

# *SIP Call Button Operations Guide*

Part #011049

Document Part #930801H  
for Firmware Version 11.3.0

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

---

---

**SIP Call Button Operations Guide 930801H**  
**Part # 011049**

**COPYRIGHT NOTICE:**

© 2015, CyberData Corporation, ALL RIGHTS RESERVED.

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

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

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

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

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



**Technical Support**

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

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 930801H, which corresponds to firmware version 11.3.0, was released on April 9, 2015, and has the following changes:

- Updates [Figure 2-2, "Wiring Diagram"](#)
- Updates the following text in [Section 2.2.2, "Using the On-Board Relay"](#):
  - “This relay can be used to trigger low current devices like LED strobes and security camera input signals as long as the load is not an inductive type and the relay is limited to a maximum of 1 Amp @ 30 VDC. Inductive loads can cause excessive “hum” and can interfere with or damage the unit’s electronics.”
- Adds the following text to [Section 2.2.3.1, "Devices Less than 1A at 30 VDC"](#):
  - “When configuring with an inductive load, please use an intermediary relay with a High PIV Ultrafast Switching Diode. We recommend using the CyberData Door Strike Intermediate Relay Module (CD# 011269) (see [Section 2.2.3.2, "Connecting the Door Strike Intermediate Relay Module"](#)).”

---

## Browsers Supported

The following browsers have been tested against firmware version 11.3.0:




- Internet Explorer (version: 10)
- Firefox (also called Mozilla Firefox) (version: 23.0.1 and 25.0)
- Chrome (version: 29.0.1547.66 m)
- Safari (version: 5.1.7)

---

# Important Safety Instructions



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

**14. WARNING: The SIP Call Button enclosure is not rated for any AC voltages!**

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

---

## Pictorial Alert Icons

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

---

## Hazard Levels

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

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

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

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

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

---

# Abbreviations and Terms

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

# Contents

---

|  |           |
|--|-----------|
| <b>Chapter 1 Product Overview</b>                                  | <b>1</b>  |
| 1.1 How to Identify This Product .....                             | 1         |
| 1.2 Typical System Installation .....                              | 2         |
| 1.3 Product Features .....   | 3         |
| 1.4 Supported Protocols .....                                      | 3         |
| 1.5 Supported SIP Servers .....                                    | 4         |
| 1.6 Product Specifications .....                                   | 4         |
| <b>Chapter 2 Installing the SIP Call Button</b>                    | <b>5</b>  |
| 2.1 Parts List .....   | 5         |
| 2.2 SIP Call Button Setup .....                                    | 6         |
| 2.2.1 SIP Call Button Connections .....                            | 6         |
| 2.2.2 Using the On-Board Relay .....                               | 7         |
| 2.2.3 Wiring the Circuit .....                                     | 8         |
| 2.2.4 Identifying the SIP Call Button Connectors and Jumpers ..... | 11        |
| 2.2.5 Activity and Link LEDs .....                                 | 13        |
| 2.2.6 Restore the Factory Default Settings .....                   | 14        |
| 2.2.7 Call Button and the Call Button LED .....                    | 15        |
| 2.3.1 Factory Default Settings .....                               | 16        |
| 2.3.2 SIP Call Button Web Page Navigation .....                    | 17        |
| 2.3.3 Using the Toggle Help Button .....                           | 18        |
| 2.3.4 Log in to the Configuration Home Page .....                  | 20        |
| 2.3.5 Configure the Device .....                                   | 24        |
| 2.3.6 Configure the Network Parameters .....                       | 30        |
| 2.3.7 Configure the SIP Parameters .....                           | 33        |
| 2.3.8 Configure the Sensor Configuration Parameters .....          | 40        |
| 2.3.9 Configure the Audio Configuration Parameters .....           | 44        |
| 2.3.10 Configure the Event Parameters .....                        | 48        |
| 2.3.11 Configure the Door Strike Relay .....                       | 53        |
| 2.3.12 Configure the Device (on the DSR page) .....                | 57        |
| 2.3.13 Configure the Autoprovisioning Parameters .....             | 60        |
| 2.4.1 Reboot the Device .....                                      | 74        |
| 2.5.1 Command Interface Post Commands .....                        | 75        |
| <b>Appendix A Mounting the SIP Call Button</b>                     | <b>1</b>  |
| A.1 Mount the SIP Call Button .....                                | 1         |
| <b>Appendix B Troubleshooting/Technical Support</b>                | <b>6</b>  |
| B.1 Frequently Asked Questions (FAQ) .....                         | 6         |
| B.2 Documentation .....  | 6         |
| B.3 Contact Information .....                                      | 7         |
| B.4 Warranty .....   | 8         |
| B.4.1 Warranty & RMA Returns within the United States .....        | 8         |
| B.4.2 Warranty & RMA Returns outside of the United States .....    | 9         |
| B.4.3 Spare in the Air Policy .....                                | 9         |
| B.4.4 Return and Restocking Policy .....                           | 9         |
| B.4.5 Warranty and RMA Returns Page .....                          | 9         |
| <b>Index</b>   | <b>10</b> |

# 1 Product Overview

## 1.1 How to Identify This Product

To identify the SIP Call Button, 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 **011049**.
- The serial number on the label should begin with **0491**.

Figure 1-1. Model Number Label



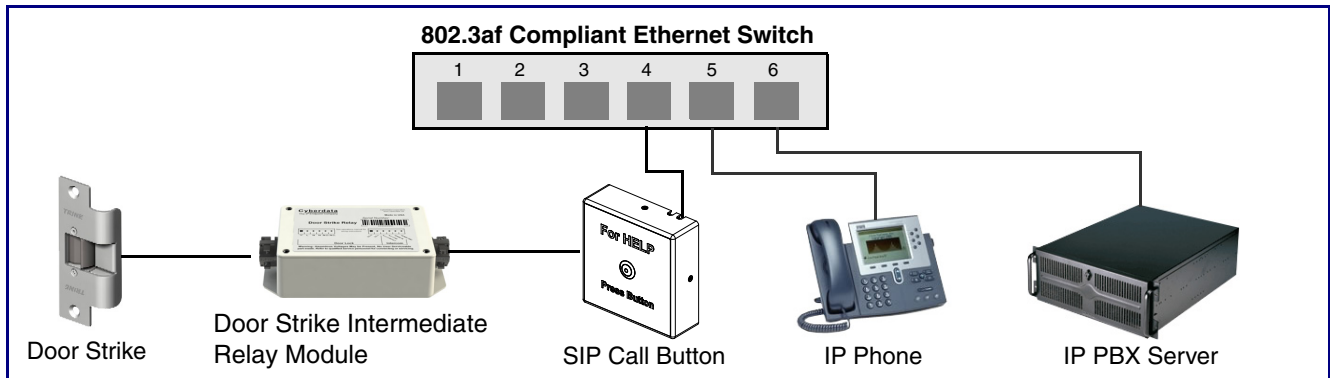


## 1.2 Typical System Installation

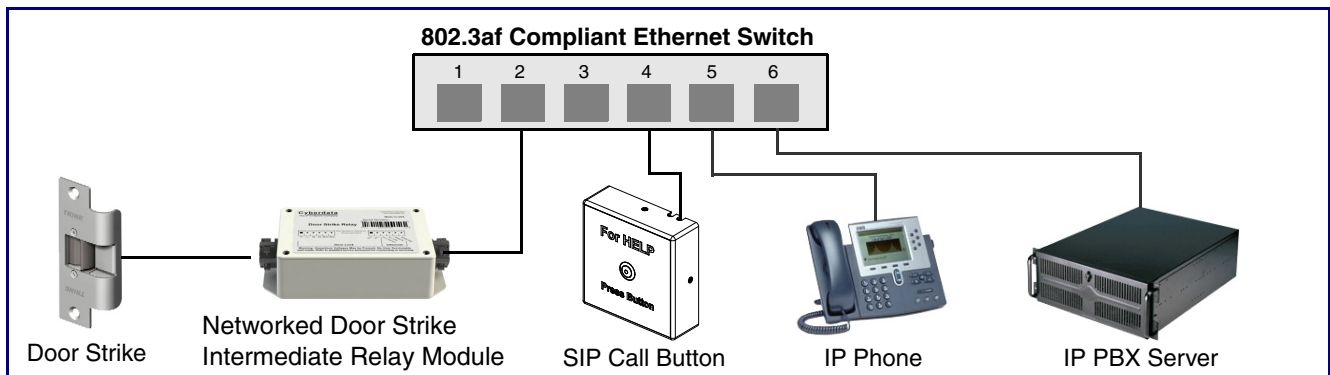
The Session Initiation Protocol (SIP) SIP Call Button is a SIP endpoint designed to provide VoIP phone connectivity in a tamper proof and secure package.

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

**Figure 1-2. Typical Installation—Door Strike Intermediate Relay Module**



**Figure 1-3. Typical Installation—Networked Door Strike Intermediate Relay Module**



---

## 1.3 Product Features

- SIP
- User downloadable message up to 80 seconds
- Single button call to pre-set number
- Continuous repeat of message
- Call progress light
- Event-controlled relay
- Tamper sensor
- Web-based setup
- PoE-powered

---

## 1.4 Supported Protocols

The SIP Call Button supports:

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

---

## 1.5 Supported SIP Servers

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

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

---




## 1.6 Product Specifications

| Category          | Specification   |
|-------------------|---|
| Network Rate      | 10/100 Mbps   |
| Power Requirement | PoE 802.3af or 8 to 12 VDC at 1000 mA                                     |
| Protocol          | SIP   |
| Part Number       | 011049  |
| Dimensions        | 4.5" x 4.5" x 1.5"  |
| Weight            | 1.6 lbs./shipping weight of 2.2 lbs.<br>(0.7 kg/shipping weight of 1.0kg) |
| Auxiliary Relay   | 1A at 30 VDC  |

# 2 Installing the SIP Call Button

## 2.1 Parts List

Table 2-1 illustrates the SIP Call Button parts.


| Table 2-1. Parts List |  |   |
|-----------------------|--|---|
| Quantity              | Part Name                              | Illustration  |
| 1                     | SIP Call Button Assembly               |    |
| 1                     | Installation Quick Reference Guide     |    |
| 1                     | SIP Call Button Mounting Accessory Kit |  |

## 2.2 SIP Call Button Setup

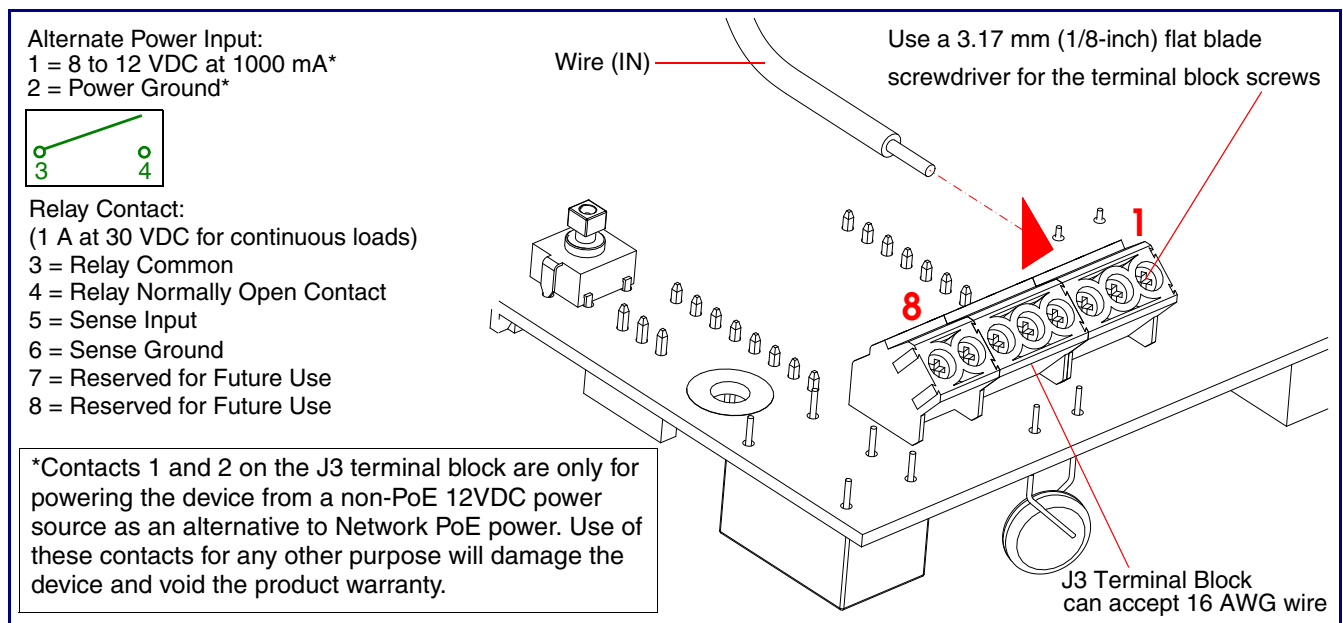
### 2.2.1 SIP Call Button Connections

**Figure 2-1** shows the pin connections on the J3 (terminal block). This terminal block can accept 16 AWG gauge wire.




**Note** As an alternative to using PoE power, you can supply 8 to 12 VDC at 1000 mA into the terminal block.

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

**Figure 2-1. Connections**



## 2.2.2 Using the On-Board Relay

|  |  |
|--|--|
| <br>GENERAL ALERT | <p><b>Warning</b></p> <p><i>Electrical Hazard:</i> This product should be installed by a licensed electrician according to all local electrical and building codes.</p>  |
| <br>GENERAL ALERT | <p><b>Warning</b></p> <p><i>Electrical Hazard:</i> The relay contacts are dry and provided for a normally open and momentarily closed configuration. Neither the alternate power input nor PoE power can be used to drive a door strike.</p>     |
| <br>GENERAL ALERT | <p><b>Warning</b></p> <p><i>Electrical Hazard:</i> The relay does not support AC powered door strikes. Any use of this relay beyond its normal operating range can cause damage to the product and is not covered under our warranty policy.</p> |

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

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

We highly recommend that inductive load and high current devices use our Door Strike Intermediate Relay product (CD# 011269) (see [Section 2.2.3.2, "Connecting the Door Strike Intermediate Relay Module"](#)).

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

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

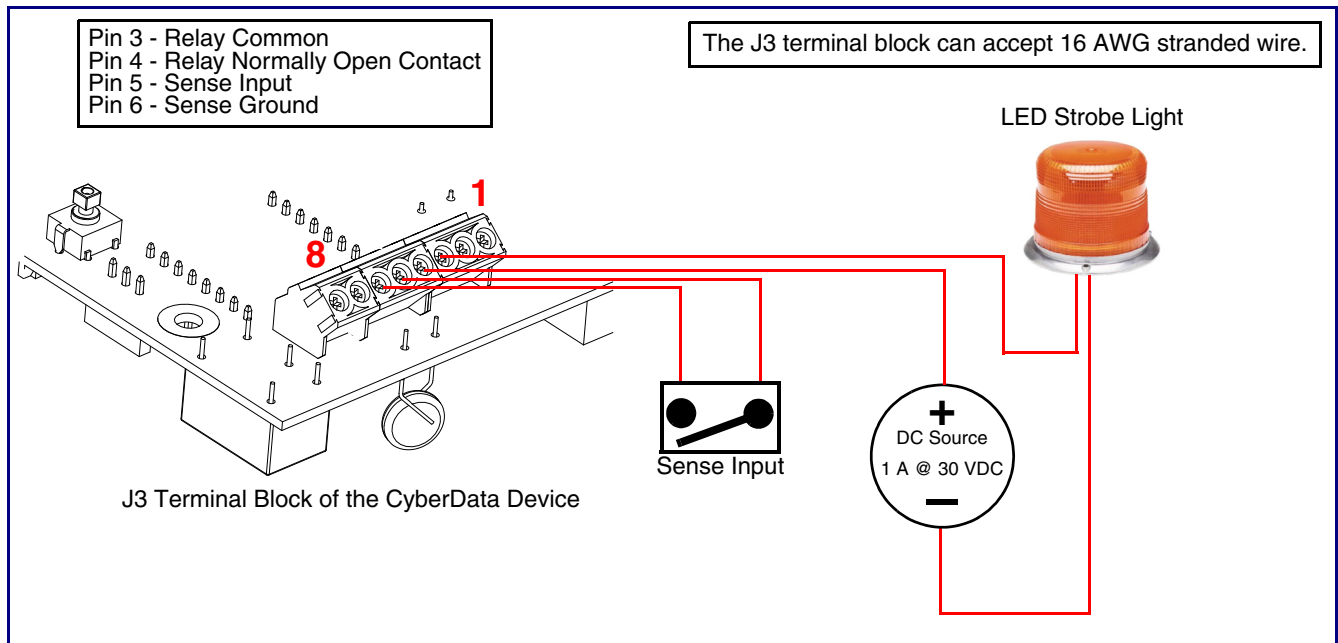
## 2.2.3 Wiring the Circuit

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

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

When configuring with an inductive load, please use an intermediary relay with a High PIV Ultrafast Switching Diode. We recommend using the CyberData Door Strike Intermediate Relay Module (CD# 011269) (see [Section 2.2.3.2, "Connecting the Door Strike Intermediate Relay Module"](#)).

**Figure 2-2. Wiring Diagram**

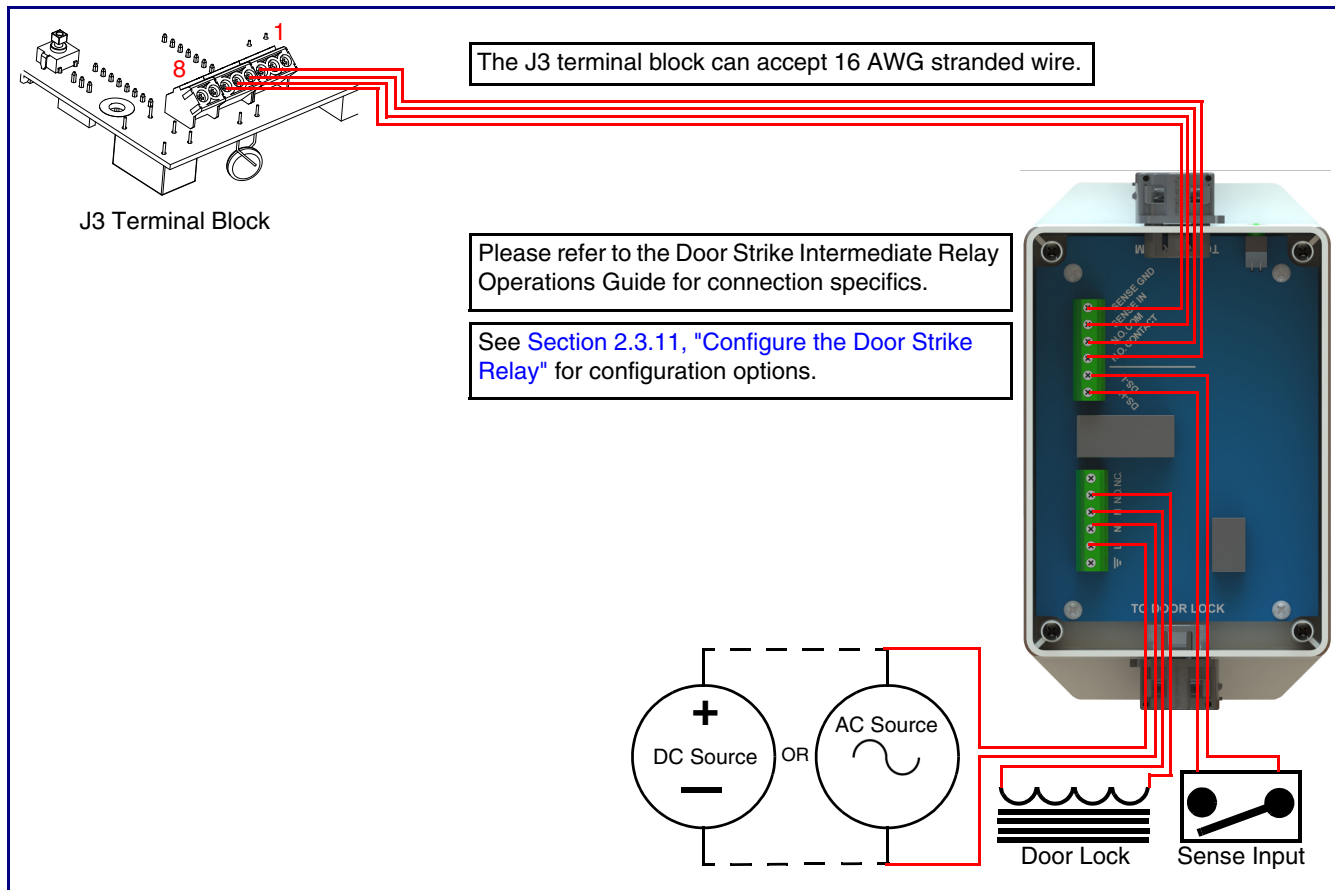


### 2.2.3.2 Connecting the Door Strike Intermediate Relay Module

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

This product provides an easier method of connecting standard door strikes as well as AC and higher voltage devices. See [Figure 2-3](#) for the wiring diagram.

**Figure 2-3. Wiring Diagram**



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

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

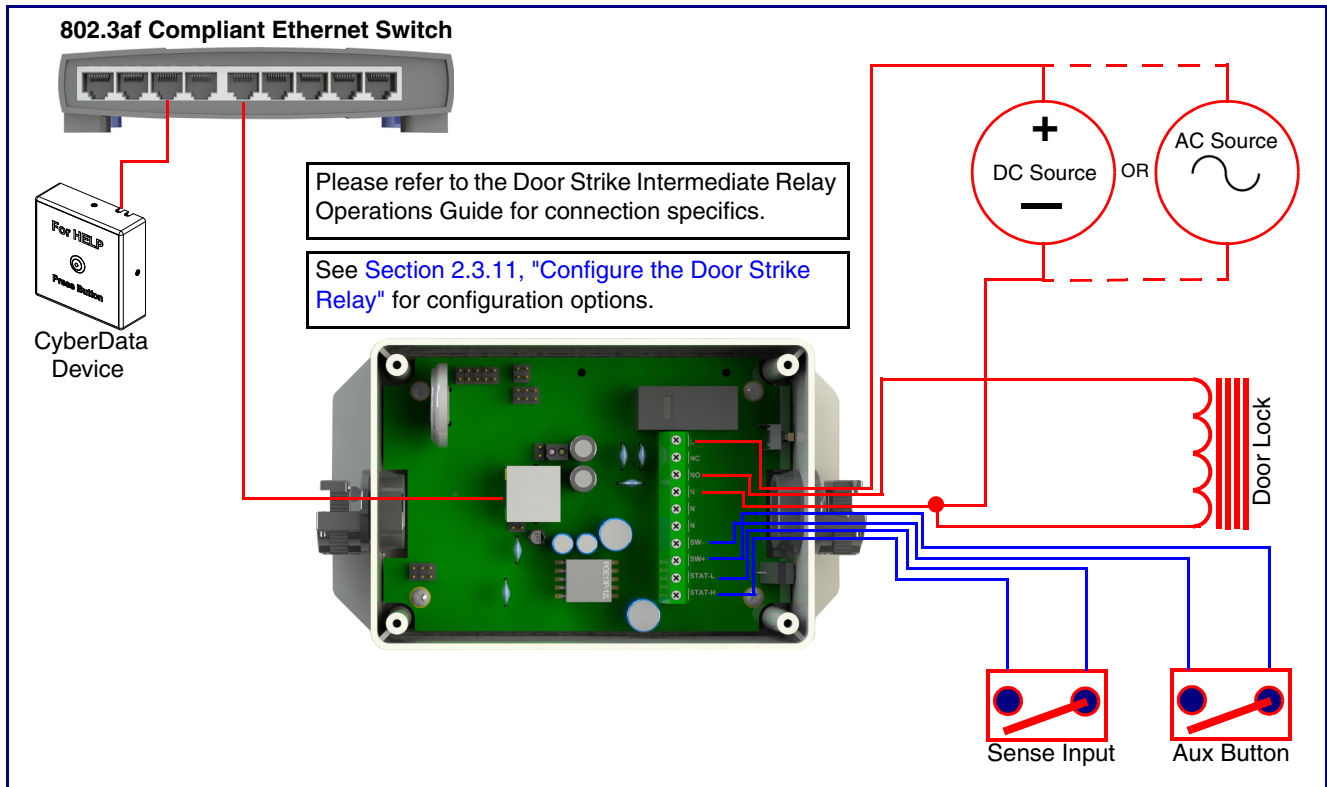


### 2.2.3.3 Connecting the Networked Door Strike Intermediate Relay

For wiring an electronic door strike to work over a network, we recommend the use of our external Networked Door Strike Intermediate Relay (CD# 011270).

This product provides an easier method of connecting standard door strikes as well as AC and higher voltage devices. See [Figure 2-4](#) for the wiring diagram.

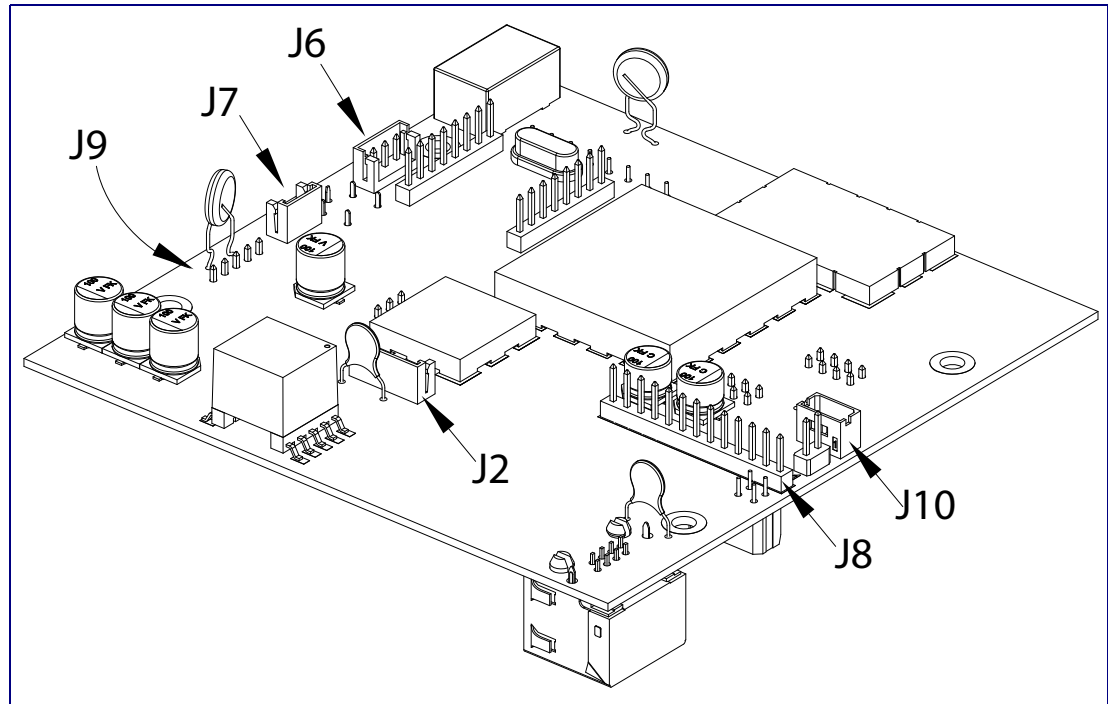
**Figure 2-4. Wiring Diagram**



## 2.2.4 Identifying the SIP Call Button Connectors and Jumpers

See the following figures and tables to identify the SIP Call Button connector locations and functions.

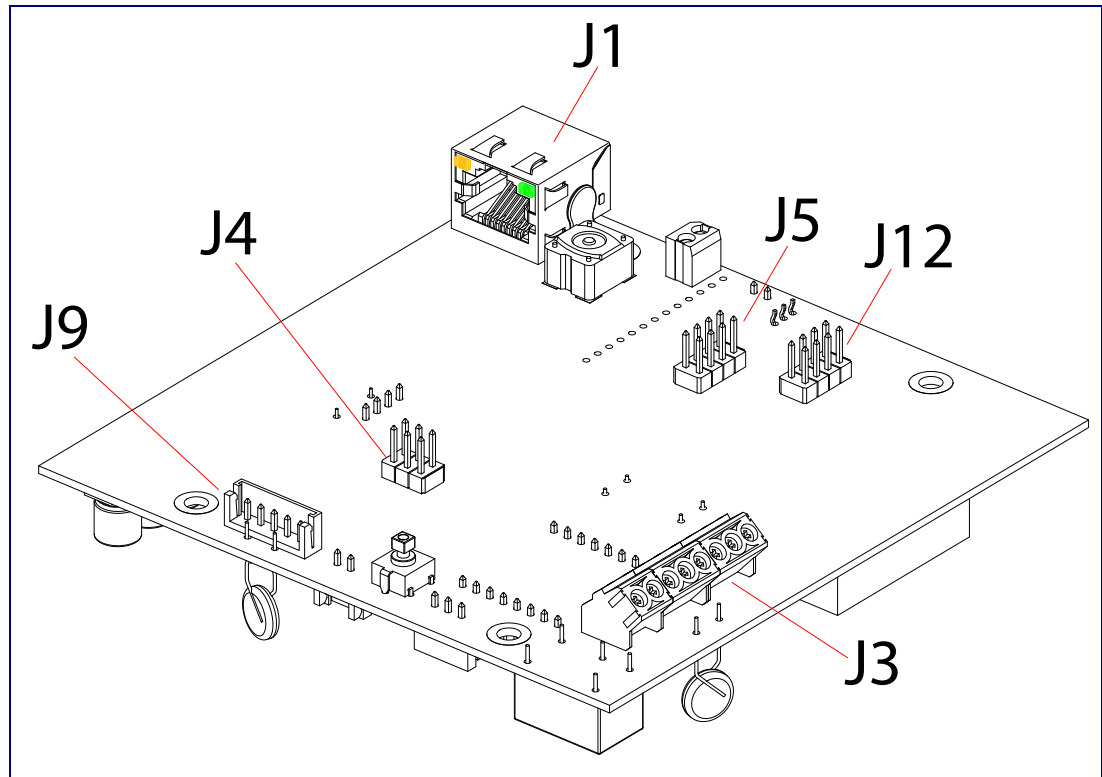
**Figure 2-5. Connector Locations**



**Table 2-2. Connector Functions**

| Connector | Function                              |
|-----------|---------------------------------------|
| J2        | Call Button LED Interface — Not Used  |
| J6        | Microphone Interface — Not Used       |
| J7        | Speaker Interface — Not Used          |
| J8        | Keypad Interface — Not Used           |
| J9        | Auxiliary Strobe Connector — Not Used |
| J10       | Proximity Sensor Interface — Not Used |

**Figure 2-6. Connector Locations**



**Table 2-3. Connector Functions**

| Connector | Function   |
|-----------|--|
| J1        | PoE Network Connection (RJ-45 ethernet)          |
| J3        | Terminal Block (see <a href="#">Figure 2-1</a> ) |
| J4        | Console Port (Factory Use Only)                  |
| J5        | JTAG (Factory Use Only)                          |
| J9        | Auxiliary Strobe Connector — Not Used            |
| J12       | Reserved (Factory Use Only)                      |

---

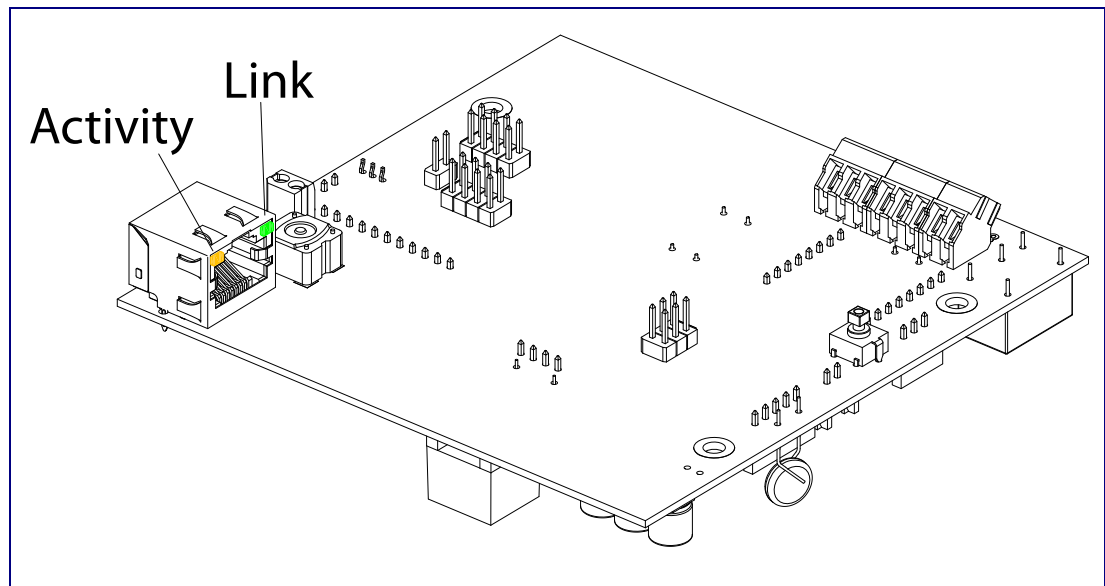
## 2.2.5 Activity and Link LEDs

### 2.2.5.1 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, **YELLOW Activity** LED blinks when there is network activity (see [Figure 2-7](#)).
- The square, **GREEN Link** LED above the Ethernet port indicates that the network connection has been established (see [Figure 2-7](#)).

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



## 2.2.6 Restore the Factory Default Settings

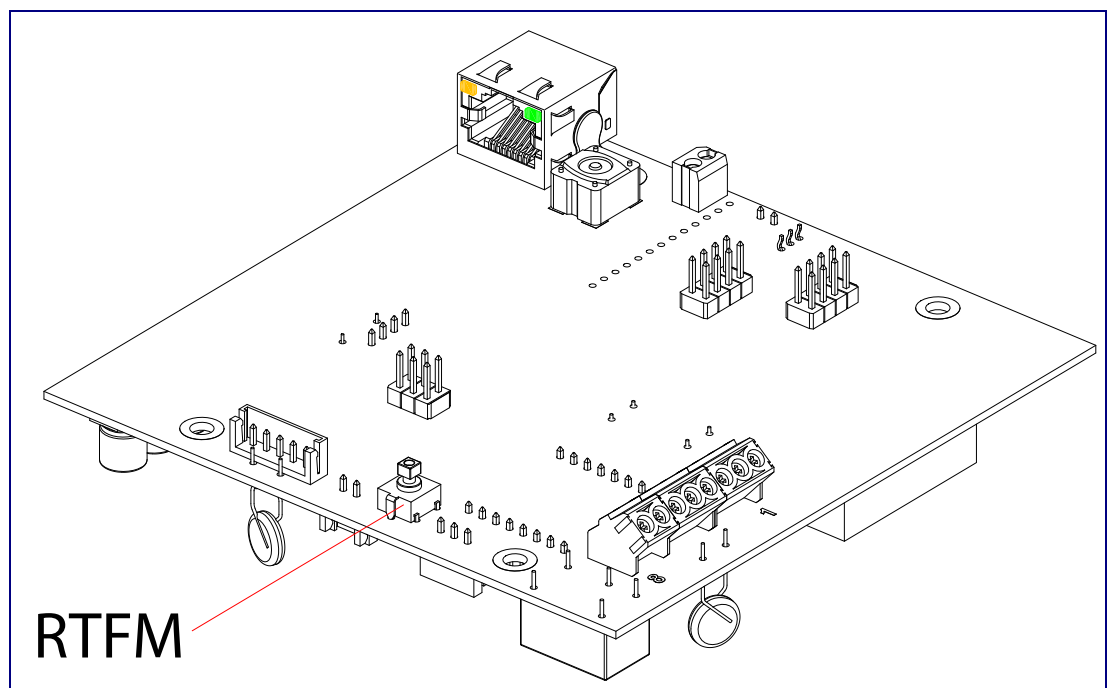
### 2.2.6.1 RTFM Switch

When the SIP Call Button is operational and linked to the network, use the Reset Test Function Management (RTFM) switch ([Figure 2-8](#)) to set the factory default settings.

**Note** Each SIP Call Button is delivered with factory set default values.

**Note** The SIP Call Button 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 2-8. RTFM Switch**



To set the factory default settings:

1. Press and hold the **RTFM** switch until the button LED starts blinking rapidly (about 10 seconds), then release the RTFM switch.

---

## 2.2.7 Call Button and the Call Button LED

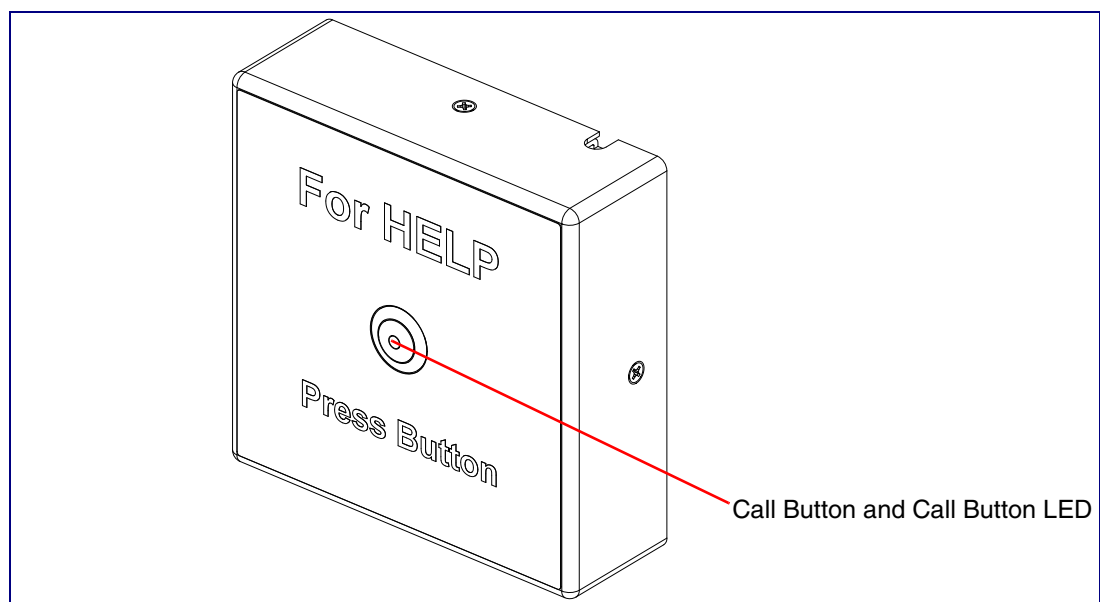
### 2.2.7.1 Calling with the The Call Button

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

### 2.2.7.2 Call Button LED Function

- Upon initial power or reset, the Call Button LED will illuminate.
- On boot, the Call Button LED will flash ten times a second while setting up the network and downloading autoprovisioning files.
- The device “autoprovisions” by default, and the initial process may take several minutes as the device searches for and downloads updates. The Call Button LED will blink during this process. During the initial provisioning, or after the factory defaults have been reset, the device may download firmware twice. The device will blink, remain solid for 10 to 20 seconds, and then resume blinking. This process will take longer if there are many audio files downloading.
- When the software has finished initialization, the Call Button LED will blink twice.
- When a call is established (not just ringing), the Call Button LED will blink.
- On the [Device Configuration Page](#) (see [Section 2.3.5, "Configure the Device"](#)), there is an option called [Button Lit When Idle](#). This option sets the normal state for the indicator LED. The Call Button LED will still blink during initialization and calls.
- The Call Button LED flashes briefly at the beginning of RTFM mode.

**Figure 2-9. Call Button and Call Button LED**



---

## 2.3 Configure the SIP Call Button Parameters

To configure the SIP Call Button online, use a standard web browser.

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

---

### 2.3.1 Factory Default Settings

All SIP Call Buttons are initially configured with the following default IP settings:

When configuring more than one SIP Call Button, attach the SIP Call Buttons to the network and configure one at a time to avoid IP address conflicts.

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

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

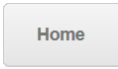
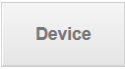
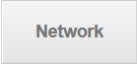

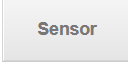
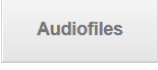


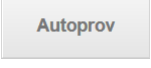
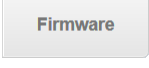
a. Default if there is not a DHCP server present.

---

## 2.3.2 SIP Call Button Web Page Navigation

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

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

| Web Page Item   | Description                                |
|---|--|
|    | Link to the <b>Home</b> page.              |
|    | Link to the <b>Device</b> page.            |
|    | Link to the <b>Network</b> page.           |
|    | Link to go to the <b>SIP</b> page.         |
|    | Link to the <b>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.          |



### 2.3.3 Using the Toggle Help Button

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

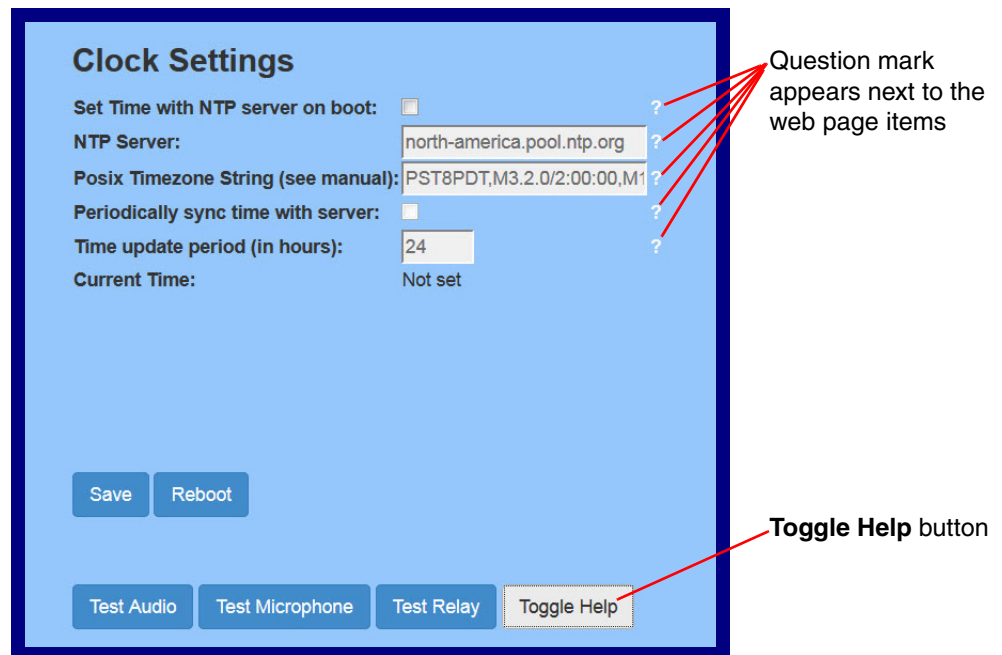
1. Click on the **Toggle Help** button that is on the UI webpage. See [Figure 2-10](#) and [Figure 2-11](#).

**Figure 2-10. Toggle/Help Button**



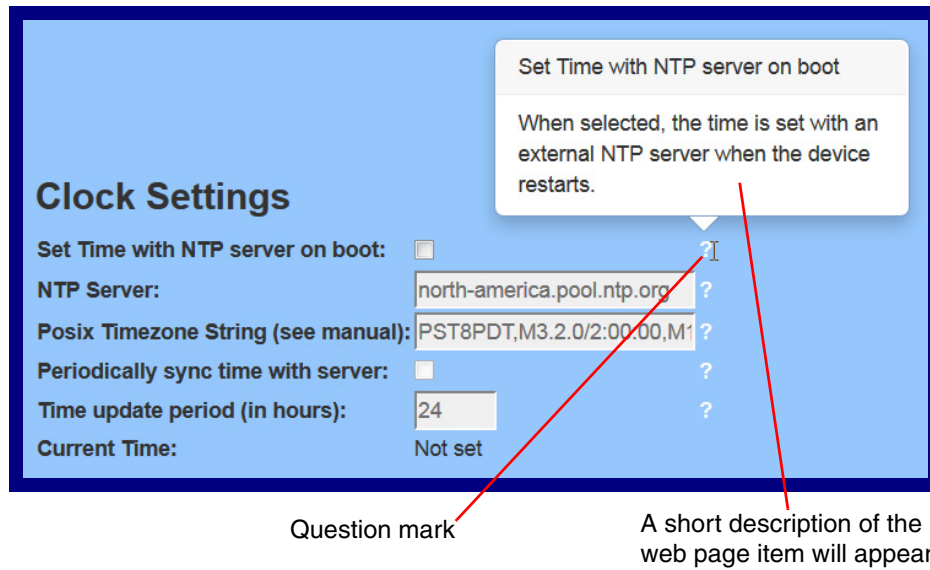
2. You will see a question mark (?) appear next to each web page item that has been provided with a short description by the Help feature. See [Figure 2-11](#).

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

**Figure 2-12. Short Description Provided by the Help Feature**



---

## 2.3.4 Log in to the Configuration Home Page

1. Open your browser to the SIP Call Button 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 Call Button.

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

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

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

**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 2-13):

Web Access Username: **admin**

Web Access Password: **admin**

Figure 2-13. Home Page

Home
Device
Network
SIP
Sensor
Audiofiles
Events
DSR
Autopro
Firmware

# CyberData SIP Call Button

## Current Status

Serial Number: 049100256

Mac Address: 00:20:17:02:56:16

Firmware Version: v11.3.0

IP Addressing: DHCP

IP Address: 10.10.1.46

Subnet Mask: 255.0.0.0

Default Gateway: 10.0.0.1

DNS Server 1: 10.0.0.252

DNS Server 2:

SIP Volume: 0

Multicast Volume: 0

Ring Volume: 0

Sensor Volume: 0

Volume Boost: Off

Microphone Gain: 0

SIP Mode: Enabled

Multicast Mode: Disabled

Event Reporting: Disabled

Nightringer: Disabled

Primary SIP Server: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

Browse... No file selected.

Import Config

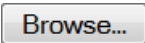

## Export Settings

Export Config





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

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

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

| Web Page Item   | Description  |
|---|--|
| <b>Admin Settings</b>   |  |
| Username ?  | The username to access the web interface. Enter up to 25 characters.   |
| Password ?  | The password to access the web interface. Enter up to 25 characters.   |
| Confirm Password ?  | Confirm the web interface password.  |
| <b>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.   |
| Volume Boost  | Shows the current Volume Boost level.  |
| Microphone Gain   | Shows the current microphone gain level.   |
| SIP Mode  | Shows the current status of the SIP mode.  |
| Multicast Mode  | Shows the current status of the Multicast mode.  |
| Event Reporting   | Shows the current status of the Event Reporting mode.  |
| Nightringer   | Shows the current status of the Nightringer mode.  |
| Primary SIP Server  | Shows the current status of the Primary SIP Server.  |
| Backup Server 1   | Shows the current status of Backup Server 1.   |
| Backup Server 2   | Shows the current status of Backup Server 2.   |
| Nightringer Server  | Shows the current status of Nightringer Server.  |
| <b>Import Settings</b>  |  |
|  | Use this button to select a configuration file to import.  |
|  | After selecting a configuration file, click Import to import the configuration from the selected file. Then, click Save and Reboot to store changes. |

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

| Web Page Item   | Description   |
|---|---|
| <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.<br><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. |

## 2.3.5 Configure the Device

1. Click the **Device Configuration** button to open the **Device Configuration** page. See [Figure 2-14](#).

Figure 2-14. Device Configuration Page

**Home** | **Device** | Network | SIP | Sensor | Audiofiles | Events | DSR | Autoprov | Firmware

# CyberData SIP Call Button

### Relay Settings

Activate Relay with DTMF code: ☒

DTMF Activation Code:

DTMF Activation Duration (in seconds):

Activate Relay While Call Active: ☐

Activate Relay On Button Press: ☐

Relay On Button Press Duration:

### 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:

### Misc Settings

Device Name:

Auto-Answer Incoming Calls: ☐

Button Lit when Idle: ☒

Button Brightness (0-255):

Play Ringback Tone: ☐

Enable Push to Talk: ☐

Disable HTTPS (NOT recommended): ☐

**Save** **Reboot**

**Test Relay** **Toggle Help**

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













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

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

| Web Page Item                           | Description  |
|---|--|
| <b>Relay Settings</b>                   |  |
| Activate Relay with DTMF Code ?         | Activates the relay when the DTMF Activation Code is entered on the phone during a SIP call with the device. RFC2833 DTMF payload types are supported.   |
| DTMF Activation Code ?                  | Activation code used to activate 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).  |
| DTMF Activation Duration (in seconds) ? | The length of time (in seconds) during which the relay will be activated when the DTMF Activation Code is detected. Enter up to 5 digits.<br><br><b>NOTE:</b> A DTMF activation duration of 0 will toggle the relay indefinitely or until the activation code is sent again  |
| Activate Relay While Call Active ?      | When selected, the relay will be activated as long as the SIP call is active.  |
| Activate Relay on Button Press ?        | When selected, the relay will be activated when the Call button is pressed.  |
| Relay on Button Press Duration ?        | The length of time (in seconds) during which the relay will be activated when the Call button is pressed. Enter up to 5 digits. A Relay on Button Press Duration value of 0 will pulse the relay once when the Call button is pressed.   |
| <b>Misc Settings</b>                    |  |
| Device Name ?                           | Type the device name. Enter up to 25 characters.   |
| Auto-Answer Incoming Calls ?            | When selected, the device will automatically answer incoming calls. When Auto-Answer Incoming Calls is disabled, the device will play a ring tone (corresponds to Ring Tone on the Audiofiles page) out of the speaker until someone presses the Call button to answer the call or the caller disconnects before the call can be answered. |
| Button Lit When Idle ?                  | When selected, the Call button LED is illuminated while the device is idle (a call is not in progress).  |
| Button Brightness (0-255) ?             | The desired Call button LED brightness level. Acceptable values are 0-255, where 0 is the dimmest and 255 is the brightest. Enter up to three digits.  |
| 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.   |



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

| Web Page Item  | Description   |
|--|---|
| Enable Push to Talk                 | This option is for noisy environments. When enabled, the microphone will be muted normally. When the Call button is pressed and held, it will unmute the microphone and allow the operator to send audio back. Using Push to Talk prevents the operator from terminating a call by pressing the Call button. The call must be terminated by the phone user.   |
| Disable HTTPS (NOT recommended)     | Disables the encrypted connection to the webpage. We do not recommend disabling HTTPS for security reasons.   |
| <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.  |
| Posix Timezone String               | See <a href="#">Section 2.3.5.1, "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.   |
| 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.  |
| Current Time   | Allows you to input the current time. (6 character limit)   |
|                                   | Click the <b>Save</b> button to save your configuration settings.<br><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>Test Relay</b> button to do a relay 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. |

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

### 2.3.5.1 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 2-8](#) shows some common strings.

**Table 2-8. 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 2-9](#) 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 2-9. 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 2-10 has some more examples of time zone strings.

**Table 2-10. 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 2-15. 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 2-11 has information about the GMT time in various time zones.

**Table 2-11. 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 2-11. 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       |

## 2.3.6 Configure the Network Parameters

1. Click the **Networking** button to open the **Network Configuration** page (Figure 2-16).

**Figure 2-16. Network Configuration Page**

**CyberData SIP Call Button**

**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: 10.10.1.46

Subnet Mask: 255.0.0.0

Default Gateway: 10.0.0.1

DNS Server 1: 10.0.0.252

DNS Server 2:



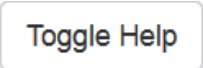
2. On the **Network** page, enter values for the parameters indicated in [Table 2-12](#).

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

**Table 2-12. 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 2.3.1, "Factory Default Settings"</a> for factory default settings. Be sure to click <b>Save</b> and <b>Reboot</b> to store changes when configuring a Static address. |
| Hostname ?                      | This is the hostname provided by the DHCP server. See the DHCP/ DNS server documentation for more information. Enter up to 64 characters.   |
| IP Address ?                    | Enter the Static IPv4 network address in dotted decimal notation.   |
| Subnet Mask ?                   | Enter the Subnet Mask in dotted decimal notation.   |
| Default Gateway ?               | Enter the Default Gateway IPv4 address in dotted decimal notation.  |
| DNS Server 1 ?                  | Enter the primary DNS Server IPv4 address in dotted decimal notation.   |
| DNS Server 2 ?                  | Enter the secondary DNS Server IPv4 address in dotted decimal notation.   |
| 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>Current Network Settings</b> |   |
| IP Address                      | Shows the current Static IP address.  |
| Subnet Mask                     | Shows the current Subnet Mask address.  |
| Default Gateway                 | Shows the current Default Gateway address.  |
| DNS Server 1                    | Shows the current DNS Server 1 address.   |
| DNS Server 2                    | Shows the current DNS Server 2 address.   |
| <b>VLAN Settings</b>            |   |
| VLAN ID (0-4095) ?              | Specify the IEEE 802.1Q VLAN ID number. Enter up to 4 digits.<br><br><b>Note:</b> The device supports 802.1Q VLAN tagging support. The switch port connected to the device will need to be in "trunking mode" for the VLAN tags to propagate.   |
| VLAN Priority (0-7) ?           | Specify the IEEE 802.1p VLAN priority level. Enter 1 digit. A value of 0 may cause the VLAN ID tag to be ignored.   |

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

| Web Page Item   | Description   |
|---|---|
|  | Click the <b>Save</b> button to save your configuration settings.<br><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.

## 2.3.7 Configure the SIP Parameters

1. Click **SIP Config** to open the **SIP Configuration** page (Figure 2-17).

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

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

Figure 2-17. SIP Configuration Page

**CyberData SIP Call Button**

**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: [proxy]

Outbound Proxy Port: 0

Disable rport Discovery: ☐

Re-registration Interval (in seconds): 360

Unregister on Boot: ☐

Keep Alive Period: 10000

**Dial Out Settings**

Dial out Extension: 204

Extension ID: id204

**RTP Settings**

RTP Port (even): 10500

Save Reboot Toggle Help



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

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

**Table 2-13. 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 2.3.7.2, "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.       |




**Table 2-13. SIP Configuration Parameters (continued)**

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

**Table 2-13. SIP Configuration Parameters (continued)**

| Web Page Item                           | Description   |
|---|---|
| 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.  |
| 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>Dial Out Settings</b>                |   |
| Dial Out Extension ?                    | Specify the extension the device will call when someone presses the Call button. Enter up to 64 alphanumeric characters.<br><br><b>Note:</b> For information about dial-out extension strings and DTMF tones, see <a href="#">Section 2.3.7.1, "Dial Out Extension Strings and DTMF Tones (using rfc2833)"</a> .  |
| Extension ID ?                          | A Caller identification string added to outbound calls. Enter up to 64 alphanumeric characters.   |
| <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.   |

**Table 2-13. SIP Configuration Parameters (continued)**

| Web Page Item   | Description   |
|---|---|
|  | Click the <b>Save</b> button to save your configuration settings.<br><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.

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

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

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

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

**Table 2-14. Examples of Dial-Out Extension Strings**

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

**Note** The maximum number of total characters in the dial-out field is 64.

### 2.3.7.2 Point-to-Point Configuration

When the board is set to not register with a SIP server (see [Figure 2-18](#)), it's possible to set the device to dial out to a single endpoint.

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

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

**Figure 2-18. SIP Configuration Page Set to Point-to-Point Mode**

The screenshot shows the 'SIP' configuration page for the 'CyberData SIP Call Button'. The page has a navigation bar at the top with tabs: Home, Device, Network, SIP (selected), Sensor, Audiofiles, Events, DSR, Autopro, and Firmware. The main title is 'CyberData SIP Call Button'.

**SIP Settings**

- Enable SIP operation: ☒
- Register with a SIP Server: ☐ (A red 'X' is drawn over this checkbox and the 'Primary SIP Server' field below it.)
- 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: [proxy]
- Outbound Proxy Port: 0
- Disable rport Discovery: ☐
- Re-registration Interval (in seconds): 360
- Unregister on Boot: ☐
- Keep Alive Period: 10000

**Dial Out Settings**

- Dial out Extension: 10.0.1.40
- Extension ID: id204

**RTP Settings**

- RTP Port (even): 0500

Buttons: Save, Reboot, Toggle Help

Device is set to NOT register with a SIP server

### 2.3.7.3 Delayed DTMF

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

**Table 2-15. Examples of Dial-Out Extension Strings**

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

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

---

## 2.3.8 Configure the Sensor Configuration Parameters

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

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

For each sensor there are four actions the Call Button can take:

- Flash the LED until the sensor is deactivated (roughly 10 times/second)
- Activate the relay until the sensor is deactivated
- Call a preset extension and play a pre-recorded audio file (once)

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

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

Figure 2-19. Sensor Configuration Page

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

# CyberData SIP Call Button

## Door Sensor Settings

Door Sensor Normally Closed: ☐ Yes ☒ No

Door Open Timeout (in seconds):

Flash Button LED: ☐

Activate Relay: ☐

Make call to extension: ☐

Dial Out Extension:

Dial Out ID:

Play recorded audio: ☐

## Intrusion Sensor Settings

Flash Button LED: ☐

Activate Relay: ☐

Make call to extension: ☐

Dial Out Extension:

Dial Out ID:

Play recorded audio: ☐




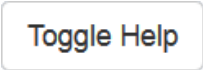


2. On the **Sensor** page, enter values for the parameters indicated in [Table 2-16](#).

**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. Sensor Configuration Parameters**

| Web Page Item                    | Description   |
|----------------------------------|---|
| <b>Door Sensor Settings</b>      |   |
| Door Sensor Normally Closed ?    | Select the inactive state of the door sensor. The door sensor is also known as the Sense Input on the device's terminal block.  |
| Door Open Timeout (in seconds) ? | The time (in seconds) the device will wait before it performs an action when the on-board door sensor is activated. The action(s) performed are based on the configured Door Sensor Settings below. Enter up to 5 digits.                             |
| Flash Button LED ?               | When selected, the Call button LED will flash until the on-board door sensor is deactivated (roughly 10 times/second).  |
| Activate Relay ?                 | When selected, the device's on-board relay will be activated until the on-board door sensor is deactivated.   |
| Make call to extension ?         | When selected, the device will call an extension when the on-board door sensor is activated. Use the <b>Dial Out Extension</b> field below to specify the extension the device will call.   |
| Dial Out Extension ?             | Specify the extension the device will call when the on-board door sensor is activated. Enter up to 64 alphanumeric characters.  |
| Dial Out ID ?                    | An additional Caller identification string added to outbound calls. Enter up to 64 alphanumeric characters.   |
| Play recorded audio ?            | When selected, the device will call the <b>Dial Out Extension</b> and play an audio file to the phone answering the SIP call (corresponds to <b>Door Ajar</b> on the <b>Audiofiles</b> page).   |
| <b>Intrusion Sensor Settings</b> |   |
| Flash Button LED ?               | When selected, the Call button LED will flash until the intrusion sensor is deactivated (roughly 10 times/second).  |
| Activate Relay ?                 | When selected, the device's on-board relay will be activated until the intrusion sensor is deactivated.   |
| Make call to extension ?         | When selected, the device will call an extension when the intrusion sensor is activated. Use the <b>Dial Out Extension</b> field below to specify the extension the device will call.   |
| Dial Out Extension ?             | Specify the extension the device will call when the intrusion sensor is activated. Enter up to 64 alphanumeric characters.  |
| Dial Out ID ?                    | An additional Caller identification string added to outbound calls. Enter up to 64 alphanumeric characters.   |
| Play recorded audio ?            | When selected, the device will call the <b>Dial Out Extension</b> and play an audio file (corresponds to <b>Intrusion Sensor Triggered</b> on the <b>Audiofiles</b> page) to the phone answering the SIP call when the intrusion sensor is activated. |
| <b>Save</b>                      | Click the <b>Save</b> button to save your configuration settings.<br><b>Note:</b> You need to reboot for changes to take effect.  |

**Table 2-16. Sensor 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. |
|  | Click the <b>Test Door Sensor</b> button to test the door sensor.   |
|  | Click the <b>Test Intrusion Sensor</b> button to test the Intrusion sensor.   |

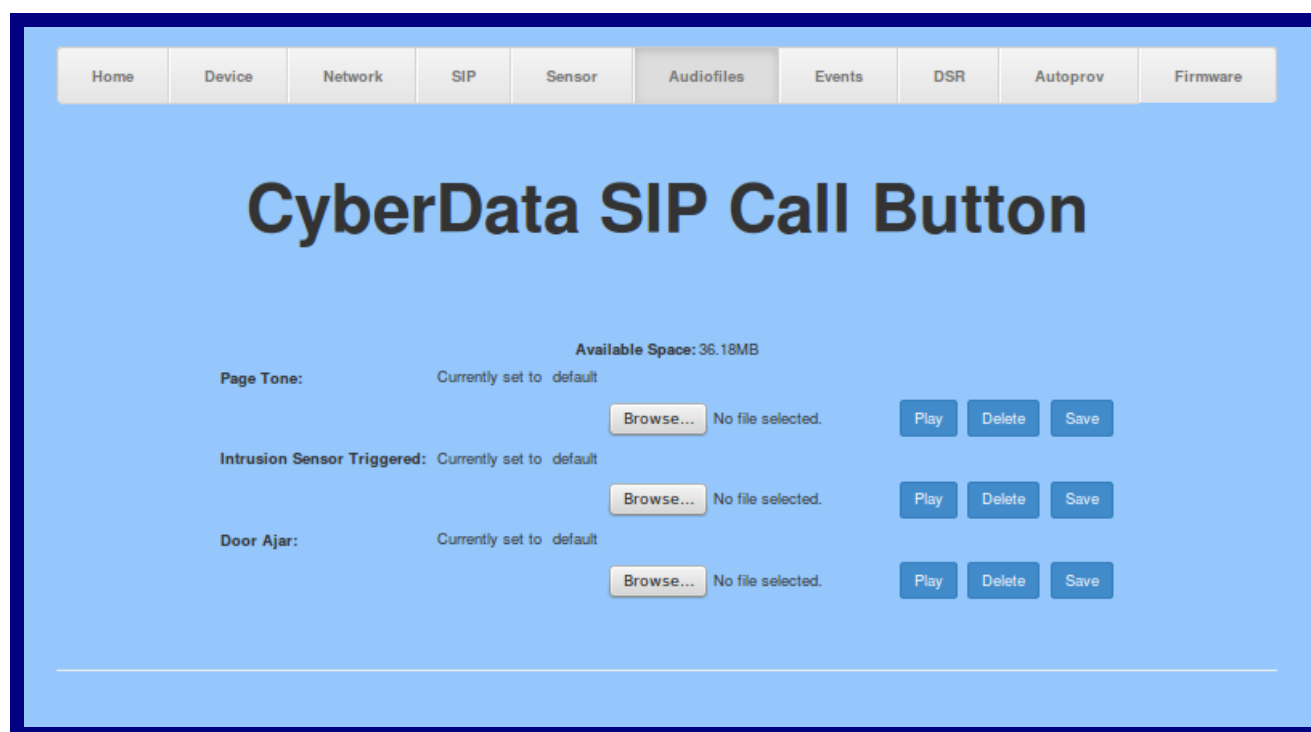
**Note** You must click on the **Save** button and then the **Reboot** button for the changes to take effect.

## 2.3.9 Configure the Audio Configuration Parameters

The **Audio Configuration** page is used to add custom audio to the board. User uploaded audio will take precedence over the audio files shipped with the Call Button.

1. Click **Audio Config** to open the **Audio Configuration** page (Figure 2-20).

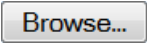

**Figure 2-20. Audio Configuration Page**





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. |
| Page tone   | Corresponds to a simple tone used for beep on initialization and beep on page (24 character limit).  |
| Intrusion Sensor Triggered  | Corresponds to the message "Intrusion Sensor Triggered" (24 character limit).  |
| Door Ajar   | Corresponds to the message "Door Ajar" (24 character limit).   |
|  | Click on the <b>Browse</b> button to navigate to and select an audio file.   |
|  | The <b>Play</b> button will play that audio file.  |

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

| Web Page Item   | Description   |
|---|---|
|  | The <b>Delete</b> button will delete any user uploaded audio and restore the stock audio file.  |
|  | The <b>Save</b> button will download a new user audio file to the board once you've selected the file by using the <b>Browse</b> button. The <b>Save</b> button will delete any pre-existing user-uploaded audio files. |

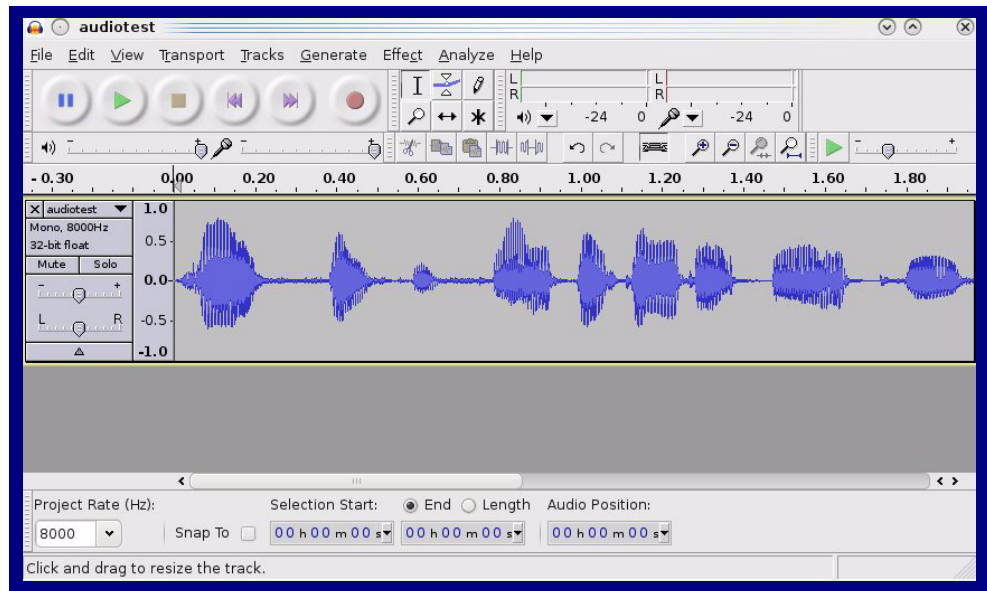
### 2.3.9.1 User-created Audio Files

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

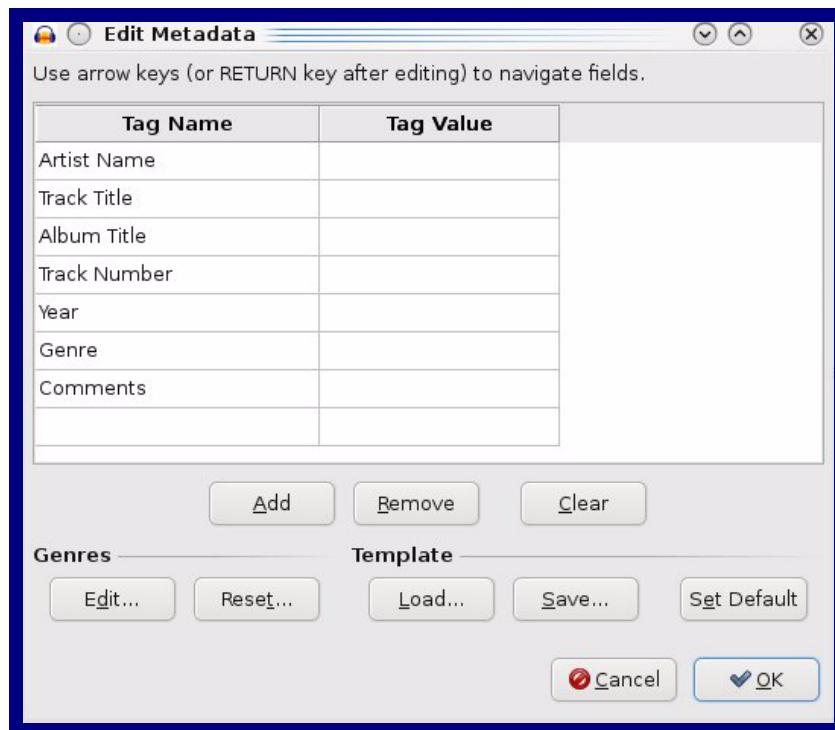
RIFF (little-endian) data, WAVE audio, Microsoft PCM, 16 bit, mono 8000 Hz

You can use the free utility *Audacity* to convert audio files into this format. See [Figure 2-21](#) through [Figure 2-23](#).

**Figure 2-21. Audacity 1**



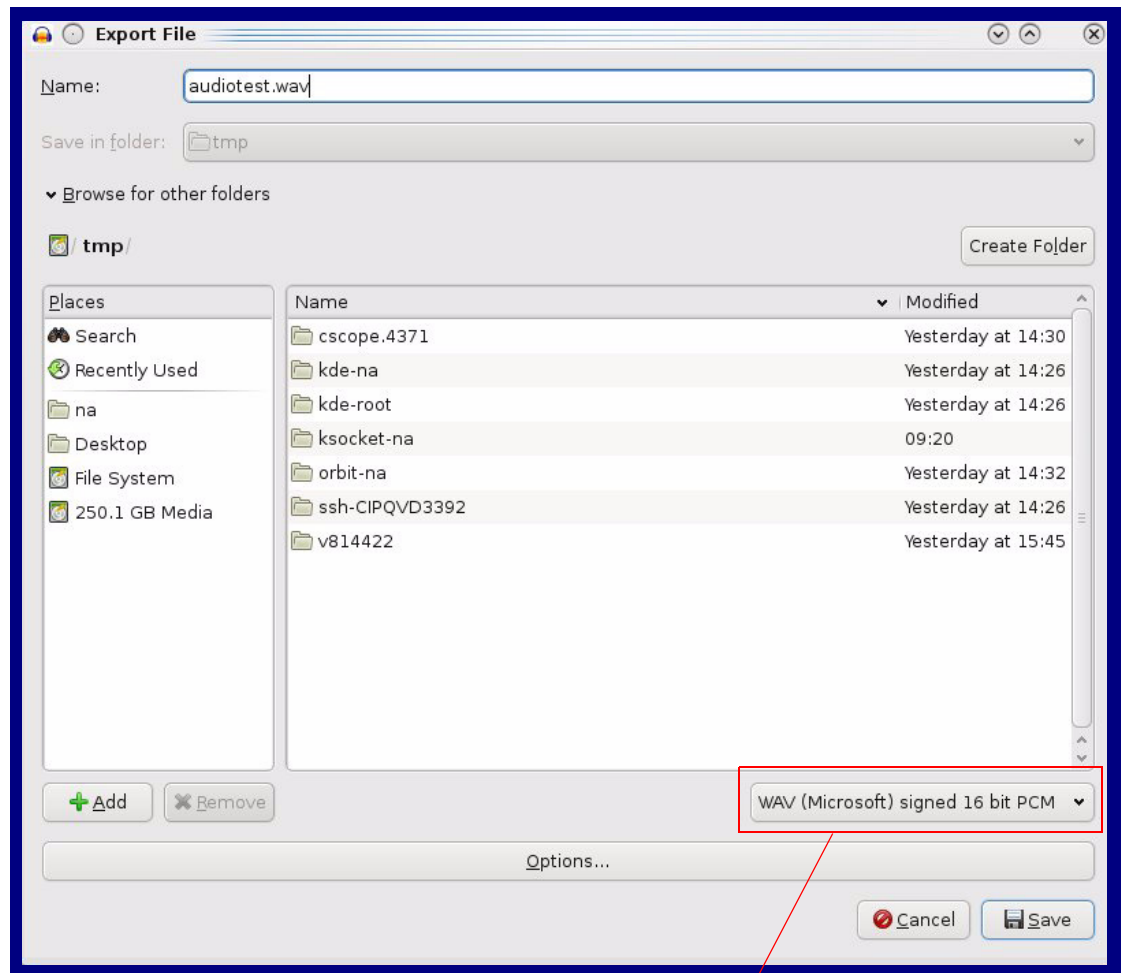
**Figure 2-22. Audacity 2**



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

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

**Figure 2-23. WAV (Microsoft) signed 16 bit PCM**



WAV (Microsoft) signed 16 bit PCM

## 2.3.10 Configure the Event Parameters

1. Click the **Event Config** button to open the **Event Configuration** page (Figure 2-24). The **Event Configuration** page specifies a remote server that can be used to receive HTTP POST events when actions take place on the board.

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

Home Device Network SIP Sensor Audiofiles **Events** DSR Autoprov Firmware

# CyberData SIP Call Button

Enable Event Generation: ☐

## Events

Enable Button Events: ☐

Enable Call Start Events: ☐

Enable Call Terminated Events: ☐

Enable Relay Activated Events: ☐

Enable Relay Deactivated Events: ☐

Enable Power On Events: ☐

Enable Sensor Events: ☐

Enable Remote Relay Events: ☐

Enable Security Events: ☐

Enable 60 Second Heartbeat: ☐

[Check All](#) [Uncheck All](#)

## Event Server

Server IP Address: 10.0.0.250

Server Port: 8080

Server URL: xmiparse\_engine

[Save](#) [Reboot](#) [Toggle Help](#)

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

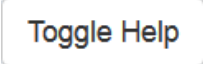
**Note** The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

**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 Power On Events ?            | When selected, the device will report when it boots.   |
| Enable Sensor Events ?              | When selected, the device will report when the on-board sensor is activated.   |
| Enable Remote Relay Events ?        | When selected, the device will report when the remote relay (DSR) is activated.  |
| Enable Security Events ?            | When enabled, the device will report when the intrusion sensor is activated.   |
| Enable 60 Second Heartbeat Events ? | When enabled, the device will report a Heartbeat event every 60 seconds. SIP registration is not required to generate Heartbeat events.  |
| Check All                           | Click on <b>Check All</b> to select all of the events on the page.   |
| Uncheck All                         | Click on <b>Uncheck All</b> to de-select all of the events on the page.  |
| <b>Event Server</b>                 |  |
| Server IP Address ?                 | The IPv4 address of the event server in dotted decimal notation.   |
| Server Port ?                       | Specify the event server port number. The supported range is 0-65536. Enter up to 5 digits.  |
| 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. |
| <b>Save</b>                         | Click the <b>Save</b> button to save your configuration settings.<br><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.  |



**Table 2-18. Events Configuration Parameters(continued)**

| Web Page Item   | Description   |
|---|---|
|  | 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 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 SIP 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 SIP 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 SIP 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 SIP 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 SIP 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 SIP 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 SIP 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 SIP 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 SIP Device' MAC='0020f70015b6'>
<event>NIGHTRINGING</event>
</cyberdata>
```

## 2.3.11 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, during different call events, manually through the web interface, or by using a Windows application.

1. Click on the **DSR** menu button to open the **DSR** page (Figure 2-25).

Figure 2-25. DSR Page

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

# CyberData SIP Call Button

### Remote Relay Settings

Not associated with any DSRs

Activate Remote Relay with DTMF code: ☐

DTMF Activation Code:

DTMF Activation Duration (in seconds):

Activate Remote Relay During Ring: ☐

Activate Remote Relay During Night Ring: ☐

Activate Remote Relay While Call Active: ☐

Activate Remote Relay On Button Press: ☐

Remote Relay On Button Press Duration (in seconds):

Listen Port for Remote Relay Status:

### Remote Door Sensor Settings

Door Open Timeout (in seconds):

Flash Button LED: ☐

Activate Local Relay: ☐

Play Audio Locally: ☐

Make call to extension: ☐

Play recorded audio: ☐

Dial Out Extension:

Dial Out ID:

### Discovered Remote Relays

| Product Type | IP Address  | MAC Address       | Serial Number | Name          | Version |                                     |  |
|--------------|-------------|-------------------|---------------|---------------|---------|-------------------------------------|--|
| DoorLock     | 10.10.1.147 | 00:20:F7:02:6C:F7 | 270000001     | LOCK270000001 | V1.6A   | <input type="button" value="View"/> | <input type="button" value="Associate"/> |
| DoorLock     | 10.10.0.242 | 00:20:F7:02:A7:A3 | 270000022     | LOCK270000022 | V1.9A   | <input type="button" value="View"/> | <input type="button" value="Associate"/> |
| DoorLock     | 10.10.1.102 | 00:20:F7:02:A7:E2 | 270000078     | LOCK270000078 | V1.9A   | <input type="button" value="View"/> | <input type="button" value="Associate"/> |

Cache age: 01:06

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**

| Web Page Item  | Description  |
|--|--|
| <b>Remote Relay Settings</b>                         |  |
| Activate Relay with DTMF Code ?                      | Activates the remote relay (DSR) when the DTMF Activation Code is entered on the phone during a SIP call with the device. RFC2833 DTMF payload types are supported.  |
| DTMF Activation Code ?                               | Activation code used to activate the remote relay (DSR) when entered on a phone during a SIP call with the device. Activate Remote Relay with DTMF Code must be enabled. Enter up to 25 digits (* and # are supported).  |
| DTMF Activation Duration (in seconds) ?              | The length of time (in seconds) during which the remote relay (DSR) will be activated when the DTMF Activation Code is detected. Enter up to 5 digits.   |
| Activate Remote Relay During Ring ?                  | When selected, the remote relay (DSR) will be activated for as long as the device is ringing. When Auto-Answer Incoming Calls is enabled, the device will not ring and this option does nothing. When selected, the network relay will be activated for as long as the call is active. |
| Activate Remote Relay During Night Ring ?            | When selected, the remote relay (DSR) will be activated as long as the Nightringer extension is ringing.   |
| Activate Remote Relay While Call Active ?            | When selected, the remote relay (DSR) will be activated as long as the call is active.   |
| Activate Remote Relay on Button Press ?              | When selected, the remote relay (DSR) will be activated when the Call Button is pressed.   |
| Remote Relay on Button Press Duration (in seconds) ? | The length of time (in seconds) during which the remote relay (DSR) will be activated when the Call button is pressed. Enter up to 5 digits. A Remote Relay on Button Press Duration value of 0 will pulse the remote relay (DSR) once when the Call button is pressed.                |
| Listen Port for Remote Relay Status ?                | Specify the port to listen for remote relay (DSR) status packets.  |
| <b>Remote Door Sensor Settings</b>                   |  |
| Door Open Timeout (in seconds) ?                     | The time (in seconds) the device will wait before it performs an action when the remote (DSR) door sensor is activated. The action(s) performed are based on the configured Remote Door Sensor Settings below.   |
| Flash Button LED ?                                   | When selected, the Call button LED will flash until the remote (DSR) door sensor is deactivated (roughly 10 times/second).   |
| Activate Local Relay ?                               | When selected, the device's on-board relay will be activated until the remote (DSR) door sensor is deactivated.  |
| Play Audio Locally ?                                 | When selected, the device will loop an audio file out of the speaker until the remote (DSR) door sensor is deactivated.  |

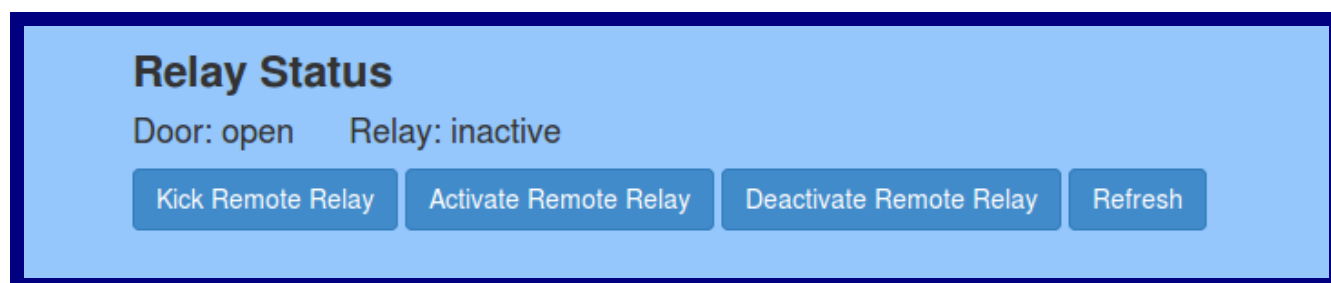
**Table 2-19. DSR Configuration Parameters (continued)**

| Web Page Item                   | Description  |
|---------------------------------|--|
| Make call to extension ?        | When selected, the device will call an extension when the remote (DSR) door sensor is activated. Use the 'Dial Out Extension' field below to specify the extension the device will call.   |
| Play recorded audio ?           | When selected, the device will call the Dial Out Extension and play an audio file to the phone answering the SIP call (corresponds to Door Ajar on the Audiofiles page) when the remote (DSR) door sensor is activated.  |
| Dial Out Extension ?            | Specify the extension the device will call when the remote (DSR) door sensor is activated. Enter up to 64 alphanumeric characters.   |
| Dial Out ID ?                   | An additional Caller identification string added to outbound calls. Enter up to 64 alphanumeric characters.  |
| Save                            | Click the <b>Save</b> button to save your configuration settings.<br><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.      |
| <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.  |
| Discover                        | Use this button to search for and find any remote relays that are available on the network.  |
| View                            | Use this button to view the settings of a remote relay that has been "discovered" after pressing the <b>Discover</b> button.   |
| Associate                       | Use this button to associate the remote relay with the device. Only one relay may be associated with a device.   |

Table 2-19. DSR Configuration Parameters (continued)

| Web Page Item                  | Description  |
|--------------------------------|--|
| <b>Relay Status</b>            | <b>Note:</b> The <b>Relay Status</b> section and settings only appear on the webpage when there is an associated door strike relay.                        |
| Door                           | Shows the status of the door.  |
| Relay                          | Shows the status of the remote relay.  |
| <b>Kick Remote Relay</b>       | Click on the <b>Kick Remote Relay</b> button to activate the remote relay for a specified time. The time is equal to the DTMF timeout.                     |
| <b>Activate Remote Relay</b>   | Click on the <b>Activate Remote Relay</b> button to activate the remote relay until the <b>Deactivate Remote Relay</b> button is pressed.                  |
| <b>Deactivate Remote Relay</b> | Click on the <b>Deactivate Remote Relay</b> button to deactivate the remote relay.   |
| <b>Refresh</b>                 | Click on the <b>Refresh</b> button to refresh the web page and accurately display the status of the remote relay (active/inactive) and door (open/closed). |

Figure 2-26. Relay Status Section



## 2.3.12 Configure the Device (on the DSR page)

1. Click the **View** button on the **DSR** page to open the **Configure Device** page (Figure 2-27).

**Figure 2-27. DSR Page Configure Device Page**

### Configure Device

|  |   |   |
|--|---|---|
| Serial Number  | <input type="text" value="270000002"/>  | <input type="button" value="Refresh"/>      |
| MAC Address  | <input type="text" value="00:20:F7:02:6C:F8"/>                                | <input type="button" value="Get Log"/>      |
| Version  | <input type="text" value="V1.2A"/>  | <input type="button" value="Clear Log"/>    |
| Device Name  | <input type="text" value="LOCK270000003"/>                                    | <input type="button" value="Reboot"/>       |
| Addressing Mode  | <input checked="" type="radio"/> Static <input checked="" type="radio"/> DHCP | <input type="button" value="Set Time"/>     |
| IP Address:  | <input type="text" value="192.168.70.74"/>                                    | <input type="button" value="Save Changes"/> |
| Subnet Mask:   | <input type="text" value="255.255.240.0"/>                                    | <input type="button" value="Cancel"/>       |
| Default Gateway:   | <input type="text" value="192.168.64.1"/>                                     |   |
| Command Port:  | <input type="text" value="59999"/>  |   |
| Send Events  | <input checked="" type="radio"/> Off <input type="radio"/> On                 |   |
| Event IP Address:  | <input type="text" value="192.168.79.255"/>                                   |   |
| Event Port:  | <input type="text" value="49999"/>  |   |
| Energize Time:   | <input type="text"/>  |   |
| DST  | <input checked="" type="radio"/> Off <input type="radio"/> On                 |   |
| DST Start:   | <input type="text" value="M3.2.0/02.00.00"/>                                  |   |
| DST End:   | <input type="text" value="M11.1.0/02.00.00"/>                                 |   |
| Current Time:  | <input type="text" value="17:45:26 08182014"/>                                |   |
| Encryption:  | <input checked="" type="radio"/> None <input type="radio"/> AES-256           |   |
| Encryption Key:  | <input type="text"/>  |   |
|  |   |   |
| Door State   | <input type="text" value="open"/>   |   |
| Relay State  | <input type="text" value="inactive"/>   |   |
| Button State   | <input type="text" value="inactive"/>   |   |
| LED  | <input type="text" value="red"/>  |   |
| Alarm State  | <input type="text" value="alarm"/>  |   |
| JP4, 6, 9, 10  | <input type="text" value="0000"/>   |   |
| <input type="button" value="Browse..."/> No file selected. |   | <input type="button" value="Upgrade"/>      |












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

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

**Table 2-20. DSR Page Configure Device Parameters**

| Web Page Item    | Description  |
|------------------|--|
| Serial Number    | Displays the serial number of the door strike relay.   |
| MAC Address      | Displays the mac address of the door strike relay.   |
| Version          | Displays the firmware version of the door strike relay.  |
| Device Name      | Displays the name of the door strike relay. The default name is "LOCK," followed by the 9 digit ASCII serial number. The maximum name length is 13 characters. The unit will always respond to its default name.   |
| Addressing Mode  | Determines whether an IP address will be manually assigned through Static mode or dynamically assigned through a DHCP server.  |
| IP Address       | Displays the IP address of the door strike relay.  |
| Subnet Mask      | Displays the subnet mask of the door strike relay.   |
| Default Gateway  | Displays the default gateway of the door strike relay.   |
| Command Port     | This shows the port on which the door strike relay sends status packets to the device (defaults to 49999).   |
| Send Events      | When enabled, events can be sent to the associated device.   |
| Event IP Address | The IP address of the associated device.   |
| Event Port       | This is the port by which the door strike relay receives commands (defaults to 59999).   |
| Energize Time    | This is the number of seconds that the relay will be energized.  |
| DST              | Allows you to either enable or disable the Daylight Savings Time feature.  |
| DST Start        | <p>Sets the Daylight Savings Time starting time in the following format:</p> <p><b>M3.2.0/02:00:00</b></p> <p><b>M3</b> is the third month (March).</p> <p><b>.2</b> is the second occurrence of the day in the month.</p> <p><b>.0</b> is Sunday.</p> <p><b>/02:00:00</b> is the time.</p> <p><b>Note:</b> When the occurrence is set to <b>5</b>, the final occurrence of the day in the specified month is used.</p>      |
| DST End          | <p>Sets the Daylight Savings Time ending time in the following format:</p> <p><b>M11.1.0/02:00:00</b></p> <p><b>M11</b> is the eleventh month (November).</p> <p><b>.1</b> is the first occurrence of the day in the month.</p> <p><b>.0</b> is Sunday.</p> <p><b>/02:00:00</b> is the time.</p> <p><b>Note:</b> When the occurrence is set to <b>5</b>, the final occurrence of the day in the specified month is used.</p> |

Table 2-20. DSR Page Configure Device Parameters (continued)

| Web Page Item   | Description  |
|---|--|
| Current Time  | Sets the current time.<br><b>Note:</b> Be sure to save the current time by clicking on the <b>Set Time</b> button.   |
| Encryption  | Encryption can either be set to <b>None</b> or <b>AES-256</b> .  |
| Encryption Key  | Sets the AES encryption key. If encryption is currently enabled, the response to this command will be sent using the “old” key. The new key should be sent as 64 ASCII hexadecimal characters.   |
| Door State  | This field displays the current door state and is not configurable.  |
| Relay State   | This field displays the current relay state and is not configurable.   |
| Button State  | This field displays the current button state and is not configurable.  |
| LED   | This field displays the current LED state and is not configurable.   |
| Alarm State   | This field displays the current alarm state and is not configurable.   |
| JP4, 6, 9, 10   | This shows whether jumpers JP4, JP6, JP9, or JP10 are either enabled or disabled through the four digit sequence ( <b>0000</b> ). The <b>0</b> turns to <b>1</b> for an enabled jumper. For example, <b>0011</b> would mean jumpers JP9 and JP10 are activated, but JP4 and JP9 are not. |
|    | Click on the <b>Refresh</b> button to refresh the <b>Device Configuration</b> page.  |
|   | Click on the <b>Get Log</b> button to get a log of the associated door strike relay activity. The door strike relay has 128Kb non-volatile storage for log data, storing an average of 10 days' worth of log data before it is overwritten.  |
|  | Click on the <b>Clear Log</b> button to clear the log from the door strike relay   |
|  | Click on the <b>Reboot</b> button to reboot any “discovered” remote relays and clear any associated devices.   |
|  | Click on the <b>Set Time</b> button to change the time.  |
|  | Click on the <b>Save Changes</b> button to save any changes that are made to the Device Configuration page.<br><b>Note:</b> The time setting must be saved by pressing the <b>Set Time</b> button.   |
|  | Click on the <b>Cancel</b> button to cancel any changes that were made to the <b>Configure Device</b> page and return to the <b>DSR</b> page.  |
|  | Click on the <b>Browse</b> button to navigate through your computer and find firmware files.   |
|  | Click on the <b>Upgrade</b> button to upgrade the firmware of the door strike relay.   |

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

## 2.3.13 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 2-28](#).

**Figure 2-28. Autoprovisioning Page**

Home Device Network SIP Sensor Audiofiles Events DSR **Autoprov** Firmware

# CyberData SIP Call Button

Disable Autoprovisioning: ☐

Autoprovisioning Server:

Autoprovisioning Filename:

Use tftp: ☐

Username:

Password:

Autoprovisioning autoupdate (in minutes):

Autoprovision at time (HHMMSS):

Autoprovision when idle (in minutes > 10):

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

Autoprovisioning happens on boot.

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

If these haven't been configured, it will look for an autoprovisioning server in your list of DHCP options and try to download '0020f702bf15.xml' and if this fails, '000000cd.xml'.

Save Reboot Toggle Help

Download Template


### Autoprovisioning log

```
00:00 Failed to fetch autoprov file
00:00 Autoprov found option 150 in DHCP server="10.0.0.252"
00:00 Autoprov looking for 0020f702bf15.xml at 10.0.0.252
00:00 Autoprov looking for 000000cd.xml at 10.0.0.252
00:00 Failed to fetch autoprov file
00:00 Autoprov found option 66 in DHCP server="http://chalmers.cyberdata.net"
Treating this like an http address
00:00 Autoprov looking for 0020f702bf15.xml at http://chalmers.cyberdata.net
00:00 Autoprov looking for 000000cd.xml at http://chalmers.cyberdata.net
00:00 Failed to fetch autoprov file
```


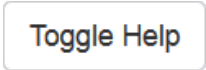

2. On the **Autoprovisioning** page, you may enter values for the parameters indicated in [Table 2-21](#).

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

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

| Web Page Item   | Description   |
|---|---|
| Disable Autoprovisioning ?  | Prevent the device from automatically trying to download a configuration file. See <a href="#">Section 2.3.13.1, "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 2-7</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 2-7</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 2-7</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 2-21. 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 2.3.13.3, "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.

### 2.3.13.1 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 2.3.13.2, "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 2-21](#)). This file contains every configuration option that can be set on the board.

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

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

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

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

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

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

The file 0020f7123456.xml contains:

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

1. The device will first set it's name to 'Newname'.
2. It will try to download <http://example.com/common.xml>.
3. It will try to download [http://example.com/sip\\_reg0020f7123456.xml](http://example.com/sip_reg0020f7123456.xml).
4. It will try to download <http://example.com/audio0020f7123456>.
5. It will try to download <http://example.com/device.xml>.

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

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

#### Checking for New Autoprovisioning Files after Boot

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

## The Autoprovisioning Filename

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

**Table 2-22. Autoprovisioning File Name**

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

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

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

For example:

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

The autoprovisioning filename is set to “cyberdata/”

On boot, the device will try to download:

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

...and if this fails:

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

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



```

Autoprovisioning <FirmwareSettings>
Firmware Updates <FirmwareFile>505-uImage-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.

### 2.3.13.2 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; }
```

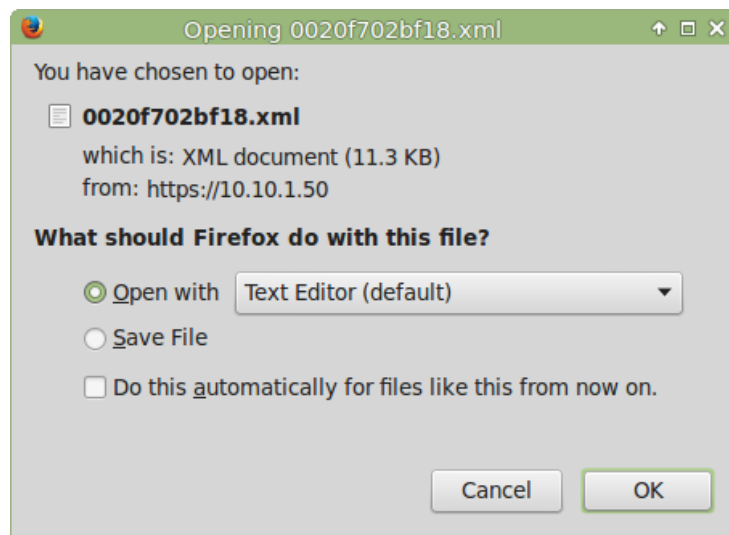
### 2.3.13.3 Download Template Button

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

**Figure 2-29. 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 Call Button

|  |   |
|--|---|
| <br>GENERAL ALERT | <p><b>Caution</b></p> <p><b>Equipment Hazard:</b> Devices with a serial number that begins with 0491xxxxx can only run firmware versions 10.0.0 or later.</p> |
|--|---|

To upload the firmware from your computer:

1. Retrieve the latest SIP Call Button firmware file from the SIP Call Button **Downloads** page at:  
<http://www.cyberdata.net/products/voip/digitalanalog/callbutton/downloads.html>
2. Unzip the firmware version file. This file may contain the following:
  - Firmware file
  - Release notes
3. Log in to the SIP Call Button home page as instructed in [Section 2.3.4, "Log in to the Configuration Home Page"](#).
4. Click on the **Firmware** menu button to open the **Firmware** page. See [Figure 2-30](#).


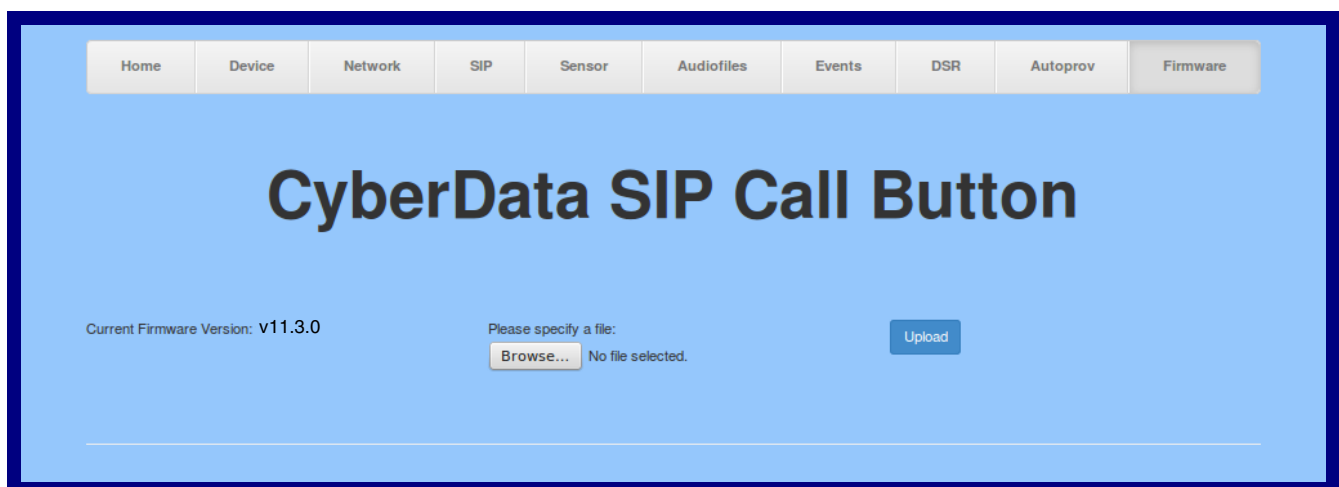
|  |   |
|--|---|
| <br>GENERAL ALERT | <p><b>Caution</b></p> <p><b>Equipment Hazard:</b> CyberData strongly recommends that you first reboot the device before attempting to upgrade the firmware of the device. See <a href="#">Section 2.4.1, "Reboot the Device"</a>.</p> |
|--|---|

Figure 2-30. 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 Call Button has uploaded the file, the **Uploading Firmware** countdown page appears, indicating that the firmware is being written to flash. The SIP Call Button 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).

8. [Table 2-23](#) shows the web page items on the **Firmware** page.

**Table 2-23. 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 Intercom firmware file that you want to upload. |
|  | Click on the <b>Upload</b> button to automatically upload the selected firmware and reboot the system.          |

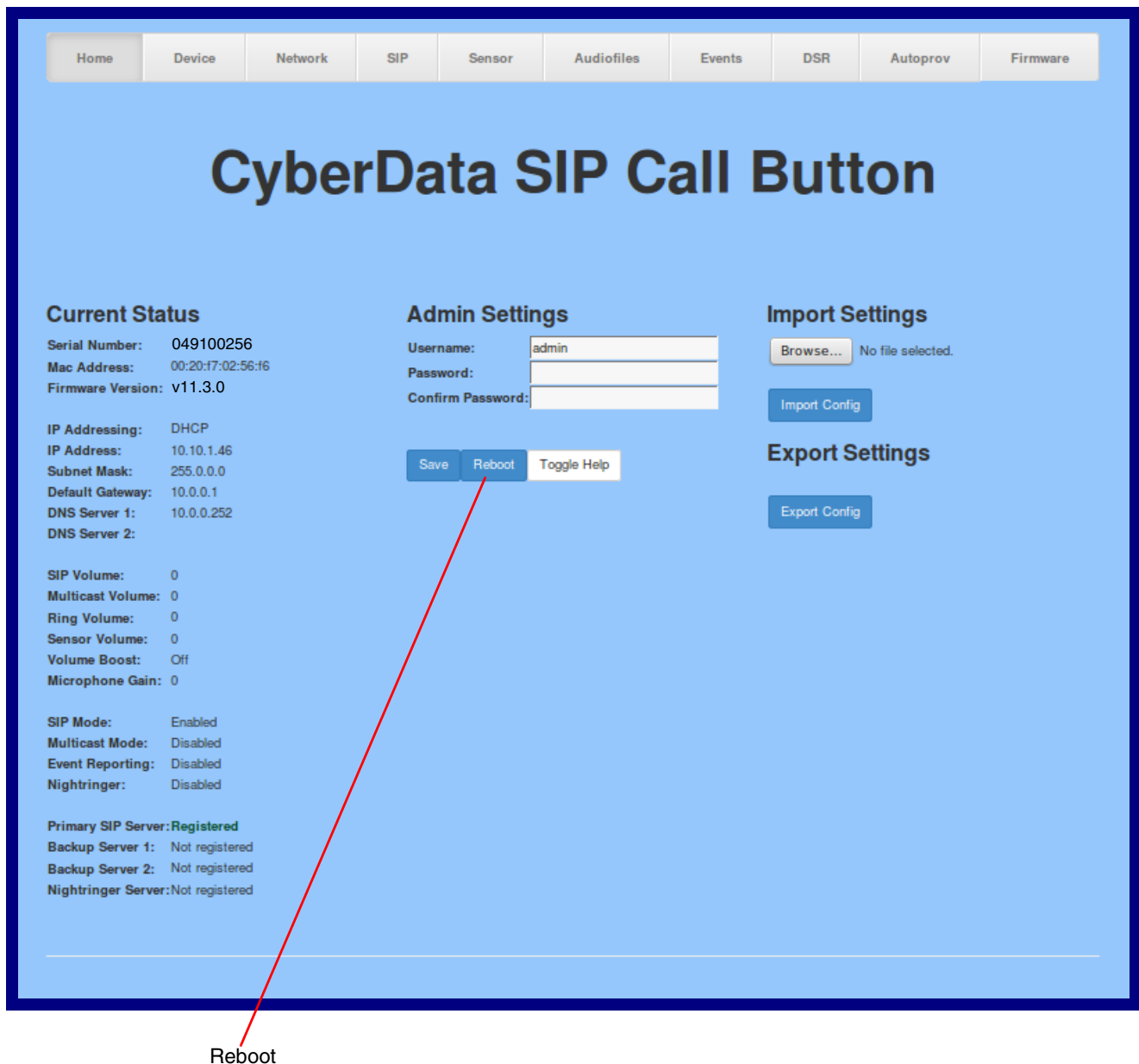


## 2.4.1 Reboot the Device

To reboot a SIP Call Button, log in to the web page as instructed in [Section 2.3.4, "Log in to the Configuration Home Page"](#).

1. Click on the **Reboot** button on the **Home** page ([Figure 2-31](#)). A normal restart will occur.

**Figure 2-31. Home Page**



## 2.5 Command Interface

Some functions on the device can be activated using simple POST commands to the web interface. The examples in [Table 2-24](#) 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 2-24. 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"               |
| 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"             |
| 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/sensorconfig.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/sensorconfig.cgi" --post-data "intrusiontest=yes" |

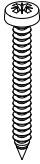
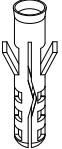
a. Type and enter all of each http POST command on one line.

# Appendix A: Mounting the SIP Call Button

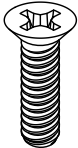
## A.1 Mount the SIP Call Button

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

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

| Quantity | Part Name                          | Illustration  |
|----------|------------------------------------|---|
| 4        | #6 x 1.25 inches Sheet Metal Screw |  |
| 4        | #6 Ribbed Plastic Anchor           |  |

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

| Quantity | Part Name                                   | Illustration  |
|----------|---|---|
| 4        | #6-32 x 0.625-inch Flat-Head Machine Screw. |  |

After the SIP Call Button is assembled, plug the Ethernet cable into the SIP Call Button Assembly (see [Figure A-1](#)).

[Section 2.2.5, "Activity and Link LEDs"](#) explains how the **Link** and **Status** LEDs work.

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

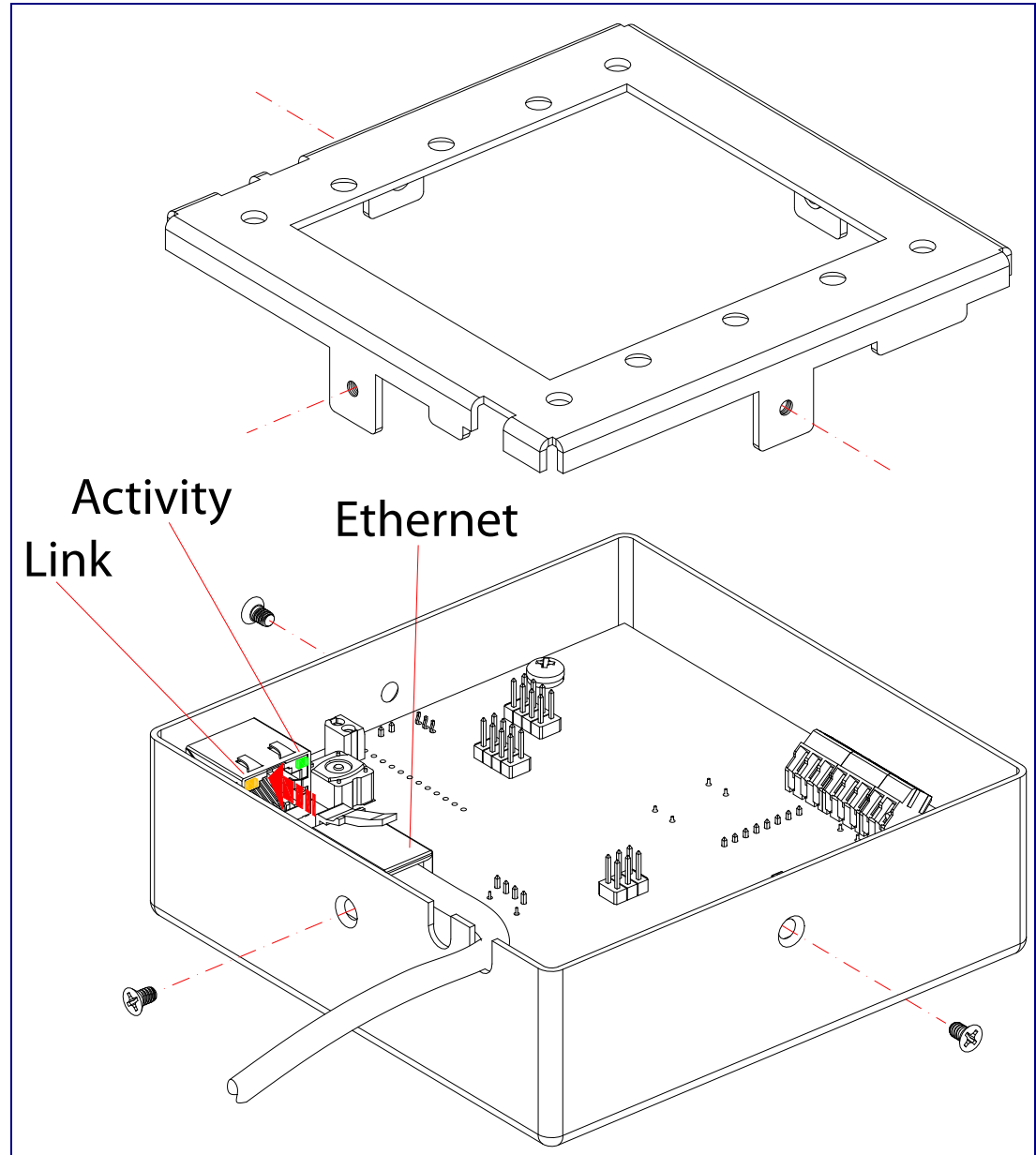


Figure A-3 shows the wall mounting options for the SIP Call Button.

**Note** Be sure to connect the SIP Call Button to the Earth Ground.

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

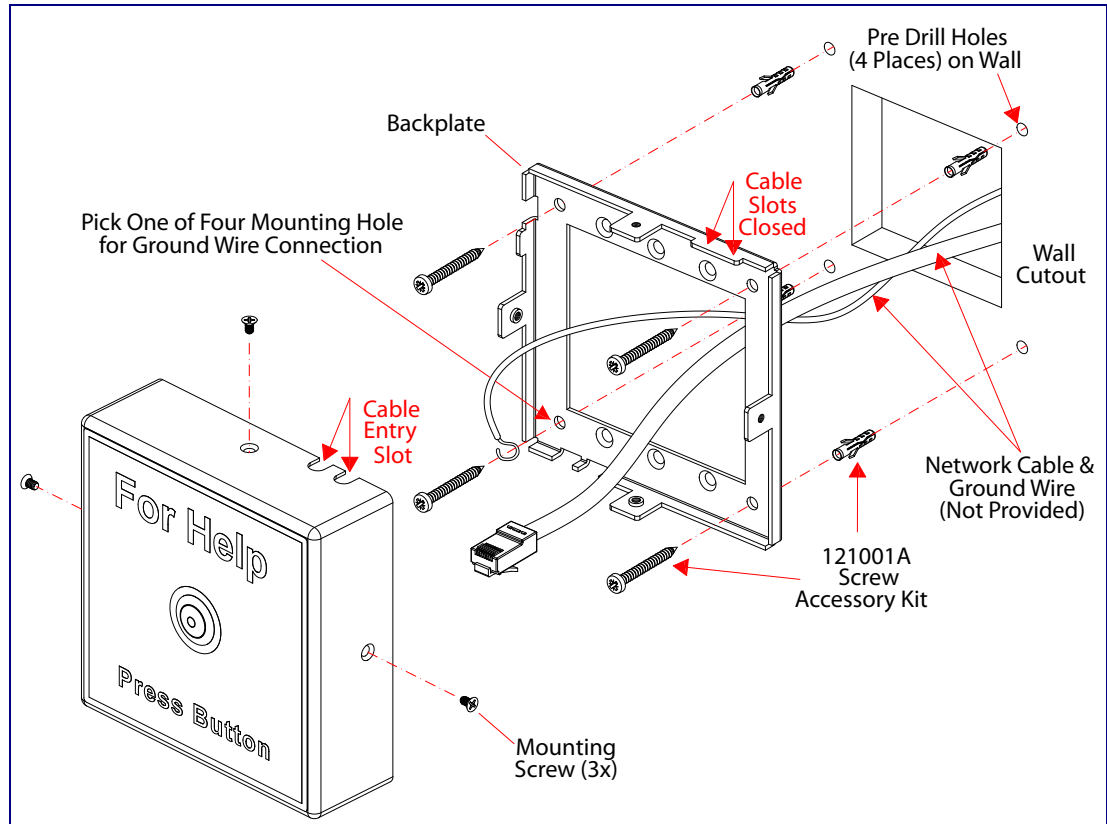


Figure A-3 shows the gang box mounting options for the SIP Call Button.

**Note** Be sure to connect the SIP Call Button to the Earth Ground.

**Figure A-3. Mounting Options**

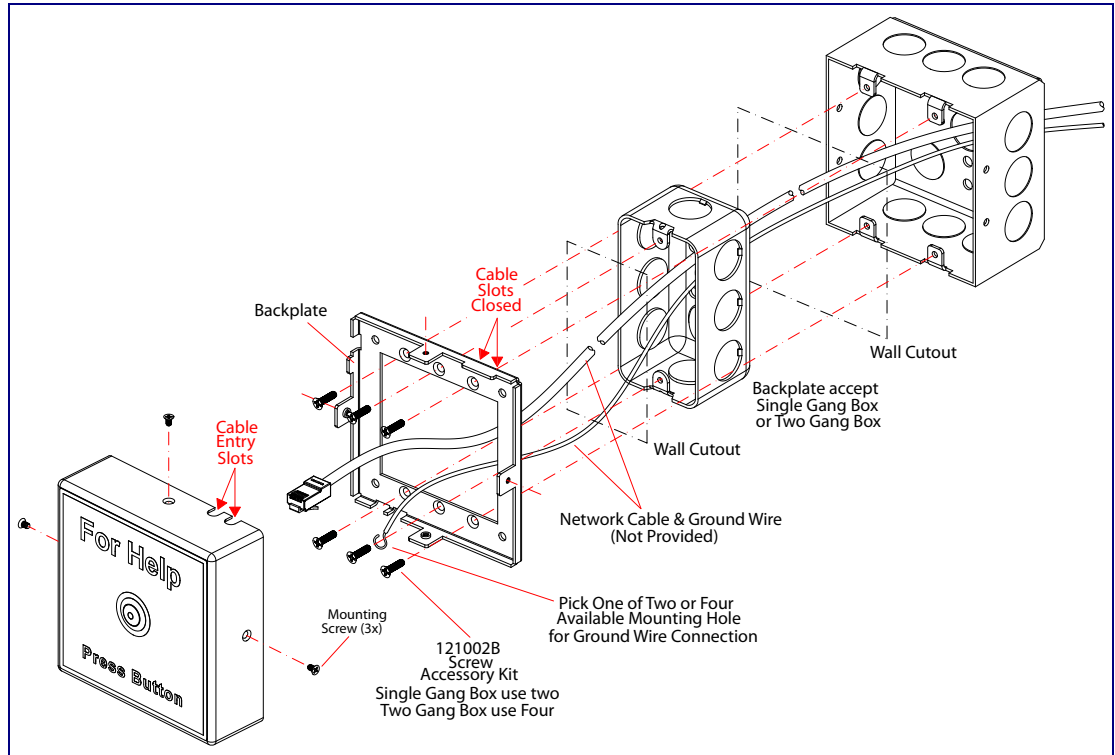
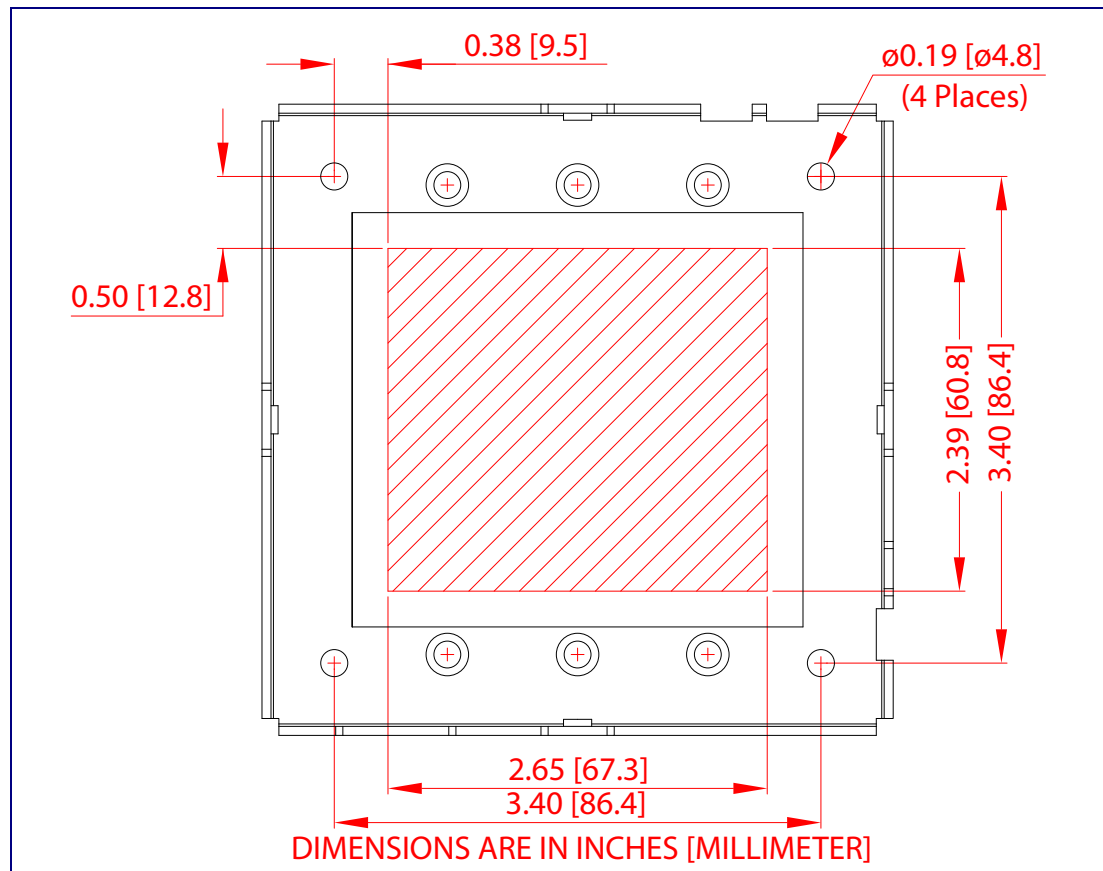


Figure A-4 shows the maximum recommended wall cutout dimensions for mounting the SIP Call Button.

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



# Appendix B: Troubleshooting/Technical Support

---

## B.1 Frequently Asked Questions (FAQ)

A list of frequently asked questions (FAQs) are available on the SIP Call Button product page at:

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

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

---

## B.2 Documentation

The documentation for this product is released in an English language version only. You can download PDF copies of CyberData product documentation from the SIP Call Button product page at:

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



## B.3 Contact Information

|                                  |   |
|----------------------------------|---|
| Contact                          | <p>CyberData Corporation<br/> 3 Justin Court<br/> Monterey, CA 93940 USA<br/> <a href="http://www.CyberData.net">www.CyberData.net</a><br/> Phone: 800-CYBERDATA (800-292-3732)<br/> Fax: 831-373-4193</p>  |
| Sales                            | <p>Sales 831-373-2601 Extension 334</p>   |
| Technical Support                | <p>The fastest way to get technical support for your VoIP product is to submit a VoIP Technical Support form at the following website:</p> <p><a href="http://www.cyberdata.net/support/contactsupportvoip.php">http://www.cyberdata.net/support/contactsupportvoip.php</a></p> <p>The Support Form initiates a ticket which CyberData uses for tracking customer requests. Most importantly, the Support Form tells us which PBX system and software version that you are using, the make and model of the switch, and other important information. This information is essential for troubleshooting. Please also include as much detail as possible in the <b>Comments</b> section of the Support Form.</p> <p>Phone: (831) 373-2601, Ext. 333<br/> Email: support@cyberdata.net</p> |
| Returned Materials Authorization | <p>To return the product, contact the Returned Materials Authorization (RMA) department:</p> <p>Phone: 831-373-2601, Extension 136<br/> Email: RMA@CyberData.net</p> <p>When returning a product to CyberData, an approved CyberData RMA number must be printed on the outside of the original shipping package. Also, RMA numbers require an active VoIP Technical Support ticket number. A product will not be accepted for return without an approved RMA number. Send the product, in its original package, to the following address:</p> <p>CyberData Corporation<br/> 3 Justin Court<br/> Monterey, CA 93940<br/> Attention: RMA "your RMA number"</p>  |
| RMA Status Form                  | <p>If you need to inquire about the repair status of your product(s), please use the CyberData RMA Status form at the following web address:</p> <p><a href="http://www.cyberdata.net/support/rmastatus.html">http://www.cyberdata.net/support/rmastatus.html</a></p>   |

---

## B.4 Warranty

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

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

**End of Life Devices out of warranty** are included under this policy. However, End of Life devices are not eligible for our Spare in the Air program. End of Life devices are devices that are no longer produced or sold. Therefore, we cannot offer a Spare in the Air replacement. Technical support is still available for these devices. However, no firmware revisions or updates will be scheduled. If an End of Life device cannot be repaired, a replacement of a current version of the device may be offered at MSRP.

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

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

---

### B.4.1 Warranty & RMA Returns within the United States

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

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

CyberData Corporation

3 Justin Court.

Monterey, CA 93940

Attn: RMA "xxxxxx"

---

## B.4.2 Warranty & RMA Returns outside of the United States

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

---

## B.4.3 Spare in the Air Policy

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

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

---

## B.4.4 Return and Restocking Policy

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

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

---

## B.4.5 Warranty and RMA Returns Page

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

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

# Index

## Numerics

16 AWG gauge wire 6

## A

activate local relay (door sensor) 54  
 activate relay (door sensor) 42  
 activate relay (intrusion sensor) 42  
 activity LED 13  
 address, configuration login 20  
 announcing a speaker's IP address 14  
 audio configuration 44  
 audio configuration page 44  
 audio encodings 3  
 audio files, user-created 46  
 autoprovision at time (HHMMSS) 61  
 autoprovision when idle (in minutes > 10) 61  
 autoprovisioning 62  
   download template button 62  
 autoprovisioning autoupdate (in minutes) 61, 62  
 autoprovisioning configuration 60, 61  
 autoprovisioning filename 61  
 autoprovisioning server (IP Address) 61

## B

backup SIP server 1 34  
 backup SIP server 2 34  
 backup SIP servers, SIP server  
   backups 34  
 browsers supported 3

## C

call button 13  
 call button configuration  
   default IP settings 16  
 call button LED 15  
 changing  
   the web access password 24  
 Chrome (web browser) 3  
 Cisco SRST 34  
 command interface 75  
 commands 75  
 configurable parameters 25, 31, 34, 58  
 configuration  
   audio 44

  default IP settings 16  
   door sensor 40  
   intrusion sensor 40  
   network 30, 57  
   SIP 33  
   using Web interface 16  
 configuration home page 20  
 configuration page  
   configurable parameters 25, 31, 58  
 contact information for CyberData 7  
 Current Network Settings 31  
 current network settings 31

## D

default  
   device settings 10  
   gateway 16  
   IP address 16  
   subnet mask 16  
   username and password 16  
   web login username and password 20  
 default device settings 14  
 default gateway 16, 31  
 default IP settings 16  
 default login address 20  
 device configuration 24  
   device configuration parameters 61  
   the device configuration page 60  
 device configuration page 24  
 device configuration parameters 25  
 device configuration password  
   changing for web configuration access 24  
 DHCP Client 3  
 dial out extension (door sensor) 42, 55  
 dial out extension (intrusion sensor) 42  
 dial out extension strings 37, 39  
 dimensions 4  
 discovery utility program 20  
 DNS server 31  
 door sensor 40, 42, 54  
   activate local relay 54  
   activate relay 42  
   dial out extension 42, 55  
   door open timeout 42, 54  
   door sensor normally closed 42  
   flash button LED 42, 54  
   play audio locally 54  
 door strike intermediate relay 9, 10  
 download autoprovisioning template button 62  
 DTMF tones 37, 39  
 DTMF tones (using rfc2833) 37

## E

earth ground 3, 4  
ethernet cable 2  
expiration time for SIP server lease 35, 36  
export settings 22, 23

## F

factory default settings 14  
    how to set 14  
Firefox (web browser) 3  
firmware  
    where to get the latest firmware 72  
flash button LED (door sensor) 42, 54  
flash button LED (intrusion sensor) 42

## G

gang box mounting 3, 4  
get autoprovisioning template 62  
GMT table 28  
GMT time 28

## H

home page 20  
http POST command 75  
http web-based configuration 3

## I

identifier names (PST, EDT, IST, MUT) 28  
identifying your product 1  
illustration of device mounting process 1  
import settings 22, 23  
import/export settings 22, 23  
installation, typical device system 2  
intercom configuration page  
    configurable parameters 34  
Internet Explorer (web browser) 3  
intrusion sensor 40, 42  
    activate relay 42  
    dial out extension 42  
    flash button LED 42  
IP address 16, 31  
IP addressing  
    default

IP addressing setting 16

## J

J3 terminal block, 16 AWG gauge wire 6

## L

lease, SIP server expiration time 35, 36  
LED  
    green link LED 13  
    yellow activity LED 13  
link LED 13, 2  
local SIP port 35  
log in address 20

## M

mounting the device 1  
Mozilla Firefox (web browser) 3

## N

navigation (web page) 17  
navigation table 17  
network configuration 30  
network configuration of intercom 57  
network rate 4  
Network Setup 30, 57  
Nightringer 6, 71, 72  
nightringer settings 35  
NTP server 26

## O

on-board relay 7

## P

packet time 3  
part number 4  
parts list 5  
password  
    for SIP server login 34  
    login 20

- restoring the default 16
- play audio locally (door sensor) 54
- point-to-point configuration 38
- port
  - local SIP 35
  - remote SIP 35
- posix timezone string
  - timezone string 26
- POST command 75
- power requirement 4
- product
  - configuring 16
  - mounting 1
  - parts list 5
- product features 3
- product overview
  - product features 3
  - product specifications 4
  - supported protocols 3
  - supported SIP servers 4
  - typical system installation 2
- product specifications 4
- protocols supported 3

## R

- reboot 73, 74
- remote SIP port 35
- Reset Test Function Management (RTFM) switch 14
- resetting the IP address to the default 1, 6
- restoring factory default settings 14, 10
- restoring the factory default settings 14
- return and restocking policy 9
- RMA returned materials authorization 7
- RMA status 7
- rport discovery setting, disabling 35
- RTFM switch 14
- RTP/AVP 3

## S

- Safari (web browser) 3
- sensor setup page 41, 53
- sensor setup parameters 40
- sensors 42, 54
- server address, SIP 34
- set time with external NTP server on boot 26
- setting up the device 6
- settings, default 14
- SIP
  - enable SIP operation 34
  - local SIP port 35

- user ID 34
- SIP (session initiation protocol) 3
- SIP configuration 33
  - SIP Server 34
- SIP configuration parameters
  - outbound proxy 35, 36
  - registration and expiration, SIP server lease 35, 36
  - unregister on reboot 35
  - user ID, SIP 34
- SIP registration 34
- SIP remote SIP port 35
- SIP server 34
  - password for login 34
  - SIP servers supported 4
  - unregister from 35
  - user ID for login 34
- Spare in the Air Policy 9
- SRST 34
- status LED 2
- subnet mask 16, 31
- supported protocols 3

## T

- technical support, contact information 7
- terminal block, 16 AWG gauge wire 6
- time zone string examples 28

## U

- user ID
  - for SIP server login 34
- username
  - changing for web configuration access 24
  - default for web configuration access 20
  - restoring the default 16

## V

- VLAN ID 31
- VLAN Priority 31
- VLAN tagging support 31
- VLAN tags 31

## W

- warranty 8
- warranty & RMA returns outside of the United States 9
- warranty and RMA returns page 9

- warranty policy at CyberData 8
- web access password 16
- web access username 16
- web browsers supported 3
- web configuration log in address 20
- web page
  - navigation 17
- web page navigation 17
- web-based configuration 16
- weight 4
- wget, free unix utility 75
- wiring the circuit 8
  - devices less than 1A at 30 VDC 8