



# *SIP Outdoor Intercom with Keypad Operations Guide*

Part #011214

Document Part #931562B  
for Firmware Version 20.0.0

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

---

**SIP Outdoor Intercom with Keypad Operations Guide 931562B**  
**Part # 011214**

**COPYRIGHT NOTICE:**

© 2018, CyberData Corporation, ALL RIGHTS RESERVED.

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

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

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

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

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



Technical Support

The fastest way to get technical support for your VoIP product is to submit a VoIP Technical Support form at the following website:  
<http://support.cyberdata.net/>

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



Email: [support@cyberdata.net](mailto:support@cyberdata.net)

Fax: (831) 373-4193

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

---

## Pictorial Alert Icons

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

---

## Hazard Levels

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

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

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




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

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

---

# Important Safety Instructions

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

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



---

## Revision Information

Revision 931562B, which corresponds to firmware version 20.0.0, was released on January 28, 2019, and has the following changes:

- Updates [Section 1.2, "Typical System Installation"](#)
- Updates [Section 1.3, "Product Features"](#)
- Updates [Section 1.6, "Specifications"](#)

---

## Browsers Supported

The following browsers have been tested against firmware version 20.0.0:

- Internet Explorer (version: 11)
- Firefox (also called Mozilla Firefox) (version: 62.0)
- Chrome (version: 63.0.3239.132)
- Safari (version: 12)
- Microsoft Edge (version: 42.17134.1.0)

<b>Chapter 1 Product Overview</b>	<b>1</b>
1.1 How to Identify This Product .....	1
1.2 Typical System Installation .....	2
1.3 Product Features .....	3
1.4 Supported Protocols .....	4
1.5 Supported SIP Servers .....	4
1.6 Specifications .....	5
1.7 Compliance .....	6
1.7.1 CE Testing .....	6
1.7.2 FCC Statement .....	6
 <b>Chapter 2 Installing the SIP Outdoor Intercom with Keypad</b>	 <b>7</b>
2.1 Parts List .....	7
2.2 Intercom Components .....	8
2.2.1 Call Button and Indicator Light .....	9
2.2.2 Dialing from the Keypad .....	9
2.3 Intercom Setup .....	10
2.3.1 Intercom Connections .....	10
2.3.2 Using the On-Board Relay .....	12
2.3.3 Wiring the Circuit .....	13
2.3.4 Intercom Connectors .....	17
2.3.5 Activity and Link LEDs .....	21
2.3.6 RTFM Button .....	22
2.3.7 Adjust the Volume .....	24
2.4 Configure the Intercom Parameters .....	25
2.4.1 Factory Default Settings .....	25
2.4.2 Intercom Web Page Navigation .....	26
2.4.3 Using the Toggle Help Button .....	27
2.4.4 Log in to the Configuration Home Page .....	29
2.4.5 Configure the Device .....	33
2.4.6 Configure the Button Parameters .....	37
2.4.7 Configure the Security .....	41
2.4.8 Configure the Network Parameters .....	47
2.4.9 Configure the SIP Parameters .....	50
2.4.10 Configure the SSL Parameters .....	55
2.4.11 Configure the Multicast Parameters .....	60
2.4.12 Configure the Access Log Parameters .....	63
2.4.13 Configure the Sensor Configuration Parameters .....	65
2.4.14 Configure the Audio Configuration Parameters .....	69
2.4.15 Configure the Events Parameters .....	75
2.4.16 Configure the Door Strike Relay .....	81
2.4.17 Configure the Autoprovisioning Parameters .....	83
2.5 Upgrade the Firmware .....	94
2.5.1 Reboot the Device .....	97
2.6 Command Interface .....	98
2.6.1 Command Interface Post Commands .....	98
 <b>Appendix A Mounting the SIP Outdoor Intercom with Keypad</b>	 <b>101</b>
A.1 Mount the Intercom .....	101
A.2 Dimensions .....	102
A.3 Overview of Installation Types .....	105
A.4 Network Cable Entry Restrictions .....	106
A.4.1 Rear Conduit Network Cable Entry Restrictions (without Shroud) .....	106
A.4.2 Rear Conduit Network Cable Entry Restrictions (with Shroud) .....	106
A.5 Service Loop Cable Routing .....	107
A.6 Securing the Intercom .....	108

A.7 Additional Mounting Options .....	109
A.7.1 Rear Conduit Mounting Option (Not Provided) .....	109
A.7.2 Concrete Wall Mounting Option (Not Provided) .....	110
A.7.3 Goose Neck Mounting Option (Not Provided) .....	111
<b>Appendix B Setting up a TFTP Server</b> .....	<b>112</b>
B.1 Set up a TFTP Server .....	112
B.1.1 In a LINUX Environment .....	112
B.1.2 In a Windows Environment .....	112
<b>Appendix C Troubleshooting/Technical Support</b> .....	<b>113</b>
C.1 Frequently Asked Questions (FAQ) .....	113
C.2 Documentation .....	113
C.3 Contact Information .....	114
C.4 Warranty and RMA Information .....	114
<b>Index</b> .....	<b>115</b>

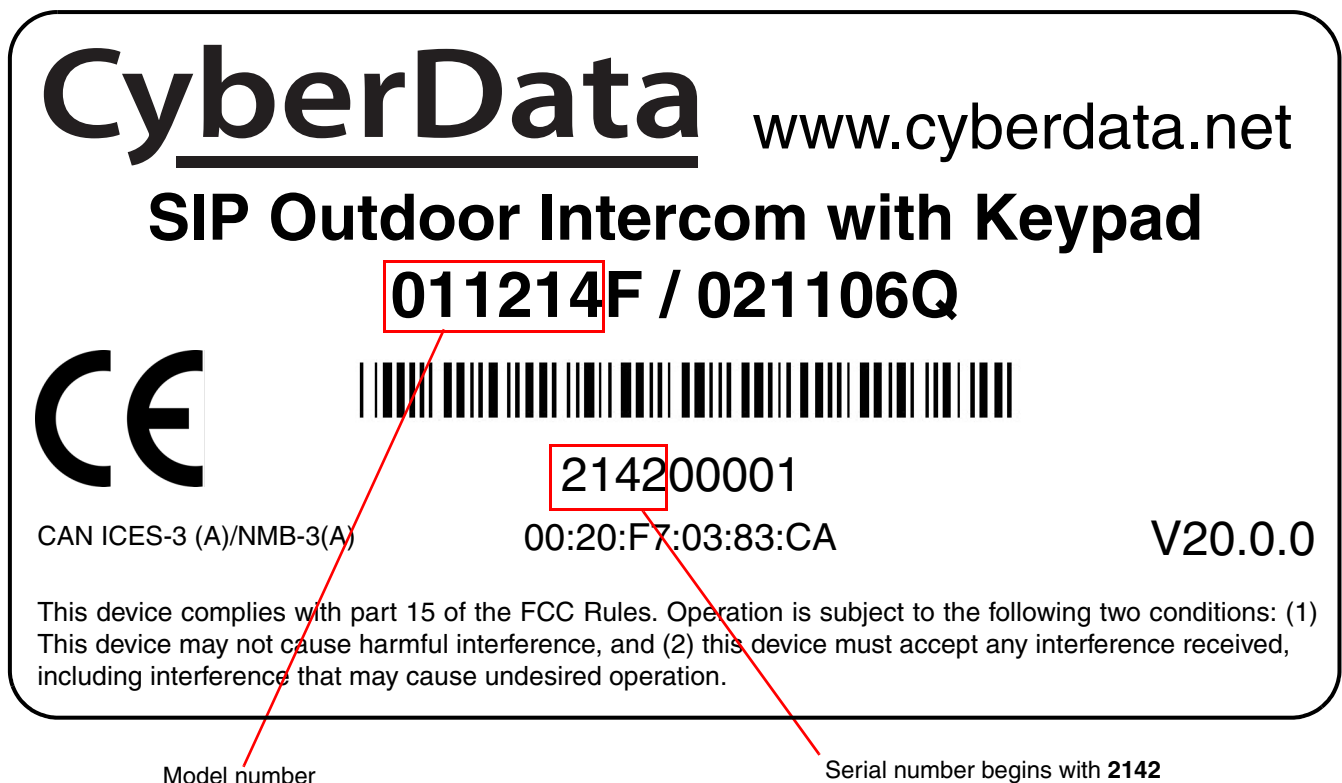
# 1 Product Overview

## 1.1 How to Identify This Product

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

- The model number on the label should be **011214**.
- The serial number on the label should begin with **2142**.

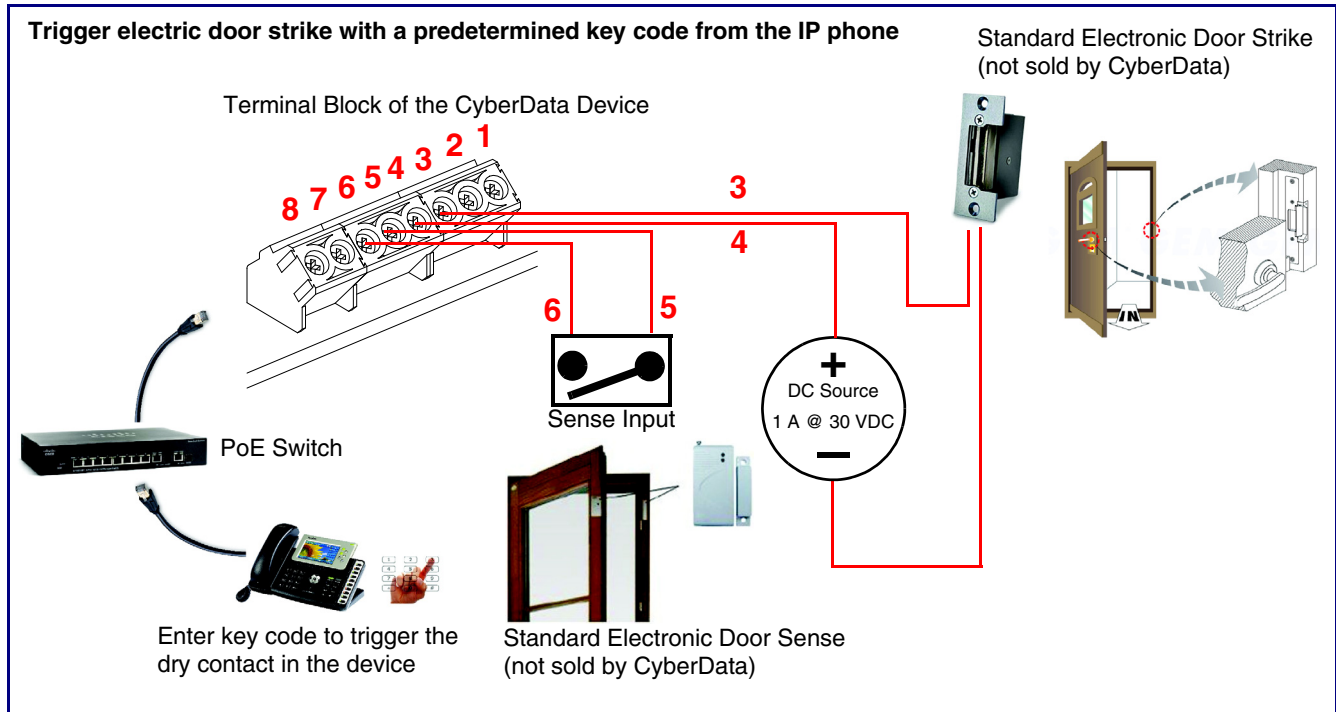
Figure 1-1. Model Number Label



## 1.2 Typical System Installation

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

**Figure 1-2. Typical Installation**



---

## 1.3 Product Features

The SIP Outdoor Intercom with Keypad has the following features:

- TLS 1.2, Enhanced security for IP Endpoints in a local or cloud based environment
- Relay configurable for secure access in all modes
- Security mode allows for up to 500 user codes with configurable times and blacklisting plus extension dialing
- Phone mode allows use as a hands-free phone
- Enhanced acoustic echo canceler
- 12-key keypad with backlight
- Programmable speed dial
- Full-duplex voice operation
- Supports SRST (Survivable Remote Site Telephony) in a Cisco environment
- Streamlined case design
- Network web management and firmware download
- Network adjustable speaker volume
- Concurrent SIP and multicast paging
- Dry relay contact for auxiliary control
- Door closure and tamper alert signal
- Downloadable alert, ringtones and callout

---

## 1.4 Supported Protocols

The Intercom supports:

- SIP
- HTTP Web-based configuration
- Provides an intuitive user interface for easy system configuration and verification of Intercom operations.
- DHCP Client
- Dynamically assigns IP addresses in addition to the option to use static addressing.
- TFTP Client
- Facilitates hosting for the Autoprovisioning configuration file.
- RTP
- 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**

Specification	
Ethernet I/F	10/100 Mbps
Protocol	SIP RFC 3261 Compatible
Power Input	PoE 802.3af compliant or +8 to +12VDC @ 1000mA Regulated Power Supply <sup>a</sup>
Speaker Output	2 Watts Peak Power
On-Board Relay	1A at 30 VDC
Operating Range	Temperature: -40° C to 55° C (-40° F to 131° F) 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)
IP Rating	IP65
Network Security	TLS/SSL 1.2
Payload Types	G711, A-law and $\mu$ -law, G.722, G.729
Dimensions <sup>b</sup>	7.480 in. [190 mm] Length 2.284 in. [58 mm] Width 5.118 in. [130 mm] Height
Weight	2.8 lbs. [1.27 kg]
Boxed Weight	4.0 lbs. [1.81 kg] Weather Shroud is 1.2 lbs. [0.54 kg]
Compliance	CE; EMC Directive – Class A EN 55032 & EN 55024, LV Safety Directive – EN 60950-1, RoHS Compliant, FCC; Part 15 Class A, Industry Canada; ICES-3 Class A, IEEE 802.3 Compliant
Part Number	011214 011215 Weather Shroud (sold separately)

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 Testing

CE testing has been performed according to EN ISO/IEC 17050 for Emissions, Immunity, and Safety. The Declaration of Conformity can be supplied upon request.

---

### 1.7.2 FCC Statement

This equipment has been tested and found to comply with the limits for a Class B 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.

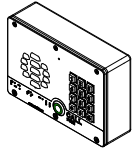
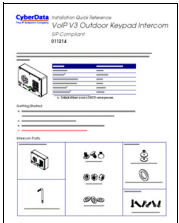

## 2 Installing the SIP Outdoor Intercom with Keypad

### 2.1 Parts List

[Table 2-2](#) illustrates the parts for the SIP Outdoor Intercom with Keypad.

**Note** See [Appendix A, "Mounting the SIP Outdoor Intercom with Keypad"](#) for physical mounting information.

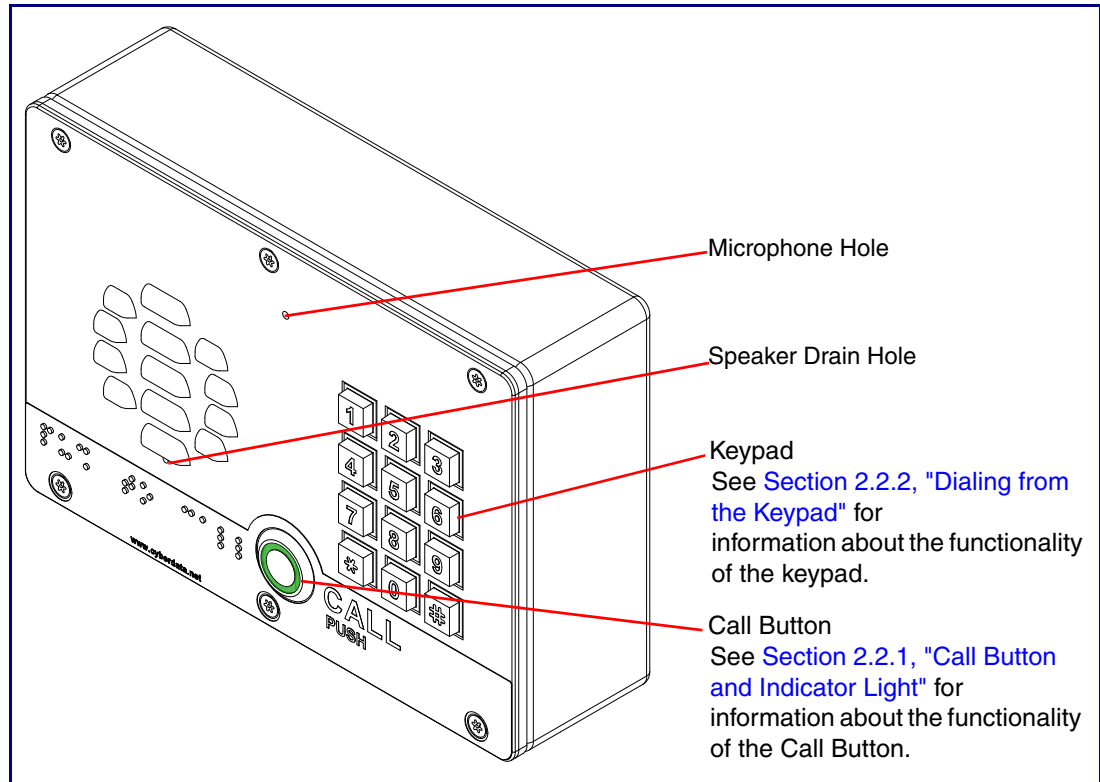
**Table 2-2. Parts List**

Quantity	Part Name	Illustration
1	SIP Outdoor Intercom with Keypad Assembly	
1	Installation Quick Reference Guide	
1	Mounting Accessory Kit	

## 2.2 Intercom Components

Figure 2-1 shows the components of the Intercom.

**Figure 2-1. Intercom Components**



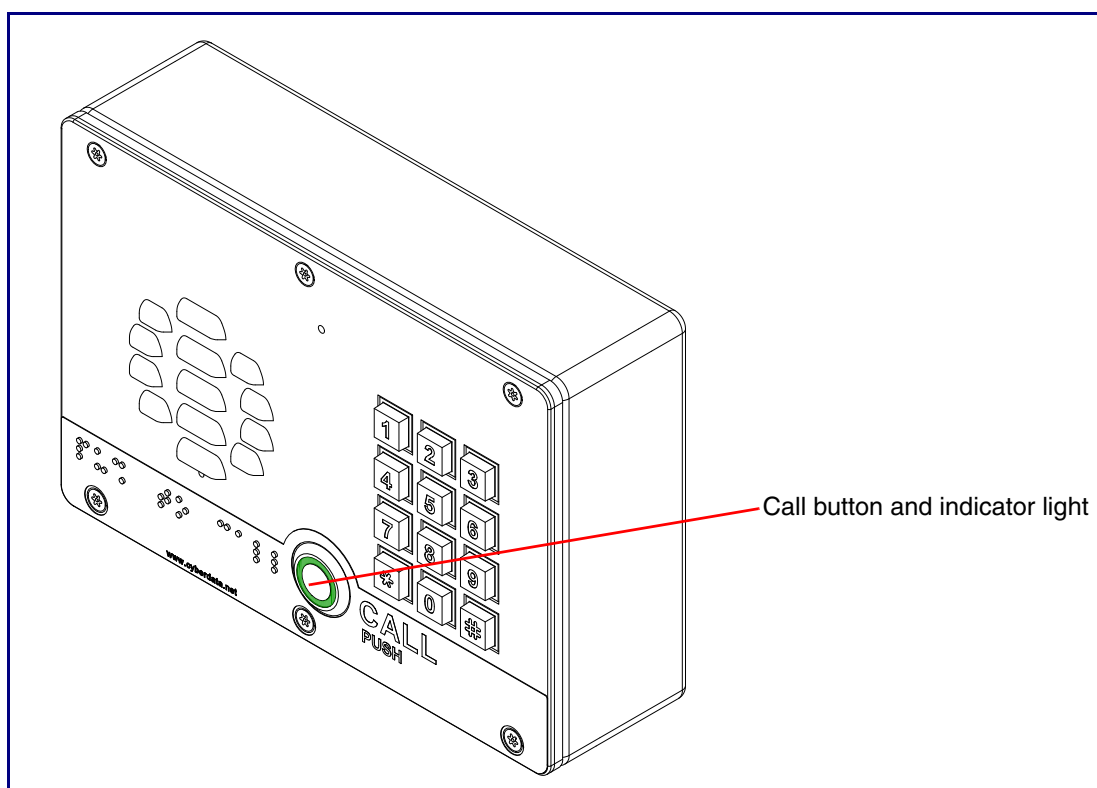
---

## 2.2.1 Call Button and Indicator Light

### 2.2.1.1 Indicator Light Function

- Upon initial power or reset, the Call Button LED will illuminate.
- During network setup the Call Button LED will blink 10 times per second until the device can find a network address. This can take from 5 to 60 seconds.
- When the software has finished initialization, the Call Button LED will blink twice.
- When a call is established (not just ringing), the Call Button LED will blink.
- On the **Device Configuration Page**, there is an option called **Button and Keypad Lit when Idle**. This option sets the normal state for the indicator light. The indicator light will still blink during initialization and calls.
- The indicator light flashes briefly at the beginning of RTFM mode.

**Figure 2-2. Call Button and Indicator Light**



---

## 2.2.2 Dialing from the Keypad


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

## 2.3 Intercom Setup


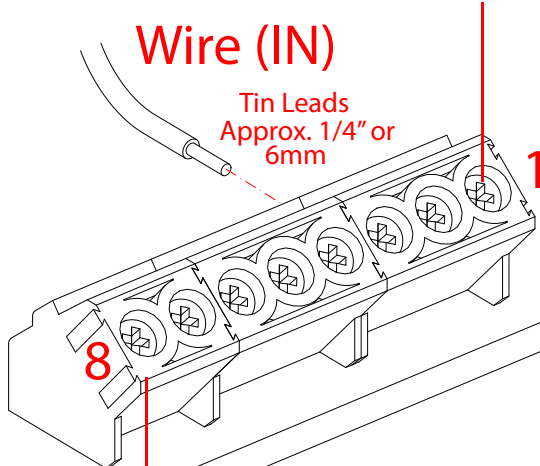
### 2.3.1 Intercom Connections

**Figure 2-3** shows the pin connections on the terminal block. This terminal block can accept 16 AWG gauge wire.

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

 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>
--	--

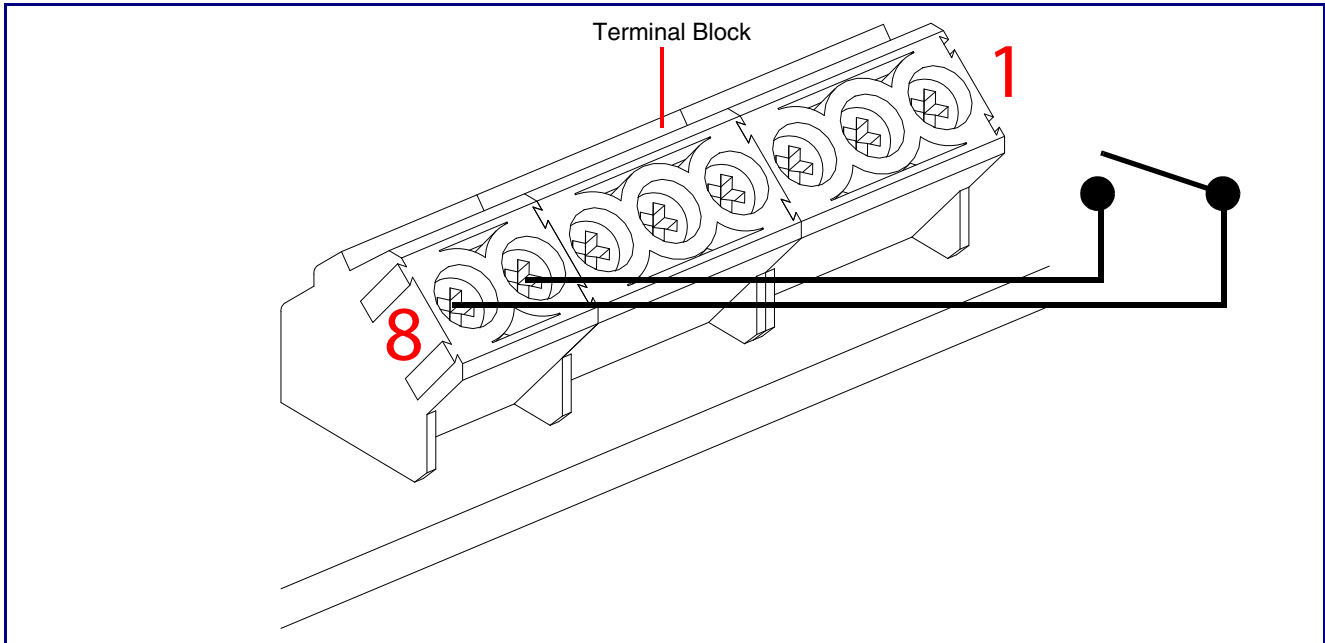
**Figure 2-3. Connections and Alternate Power Input**

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



## 2.3.2 Using the On-Board Relay

 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>
 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>
 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.

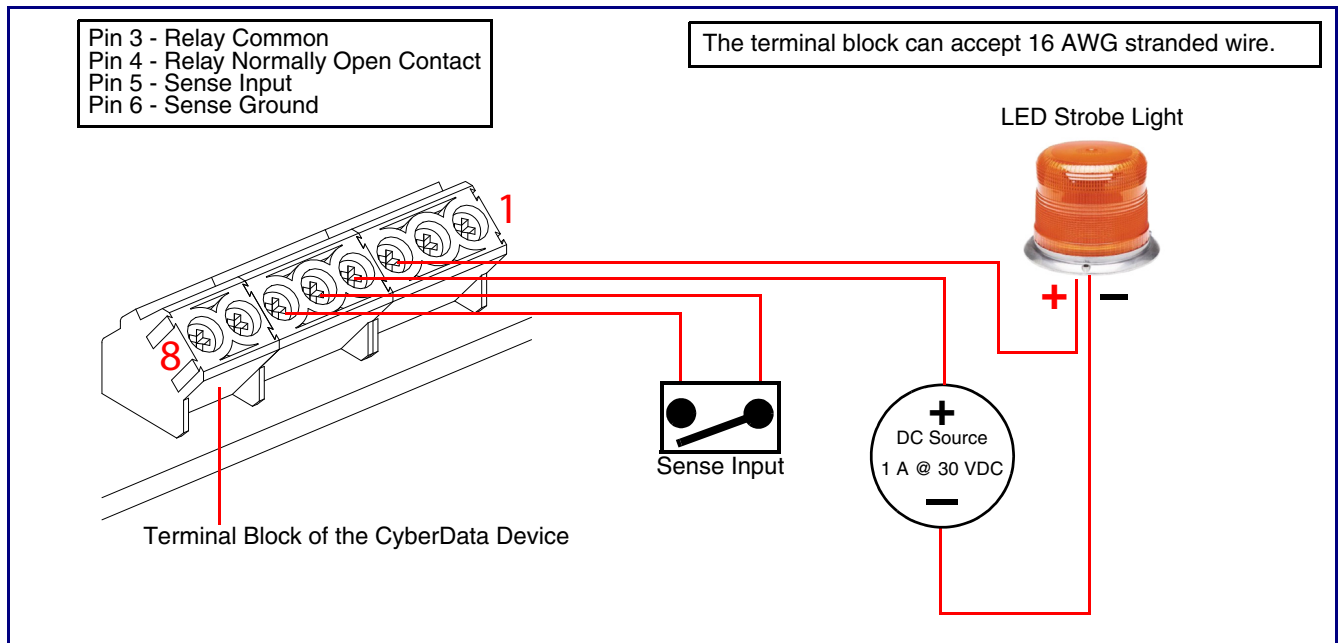
## 2.3.3 Wiring the Circuit

### 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 2-5](#) for the wiring diagram.

When configuring with an inductive load, please use an intermediary relay with a High PIV Ultrafast Switching Diode. We recommend using the 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 2-5. 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 2-6](#) and [Figure 2-7](#) for the wiring diagrams.

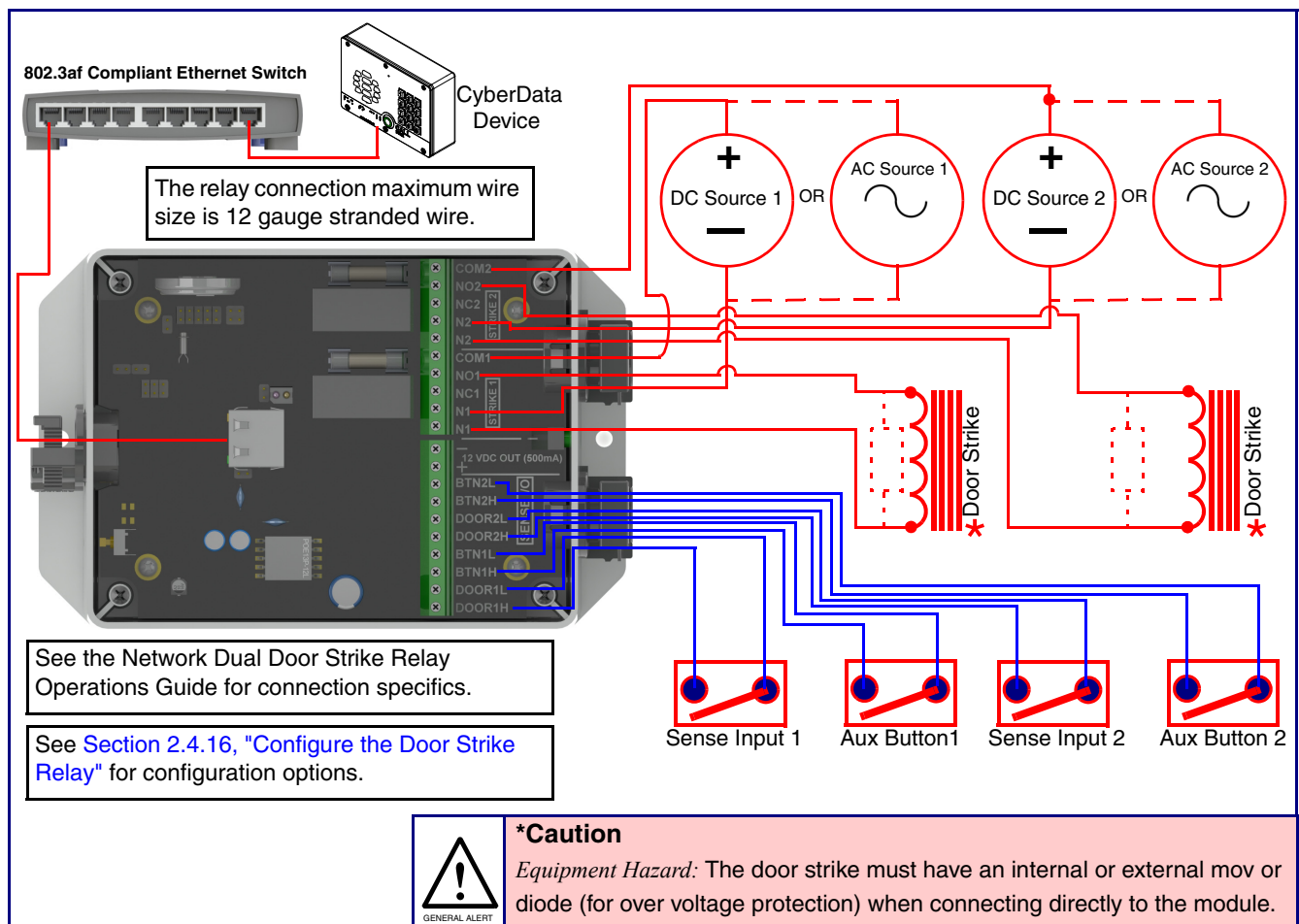


GENERAL ALERT

**Warning**

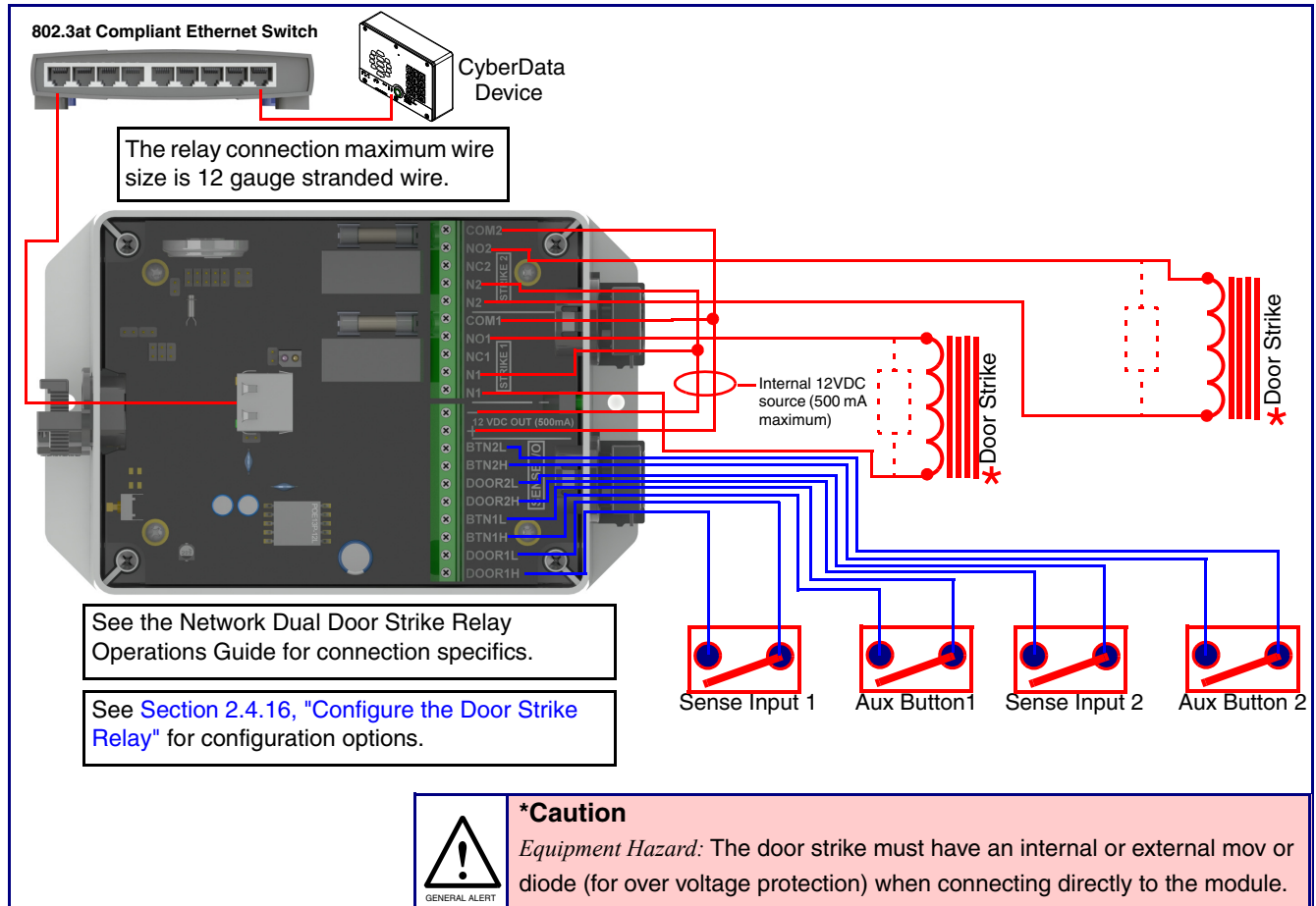
*Electrical Hazard:* Hazardous voltages may be present. No user serviceable part inside. Refer to qualified service personnel for connecting or servicing.

**Figure 2-6. 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 2-7. 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:

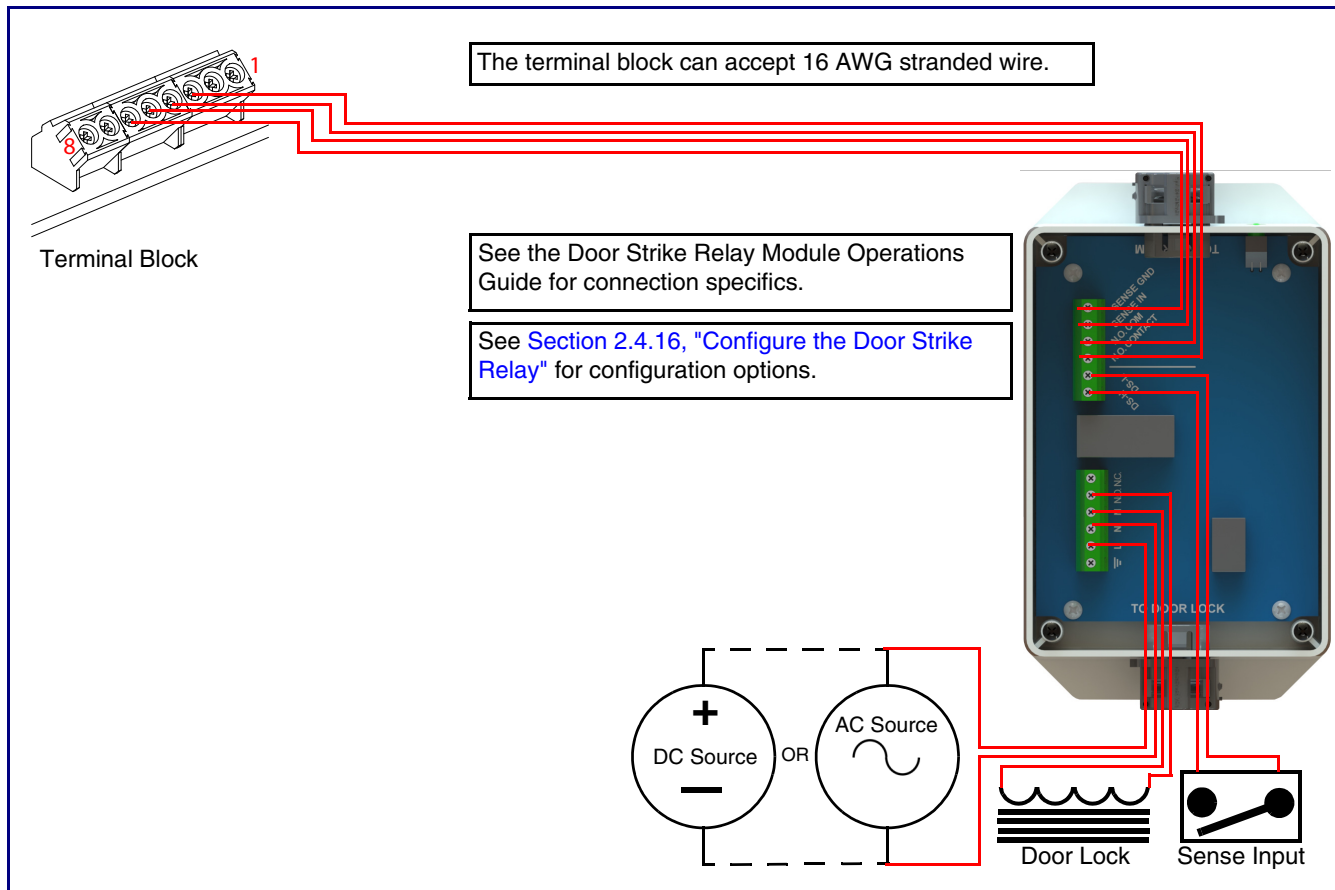
<http://support.cyberdata.net/>

#### 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 2-8](#) for the wiring diagram.

### Figure 2-8. Door Strike Relay Module Wiring Diagram from Intercom



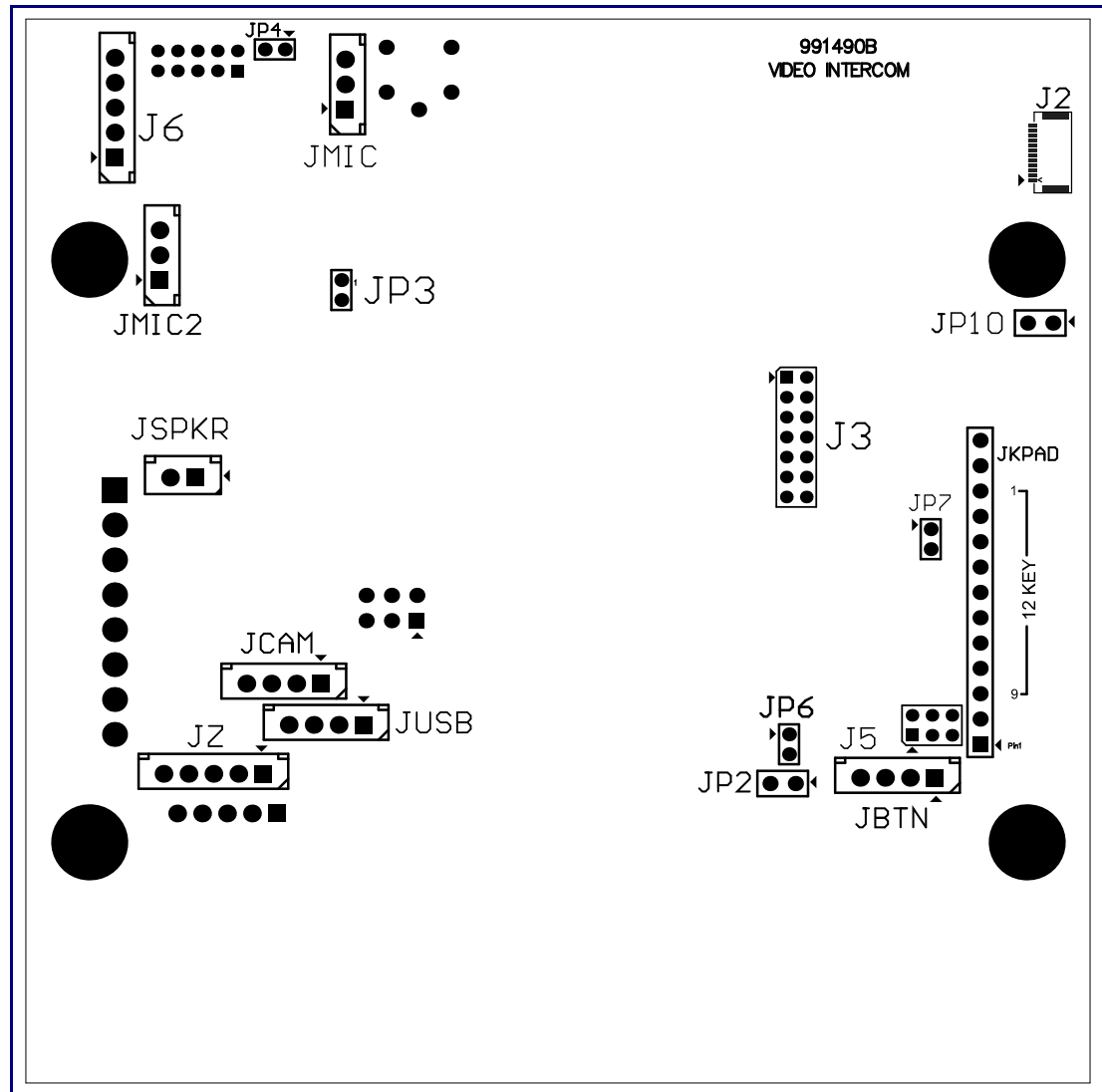
If you have questions about connecting door strikes or setting up the web configurable options, please contact our support department at the following website:

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

## 2.3.4 Intercom Connectors

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

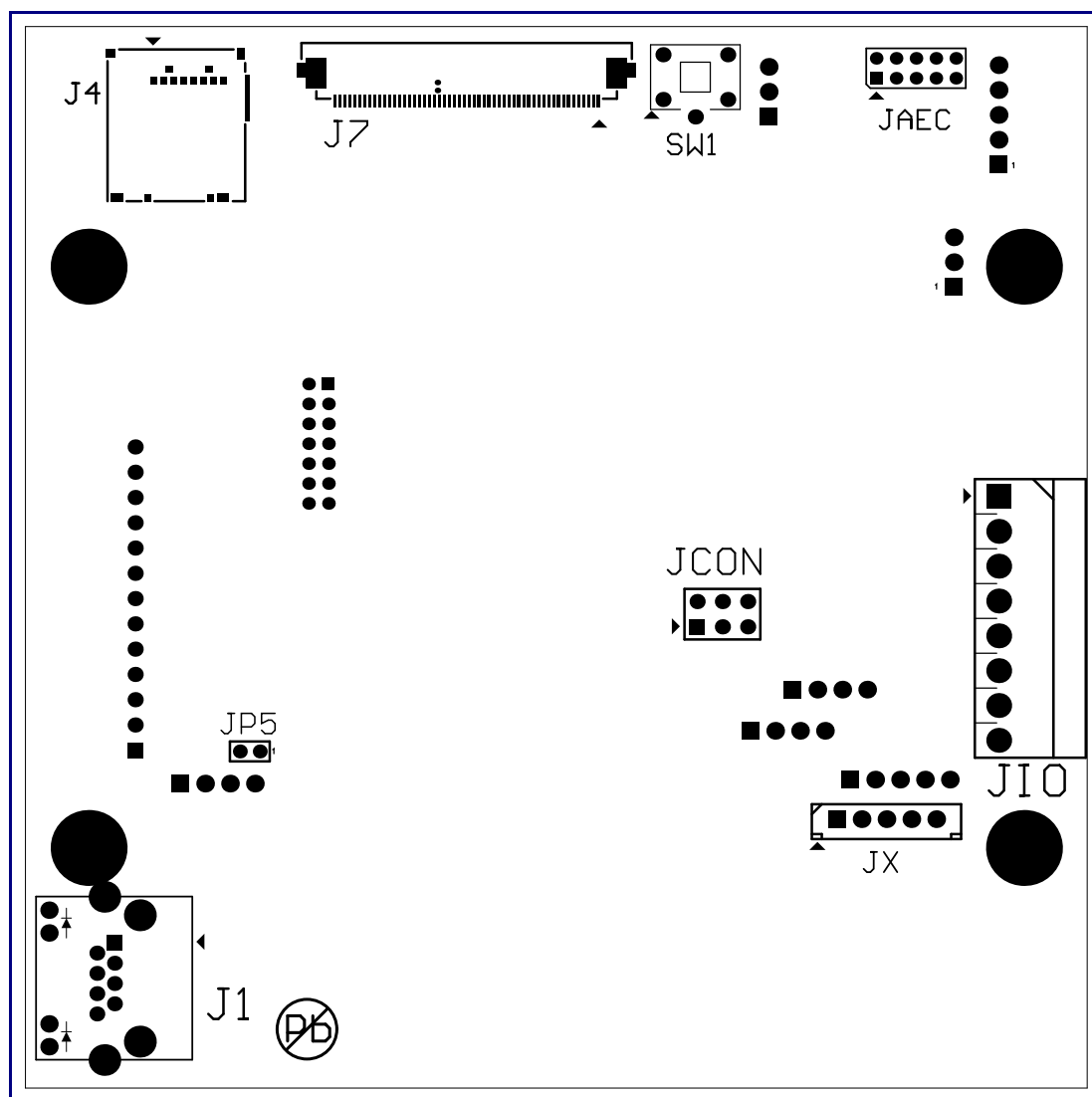
**Figure 2-9. Connector Locations—Board Top**



**Table 2-3. 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 2-4. 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 2-3</a> )
JP5	Reset jumper <sup>a</sup>
JX	Auxiliary Strobe Connector
SW1	See <a href="#">Section 2.3.6, "RTFM Button"</a>

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

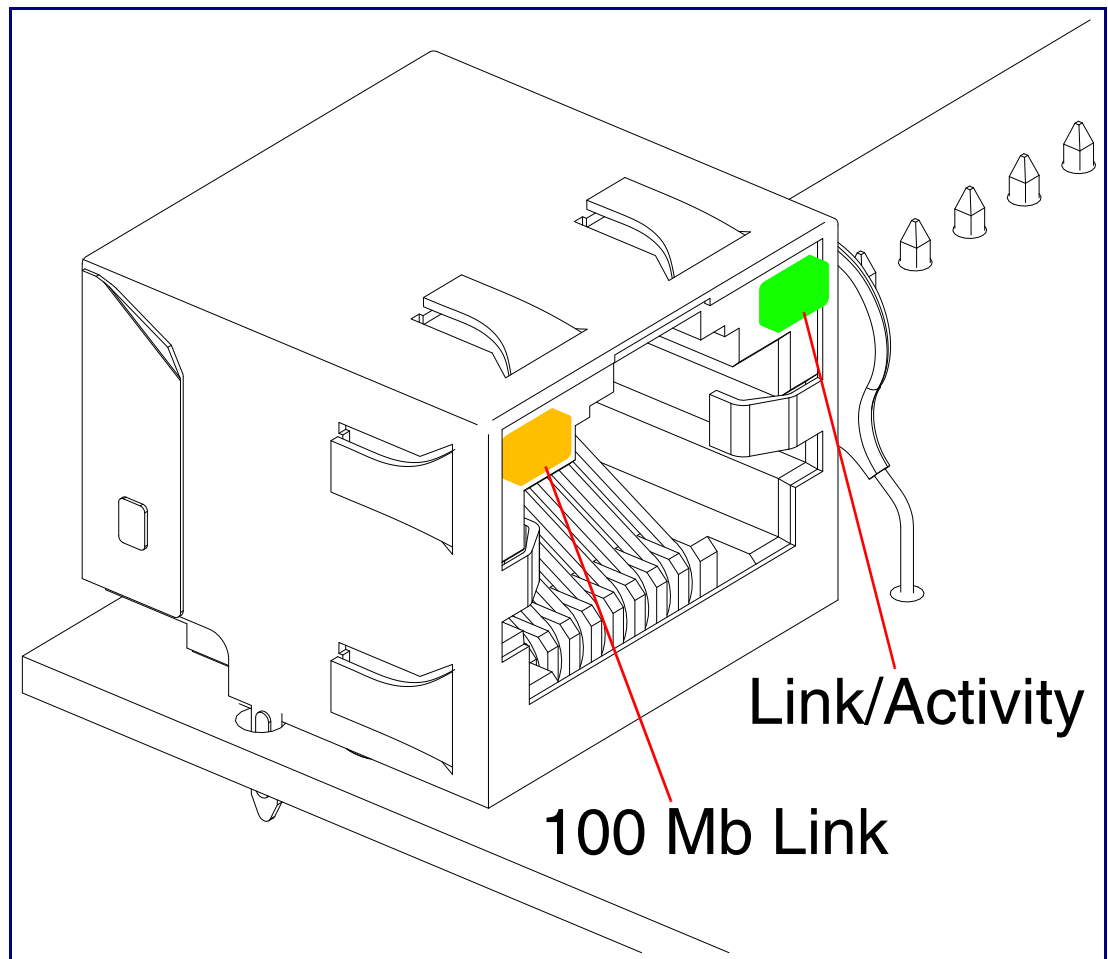
## 2.3.5 Activity and Link LEDs

### 2.3.5.1 Verifying the Network Connectivity and Data Rate

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

- The square, **GREEN 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**





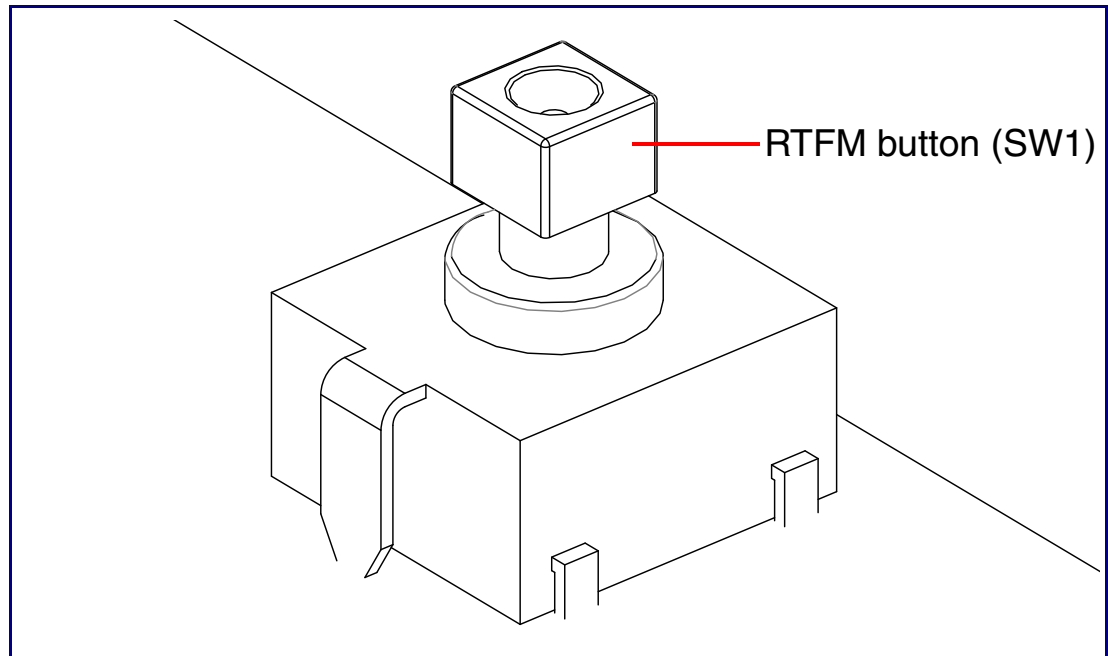
---

## 2.3.6 RTFM Button

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

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

**Figure 2-12. RTFM Button**



### 2.3.6.1 Announcing the IP Address

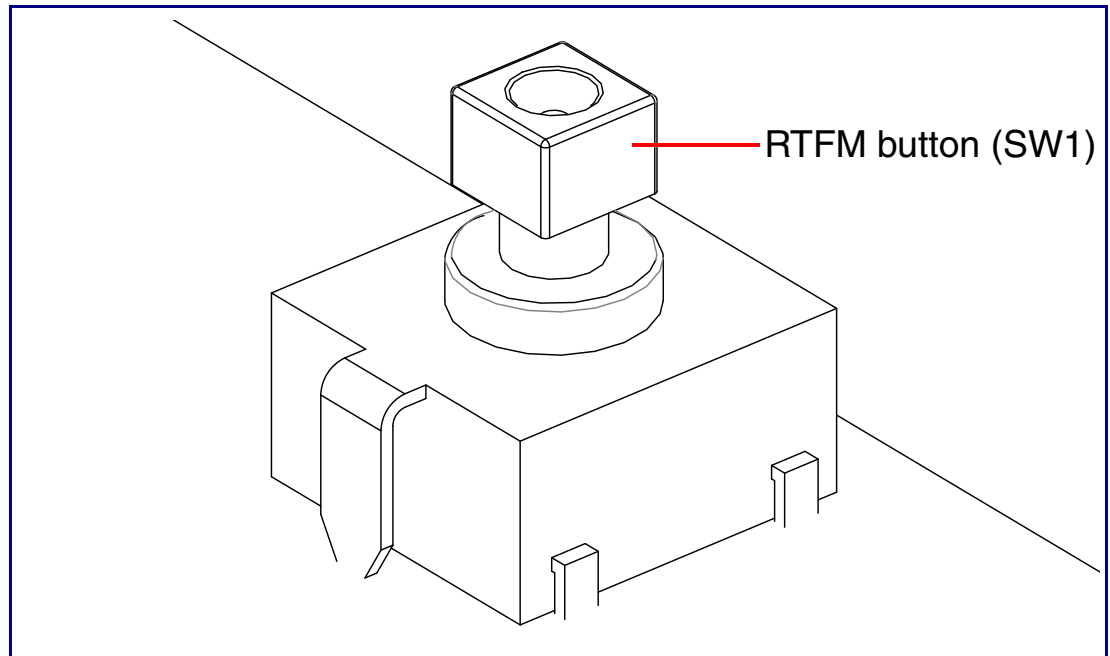
To announce a device's current IP address:

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

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

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

**Figure 2-13. RTFM Button**



### 2.3.6.2 Restoring the Factory Default Settings

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

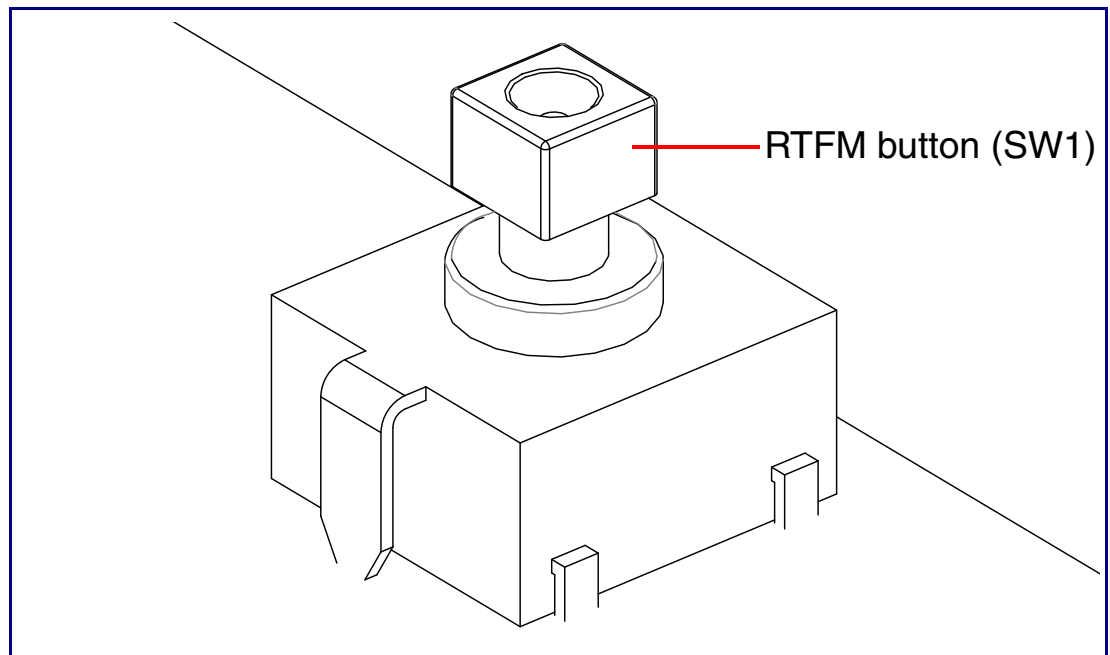
**Note** Each Intercom is delivered with factory set default values.

To restore the factory default settings:

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

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

**Figure 2-14. RTFM Button**



---

### 2.3.7 Adjust the Volume

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

---

## 2.4 Configure the Intercom Parameters

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

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

---

### 2.4.1 Factory Default Settings

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

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

**Table 2-5. Factory Default Settings**

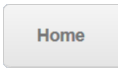
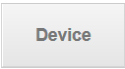
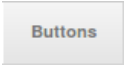

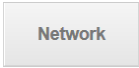
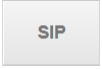

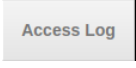

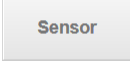
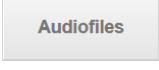
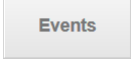


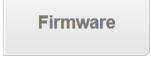
Parameter	Factory Default Setting
IP Addressing	DHCP
IP Address <sup>a</sup>	10.10.10.10
Web Access Username	admin
Web Access Password	admin
Subnet Mask <sup>a</sup>	255.0.0.0
Default Gateway <sup>a</sup>	10.0.0.1

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

## 2.4.2 Intercom Web Page Navigation

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

**Table 2-6. Web Page Navigation**

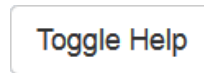
Web Page Item	Description
	Link to the <b>Home</b> page.
	Link to the <b>Device</b> page.
	Link to the <b>Buttons</b> page.
	Link to the <b>Security</b> page.
	Link to the <b>Network</b> page.
	Link to go to the <b>SIP</b> page.
	Link to the <b>Multicast</b> page.
	Link to the <b>Access Log</b> page.
	Link to the <b>SSL</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:

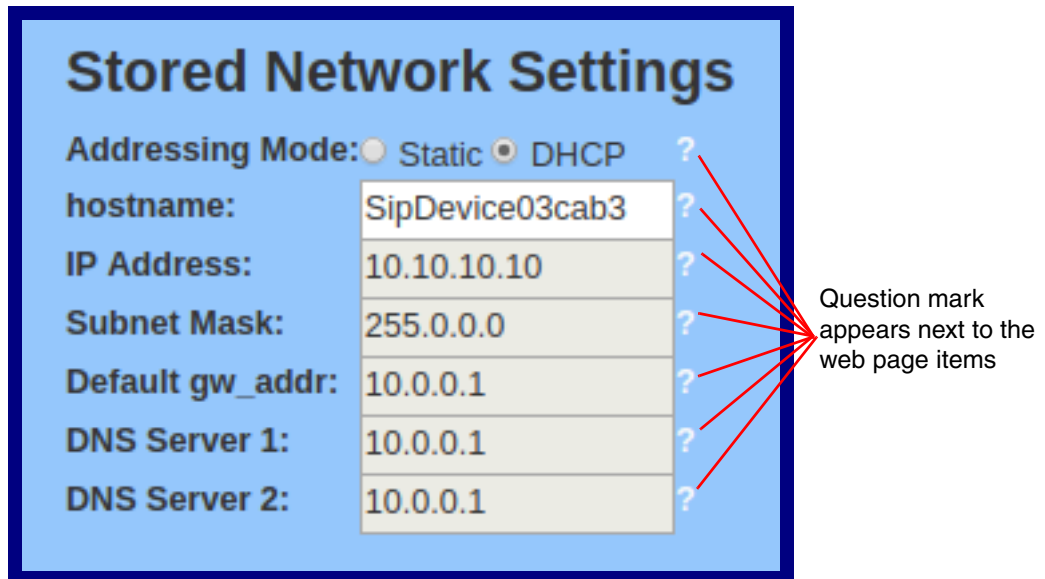
1. Click on the **Toggle Help** button that is on the UI webpage. See [Figure 2-15](#) and [Figure 2-16](#).

**Figure 2-15. Toggle/Help Button**



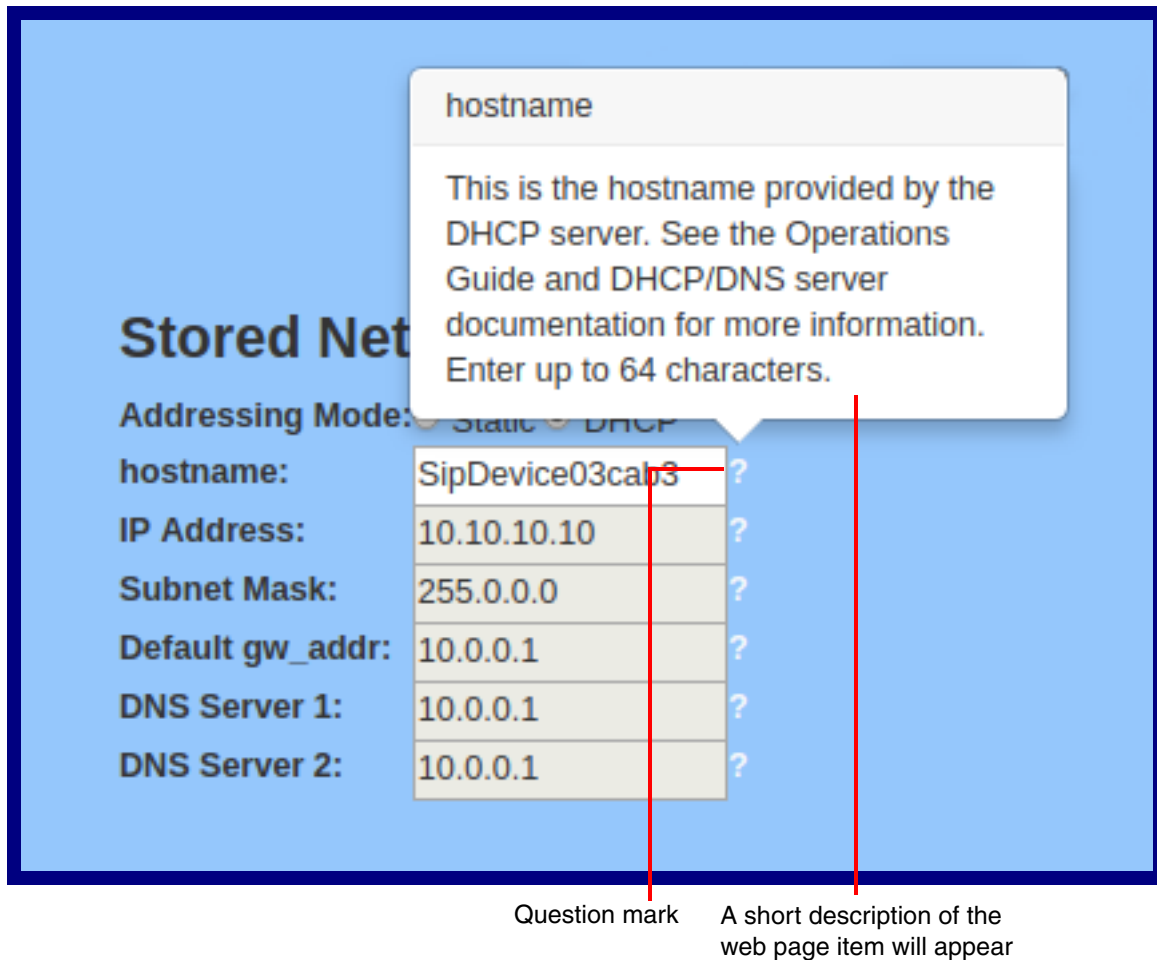
2. You will see a question mark (?) appear next to each web page item that has been provided with a short description by the Help feature. See [Figure 2-16](#).

**Figure 2-16. Toggle Help Button and Question Marks**



3. Move the mouse pointer to hover over the question mark (?), and a short description of the web page item will appear. See [Figure 2-17](#).

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



---

## 2.4.4 Log in to the Configuration Home Page

1. Open your browser to the Intercom IP address.

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

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

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

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

<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 2-18):

Web Access Username: **admin**

Web Access Password: **admin**



Figure 2-18. Home Page

Home
Device
Buttons
Security
Network
SIP
SSL
Multicast
Access Log
Sensor
Audiofiles
Events
DSR
Autoprov
Firmware

# CyberData Keypad Intercom

### Current Status

Serial Number: 214200001

Mac Address: 00:20:f7:03:fd:5b

Firmware Version: v20.0.0

Partition 2: v20.0.0

Partition 3: v20.0.0

Booting From: partition 2

Boot From Other Partition

### Admin Settings

Username: admin

Password: \*\*\*\*\*

Confirm Password: \*\*\*\*\*

Save Reboot Toggle Help

### Import Settings

Browse... No file chosen

Import Config

### Export Settings

Export Config

IP Addressing: DHCP

IP Address: 10.10.0.103

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

Nightringer: Disabled

Primary SIP Server: Not registered

Backup Server 1: Not registered

Backup Server 2: Not registered

Nightringer Server: Not registered

Intrusion Sensor: Inactive

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

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

**Table 2-7. Home Page Overview**


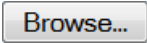





Web Page Item	Description
<b>Admin Settings</b>	
Username ?	The username to access the web interface. Enter up to 25 characters.
Password ?	The password to access the web interface. Enter up to 25 characters.
Confirm Password ?	Confirm the web interface password.
<b>Current Status</b>	
Serial Number	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 2-7. Home Page Overview (continued)

Web Page Item	Description
Nightringer Server	Shows the current status of Nightringer Server.
Intrusion Sensor	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 2-19](#).

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

Home Device Buttons Security Network SIP SSL Multicast Access Log Sensor Audiofiles Events DSR Autopro Firmware

# CyberData Keypad Intercom

### Volume Settings (0-9)

SIP Volume:

Multicast Volume:

Ring Volume:

Sensor Volume:

Push to Talk Volume:

### 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:

### Microphone Settings (0-9)

Microphone Gain:

Push to Talk Microphone Gain:

### Misc Settings

Device Name:

Auto-Answer Incoming Calls: ☒

Button Lit when Idle: ☒

Button Brightness (0-255):

Keypad Lit when Idle: ☒

Keypad Brightness (0-255):

Play Ringback Tone: ☐

Enable Push to Talk: ☐

Enable DTMF Push to Talk: ☐

Prevent Call Termination: ☐

Disable HTTPS (NOT recommended): ☐

Enable NTP: ☒

NTP Server:

Timezone:

Current Time: Tue, 20 Nov 2018 13:52:26

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 2-8](#).

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

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

Web Page Item	Description
<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 (0-9)</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.  Examples: America/Los_Angeles America/New_York Europe/London America/Toronto  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 2-8. 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 Relay on Button Press Duration 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.
Keypad Lit When Idle ?	When selected, the keypad is illuminated while the device is idle (a call is not in progress).
Keypad Brightness (0-255) ?	The desired keypad 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 2-8. 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) ?	Disables the encrypted connection to the webpage. We do not recommend disabling HTTPS for security reasons.
Test Audio	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.
Test Microphone	<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 play back the recorded audio.</li> </ol>
Test Relay	Click on the <b>Test Relay</b> button to do a relay test.
Save	Click the <b>Save</b> button to save your configuration settings.
Reboot	Click on the <b>Reboot</b> button to reboot the system.
Toggle Help	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 Button Parameters

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

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

Home Device Buttons Security Network SIP SSL Multicast Access Log Sensor Audiofiles Events DSR Autopro Firmware

# CyberData Keypad Intercom

### Dial Mode

Enable Telephone Operation: ☐

Enable Cell Phone Operation: ☐

Enable Speed Dial Operation: ☐

Enable Security Operation: ☐

### Security Mode Settings

Relay Activation Code: 9876123

Relay Deactivation Code: 9876456

Allow Telephone Dialout: ☒

Call Button: 204 ID: id204

Send Multicast Audio: ☒

Multicast Address: 224.5.5.5

Multicast Port: 5050

Repeat Message: 1

### Speed Dial Settings

Speed Dial Timeout: 2

Keypad 1:	241	ID: id241
Keypad 2:	242	ID: id242
Keypad 3:	243	ID: id243
Keypad 4:	244	ID: id244
Keypad 5:	245	ID: id245
Keypad 6:	246	ID: id246
Keypad 7:	247	ID: id247
Keypad 8:	248	ID: id248
Keypad 9:	249	ID: id249
Keypad 0:	2411	ID: id2411
Keypad *:	2410	ID: id2410
Keypad #:	2412	ID: id2412
Call Button:	204	ID: id204

### Button Tones

Play Button Tones: ☒

Save Reboot

Start Button Test Toggle Help









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

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

Web Page Item	Description
<b>Dial Mode</b>	
Enable Telephone Operation ?	Dial extensions like a normal telephone. Pressing the call button will start a dial tone. Pressing the call button in a call will cancel a call.
Enable Cellphone Operation ?	Enter your extension and press the call button to start the call. Press the call button again to cancel the call.
Enable Speed Dial Operation ?	In speed dial mode every button can be configured to call a different extension when pressed.
Enable Security Operation ?	Security mode allows the user to secure the local or remote relay by requiring a code (up to 8 digits) to be entered into the device's keypad. The security codes may be entered within a phone call to a preset extension or independently. Security codes start with the pound key (#) and will be recognized when the user stops pressing buttons or hits the pound key again.
<b>Security Mode Settings</b>	
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. 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. Enter up to 25 digits (* and # are supported).
Allow Telephone Dialout ?	When enabled, the user will be able to use the keypad to dial while the device is in Security mode.
Call Button ?	Dial this extension when the call button is pressed. Up to 64 characters.
ID ?	Type the desired Extension ID. Up to 64 characters.
Send Multicast Audio ?	When selected, the device will play an audio file to the specified multicast address and port. <b>Note:</b> The keypad must be in Security mode to send Multicast Audio.
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>Speed Dial Settings</b>	
Speed Dial Timeout ?	The amount of time you must hold the button before it calls the configured extension. When this is set to 0 the phone will dial the configured extension as soon as the button is released.
Keypad 1	Dial this extension when the 1 key is pressed.
Keypad 2	Dial this extension when the 2 key is pressed.
Keypad 3	Dial this extension when the 3 key is pressed.
Keypad 4	Dial this extension when the 4 key is pressed.
Keypad 5	Dial this extension when the 5 key is pressed.
Keypad 6	Dial this extension when the 6 key is pressed.
Keypad 7	Dial this extension when the 7 key is pressed.

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

Web Page Item	Description
Keypad 8	Dial this extension when the 8 key is pressed.
Keypad 9	Dial this extension when the 9 key is pressed.
Keypad 0	Dial this extension when the 0 key is pressed.
Keypad *	Dial this extension when the * key is pressed.
Keypad #	Dial this extension when the # key is pressed.
Call Button	Dial this extension when the call button is pressed.
Button Tones	
Play Button Tones 	Play a tone when the keypad buttons are pressed.
	Click the <b>Save</b> button to save your configuration settings.
	Click on the <b>Reboot</b> button to reboot the system.
	Click on the <b>Start</b> button to start a button test.
	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.

#### 2.4.6.1 Dial Out Extension Strings and DTMF Tones (using rfc2833)

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

**Table 2-10. 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 25.

### 2.4.6.2 Triggering a Dial Out Call or Security Code

You can instantly trigger a dial out call or security code by pressing the # key after dialing a number. [Table 2-11](#) shows the various actions that result from different keypad input.

**Table 2-11. Triggering a Dial Out Call or Security Code**

<b>Allow Telephone Dialout Option Enabled (in security mode with default security settings)</b>	
<b>Input</b>	<b>Resulting Action</b>
Dialing <b>123</b> (and waiting for several seconds)	The device will call extension <b>123</b> through the default SIP server.
Dialing <b>#123</b> (and waiting for several seconds)	The device will do nothing. The entry is an unrecognized security entry.
Dialing <b>#1234560</b> (and waiting for several seconds)	The device will activate the relay for <b>Security Code 0</b> for <b>6</b> seconds.
Dialing <b>#124560#</b>	The device will instantly activate the relay for <b>6</b> seconds.
Dialing <b>123#</b>	The device will instantly call extension <b>123</b> through the default SIP server.
<b>Allow Telephone Dialout Option Disabled (in security mode with default security settings)</b>	
<b>Input</b>	<b>Resulting Action</b>
Dialing <b>123456</b> (and waiting several seconds)	The device will activate the relay specified on the <a href="#">Security Configuration Page</a> (local or DSR) for the seconds specified in the <a href="#">Relay Timeout (seconds)</a> setting.
Dialing <b>9876123</b> (and waiting several seconds)	The device will activate the local relay.
Dialing <b>9876456</b> (and waiting several seconds)	The device will deactivate the local relay.

## 2.4.7 Configure the Security

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

**Figure 2-21. Security Configuration Page**

ID	Name	Code	Valid From	Valid To	Blacklist	Edit	Delete
1	Jason	123456	All	All	No	Edit	Delete
2	Emily	8523	Wdy	Wdy	No	Edit	Delete
3	Noah	6547	All	All	No	Edit	Delete
4	Emma	7896	All	All	No	Edit	Delete
5	Liam	2569	All	All	No	Edit	Delete
6	Madison	2547	All	All	No	Edit	Delete
7	Mason	7412	All	All	No	Edit	Delete
8	Abigail	6541	All	All	No	Edit	Delete
9	Jacob	2569	Wnd	Wnd	No	Edit	Delete
10	Olivia	0147	All	All	No	Edit	Delete
11	William	0122	All	All	No	Edit	Delete
12	Isabella	9632	All	All	No	Edit	Delete
13	Ethan	5698	All	All	Blacklisted	Edit	Delete
14	Hannah	8412	All	All	No	Edit	Delete
15	James	3689	All	All	No	Edit	Delete
16	Samantha	7452	All	All	No	Edit	Delete
17			All	All	No	Add	Delete
18			All	All	No	Add	Delete

2. On the **Security** page, you may 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. Security Configuration Parameters**




Web Page Item	Description
<b>Security Settings</b>	
ID ?	Displays the ID associated with this security record.
Name ?	Displays the name associated with this security record.
Code ?	Displays the security code associated with this security record.
Valid From ?	See <a href="#">Section 2.4.7.2, "The "Valid From" and "Valid To" Settings"</a> .
Valid To ?	See <a href="#">Section 2.4.7.2, "The "Valid From" and "Valid To" Settings"</a> .
Blacklist ?	Displays the Blacklisted status of this security record. Blacklist is used to deny entry to the specified security code. Entering a blacklisted code will trigger the buzzer, and can trigger a call to an extension or a multicast of a pre-recorded message.
	Opens the <a href="#">Configure Security Code Page</a> . See <a href="#">Section 2.4.7.1, "Configure the Security Code Page"</a> .
	Removes the security code record.
	Opens a new Configure Security Code window.
<b>Relay Settings</b>	
Activate Relay on Valid Code ?	Activates the relay when a valid code is entered. This would likely be used to open a door.
Activate DSR on Valid Code ?	Activates the remote relay when a valid code is entered. This would likely be used to open a door.
Relay Timeout (seconds) ?	Specifies how many seconds the relay will be activated after a valid code entry. In a typical use case, this would specify how long the door is unlocked.
<b>Audio Settings</b>	
Play tone while Relay Active ?	When selected, an audible tone will indicate the relay is active.
Play tone on Invalid Code Entry ?	When selected, a tone will play on the speaker to indicate an invalid code was entered.
<b>Sensor Settings</b>	
Buzz on Door Open Timeout ?	When selected, the buzzer will beep until the on board sensor is deactivated.
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.
Sensor Open Timeout (in seconds) ?	The time (in seconds) the device will wait before it triggers the buzzer when the door sensor is active.
DSR Open Timeout (in seconds) ?	The time (in seconds) the device will wait before it triggers the buzzer when the remote door sensor (DSR) is active.

Table 2-12. Security Configuration Parameters (continued)

Web Page Item	Description
<b>Blacklist Actions</b>	
Play Message to SIP Extension ?	When selected, the device will make a SIP call and play the “blacklist” audio file when a blacklisted code is entered.
Dial Out SIP Extension ?	The extension that will be dialed if “Play Message to SIP Extension” is selected above. Enter up to 64 alphanumeric characters.
Dial Out SIP ID ?	Additional caller identification string added to outbound calls. Enter up to 64 alphanumeric characters.
Multicast Audio Message ?	When selected, the device will multicast the “blacklist” audio file to the specified address and port.
Multicast Address ?	The multicast address that the “blacklist” audiofile will be played to.
Multicast Port ?	The multicast port that the “blacklist” audofile will be played to.
Times to Play Multicast Message ?	The number of times the “blacklist” audio file will be played via multicast. Enter a value between 1 and 65535.
<b>Save</b>	Click the <b>Save</b> button to save your configuration settings.
<b>Reboot</b>	Click on the <b>Reboot</b> button to reboot the system.
<b>Export Security Settings</b>	Click on the <b>Export Security Settings</b> button to export the current security list to a file.
<b>Toggle Help</b>	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.

### 2.4.7.1 Configure the Security Code Page

1. Click the **Edit** button to open the **Configure Security Code** page. See [Figure 2-22](#).

Figure 2-22. Configure Security Code Page

## Configure Security Code

Security Code # 9

Name

William B. Smith

Code

123023

Valid From

All

Valid To

All

Blacklist



☐

Save Changes

Cancel

2. On the **Configure Security Code** page, you may enter values for the parameters indicated in [Table 2-12](#).

**Table 2-13. Security Code Page Parameters**

Web Page Item	Description
<b>Security Configuration</b>	
Name ?	Enter name.
Code ?	Enter a security code, maximum 8 digits, must be distinct.
Valid From ?	See <a href="#">Section 2.4.7.2, "The "Valid From" and "Valid To" Settings"</a> .
Valid To ?	See <a href="#">Section 2.4.7.2, "The "Valid From" and "Valid To" Settings"</a> .
Blacklist ?	Blacklist is used to deny entry to the specified security code. Entering a blacklisted code will trigger the buzzer, and can trigger a call to an extension or a multicast of a pre-recorded message.
	Saves the changes of the security configuration.
	Cancels the changes of the security configuration.



### 2.4.7.2 The “Valid From” and “Valid To” Settings

**ValidFrom** and **ValidTo** fields specify the day(s) a security code is valid, and, optionally the time, in 24:00 format.

The Day of the week can be **Mon**, **Tue**, **Wed**, **Thu**, **Fri**, **Sat**, **Sun**, or one of the special identifiers: **All**, **Wdy**, and **Wnd**.

**Wdy** indicates weekdays (Monday-Friday).

**Wnd** indicates weekends (Saturday-Sunday).

**All** allows entrance at all times.

A valid string consists of a day of the week or a special identifier, plus an optional time, except if using **All**, which will not use a time.

Some examples:

`<ValidFrom0>Mon9:00</ValidFrom0>`

`<ValidTo0>Fri17:00</ValidTo0>`    monday through friday 9am to 5pm

`<ValidFrom0>All</ValidFrom0>`

`<ValidTo0>All</ValidTo0>`                    all day every day

`<ValidFrom0>All</ValidFrom0>`

`<ValidTo0>All12:00</ValidTo0>`    every day till 12:00

`<ValidFrom0>Mon12:00</ValidFrom0>`

`<ValidTo0>Mon12:00</ValidTo0>`    times are inclusive - this code is only valid on monday at 12:00

`<ValidFrom0>Wdy9:00</ValidFrom0>`

`<ValidTo0>Wdy17:00</ValidTo0>`    Weekdays from 9am to 5pm

**Note**    The identifiers in **to** and **from** must match (for example, **named day/named day**, **Wdy/Wdy**, **Wnd/Wnd**, **All/All**).

**Note**    The device must set time with an **NTP Server** (see the **Device Configuration Page**). If an NTP server is not used, all **Valid From** and **Valid To** fields must be set to **All**.

## 2.4.8 Configure the Network Parameters

1. Click the **Network** menu button to open the **Network** page ([Figure 2-23](#)).

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

Home Device Buttons Security Network SIP SSL Multicast Access Log Sensor Audiofiles Events DSR Autopro Firmware

# CyberData Keypad Intercom

### Stored Network Settings

Addressing Mode: ☒ Static ☐ DHCP

hostname: SipDevice03fd5b

IP Address: 10.10.10.10

Subnet Mask: 255.0.0.0

Default Gateway: 10.0.0.1

DNS Server 1: 10.0.0.1

DNS Server 2: 10.0.0.1

### VLAN Settings

VLAN ID (0-4095): 0

VLAN Priority (0-7): 0

### Current Network Settings

IP Address: 10.10.0.103

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



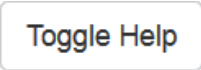
2. On the **Network** page, enter values for the parameters indicated in [Table 2-14](#).

**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. 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> to store changes when configuring a Static address.
Hostname ?	This is the hostname provided by the DHCP server. See the DHCP/DNS server documentation for more information. Enter up to 64 characters.
IP Address ?	Enter the Static IPv4 network address in dotted decimal notation.
Subnet Mask ?	Enter the Subnet Mask in dotted decimal notation.
Default Gateway ?	Enter the Default Gateway IPv4 address in dotted decimal notation.
DNS Server 1 ?	Enter the primary DNS Server IPv4 address in dotted decimal notation.
DNS Server 2 ?	Enter the secondary DNS Server IPv4 address in dotted decimal notation.
DHCP Timeout in seconds ?	Specify the desired time-out duration (in seconds) that the device will wait for a response from the DHCP server before reverting back to the stored static IP address. The stored static IP address may be the last known IP address or the factory default address if no prior DHCP lease was established. Enter up to 8 characters. A value of -1 will retry forever.
<b>VLAN Settings</b>	
VLAN ID (0-4095) ?	Specify the IEEE 802.1Q VLAN ID number. Enter up to 4 digits.  <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.
<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.

Table 2-14. Network 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.

## 2.4.9 Configure the SIP Parameters

1. Click on the **SIP** menu button to open the **SIP** page (Figure 2-24).

**Figure 2-24. SIP Configuration Page**

**CyberData Keypad Intercom**

**SIP Settings**

Enable SIP operation: ☒

Register with a SIP Server: ☒

Primary SIP Server: 10.0.0.253

Primary SIP User ID: 199

Primary SIP Auth ID: 199

Primary SIP Auth Password: \*\*\*\*\*

Re-registration Interval (in seconds): 360

Backup SIP Server 1:

Backup SIP User ID:

Backup SIP Auth ID:

Backup SIP Auth Password:

Re-registration Interval (in seconds): 360

Backup SIP Server 2:

Backup SIP User ID:

Backup SIP Auth ID:

Backup SIP Auth Password:

Re-registration Interval (in seconds): 360

Remote SIP Port: 5060

Local SIP Port: 5060

SIP Transport Protocol: UDP

TLS Version: 1.2 only (recommended)

Verify Server Certificate: ☐

Outbound Proxy:

Outbound Proxy Port: 0

Use Cisco SRST: ☐

Disable rport Discovery: ☐

Unregister on Boot: ☐

Keep Alive Period: 10000

**Nightringer Settings**

SIP Server:

SIP User ID:

SIP Auth ID:

SIP Auth Password:

Re-registration Interval (in seconds): 360

**Call Disconnection**

Terminate Call after delay: 0

**Audio Codec Selection**

Codec: Auto Select

**RTP Settings**

RTP Port (even): 10500

Jitter Buffer: 50

Save Reboot Toggle Help

2. On the **SIP** 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.



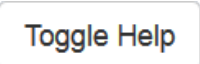
**Table 2-15. SIP Configuration Parameters**

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 2.4.9.1, "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 2-15. 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>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.

**Table 2-15. SIP Configuration Parameters (continued)**

Web Page Item	Description
SIP Auth Password ?	Specify the Authenticate Password for the SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Re-registration Interval (in seconds) ?	The SIP Re-registration Interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
<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.
Jitter Buffer ?	Specify the size of the jitter buffer (in milliseconds) used for SIP calls. Valid values are 50-1000.
	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>



### 2.4.9.1 Point-to-Point Configuration

When the device is set to not register with a SIP server (see [Figure 2-25](#)), 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 2-25. SIP Page Set to Point-to-Point Mode**

The screenshot shows the 'SIP Settings' page of the CyberData Keypad Intercom. The page has a navigation bar at the top with tabs: Home, Device, Buttons, Security, Network, SIP, SSL, Multicast, Access Log, Sensor, Audiofiles, Events, DSR, Autopro, and Firmware. The main title is 'CyberData Keypad Intercom'. Below the title, there are two main sections: 'SIP Settings' and 'Nightringer Settings'. In the 'SIP Settings' section, the 'Enable SIP operation:' checkbox is checked. The 'Register with a SIP Server:' checkbox is unchecked, and a red box highlights this checkbox and the 'Primary SIP Server:' field. The 'Primary SIP Server:' field contains the value '10.0.0.253'. Other fields in the 'SIP Settings' section include 'Primary SIP User ID:' (199), 'Primary SIP Auth ID:' (199), 'Primary SIP Auth Password:' (masked with asterisks), 'Re-registration Interval (in seconds):' (360), 'Backup SIP Server 1:', 'Backup SIP User ID:', 'Backup SIP Auth ID:', 'Backup SIP Auth Password:', and 'Re-registration Interval (in seconds):' (360). The 'Nightringer Settings' section includes 'SIP Server:', 'SIP User ID:', 'SIP Auth ID:', 'SIP Auth Password:', 'Re-registration Interval (in seconds):' (360), 'Call Disconnection' with 'Terminate Call after delay:' (0), and 'Audio Codec Selection' with 'Codec:' (Auto Select).

Device is set to NOT register with a SIP server

## 2.4.10 Configure the SSL Parameters

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

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

Home Device Buttons Security Network SIP **SSL** Multicast Access Log Sensor Audiofiles Events DSR Autoprov Firmware

# CyberData Keypad Intercom

### Server CAs

**Browse...** No file chosen

Import CA Certificate

Restore Defaults Remove All

Toggle Help

### Client Certificate

```

subject=
countryName      = US
stateOrProvinceName = California
localityName     = Monterey
organizationName  = Cyberdata
commonName       = Cyberdata_Dev
notBefore=Mar 22 16:50:02 2017 GMT
notAfter=Mar 20 16:50:02 2027 GMT
                    
```

Client CA

### Test SSL Connection

Server: 10.0.0.253

Port: 5060

Test TLS Connection

### List of Trusted CAs

1	CyberData_CA.pem	Info	Remove
2	DST_ACES_CA_X6.crt	Info	Remove
3	DST_Root_CA_X3.crt	Info	Remove
4	Deutsche_Telekom_Root_CA_2.crt	Info	Remove
5	DigiCert_Assured_ID_Root_CA.crt	Info	Remove
6	DigiCert_Assured_ID_Root_G2.crt	Info	Remove
7	DigiCert_Assured_ID_Root_G3.crt	Info	Remove
8	DigiCert_Global_Root_CA.crt	Info	Remove
9	DigiCert_Global_Root_G2.crt	Info	Remove
10	DigiCert_Global_Root_G3.crt	Info	Remove
11	DigiCert_High_Assurance_EV_Root_CA.crt	Info	Remove
12	DigiCert_Trusted_Root_G4.crt	Info	Remove

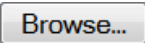

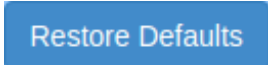




**Figure 2-27. SSL Configuration Page**

13	Equifax_Secure_CA.crt	Info	Remove
14	Equifax_Secure_Global_eBusiness_CA.crt	Info	Remove
15	Equifax_Secure_eBusiness_CA_1.crt	Info	Remove
16	GeoTrust_Global_CA.crt	Info	Remove
17	GeoTrust_Global_CA_2.crt	Info	Remove
18	GeoTrust_Primary_Certification_Authority.crt	Info	Remove
19	GeoTrust_Primary_Certification_Authority_-_G2.crt	Info	Remove
20	GeoTrust_Primary_Certification_Authority_-_G3.crt	Info	Remove
21	GeoTrust_Universal_CA.crt	Info	Remove
22	GeoTrust_Universal_CA_2.crt	Info	Remove
23	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G4.crt	Info	Remove
24	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5.crt	Info	Remove
25	VeriSign_Universal_Root_Certification_Authority.crt	Info	Remove
26	Verisign_Class_1_Public_Primary_Certification_Authority.crt	Info	Remove
27	Verisign_Class_1_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
28	Verisign_Class_2_Public_Primary_Certification_Authority_-_G2.crt	Info	Remove
29	Verisign_Class_2_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
30	Verisign_Class_3_Public_Primary_Certification_Authority.crt	Info	Remove
31	Verisign_Class_3_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
32	asterisk34.crt.pem	Info	Remove
33	thawte_Primary_Root_CA.crt	Info	Remove
34	thawte_Primary_Root_CA_-_G2.crt	Info	Remove
35	thawte_Primary_Root_CA_-_G3.crt	Info	Remove

2. On the **SSL** 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.

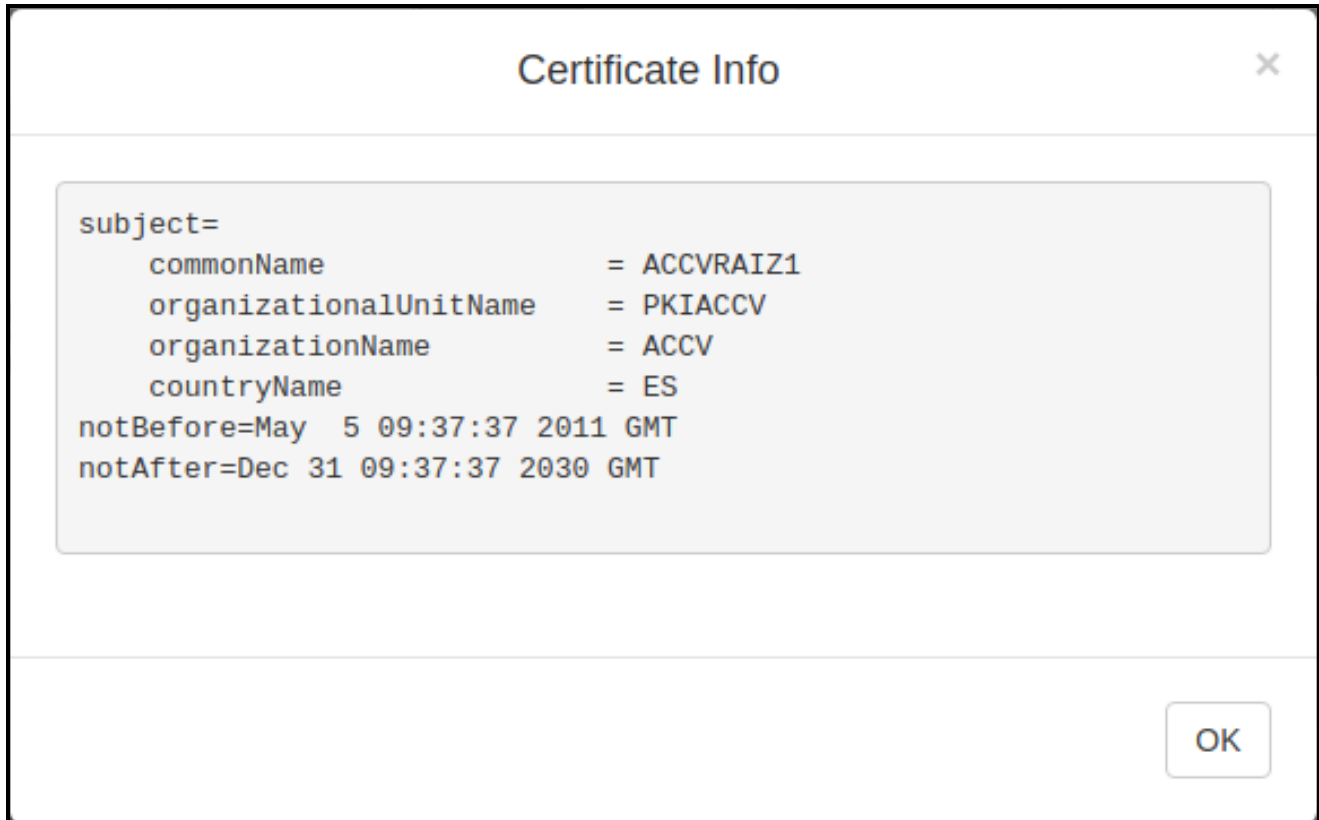
**Table 2-16. SSL Configuration Parameters**

Web Page Item	Description
<b>Server 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.
<b>Client Certificate</b>	
Client CA ?	When doing mutual authentication this device will present a client certificate with these parameters. Right click and <b>Save Link As...</b> to get the Cyberdata CA used to sign this client certificate.
<b>Test SSL Connection</b>	
Server ?	The ssl test server address as a fully qualified domain name or in IPv4 dotted decimal notation.
Port ?	The ssl test server port. The supported range is 0-65536. SIP connections over TLS to port 5060 will do the same.
	Use this button to test a TLS connection to a remote server. 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.
<b>List of Trusted CAs</b>	
	Provides details of the certificate. After clicking on this button, the <b>Certificate Info Window</b> appears. See <a href="#">Section 2.4.10.1, "Certificate Info Window"</a> .
	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 2.4.10.2, "Remove Server Certificate Window"</a> .

### 2.4.10.1 Certificate Info Window

The **Certificate Info Window** provides details of the certificate. This window appears after clicking on the **Info** button. See [Figure 2-28](#).

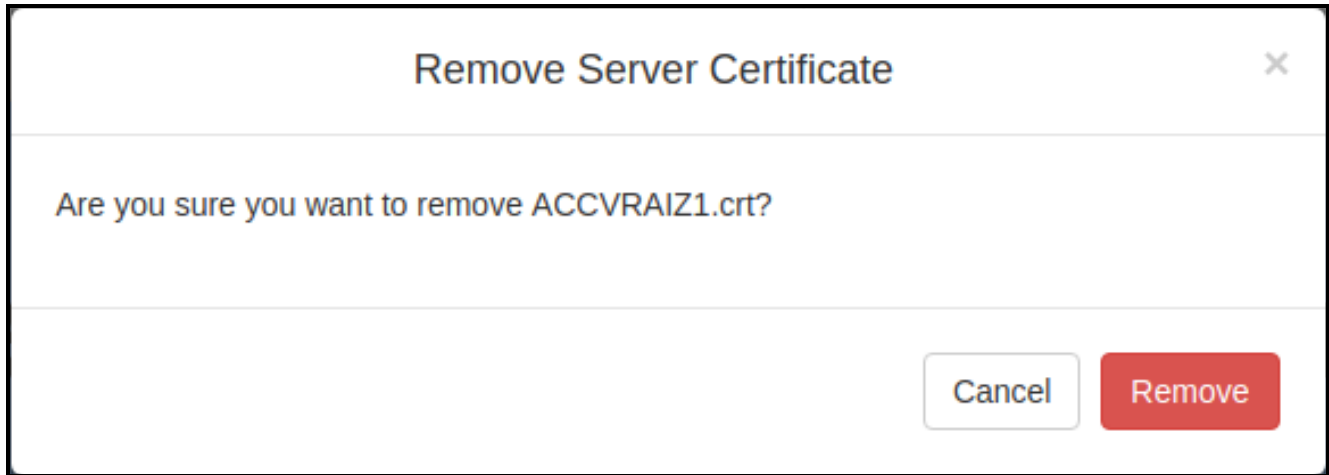
**Figure 2-28. Certificate Info Window**



### 2.4.10.2 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 2-29](#).

**Figure 2-29. Remove Server Certificate Window**



## 2.4.11 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 2-30](#).

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

**CyberData Keypad Intercom**

**Multicast Settings**

Enable Multicast Operation: ☐

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

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*

2. On the **Multicast** 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. 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 2.4.11.1, "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]).  <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.
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.
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.
	Click the <b>Save</b> button to save your configuration settings.
	Click on the <b>Reboot</b> button to reboot the system.



### 2.4.11.1 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.

## 2.4.12 Configure the Access Log Parameters

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

Figure 2-31. Access Log Page

Home Device Buttons Security Network SIP SSL Multicast Access Log Sensor Audiofiles Events DSR Autopro Firmware

# CyberData Keypad Intercom

## Access Log

Refresh Clear Download

Search

Event #	Timestamp	Action	User ID	User Name
23	Wed 2018-11-21 15:18:25 PM	DSR deactivated		
22	Wed 2018-11-21 15:18:18 PM	DSR activated		
21	Wed 2018-11-21 15:18:18 PM	User authenticated	14	Hannah
20	Wed 2018-11-21 15:18:18 PM	Valid code	14	Hannah
19	Wed 2018-11-21 14:58:13 PM	User blacklisted	13	Ethan
18	Wed 2018-11-21 14:51:56 PM	User blacklisted	13	Ethan
17	Wed 2018-11-21 14:50:58 PM	Relay deactivated		
16	Wed 2018-11-21 14:50:51 PM	Relay activated		
15	Wed 2018-11-21 14:50:51 PM	User authenticated	12	Isabella
14	Wed 2018-11-21 14:50:51 PM	Valid code	12	Isabella

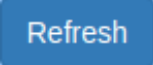
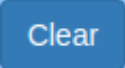







Showing 1 to 10 of 23 rows 10 rows per page

< 1 2 3 >

2. On the **Access Log** 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.

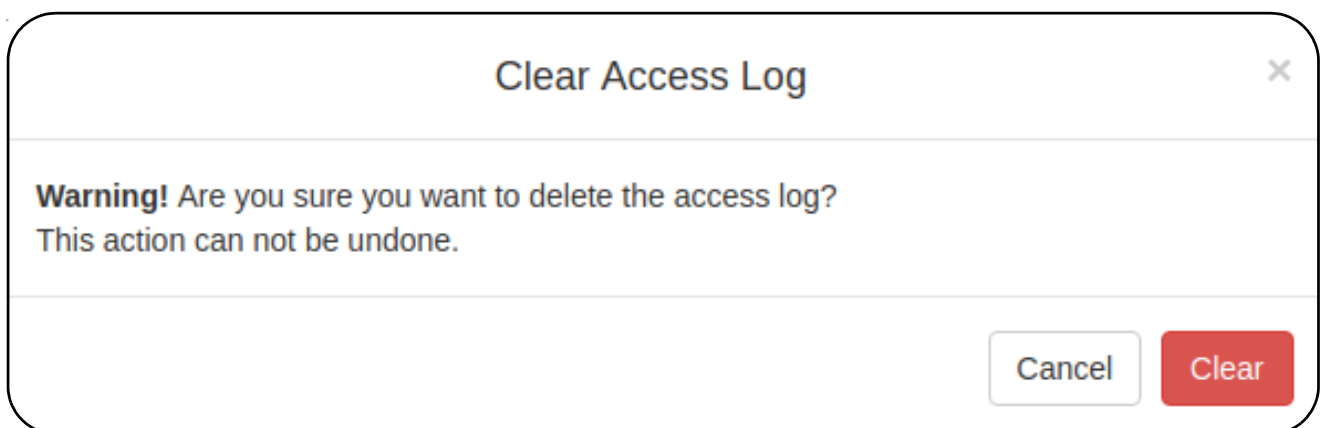
**Table 2-18. Access Log Configuration Parameters**

Web Page Item	Description
<b>Access Log</b>	
	Refresh the web page view new log entries.
	Erases the log. When pressed, the <b>Clear Access Log Confirmation Window</b> appears. See <a href="#">Section 2.4.12.1, "Clear Access Log Confirmation Window"</a> .
	Downloads the access log.
Search 	Search the access log.
Event # 	System generated number to identify the event.
Timestamp 	Displays the time of the event ( <b>Day of week Year-Month-Day Hour:Minute:Seconds AM/PM</b> ).
Action 	Describes the event.
User ID 	Displays the ID number of the user.
User Name 	Displays the name of the user.

#### 2.4.12.1 Clear Access Log Confirmation Window

The **Clear Access Log Confirmation Window** will ask if the user wants to delete the access log. This window appears after clicking on the **Clear** button. See [Figure 2-32](#).

**Figure 2-32. Clear Access Log Confirmation Window**



---

## 2.4.13 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 2-33).

Figure 2-33. Sensor Configuration Page

Home Device Buttons Security Network SIP SSL Multicast Access Log Sensor Audiofiles Events DSR Autopro Firmware

## CyberData Keypad Intercom

### Door Sensor Settings

Door Sensor Normally Closed: ☐ Yes ☒ No

Door Open Timeout (in seconds):

Flash Button LED: ☐

Activate Relay: ☐

Play Audio Locally: ☐

Make call to extension: ☐

Dial Out Extension:

Dial Out ID:

Play recorded audio: ☐

Repeat Sensor Message:

Save Reboot Toggle Help

Test Door Sensor Test Intrusion Sensor

### 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:

2. On the **Sensor** page, enter values for the parameters indicated in [Table 2-19](#).

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

**Table 2-19. Sensor Configuration Parameters**

Web Page Item	Description
<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>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.

Table 2-19. Sensor Configuration Parameters (continued)

Web Page Item	Description
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.
Test Door Sensor	Click the <b>Test Door Sensor</b> button to test the door sensor.
Test Intrusion Sensor	Click the <b>Test Intrusion Sensor</b> button to test the Intrusion sensor.
Save	Click the <b>Save</b> button to save your configuration settings.
Reboot	Click on the <b>Reboot</b> button to reboot the system.
Toggle Help	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.

## 2.4.14 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 2-34).

**Figure 2-34. Audiofiles Configuration Page**

Button	Current Setting	Action	Status	Controls
0:	Currently set to: default	Browse...	No file chosen	Play Delete Save
1:	Currently set to: default	Browse...	No file chosen	Play Delete Save
2:	Currently set to: default	Browse...	No file chosen	Play Delete Save
3:	Currently set to: default	Browse...	No file chosen	Play Delete Save
4:	Currently set to: default	Browse...	No file chosen	Play Delete Save
5:	Currently set to: default	Browse...	No file chosen	Play Delete Save
6:	Currently set to: default	Browse...	No file chosen	Play Delete Save
7:	Currently set to: default	Browse...	No file chosen	Play Delete Save
8:	Currently set to: default	Browse...	No file chosen	Play Delete Save
9:	Currently set to: default	Browse...	No file chosen	Play Delete Save



**Figure 2-35. Audiofiles Configuration Page (continued)**

<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>Audio Test:</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>Page Tone:</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>Your IP Address Is:</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>Restoring Default:</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 Tone:</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>Ring Tone:</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>Intrusion Sensor Triggered:</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>Door Ajar:</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>Night Ring:</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>SIP Multicast Message:</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>Blacklist Message:</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 2-20](#).

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

**Table 2-20. Audiofiles Configuration Parameters**

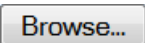

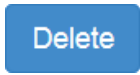

Web Page Item	Description
Available Space	Shows the space available for the user to save custom audio files if they want to change the message when the door or sensor is triggered.
0-9	The name of the audio configuration option is the same as the spoken audio that plays on the board (24 character limit).  '0' corresponds to the spoken word "zero." '1' corresponds to the spoken word "one." '2' corresponds to the spoken word "two." '3' corresponds to the spoken word "three." '4' corresponds to the spoken word "four." '5' corresponds to the spoken word "five." '6' corresponds to the spoken word "six." '7' corresponds to the spoken word "seven." '8' corresponds to the spoken word "eight." '9' corresponds to the spoken word "nine."
Dot	Corresponds to the spoken word "dot." (24 character limit)
Audio Test	Corresponds to the message <b><i>"This is the CyberData IP speaker test message..."</i></b> (24 character limit)
Page Tone	Corresponds to a simple tone used for beep on initialization and beep on page (24 character limit).
Your IP Address Is	Corresponds to the message "Your IP address is..." (24 character limit).
Rebooting	Corresponds to the spoken word "Rebooting" (24 character limit).
Restoring Default	Corresponds to the message "Restoring default" (24 character limit).
Ringback Tone	This is the ringback tone that plays when calling a remote extension (24 character limit).
Ring Tone	This is the tone that plays when set to ring when receiving a call (24 character limit).
Intrusion Sensor Triggered	Corresponds to the message "Intrusion Sensor Triggered" (24 character limit).
Door Ajar	Corresponds to the message "Door Ajar" (24 character limit).
Night Ring	Specifies the ringtone for nightring. By default this parameter uses the same audio file that is selected for the <b>Ring Tone</b> parameter.
SIP Multicast Message	This is the message that plays when multicast audio is initiated by the call button.
Blacklist Message	The audio file that will play if a blacklisted security code is entered.
	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 2-20. 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.

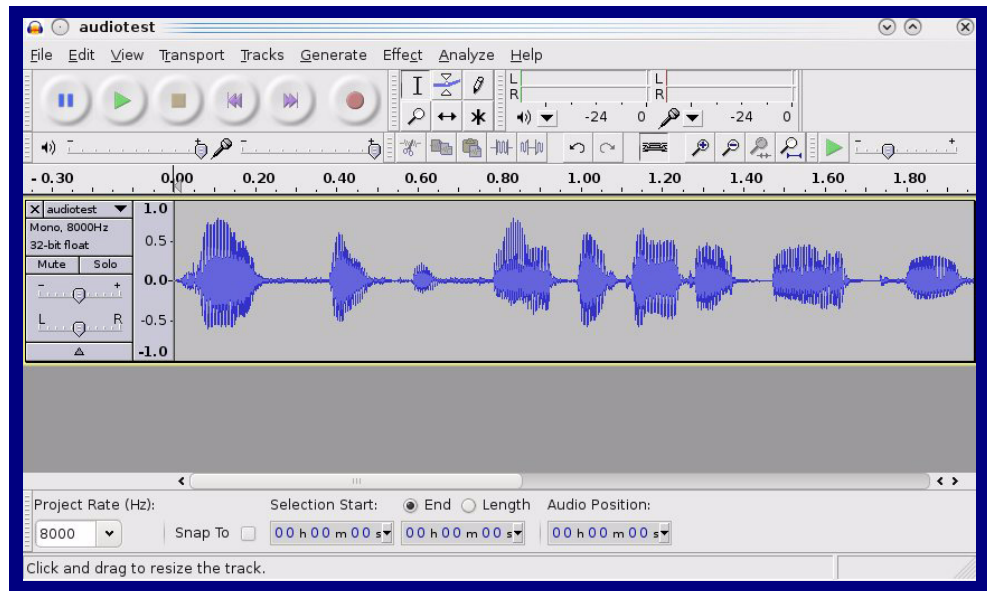
### 2.4.14.1 User-created Audio Files

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

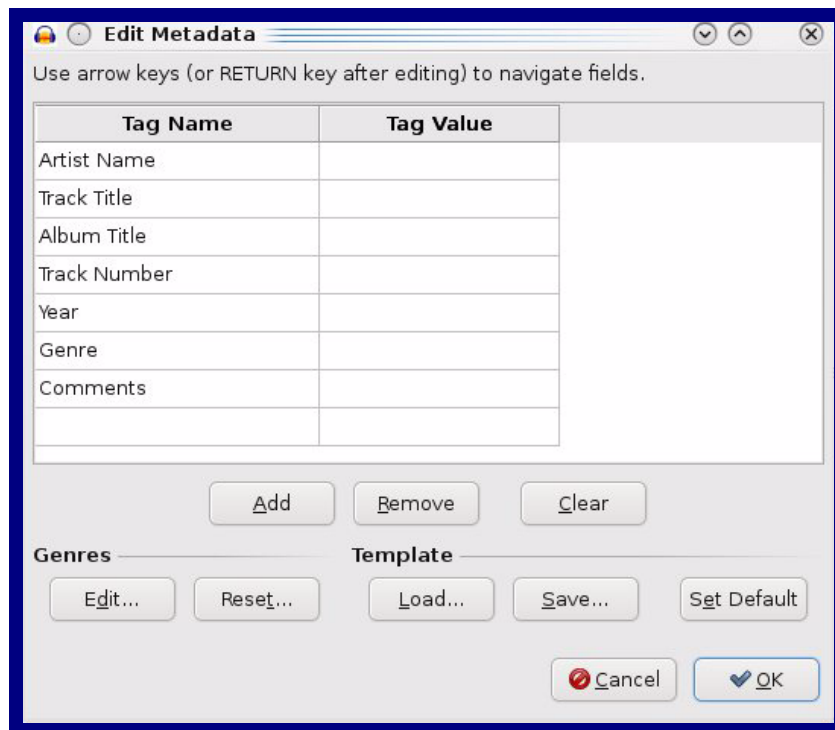
RIFF (little-endian) data, WAVE audio, Microsoft PCM, 16 bit, mono 8000 Hz

You can use the free utility *Audacity* to convert audio files into this format. See [Figure 2-36](#) through [Figure 2-38](#).

**Figure 2-36. Audacity 1**



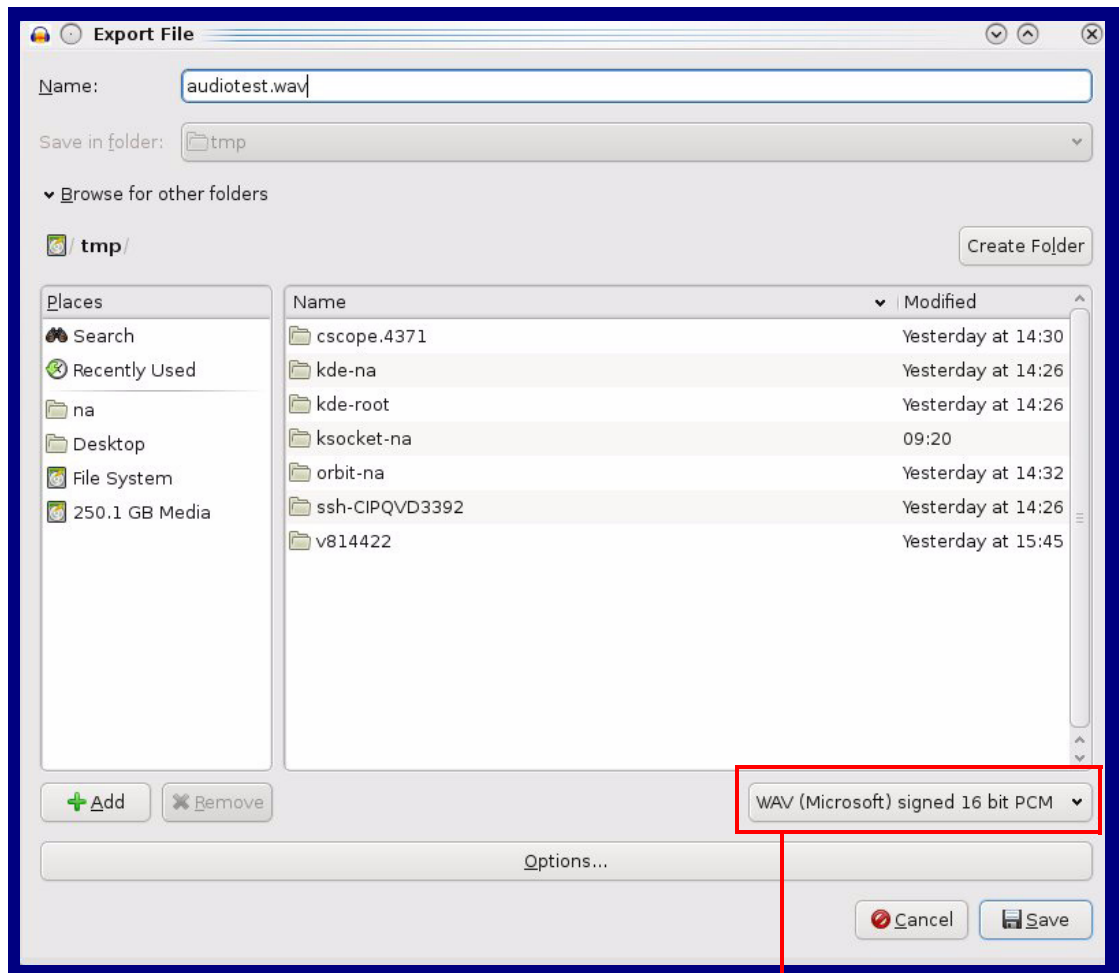
**Figure 2-37. Audacity 2**



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

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

**Figure 2-38. WAV (Microsoft) signed 16 bit PCM**



WAV (Microsoft) signed 16 bit PCM

## 2.4.15 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 2-39](#)).

**Figure 2-39. Event Configuration Page**

Home Device Buttons Security Network SIP SSL Multicast Access Log Sensor Audiofiles Events DSR Autopro Firmware

# CyberData Keypad Intercom

Enable Event Generation: ☐

## Events

Enable Button Events:	<input type="checkbox"/>
Enable Call Start Events:	<input type="checkbox"/>
Enable Call Terminated Events:	<input type="checkbox"/>
Enable Relay Activated Events:	<input type="checkbox"/>
Enable Relay Deactivated Events:	<input type="checkbox"/>
Enable Ring Events:	<input type="checkbox"/>
Enable Night Ring Events:	<input type="checkbox"/>
Enable Multicast Start Events:	<input type="checkbox"/>
Enable Multicast Stop Events:	<input type="checkbox"/>
Enable Power On Events:	<input type="checkbox"/>
Enable Sensor Events:	<input type="checkbox"/>
Enable Remote Relay Events:	<input type="checkbox"/>
Enable Security Events:	<input type="checkbox"/>
Enable 60 Second Heartbeat:	<input type="checkbox"/>

## 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 2-21](#).

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

**Table 2-21. Events Configuration Parameters**

Web Page Item	Description
Enable Event Generation ?	The device will send HTTP POST events to the specified remote server and port number whenever a certain action takes place. Select an event type below to generate an HTTP POST event.
<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 ?	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.

Table 2-21. Events Configuration Parameters(continued)

Web Page Item	Description
<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.
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.



### 2.4.15.1 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>
```

## 2.4.16 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.

The DSR must be running firmware version 4.8 or later to work with this CyberData device. 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 2-40).

1. Click on the **DSR** menu button to open the **DSR** page (Figure 2-40).

**Figure 2-40. DSR Page (not associated with any DSRs)**

Home Device Buttons Security Network SIP SSL Multicast Access Log Sensor Audiofiles Events DSR Autoprovisioning Firmware

# CyberData Keypad 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 2-22](#).

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

**Table 2-22. DSR Configuration Parameters (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.
	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.

## 2.4.17 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 2-41](#).

**Figure 2-41. Autoprovisioning Page**

Home Device Buttons Security Network SIP SSL Multicast Access Log Sensor Audiofiles Events DSR Autoprov Firmware

# CyberData Keypad 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 '0020f703fd5b.xml' and if this fails, '000000cd.xml'.

Save Reboot Toggle Help

Download Template





### Autoprovisioning log

```
2018-11-20 13:27:14 Autoprovdi: no autoprov triggers. Exiting...
2018-11-20 13:27:15 Autoprovisioning on boot
2018-11-20 13:27:15 Autoprov found server='https://10.0.0.242:4444' in dhcp option 43
2018-11-20 13:27:15 Autoprov looking for https://10.0.0.242:4444/0020f703fd5b.xml
2018-11-20 13:27:15 Autoprov not verifying server certificate
2018-11-20 13:27:16 Autoprov: download failed
2018-11-20 13:27:16 Autoprov looking for 000000cd.xml at https://10.0.0.242:4444
2018-11-20 13:27:16 Autoprov looking for https://10.0.0.242:4444/000000cd.xml
2018-11-20 13:27:16 Autoprov not verifying server certificate
2018-11-20 13:27:16 Autoprov: download failed
```

2. On the **Autoprovisioning** page, you may enter values for the parameters indicated in [Table 2-23](#).

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

**Table 2-23. Autoprovisioning Configuration Parameters**

Web Page Item	Description
Disable Autoprovisioning ?	Prevent the device from automatically trying to download a configuration file. See <a href="#">Section 2.4.17.1, "Autoprovisioning"</a> for more information.
Autoprovisioning Server ?	Enter the IPv4 address of the provisioning server in dotted decimal notation.
Autoprovisioning Filename ?	<p>The autoprovisioning filename is the configuration filename. The default autoprovisioning filename is in the format of <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 2.4.17.3, "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).

### 2.4.17.1 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 2.4.17.2, "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 2-23](#)). This file contains every configuration option that can be set on the board.

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

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

```
<MiscSettings>
    <DeviceName>CyberData VoIP Intercom</DeviceName>
<!--    <AutoprovFile>common.xml</AutoprovFile>-->
<!--    <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](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 2-24. Autoprovisioning File Name**

Autoprovisioning Filename	Autoprovisioning Server	File Downloaded
config.xml	10.0.1.3	10.0.1.3/config.xml
/path/to/config.xml	10.0.1.3	10.0.1.3/path/to/config.xml
subdirectory/path/	10.0.1.3	10.0.1.3/subdirectory/path/0020f7020002.xml

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

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

For example:

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

The autoprovisioning filename is set to “cyberdata/”

On boot, the device will try to download:

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

...and if this fails:

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

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

```

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

```

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

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

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

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

The list of valid product strings:

```

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

```

Autoprovisioning  
Example 1

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

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

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

**000000cd.xml**

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

**sip\_common.xml**

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

**sip\_0020f7020001.xml**

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

**sip\_0020f7020002.xml**

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

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

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

Device2 goes through the same steps by setting its device name to **CyberData Autoprovisioned**, its SIP server to **10.0.0.253**, and its port to **5060**. When Device2 “sees” **sip\_[macaddress].xml**, Device2 replaces it with its own mac address and downloads **sip\_0020f7020002.xml** from “https://autoprotest.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 Configuration** page or by changing the autoprovisioning file with “**default**” set as the file name.

## 2.4.17.2 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; }
```

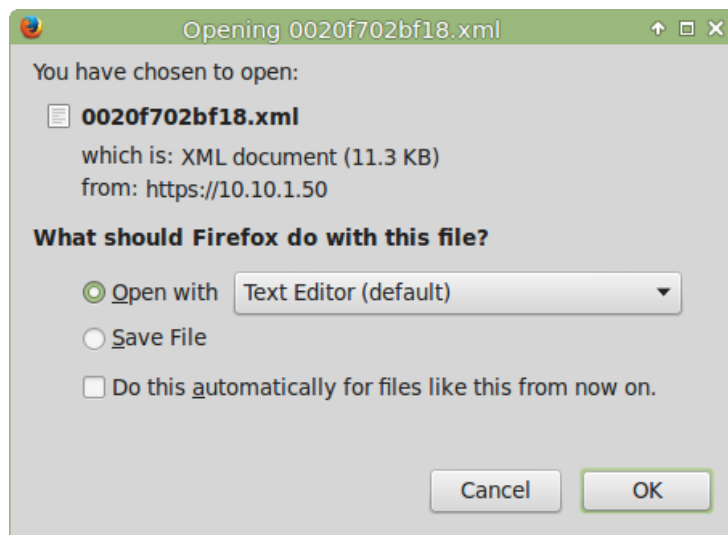
### 2.4.17.3 Download Template Button

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 2-42](#)). 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 2-42](#).

**Figure 2-42. 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

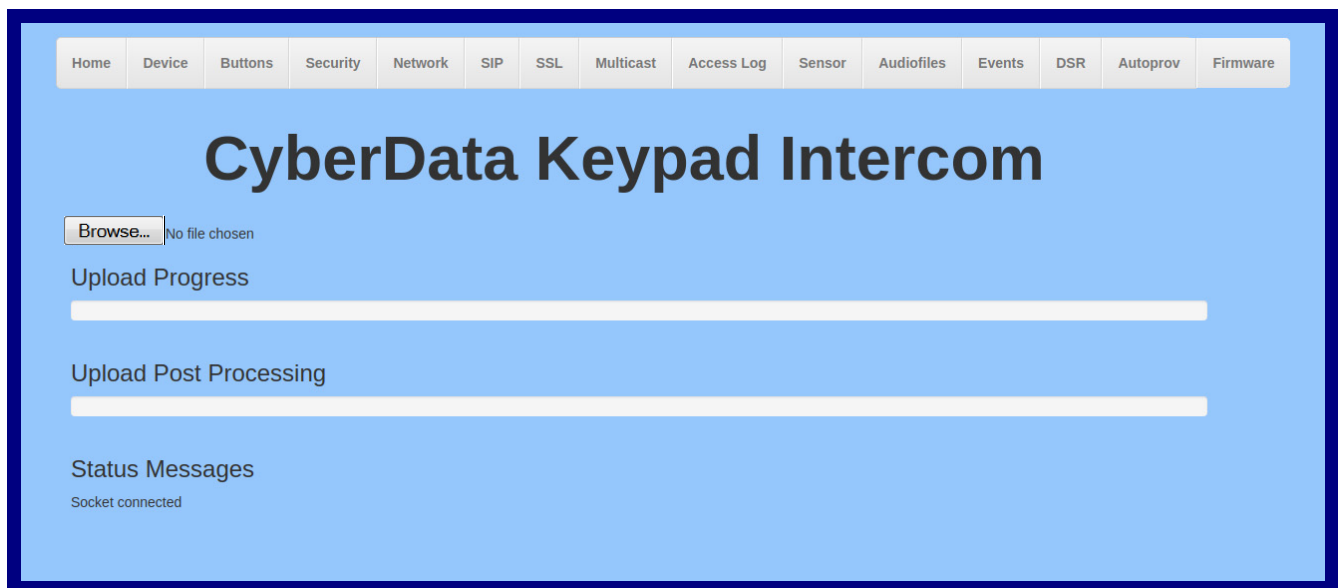
**Note** CyberData strongly recommends that you do not upgrade the firmware when the device is likely to be in use.

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/011214>
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 2-43](#)).

 <small>GENERAL ALERT</small>	<p><b>Caution</b></p> <p><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>.</p>
--	--

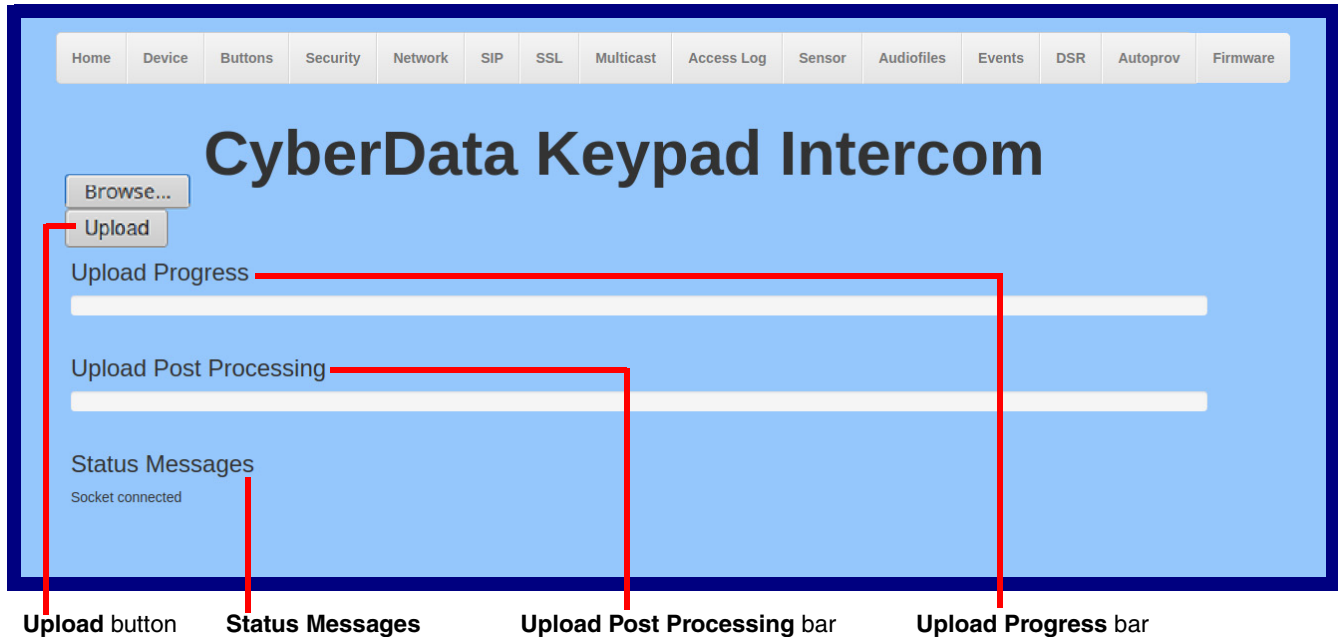
**Figure 2-43. Firmware Page**



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 2-44).

Figure 2-44. Upload Button



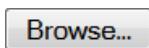
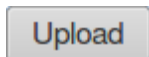
7. Click on the **Upload** button. After selecting the **Upload** button, you will see the progress of the upload in the **Upload Progress** bar.
8. When the upload is complete, you will see the words **Upload finished** under **Status Messages**.
9. At this point, you will see the progress of the upload's 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 2-25 shows the web page items on the **Firmware** page.

**Table 2-25. Firmware Page Parameters**

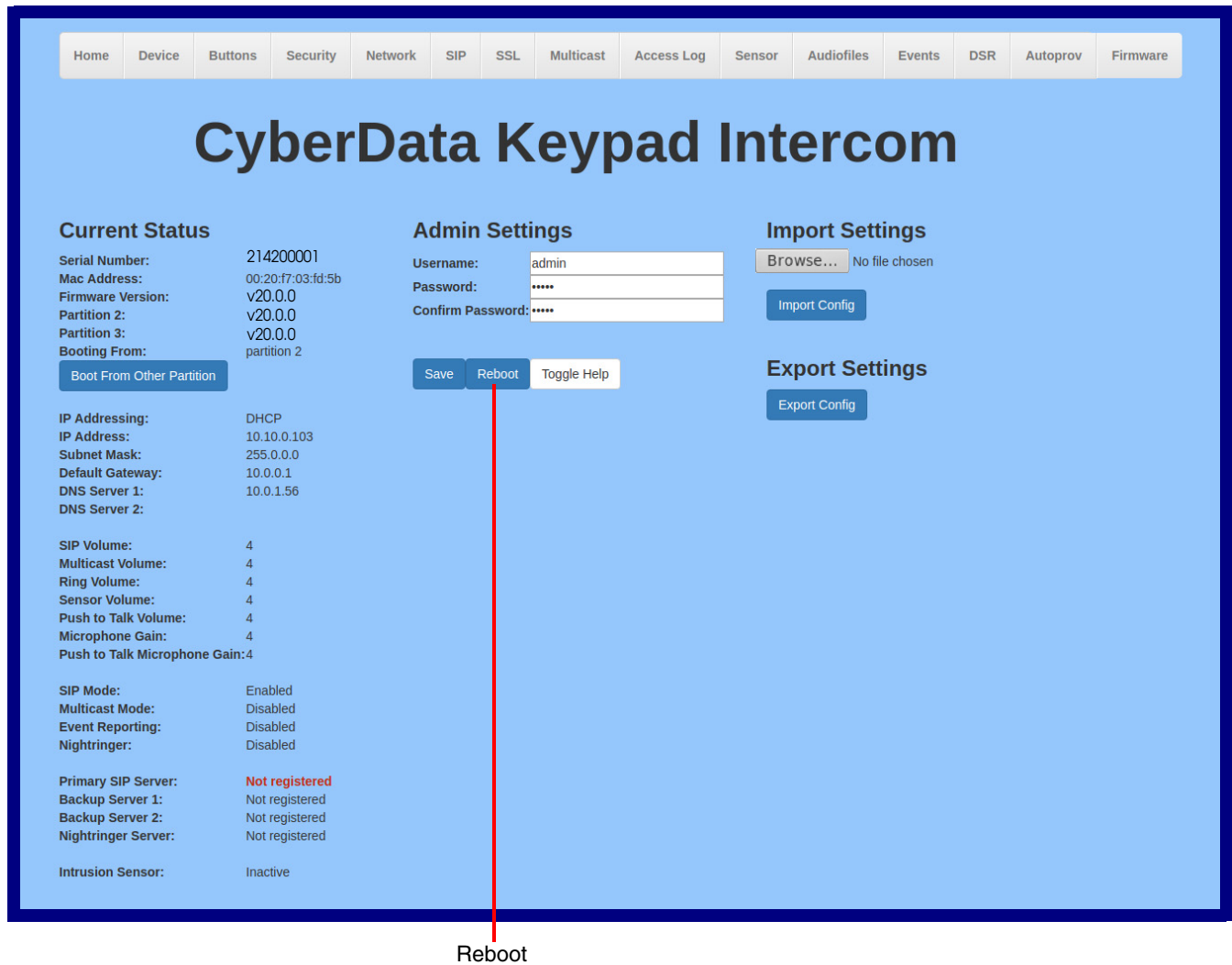
Web Page Item	Description
	Use the <b>Browse</b> button to navigate to the location of the firmware file that you want to upload.
	Click on the <b>Upload</b> button to automatically upload the selected firmware and reboot the system. <b>Note:</b> This button only appears after the user has selected a 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.

## 2.5.1 Reboot the Device

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

1. Click on the **Reboot** button on the **Home** page ([Figure 2-45](#)). A normal restart will occur.

**Figure 2-45. Home Page**



## 2.6 Command Interface

Some functions on the device can be activated using simple POST commands to the web interface. The examples in [Table 2-26](#) use the free unix utility, **wget** **commands**. However, any program that can send HTTP POST commands to the device should work.

### 2.6.1 Command Interface Post Commands

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

**Table 2-26. 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 2-26. Command Interface Post Commands (continued)**

<b>Device Action</b>	<b>HTTP Post Command<sup>a</sup></b>
Play the "5" 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 "5=Play"
Play the "6" 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 "6=Play"
Play the "7" 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 "7=Play"
Play the "8" 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 "8=Play"
Play the "9" 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 "9=Play"
Play the "Dot" 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 "d=Play"
Play the Audio Test	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"
Play the "Page Tone" 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 "pagetone=Play"
Play the "Your IP Address Is" 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 "youripaddressis=Play"
Play the "Rebooting" 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 "rebooting=Play"
Play the "Restoring Default" 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 "restoringdefault=Play"
Play the "Ringback tone" 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 "ringback=Play"
Play the "Ring tone" 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 "ringtone=Play"
Play the "Intrusion Sensor Triggered" 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 "intrusionsensortriggered=Play"
Play the "Door Ajar" 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 "doorajar=Play"
Play the "Night Ring" 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 "nightring=Play"

**Table 2-26. 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 - O /dev/null --no-check-certificate "https://10.10.1.154/command" -- post-data "request=swap_boot_partition"

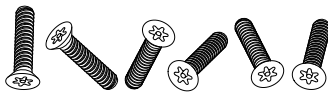

a. Type and enter all of each http POST command on one line.

# Appendix A: Mounting the SIP Outdoor Intercom with Keypad

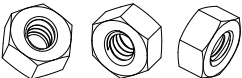


## A.1 Mount the Intercom

Before you mount the Intercom, make sure that you have received all the parts for each Intercom. Refer to [Table A-1](#). See [Table A-2](#) and [Table A-3](#) for optional accessories.


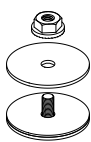
**Table A-1. Mounting Components (Part of the Accessory Kit)**

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

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

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

**Table A-3. Optional Accessories**

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



## A.2 Dimensions

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

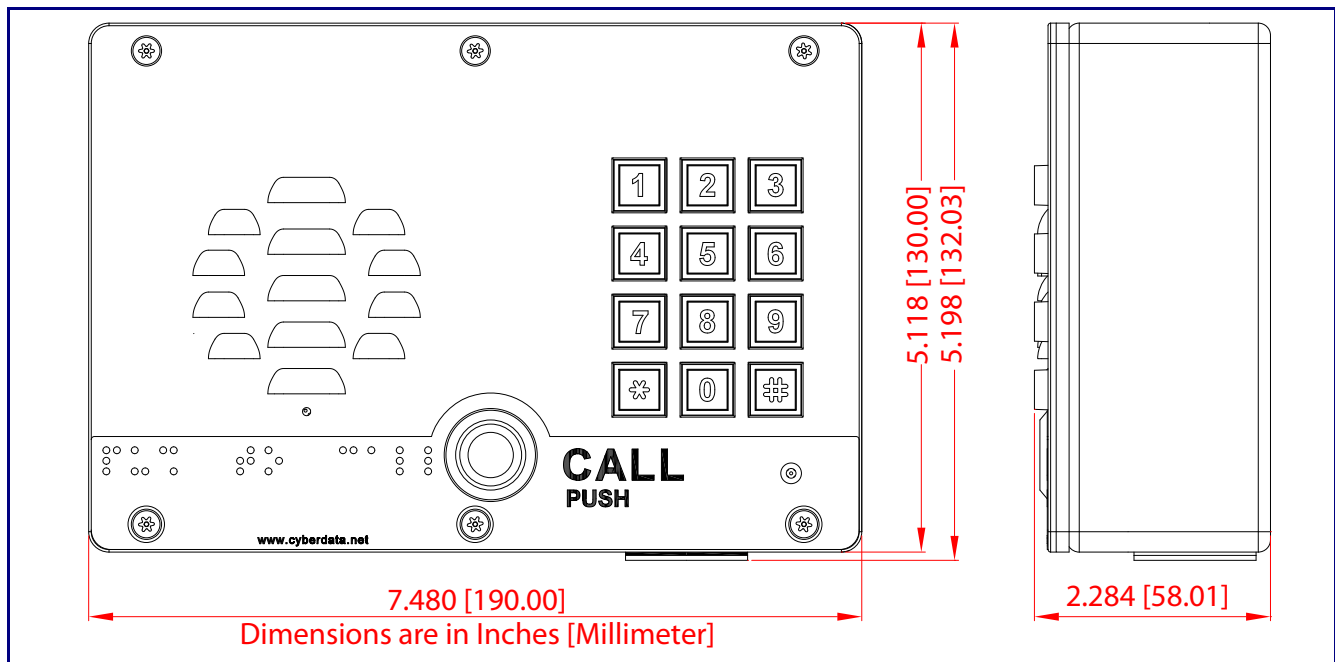


Figure A-1. Unit Dimensions—Rear View with Mounting Hole Locations

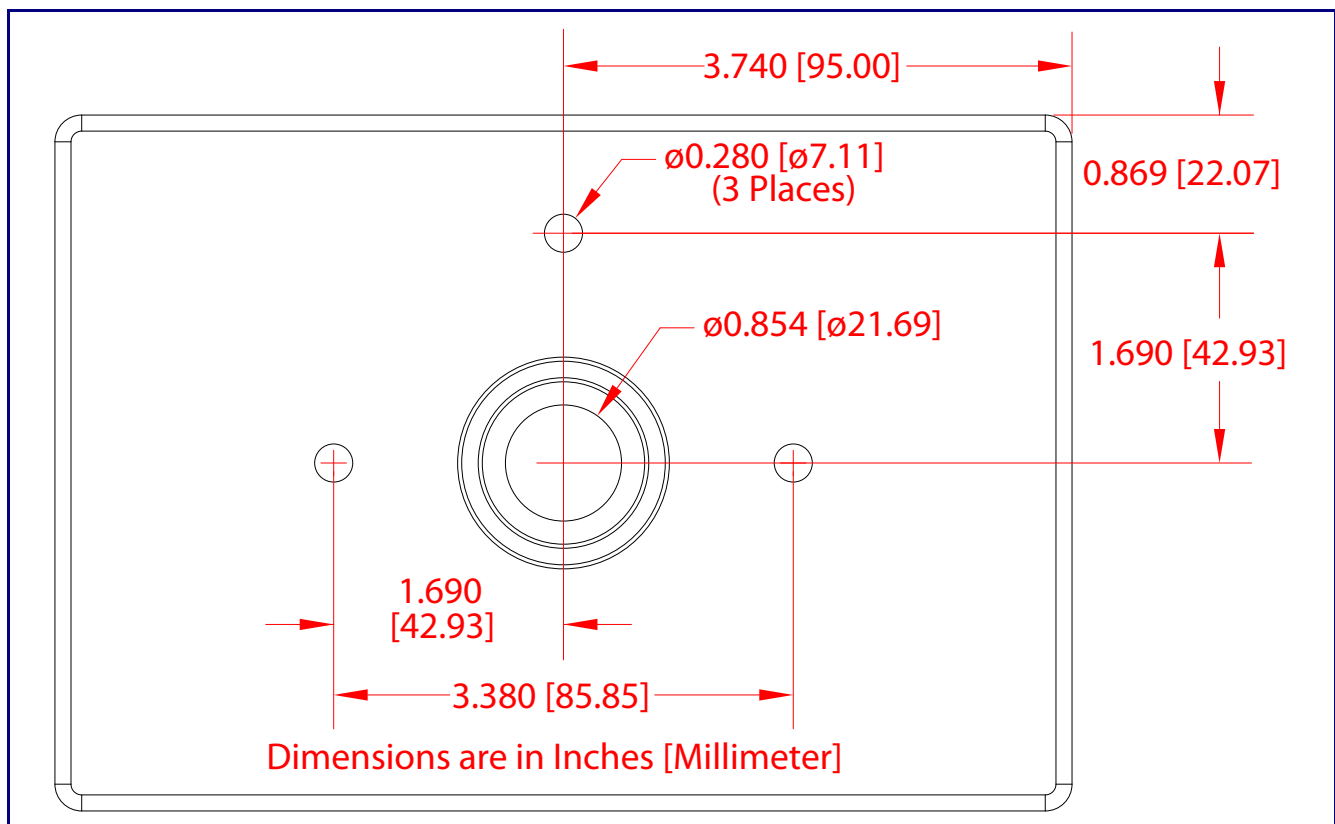


Figure A-2. Shroud Dimensions and Mounting Hole Locations

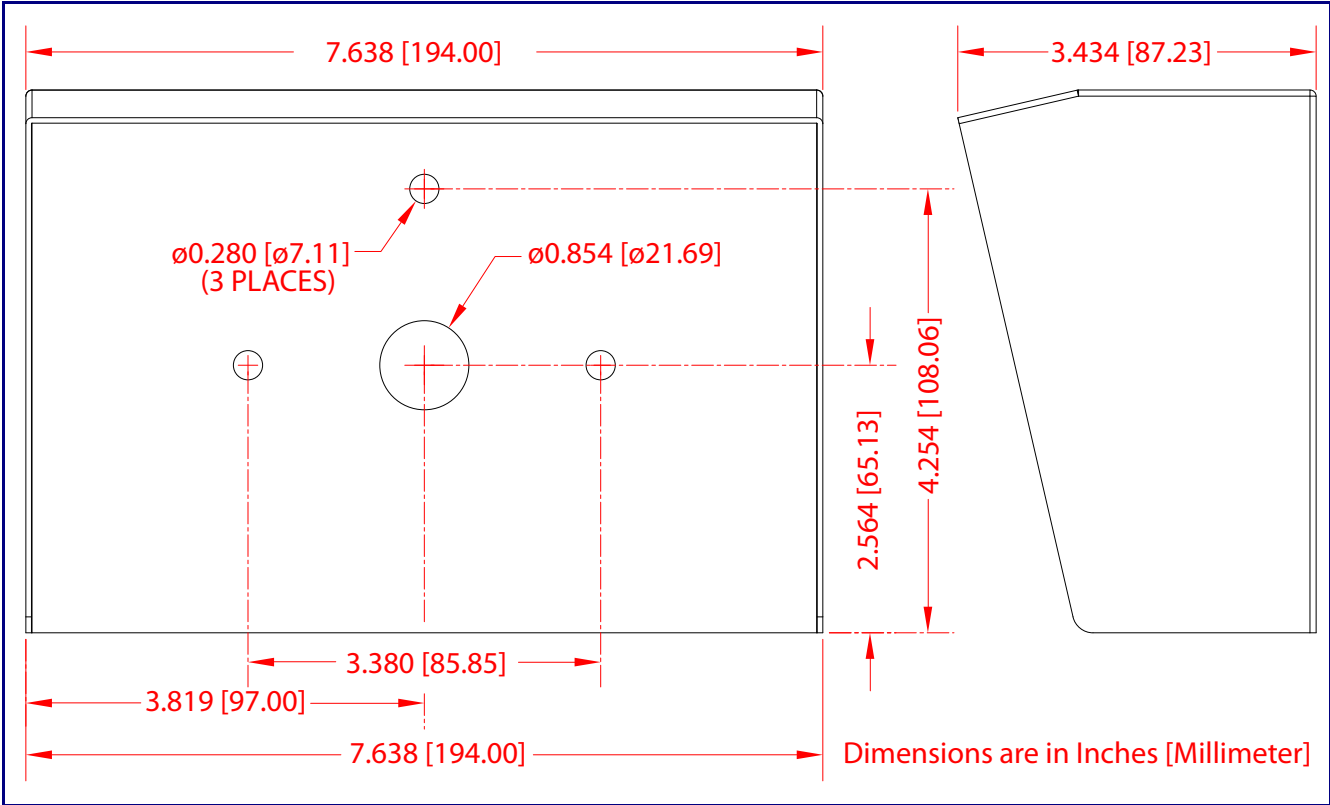
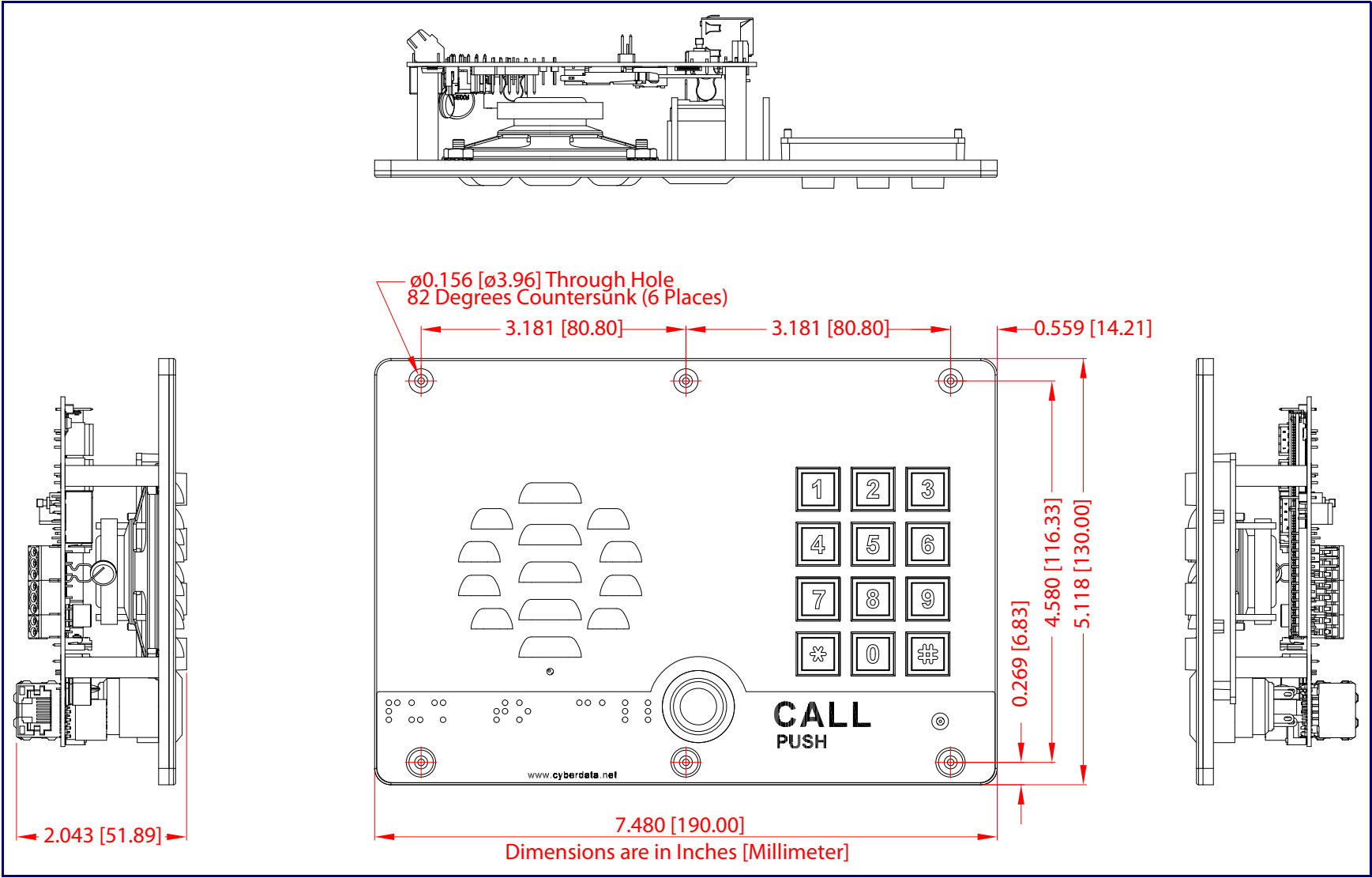


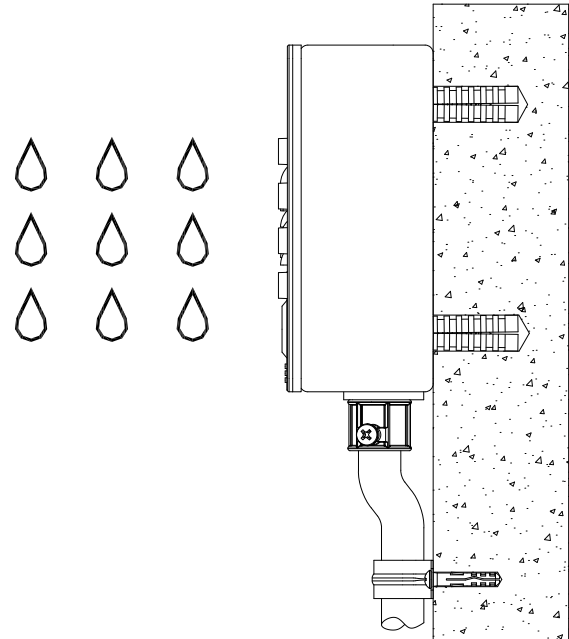
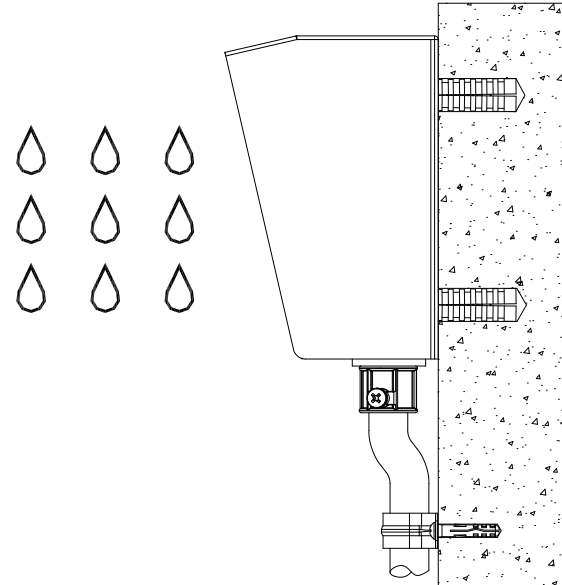
Figure A-3. Unit Dimensions—Faceplate and Board Assembled



# A.3 Overview of Installation Types

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

Table A-4. Overview of Installation Types

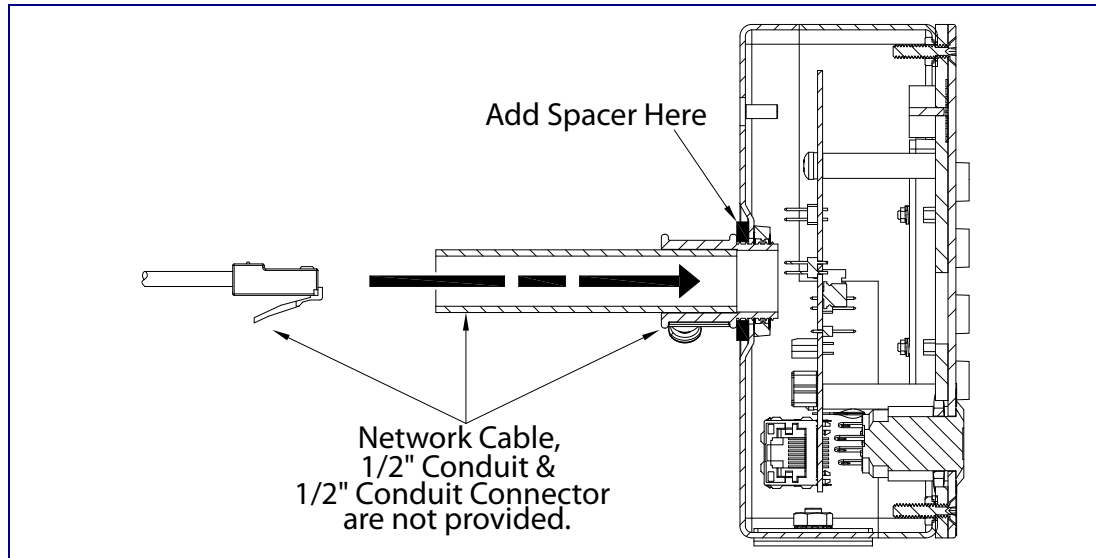
Installation Type	What You Need
Outdoor, on surface	011214 Intercom only
	
Outdoor, on surface with shroud (increased resistance)	011214 Intercom 011215 Weather Shroud (sold separately)
	

## A.4 Network Cable Entry Restrictions

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

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

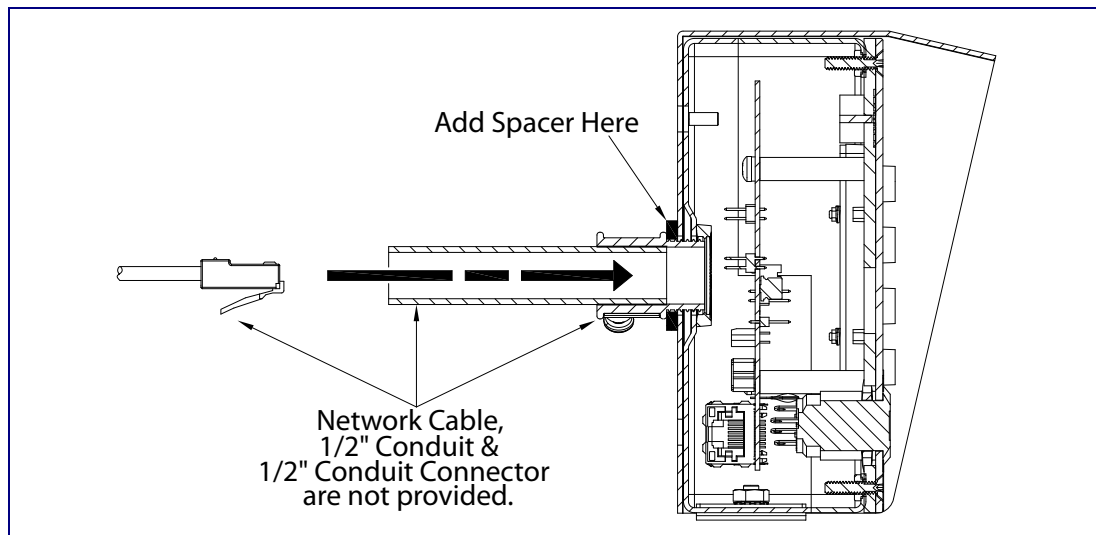
**Figure A-4. Rear Conduit Network Cable Entry Restrictions—Without Shroud**



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

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

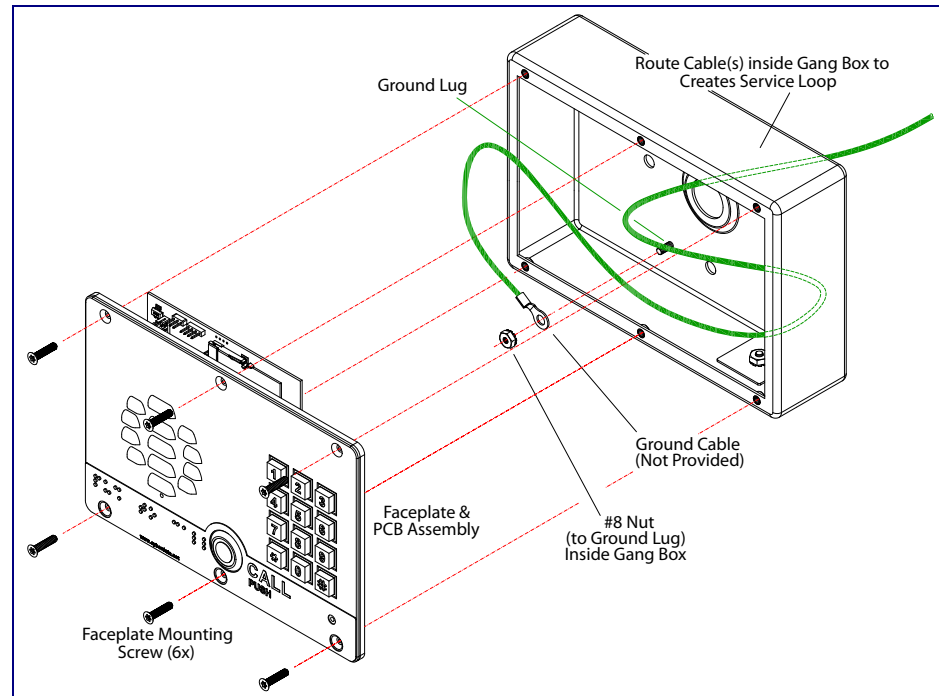
**Figure A-5. Rear Conduit Network Cable Entry Restrictions—With Shroud**



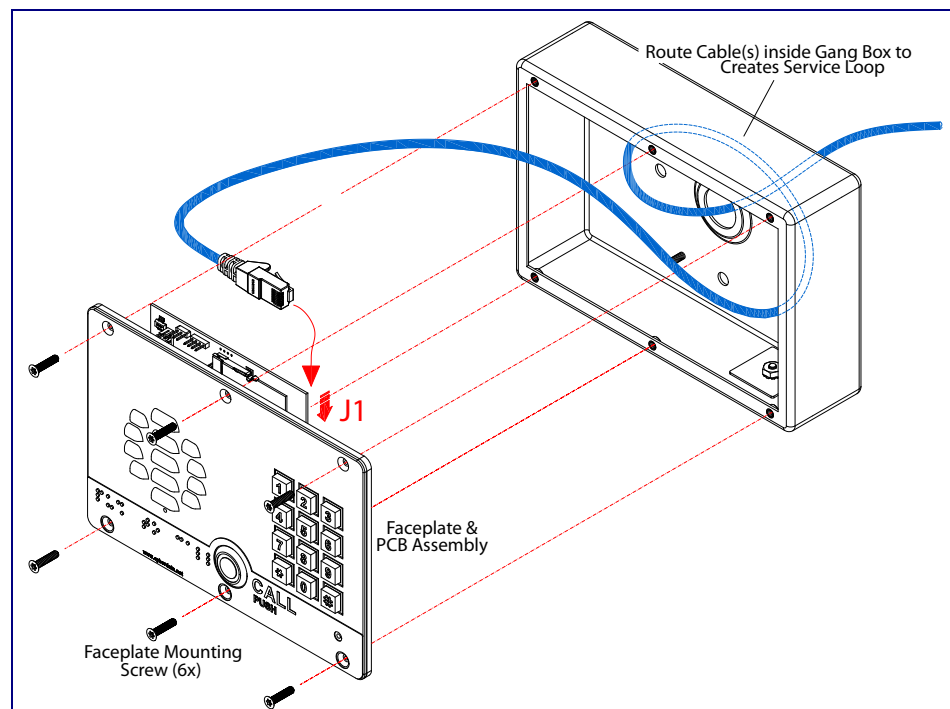
## A.5 Service Loop Cable Routing

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

**Figure A-6. Ground Cable Service Loop Routing**



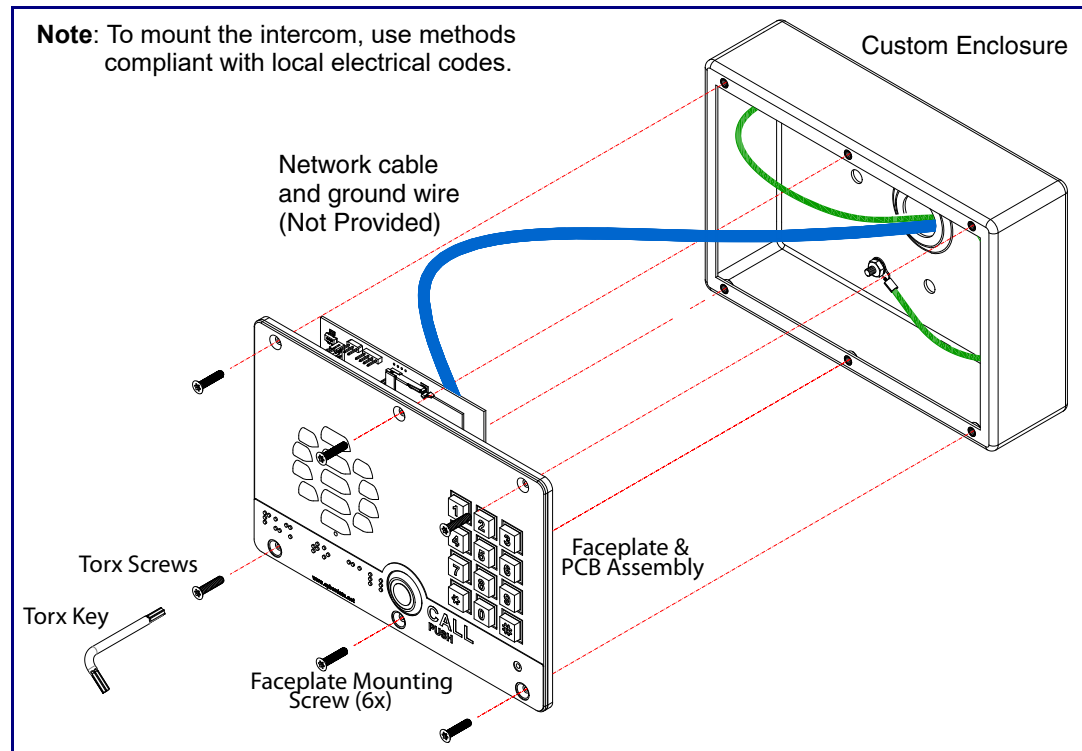
**Figure A-7. Network Cable Service Loop Routing**



## A.6 Securing the Intercom

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

**Figure A-8. Securing the Intercom**



GENERAL ALERT

### Caution

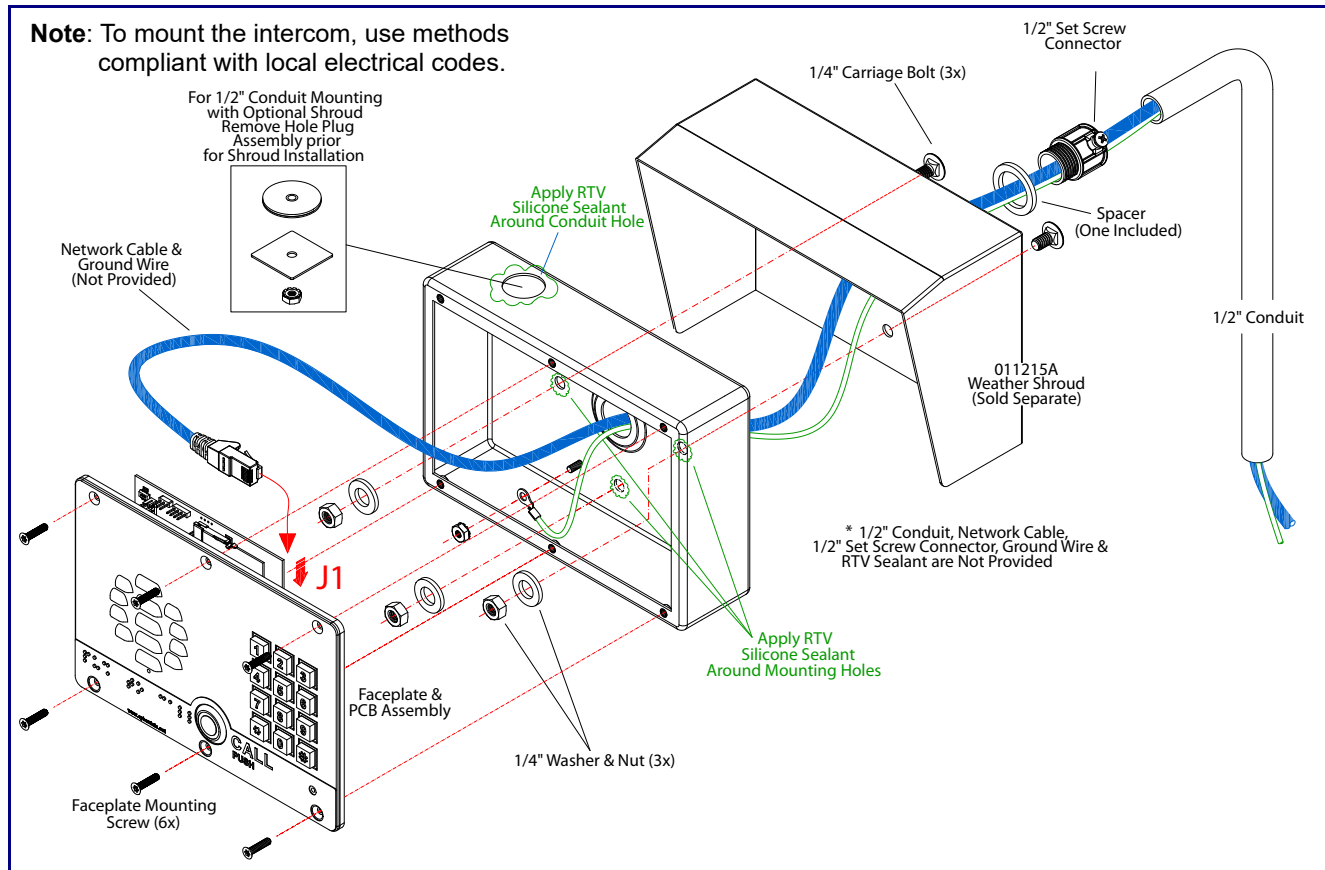
*Equipment Hazard:* Do not use an electric or power screwdriver to fasten the face plate and PCB assembly to the gang box. To prevent over-torque damage to the gasket, do not apply more than 10 inch-pounds force. Over-torquing will cause the gasket to tear, risk moisture intrusion, and effectively void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

## A.7 Additional Mounting Options

### A.7.1 Rear Conduit Mounting Option (Not Provided)

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

**Figure A-9. Optional Rear Conduit Mounting**

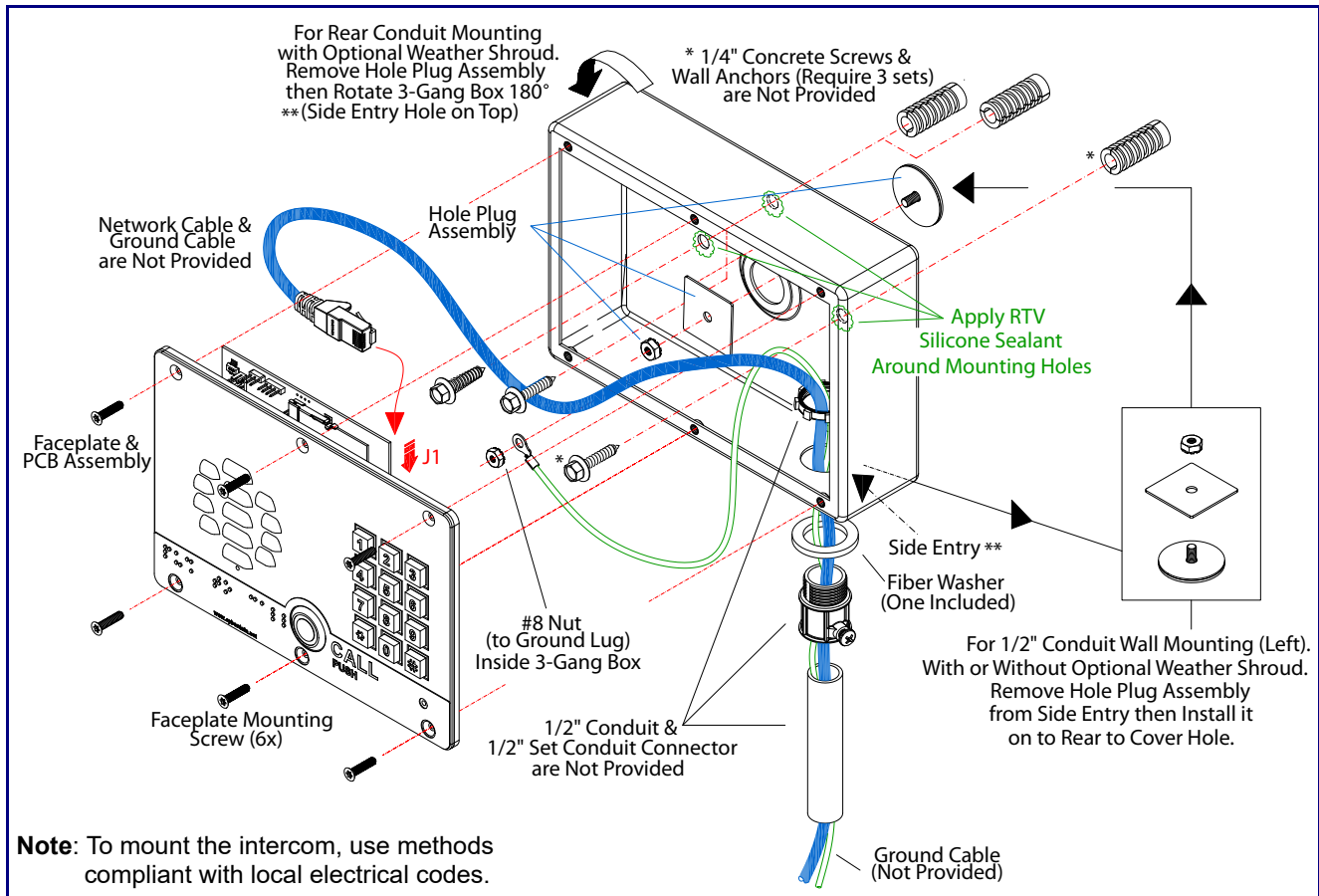




## A.7.2 Concrete Wall Mounting Option (Not Provided)

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

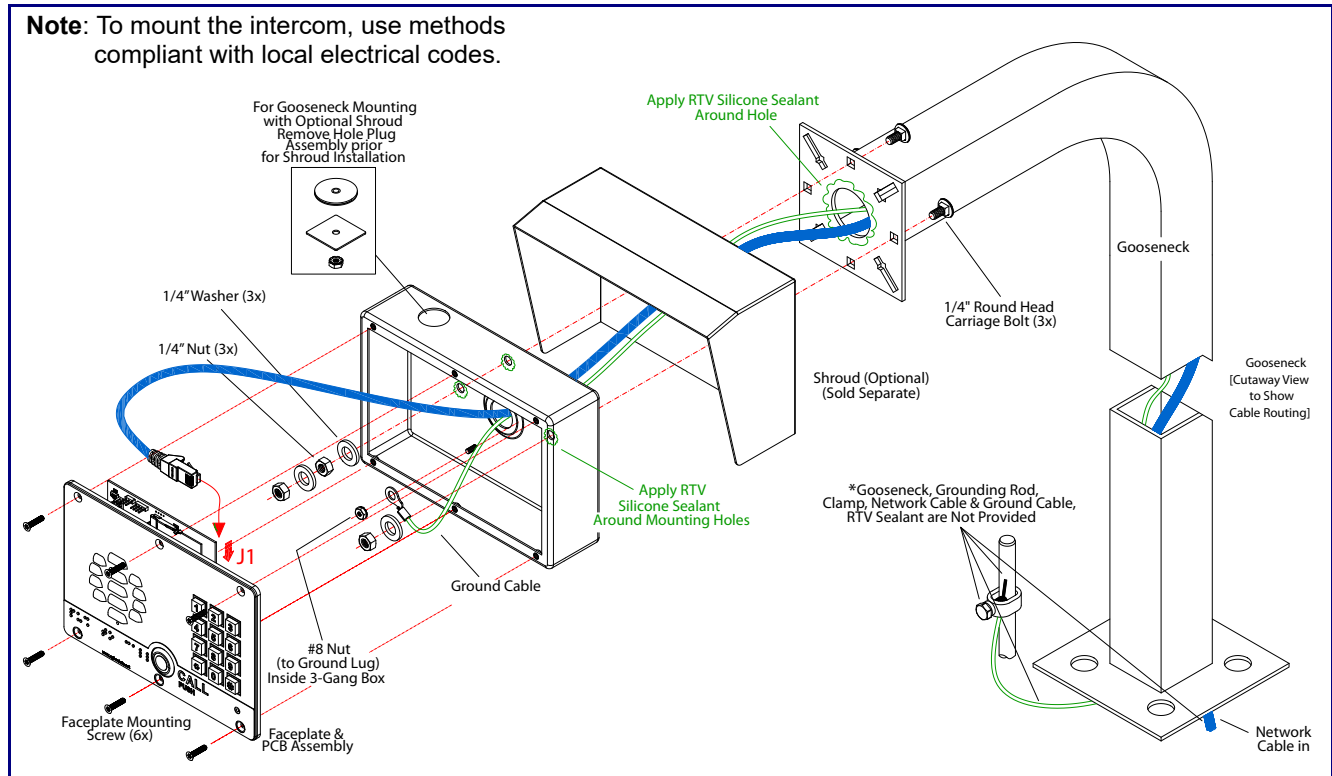
**Figure A-10. Optional Concrete Wall Mounting**



## A.7.3 Goose Neck Mounting Option (Not Provided)

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

**Figure A-11. Optional Goose Neck Mounting**



# Appendix B: Setting up a TFTP Server

---

## B.1 Set up a TFTP Server

Autoprovisioning requires a TFTP server for hosting the configuration file.

---

### B.1.1 In a LINUX Environment

To set up a TFTP server on LINUX:

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

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

---

### B.1.2 In a Windows Environment

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

<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/011214>

---

## C.2 Documentation

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

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

<https://www.cyberdata.net/products/011214>

---

## C.3 Contact Information

Contact	<p>CyberData Corporation 3 Justin Court Monterey, CA 93940 USA <a href="http://www.CyberData.net">www.CyberData.net</a> Phone: 800-CYBERDATA (800-292-3732) Fax: 831-373-4193</p>
Sales	<p>Sales 831-373-2601, Extension 334</p>
Technical Support	<p>The fastest way to get technical support for your VoIP product is to submit a VoIP Technical Support form at the following website:</p> <p><a href="http://support.cyberdata.net/">http://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:

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

# Index

---

## Numerics

16 AWG gauge wire 10

## A

activate relay (door sensor) 67  
 activate relay (intrusion sensor) 67  
 activity LED 21  
 address, configuration login 29  
 alternative power input 5  
 announcing a device's IP address 23  
 audio configuration 69  
     night ring tone parameter 71  
 audio configuration page 69  
 audio encodings 4  
 audio files, user-created 73  
 autoprovision at time (HHMMSS) 84  
 autoprovision when idle (in minutes > 10) 84  
 autoprovisioning 84, 85  
     download template button 84  
 autoprovisioning autoupdate (in minutes) 84  
 autoprovisioning configuration 83, 84  
 autoprovisioning filename 84  
 autoprovisioning server (IP Address) 84

## B

backup SIP server 1 51  
 backup SIP server 2 51  
 backup SIP servers, SIP server  
     backups 51

## C

call button  
     indicator light 9  
 call termination 36  
 changing  
     the web access password 33  
 Cisco SRST 52  
 command interface 98  
 commands 98  
 concrete wall mounting option (not provided) 110  
 conduit mounting option (not provided) 109  
 configurable parameters 34, 48, 51

configuration  
     audio 69  
     default IP settings 25  
     door sensor 55, 63, 65  
     intrusion sensor 55, 63, 65  
     network 47  
     SIP 50  
     using Web interface 25  
 configuration home page 29  
 configuration page  
     configurable parameters 34, 48  
 contact information 114  
 contact information for CyberData 114  
 current network settings 48  
 CyberData contact information 114

## D

default  
     gateway 25  
     intercom settings 115  
     IP address 25  
     subnet mask 25  
     username and password 25  
     web login username and password 29  
 default gateway 25, 48  
 default intercom settings 24  
 default IP settings 25  
 default login address 29  
 device configuration 33  
     device configuration parameters 84  
     the device configuration page 83  
 device configuration page 33, 37, 38  
 device configuration parameters 34  
 device configuration password  
     changing for web configuration access 33  
 DHCP Client 4  
 dial mode 38  
 dial out call 40  
 dial out extension (door sensor) 67  
 dial out extension (intrusion sensor) 67  
 dial out extension strings 39, 54  
 dimensions 5, 102  
     shroud dimensions and mounting hole locations 103  
     unit dimensions and intrusion sensor range without  
         the gang box 104  
     unit dimensions—front and side view 102  
     unit dimensions—rear view and mounting hole  
         locations 102  
 discovery utility program 29

DNS server 48  
 door sensor 65, 67  
     activate relay 67  
     dial out extension 67  
     door open timeout 67  
     door sensor normally closed 42, 67  
     flash button LED 67  
     play audio locally 67  
 download autoprovisioning template button 84  
 DTFM  
     play tone during DTMF activation 35  
 DTMF push to talk 36  
 DTMF tones 39  
 DTMF tones (using rfc2833) 39, 54

## E

electric screwdriver 108  
 enable night ring events 76  
 enable security operation 38  
 ethernet I/F 5  
 event configuration  
     enable night ring events 76  
 expiration time for SIP server lease 51, 52, 53  
 export settings 32

## F

factory default settings 24  
 fastening, gang box 108  
 firmware  
     where to get the latest firmware 94  
 flash button LED (door sensor) 67  
 flash button LED (intrusion sensor) 67

## G

gang box, fastening 108  
 gasket, avoid over-torque damage 108  
 get autoprovisioning template 84  
 goose neck mounting option (not provided) 111

## H

home page 29  
 http POST command 98  
 http web-based configuration 4

## I

identifying your product 1  
 import settings 32  
 import/export settings 32  
 indicator light 9  
 installation, typical intercom system 2  
 intercom configuration  
     default IP settings 25  
 intercom configuration page  
     configurable parameters 51  
 intrusion sensor 65, 67  
     activate relay 67  
     dial out extension 67  
     flash button LED 67  
     play audio locally 67  
 intrusion sensor range 104  
 IP address 25, 48  
 IP addressing  
     default  
         IP addressing setting 25

## K

keypad configuration page 37

## L

lease, SIP server expiration time 51, 52, 53  
 LED  
     yellow activity LED 21  
 lengthy pages 62  
 Linux, setting up a TFTP server on 112  
 local SIP port 52  
 log in address 29

## M

MGROUP  
     MGROUP Name 61  
 mounting 101  
     additional mounting options 109  
     concrete wall mounting option (not provided) 110  
     conduit mounting option (not provided) 109  
     goose neck mounting option (not provided) 111  
     illustration of intercom mounting process 101  
     mounting an intercom 101  
     mounting components (part of the accessory kit) 101  
     network cable entry restrictions 106  
     overview of installation types 105

- rear conduit network cable entry restrictions (with shroud) 106
- rear conduit network cable entry restrictions (without shroud) 106
- securing the intercom 108
- service loop cable routing 107
- mounting components (part of the accessory kit) 101
- multicast configuration 69
- Multicast IP Address 61

## N

- navigation (web page) 26
- navigation table 26
- network cable entry restrictions 106
- network configuration of intercom 47
- Network Setup 47
- nightring tones 62
- Nightringer 10, 93
- nightringer settings 52
- NTP server 34

## O

- on-board relay 12
- on-board relay, 1A at 30 VDC 5
- output 5
- overview of installation types 105

## P

- packet time 4
- pages (lengthy) 62
- part number 5
- parts list 7
- password
  - for SIP server login 51
  - login 29
  - restoring the default 25
- payload types 5
- play audio locally (door sensor) 67
- play audio locally (intrusion sensor) 67
- play tone during DTMF activation 35
- point-to-point configuration 54
- polycom default channel 61
- polycom emergency channel 61
- polycom priority channel 61
- port
  - local SIP 52
  - remote SIP 52
- POST command 98

- power input 5
  - alternative 5
- power screwdriver 108
- priority
  - assigning 62
- product
  - configuring 25
- product features 3
- product overview
  - product features 3
  - product specifications 5
  - supported protocols 4
  - supported SIP servers 5
  - typical system installation 2
- product specifications 5
- protocol 5
- protocols supported 4
- push to talk, DTMF 36

## R

- rear conduit network cable entry restrictions (with shroud) 106
- rear conduit network cable entry restrictions (without shroud) 106
- reboot 96, 97
- remote SIP port 52
- reset test function management button 22
- resetting the IP address to the default 101
- restoring factory default settings 24, 115
- ringtones 62
  - lengthy pages 62
- RJ-45 20
- rport discovery setting, disabling 52
- RTFM button 22
- RTFM jumper 22, 23, 24
- RTP/AVP 4

## S

- sales 114
- securing the intercom 108
- security code 40
- security mode settings 38
- sensor setup page 55, 63, 66, 81
- sensor setup parameters 55, 63, 65
- sensors 67
- server address, SIP 51
- service 114
- service loop cable routing 107
- setting up the device 10
- settings, default 24



- shroud dimensions and mounting hole locations 103
- SIP
  - enable SIP operation 51
  - local SIP port 52
  - user ID 51
- SIP (session initiation protocol) 4
- SIP configuration 50
- SIP configuration parameters
  - outbound proxy 52
  - registration and expiration, SIP server lease 51, 52, 53
  - unregister on reboot 52
  - user ID, SIP 51
- SIP registration 51
- SIP remote SIP port 52
- SIP server 51
  - password for login 51
  - SIP servers supported 5
  - unregister from 52
  - user ID for login 51
- SIP server configuration 51
- SIP volume 34
- speaker output 5
- SRST 52
- subnet mask 25, 48
- supported protocols 4

## T

- tech support 114
- technical support, contact information 114
- TFTP server 4, 112
- triggering a dial out call or security code 40

## U

- unit dimensions and intrusion sensor range without the gang box 104
- unit dimensions—front and side view 102
- unit dimensions—rear view and mounting hole locations 102
- upgrading to firmware 6.x.x from 5.x.x 108
- user ID
  - for SIP server login 51
- username
  - changing for web configuration access 33
  - default for web configuration access 29
  - restoring the default 25

## V

- VLAN ID 48
- VLAN Priority 48
- VLAN tagging support 48
- VLAN tags 48
- volume
  - microphone gain 34
  - multicast volume 34
  - push to talk volume 34
  - ring volume 34
  - sensor volume 34
  - SIP volume 34

## W

- warranty policy at CyberData 114
- web access password 25
- web access username 25
- web configuration log in address 29
- web page
  - navigation 26
- web page navigation 26
- web-based intercom configuration 25
- weight 5
- wget, free unix utility 98
- Windows, setting up a TFTP server on 112
- wiring the circuit 13
  - devices less than 1A at 30 VDC 13