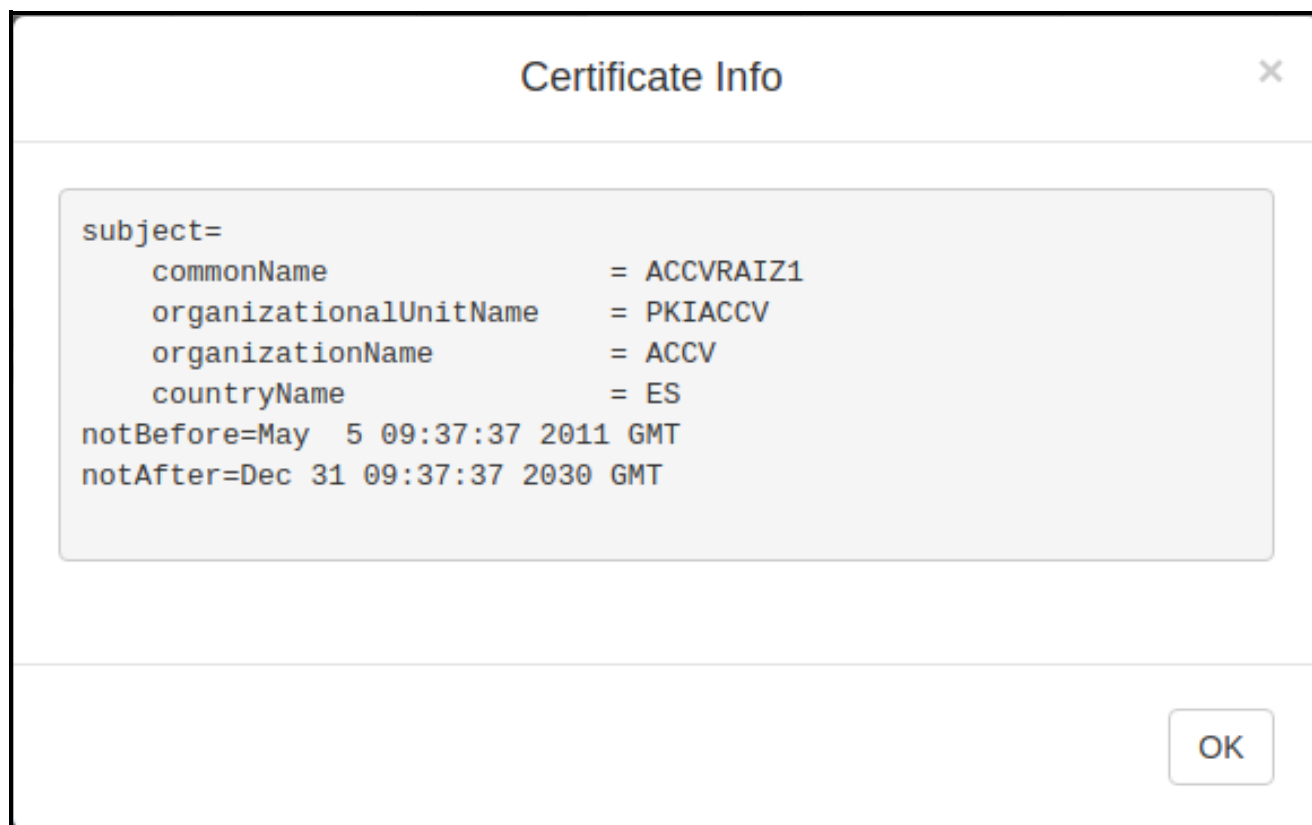
**Table 2-12. SSL Configuration Parameters (continued)**

| Web Page Item   | Description   |
|---|---|
|  | Removes this certificate from the list of trusted certificates. After clicking on this button, the <b>Remove Server Certificate Window</b> appears. See <a href="#">Section 2.4.8.2, "Remove Server Certificate Window"</a> . |

### 2.4.8.1 Certificate Info Window

The **Certificate Info Window** provides details of the certificate. This window appears after clicking on the **Info** button. See [Figure 2-27](#).

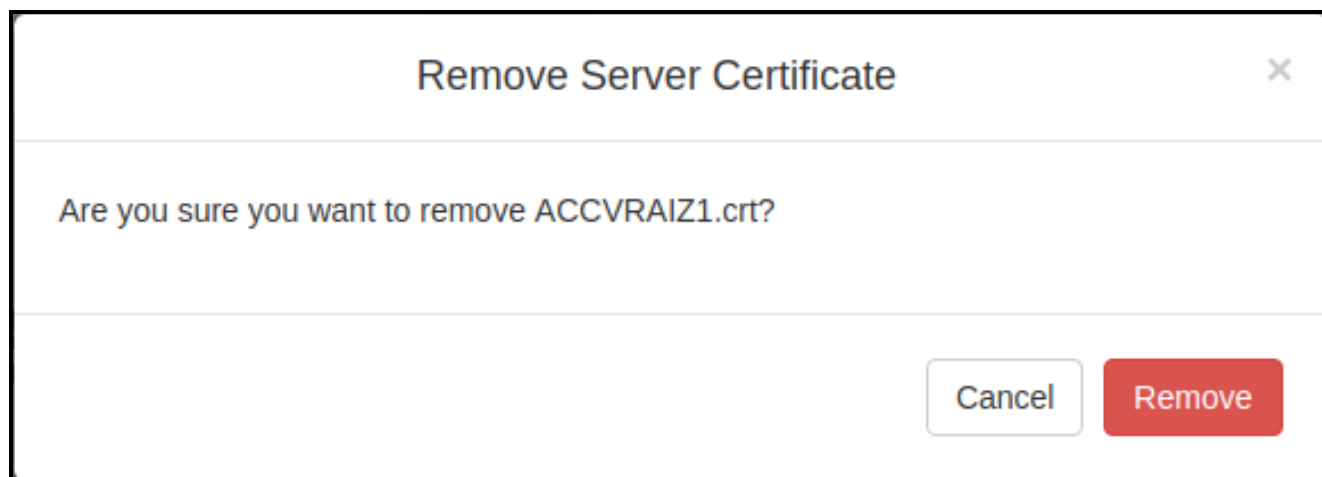
**Figure 2-27. Certificate Info Window**



### 2.4.8.2 Remove Server Certificate Window

The **Remove Server Certificate Window** will ask if the user wants to remove a certificate from the list of trusted certificates. This window appears after clicking on the **Remove** button. See [Figure 2-28](#).

**Figure 2-28. Remove Server Certificate Window**



## 2.4.9 Configure the Multicast Parameters

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

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

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

1. Click on the **Multicast** menu button to open the **Multicast** page. See [Figure 2-29](#).

**Figure 2-29. Multicast Configuration Page**

**CyberData Intercom**

**Multicast Settings**

Enable Multicast Operation: ☒

| Priority | Address      | Port  | Name             | Beep                     | Relay                    | Scene        | Brightness | Color   | Red | Green | Blue |         |
|----------|--------------|-------|------------------|--------------------------|--------------------------|--------------|------------|---------|-----|-------|------|---------|
| 0        | 239.168.3.1  | 2000  | Background Music | <input type="checkbox"/> | <input type="checkbox"/> | Slow Fade ▾  | 255        | Color ▾ | 255 | 255   | 255  | Preview |
| 1        | 239.168.3.2  | 3000  | MG1              | <input type="checkbox"/> | <input type="checkbox"/> | Fast Fade ▾  | 25         | White   |     |       | 0    | Preview |
| 2        | 239.168.3.3  | 4000  | MG2              | <input type="checkbox"/> | <input type="checkbox"/> | Slow Blink ▾ | 125        | Yellow  |     |       | 0    | Preview |
| 3        | 239.168.3.4  | 5000  | MG3              | <input type="checkbox"/> | <input type="checkbox"/> | Fast Blink ▾ | 240        | Orange  |     |       |      | Preview |
| 4        | 239.168.3.5  | 6000  | MG4              | <input type="checkbox"/> | <input type="checkbox"/> | Fast Fade ▾  | 80         | Red     |     |       | 128  | Preview |
| 5        | 239.168.3.6  | 7000  | MG5              | <input type="checkbox"/> | <input type="checkbox"/> | Slow Blink ▾ | 15         | Pink    |     |       | 255  | Preview |
| 6        | 239.168.3.7  | 8000  | MG6              | <input type="checkbox"/> | <input type="checkbox"/> | Off ▾        | 255        | Purple  |     |       | 60   | Preview |
| 7        | 239.168.3.8  | 9000  | MG7              | <input type="checkbox"/> | <input type="checkbox"/> | Slow Fade ▾  | 35         | Blue    |     |       | 255  | Preview |
| 8        | 239.168.3.9  | 10000 | MG8              | <input type="checkbox"/> | <input type="checkbox"/> | Fast Blink ▾ | 255        | Teal    |     |       |      | Preview |
| 9        | 239.168.3.10 | 11000 | Emergency        | <input type="checkbox"/> | <input type="checkbox"/> | ADA ▾        | 255        | Green   |     |       | 0    | Preview |
|          |              |       |                  | <input type="checkbox"/> | <input type="checkbox"/> |              |            | Lime    |     |       | 0    | Preview |
|          |              |       |                  | <input type="checkbox"/> | <input type="checkbox"/> |              |            | Color ▾ | 255 | 255   | 255  | Preview |

Polycom Default Channel   
 Polycom Priority Channel   
 Polycom Emergency Channel

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

Save Reboot

The strobe settings will only appear if a CyberData Strobe product is connected to your device.

If a CyberData Strobe product is not connected to your device, you will not see the strobe settings.

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




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

**Table 2-13. Multicast Page Parameters**

| Web Page Item              | Description   |
|----------------------------|---|
| Enable Multicast Operation | Enables or disables multicast operation.  |
| Priority                   | Indicates the priority for the multicast group. Priority <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 2.4.9.1, "Assigning Priority"</a> for more details. |
| Address                    | Enter the multicast IP Address for this multicast group (15 character limit).   |
| Port                       | Enter the port number for this multicast group (5 character limit [range can be from 2000 to 65535]).<br><br><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.  |
| Relay                      | When selected, the device will activate a relay before multicast audio is sent.   |
| Scene ?                    | Select desired scene (only one may be chosen).<br><br><b>Note: The strobe settings will only appear if you are using the Strobe Kit. If you are not using the Strobe Kit, you will not see the strobe settings.</b>   |
| ADA Compliant ?            | Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.   |
| Slow Fade ?                | Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.  |
| Fast Fade ?                | Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.  |
| Slow Blink ?               | Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.   |
| Fast Blink ?               | Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.   |
| Color ?                    | Select desired color (only one may be chosen).  |
| Brightness ?               | How bright the strobe will blink on a multicast page. This is the maximum brightness for "fade" type scenes.  |
| Red ?                      | The red LED value for Multicast.  |
| Green ?                    | The green LED value for Multicast.  |
| Blue ?                     | The blue LED value for Multicast.   |
| Polycom Default Channel    | When a default Polycom channel/group number is selected, the device will subscribe to the default channel for one-way group pages. Group Numbers 1-25 are supported. Or, select <b>Disabled</b> to disable this channel.  |
| Polycom Priority Channel   | When a priority Polycom channel/group number is selected, the device will subscribe to the priority channel for one-way group pages. Group Numbers 1-25 are supported. Or, select <b>Disabled</b> to disable this channel.  |



**Table 2-13. Multicast Page Parameters (continued)**

| Web Page Item   | Description   |
|---|---|
| Polycom Emergency Channel   | When an emergency Polycom channel/group number is selected, the device will subscribe to the default channel for one-way group pages. Group Numbers 1-25 are supported. Or, select <b>Disabled</b> to disable this channel. |
|  | Use this button to preview the strobe flashing behavior for the <b>Multicast Strobe Settings</b> .  |
|  | Click the <b>Save</b> button to save your configuration settings.   |
|  | Click on the <b>Reboot</b> button to reboot the system.   |

### 2.4.9.1 Assigning Priority

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

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

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

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

Ringtones and  
Nightringtones

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

## 2.4.10 Configure the Sensor Configuration Parameters

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

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

Each sensor can trigger up to five different actions:

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

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

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

Figure 2-30. Sensor Configuration Page

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

# CyberData Intercom

### Door Sensor Settings

Door Sensor Normally Closed: ☐ Yes ☒ No

Door Open Timeout (in seconds):

Flash Button LED: ☐

Activate Relay: ☐

Play Audio Locally: ☐

Make call to extension: ☐

Dial Out Extension:

Dial Out ID:

Play recorded audio: ☐

Repeat Sensor Message:

### Intrusion Sensor Settings

Flash Button LED: ☐

Activate Relay: ☐

Play Audio Locally: ☐

Make call to extension: ☐

Dial Out Extension:

Dial Out ID:

Play recorded audio: ☐

Repeat Intrusion Message:

### Intrusion Strobe Settings

Blink Strobe on Intrusion: ☐

| Scene | Brightness | Color | Red | Green | Blue |
|-------|------------|-------|-----|-------|------|
| ADA   | 255        | Color | 255 | 255   | 255  |

Preview

The strobe settings will only appear if a CyberData Strobe product is connected to your device. If a CyberData Strobe product is not connected to your device, you will not see the strobe settings.

Save Reboot Toggle Help

Test Door Sensor Test Intrusion Sensor


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

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






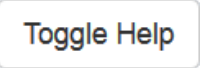
**Table 2-14. Sensor Configuration Parameters**

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

**Table 2-14. Sensor Configuration Parameters (continued)**

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

**Table 2-14. Sensor Configuration Parameters (continued)**

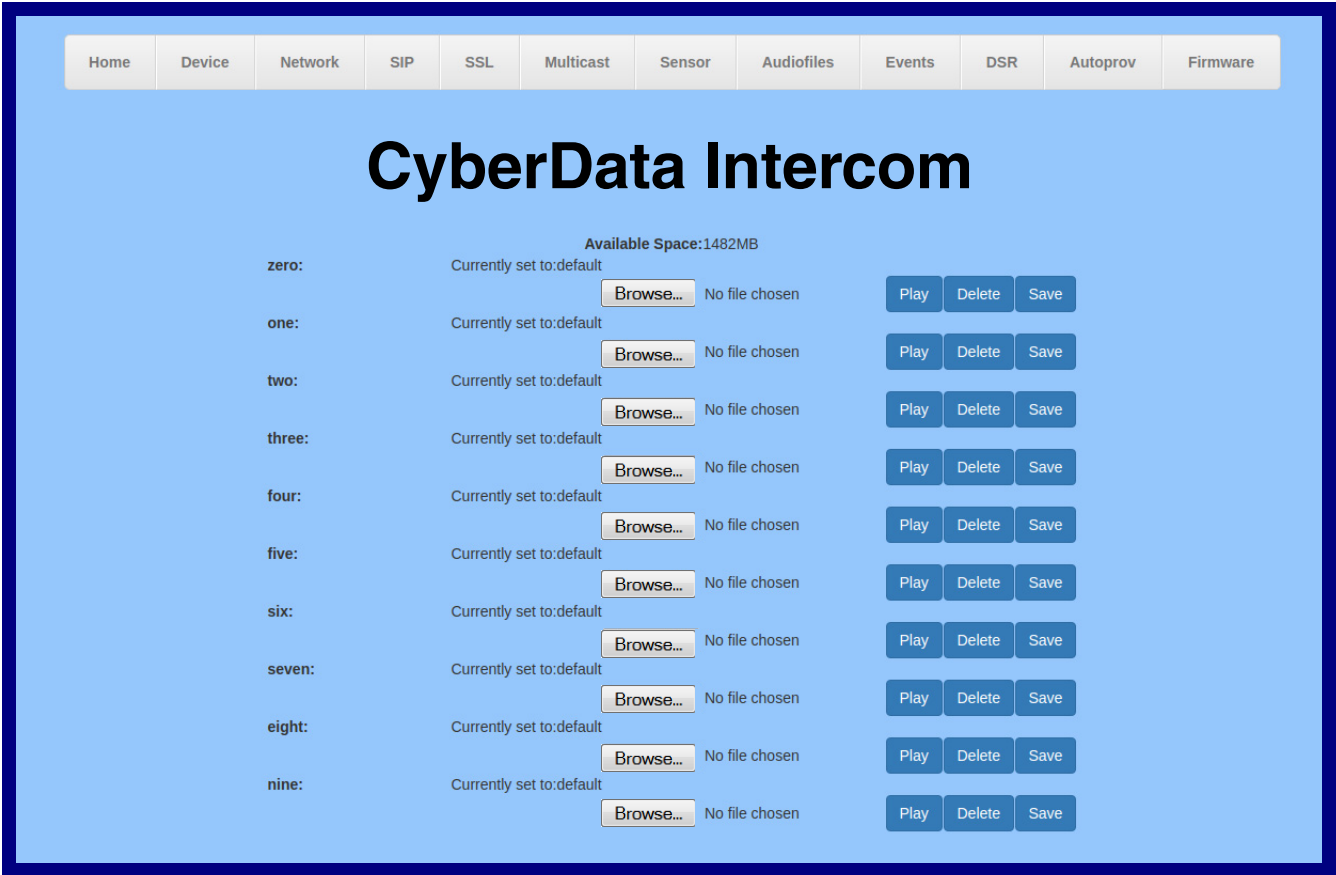
| Web Page Item   | Description   |
|---|---|
| Slow Fade ?   | Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.  |
| Fast Fade ?   | Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.  |
| Slow Blink ?  | Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.   |
| Fast Blink ?  | Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.   |
| Color ?   | Select desired color (only one may be chosen).  |
| Brightness ?  | How bright the strobe will blink when the intrusion sensor is triggered. This is the maximum brightness for "fade" type scenes.   |
| Red ?   | The red LED value for the Intrusion Sensor.   |
| Green ?   | The green LED value for the Intrusion Sensor.   |
| Blue ?  | The blue LED value for the Intrusion Sensor.  |
|    | Use this button to preview the strobe flashing behavior for the <b>Intrusion Sensor Strobe Settings</b> .   |
|  | Click the <b>Test Door Sensor</b> button to test the door sensor.   |
|  | Click the <b>Test Intrusion Sensor</b> button to test the Intrusion sensor.   |
|  | Click the <b>Save</b> button to save your configuration settings.   |
|  | Click on the <b>Reboot</b> button to reboot the system.   |
|  | Click on the <b>Toggle Help</b> button to see a short description of some of the web page items. First click on the <b>Toggle Help</b> button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item. |

## 2.4.11 Configure the Audio Configuration Parameters

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

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

Figure 2-31. Audiofiles Configuration Page



**Figure 2-32. Audiofiles Page**

|                                  |                          |  |                |                                     |                                       |                                     |
|----------------------------------|--------------------------|--|----------------|-------------------------------------|---------------------------------------|-------------------------------------|
| <b>dot:</b>                      | Currently set to:default | <input type="button" value="Browse..."/> | No file chosen | <input type="button" value="Play"/> | <input type="button" value="Delete"/> | <input type="button" value="Save"/> |
| <b>audiotest:</b>                | Currently set to:default | <input type="button" value="Browse..."/> | No file chosen | <input type="button" value="Play"/> | <input type="button" value="Delete"/> | <input type="button" value="Save"/> |
| <b>pagetone:</b>                 | Currently set to:default | <input type="button" value="Browse..."/> | No file chosen | <input type="button" value="Play"/> | <input type="button" value="Delete"/> | <input type="button" value="Save"/> |
| <b>youripaddressis:</b>          | Currently set to:default | <input type="button" value="Browse..."/> | No file chosen | <input type="button" value="Play"/> | <input type="button" value="Delete"/> | <input type="button" value="Save"/> |
| <b>rebooting:</b>                | Currently set to:default | <input type="button" value="Browse..."/> | No file chosen | <input type="button" value="Play"/> | <input type="button" value="Delete"/> | <input type="button" value="Save"/> |
| <b>restoringdefault:</b>         | Currently set to:default | <input type="button" value="Browse..."/> | No file chosen | <input type="button" value="Play"/> | <input type="button" value="Delete"/> | <input type="button" value="Save"/> |
| <b>ringback:</b>                 | Currently set to:default | <input type="button" value="Browse..."/> | No file chosen | <input type="button" value="Play"/> | <input type="button" value="Delete"/> | <input type="button" value="Save"/> |
| <b>ringtone:</b>                 | Currently set to:default | <input type="button" value="Browse..."/> | No file chosen | <input type="button" value="Play"/> | <input type="button" value="Delete"/> | <input type="button" value="Save"/> |
| <b>intrusionsensortriggered:</b> | Currently set to:default | <input type="button" value="Browse..."/> | No file chosen | <input type="button" value="Play"/> | <input type="button" value="Delete"/> | <input type="button" value="Save"/> |
| <b>doorajar:</b>                 | Currently set to:default | <input type="button" value="Browse..."/> | No file chosen | <input type="button" value="Play"/> | <input type="button" value="Delete"/> | <input type="button" value="Save"/> |
| <b>nightring:</b>                | Currently set to:default | <input type="button" value="Browse..."/> | No file chosen | <input type="button" value="Play"/> | <input type="button" value="Delete"/> | <input type="button" value="Save"/> |
| <b>sipmcast:</b>                 | Currently set to:default | <input type="button" value="Browse..."/> | No file chosen | <input type="button" value="Play"/> | <input type="button" value="Delete"/> | <input type="button" value="Save"/> |



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

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

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

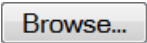


| Web Page Item   | Description  |
|---|--|
| Available Space   | Shows the space available for the user to save custom audio files if they want to change the message when the door or sensor is triggered.   |
| 0-9   | The name of the audio configuration option is the same as the spoken audio that plays on the board (24 character limit).<br><br>'0' corresponds to the spoken word "zero."<br>'1' corresponds to the spoken word "one."<br>'2' corresponds to the spoken word "two."<br>'3' corresponds to the spoken word "three."<br>'4' corresponds to the spoken word "four."<br>'5' corresponds to the spoken word "five."<br>'6' corresponds to the spoken word "six."<br>'7' corresponds to the spoken word "seven."<br>'8' corresponds to the spoken word "eight."<br>'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).  |
| youripaddressis   | Corresponds to the message "Your IP address is..." (24 character limit).   |
| rebooting   | Corresponds to the spoken word "Rebooting" (24 character limit).   |
| restoringdefault  | Corresponds to the message "Restoring default" (24 character limit).   |
| ringback  | This is the ringback tone that plays when calling a remote extension (24 character limit).   |
| ringtone  | This is the tone that plays when set to ring when receiving a call (24 character limit).   |
| intrusionsensortriggered  | Corresponds to the message "Intrusion Sensor Triggered" (24 character limit).  |
| doorajar  | Corresponds to the message "Door Ajar" (24 character limit).   |
| nightring   | Specifies the ringtone for nightring. By default this parameter uses the same audio file that is selected for the <b>Ring Tone</b> parameter.  |
| sipmcast  | This is the message that plays when multicast audio is initiated by the call button.   |
|  | Click on the <b>Browse</b> button to navigate to and select an audio file.   |
|  | The <b>Play</b> button will play that audio file.  |

Table 2-15. Audiofiles Configuration Parameters (continued)

| Web Page Item   | Description   |
|---|---|
|  | 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. |

2.4.11.1 User-created Audio Files

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

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

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

Figure 2-33. Audacity 1

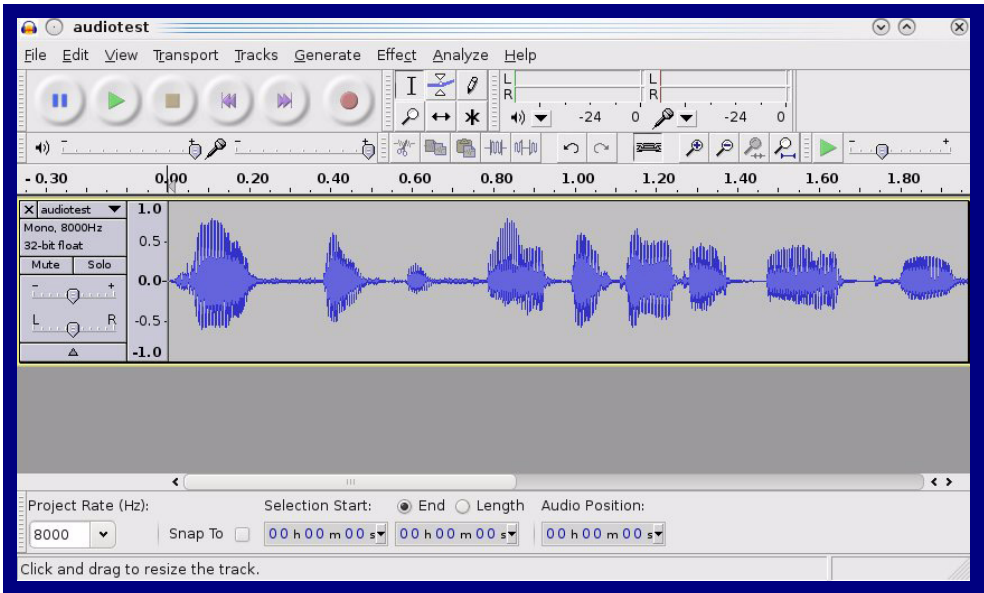
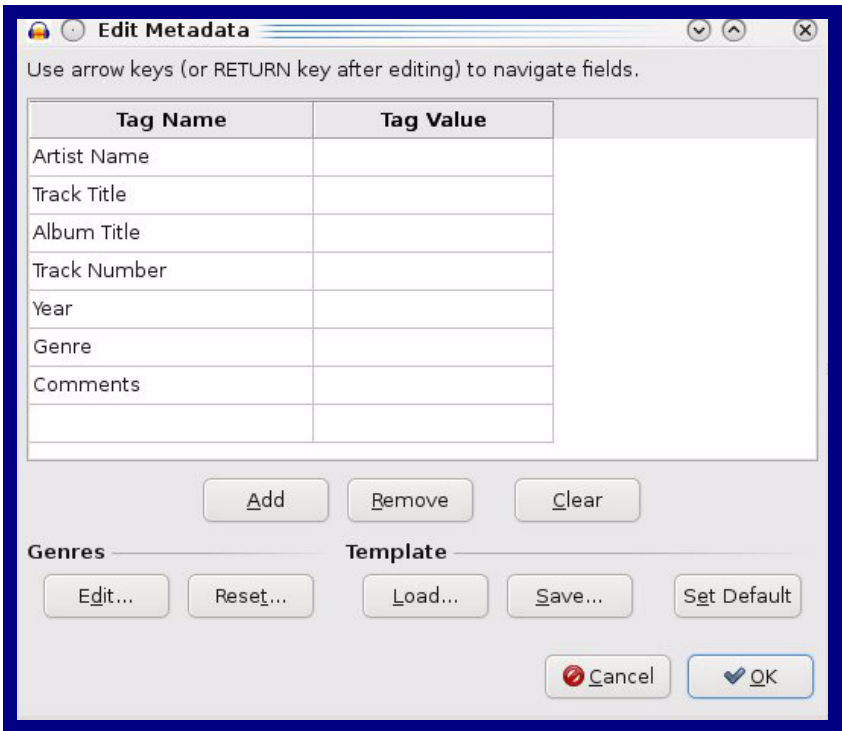


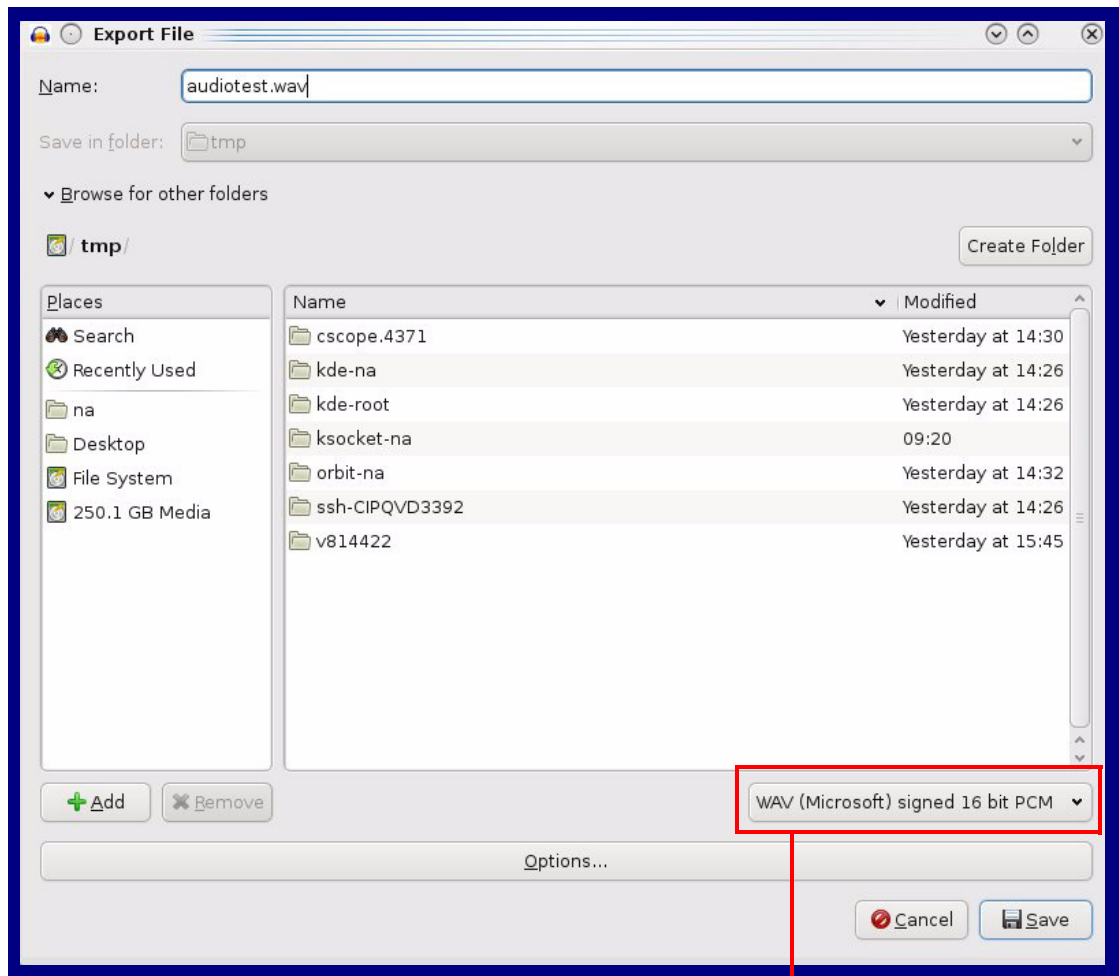
Figure 2-34. Audacity 2



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

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

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



WAV (Microsoft) signed 16 bit PCM

## 2.4.12 Configure the Events Parameters

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

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

Figure 2-36. Event Configuration Page

HomeDeviceNetworkSIPSSLMulticastSensorAudiofilesEventsDSRAutoprovFirmware

CyberData Intercom

Enable Event Generation: ☐

Events

Enable Button Events:

Enable Call Start Events:

Enable Call Terminated Events:

Enable Relay Activated Events:

Enable Relay Deactivated Events:

Enable Ring Events:

Enable Night Ring Events:

Enable Multicast Start Events:

Enable Multicast Stop Events:

Enable Power On Events:

Enable Sensor Events:

Enable Remote Relay Events:

Enable Security Events:

Enable 60 Second Heartbeat:

Event Server

Server IP Address:

10.0.0.250

Server Port:

8080

Server URL:

xmlparse\_engine

Save

Reboot

Toggle Help






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

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

**Table 2-16. Events Configuration Parameters**

| Web Page Item                       | Description   |
|-------------------------------------|---|
| Enable Event Generation ?           | The device will send HTTP POST events to the specified remote server and port number whenever a certain action takes place. Select an event type below to generate an HTTP POST event.  |
| <b>Events</b>                       |   |
| Enable Button Events ?              | When selected, the device will report Call button presses.  |
| Enable Call Start Events ?          | When selected, the device will report the start of a SIP call.  |
| Enable Call Terminated Events ?     | When selected, the device will report the end of a SIP call.  |
| Enable Relay Activated Events ?     | When selected, the device will report relay activation.   |
| Enable Relay Deactivated Events ?   | When selected, the device will report relay deactivation.   |
| Enable Ring Events ?                | When selected, the device will report when it starts ringing upon an incoming SIP call. A Ring Event will not be generated when <b>Auto-Answer Incoming Calls</b> is enabled on the <b>Device</b> page.   |
| Enable Night Ring Events ?          | When selected, the device will report when it starts ringing upon an incoming SIP call to the Nightringer extension. As a reminder, the Nightringer extension always rings upon an incoming SIP call and it is not possible to alter this behavior. |
| Enable Multicast Start Events ?     | When selected, the device will report when the device starts playing a multicast audio stream.  |
| Enable Multicast Stop Events ?      | When selected, the device will report when the device stops playing a multicast audio stream.   |
| Enable Power On Events ?            | When selected, the device will report when it boots.  |
| Enable Sensor Events ?              | When selected, the device will report when the on-board sensor is activated.  |
| Enable Remote Relay Events ?        | When selected, the device will report when the remote relay (DSR) is activated.   |
| Enable Security Events ?            | When enabled, the device will report when the intrusion sensor is activated.  |
| Enable 60 Second Heartbeat Events ? | When enabled, the device will report a Heartbeat event every 60 seconds. SIP registration is not required to generate Heartbeat events.   |
| Check All                           | Click on <b>Check All</b> to select all of the events on the page.  |
| Uncheck All                         | Click on <b>Uncheck All</b> to de-select all of the events on the page.   |
| <b>Event Server</b>                 |   |
| Server IP Address ?                 | The IPv4 address of the event server in dotted decimal notation.  |
| Server Port ?                       | Specify the event server port number. The supported range is 0-65536. Enter up to 5 digits.   |

**Table 2-16. Events Configuration Parameters(continued)**

| Web Page Item  | Description   |
|--|---|
| Server URL  | Generally, the destination URL is the name of the application that receives the events and the string in the HTTP POST command. It can be a script used to parse and process the HTTP POST events. Enter up to 127 characters.  |
|             | Click the <b>Save</b> button to save your configuration settings.   |
|             | Click on the <b>Reboot</b> button to reboot the system.   |
|             | Click on the <b>Toggle Help</b> button to see a short description of some of the web page items. First click on the <b>Toggle Help</b> button, and you will see a question mark (  ) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item. |

### 2.4.12.1 Example Packets for Events

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

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

Here are example packets for every event:

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

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

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

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

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

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

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

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



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

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

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

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

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

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

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

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

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

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

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

## 2.4.13 Configure the Door Strike Relay

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

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

This section describes operations for running firmware version 4.8 or later of the Dual Door Strike Relay. If you have an older version of the firmware, then please contact CyberData Technical Support. The version number appears in the **Discovered Remote Relays** section on the **DSR** page ([Figure 2-37](#)).

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

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

Home Device Network SIP SSL Multicast Sensor Audiofiles Events DSR Autoprovisioning Firmware

# CyberData Intercom

### Remote Relay Settings

Not associated with any DSRs

Save Reboot Toggle Help

### Discovered Remote Relays

| Product Type | IP Address  | MAC Address       | Serial Number | Name          | Version |      |           |
|--------------|-------------|-------------------|---------------|---------------|---------|------|-----------|
| DoorLock     | 10.10.1.45  | 00:20:F7:02:A7:9A | 270000004     | LOCK270000004 | V2.2AM  | View | Associate |
| DoorLock     | 10.10.1.19  | 00:20:F7:03:54:BE | 375000016     | LOCK375000016 | V4.8T   | View | Associate |
| DoorLock     | 10.10.1.187 | 00:20:F7:03:74:D4 | 375000046     | LOCK375000046 | V4.8T   | View | Associate |




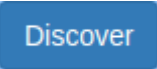



Discover

This is the default page when the device is **not associated with any DSRs**. Please see the Dual Door Strike Relay Operations Guide for more settings and options on the DSR page when the device is associated with a DSR.

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

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

**Table 2-17. DSR Configuration Parameters (not associated with any DSRs)**

| Web Page Item   | Description  |
|---|--|
| <b>Remote Relay Settings</b>  | The settings in this section will activate an associated door strike relay. If a door strike relay is not associated with the device, then you will only see the words <b>Not associated with any DSRs</b> .   |
|    | Click the <b>Save</b> button to save your configuration settings.  |
|    | Click on the <b>Reboot</b> button to reboot the system.  |
|    | Click on the <b>Toggle Help</b> button to see a short description of some of the web page items. First click on the <b>Toggle Help</b> button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.      |
| <b>Discovered Remote Relays</b>   | The <b>Discovered Remote Relays</b> section lists all of the networked door strike relays on the network. To associate your device with a door strike relay, click on the <b>Associate</b> button. This action allows the user to configure the door strike relay. Keep in mind that a device may only be associated with one door strike relay. |
| Product Type  | Displays the product type of the remote relay.   |
| IP Address  | Displays the IP address of the remote relay.   |
| MAC Address   | Displays the MAC address of the remote relay.  |
| Serial Number   | Displays the serial number of the remote relay.  |
| Name  | Displays the name of the remote relay.   |
| Version   | Displays the version of the remote relay.  |
|  | Use this button to search for and find any remote relays that are available on the network.  |
|  | Use this button to view the settings of a remote relay that has been “discovered” after pressing the <b>Discover</b> button.   |
|  | Use this button to associate the remote relay with the device. Only one relay may be associated with a device.   |
|  | Use this button to disassociate the remote relay from the device. Only one relay may be associated with a device. This button is only available when a relay is associated with a device.  |

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

## 2.4.14 Configure the Autoprovisioning Parameters

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

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

1. Click the **Autoprov** menu button to open the **Autoprovisioning** page. See [Figure 2-38](#).

**Figure 2-38. Autoprovisioning Page**

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

# CyberData Intercom

Enable Autoprovisioning: ☒

Autoprovisioning Server:

Autoprovisioning Filename:

Use tftp: ☐

Verify Server Certificate: ☐

Username:

Password:

Autoprovisioning autoupdate (in minutes):

Autoprovision at time (HHMM):

Autoprovision when idle (in minutes > 10):

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

Autoprovisioning happens on boot.

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

If these haven't been configured, it will look for an autoprovisioning server in your list of DHCP options and try to download '0020f703efb7.xml' and if this fails, '000000cd.xml'.

Save Reboot Toggle Help

Download Template

Autoprovisioning log



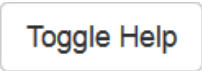

```

2018-09-21 15:00:43 Autoprov: no autoprov triggers. Exiting...
2018-09-21 15:00:44 Autoprovisioning on boot
2018-09-21 15:00:44 Autoprov found server='https://10.0.0.242:4444' in dhcp option 43
2018-09-21 15:00:44 Autoprov looking for https://10.0.0.242:4444/0020f703efb7.xml
2018-09-21 15:00:44 Autoprov not verifying server certificate
2018-09-21 15:00:44 Autoprov: download failed
2018-09-21 15:00:44 Autoprov looking for 000000cd.xml at https://10.0.0.242:4444
2018-09-21 15:00:44 Autoprov looking for https://10.0.0.242:4444/000000cd.xml
2018-09-21 15:00:44 Autoprov not verifying server certificate
2018-09-21 15:00:44 Autoprov: download failed
  
```

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

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

**Table 2-18. Autoprovisioning Page Parameters**

| Web Page Item   | Description   |
|---|---|
| Enable Autoprovisioning ?   | The device will automatically fetch a configuration file, also known as the 'autoprovisioning file', based on the configured settings below.  |
| Autoprovisioning Server ?   | Enter the IPv4 address of the provisioning server in dotted decimal notation.   |
| Autoprovisioning Filename ?   | <p>The autoprovisioning filename is the configuration filename. The default autoprovisioning filename is in the format of <b>&lt;mac address&gt;.xml</b>.</p> <p>Supported filename extensions are .txt, and .xml. The current filename is denoted by an asterisk at the bottom of the <a href="#">Autoprovisioning Page</a>. Enter up to 256 characters.</p> <p>A file may have any name with an xml extension. If a file name is entered, the device will look for the specified file name, and only that file.</p> |
| Use tftp ?  | The device will use TFTP (instead of http) to download autoprovisioning files.  |
| Verify Server Certificate ?   | When using ssl to download autoprovisioning files, reject connections where the server address doesn't match the server certificate's common name.  |
| Username ?  | The username used to authenticate with an autoprovisioning server. Leave this field blank to disable authentication.  |
| Password ?  | The password used to authenticate with an autoprovisioning server. Leave this field blank to disable authentication.  |
| Autoprovisioning Autoupdate (in minutes) ?  | The reoccurring time (in minutes) the device will wait before checking for new autoprovisioning files. Enter up to 6 digits. A value of 0 will disable this option.   |
| Autoprovision at time (HHMMSS) ?  | The time of day the device will check for a new autoprovisioning file. The time must be 6 characters in length and in HHMMSS format. An empty value will disable this option.   |
| Autoprovision when idle (in minutes > 10) ?   | The idle time (in minutes greater than 10) after which the device will check for a new autoprovisioning file. Enter up to 6 digits. A value of 0 will disable this option.  |
|  | Click the <b>Save</b> button to save your configuration settings.   |
|  | Click on the <b>Reboot</b> button to reboot the system.   |
|  | Click on the <b>Toggle Help</b> button to see a short description of some of the web page items. First click on the <b>Toggle Help</b> button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.   |
|  | Press the <b>Download Template</b> button to create an autoprovisioning file for the device. See <a href="#">Section 2.4.14.3, "Download Template Button"</a>   |
| Autoprovisioning log  | The autoprovisioning log provides information about the latest autoprovisioning attempt (i.e. dhcp options and server accessed and files parsed or not found).  |

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

### 2.4.14.1 Autoprovisioning

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

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

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

By default, the device will get its autoprovisioning server from the DHCP options. See [Section 2.4.14.2, "Sample dhcpd.conf"](#) for an example of how to configure dhcpd to offer autoprovisioning server addresses. If multiple options are set, the device will attempt to download autoprovisioning files from every server.

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

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

You can download an autoprovisioning template file from the [Autoprovisioning Page](#) using the **Download Template** button (see [Table 2-18](#)). This file contains every configuration option that can be set on the board.

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

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

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

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

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

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

The file 0020f7123456.xml contains:

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

1. The device will first set it's name to 'Newname'.
2. It will try to download http://example.com/common.xml.
3. It will try to download http://example.com/sip\_reg0020f7123456.xml.
4. It will try to download http://example.com/audio0020f7123456.
5. It will try to download http://example.com/device.xml.

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

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

#### Checking for New Autoprovisioning Files after Boot

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



The  
Autoprovisioning  
Filename

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

**Table 2-19. Autoprovisioning File Name**

| <b>Autoprovisioning<br/>Filename</b> | <b>Autoprovisioning<br/>Server</b> | <b>File Downloaded</b>                      |
|--------------------------------------|------------------------------------|---|
| config.xml                           | 10.0.1.3                           | 10.0.1.3/config.xml                         |
| /path/to/config.xml                  | 10.0.1.3                           | 10.0.1.3/path/to/config.xml                 |
| subdirectory/path/                   | 10.0.1.3                           | 10.0.1.3/subdirectory/path/0020f7020002.xml |

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

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

For example:

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

The autoprovisioning filename is set to “cyberdata/”

On boot, the device will try to download:

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

...and if this fails:

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

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

```
Autoprovisioning <FirmwareSettings>
Firmware Updates <FirmwareFile>505-ulmage-ceilingspeaker</FirmwareFile>
                  <FirmwareServer>10.0.1.3</FirmwareServer>
                  <OutdoorIntercom30>firmware_file_v9.3.0</OutdoorIntercom30>
                  <OutdoorIntercom31>firmware_file_v10.3.0</OutdoorIntercom31>
                  <CallButton31>firmware_file_v10.3.0</CallButton31>
                  </FirmwareSettings>
```

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

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

The <FirmwareFile> name can contain path elements (i.e. /path/to/firmware/10.3.0-ulmage-[device\_file\_name]).

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

The list of valid product strings:

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

Autoprovisioning  
Example 1

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

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

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

**000000cd.xml**

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

**sip\_common.xml**

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

**sip\_0020f7020001.xml**

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

**sip\_0020f7020002.xml**

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

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

1. Device1 changes its device name to **CyberData Autoprovisioned**.
2. Device1 finds an AutoprovFile element containing the filename **sip\_common.xml**. The device downloads **sip\_common.xml** from "https://autoprovtest.server.net," and imports this configuration, setting the sip server to **10.0.0.253** and the remote port to **5060.3**.
3. Device1 finds another AutoprovFile element containing the filename **sip\_[macaddress].xml**. The device replaces the **[macaddress]** with its own mac address value creating **sip\_0020f7020001.xml**, downloads this file from "https://autoprovtest.server.net," and imports this configuration. This sets the user ID to **198**, the password to **ext198**, and the dialout extension to **204**. Device1 is now finished with autoprovisioning.

Device2 goes through the same steps by setting its device name to **CyberData Autoprovisioned**, its SIP server to **10.0.0.253**, and its port to **5060**. When Device2 “sees” **sip\_[macaddress].xml**, Device2 replaces it with its own mac address and downloads **sip\_0020f7020002.xml** from “https://autoprovtest.server.net.” Device2 sets the SIP User ID to **500**, the password to **ext500**, and the dialout extension to **555**.

#### Autoprovisioning Example 2

Here is another example of setting up your autoprovisioning files:

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

##### **0020f7020001.xml**

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

##### **0020f7020002.xml**

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

##### **common\_settings.xml**

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

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

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

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

## XML Files

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

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

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

From the device specific xml, a pointer to a sip\_common file

From the device specific xml, a pointer to the device specific sip\_[macaddress].xml

From the common file, a pointer to sip\_common.xml

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

## Autoprovisioned Audio Files

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

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

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

## 2.4.14.2 Sample dhcpd.conf

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

ddns-update-style none;

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

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

    option routers                10.0.0.1;
    option subnet-mask            255.0.0.0;

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

    option time-offset            -8;          # Pacific Standard Time

#    option www-server            99.99.99.99;          # OPTION 72

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

#    option option-150            10.0.0.252;          # OPTION 150

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

    range 10.10.0.1 10.10.2.1; }
```

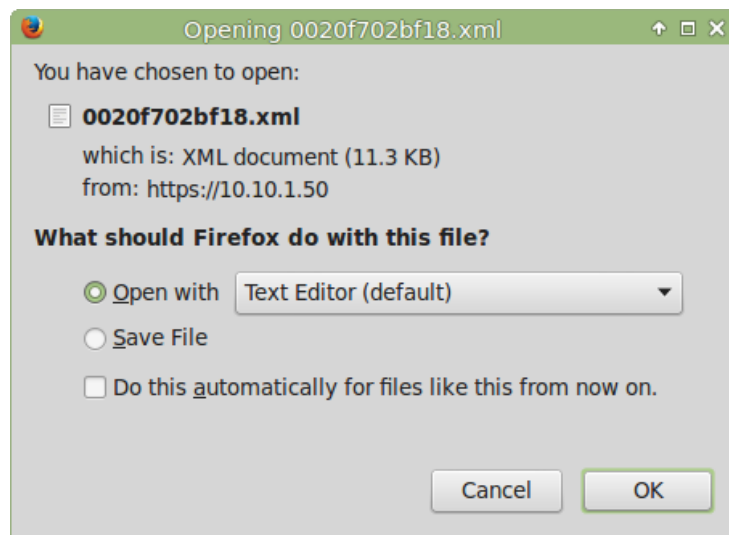
### 2.4.14.3 Download Template Button

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

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

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

**Figure 2-39. Configuration File**



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

## 2.5 Upgrade the Firmware

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

To upgrade the firmware of your device:

1. Download the latest firmware file from the **Downloads** tab at the following webpage:  
<https://www.cyberdata.net/products/011211>
2. Unzip the firmware version file. This file may contain the following:
  - Firmware file
  - Release notes
  - Autoprovisioning template
3. Log in to the **Home** page as instructed in [Section 2.4.4, "Log in to the Configuration Home Page"](#).
4. Click on the **Firmware** menu button to open the **Firmware** page ([Figure 2-40](#)).


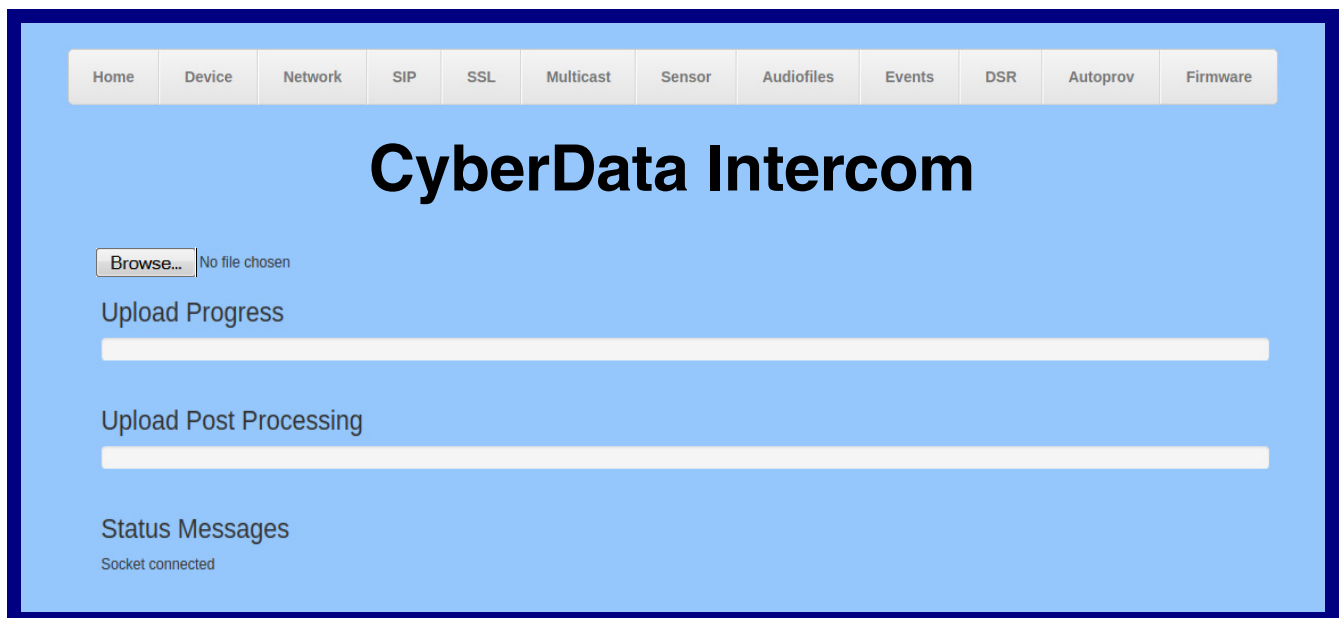
|   |  |
|---|--|
| <br>GENERAL ALERT | <b>Caution</b><br><b>Equipment Hazard:</b> CyberData strongly recommends that you first reboot the device before attempting to upgrade the firmware of the device. See <a href="#">Section 2.5, "Upgrade the Firmware"</a> . |
|---|--|

Figure 2-40. Firmware Page

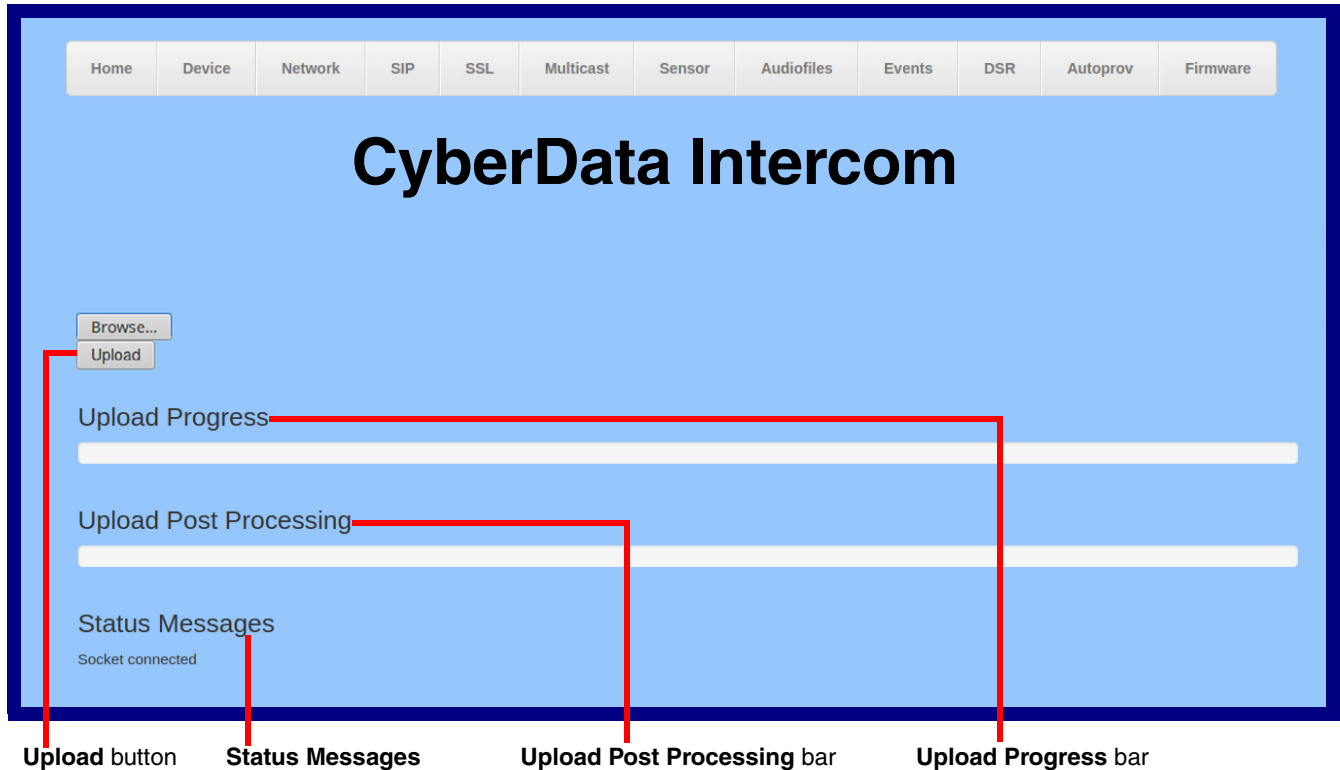


5. Click on the **Browse** button, and then navigate to the location of the firmware file.



6. Select the firmware file. This reveals the **Upload** button (Figure 2-41).

Figure 2-41. Upload Button



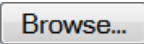

7. Click on the **Upload** button. After selecting the **Upload** button, you will see the progress of the upload in the **Upload Progress** bar.
8. When the upload is complete, you will see the words **Upload finished** under **Status Messages**.
9. At this point, you will see the progress of the upload's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

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

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

Table 2-20 shows the web page items on the **Firmware** page.

**Table 2-20. Firmware Page Parameters**

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

## 2.6 Reboot the Device

To reboot the device, complete the following steps:

1. Log in to the **Home** page as instructed in [Section 2.4.4, "Log in to the Configuration Home Page"](#).
2. Click on the **Reboot** button on the **Home** page ([Figure 2-42](#)). A normal restart will occur.

**Figure 2-42. Home Page**

**CyberData Intercom**

**Device Status**

Serial Number: 211200001  
 Mac Address: 00:20:f7:03:fb:79  
 Firmware Version: v20.4.1  
 Partition 2: v20.4.1  
 Partition 3: v20.4.1  
 Booting From: partition 3

**Boot From Other Partition**

IP Addressing: DHCP  
 IP Address: 10.10.0.95  
 Subnet Mask: 255.0.0.0  
 Default Gateway: 10.0.0.1  
 DNS Server 1: 10.0.1.56  
 DNS Server 2:

SIP Volume: 4  
 Multicast Volume: 4  
 Ring Volume: 4  
 Sensor Volume: 4  
 Push to Talk Volume: 4  
 Microphone Gain: 4  
 Push to Talk Microphone Gain: 4

SIP Mode: Enabled  
 Multicast Mode: Disabled  
 Event Reporting: Disabled

Primary SIP Server: **Not registered**  
 Backup Server 1: Not registered  
 Backup Server 2: Not registered  
 Nightringer Server: Not registered

**Sensor Status**

Relay Status: Locked  
 Door Status: Closed  
 Intrusion: Closed

**Admin Settings**

Username: admin  
 Password: \*\*\*\*\*  
 Confirm Password: \*\*\*\*\*

**Save Reboot Toggle Help**

**Import Settings**

**Browse...** No file chosen  
**Import Config**

**Export Settings**

**Export Config**

Reboot

## 2.7 Command Interface

Some functions on the device can be activated using simple POST commands to the web interface. The examples in [Table 2-21](#) use the free unix utility, **wget** **commands**. However, any program that can send HTTP POST commands to the device should work.

### 2.7.1 Command Interface Post Commands

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

**Table 2-21. Command Interface Post Commands**

| Device Action                                    | HTTP Post Command <sup>a</sup>  |
|--|---|
| Reboot   | wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.154/command" --post-data "request=reboot"             |
| Place call to extension (example: extension 600) | wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.154/command" --post-data "request=call&extension=600" |
| Test Relay                                       | wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.154/command" --post-data "request=test_relay"         |
| Test Audio                                       | wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.154/command" --post-data "request=test_audio"         |
| Speak IP Address                                 | wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.154/command" --post-data "request=speak_ip_address"   |
| Test Mic   | wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.154/command" --post-data "request=test_mic"           |
| Play the "0" audio file                          | wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "0=Play"                 |
| Play the "1" audio file                          | wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "1=Play"                 |
| Play the "2" audio file                          | wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "2=Play"                 |
| Play the "3" audio file                          | wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "3=Play"                 |
| Play the "4" audio file                          | wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "4=Play"                 |

**Table 2-21. Command Interface Post Commands (continued)**

| <b>Device Action</b>                             | <b>HTTP Post Command<sup>a</sup></b>  |
|--|---|
| Play the "5" audio file                          | <code>wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "5=Play"</code>                        |
| Play the "6" audio file                          | <code>wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "6=Play"</code>                        |
| Play the "7" audio file                          | <code>wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "7=Play"</code>                        |
| Play the "8" audio file                          | <code>wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "8=Play"</code>                        |
| Play the "9" audio file                          | <code>wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "9=Play"</code>                        |
| Play the "Dot" audio file                        | <code>wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "d=Play"</code>                        |
| Play the Audio Test                              | <code>wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "audiotest=Play"</code>                |
| Play the "Page Tone" audio file                  | <code>wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "pagetone=Play"</code>                 |
| Play the "Your IP Address Is" audio file         | <code>wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "youripaddressis=Play"</code>          |
| Play the "Rebooting" audio file                  | <code>wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "rebooting=Play"</code>                |
| Play the "Restoring Default" audio file          | <code>wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "restoringdefault=Play"</code>         |
| Play the "Ringback tone" audio file              | <code>wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "ringback=Play"</code>                 |
| Play the "Ring tone" audio file                  | <code>wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "ringtone=Play"</code>                 |
| Play the "Intrusion Sensor Triggered" audio file | <code>wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "intrusionsensortriggered=Play"</code> |
| Play the "Door Ajar" audio file                  | <code>wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "doorajar=Play"</code>                 |
| Play the "Night Ring" audio file                 | <code>wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "nightring=Play"</code>                |

**Table 2-21. Command Interface Post Commands (continued)**

| Device Action        | HTTP Post Command <sup>a</sup>   |
|----------------------|--|
| Swap boot partitions | wget --user admin --password admin --auth-no-challenge --quiet -<br>O /dev/null --no-check-certificate "https://10.10.1.154/command" --<br>post-data "request=swap_boot_partition" |

a. Type and enter all of each http POST command on one line.


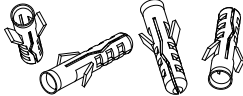


# Appendix A: Mounting the Indoor Intercom


## A.1 Wall Mounting Components

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

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

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

**Table A-2. Gang Box Mounting Components**

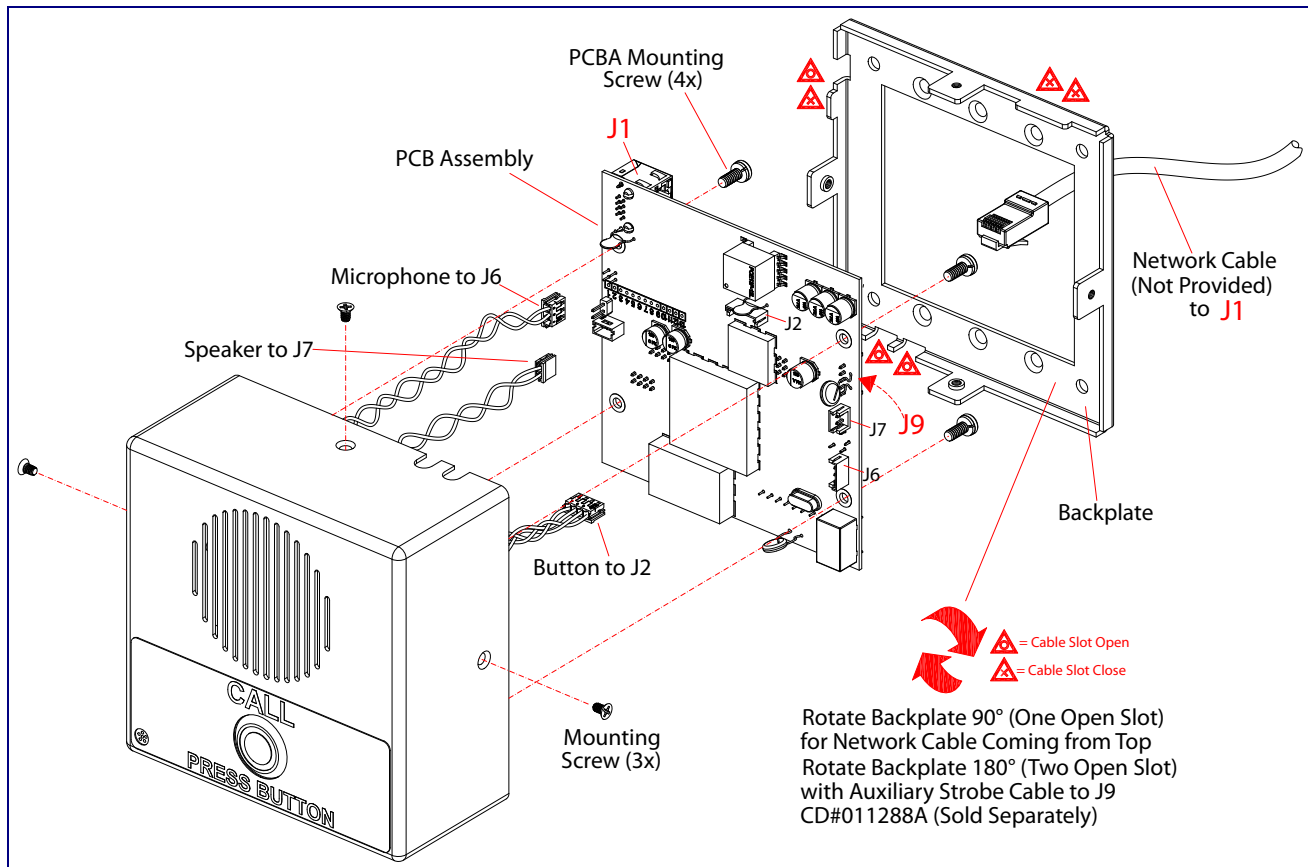
| Quantity | Part Name                                | Illustration  |
|----------|--|---|
| 4        | #6-32 FlatHead Countersunk Machine Screw |  |



## A.2 Cable Connections

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

**Figure A-1. Cable Connections**

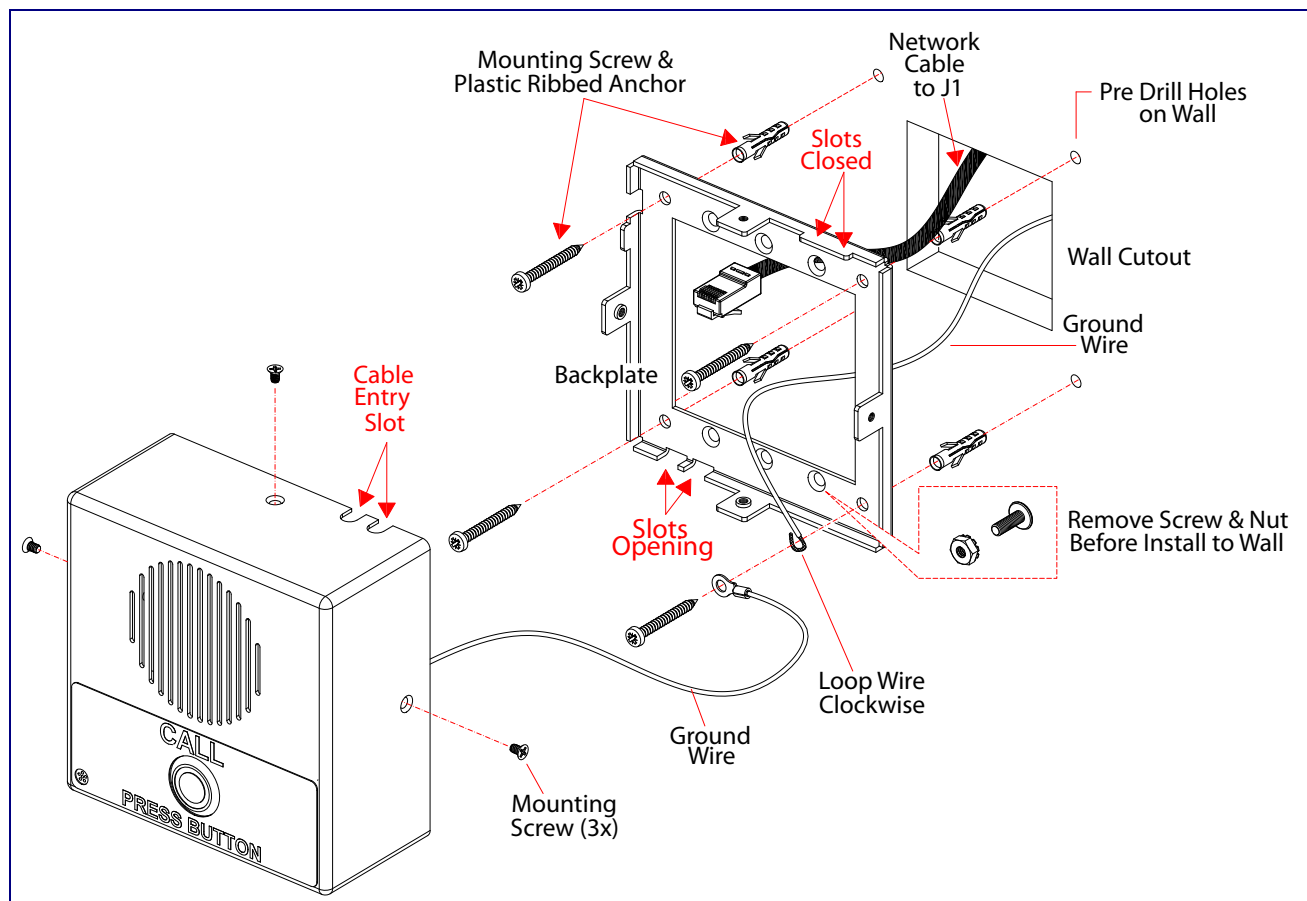


## A.3 Wall Mounting Option

Figure A-2 shows a wall mounting option.

**Note** Be sure to connect the SIP Indoor Intercom to the Earth Ground.

**Figure A-2. Wall Mounting Option**

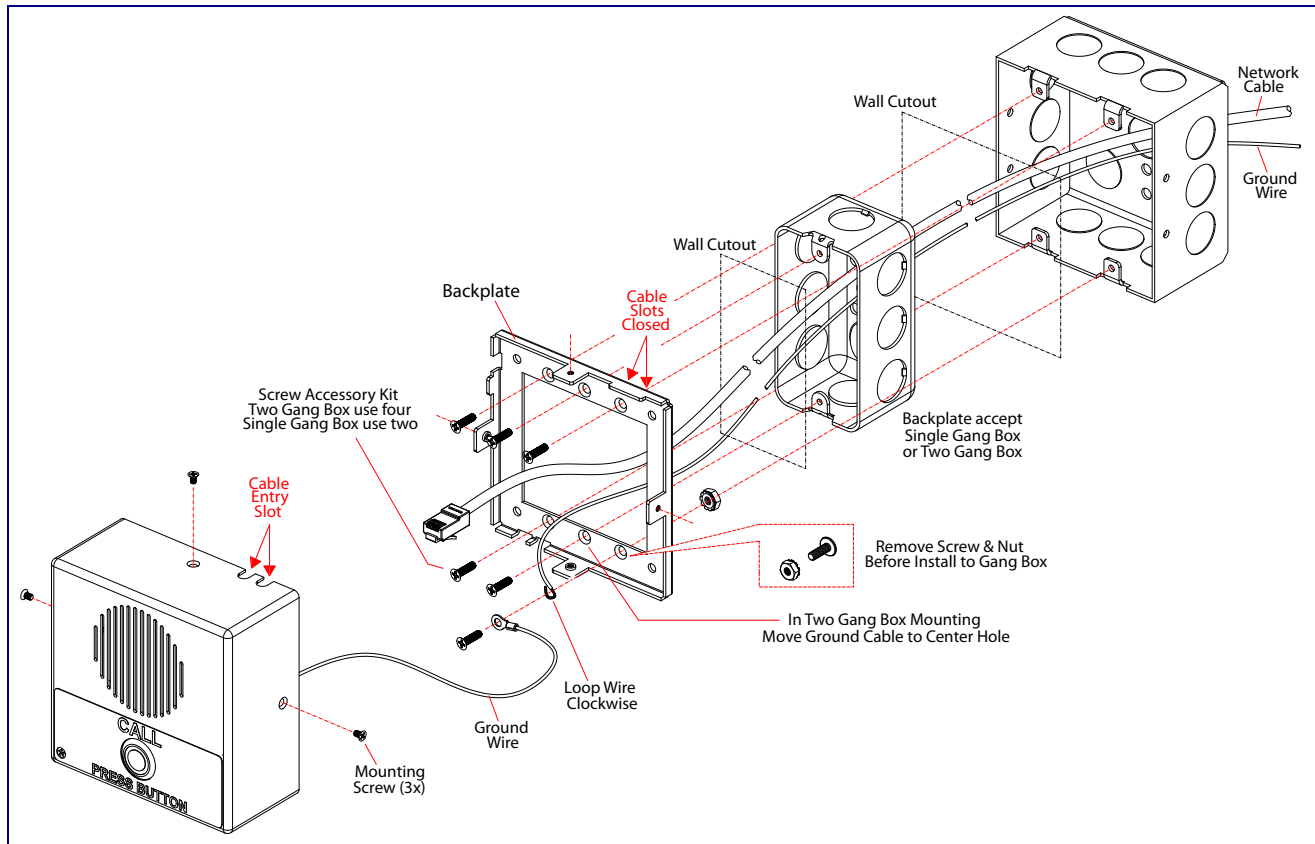


## A.4 Gang Box Option

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

**Note** Be sure to connect the SIP Indoor Intercom to the Earth Ground.

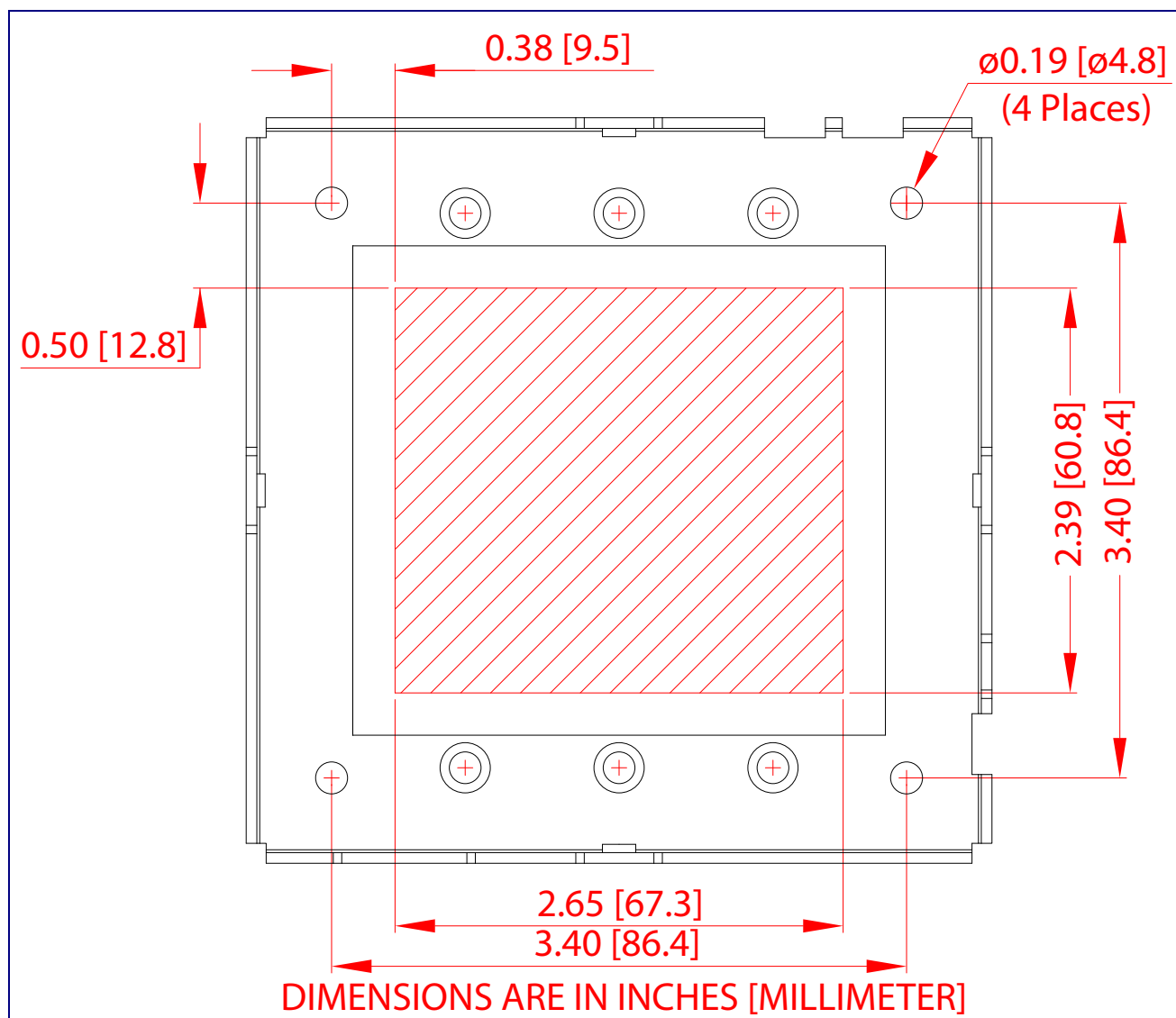
**Figure A-3. Gang Box Mounting**



## A.5 Wall Cutout Dimensions

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

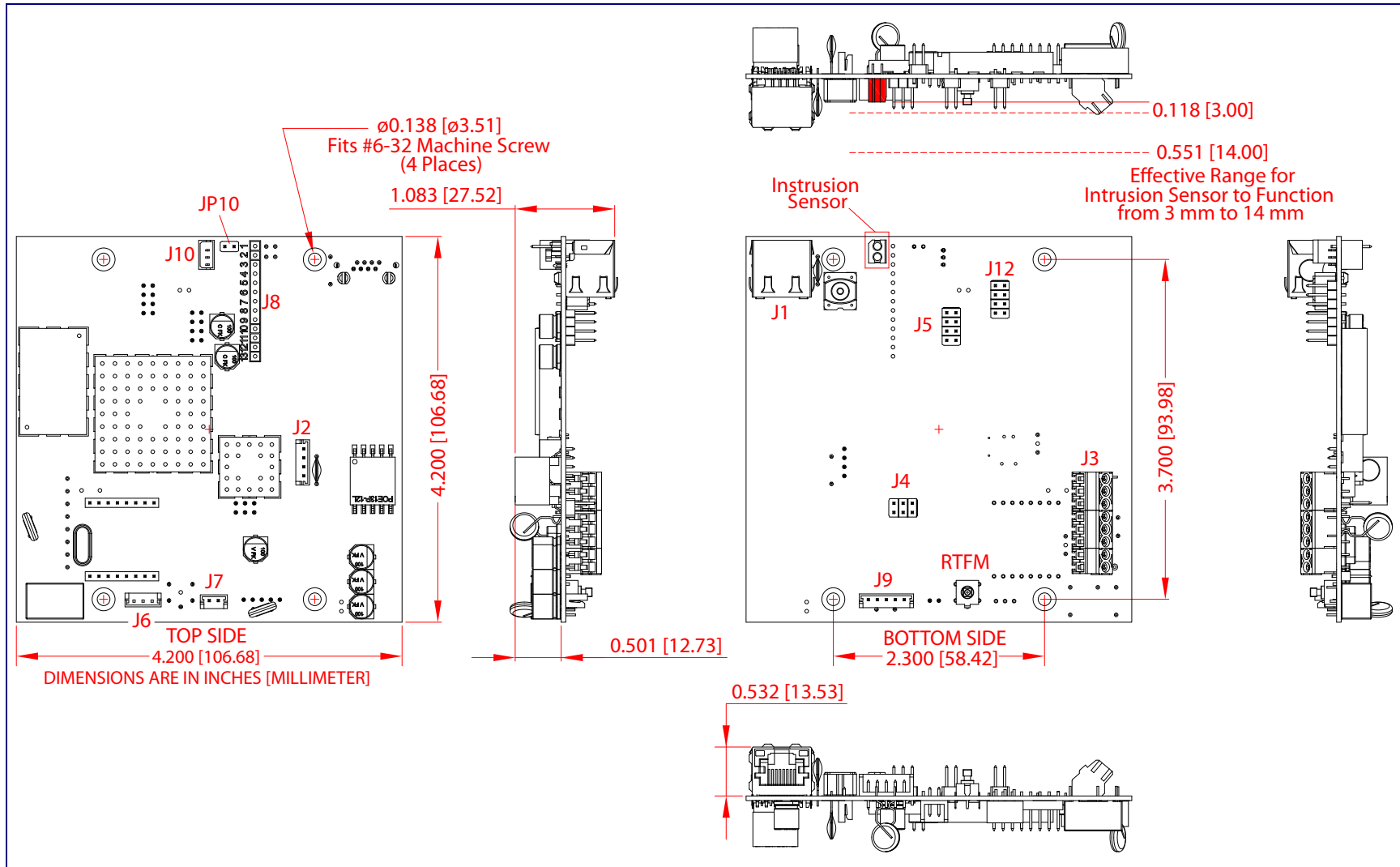
**Figure A-4. Maximum Recommended Wall Cutout Dimensions**



## A.6 PCB Dimensions

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

Figure A-5. PCB Dimensions and Intrusion Sensor Range



# Appendix B: Setting up a TFTP Server

---

## B.1 Set up a TFTP Server

Autoprovisioning requires a TFTP server for hosting the configuration file.

---

### B.1.1 In a LINUX Environment

To set up a TFTP server on LINUX:

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

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

---

### B.1.2 In a Windows Environment

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

<https://www.cyberdata.net/pages/solarwinds>

To set up a TFTP server on Windows:

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

# Appendix C: Troubleshooting/Technical Support

---

## C.1 Frequently Asked Questions (FAQ)

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

<https://www.cyberdata.net/products/011211>

---

## C.2 Documentation

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

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

<https://www.cyberdata.net/products/011211>

---

## C.3 Contact Information

|                   |  |
|-------------------|--|
| Contact           | <p>CyberData Corporation<br/>3 Justin Court<br/>Monterey, CA 93940 USA<br/><a href="http://www.CyberData.net">www.CyberData.net</a><br/>Phone: 800-CYBERDATA (800-292-3732)<br/>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="https://support.cyberdata.net/">https://support.cyberdata.net/</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, Extension 333</p> |

---

## C.4 Warranty and RMA Information

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

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



# Index

---

## Numerics

16 AWG gauge wire 9

## A

activate relay (door sensor) 60  
 activate relay (intrusion sensor) 61  
 activity LED 21  
 address, configuration login 30  
 alternative power input 5  
 announcing a device's IP address 23  
 audio configuration 63  
     night ring tone parameter 65  
 audio configuration page 63  
 audio encodings 4  
 audio files, user-created 67  
 autoprovision at time (HHMMSS) 78  
 autoprovision when idle (in minutes > 10) 78  
 autoprovisioning 78, 79  
     download template button 78  
     setting up a TFTP server 102  
 autoprovisioning autoupdate (in minutes) 78  
 autoprovisioning configuration 77, 78  
 autoprovisioning filename 78  
 autoprovisioning server (IP Address) 78

## B

backup SIP server 1 42  
 backup SIP server 2 42  
 backup SIP servers, SIP server  
     backups 42

## C

cable connections 97  
 call button 9, 25  
 call button LED 9, 25  
 call termination 37  
 changing  
     the web access password 34  
 Cisco SRST 43  
 configurable parameters 35, 39, 42  
 configuration  
     audio 63

    default IP settings 26  
     door sensor 49, 59  
     intrusion sensor 49, 59  
     network 38  
     SIP 40  
 configuration home page 30  
 configuration page  
     configurable parameters 35, 39  
 contact information 104  
 contact information for CyberData 104  
 current network settings 39  
 cutout dimensions 100  
 cutout dimensions, maximum recommended 100  
 CyberData contact information 104

## D

default  
     gateway 26  
     intercom settings 105  
     IP address 26  
     subnet mask 26  
     username and password 26  
     web login username and password 30  
 default gateway 26, 39  
 default intercom settings 24  
 default IP settings 26  
 default login address 30  
 device configuration 34  
     device configuration parameters 78  
     the device configuration page 77  
 device configuration page 34  
 device configuration parameters 35  
 device configuration password  
     changing for web configuration access 34  
 DHCP Client 4  
 dial out extension (door sensor) 60  
 dial out extension (intrusion sensor) 61  
 dial out extension strings 47  
 dial-out extension strings 48  
 dimensions 5  
     maximum recommended wall cutout dimensions 100  
     pcb dimensions and intrusion sensor range 101  
 discovery utility program 30  
 DNS server 39  
 door sensor 59, 60  
     activate relay 60  
     dial out extension 60  
     door open timeout 60  
     door sensor normally closed 60

- flash button LED 60
- play audio locally 60
- download autoprovisioning template button 78
- DTMF push to talk 37
- DTMF tones 47, 48
- DTMF tones (using rfc2833) 47

## E

- earth ground 98, 99
- enable night ring events 70
- ethernet I/F 5
- event configuration
  - enable night ring events 70
- expiration time for SIP server lease 42, 43, 45
- export settings 33

## F

- factory default settings 24
- firmware
  - where to get the latest firmware 88
- flash button LED (door sensor) 60
- flash button LED (intrusion sensor) 61

## G

- gang box option 99
- gauge wire (terminal block) 9
- get autoprovisioning template 78

## H

- home page 30
- http web-based configuration 4

## I

- identifying your product 1
- illustration of intercom mounting process 96
- import settings 33
- import/export settings 33
- installation, typical intercom system 2
- intercom configuration
  - default IP settings 26
- intercom configuration page
  - configurable parameters 42

- intrusion sensor 59, 61
  - activate relay 61
  - dial out extension 61
  - flash button LED 61
  - play audio locally 61
- IP address 26, 39
- IP addressing
  - default
    - IP addressing setting 26

## L

- lease, SIP server expiration time 42, 43, 45
- LED
  - yellow activity LED 21
- lengthy pages 58
- Linux, setting up a TFTP server on 102
- local SIP port 43
- log in address 30

## M

- MGROUP
  - MGROUP Name 56
- mounting
  - gang box mounting 99
  - gang box option 99
  - maximum recommended wall cutout dimensions 100
  - wall cutout dimensions 100, 101
  - wall mounting 98
  - wall mounting components 96
  - wall mounting option 98
- mounting an intercom 96
- multicast configuration 63
- Multicast IP Address 56

## N

- navigation (web page) 27
- navigation table 27
- network configuration 38
- nightring tones 58
- Nightringer 9, 87
- nightringer settings 45
- NTP server 35

## O

- on-board relay 5, 11

## P

- packet time 4
- pages (lengthy) 58
- part number 5
- password
  - for SIP server login 42
  - login 30
  - restoring the default 26
- payload types 5
- pcb dimensions and intrusion sensor range 101
- play audio locally (door sensor) 60
- play audio locally (intrusion sensor) 61
- point-to-point configuration 48
- polycom default channel 56
- polycom emergency channel 57
- polycom priority channel 56
- port
  - local SIP 43
  - remote SIP 43
- power input 5
  - alternative 5
- priority
  - assigning 58
- product
  - mounting 96
  - parts list 7
- product features 3
- product overview
  - product features 3
  - product specifications 5
  - supported protocols 4
  - supported SIP servers 4
  - typical system installation 2
- product specifications 5
- protocol 5
- protocols supported 4
- push to talk, DTMF 37

## R

- reboot 90
- remote SIP port 43
- reset test function management button 22
- resetting the IP address to the default 96, 103
- restoring factory default settings 24, 105
- ringtones 58
  - lengthy pages 58
- RJ-45 20
- rport discovery setting, disabling 43
- RTFM button 22
- RTFM jumper 22, 23, 24
- RTP/AVP 4

## S

- sales 104
- sensor setup page 49, 59, 75
- sensor setup parameters 49, 59
- sensors 60
- server address, SIP 42
- service 104
- setting up the device 9
- settings, default 24
- SIP
  - enable SIP operation 42
  - local SIP port 43
  - user ID 42
- SIP configuration 40
- SIP configuration parameters
  - outbound proxy 43
  - registration and expiration, SIP server lease 42, 43, 45
  - unregister on reboot 43
  - user ID, SIP 42
- SIP registration 42
- SIP remote SIP port 43
- SIP server 42
  - password for login 42
  - SIP servers supported 4
  - unregister from 43
  - user ID for login 42
- SIP server configuration 42
- SIP volume 35
- speaker output 5
- SRST 43
- subnet mask 26, 39
- supported protocols 4

## T

- tech support 104
- technical support, contact information 104
- terminal block connections 9
- TFTP server 4, 102

## U

- user ID
  - for SIP server login 42
- username
  - changing for web configuration access 34
  - default for web configuration access 30
  - restoring the default 26

## V

- VLAN ID 39
- VLAN Priority 39
- VLAN tagging support 39
- VLAN tags 39
- volume
  - microphone gain 35
  - multicast volume 35
  - push to talk volume 35
  - ring volume 35
  - sensor volume 35
  - SIP volume 35

## W

- wall cutout dimensions 100, 101
- wall cutout dimensions, maximum recommended 100
- wall mounting option 98
- warranty policy at CyberData 104
- web access password 26
- web access username 26
- web configuration log in address 30
- web page
  - navigation 27
- web page navigation 27
- Windows, setting up a TFTP server on 102
- wire gauge (terminal block) 9
- wiring the circuit 12
  - devices less than 1A at 30 VDC 12