



# *SIP Heavy Duty Emergency Keypad Call Station Operations Guide*

Part #011463

Document Part #931490A  
for Firmware Version 11.0.0

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

---

**SIP Heavy Duty Emergency Keypad Call Station Operations Guide 931490A**  
**Part # 011463**

**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).

---

## Revision Information

Revision 931490A, which corresponds to firmware version 11.0.0, was released on June 13, 2018.

---



## Browsers Supported

The following browsers have been tested against firmware version 11.0.0:

- Internet Explorer (version: 10)
- Firefox (also called Mozilla Firefox) (version: 33.0)
- Chrome (version 48.0.2564.116)
- Safari (version: 5.1.7)

---

## Pictorial Alert Icons

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

---

## Hazard Levels

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

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

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

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

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






---

# Important Safety Instructions

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

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

 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> To prevent injury, this apparatus must be securely attached to the floor/wall in accordance with the installation instructions.</p>
 GENERAL ALERT	<p><b>Warning</b></p> <p>The PoE connector is intended for intra-building connections only and does not route to the outside plant.</p>

<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 Heavy Duty Emergency Keypad Call Station</b>	<b>7</b>
2.1 Parts List .....	7
2.2 SIP Heavy Duty Emergency Keypad Call Station Components .....	8
2.2.1 Operation .....	9
2.2.2 Dialing from the Keypad .....	9
2.3 Setting up the Device .....	10
2.3.1 Terminal Block Connections .....	10
2.3.2 Using the On-Board Relay .....	11
2.3.3 SIP Heavy Duty Emergency Keypad Call Station Connectors .....	13
2.3.4 Wiring .....	14
2.3.5 Activity and Link LEDs .....	15
2.3.6 Adjusting the Volume .....	19
2.3.7 SIP Heavy Duty Emergency Keypad Call Station Web Page Navigation .....	20
2.3.8 Using the Toggle Help Button .....	21
2.3.9 Log in to the Configuration Home Page .....	23
2.3.10 Configure the Device .....	27
2.3.11 Configure the Button Parameters .....	34
2.3.12 Configure the Security .....	38
2.3.13 Configure the Network Parameters .....	44
2.3.14 Configure the SIP (Session Initiation Protocol) Parameters .....	47
2.3.15 Configure the Multicast Parameters .....	53
2.3.16 Configure the Audio Configuration Parameters .....	57
2.3.17 Configure the Events Parameters .....	63
2.3.18 Configure the Door Strike Relay .....	69
2.3.19 Configure the Autoprovisioning Parameters .....	72
2.4 Upgrade the Firmware and Reboot the SIP Heavy Duty Emergency Keypad Call Station ...	84
2.4.1 Downloading the Firmware .....	84
2.4.2 Reboot the Device .....	86
2.5 Command Interface .....	87
2.5.1 Command Interface Post Commands .....	87
<b>Appendix A Mounting the SIP Heavy Duty Emergency Keypad Call Station</b>	<b>91</b>
A.1 Parts List .....	91
A.2 Installation .....	92
A.3 Dimensions .....	93
A.4 Mounting .....	94
<b>Appendix B Setting up a TFTP Server</b>	<b>95</b>
B.1 Set up a TFTP Server .....	95
B.1.1 In a LINUX Environment .....	95
B.1.2 In a Windows Environment .....	95
<b>Appendix C Troubleshooting/Technical Support</b>	<b>96</b>
C.1 Frequently Asked Questions (FAQ) .....	96

---

C.2 Documentation .....	96
C.3 Contact Information .....	97
C.4 Warranty and RMA Information .....	97
<b>Index</b>	<b>98</b>

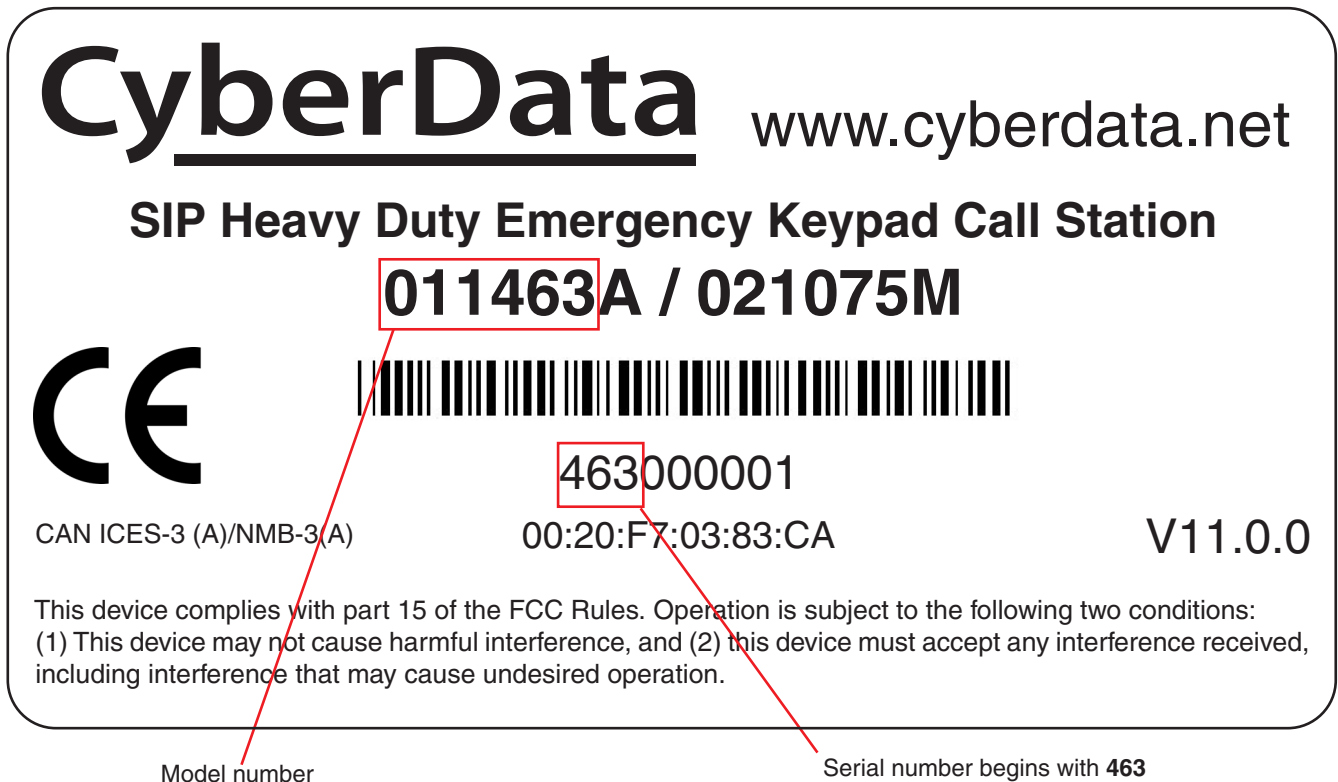
# 1 Product Overview

## 1.1 How to Identify This Product

To identify the SIP Heavy Duty Emergency Keypad Call Station, 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 **011463**.
- The serial number on the label should begin with **463**.

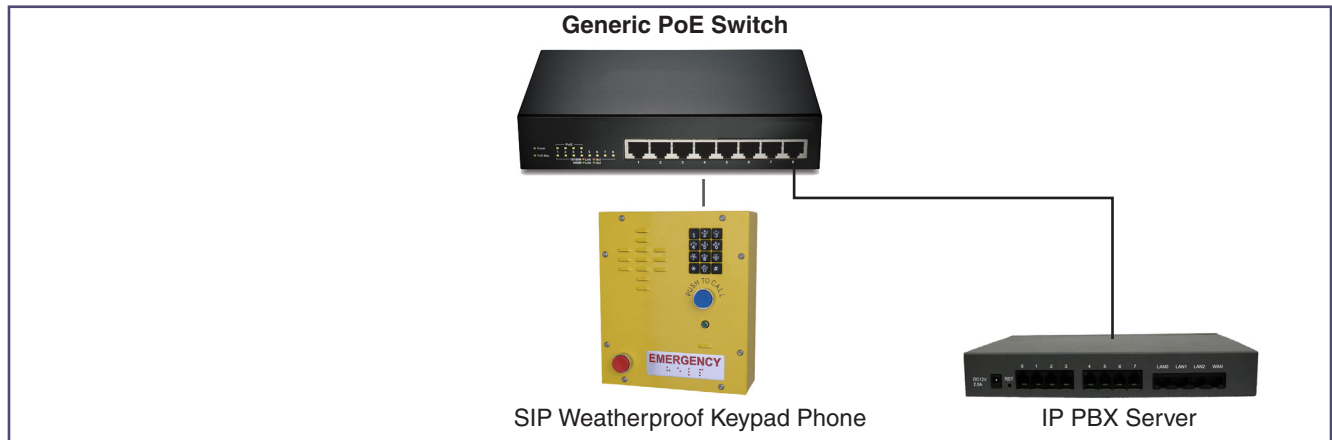
Figure 1-1. Model Number Label



## 1.2 Typical System Installation

The following figures illustrate how the SIP Heavy Duty Emergency Keypad Call Station can be installed as part of a VoIP phone system.

**Figure 1-2. Typical Installation**



---

## 1.3 Product Features

The SIP Heavy Duty Emergency Keypad Call Station has the following features:

- PoE 802.3af enabled (Power-over-Ethernet)
- Doubles as a paging speaker
- Corrosion protected and powder coated steel faceplate
- Hands free operation
- Push to call and emergency call buttons
- Surge arrestor to prevent voltage spike damage
- Easy support drill guides for top and bottom mount glands
- LED for visual indication of call
- Electronic ringer
- Concurrent SIP call and multicast paging
- Supports SRST (Survivable Remote Site Telephony) in a Cisco environment
- Network web management and firmware download
- Programmable speed dial

---

## 1.4 Supported Protocols

The SIP Heavy Duty Emergency Keypad Call Station supports the following protocols:

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

Provides an intuitive user interface for easy system configuration and verification of SIP Heavy Duty Emergency Keypad Call Station 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

Facilitates autoprovisioning configuration values on boot

- Audio Encodings

PCMU (G.711 mu-law)

PCMA (G.711 A-law)

G.722

Packet Time 20 ms

---

## 1.5 Supported SIP Servers

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

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

## 1.6 Specifications

**Table 1-1. Specifications**

<b>Specifications</b>	
Ethernet I/F	10/100 Mbps
Protocol	SIP RFC 3261 Compatible
Power Input	PoE 802.3af compliant or +24 VDC @ 1000mA Regulated Power Supply <sup>a</sup>
On-Board Relay	1A at 30 VDC
Environmental	Temperature: -40° to +140° F (-40° to + 60° C) Humidity: 0 - 95% RH Non-Condensing
Storage Temperature	-40° C to 70° C (-40° F to 158° F)
Storage Altitude	Up to 15,000 ft. (4573 m)
Payload Types	G711, A-law and $\mu$ -law, G.722
Dimensions <sup>b</sup>	9.0 inches [229 mm] Length 3.6 inches [91 mm] Width 10.5 inches [267 mm] Height
Weight	7 lbs (3.2 kg)
Boxed Weight	10.0 lbs (4.6 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	011463

a. Contacts 3 and 4 on the terminal block are only for powering the device from a non-PoE +24VDC 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.

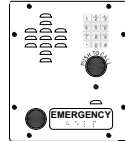


# 2 Installing the SIP Heavy Duty Emergency Keypad Call Station

## 2.1 Parts List

Table 2-1 illustrates the SIP Heavy Duty Emergency Keypad Call Station parts.

**Note** See [Appendix A, "Mounting the SIP Heavy Duty Emergency Keypad Call Station"](#) for physical mounting information.

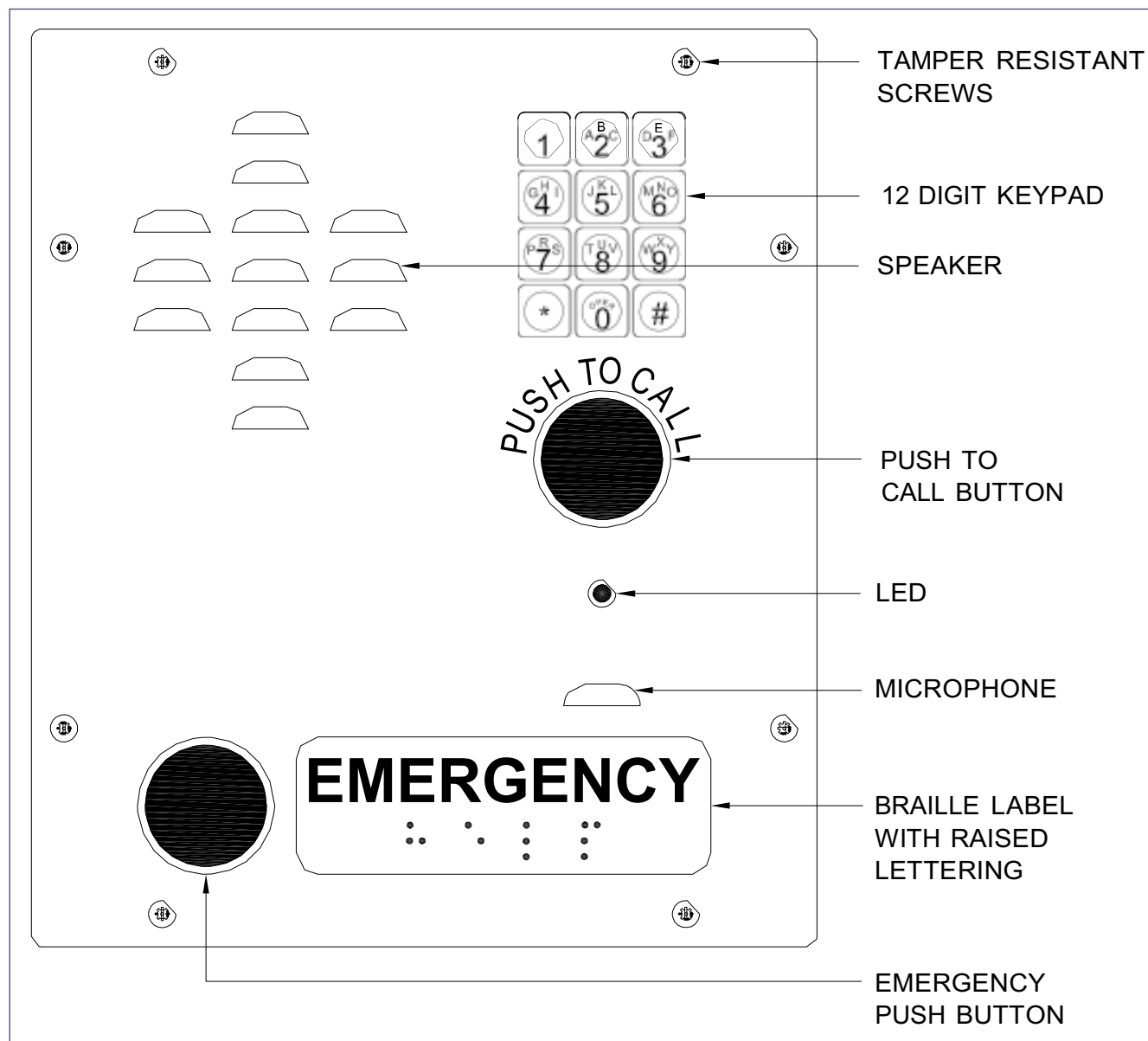
**Table 2-1. Parts List**

Quantity	Part Name	Illustration
1	SIP Heavy Duty Emergency Keypad Call Station Assembly	
1	Installation Quick Reference Guide	
1	SIP Heavy Duty Emergency Keypad Call Station Mounting Accessory Kit	

## 2.2 SIP Heavy Duty Emergency Keypad Call Station Components

Figure 2-1 shows the components of the SIP Heavy Duty Emergency Keypad Call Station.

**Figure 2-1. SIP Heavy Duty Emergency Keypad Call Station Components**



## 2.2.1 Operation

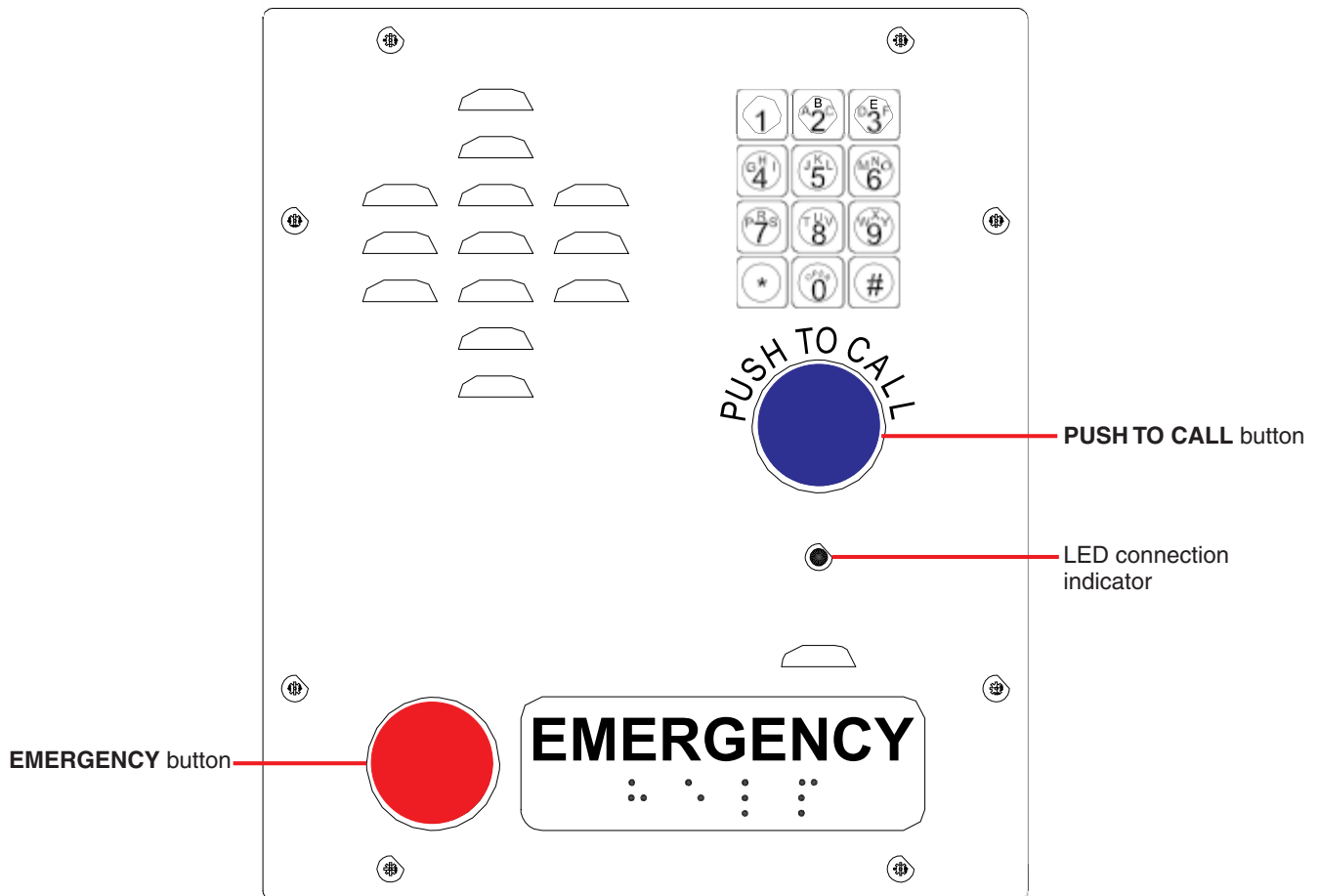
**EMERGENCY**—When the **EMERGENCY** button is pressed (Figure 2-2), it dials the extension specified on the **Button Configuration Page**. When the dialed extension answers the call, the LED will commence blinking, and it will continue to do so until the call is terminated.

**TO CALL**—See Section 2.3.11.1, "Triggering a Dial Out Call or Security Code."

## 2.2.2 Dialing from the Keypad

- See the **Enable Telephone Operation** setting in Section 2.3.11, "Configure the Button Parameters".

Figure 2-2. EMERGENCY Button and Push TO CALL Button




## 2.3 Setting up the Device

### 2.3.1 Terminal Block Connections

Figure 2-3 shows the pin connections on the J9 terminal block. This terminal block can accept a wire range from 16 AWG to 24 AWG.

**Note** As an alternative to using PoE power +24 VDC at 1000 mA can be supplied to the terminal block.

	<p><b>Caution</b></p> <p><i>Equipment Hazard:</i> Contacts 3 and 4 on the terminal block are only for powering the device from a non-PoE +24 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. Terminal Block Connections and Alternate Power Input**

Alternate Power Input:

- 1 = Normally Open Common
- 2 = Normally Open Contact



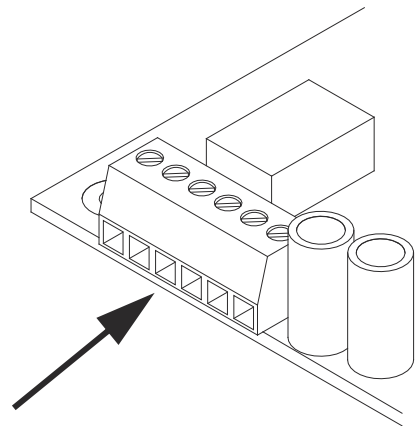
Relay Contact:

(0.5 A at 30 VDC for continuous loads)




- 3 = +24 VDC @ 1000mA
- 4 = Power Ground
- 5 = Ringer +
- 6 = Ringer -

\*Contacts 3 and 4 on the terminal block are only for powering the device from a non-PoE +24 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.


**WIRE IN**  
Can accept wire range from  
16 AWG to 24 AWG



## 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 SIP Heavy Duty Emergency Keypad Call Station incorporates one on-board relay located on the PCBA, which enables users to control a low current external relay or device (see [Figure 2-4](#)). An external relay could control a ringer, strobe light, door lock or any other apparatus. The on board relay is protected by a 1 Amp, non-replaceable fuse. Power switched by the relay should not exceed 0.5 Amps @ 30VDC. The PCBA is not designed to handle AC voltages.

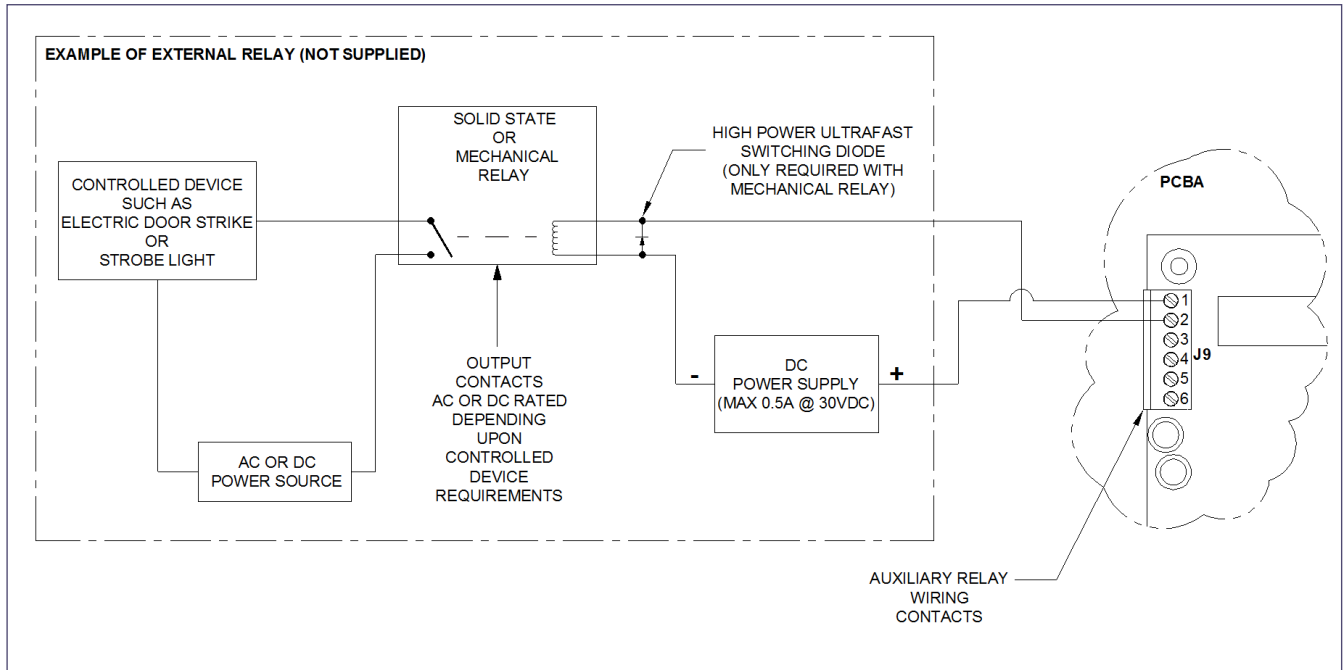
 GENERAL ALERT	<p><b>Warning</b></p> <p><i>Equipment Hazard:</i> The relay circuitry contains a non-replaceable 250VAC 1A fuse. If the fuse blows, the board must be returned to CyberData or an approved service center for repair.</p>
--	---

The device relay activation time is selectable through the web interface on the Device Configuration Page (see [Section 2.3.10, "Configure the Device"](#)). The relay is controlled by DTMF tones generated from the phone to which the VoIP phone is connected; no matter which one initiated the call.

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.

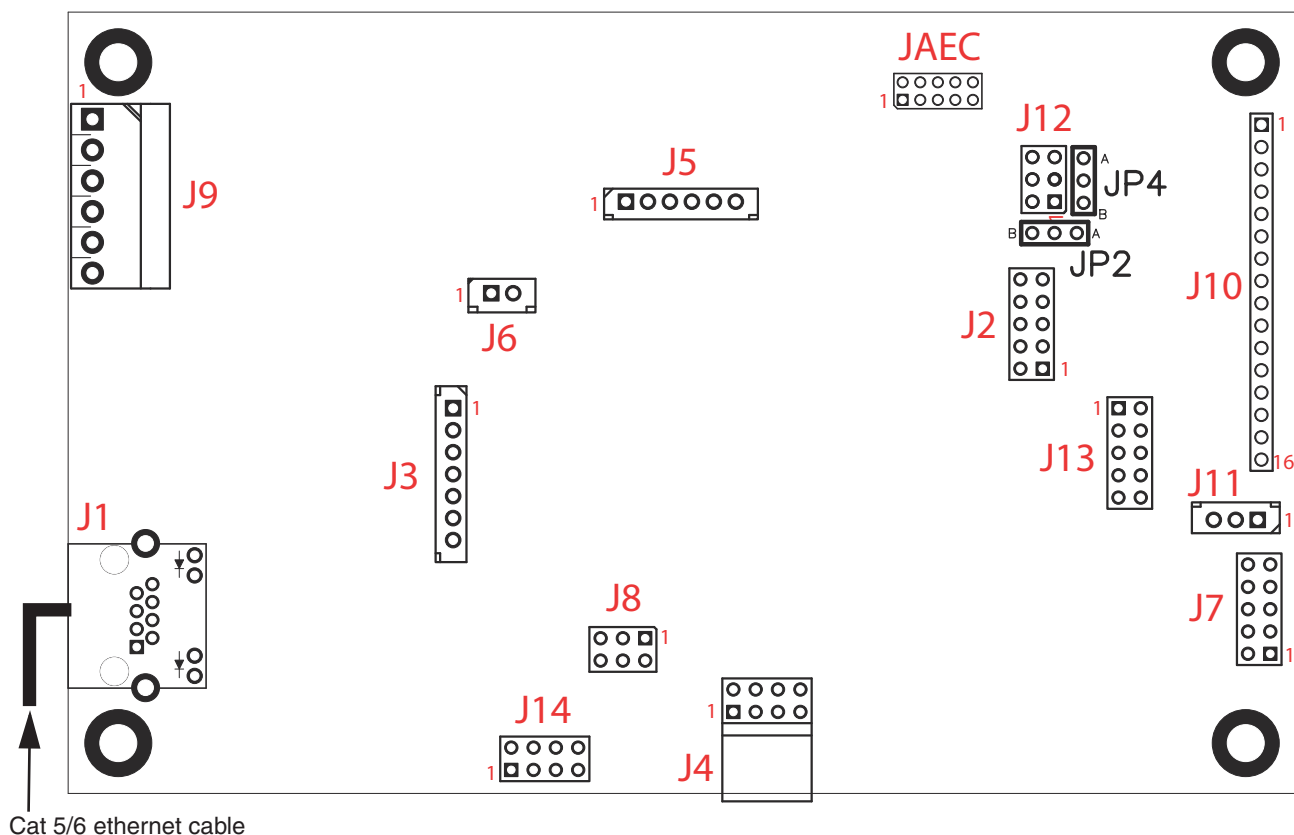
**Figure 2-4. Auxiliary Relay Wiring Diagram**



## 2.3.3 SIP Heavy Duty Emergency Keypad Call Station Connectors

See [Figure 2-5](#) and [Table 2-2](#) to identify the connectors and functions of the board.

**Figure 2-5. Connector Locations**



**Table 2-2. Connector Functions**

Connector	Function
J1	PoE Network Connection (RJ-45) J1: STANDARD 8 PIN RJ45 10/100Base-T And power input via Power over Ethernet
J2	Hands free Microphone Interface/LED Interface
J3	Opto-Isolated Inputs/Outputs
J4	JTAG Interface — Factory Only
J5	Handset/Reed Switch Interface
J6	Speaker Interface
J7	Keypad Interface
J8	Console Port — Factory Only
J9	Terminal Block (see <a href="#">Figure 2-3</a> ) — Users Interface
J10	LCD Interface — Not Used
J11	Handset Volume Control Interface



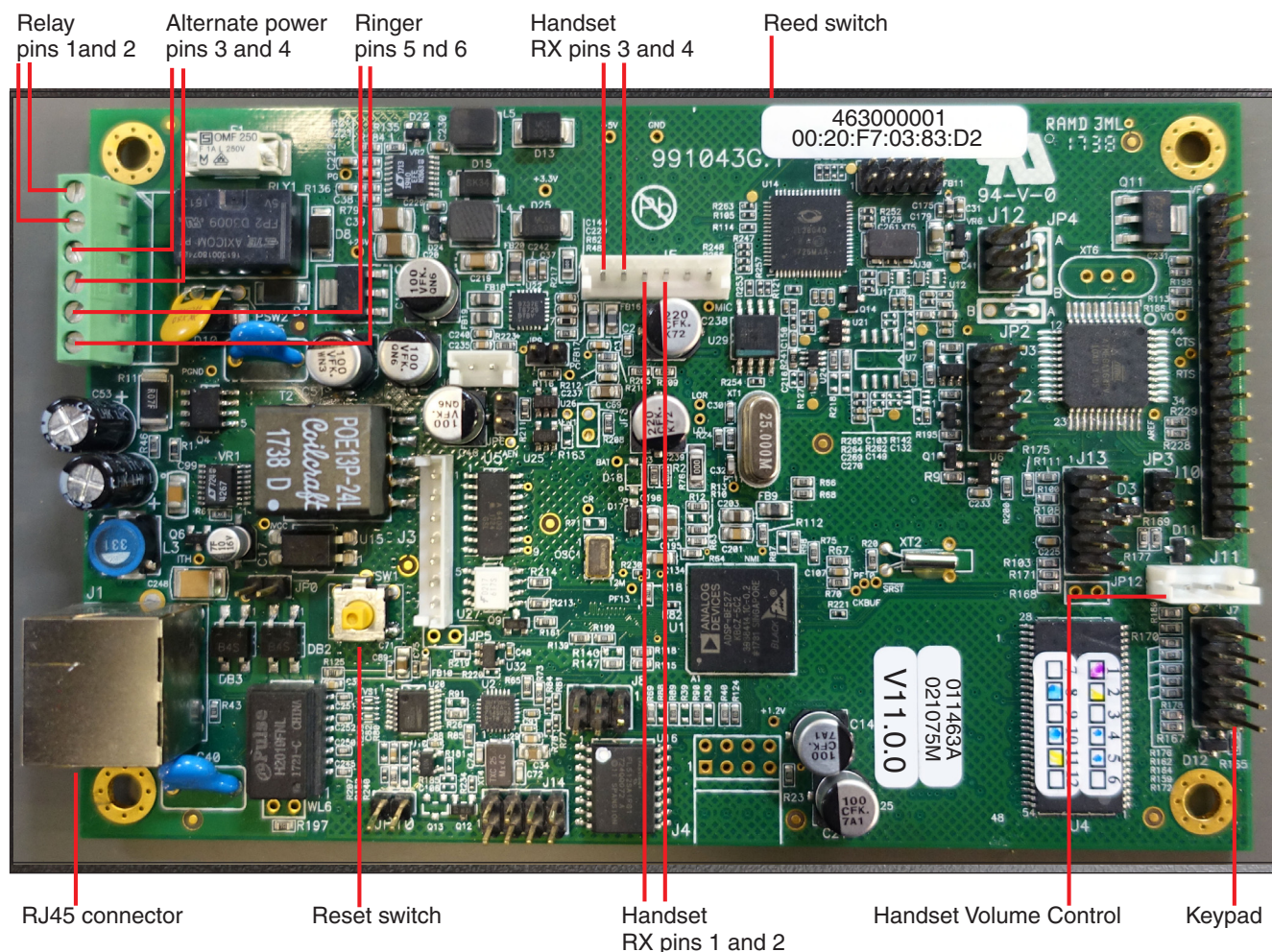
**Table 2-2. Connector Functions (continued)**

Connector	Function
J12	ISP-DIP/Debug UART — Factory Only
JAEC	AEC ISP — Factory Only

## 2.3.4 Wiring

See [Figure 2-6](#) for the wiring of the SIP Heavy Duty Emergency Keypad Call Station.

**Figure 2-6. Wiring<sup>1</sup>**



1. This figure is just an example, and the information on the board and labels may be different.

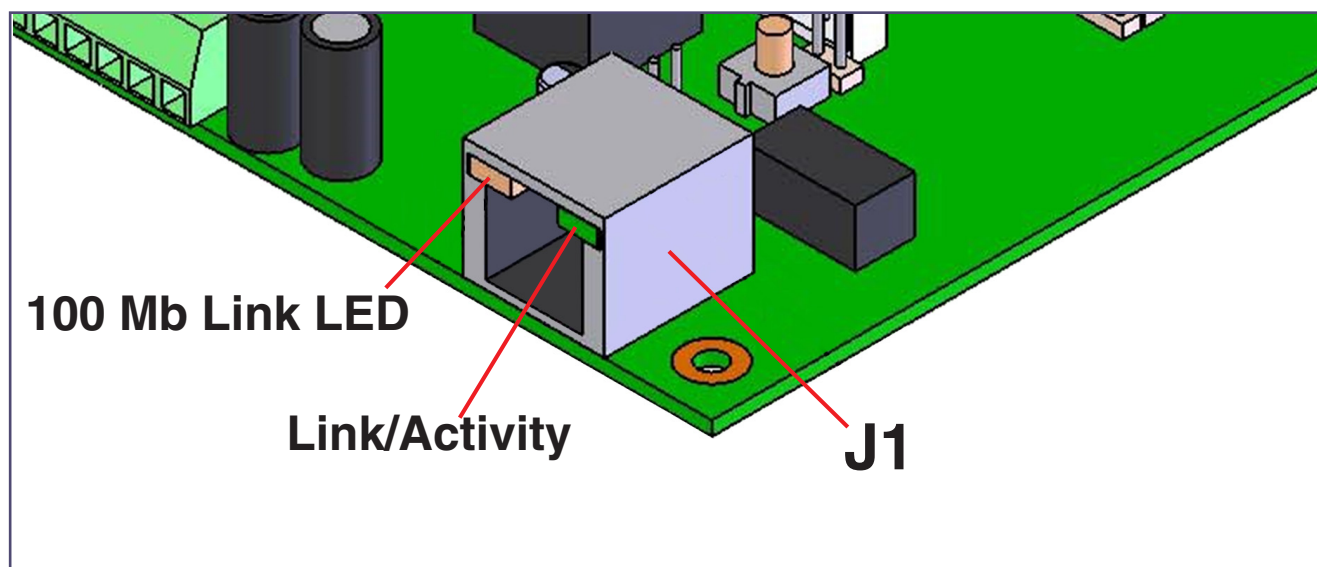
## 2.3.5 Activity and Link LEDs

### 2.3.5.1 Verifying the Network Connectivity and Data Rate

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

- The square, **AMBER 100 Mb Link** LED above the Ethernet port indicates that the network connection has been established with a 100 Mb connection (see [Figure 2-7](#)).
- The square, **GREEN Link/Activity** LED indicates and Ethernet link and blinks when there is network activity (see [Figure 2-7](#)).

**Figure 2-7. Activity and Link LED**

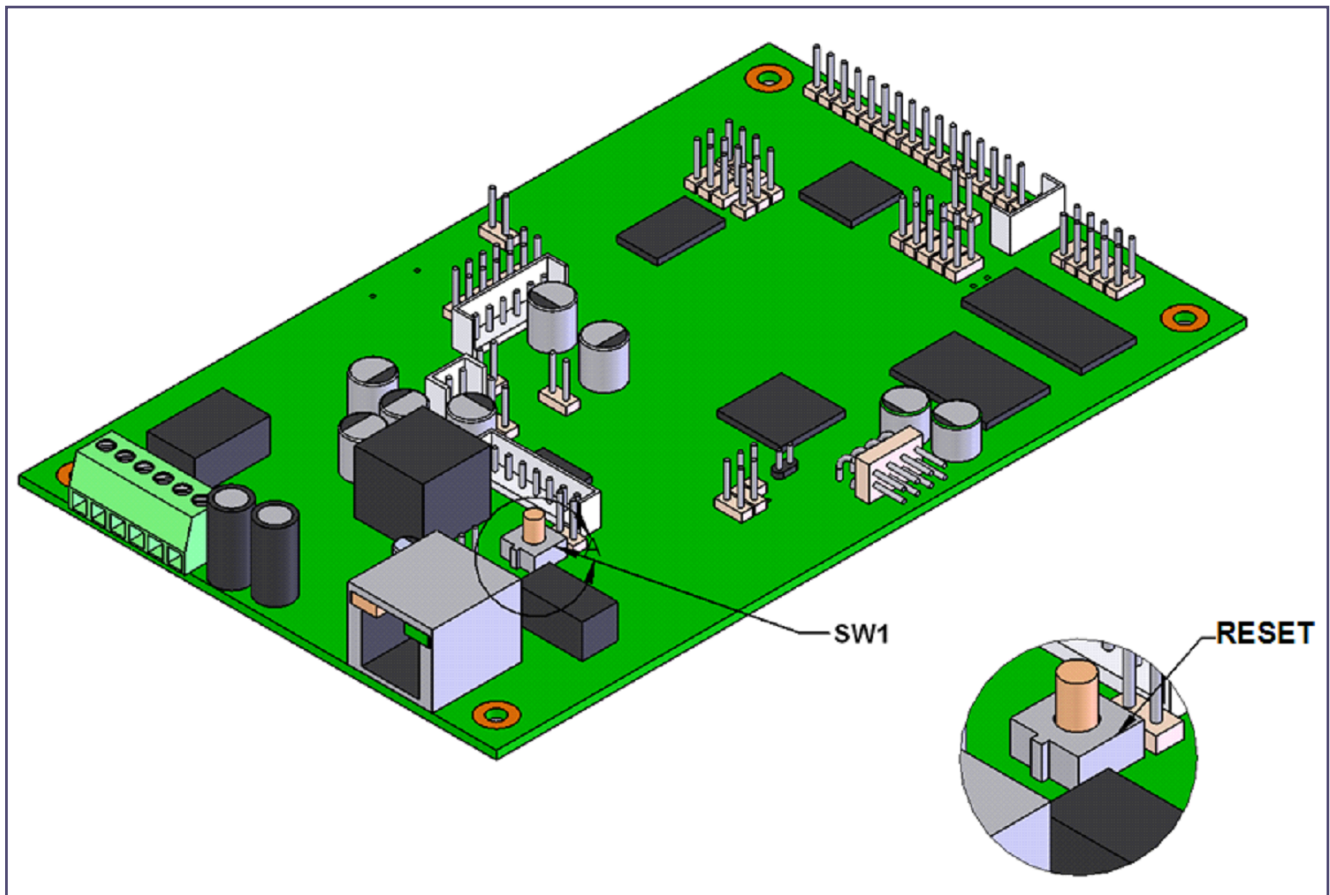


### 2.3.5.2 Reset Test Function Management (RESET) Switch

When the device is operational and linked to the network, use the Reset Test Function Management (RESET) switch on the board (see **SW1** in [Figure 2-8](#)) to announce the device's IP Address and test that the audio is working (see [Section 2.3.5.3, "Announcing the IP Address"](#)). During the IP address announcement, you will hear the IP address through the speaker of the device.

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

**Figure 2-8. RESET Switch**





### 2.3.5.3 Announcing the IP Address

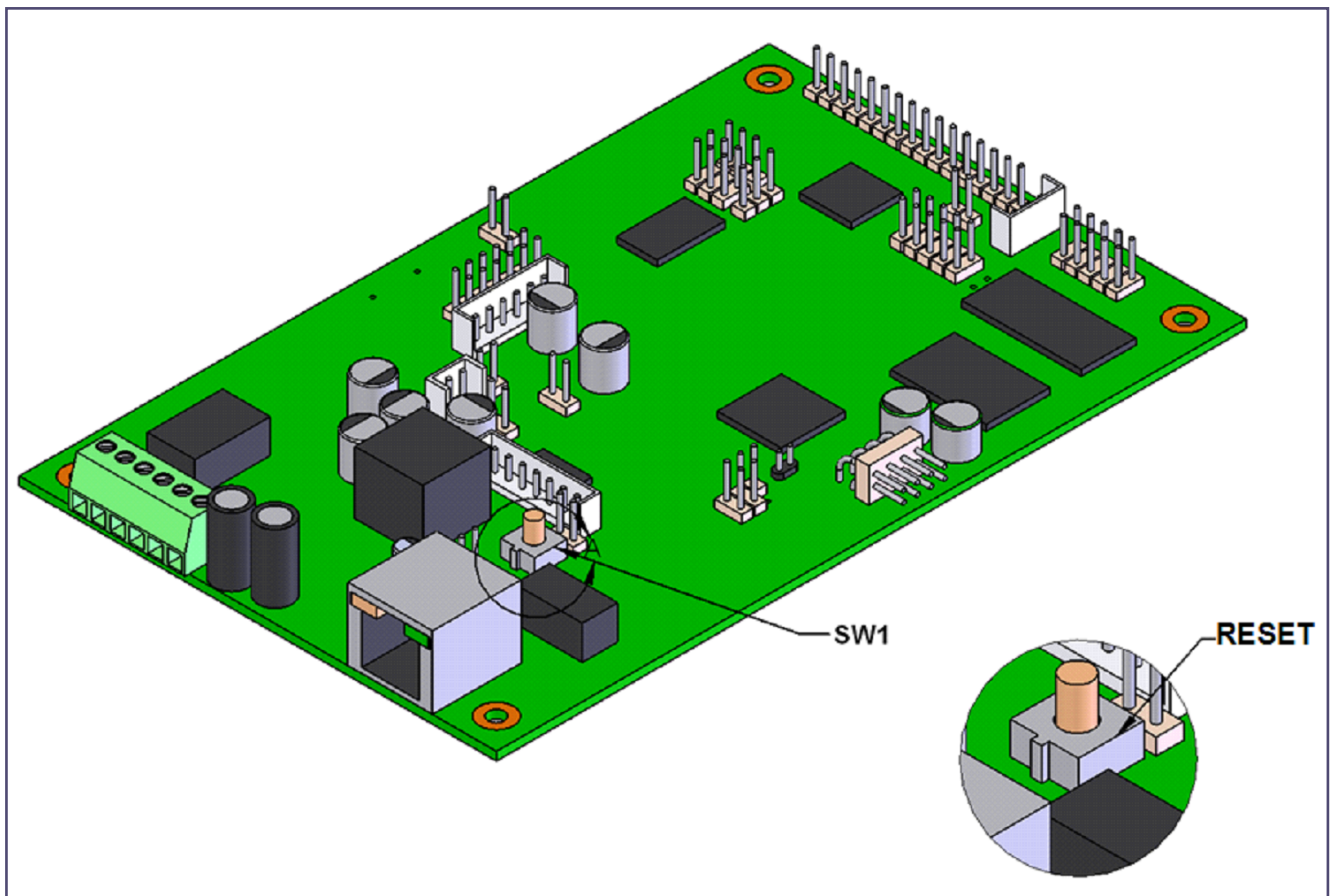
To announce the device's current IP address:

1. Press and hold for two seconds.
2. Release the **RESET** switch (see **SW1** in [Figure 2-9](#)).

**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 RESET switch for longer than five seconds will restore the device to the factory default settings.

**Figure 2-9. RESET Switch**



### 2.3.5.4 Restoring the Factory Default Settings

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

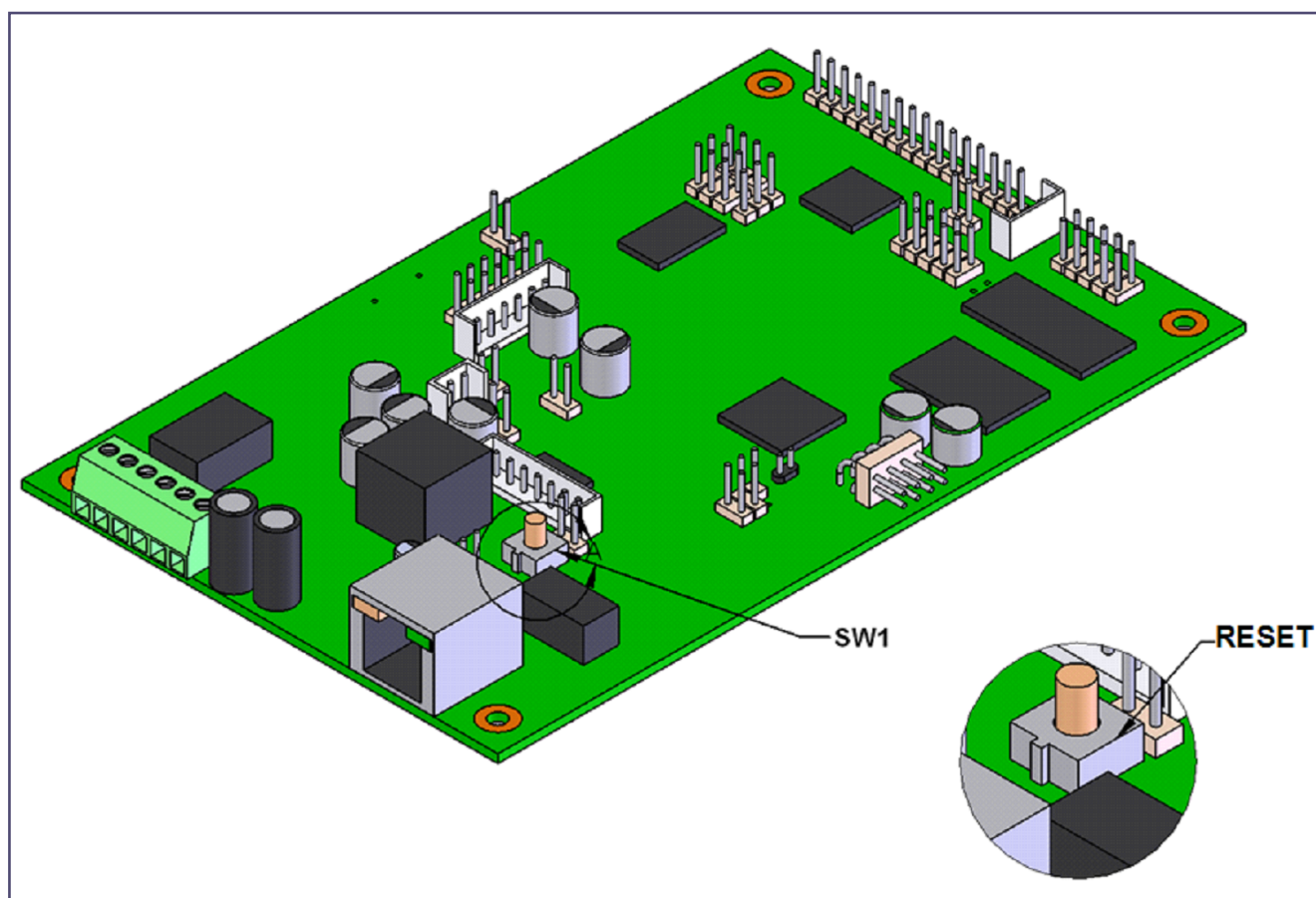
**Note** Each SIP Heavy Duty Emergency Keypad Call Station is delivered with factory set default values.

To restore the factory default settings:

1. Press and hold the **RESET** switch (see **SW1** in [Figure 2-10](#)) until the device announces it is restoring to factory defaults (approximately 5 seconds).
2. Release the **RESET** switch.

**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 2-10. RESET Switch**



---

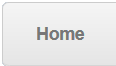

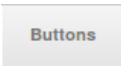

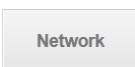

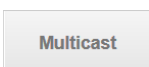
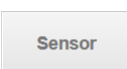
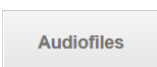


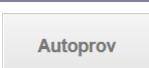
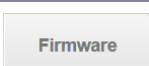
## 2.3.6 Adjusting the Volume

You can adjust the SIP Heavy Duty Emergency Keypad Call Station default volume through the volume settings on the [Device Configuration Page](#).

## 2.3.7 SIP Heavy Duty Emergency Keypad Call Station Web Page Navigation

Table 2-3 shows the navigation buttons that you will see on every SIP Heavy Duty Emergency Keypad Call Station web page.

**Table 2-3. 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>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.

## 2.3.8 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:

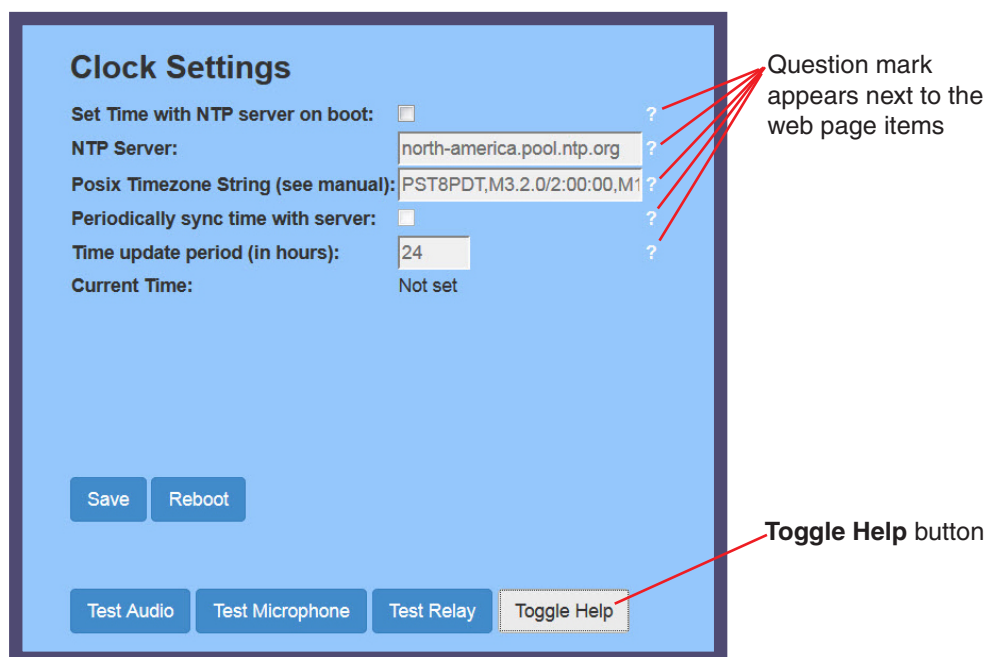
1. Click on the **Toggle Help** button that is on the UI webpage. See [Figure 2-11](#) and [Figure 2-12](#).

**Figure 2-11. 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 2-12](#).

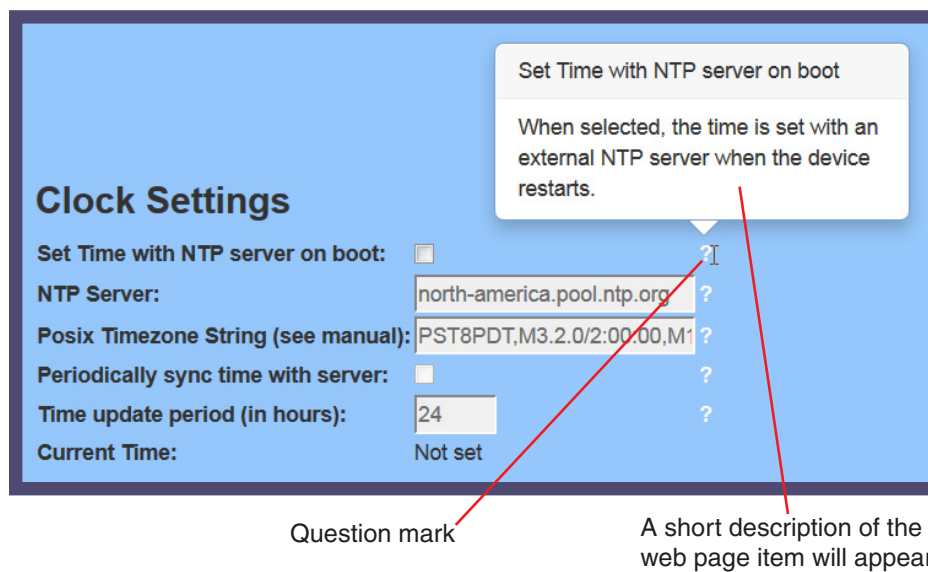
**Figure 2-12. Toggle Help Button and Question Marks**





3. Move the mouse pointer to hover over the question mark (?), and a short description of the web page item will appear. See Figure 2-13.

**Figure 2-13. Short Description Provided by the Help Feature**



---

## 2.3.9 Log in to the Configuration Home Page

1. Open your browser to the SIP Heavy Duty Emergency Keypad Call Station 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 SIP Heavy Duty Emergency Keypad Call Station.

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

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

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

**Note** The device 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 2-14):

Web Access Username: **admin**

Web Access Password: **admin**

Figure 2-14. Home Page

HomeDeviceButtonsSecurityNetworkSIPMulticastAudiofilesEventsDSRAutoprovFirmware

# CyberData Handsfree w/Keypad

### Current Status

Serial Number: 463100001  
Mac Address: 00:20:f7:03:b8:58  
Firmware Version: v11.0.0

IP Addressing: DHCP  
IP Address: 10.10.0.116  
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  
Push to Talk Volume: 4  
Volume Boost: Off  
Microphone Gain: 4  
Push to Talk Microphone Gain:4

SIP Mode: Enabled  
Event Reporting: Disabled  
Nightringer: Disabled

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

### Admin Settings

Username: admin  
Password:  
Confirm Password:

SaveRebootToggle Help

### Import Settings

Choose File No file chosen

Import Config

### Export Settings

Export Config

Operations Guide

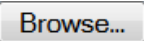
931490A

CyberData Corporation






3. On the **Home** page, review the setup details and navigation buttons described in [Table 2-4](#).

**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 2-4. 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.
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 level.
Volume Boost	Shows the current Volume Boost level.
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.
Event Reporting	Shows the current status of the Event Reporting mode.
Nightringer	Shows the current status of the Nightringer mode.
Primary SIP Server	Shows the current status of the Primary SIP Server.
Backup Server 1	Shows the current status of Backup Server 1.
Backup Server 2	Shows the current status of Backup Server 2.
Nightringer Server	Shows the current status of Nightringer Server.
<b>Import Settings</b>	
	Use this button to select a configuration file to import.

**Table 2-4. Home Page Overview (continued)**

Web Page Item	Description
	After selecting a configuration file, click Import to import the configuration from the selected file. Then, click Save and Reboot to store changes.
<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. <b>Note:</b> You need to reboot for changes to take effect.
	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** The user name and password will be saved immediately, but the user will not be prompted to enter them until there is a reboot. It is advisable to restart the web browser after this change.

## 2.3.10 Configure the Device

1. Click the **Device** menu button to open the **Device** page. See [Figure 2-15](#).

**Figure 2-15. Device Configuration Page**

Home Device Buttons Security Network SIP Multicast Audiofiles Events DSR Autopro Firmware

# CyberData Handsfree w/Keypad

### Volume Settings (0-9)

SIP Volume:

Multicast Volume:

Ring Volume:

Push to Talk Volume:

No Volume Boost ▼

### 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: ☐

Pulse Relay During 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:

### Clock Settings

Set Time with NTP server on boot: ☐

NTP Server:

Posix Timezone String (see manual):

Periodically sync time with server: ☐

Time update period (in hours):

Current Time: 18:24:22

### Misc Settings

Device Name:

Auto-Answer Incoming Calls: ☒

Play Ringback Tone: ☐

Enable DTMF Push to Talk: ☐

Prevent Call Termination: ☐

Disable HTTPS (NOT recommended): ☐

Save Reboot

Test Relay Start Button Test Toggle Help

2. On the **Device** page, you may enter values for the parameters indicated in [Table 2-5](#).

**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 2-5. 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.  <b>Note:</b> You can change this setting without rebooting the device.
Multicast Volume ?	Set the speaker volume for multicast audio streams. A value of 0 will mute the speaker during multicasts.  <b>Note:</b> You can change this setting without rebooting the device.
Ring Volume ?	Set the ring volume for incoming calls. A value of 0 will mute the speaker instead of playing the ring tone when <b>Auto-Answer Incoming Calls</b> is disabled.  <b>Note:</b> You can change this setting without rebooting the device.
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>Note:</b> You can change this setting without rebooting the device.
Volume Boost: ? No Volume Boost Volume Boost 1 Volume Boost 2 Volume Boost 3	Set the Boost level to increase the volume output of the speaker. Using Volume Boost may introduce audio clipping or reduce intelligibility of the speaker audio. Boost will raise the volume above level <b>9</b> , regardless of the digital volume settings.
<b>Microphone Settings</b>	
Microphone Gain ?	Set the microphone gain level.
Push to Talk Microphone Gain ?	Set the microphone gain level for Push to Talk operation.
<b>Clock Settings</b>	
Set Time with NTP Server on boot ?	When selected, the time is set with an external NTP server when the device restarts.
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.  <b>Note:</b> The <b>NTP Server</b> setting needs to be restarted to spawn NTP or to change the server.
Posix Timezone String ?	See <a href="#">Section 2.3.10.1, "Time Zone Strings"</a> for information about how to use the Posix Timezone String to specify time zone and daylight savings time where applicable. Enter up to 63 characters.
Periodically sync time with server ?	When selected, the time is periodically updated with the NTP server at the configured interval below.

**Table 2-5. Device Configuration Parameters (continued)**

Web Page Item	Description
Time update period (in hours) ?	The time interval after which the device will contact the NTP server to update the time. Enter up to 4 digits.  <b>Note:</b> Syncing and changing the <b>Time update period (in hours)</b> setting does not require a reboot for the changes to take effect.
Current Time	Allows you to input the current time. (6 character limit)
<b>Relay Settings</b>	<b>Note:</b> None of the <b>Relay Settings</b> require a reboot for the changes to take effect.
Activate Relay with DTMF Code ?	Activates the relay when the DTMF Activation Code is entered on the phone during a SIP call with the device. RFC2833 DTMF payload types are supported.
Relay Pulse Code ?	DTMF code used to pulse the relay when entered on a phone during a SIP call with the device. Relay will activate for Relay Pulse Duration seconds then deactivate. Activate Relay with DTMF Code must be enabled. Enter up to 25 digits (* and # are supported).
Relay Pulse Duration (in seconds) ?	The length of time (in seconds) during which the relay will be activated when the DTMF Relay Activation Code is detected. Enter up to 5 digits.
Relay Activation Code ?	Activation code used to activate the relay when entered on a phone during a SIP call with the device. Relay will be active indefinitely, or until the DTMF Relay Deactivation code is entered. Activate Relay with DTMF Code must be enabled. Enter up to 25 digits (* and # are supported).
Relay Deactivation Code ?	Code used to deactivate the relay when entered on a phone during a SIP call with the device. Activate Relay with DTMF Code must be enabled. Enter up to 25 digits (* and # are supported).
Play tone during DTMF Activation ?	When selected, the device will play a tone out of the speaker upon DTMF relay activation. The tone plays for the DTMF Activation Duration (in seconds).
Activate Relay During Ring ?	When selected, the relay will be activated for as long as the device is ringing. When <b>Auto-Answer Incoming Calls</b> 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.
Pulse Relay During Ring ?	When selected, the relay will pulse as long as the device is ringing. When <b>Auto-Answer Incoming Calls</b> is enabled, the device will not ring and this option does nothing. Activate Relay During Ring must be selected to use this option.
Activate Relay While Call Active ?	When selected, the relay will be activated as long as the SIP call is active.
Activate Relay on Button Press ?	When selected, the relay will be activated when the Call button is pressed.
Relay on Button Press Duration ?	The length of time (in seconds) during which the relay will be activated when the Call button is pressed. Enter up to 5 digits. A <b>Relay on Button Press Duration</b> value of 0 will pulse the relay once when the Call button is pressed.
<b>Misc Settings</b>	
Device Name ?	Type the device name. Enter up to 25 characters.
Auto-Answer Incoming Calls ?	When selected, incoming calls will be answered automatically.



**Table 2-5. Device Configuration Parameters (continued)**

Web Page Item	Description
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 DTMF Push to Talk ?	<p>This option is for noisy environments. When enabled, in an active call, the remote phone can force receive only audio (setting the mic gain to max and muting the speaker) by pressing the * key.</p> <p>Pressing the # key will force send only audio (setting the max speaker volume and muting the mic). Pressing the 0 key will restore full duplex operation with the normal microphone and speaker volume.</p>
Prevent Call Termination ?	When this option is enabled, a call cannot be terminated using the call button.
Disable HTTPS (NOT recommended) ?	<p>Disables the encrypted connection to the webpage. We do not recommend disabling HTTPS for security reasons.</p> <p><b>Note:</b> This setting requires a reboot for the changes to take effect.</p>
Test Relay	Click on the <b>Test Relay</b> button to do a relay test.
Start Button Test	Click on the <b>Start</b> button to start a button test.
Save	<p>Click the <b>Save</b> button to save your configuration settings.</p> <p><b>Note:</b> You need to reboot for changes to take effect.</p>
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.

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

### 2.3.10.1 Time Zone Strings

The posix time zone string tells the internal date and time utilities how to handle daylight savings time for different time zones. [Table 2-6](#) shows some common strings.

**Table 2-6. Common Time Zone Strings**

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

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

[Table 2-7](#) shows a breakdown of the parts that constitute the following time zone string:

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

**Table 2-7. Time Zone String Parts**

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

Time Zone String Examples **Table 2-8** has some more examples of time zone strings.

**Table 2-8. Time Zone String Examples**

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

a. Tokyo does not use daylight savings time.

b. For Berlin, daylight savings time starts on the last Sunday in March at 01:00 UTC, and ends on the last Sunday in October at 01:00 UTC, and is one hour ahead of UTC.

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

**Figure 2-16. Three or Four Character Time Zone Identifier**

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

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

World GMT Table **Table 2-9** has information about the GMT time in various time zones.

**Table 2-9. World GMT Table**

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

**Table 2-9. World GMT Table (continued)**

<b>Time Zone</b>	<b>City or Area Zone Crosses</b>
GMT+5	Islamabad, Karachi
GMT+6	Almaty, Dhaka
GMT+7	Bangkok, Jakarta
GMT+8	Hong Kong, Beijing
GMT+9	Tokyo, Osaka
GMT+10	Sydney, Melbourne, Guam
GMT+11	Magadan, Solomon Is.
GMT+12	Fiji, Wellington, Auckland

## 2.3.11 Configure the Button Parameters

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

**Figure 2-17. Button Configuration Page**

**CyberData Handsfree w/Keypad**

**Dial Mode**

Enable Telephone Operation: ☐

Enable Cell Phone Operation: ☐

Enable Speed Dial Operation: ☐

Enable Security Operation: ☐

**Security Mode Settings**

Relay Activation Code:

Relay Deactivation Code:

Allow Telephone Dialout: ☒

Call Button:  ID:

Send Multicast Audio: ☐

Multicast Address:

Multicast Port:

Repeat Message:

**Speed Dial Settings**

Speed Dial Timeout:

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

**Emergency Dial Settings**

Emergency Button Dial out Extension:

Emergency Extension ID:

**Button Tones**





Play Button Tones: ☒

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

**Table 2-10. 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. 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 the keypad, preceded by the # key. 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 the keypad, preceded by the # key. Enter up to 25 digits (* and # are supported).
Allow Telephone Dialout ?	When enabled, the user will be able to use the call button to dial a pre-set extension, specified on the web page.
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. <b>Note:</b> This setting requires a reboot for the changes to take effect.
Multicast Port ?	The multicast port used for multicasting an audio file. <b>Note:</b> This setting requires a reboot for the changes to take effect.
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.

**Table 2-10. Button Configuration Parameters (continued)**

Web Page Item	Description
Keypad 6	Dial this extension when the 6 key is pressed.
Keypad 7	Dial this extension when the 7 key is pressed.
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.
<b>Emergency Dial Settings</b>	
Emergency Button Dial out Extension ?	Specify the extension the device will call when someone presses the Red Emergency Button. Enter up to 64 alphanumeric characters.
Emergency Extension ID ?	A Caller Identification string added to outbound calls initiated by the Red Emergency Button. Enter up to 64 alphanumeric characters.
<b>Button Tones</b>	
Play Button Tones ?	Play a tone when the keypad buttons are pressed.
	Click the <b>Save</b> button to save your configuration settings. <b>Note:</b> You need to reboot for changes to take effect.
	Click on the <b>Reboot</b> button to reboot the system.
	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.

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

**Note** To change dial modes, or enable (or change) multicasting, you must reboot the device.

### 2.3.11.1 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>1234560</b> (and waiting for several seconds)	The device will activate the relay for <b>Security Code 0</b> for <b>6</b> seconds.



## 2.3.12 Configure the Security

1. Click the **Security** menu button to open the **Security** page. See [Figure 2-15](#).

Figure 2-18. Security Configuration Page

HomeDeviceButtonsSecurityNetworkSIPMulticastAudiofilesEventsDSRAutoprovFirmware

# CyberData Handsfree w/Keypad

### Security Configuration

Name	Code	Valid From	Valid To	Blacklist		
Jason	123456	Mon12:00	Mon13:00	no	Edit	Delete
Olivia	123457	All	All	no	Edit	Delete
Noah	123458	Wdy	Wdy	no	Edit	Delete
Emma	223456	Wdy8:00	Wdy18:00	no	Edit	Delete
Liam	234567	Wnd12:00	Wnd16:00	no	Edit	Delete
Charlotte	321456	Wed9:00	Wed17:00	no	Edit	Delete
Jackson	412345	All	All	no	Edit	Delete
Sophia	578945	All	All	yes	Edit	Delete
Lucas	987654	Wdy8:30	Wdy17:30	no	Edit	Delete
Aria	852369	All	All	no	Edit	Delete
Logan	258741	Wdy7:00	Wdy16:30	no	Edit	Delete
Ava	741236	Wnd	Wnd	no	Edit	Delete
Benjamin	125487	All	All	no	Edit	Delete
Chloe	885522	All	All	no	Edit	Delete
						New

### Relay Settings

Activate Relay on Valid Entry ☒

Activate DSR on Valid Entry ☐

Relay Timeout (seconds)

### Audio Settings

Play tone while Relay Active ☐

Play tone on Invalid Code Entry ☒

### Blacklist Actions

Play Message to SIP Extension ☐

Dial Out SIP Extension

Dial Out SIP ID

Repeat SIP Message

Multicast Audio Message ☐

Multicast Address

Multicast Port

Times to Play Multicast Message

### Security log

2018-05-15 11:47:04 Deactivating the relay after timeout

2018-05-15 11:47:04 Deactivating the dsr relay after timeout

2018-05-15 11:46:57 Security code match for blacklisted fri test1!

2018-05-15 11:46:53 Security code for fri test5 activating the remote relay

2018-05-15 11:46:53 Security code for fri test5 activating the local relay

2018-05-15 11:46:04 Deactivating the relay after timeout

2018-05-15 11:46:04 Deactivating the dsr relay after timeout

2018-05-15 11:46:01 Security code match for blacklisted fri test1!

2018-05-15 11:45:57 Security code for fri test60 activating the remote relay

2018-05-15 11:45:57 Security code for fri test60 activating the local relay

Get Security Log

Clear Security Log

Refresh Log

Save

Reboot

Toggle Help

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 Configuration (Record)</b>	
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 2.3.12.2, "The "Valid From" and "Valid To" Settings"</a> .
Valid To ?	See <a href="#">Section 2.3.12.2, "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 2.3.12.1, "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 Entry ?	Activates the relay when a valid code is entered. This would likely be used to open a door.
Activate DSR on Valid Entry ?	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 ?	Play a tone when the relay is activated by a security code.
Play Tone on Invalid Code Entry ?	When selected, a tone will play on the speaker to indicate an invalid code was entered.
<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.

Table 2-12. Security Configuration Parameters (continued)

Web Page Item	Description
Repeat SIP Message ?	The number of times to repeat the “blacklist” audio file played during the SIP call. Enter a value between 0 and 65535. 0 will cause the message to play indefinitely, until the call is terminated.
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” audiofile 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.
Security log ?	A file with a maximum of three log files, each 1 MB, that records security actions.
Get Security Log	Downloads a file with a maximum of 3 log files, each 1 M.
Clear Security Log	Clears the on screen display of the log.
Refresh Log	Refreshes the on screen display of the log to show the most recent activity.
Save	Click the <b>Save</b> button to save your configuration settings. <b>Note:</b> You need to reboot for changes to take effect.
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.

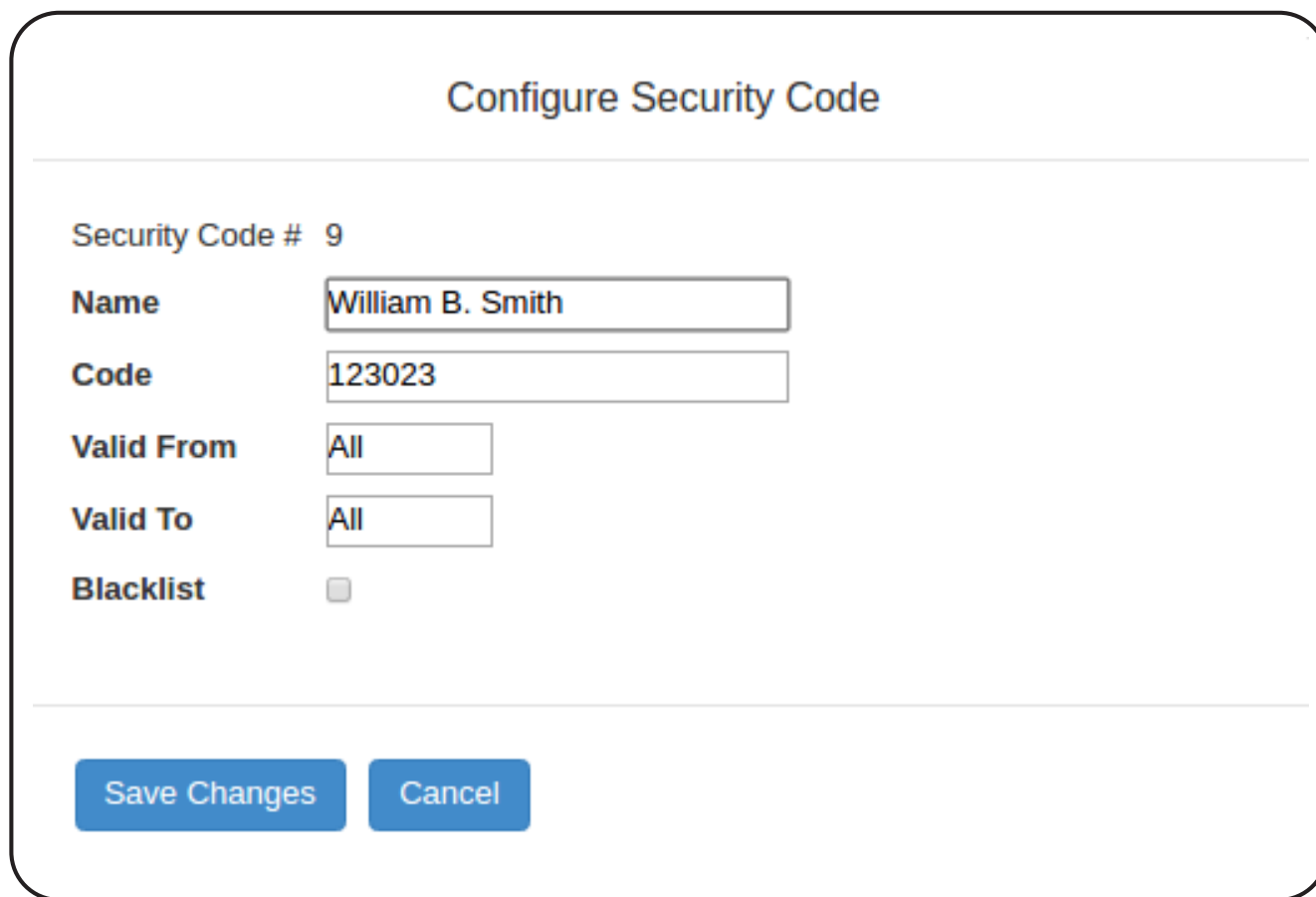
**Note** You must click on the **Save** button and then the **Reboot** button for the changes to take effect.

**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**.

### 2.3.12.1 Configure the Security Code Page

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

**Figure 2-19. 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 2.3.12.2</a> , "The "Valid From" and "Valid To" Settings".
Valid To ?	See <a href="#">Section 2.3.12.2</a> , "The "Valid From" and "Valid To" Settings".
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.

### 2.3.12.2 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, Wnd**, and **Wdy**.

**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**).

## 2.3.13 Configure the Network Parameters

1. Click the **Network** menu button to open the **Network** page (Figure 2-20).

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

Home Device Buttons Security **Network** SIP Multicast Audiofiles Events DSR Autoprov Firmware

# CyberData Handsfree w/Keypad

### Stored Network Settings

Addressing Mode: ☒ Static ☐ DHCP

Hostname:

IP Address:

Subnet Mask:

Default Gateway:

DNS Server 1:

DNS Server 2:

DHCP Timeout in seconds\*:

\* A value of -1 will retry forever

### VLAN Settings

VLAN ID (0-4095):

VLAN Priority (0-7):

### Current Network Settings

IP Address: 10.10.0.116

Subnet Mask: 255.0.0.0

Default Gateway: 10.0.0.1

DNS Server 1: 10.0.1.56

DNS Server 2:

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




**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 2.3.5.4, "Restoring the Factory Default Settings"</a> for factory default settings. Be sure to click <b>Save</b> and <b>Reboot</b> to store changes when configuring a Static address.
Hostname ?	This is the hostname provided by the DHCP server. See the DHCP/ DNS server documentation for more information. Enter up to 64 characters.
IP Address ?	Enter the Static IPv4 network address in dotted decimal notation.
Subnet Mask ?	Enter the Subnet Mask in dotted decimal notation.
Default Gateway ?	Enter the Default Gateway IPv4 address in dotted decimal notation.
DNS Server 1 ?	Enter the primary DNS Server IPv4 address in dotted decimal notation.
DNS Server 2 ?	Enter the secondary DNS Server IPv4 address in dotted decimal notation.
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. <b>Note:</b> You need to reboot for changes to take effect.
	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** You must click on the **Save** button and then the **Reboot** button for the changes to take effect.

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

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

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

The screenshot displays the SIP Configuration Page within the CyberData Handsfree w/Keypad interface. The page features a navigation bar at the top with tabs for Home, Device, Buttons, Security, Network, SIP (selected), Multicast, Audiofiles, Events, DSR, Autopro, and Firmware. The main title is "CyberData Handsfree w/Keypad".

**SIP Settings**

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

**Nightringer Settings**

- Enable Nightringer: ☐
- SIP Server: 10.0.0.253
- Remote SIP Port: 5060
- Local SIP Port: 5061
- Outbound Proxy:
- Outbound Proxy Port: 0
- User ID: 241
- Authenticate ID: 241
- Authenticate Password: \*\*\*\*\*
- Re-registration Interval (in seconds): 360

**RTP Settings**

- RTP Port (even): 10500

**Jitter Buffer**

- Jitter Buffer: 50

**Call Disconnection**

- Terminate Call after delay: 0

**Codec Selection**

- Force Selected Codec: ☐
- Codec: PCMU (G.711, u-law)

Buttons: Save, Reboot, Toggle Help

- 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 2.3.14.1, "Point-to-Point Configuration"</a> ).
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.
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.
Backup SIP Server 1 ?	Enter the backup SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the backup SIP server. This field can accept entries of up to 255 characters in length.
Backup SIP User ID 1 ?	Specify the SIP User ID for the first backup SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the first backup SIP server. Enter up to 64 alphanumeric characters.
Backup SIP Auth ID 1 ?	Specify the Authenticate ID for the first backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Auth Password 1 ?	Specify the Authenticate Password for the first backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Server 2 ?	Enter a second backup SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the second backup SIP server. This field can accept entries of up to 255 characters in length.
Backup SIP User ID 2 ?	Specify the SIP User ID for the second backup SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the second backup SIP server. Enter up to 64 alphanumeric characters.
Backup SIP Auth ID 2 ?	Specify the Authenticate ID for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.

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

Web Page Item	Description
Backup SIP Auth Password 2 ?	Specify the Authenticate Password for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Remote SIP Port ?	The Remote SIP Port is the port number the device will use as the destination port when sending SIP messages. The default Remote SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
Local SIP Port ?	The Local SIP Port is the port number the device will use to receive SIP messages. The default Local SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
Outbound Proxy ?	Enter the Outbound Proxy address as an IPv4 address in dotted decimal notation or a fully qualified domain name (FQDN). When an IP address is configured, the device will send all SIP messages to this IP address. When an FQDN is configured, the device will run DNS NAPTR, SRV, and A queries on the FQDN to resolve an IP address to which it will send all SIP messages. This field can accept entries of up to 255 characters in length.
Outbound Proxy Port ?	The Outbound Proxy Port is port number used as the destination port when sending SIP messages to the outbound proxy. A value of 0 will default to 5060. The supported range is 0-65536. Enter up to 5 digits.
Disable rport Discovery ?	Disabling rport Discovery will prevent the device from including the public WAN IP address and port number in the contact information that is sent to the remote SIP servers. This will generally only need to be enabled when using an SBC or SIP ALG in conjunction with a remote SIP server.
Re-registration Interval (in seconds) ?	The SIP Re-registration interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
Unregister on Boot ?	When enabled, the device will send one registration with an expiry of 0 on boot.
Keep Alive Period ?	The minimum time in milliseconds between keep-alive packets sent for nat traversal. A value of 0 will disable keep alive packets.
<b>Nightringer Settings</b>	
Enable Nightringer ?	When Nightringer is enabled, the device will attempt to register a second extension with the SIP server. Any calls made to this extension will play a ringtone (corresponds to <b>Night Ring</b> on the <b>Audiofiles</b> page). By design, it is not possible to answer a call to the Nightringer extension.
SIP Server ?	Enter the SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's Nightringer extension on the SIP server. This field can accept entries of up to 255 characters in length.
Remote SIP Port ?	The Remote SIP Port is the port number the device will use as the destination port when sending SIP messages for the Nightringer extension. The default Remote SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
Local SIP Port ?	The Local SIP Port is the port number the device will use to receive SIP messages for the Nightringer extension. This value cannot be the same as the <b>Local SIP Port</b> for the primary extension. The default Local SIP Port is 5061. The supported range is 0-65536. Enter up to 5 digits.

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

Web Page Item	Description
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 for the Nightringer extension. 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 for the Nightringer extension. 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 for the Nightringer extension. A value of 0 will default to 5060. The supported range is 0-65536. Enter up to 5 digits.
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.
Authenticate ID ?	Specify the Authenticate ID for the SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Authenticate 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>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.
<b>Jitter Buffer</b>	
Jitter Buffer ?	Specify the size of the jitter buffer (in milliseconds) used for SIP calls. Valid values are 50-1000.
<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>Note:</b> This setting does not require a reboot for the changes to take effect.
<b>Codec Selection</b>	
Force Selected Codec ?	When configured, this option will allow you to force the device to negotiate for the selected codec. Otherwise, the device will perform codec negotiation using the default list of supported codecs.
Codec ?	Select the desired codec (only one may be chosen).
<b>Save</b>	Click the <b>Save</b> button to save your configuration settings.  <b>Note:</b> You need to reboot for changes to take effect.
<b>Reboot</b>	Click on the <b>Reboot</b> button to reboot the system.
<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.

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

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

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

### 2.3.14.1 Point-to-Point Configuration

When the device is set to not register with a SIP server (see [Figure 2-22](#)), 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.

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

**Figure 2-22. SIP Page Set to Point-to-Point Mode**

The screenshot shows the 'SIP' configuration page for a CyberData Handsfree w/Keypad device. The top navigation bar includes tabs for Home, Device, Buttons, Security, Network, SIP (selected), Multicast, Audiofiles, Events, DSR, Autopro, and Firmware. The main heading is 'CyberData Handsfree w/Keypad'.

**SIP Settings**

- Enable SIP operation: ☒
- Register with a SIP Server: ☐ (indicated by a red vertical line)
- Use Cisco SRST: ☐
- Primary SIP Server: 0.0.0.253
- Primary SIP User ID: 99
- Primary SIP Auth ID: 99
- Primary SIP Auth Password: \*\*\*\*\*
- Backup SIP Server 1:
- Backup SIP User ID 1:
- Backup SIP Auth ID 1:
- Backup SIP Auth Password 1:

**Nightringer Settings**

- Enable Nightringer: ☐
- SIP Server: 10.0.0.253
- Remote SIP Port: 5060
- Local SIP Port: 5061
- Outbound Proxy:
- Outbound Proxy Port: 0
- User ID: 241
- Authenticate ID: 241
- Authenticate Password: \*\*\*\*\*
- Re-registration Interval (in seconds): 360

Device is set to NOT register with a SIP server

---

## 2.3.15 Configure the Multicast Parameters

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

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

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



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

**Figure 2-23. Multicast Page**

Home
Device
Buttons
Security
Network
SIP
Multicast
Audiofiles
Events
DSR
Autoprov
Firmware

# CyberData Handsfree w/Keypad

## Multicast Settings

Enable Multicast Operation: ☐

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

Polycom Default Channel
24
Polycom Priority Channel
24
Polycom Emergency Channel
25

SIP calls are considered priority 4.5

Port range can be from 2000-65535

Priority 9 is the highest and 0 is the lowest

A higher priority audio stream will always supersede a lower one

Priority 9 streams will play at maximum volume




\* You need to reboot for changes to take effect

Save
Reboot

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

**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. 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 2.3.15.1, "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.  <b>Note:</b> You need to reboot for changes to take effect.
	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** You must click on the **Save** button and then the **Reboot** button for the changes to take effect.

### 2.3.15.1 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

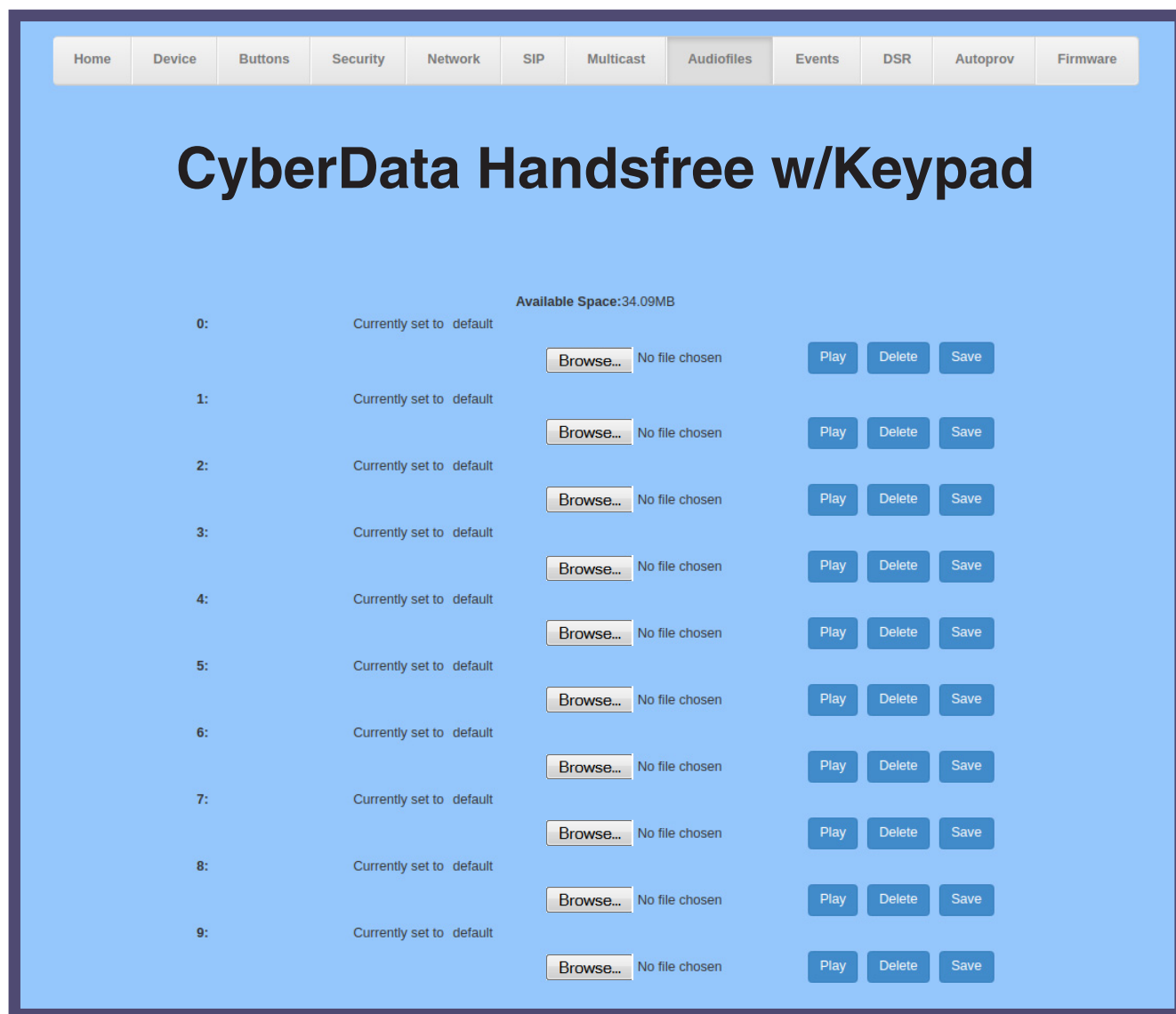
Ringtones all play at the same priority level. This means that it is possible to have a nightring tone and a normal ringtone playing at the same time.

## 2.3.16 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 device.

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

**Figure 2-24. Audiofiles Page**



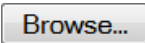


**Figure 2-25. Audiofiles Page**

<b>Dot:</b>	Currently set to default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
<b>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>SIP Multicast Message:</b>	Currently set to explosion.wav	<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 2-17](#).

**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. 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	<p>The name of the audio configuration option is the same as the spoken audio that plays on the board (24 character limit).</p> <p>'0' corresponds to the spoken word "zero."</p> <p>'1' corresponds to the spoken word "one."</p> <p>'2' corresponds to the spoken word "two."</p> <p>'3' corresponds to the spoken word "three."</p> <p>'4' corresponds to the spoken word "four."</p> <p>'5' corresponds to the spoken word "five."</p> <p>'6' corresponds to the spoken word "six."</p> <p>'7' corresponds to the spoken word "seven."</p> <p>'8' corresponds to the spoken word "eight."</p> <p>'9' corresponds to the spoken word "nine."</p>
Dot	Corresponds to the spoken word "dot." (24 character limit)
Audiotest	Corresponds to the message <b><i>"This is the CyberData IP speaker test message..."</i></b> (24 character limit)
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).
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.
	The <b>Delete</b> button will delete any user uploaded audio and restore the stock audio file.

**Table 2-17. Audiofiles Configuration Parameters (continued)**

Web Page Item	Description
	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.

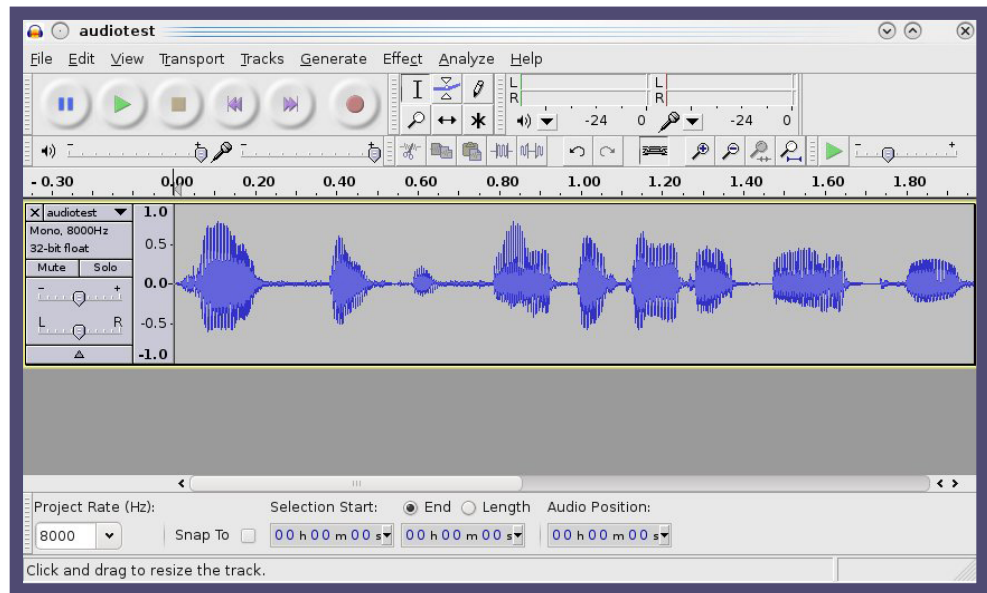
### 2.3.16.1 User-created Audio Files

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

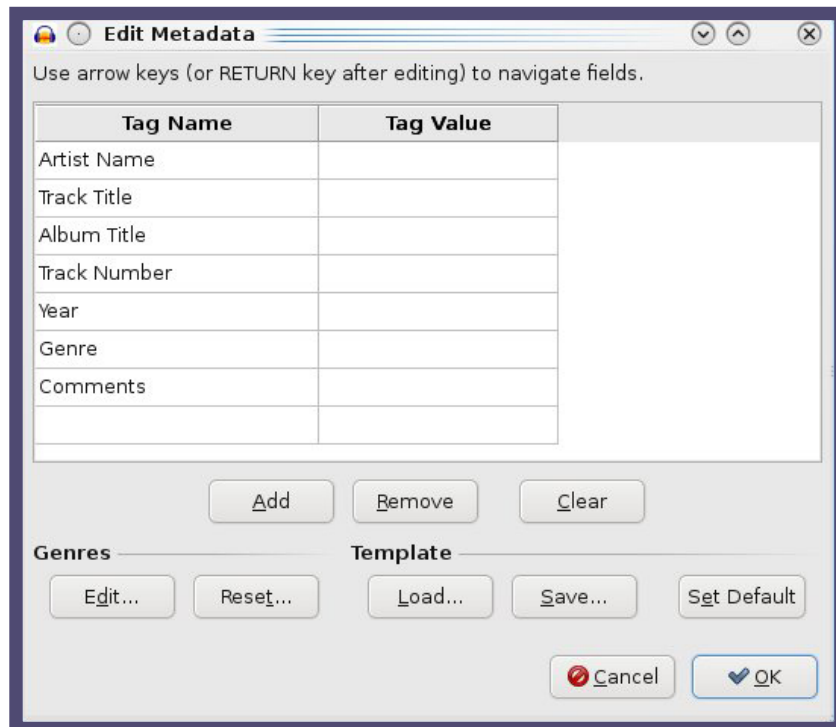
RIFF (little-endian) data, WAVE audio, Microsoft PCM, 16 bit, mono 8000 Hz

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

**Figure 2-26. Audacity 1**



**Figure 2-27. Audacity 2**

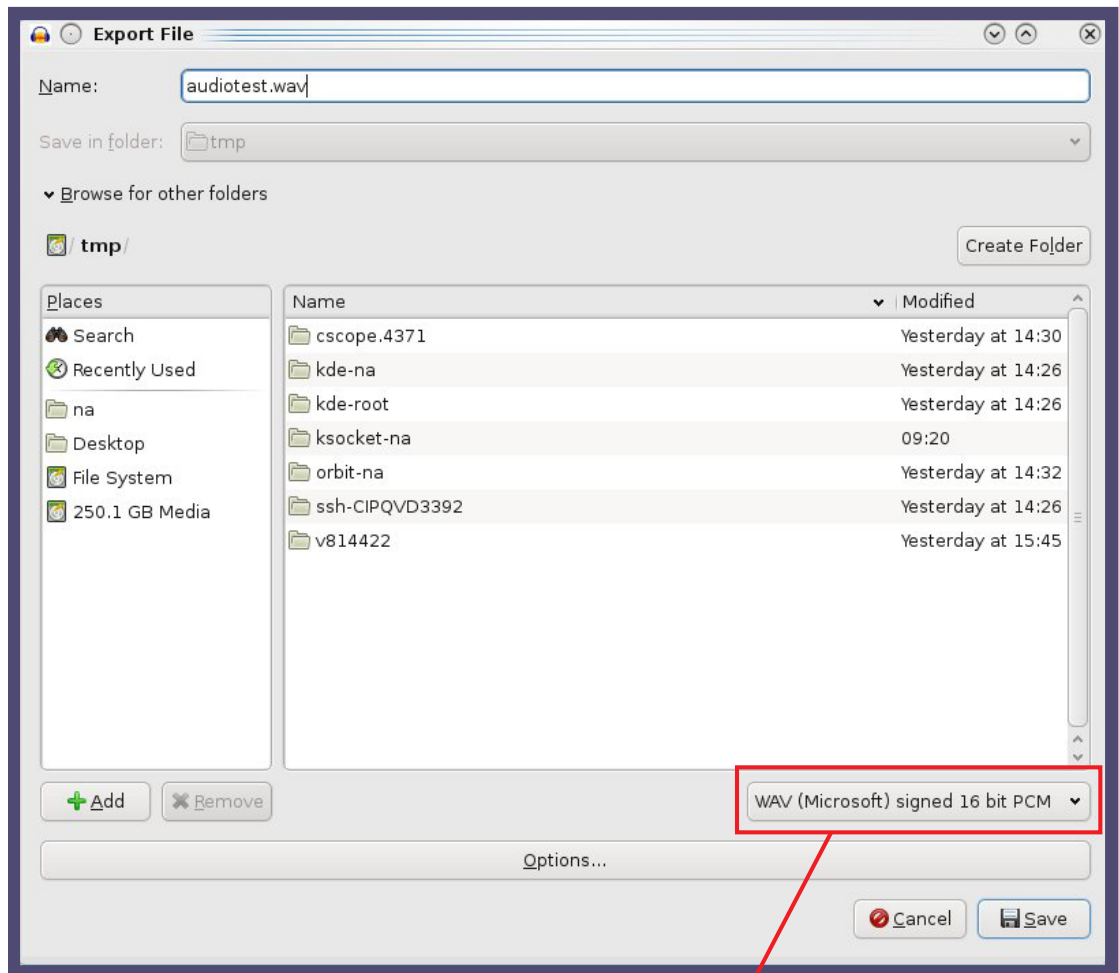




When you export an audio file with Audacity, save the output as:

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

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



WAV (Microsoft) signed 16 bit PCM

## 2.3.17 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 2-29).

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

Home Device Buttons Security Network SIP Multicast Audiofiles **Events** DSR Autopro Firmware

# CyberData Handsfree w/Keypad

Enable Event Generation: ☐

### Events

- Enable Button Events: ☐
- Enable Call Start Events: ☐
- Enable Call Terminated Events: ☐
- Enable Relay Activated Events: ☐
- Enable Relay Deactivated Events: ☐
- Enable Ring Events: ☐
- Enable Night Ring Events: ☐
- Enable Multicast Start Events: ☐
- Enable Multicast Stop Events: ☐
- Enable Power On Events: ☐
- Enable Remote Relay Events: ☐
- Enable Security Events: ☐
- Enable 60 Second Heartbeat: ☐

### Event Server

Server IP Address: 10.0.0.250

Server Port: 8080

Server URL: xmlparse\_engine

Save Reboot Toggle Help








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

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

**Table 2-18. 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 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 2-18. 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. <b>Note:</b> You need to reboot for changes to take effect.
	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** You must click on the **Save** button for the changes to take effect.

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

### 2.3.17.1 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>
```

## 2.3.18 Configure the Door Strike Relay

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

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

This section describes operations for running firmware version 4.8 or later of the Dual Door Strike Relay. If you have an older version of the firmware, then please contact CyberData Technical Support. The version number appears in the **Discovered Remote Relays** section on the **DSR** page (Figure 2-30).

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

Figure 2-30. DSR Page (not associated with any DSRs)

Home Device Buttons Security Network SIP Multicast Audiofiles Events **DSR** Autoprov Firmware

# CyberData Handsfree w/Keypad

### Remote Relay Settings

Not associated with any DSRs

Save Reboot Toggle Help

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.

### 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

Cache age: 00:03



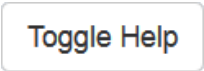




Discover



2. On the **DSR** 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. DSR Configuration Parameters (not associated with any DSRs)**

Web Page Item	Description
<b>Remote Relay Settings</b>	The settings in this section will activate an associated door strike relay. If a door strike relay is not associated with the device, then you will only see the words <b>Not associated with any DSRs</b> .
	Click the <b>Save</b> button to save your configuration settings. <b>Note:</b> You need to reboot for changes to take effect.
	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** You must click on the **Save** button and then the **Reboot** button for the changes to take effect.

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

## 2.3.19 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 2-31](#).

**Figure 2-31. Autoprovisioning Page**

Home Device Buttons Security Network SIP Multicast Audiofiles Events DSR **Autoprov** Firmware

# CyberData Handsfree w/Keypad

Disable Autoprovisioning: ☐

Autoprovisioning Server:

Autoprovisioning Filename:

Use tftp: ☐

Username:

Password:

Autoprovisioning autoupdate (in minutes): 0

Autoprovision at time (HHMMSS):

Autoprovision when idle (in minutes > 10): 0

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 '0020f703b858.xml' and if this fails, '000000cd.xml'.

### Autoprovisioning log

```


31:13 Autoprovisioning Device...
31:13 Autoprov found option 43 in DHCP server="10.0.0.242"
31:13 Autoprov looking for 0020f703b858.xml at 10.0.0.242
31:13 Autoprov: didn't find autoprov file
31:13 Autoprov looking for 000000cd.xml at 10.0.0.242
31:13 Autoprov: didn't find autoprov file
31:13 Failed to fetch autoprov file
31:13 Autoprov found option 72 in DHCP server="10.0.0.242"
31:13 Autoprov looking for 0020f703b858.xml at 10.0.0.242
31:13 Autoprov: didn't find autoprov file
31:13 Autoprov looking for 000000cd.xml at 10.0.0.242
31:13 Autoprov: didn't find autoprov file

```


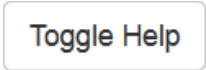

2. On the **Autoprovisioning** page, you may enter values for the parameters indicated in [Table 2-20](#).

**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. Autoprovisioning Configuration Parameters**

Web Page Item	Description
Disable Autoprovisioning ?	Prevent the device from automatically trying to download a configuration file. See <a href="#">Section 2.3.19.1, "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.
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) ?	<p>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.</p> <p><b>Note:</b> To use the auto update options, enable the <a href="#">Set Time with NTP Server on boot</a> setting on the <a href="#">Device Configuration Page</a> (see <a href="#">Table 2-5</a>).</p>
Autoprovision at time (HHMMSS) ?	<p>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.</p> <p><b>Note:</b> To use the auto update options, enable the <a href="#">Set Time with NTP Server on boot</a> setting on the <a href="#">Device Configuration Page</a> (see <a href="#">Table 2-5</a>).</p>
Autoprovision when idle (in minutes > 10) ?	<p>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.</p> <p><b>Note:</b> To use the auto update options, enable the <a href="#">Set Time with NTP Server on boot</a> setting on the <a href="#">Device Configuration Page</a> (see <a href="#">Table 2-5</a>).</p>
	<p>Click the <b>Save</b> button to save your configuration settings.</p> <p><b>Note:</b> You need to reboot for changes to take effect.</p>

**Table 2-20. Autoprovisioning Configuration Parameters (continued)**

Web Page Item	Description
	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 2.3.19.3, "Download Template Button"</a>
Autoprovisioning log	The autoprovisioning log provides information about the latest autoprovisioning attempt (i.e. dhcp options and server accessed and files parsed or not found).

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

### 2.3.19.1 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 2.3.19.2, "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 2-20](#)). This file contains every configuration option that can be set on the board.

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

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

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

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

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

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

The file 0020f7123456.xml contains:

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

1. The device will first set it's name to 'Newname'.
2. It will try to download <http://example.com/common.xml>.
3. It will try to download [http://example.com/sip\\_reg0020f7123456.xml](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 2-21. Autoprovisioning File Name**

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

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

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

For example:

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

The autoprovisioning filename is set to “cyberdata/”

On boot, the device will try to download:

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

...and if this fails:

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

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



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

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

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

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

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

The list of valid product strings:

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

Autoprovisioning  
Example 1

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

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

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

```
000000cd.xml
```

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

```
sip_common.xml
```

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

```
sip_0020f7020001.xml
```

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

```
sip_0020f7020002.xml
```

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

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

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

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

## 2.3.19.2 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; }

```

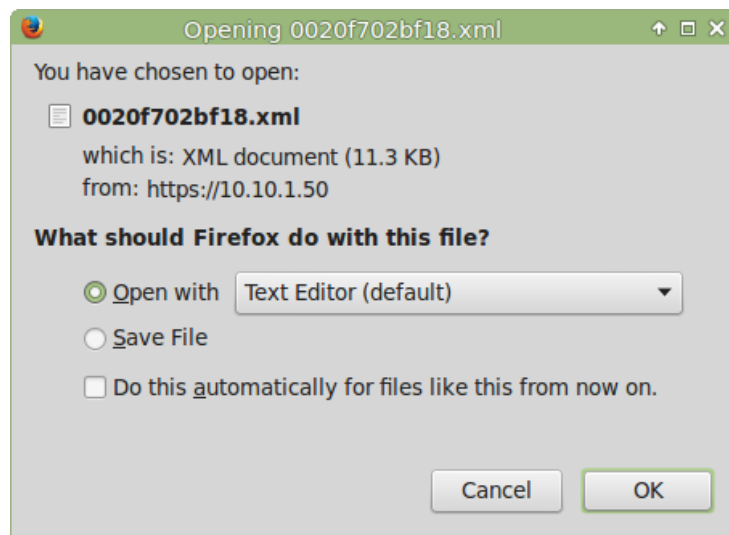
### 2.3.19.3 Download Template Button

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 2-32). 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 2-32.

**Figure 2-32. 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.

---

## 2.4 Upgrade the Firmware and Reboot the SIP Heavy Duty Emergency Keypad Call Station



GENERAL ALERT

### Caution

**Equipment Hazard:** Devices with a serial number that begins with 460xxxxxx can only run firmware versions 10.0.0 or later.

---

### 2.4.1 Downloading the Firmware

To download the firmware to your computer:

1. Download the latest firmware file from the **Downloads** tab at the following webpage:  
<http://www.cyberdata.net/voip/011463/>
2. Unzip the firmware version file. This file may contain the following:
  - Firmware file
  - Release notes
3. Log in to the SIP Heavy Duty Emergency Keypad Call Station home page as instructed in [Section 2.3.9, "Log in to the Configuration Home Page"](#).
4. Click on the **Firmware** menu button to open the **Firmware** page. See [Figure 2-33](#).

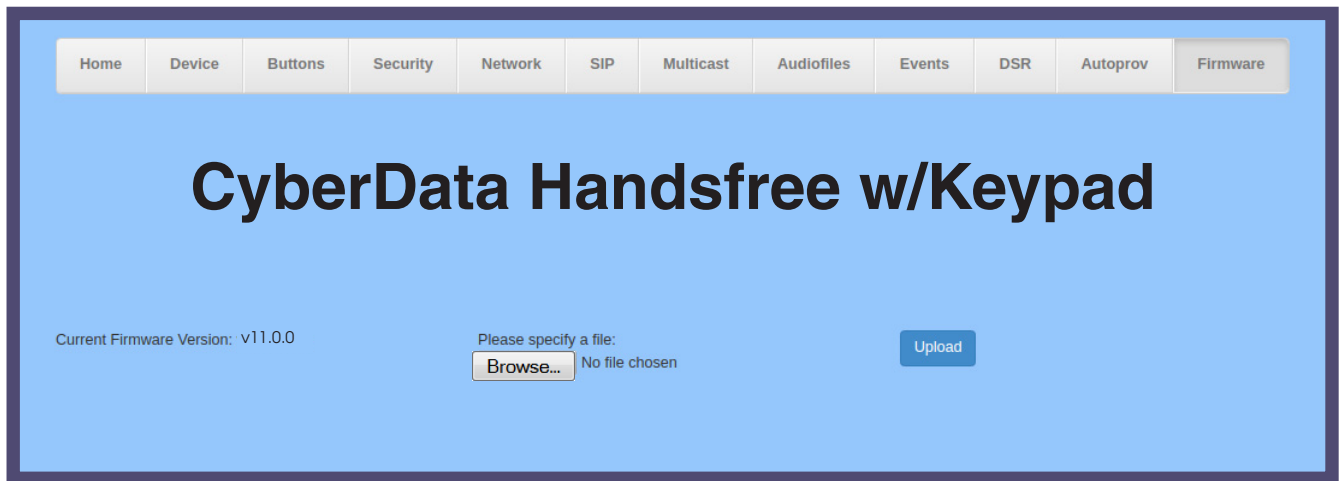


GENERAL ALERT

### Caution

**Equipment Hazard:** CyberData strongly recommends that you first reboot the device before attempting to upgrade the firmware of the device. See [Section 2.4.2, "Reboot the Device"](#).


**Figure 2-33. Firmware Page**



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

**Note** Do not reboot the device after clicking on the **Upload** button.

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





GENERAL ALERT

**Caution**

**Equipment Hazard:** Restore the factory defaults after upgrading the firmware. See [Section 2.4.2, "Reboot the Device"](#).

8. [Table 2-22](#) shows the web page items on the **Firmware** page.

**Table 2-22. Firmware Parameters**

Web Page Item	Description
Current Firmware Version	Shows the current firmware version.
	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.



## 2.4.2 Reboot the Device

To reboot a SIP Heavy Duty Emergency Keypad Call Station, log in to the web page as instructed in [Section 2.3.9, "Log in to the Configuration Home Page"](#).

1. Click on the **Reboot** button on the **Home** page ([Figure 2-34](#)). A normal restart will occur.

**Figure 2-34. Home Page**

**CyberData Handsfree w/Keypad**

**Current Status**

Serial Number: 463100001  
 Mac Address: 00:20:f7:03:b8:58  
 Firmware Version: v11.0.0

IP Addressing: DHCP  
 IP Address: 10.10.0.116  
 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  
 Push to Talk Volume: 4  
 Volume Boost: Off  
 Microphone Gain: 4  
 Push to Talk Microphone Gain: 4

SIP Mode: Enabled  
 Event Reporting: Disabled  
 Nightringer: Disabled

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

**Admin Settings**

Username: admin  
 Password:  
 Confirm Password:

Save Reboot Toggle Help

**Import Settings**

Choose File No file chosen  
 Import Config

**Export Settings**

Export Config

**Reboot button**

## 2.5 Command Interface

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

### 2.5.1 Command Interface Post Commands

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

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

Device Action	HTTP Post Command <sup>a</sup>
Trigger relay (for configured delay)	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/command.cgi" --post-data "test_relay=yes"
Place call to extension (example: extension 130)	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/command.cgi" --post-data "call=130"
Place point-to-point call <sup>b</sup> (example: IP phone address = 10.0.3.72)	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/command.cgi" --post-data "call=10.0.3.72"
Terminate active call	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/command.cgi" --post-data "terminate=yes"
Force reboot	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/command.cgi" --post-data "reboot=yes"
Test Audio button	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/command.cgi" --post-data "test_audio=yes"
Announce IP address	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/command.cgi" --post-data "speak_ip_address=yes"
Play the "0" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_0=yes"
Play the "1" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_1=yes"
Play the "2" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_2=yes"
Play the "3" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_3=yes"

**Table 2-23. Command Interface Post Commands (continued)**

<b>Device Action</b>	<b>HTTP Post Command<sup>a</sup></b>
Play the "4" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_4=yes"
Play the "5" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_5=yes"
Play the "6" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_6=yes"
Play the "7" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_7=yes"
Play the "8" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_8=yes"
Play the "9" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_9=yes"
Play the "Dot" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_d=yes"
Play the "Audio Test" audio file (from Audio Config)	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_audiotest=yes"
Play the "Page Tone" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_pagetone=yes"
Play the "Your IP Address Is" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_youripaddressis=yes"
Play the "Rebooting" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_rebooting=yes"
Play the "Restoring Default" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_restoringdefault=yes"
Play the "Ringback tone" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_ringback=yes"
Play the "Ring tone" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_ringtones=yes"
Play the "Intrusion Sensor Triggered" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_intrusionsensortriggered=yes"
Play the "Door Ajar" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_doorajar=yes"

**Table 2-23. Command Interface Post Commands (continued)**

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

**Table 2-23. Command Interface Post Commands (continued)**

Device Action	HTTP Post Command <sup>a</sup>
Delete the "Ringback tone" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_ringback=yes"
Delete the "Ring tone" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_ringtones=yes"
Delete the "Intrusion Sensor Triggered" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_intrusionsensortriggered=yes"
Delete the "Door Ajar" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_doorajar=yes"
Delete the "Night Ring" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_nightring=yes"
Trigger the Door Sensor Test (Sensor Config page)	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/sensor.cgi" --post-data "doortest=yes"
Trigger the Intrusion Sensor Test (Sensor Config page)	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/sensor.cgi" --post-data "intrusiontest=yes"

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

b. Must be in point-to-point mode see [Section 2.3.14.1, "Point-to-Point Configuration"](#)

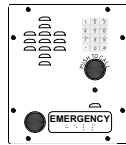
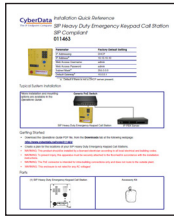
# Appendix A: Mounting the SIP Heavy Duty Emergency Keypad Call Station 91

## A.1 Parts List

Table A-1 illustrates the SIP Heavy Duty Emergency Keypad Call Station parts.

**Note** See Appendix , "Mounting the SIP Heavy Duty Emergency Keypad Call Station for physical mounting information.

Table A-1. Parts List

Quantity	Part Name	Illustration
1	SIP Heavy Duty Emergency Keypad Call Station Assembly	
1	Installation Quick Reference Guide	

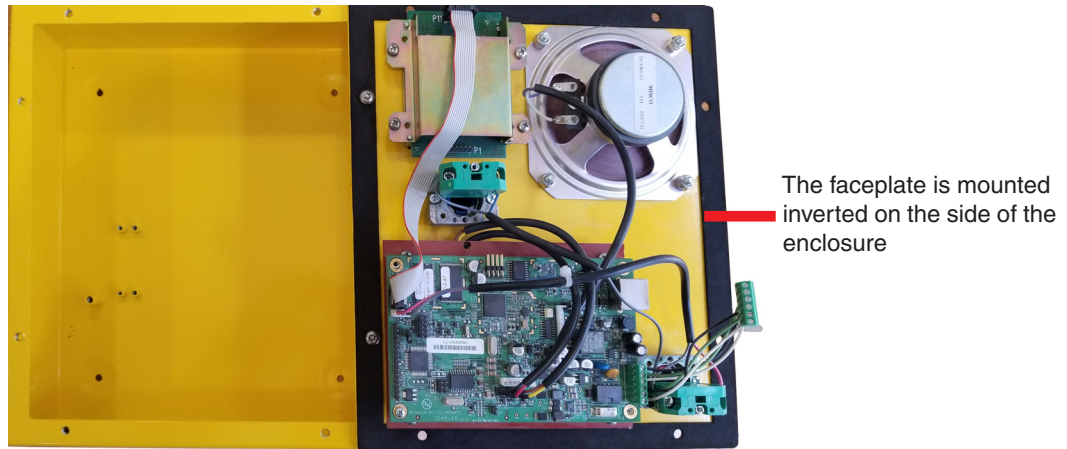
## A.2 Installation

**Follow all appropriate electrical codes and use only approved electrical fittings for the installation. If 120VAC power is provided to the Auxiliary Relay the enclosure must be properly grounded to the surge arrestor.**

1. Ensure that none of the electrical connection circuits are live.
2. No other telephones may be installed on the HDE extension.
3. Remove the cover screws from the front of the unit and carefully remove the front cover assembly. Note that the electronics are attached to the front plate.

**Note** Verify regulatory requirements before installing on public network.

4. If an additional cable entrance is required punch a hole in the enclosure in a convenient location. Ensure that the fittings and wiring will not interfere with the circuit board when the faceplate is replaced.
5. Choose a wall location that is free of obstructions and permits space for cable or conduit runs. See the mounting template on the last page of this placemat.
6. Ensure mounting can support 7 lbs (3 kg) and any additional foreseeable load.
7. Use the template provided or the enclosure itself to locate and drill holes for #8 or M4 mounting screws.
8. Secure the unit to the wall or desired installation location.
9. For convenience, while connecting wiring, the faceplate may be temporarily mounted inverted to either side of the enclosure. See the following figure:

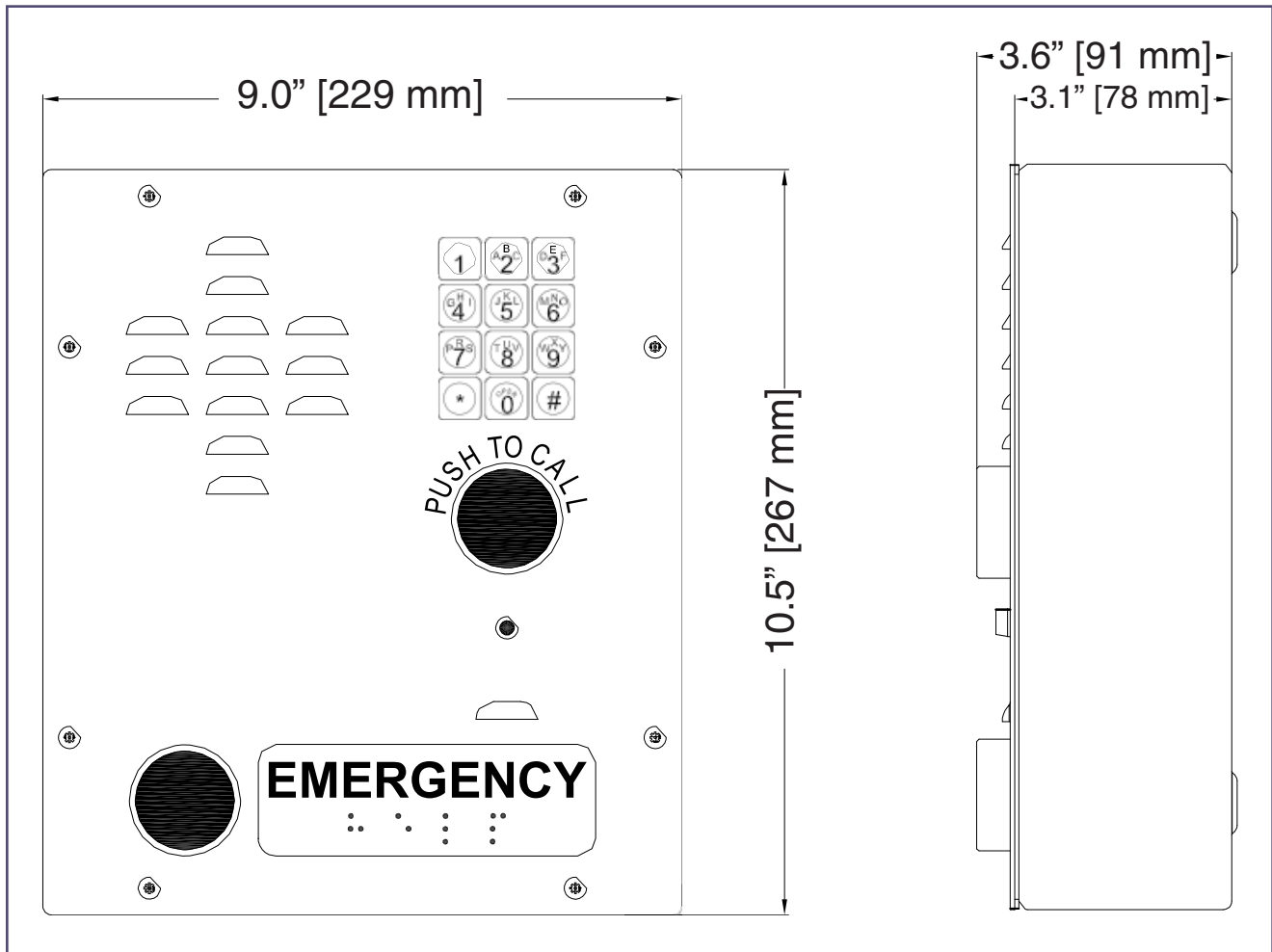


### Commissioning

1. Ensure all connections are tight, then replace and secure the cover. Use the driver bit provided to install the tamper resistant screws. Store the driver bit in a secure place for future use.
2. Connect the telephone into the system.
3. Test the unit by calling to and from another telephone.

## A.3 Dimensions

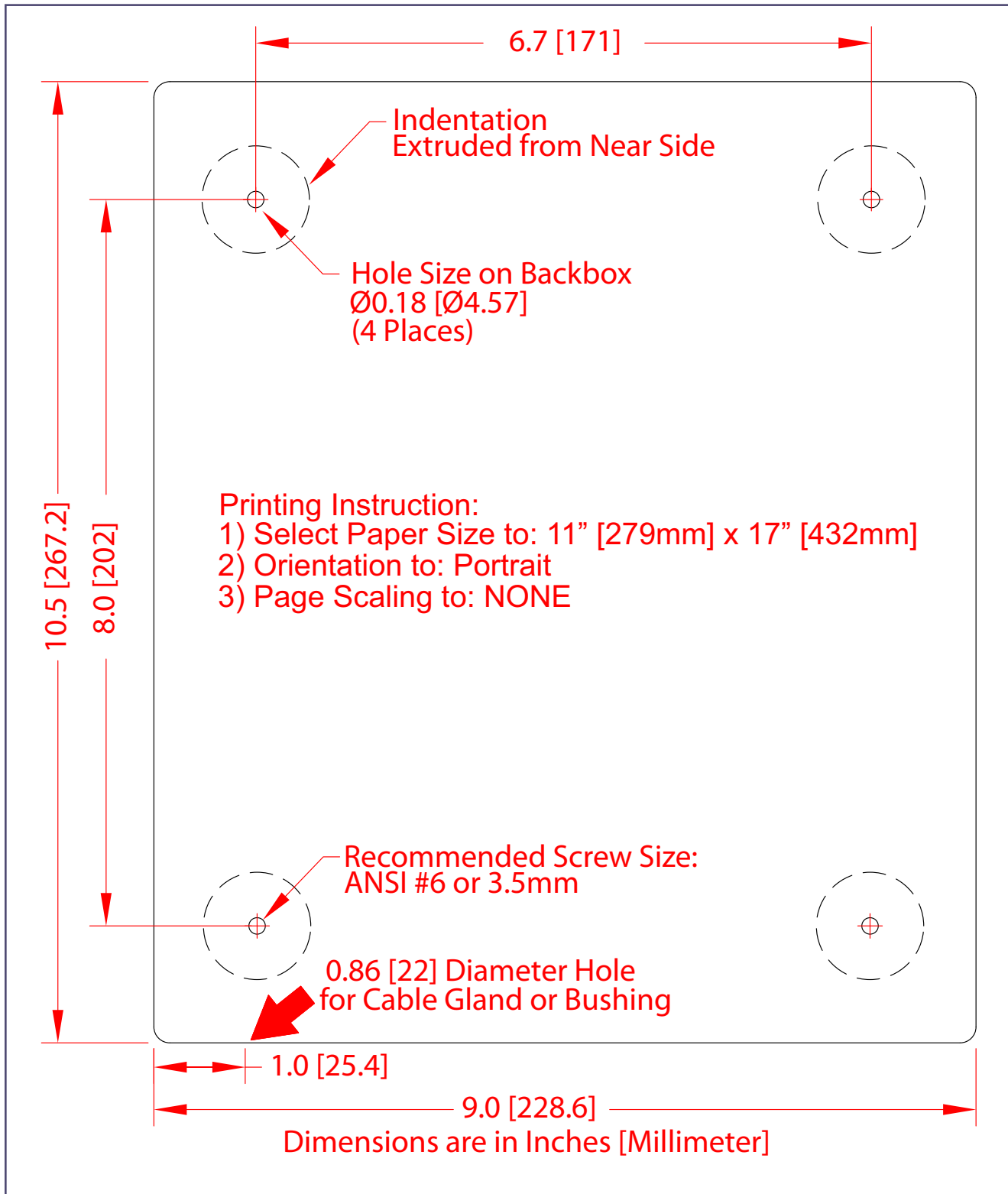
Figure A-1. Dimensions





## A.4 Mounting

Figure A-2. Mounting—Rear View



# Appendix B: Setting up a TFTP Server

---

## B.1 Set up a TFTP Server

Autoprovisioning requires a TFTP server for hosting the configuration file.

---

### B.1.1 In a LINUX Environment

To set up a TFTP server on LINUX:

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

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

---

### B.1.2 In a Windows Environment

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

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

To set up a TFTP server on Windows:

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

# Appendix C: Troubleshooting/Technical Support

---

## C.1 Frequently Asked Questions (FAQ)

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

<http://www.cyberdata.net/voip/011460/>

---

## C.2 Documentation

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

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

<http://www.cyberdata.net/voip/011460/>

---

## 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

---

## A

- activity LED 15
- address, configuration login 23
- alternative power input 5
- audio configuration 57
- audio configuration page 57
- audio encodings 4
- audio files, user-created 61
- autoprovision at time (HHMMSS) 73
- autoprovision when idle (in minutes > 10) 73
- autoprovisioning 74
  - download template button 74
  - setting up a TFTP server 95
- autoprovisioning autoupdate (in minutes) 73
- autoprovisioning configuration 72, 73
- autoprovisioning filename 73
- autoprovisioning server (IP Address) 73
- auxiliary relay wiring diagram 12

## B

- backup SIP server 1 48
- backup SIP server 2 48
- backup SIP servers, SIP server
  - backups 48

## C

- call termination 30
- changing
  - the web access password 27
- Cisco SRST 48
- command interface 87
- commands 87
- configurable parameters 28, 45
- configuration
  - audio 57
  - network 44
  - SIP 47
- configuration home page 23
- configuration page
  - configurable parameters 28, 45
- contact information 97
- contact information for CyberData 97
- current network settings 45
- CyberData contact information 97

## D

- default
  - web login username and password 23
- default gateway 45
- default login address 23
- default settings 18, 98
- device configuration 27
  - device configuration parameters 73
  - the device configuration page 72
- device configuration page 27, 34, 35
- device configuration parameters 28
- device configuration password
  - changing for web configuration access 27
- DHCP Client 4
- dial mode 35
- dial out call 37
- dial out extension strings 37
- dimensions 5, 93
  - unit dimensions—front and side view 93
- discovery utility program 23
- DNS server 45
- door sensor
  - door sensor normally closed 39
- download autoprovisioning template button 74
- DTMF push to talk 30
- DTMF tones (using rfc2833) 37

## E

- enable night ring events 64
- enable security operation 35
- ethernet I/F 5
- event configuration
  - enable night ring events 64
- expiration time for SIP server lease 49, 50
- export settings 25, 26

## F

- factory default settings 18
- firmware
  - where to get the latest firmware 84

## G

get autoprovisioning template 74  
 GMT table 32  
 GMT time 32

## H

home page 23  
 http POST command 87  
 http web-based configuration 4

## I

identifier names (PST, EDT, IST, MUT) 32  
 identifying your product 1  
 import settings 25, 26  
 import/export settings 25, 26  
 installation 2  
 IP address 45

## K

keypad configuration page 34

## L

lease, SIP server expiration time 49, 50  
 LED  
     green link LED 15  
     yellow activity LED 15  
 lengthy pages 56  
 link LED 15  
 Linux, setting up a TFTP server on 95  
 local SIP port 49  
 log in address 23

## M

MGROUP  
     MGROUP Name 55  
 mounting 91  
     overview of installation types 91, 93, 94  
 mounting components 92  
 multicast configuration 57  
 Multicast IP Address 55

## N

navigation (web page) 20  
 navigation table 20  
 network configuration 44  
 nightring tones 56  
 Nightringer 10, 83  
 nightringer settings 49  
 NTP server 28

## O

on-board relay 5, 11  
 overview of installation types 93, 94

## P

packet time 4  
 pages (lengthy) 56  
 part number 5  
 parts list 7, 91  
 password  
     for SIP server login 48  
     login 23  
 payload types 5  
 point-to-point configuration 52  
 polycom default channel 55  
 polycom emergency channel 55  
 polycom priority channel 55  
 port  
     local SIP 49  
     remote SIP 49  
 posix timezone string  
     timezone string 28  
 POST command 87  
 power input 5  
     alternative 5  
 priority  
     assigning 56  
 product features 3  
 product overview  
     product features 3  
     product specifications 5  
     supported protocols 4  
     supported SIP servers 4  
     typical system installation 2  
 product specifications 5  
 protocol 5  
 protocols supported 4  
 push to talk, DTMF 30

## R

- reboot 85, 86
- remote SIP port 49
- resetting the IP address to the default 92, 96
- restoring factory default settings 18, 98
- ringtones 56
  - lengthy pages 56
- rport discovery setting, disabling 49
- RTFM jumper 16, 17, 18
- RTP/AVP 4

## S

- sales 97
- security code 37
- security mode settings 35
- sensor setup page 69
- server address, SIP 48
- service 97
- set time with external NTP server on boot 28
- setting up the device 10
- settings, default 18
- SIP
  - enable SIP operation 48
  - local SIP port 49
  - user ID 48
- SIP configuration 47
- SIP configuration parameters
  - outbound proxy 49, 50
  - registration and expiration, SIP server lease 49, 50
  - unregister on reboot 49
  - user ID, SIP 48
- SIP registration 48
- SIP remote SIP port 49
- SIP server 48
  - password for login 48
  - SIP servers supported 4
  - unregister from 49
  - user ID for login 48
- SIP server configuration 48
- SIP volume 28
- SRST 48
- subnet mask 45
- supported protocols 4

## T

- tech support 97
- technical support, contact information 97
- TFTP server 4, 95
- time zone string examples 32

- triggering a dial out call or security code 37

## U

- unit dimensions—front and side view 93
- user ID
  - for SIP server login 48
- username
  - changing for web configuration access 27
  - default for web configuration access 23

## V

- VLAN ID 45
- VLAN Priority 45
- VLAN tagging support 45
- VLAN tags 45
- volume
  - microphone gain 28
  - multicast volume 28
  - push to talk volume 28
  - ring volume 28
  - SIP volume 28

## W

- warranty policy at CyberData 97
- web configuration log in address 23
- web page
  - navigation 20
- web page navigation 20
- wget, free unix utility 87
- Windows, setting up a TFTP server on 95