



SIP Call Button Operations Guide

Part #011049

Document Part #930801M
for Firmware Version 11.7.6

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

SIP Call Button Operations Guide 930801M
Part # 011049

COPYRIGHT NOTICE:

© 2017, CyberData Corporation, ALL RIGHTS RESERVED.

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

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

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

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

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



Technical Support

The fastest way to get technical support for your VoIP product is to submit a VoIP Technical Support form at the following website:

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

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

Email: support@cyberdata.net

Fax: (831) 373-4193

Company and product information is at www.cyberdata.net.

Revision Information

Revision 930801M, which corresponds to firmware version 11.7.6, was released on March 9, 2017, and has the following changes:

- Updates [Figure 2-1, "Connections and Alternate Power Input"](#)
- Updates [Figure 2-3, "Devices Less than 1A at 30 VDC"](#)
- Updates [Figure 2-4, "Network Dual Door Strike Relay Wiring Diagram with External Power Source"](#)
- Updates [Figure 2-5, "Network Dual Door Strike Relay Wiring Diagram Using PoE+"](#)
- Updates [Figure 2-6, "Door Strike Relay Module Wiring Diagram from Device"](#)
- Updates [Figure 2-12, "RTFM Button"](#)
- Updates [Figure 2-13, "RTFM Button"](#)
- Updates [Figure 2-14, "RTFM Button"](#)
- Adds [Section 2.3, "Connecting an Auxiliary RGB Strobe to the Device"](#)
- Adds [Section 2.4, "Connecting a SIP RGB Strobe to the Device"](#)
- Updates [Figure 2-19, "Home Page"](#)
- Updates [Figure 2-20, "Device Configuration Page"](#)
- Updates [Figure 2-23, "SIP Configuration Page"](#)
- Updates [Figure 2-24, "SIP Configuration Page Set to Point-to-Point Mode"](#)
- Updates [Figure 2-25, "Sensor Configuration Page"](#)
- Updates [Figure 2-31, "DSR Page \(not associated with any DSRs\)"](#)
- Updates [Figure 2-32, "Autoprovisioning Page"](#)
- Updates [Figure 2-34, "Firmware Page"](#)
- Updates [Figure 2-35, "Home Page"](#)
- Adds the following notes to [Table 2-7, "Device Configuration Parameters"](#):
 - Note: You must click on the Save button and then the Reboot button for the changes to take effect.
 - Note: The SIP Volume, Multicast Volume, Ring Volume, Sensor Volume, and Push to Talk Volume settings do not require a reboot for the changes to take effect.
 - Note: The NTP Server setting needs to be restarted to spawn NTP or to change the server. Syncing and changing the Time update period (in hours) setting does not require a reboot for the changes to take effect.
 - Note: None of the Relay Settings require a reboot for the changes to take effect.
 - Note: The Disable HTTPS (NOT recommended) setting requires a reboot for the changes to take effect.
- Adds the following notes to [Table 2-13, "SIP Configuration Parameters"](#):
 - Note: You must click on the Save button and then the Reboot button for the changes to take effect.
 - Note: The Terminate Call After Delay setting does not require a reboot for the changes to take effect.
- Adds the following notes to [Table 2-16, "Sensor Configuration Parameters"](#):
 - Note: You must click on the Save button for the changes to take effect.

- Note: None of the Sensor Configuration Page settings require a reboot for the changes to take effect.
- Adds the following notes to [Table 2-18, "Events Configuration Parameters"](#):
 - Note: You must click on the Save button for the changes to take effect.
 - Note: Enabling Event Generation or changing an Event Server setting requires a reboot for the changes to take effect.
 - Note: Selecting particular events, Check All, or Uncheck All does not require a reboot for the changes to take effect.

Browsers Supported




The following browsers have been tested against firmware version 11.7.6:

- Internet Explorer (version: 10)
- Firefox (also called Mozilla Firefox) (version: 33.0)
- Chrome (version 48.0.2564.116)
- Opera (version 12.16)
- 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!

 <p>GENERAL ALERT</p>	<p>Warning</p> <p><i>Electrical Hazard:</i> This product should be installed by a licensed electrician according to all local electrical and building codes.</p>
 <p>GENERAL ALERT</p>	<p>Warning</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>
 <p>GENERAL ALERT</p>	<p>Warning</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>General Alert</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>Ground</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

Chapter 1 Product Overview	1
1.1 How to Identify This Product	1
1.2 Typical System Installation	2
1.3 Product Features	4
1.4 Supported Protocols	5
1.5 Supported SIP Servers	5
1.6 Specifications	6
1.7 Compliance	7
1.7.1 CE Testing	7
1.7.2 FCC Statement	7
Chapter 2 Installing the SIP Call Button	8
2.1 Parts List	8
2.2 SIP Call Button Setup	9
2.2.1 SIP Call Button Connections	9
2.2.2 Using the On-Board Relay	11
2.2.3 Wiring the Circuit	12
2.3 Connecting an Auxiliary RGB Strobe to the Device	16
2.4 Connecting a SIP RGB Strobe to the Device	16
2.4.1 SIP Call Button Connectors	17
2.4.2 Activity and Link LEDs	19
2.4.3 RTFM Button	20
2.4.4 Call Button and the Call Button LED	23
2.5.1 Factory Default Settings	24
2.5.2 SIP Call Button Web Page Navigation	25
2.5.3 Using the Toggle Help Button	26
2.5.4 Log in to the Configuration Home Page	28
2.5.5 Configure the Device	32
2.5.6 Configure the Network Parameters	38
2.5.7 Configure the SIP Parameters	41
2.5.8 Configure the Sensor Configuration Parameters	47
2.5.9 Configure the Audio Configuration Parameters	52
2.5.10 Configure the Event Parameters	57
2.5.11 Configure the Door Strike Relay	61
2.5.12 Configure the Autoprovisioning Parameters	63
2.5.13 Downloading the Firmware	75
2.5.14 Reboot the Device	77
2.6.1 Command Interface Post Commands	78
Appendix A Mounting the SIP Call Button	79
A.1 Mount the SIP Call Button	79
Appendix B Troubleshooting/Technical Support	84
B.1 Frequently Asked Questions (FAQ)	84
B.2 Documentation	84
B.3 Contact Information	85
B.4 Warranty and RMA Information	85
Index	86

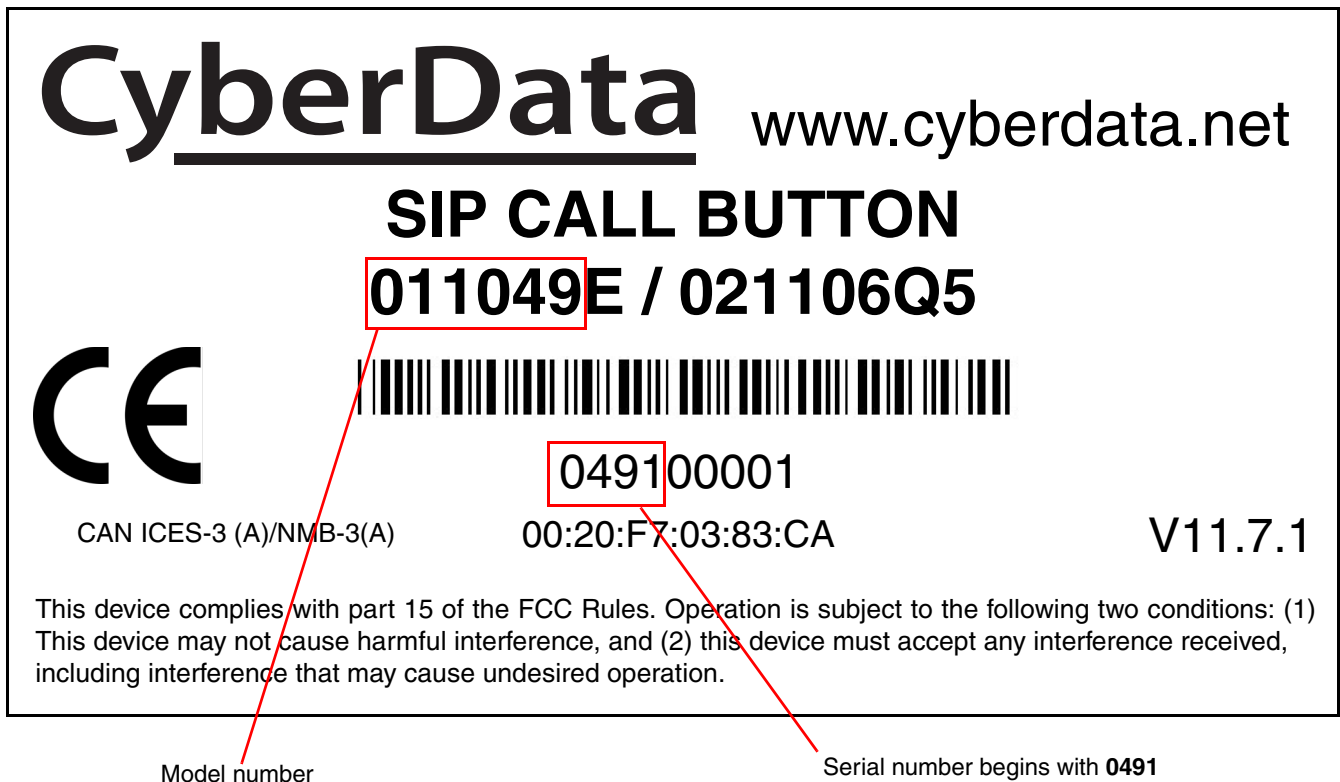
1 Product Overview

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 following figures illustrate how the SIP Call Button can be installed as part of a VoIP phone system.

Figure 1-2. Typical Installation

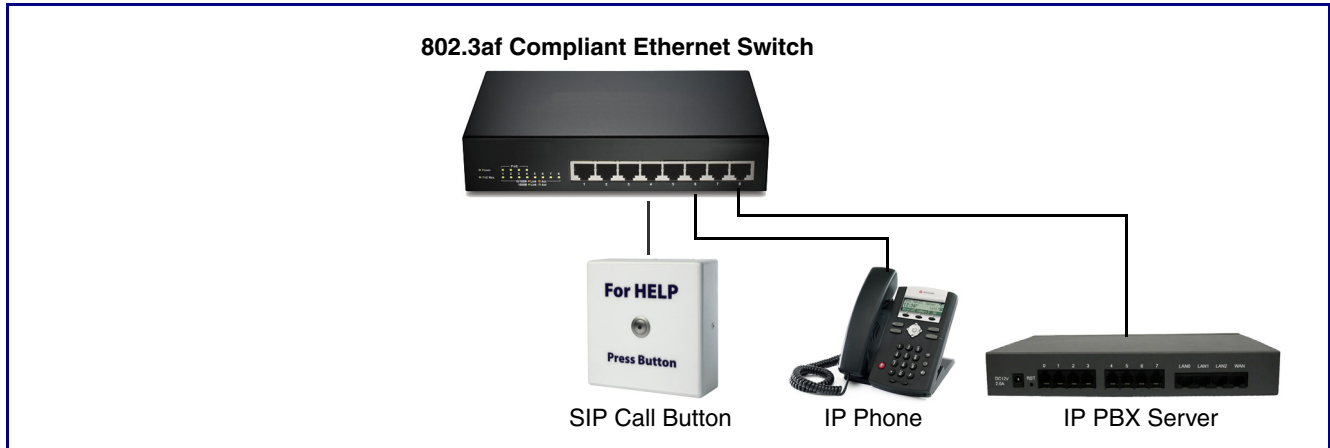


Figure 1-3. Installation with the Auxiliary RGB Strobe or the SIP RGB Strobe

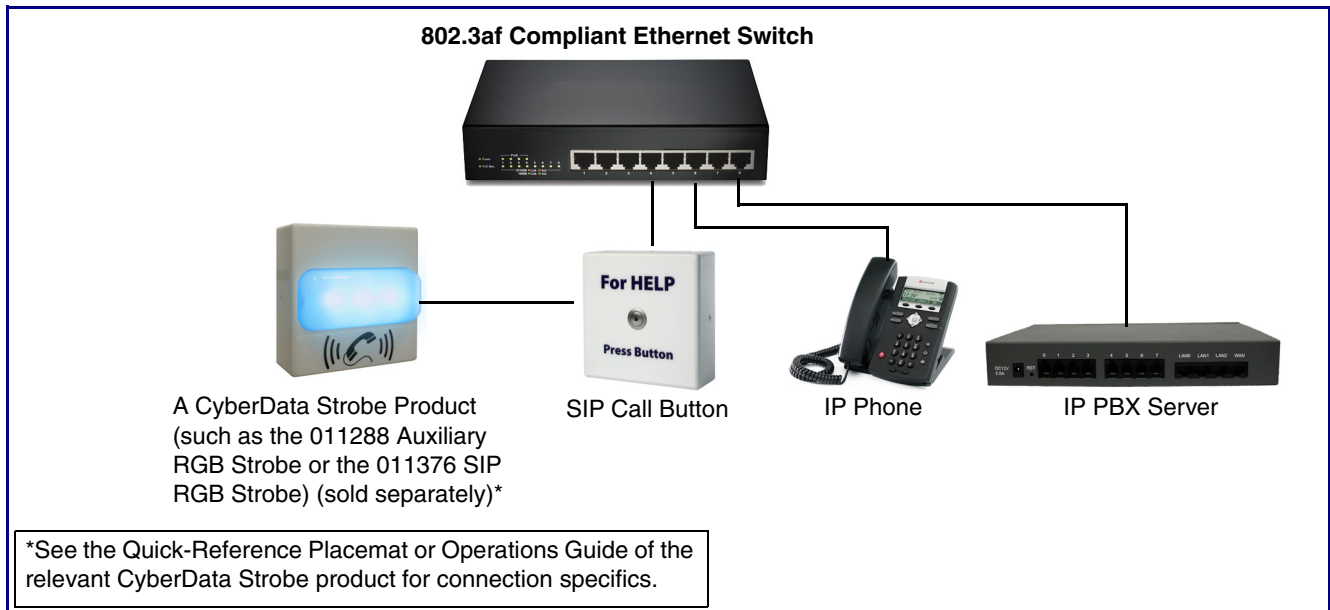


Figure 1-4. Installation with the Door Strike Relay Module

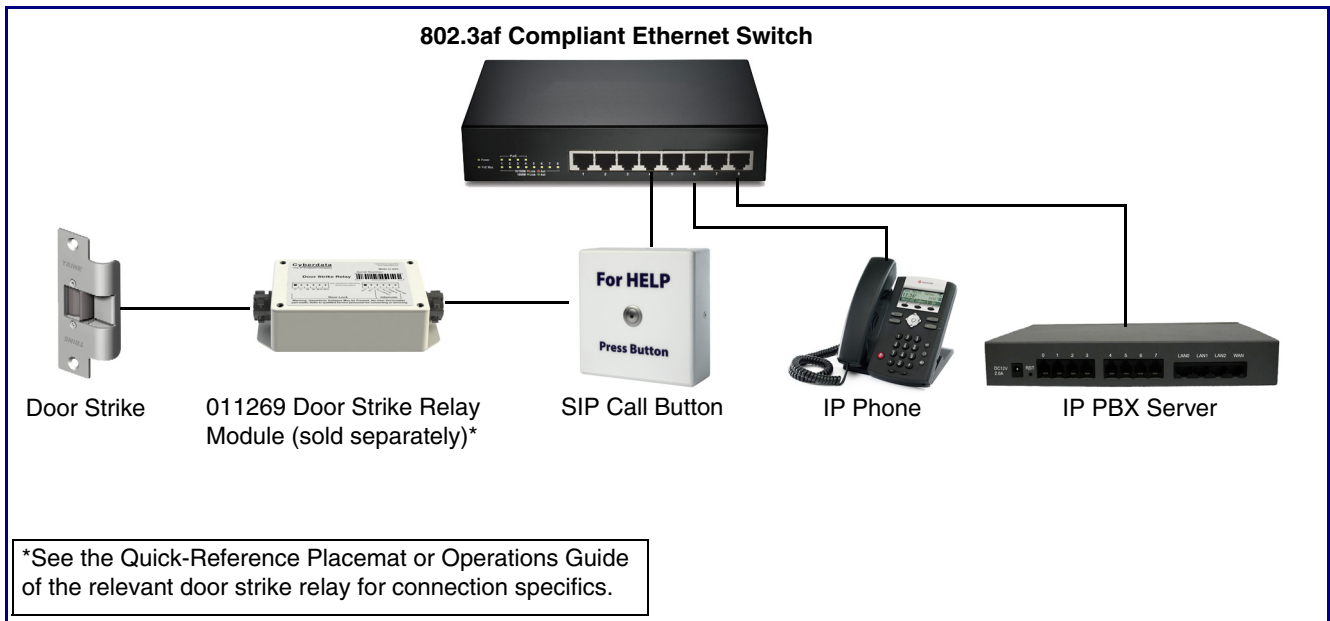
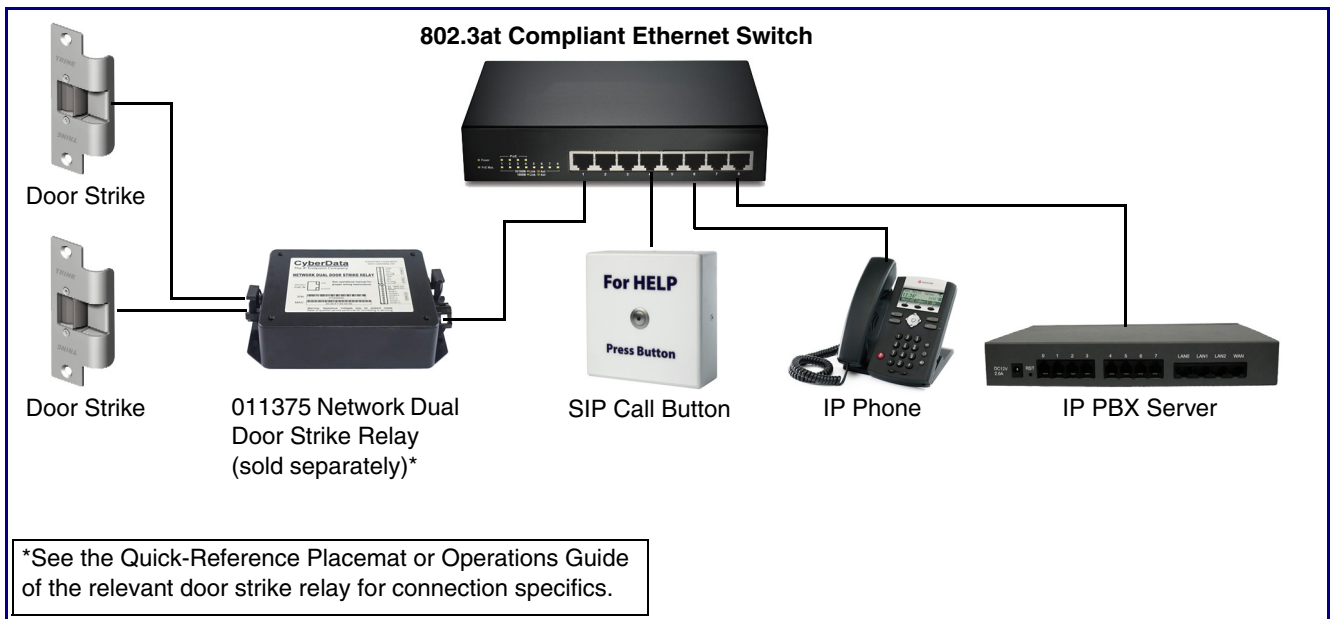


Figure 1-5. Installation with the Network Dual Door Strike Relay



1.3 Product Features

The SIP Call Button has the following features:

- Optional red/green/blue/white strobe kit connection available (part# 011288)
- Integrates with Network Dual Door Strike Relay Module (part# 011375) and Door Strike Relay Module (part# 011269)
- PoE 802.3af enabled (Power-over-Ethernet)
- SIP compliant
- Now supports SRST (Survivable Remote Site Telephony) in a Cisco environment
- Streamlined case design
- Network web management and firmware download
- Network adjustable speaker volume
- Concurrent SIP and multicast paging
- Dry relay contact for auxiliary control
- Door closure and tamper alert signal
- User downloadable message up to 80 seconds
- Single button call to pre-set number
- Continuous repeat of message
- Call progress light

1.4 Supported Protocols

The SIP Call Button supports the following protocols:

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

Provides an intuitive user interface for easy system configuration and verification of SIP Call Button operations.

- DHCP Client

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

- TFTP Client

Facilitates hosting for the Autoprovisioning configuration file.

- RTP

- RTP/AVP - Audio Video Profile

- Facilitates autoprovisioning configuration values on boot

- Audio Encodings

PCMU (G.711 mu-law)

PCMA (G.711 A-law)

G.722

Packet Time 20 ms

1.5 Supported SIP Servers

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

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

1.6 Specifications

Table 1-1. Specifications

Specifications	
Ethernet I/F	10/100 Mbps
Protocol	SIP RFC 3261 Compatible
Power Input	PoE 802.3af compliant or +8 to +12VDC @ 1000mA Regulated Power Supply ^a
On-Board Relay	1A at 30 VDC
Operating Temperature	-10° C to 50° C (14° F to 122° F)
Payload Types	G711, A-law and μ -law, G.722
Dimensions ^b	4.53 inches [115 mm] Length 1.58 inches [40.2 mm] Width 4.53 inches [115 mm] Height
Weight	1.0 lbs. (0.45 kg)
Boxed Weight	2.0 lbs. (0.90 kg)
Compliance	CE; EMC Directive – Class A EN 55032 & EN 55024, LV Safety Directive – EN 60950-1, RoHS Compliant, FCC; Part 15 Class A, Industry Canada; ICES-3 Class A, IEEE 802.3 Compliant
Part Number	011049

a. Contacts 1 and 2 on the J3 terminal block are only for powering the device from a non-PoE 12VDC power source as an alternative to Network PoE power. Use of these contacts for any other purpose will damage the device and void the product warranty.

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

1.7 Compliance

1.7.1 CE Testing

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

1.7.2 FCC Statement




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

2 Installing the SIP 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 terminal block. This terminal block can accept 16 AWG gauge wire.

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


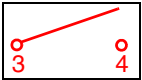
 <small>GENERAL ALERT</small>	<p>Caution</p> <p><i>Equipment Hazard:</i> Contacts 1 and 2 on the terminal block are only for powering the device from a non-PoE 12 VDC power source as an alternative to Network PoE power. Use of these contacts for any other purpose will damage the device and void the product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

Figure 2-1. Connections and Alternate Power Input

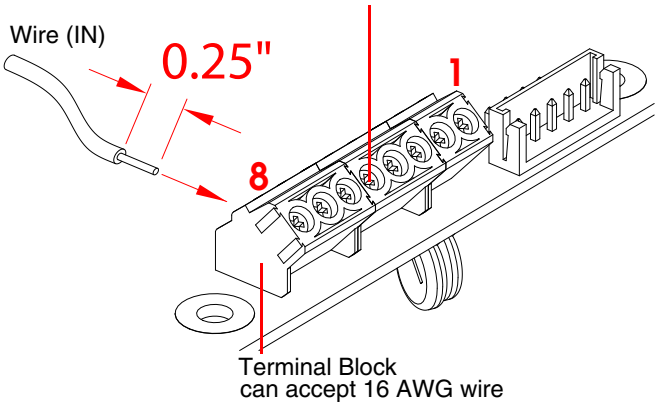
Alternate Power Input:
 1 = +8 to +12VDC @ 1000mA Regulated Power Supply*
 2 = Power Ground*



Relay Contact:
 (1 A at 30 VDC for continuous loads)
 3 = Relay Common
 4 = Relay Normally Open Contact
 5 = Sense Input
 6 = Sense Ground
 7 = Remote Switch "A"
 8 = Remote Switch "B"

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

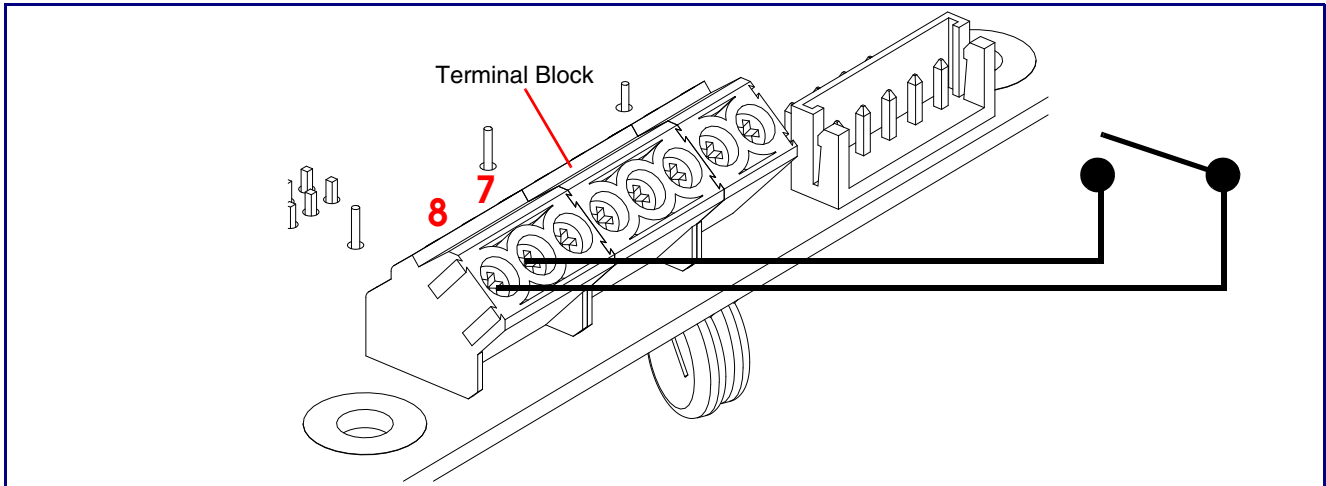
Use a 3.17 mm (1/8-inch) flat blade screwdriver for the terminal block screws






2.2.1.1 Remote Switch Connection

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

Figure 2-2. Remote Switch Connection



2.2.2 Using the On-Board Relay

 <p>GENERAL ALERT</p>	<p>Warning</p> <p><i>Electrical Hazard:</i> This product should be installed by a licensed electrician according to all local electrical and building codes.</p>
 <p>GENERAL ALERT</p>	<p>Warning</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>
 <p>GENERAL ALERT</p>	<p>Warning</p> <p><i>Electrical Hazard:</i> The relay does not support AC powered door strikes. Any use of this relay beyond its normal operating range can cause damage to the product and is not covered under our warranty policy.</p>

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

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

We highly recommend that inductive load and high current devices use our Networked Dual Door Strike Relay (CD# 011375) (see [Section 2.2.3.2, "Network Dual Door Strike Relay Wiring Diagram with External Power Source"](#)).

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

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

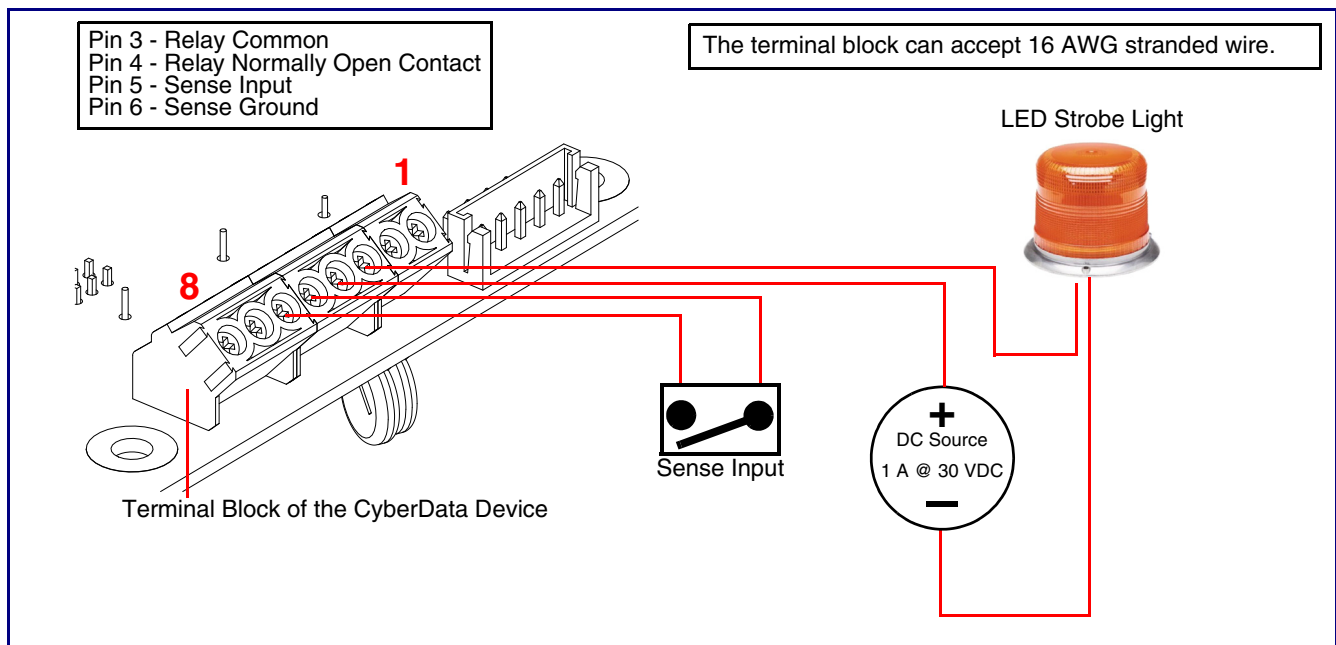
2.2.3 Wiring the Circuit

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 2-3](#) for the wiring diagram.

When configuring with an inductive load, please use an intermediary relay with a High PIV Ultrafast Switching Diode. We recommend using the Network Dual Door Strike Relay (CD# 011375) (see [Section 2.2.3.2, "Network Dual Door Strike Relay Wiring Diagram with External Power Source"](#)).

Figure 2-3. Devices Less than 1A at 30 VDC



2.2.3.2 Network Dual Door Strike Relay Wiring Diagram with External Power Source

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

This product provides an easier method of connecting standard door strikes as well as AC and higher voltage devices. See [Figure 2-4](#) and [Figure 2-5](#) for the wiring diagrams.


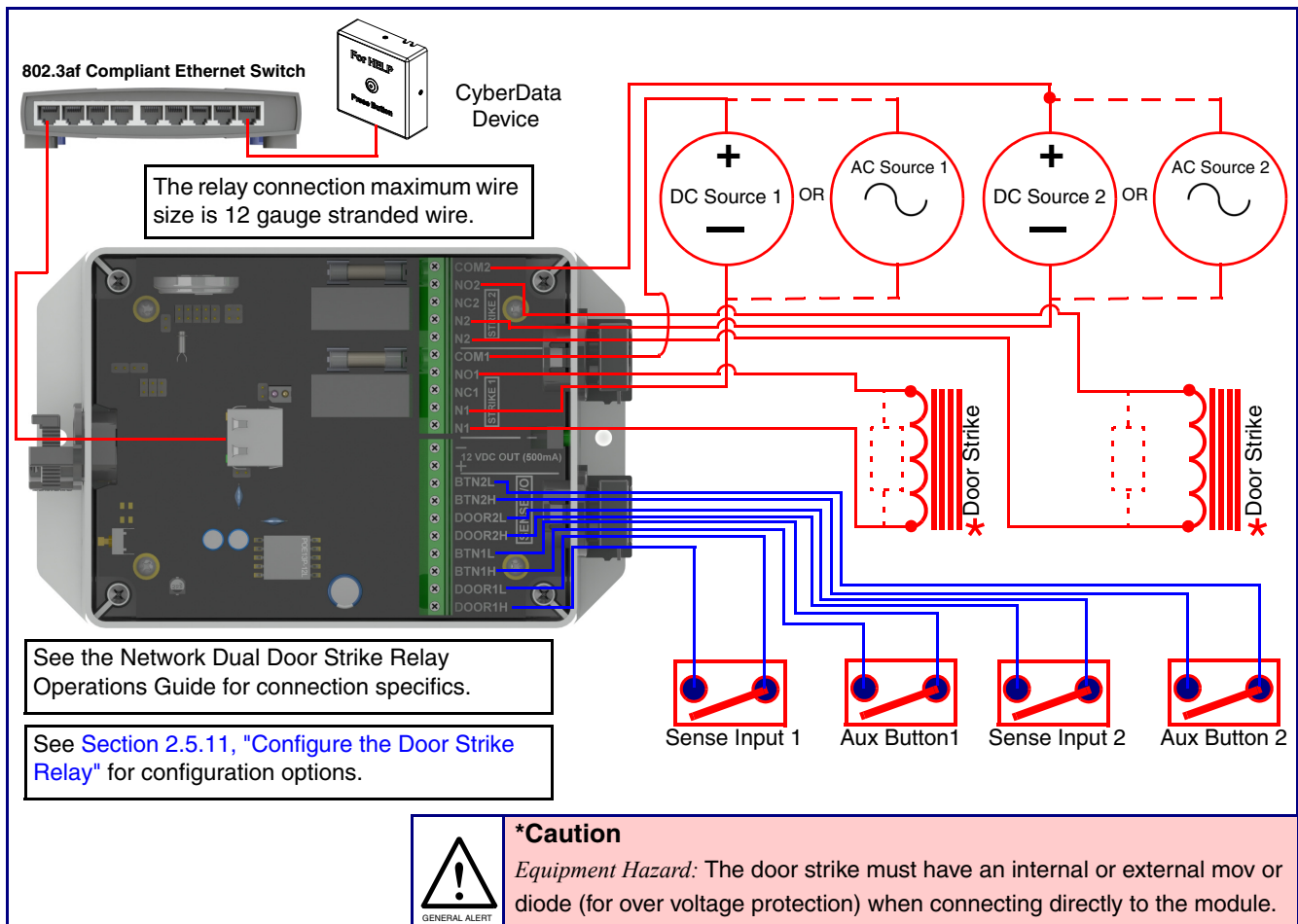
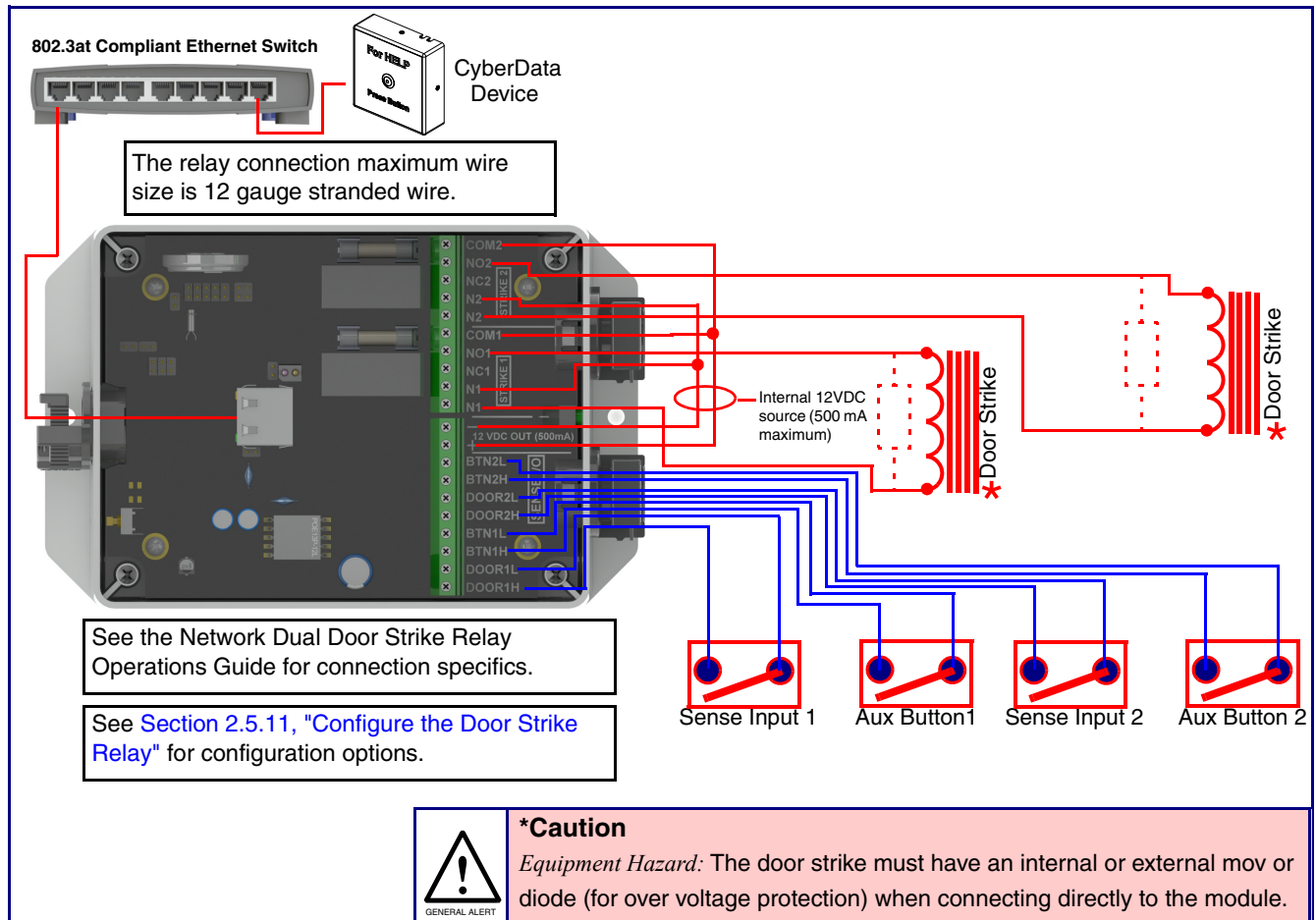
 GENERAL ALERT	<p>Warning</p> <p><i>Electrical Hazard:</i> Hazardous voltages may be present. No user serviceable part inside. Refer to qualified service personnel for connecting or servicing.</p>
--	--

Figure 2-4. Network Dual Door Strike Relay Wiring Diagram with External Power Source



2.2.3.3 Network Dual Door Strike Relay Wiring Diagram Using PoE+

Figure 2-5. Network Dual Door Strike Relay Wiring Diagram Using PoE+



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

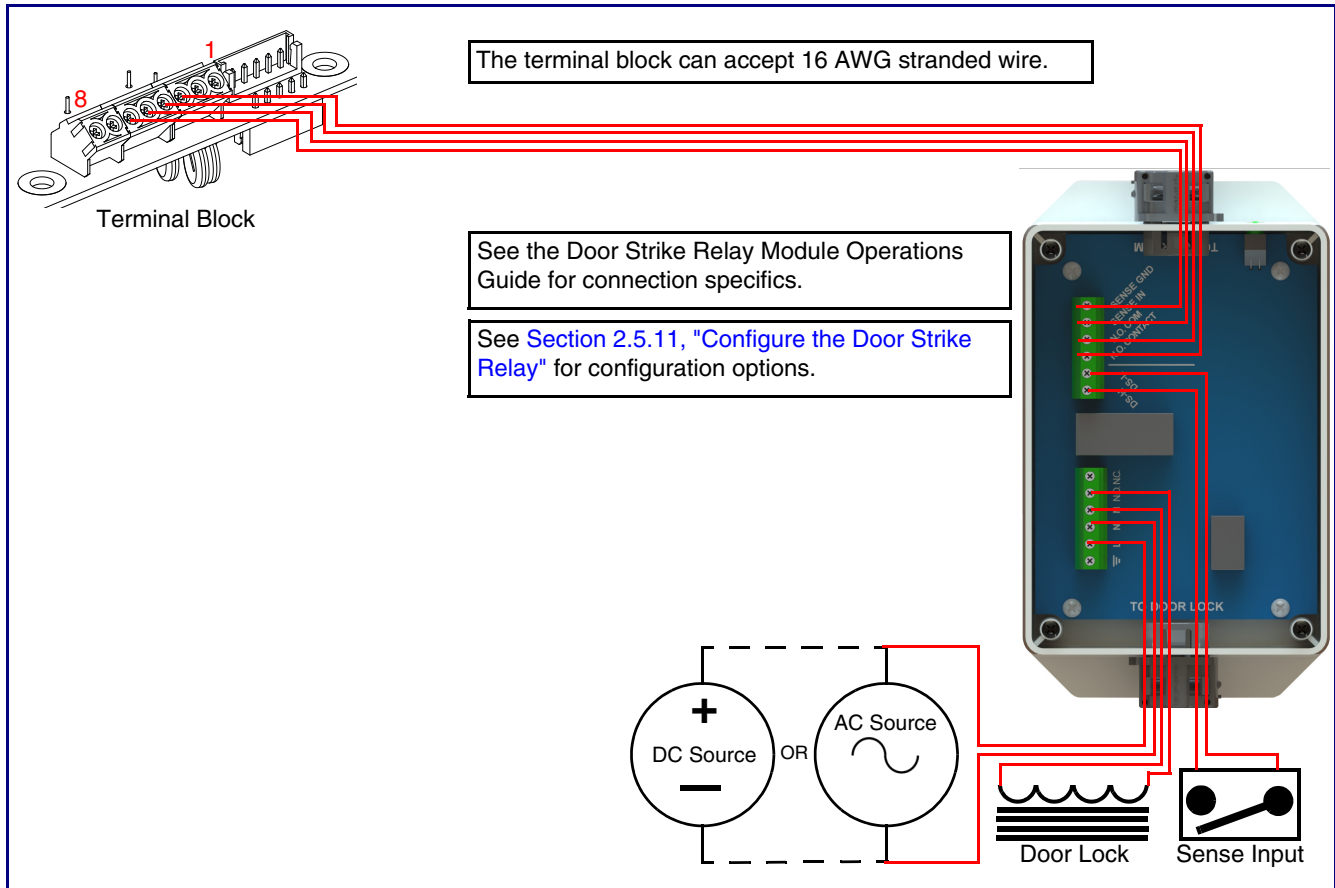
<http://support.cyberdata.net/>

2.2.3.4 Door Strike Relay Module Wiring Diagram from Device

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

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

Figure 2-6. Door Strike Relay Module Wiring Diagram from Device



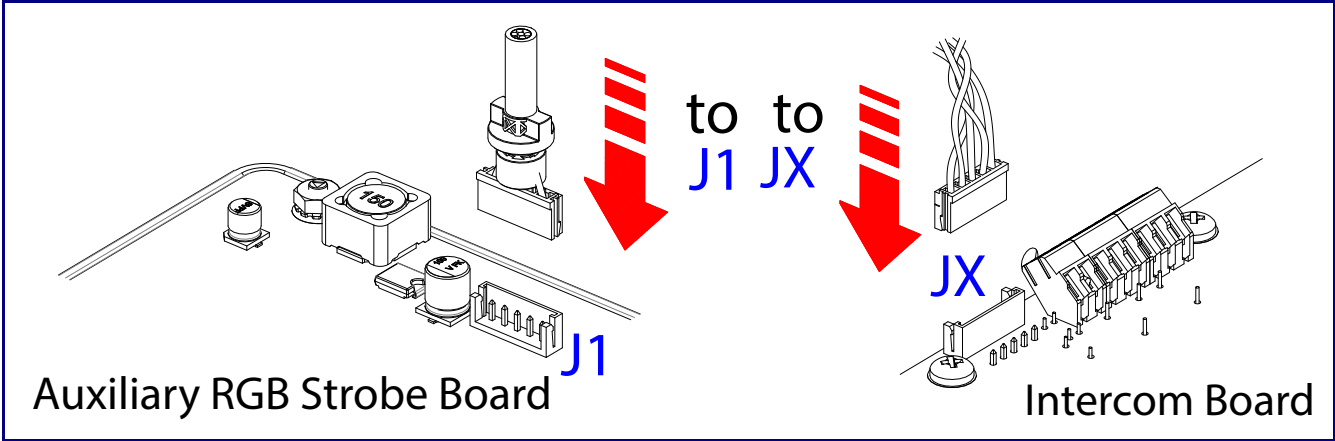
If you have questions about connecting door strikes or setting up the web configurable options, please contact our support department at the following website:

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

2.3 Connecting an Auxiliary RGB Strobe to the Device

1. Connect the strobe cable to the board of the Auxiliary RGB Strobe and the board of the device as shown in [Figure 2-7](#). Please see the Auxiliary RGB Strobe Operations Guide for more information about this product.

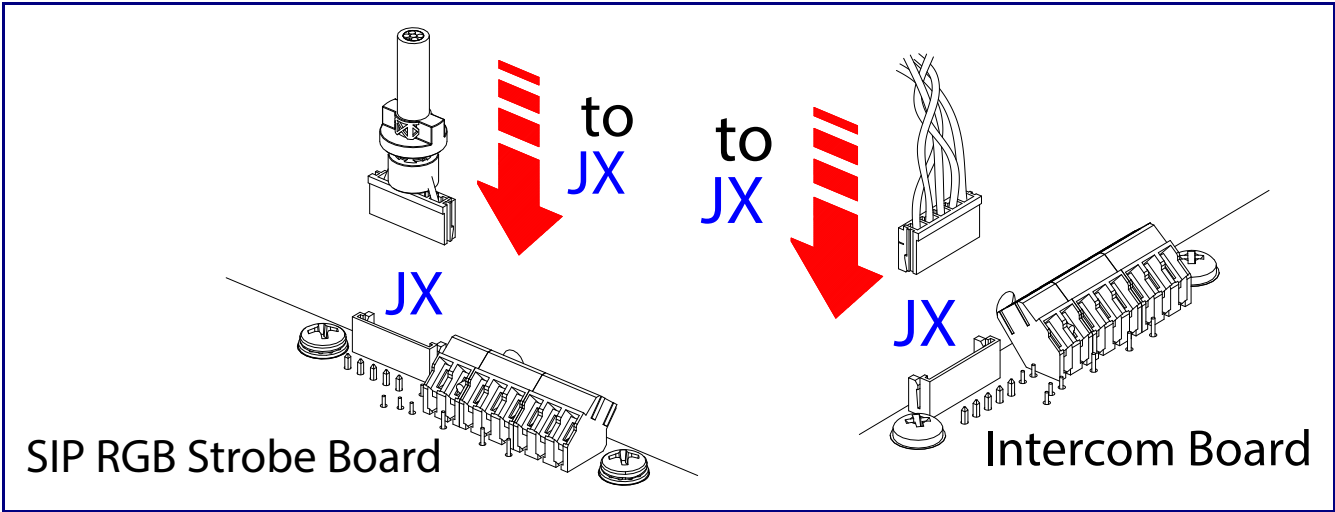
Figure 2-7. Connecting the Auxiliary RGB Strobe Kit to the Device



2.4 Connecting a SIP RGB Strobe to the Device

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

Figure 2-8. Connecting the SIP RGB Strobe to the Device



2.4.1 SIP Call Button Connectors

See the following figures and tables to identify the connectors and functions of the SIP Call Button.

Figure 2-9. Connector Locations

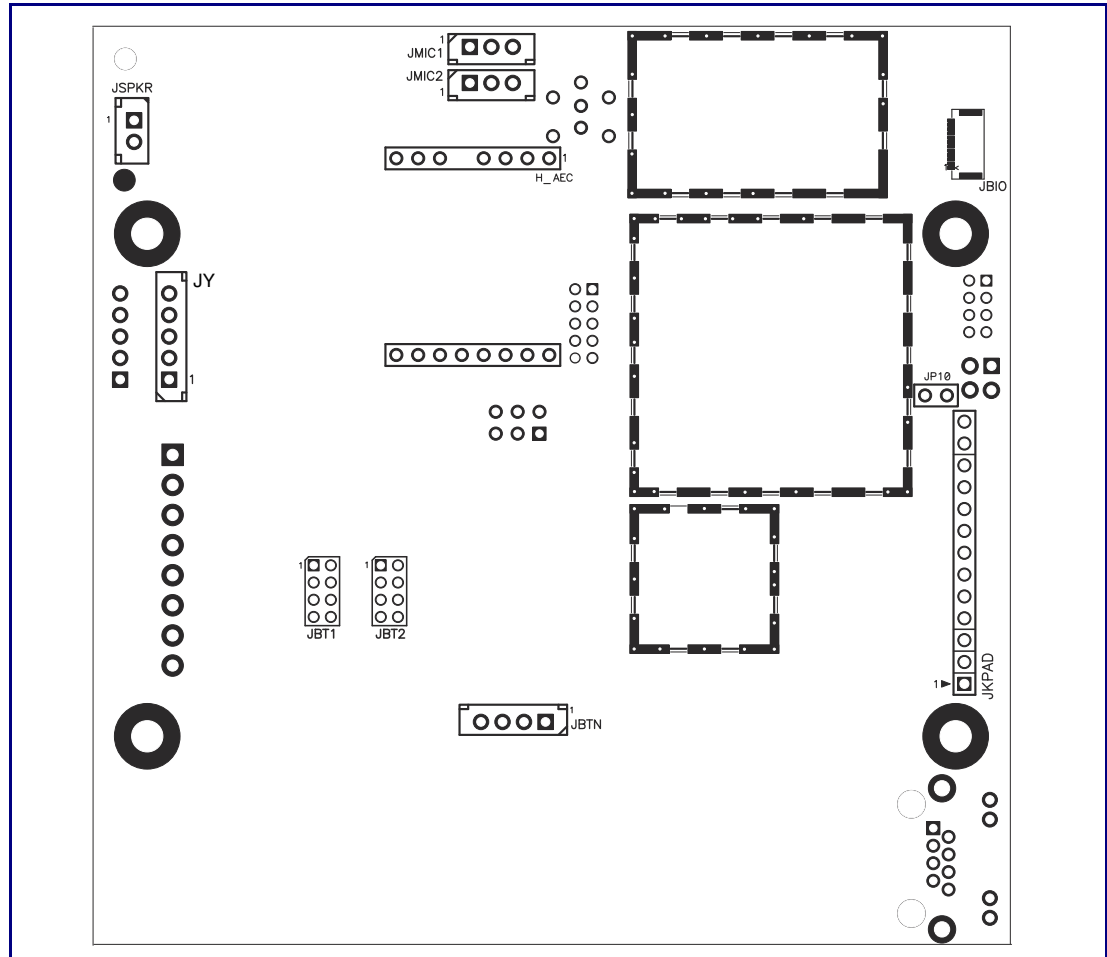


Table 2-2. Connector Functions

Connector	Function
JBTN	Call Button LED Interface
JMIC1	Microphone Interface
JSPKR	Speaker Interface
JKPAD	Keypad Interface (Not Used)
JY	I ² C 5V Peripheral Bus
JP10	Disables the intrusion sensor when installed.
JBT1	Touch Button — 1 Interface (Not Used)
JBT2	Touch Button — 2 Interface (Not Used)

Figure 2-10. Connector Locations

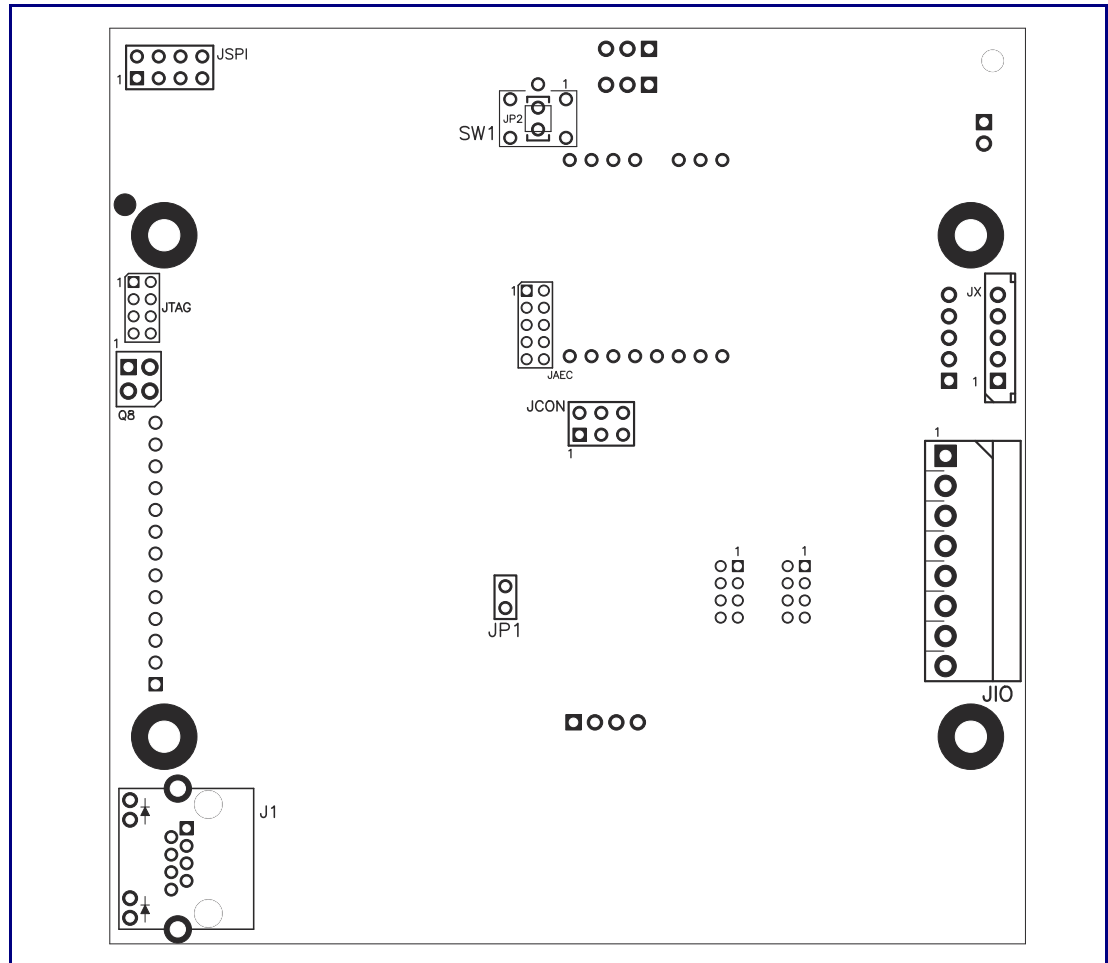


Table 2-3. Connector Functions

Connector	Function
J1	PoE Network Connection (RJ-45 ethernet)
JAEC	AEC Configuration Interface (Factory Use Only)
JIO	Terminal Block (see Figure 2-1)
JCON	Console Port (Factory Use Only)
JP1	Reset jumper ^a
JSPI	Reserved (Factory Use Only)
JTAG	JTAG (Factory Use Only)
JX	Auxiliary Strobe Connector
SW1	See Section 2.4.3, "RTFM Button"

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

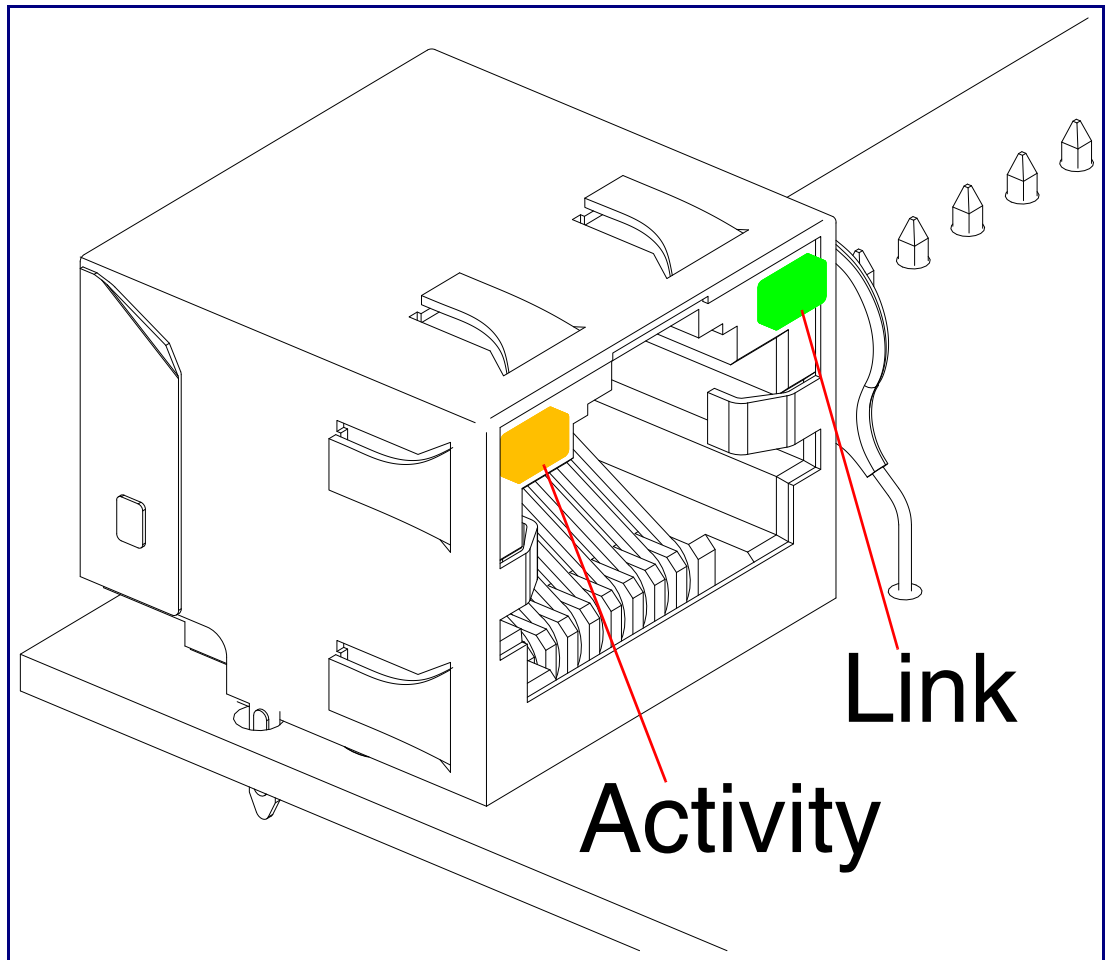
2.4.2 Activity and Link LEDs

2.4.2.1 Verifying the Network Connectivity and Data Rate

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

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

Figure 2-11. Activity and Link LED

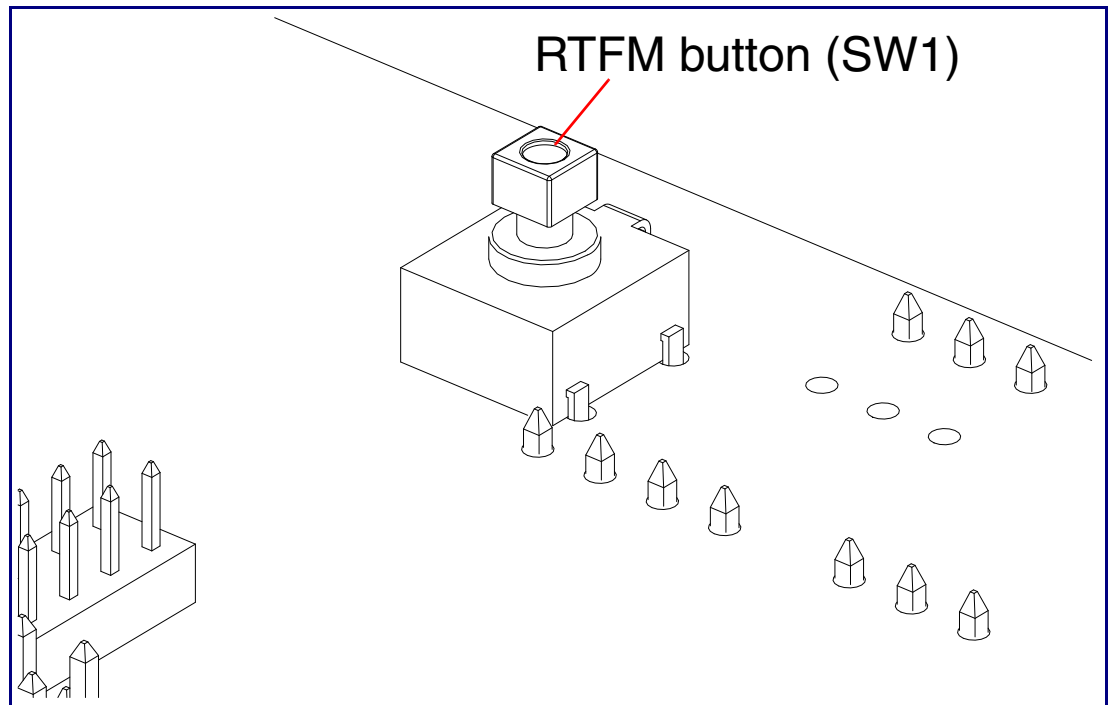


2.4.3 RTFM Button

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

Note You must do these tests prior to final assembly.

Figure 2-12. RTFM Button



2.4.3.1 Announcing the IP Address

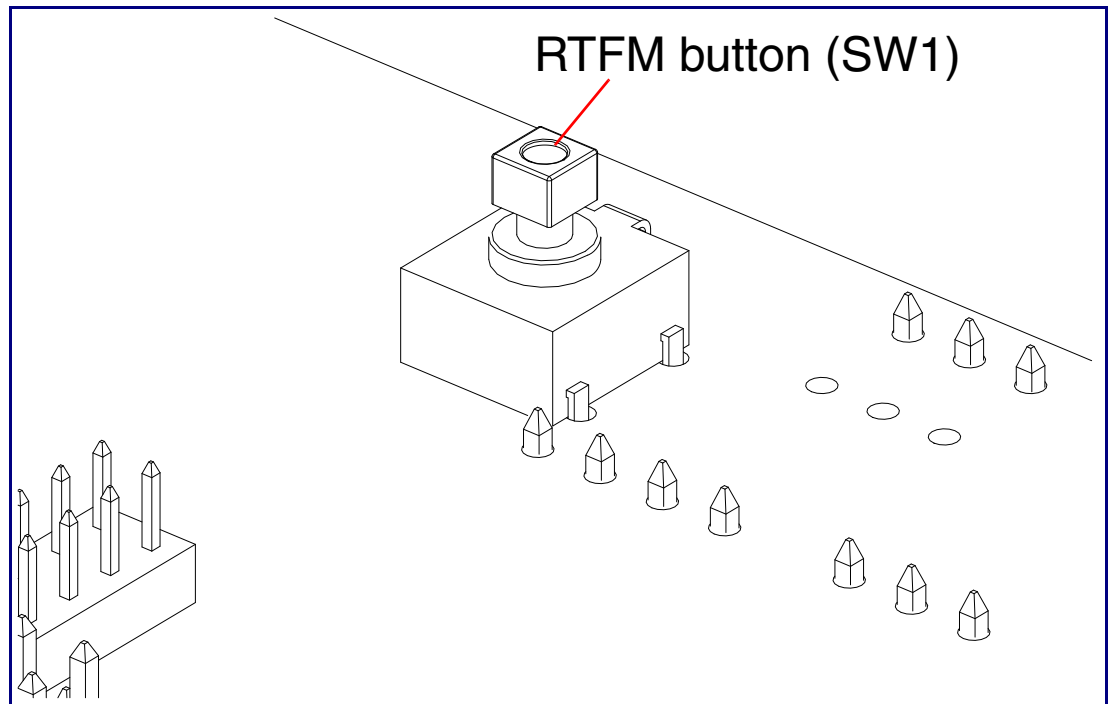
To announce a device's current IP address:

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

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

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

Figure 2-13. RTFM Button



2.4.3.2 Restoring the Factory Default Settings

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

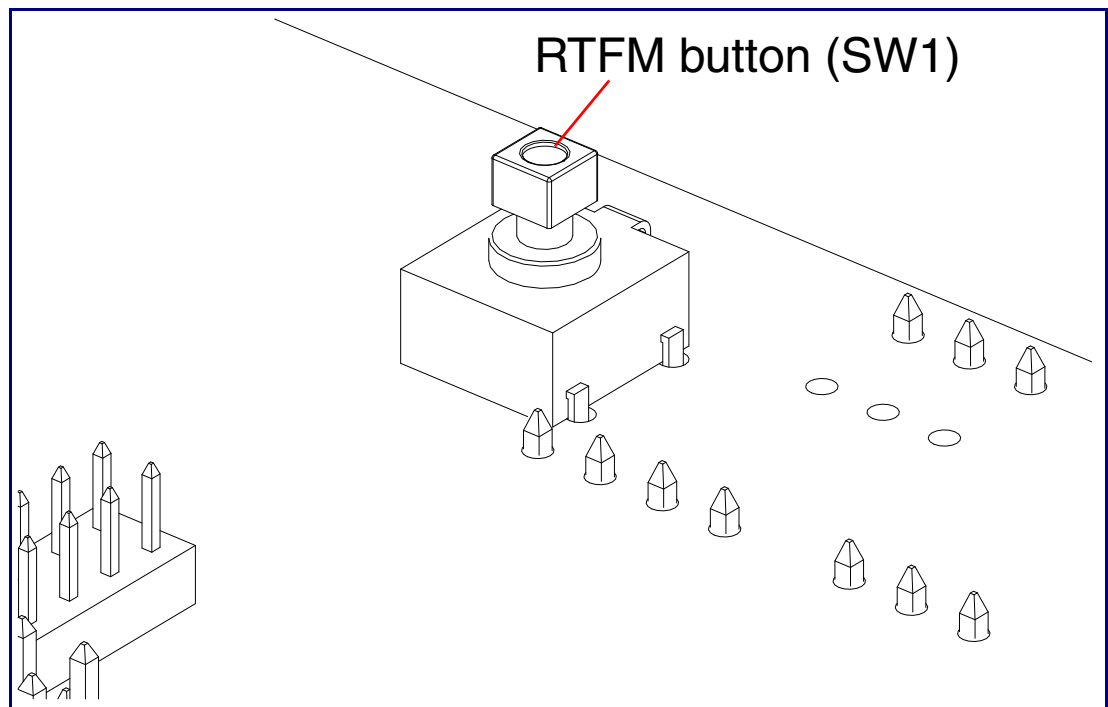
Note Each SIP Call Button is delivered with factory set default values.

To restore the factory default settings:

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

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

Figure 2-14. RTFM Button



2.4.4 Call Button and the Call Button LED

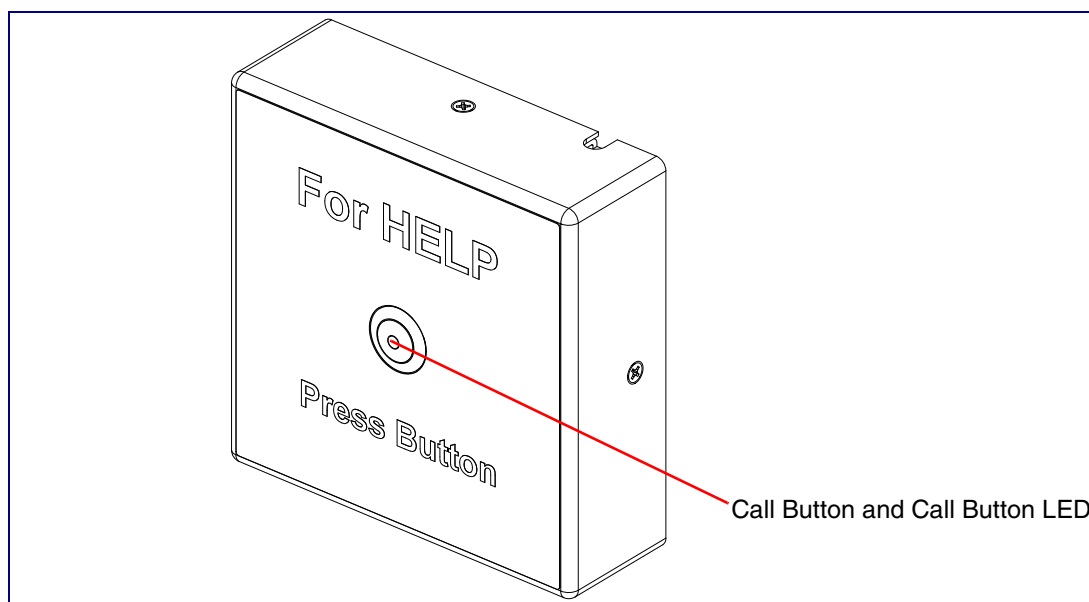
2.4.4.1 Calling with the The Call Button

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

2.4.4.2 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 2.5.5, "Configure the Device"](#)), there is an option called [Button Lit When Idle](#). This option sets the normal state for the indicator LED. The Call Button LED will still blink during initialization and calls.
- The Call Button LED flashes briefly at the beginning of RTFM mode.

Figure 2-15. Call Button and Call Button LED



2.5 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.

2.5.1 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

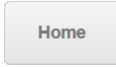
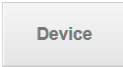
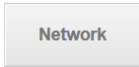


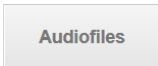
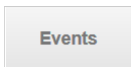

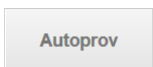
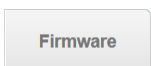
Parameter	Factory Default Setting
IP Addressing	DHCP
IP Address ^a	10.10.10.10
Web Access Username	admin
Web Access Password	admin
Subnet Mask ^a	255.0.0.0
Default Gateway ^a	10.0.0.1

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

2.5.2 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 Home page.
	Link to the Device page.
	Link to the Network page.
	Link to go to the SIP page.
	Link to the Sensor page.
	Link to the Audiofiles page.
	Link to the Events page.
	Link to the Door Strike Relay page.
	Link to the Autoprovisioning page.
	Link to the Firmware page.

2.5.3 Using the Toggle Help Button

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

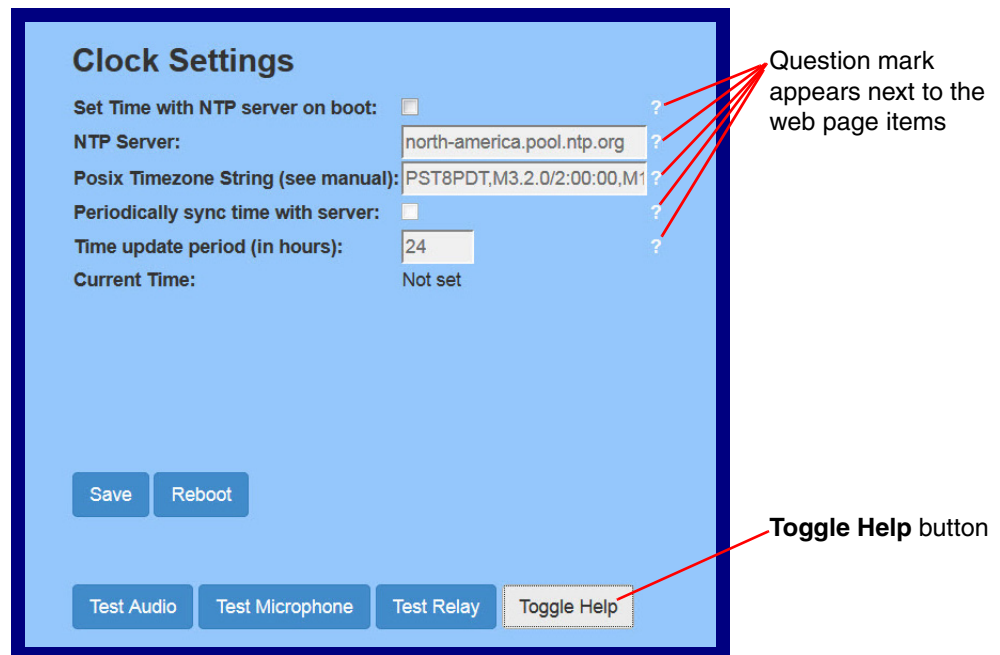
1. Click on the **Toggle Help** button that is on the UI webpage. See [Figure 2-16](#) and [Figure 2-17](#).

Figure 2-16. Toggle/Help Button



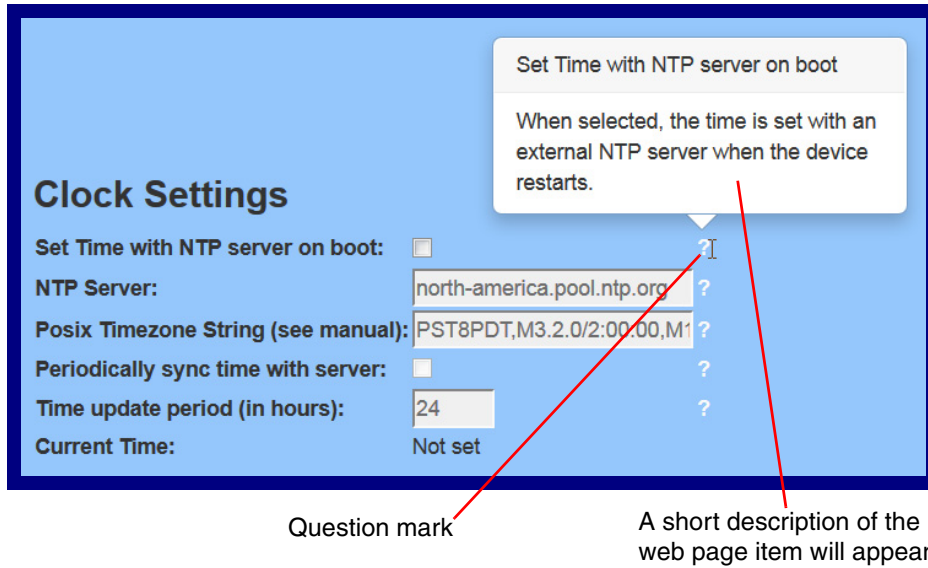
2. You will see a question mark (?) appear next to each web page item that has been provided with a short description by the Help feature. See [Figure 2-17](#).

Figure 2-17. Toggle Help Button and Question Marks



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

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



2.5.4 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/assets/common/discovery.zip>

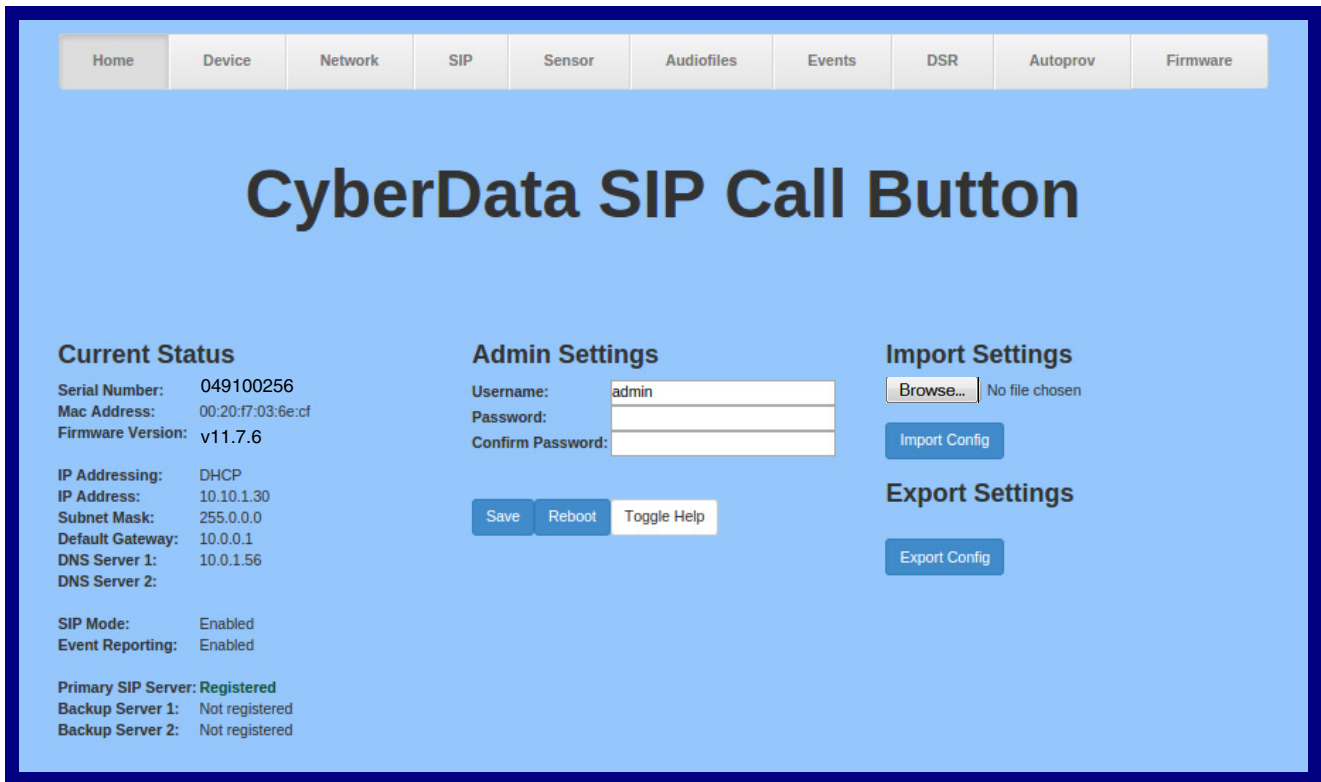
Note The device ships in DHCP mode. To get to the **Home** page, use the discovery utility to scan for the device on the network and open your browser from there.

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

Web Access Username: **admin**

Web Access Password: **admin**

Figure 2-19. Home Page



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

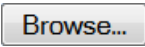




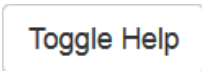
Web Page Item	Description
Admin Settings	
Username ?	The username to access the web interface. Enter up to 25 characters.
Password ?	The password to access the web interface. Enter up to 25 characters.
Confirm Password ?	Confirm the web interface password.
Current Status	
Serial Number	Shows the device serial number.
Mac Address	Shows the device Mac address.
Firmware Version	Shows the current firmware version.
IP Addressing	Shows the current IP addressing setting (DHCP or static).
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 Mode	Shows the current status of the SIP mode.
Event Reporting	Shows the current status of the Event Reporting 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.
Import Settings	
	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.
Export Settings	
	Click Export to export the current configuration to a file.
	Click the Save button to save your configuration settings. Note: You need to reboot for changes to take effect.
	Click on the Reboot button to reboot the system.

Table 2-6. Home Page Overview (continued)

Web Page Item	Description
 A rectangular button with rounded corners and a thin border. The text "Toggle Help" is centered inside the button in a dark blue font.	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help 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.

2.5.5 Configure the Device

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

Figure 2-20. Device Configuration Page

Home Device Network SIP Sensor Audiofiles Events DSR Autopro Firmware

CyberData SIP Call Button

Relay Settings

Activate Relay with DTMF code:

Relay Pulse Code:

Relay Pulse 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: 17:03:53

Misc Settings

Device Name:

Button Lit when Idle:

Button Brightness (0-255):

Prevent Call Termination:

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
Relay Settings	
Activate Relay with DTMF Code ?	Activates the relay when the DTMF Activation Code is entered on the phone during a SIP call with the device. RFC2833 DTMF payload types are supported.
Relay Pulse Code ?	DTMF code used to pulse the relay when entered on a phone during a SIP call with the device. Relay will activate for Relay Pulse Duration seconds then deactivate. Activate Relay with DTMF Code must be enabled. Enter up to 25 digits (* and # are supported).
Relay Pulse Duration (in seconds) ?	The length of time (in seconds) during which the relay will be activated when the DTMF Relay Activation Code is detected. Enter up to 5 digits.
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.
Misc Settings	
Device Name ?	Type the device name. Enter up to 25 characters.
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.
Prevent Call Termination ?	When this option is enabled, a call cannot be terminated using the call button.
Disable HTTPS (NOT recommended) ?	Disables the encrypted connection to the webpage. We do not recommend disabling HTTPS for security reasons.
Clock Settings	
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 Section 2.5.5.1, "Time Zone Strings" 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.

Table 2-7. Device Configuration Parameters (continued)

Web Page Item	Description
Current Time	Allows you to input the current time. (6 character limit)
	Click on the Test Relay button to do a relay test.
	Click the Save button to save your configuration settings. Note: You need to reboot for changes to take effect.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

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

Note The **NTP Server** setting needs to be restarted to spawn NTP or to change the server. Syncing and changing the **Time update period (in hours)** setting does not require a reboot for the changes to take effect.

Note None of the **Relay Settings** require a reboot for the changes to take effect.

Note The **Disable HTTPS (NOT recommended)** setting requires a reboot for the changes to take effect.

2.5.5.1 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 ^a	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 ^a	IST-9
Berlin ^b	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 2-21. 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)

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

2.5.6 Configure the Network Parameters

1. Click the **Networking** button to open the **Network Configuration** page (Figure 2-22).

Figure 2-22. Network Configuration Page

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

CyberData SIP Call Button

Stored Network Settings

Addressing Mode: Static DHCP

Hostname: SipDevice02b41d

IP Address: 10.10.10.10

Subnet Mask: 255.0.0.0

Default Gateway: 10.0.0.1

DNS Server 1: 10.0.0.1

DNS Server 2: 10.0.0.1

DHCP Timeout in seconds*: 60

* A value of -1 will retry forever

VLAN Settings

VLAN ID (0-4095): 0

VLAN Priority (0-7): 0

Save Reboot Toggle Help

Current Network Settings

IP Address: 10.10.0.16

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
Stored Network Settings	
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 Section 2.5.1, "Factory Default Settings" for factory default settings. Be sure to click Save and Reboot 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.
Current Network Settings	
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.
VLAN Settings	
VLAN ID (0-4095) ?	Specify the IEEE 802.1Q VLAN ID number. Enter up to 4 digits. Note: 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 Save button to save your configuration settings. Note: You need to reboot for changes to take effect.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help 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.

2.5.7 Configure the SIP Parameters

1. Click **SIP Config** to open the **SIP Configuration** page (Figure 2-23).

Figure 2-23. SIP Configuration Page

The screenshot shows the 'SIP Configuration' page for a CyberData SIP Call Button. The page has a navigation bar with tabs: Home, Device, Network, SIP (selected), Sensor, Audiofiles, Events, DSR, Autoprovisioning, and Firmware. The main title is 'CyberData SIP Call Button'. The page is divided into several sections:

- SIP Settings:** Includes checkboxes for 'Enable SIP operation' (checked), 'Register with a SIP Server' (checked), and 'Use Cisco SRST' (unchecked). It also has input fields for 'Primary SIP Server' (10.0.0.253), 'Primary SIP User ID' (199), 'Primary SIP Auth ID' (199), and 'Primary SIP Auth Password' (masked with dots). There are also fields for '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', and 'Backup SIP Auth Password 2'.
- Dial Out Settings:** Includes input fields for 'Dial out Extension' (204), 'Extension ID' (id204), 'Send Multicast Audio' (unchecked), 'Multicast Address' (224.5.5.5), 'Multicast Port' (5050), and 'Repeat Message' (1).
- Call Disconnection:** Includes an input field for 'Terminate Call after delay' (0).
- Codec Selection:** Includes a 'Force Selected Codec' checkbox (unchecked) and a 'Codec' dropdown menu (PCMU (G.711, u-law)).
- RTP Settings:** Includes input fields for 'RTP Port (even)' (10500) and 'Jitter Buffer' (50).
- SIP Call Strobe Settings:** Includes a 'Blink Strobe during Call' checkbox (unchecked) and a table for strobe settings:

Scene	Color	Brightness	Red	Green	Blue
ADA	White	100	0	0	0

Buttons for 'Save', 'Reboot', and 'Toggle Help' are located at the bottom left. A callout box at the bottom right states: 'The strobe settings will only appear if a CyberData Strobe product is connected to your device. If a CyberData Strobe product is not connected to your device, you will not see the strobe settings.'

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

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
SIP Settings	
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 SIP Operation and disable Register with a SIP Server (see Section 2.5.7.3, "Point-to-Point Configuration").
Use Cisco SRST ?	When enabled, the backup servers are handled according to Cisco SRST (Survivable Remote Site Telephony). It is required for use in clustered Cisco Unified Communications Manager topologies.
Primary SIP Server ?	Enter the SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the primary SIP server. This field can accept entries of up to 255 characters in length.
Primary SIP User ID ?	Specify the SIP User ID for the Primary SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the primary SIP server. Enter up to 64 alphanumeric characters.
Primary SIP Auth ID ?	Specify the Authenticate ID for the Primary SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Primary SIP Auth Password ?	Specify the Authenticate Password for the Primary SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Server 1 ?	Enter the backup SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the backup SIP server. This field can accept entries of up to 255 characters in length.
Backup SIP User ID 1 ?	Specify the SIP User ID for the first backup SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the first backup SIP server. Enter up to 64 alphanumeric characters.
Backup SIP Auth ID 1 ?	Specify the Authenticate ID for the first backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Auth Password 1 ?	Specify the Authenticate Password for the first backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Server 2 ?	Enter a second backup SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the second backup SIP server. This field can accept entries of up to 255 characters in length.
Backup SIP User ID 2 ?	Specify the SIP User ID for the second backup SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the second backup SIP server. Enter up to 64 alphanumeric characters.
Backup SIP Auth ID 2 ?	Specify the Authenticate ID for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.

Table 2-13. SIP Configuration Parameters (continued)

Web Page Item	Description
Backup SIP Auth Password 2 ?	Specify the Authenticate Password for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Remote SIP Port ?	The Remote SIP Port is the port number the device will use as the destination port when sending SIP messages. The default Remote SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
Local SIP Port ?	The Local SIP Port is the port number the device will use to receive SIP messages. The default Local SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
Outbound Proxy ?	Enter the Outbound Proxy address as an IPv4 address in dotted decimal notation or a fully qualified domain name (FQDN). When an IP address is configured, the device will send all SIP messages to this IP address. When an FQDN is configured, the device will run DNS NAPTR, SRV, and A queries on the FQDN to resolve an IP address to which it will send all SIP messages. This field can accept entries of up to 255 characters in length.
Outbound Proxy Port ?	The Outbound Proxy Port is port number used as the destination port when sending SIP messages to the outbound proxy. A value of 0 will default to 5060. The supported range is 0-65536. Enter up to 5 digits.
Disable rport Discovery ?	Disabling rport Discovery will prevent the device from including the public WAN IP address and port number in the contact information that is sent to the remote SIP servers. This will generally only need to be enabled when using an SBC or SIP ALG in conjunction with a remote SIP server.
Re-registration Interval (in seconds) ?	The SIP Re-registration interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
Unregister on Boot ?	When enabled, the device will send one registration with an expiry of 0 on boot.
Keep Alive Period ?	The minimum time in milliseconds between keep-alive packets sent for nat traversal. A value of 0 will disable keep alive packets.
SIP Call Strobe Settings	The following strobe settings will only appear if a CyberData Strobe product is connected to your device. If a CyberData Strobe product is not connected to your device, you will not see the strobe settings.
Blink Strobe during Call ?	When selected, the Strobe will blink a scene during a call.
Scene ?	Select desired scene (only one may be chosen).
ADA Compliant ?	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.
Slow Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink ?	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.
Fast Blink ?	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.
Color ?	Select desired color (only one may be chosen).
Brightness ?	How bright the strobe will blink when there is a SIP Call. This is the maximum brightness for "fade" type scenes.

Table 2-13. SIP Configuration Parameters (continued)

Web Page Item	Description
Red 	The red LED value for SIP Call.
Green 	The green LED value for SIP Call.
Blue 	The blue LED value for SIP Call.
	Use this button to preview the strobe flashing behavior for the SIP Call Strobe Settings .
Dial Out Settings	
Dial Out Extension 	Specify the extension the device will call when someone presses the Call button. Enter up to 64 alphanumeric characters. Note: For information about dial-out extension strings and DTMF tones, see Section 2.5.7.2, "Dial Out Extension Strings and DTMF Tones (using rfc2833)" .
Extension ID 	A Caller identification string added to outbound calls. Enter up to 64 alphanumeric characters.
Send Multicast Audio 	When selected, the device will play an audio file to the specified multicast address and port.
Multicast Address 	The multicast address used for multicasting an audio file.
Multicast Port 	The multicast port used for multicasting an audio file.
Repeat Message 	The number of times to repeat the audio message to the remote endpoint. Enter a value from 1-65536.
Call Disconnection	
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.
Codec Selection	
Force Selected Codec 	When configured, this option will allow you to force the device to negotiate for the selected codec. Otherwise, the device will perform codec negotiation using the default list of supported codecs.
Codec 	Select the desired codec (only one may be chosen).
RTP Settings	
RTP Port (even) 	Specify the port number used for the RTP stream after establishing a SIP call. This port number must be an even number and defaults to 10500. The supported range is 0-65536. Enter up to 5 digits.
Jitter Buffer 	Specify the size of the jitter buffer (in milliseconds) used for SIP calls. Valid values are 50-1000.
	Click the Save button to save your configuration settings. Note: You need to reboot for changes to take effect.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark () appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

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

Note The **Terminate Call After Delay** setting does not require a reboot for the changes to take effect.

2.5.7.1 Server Configurations

For specific server configurations, go to the following webpage:

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

2.5.7.2 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.

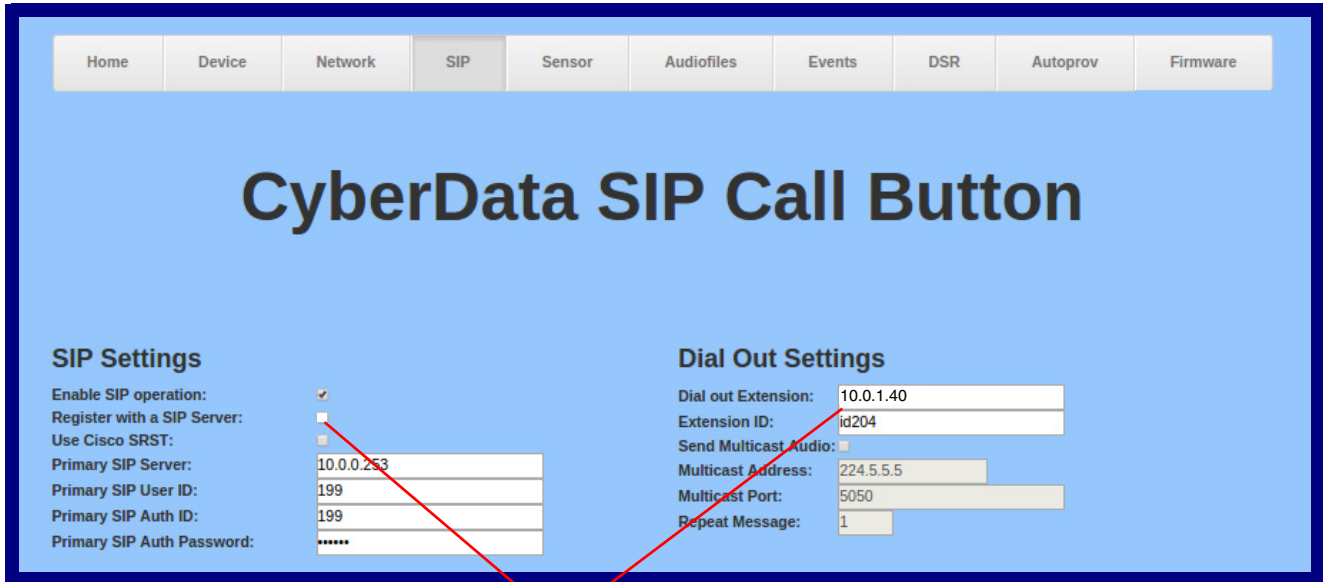
2.5.7.3 Point-to-Point Configuration

When the board is set to not register with a SIP server (see [Figure 2-24](#)), 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 2-24. SIP Configuration Page Set to Point-to-Point Mode



Device is set to NOT register with a SIP server

2.5.7.4 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.

2.5.8 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 2-25).

Figure 2-25. Sensor Configuration Page

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:

Sensor Strobe Settings

Blink Strobe on Sensor:

Scene	Color	Brightness	Red	Green	Blue	
ADA	White	100	0	255	255	Preview

Intrusion Sensor Strobe Settings

Blink Strobe on Intrusion Sensor:

Scene	Color	Brightness	Red	Green	Blue	
ADA	White	100	255	0	0	Preview

Save **Reboot** **Toggle Help**

Test Door Sensor **Test Intrusion Sensor**

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

2. On the **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
Door Sensor Settings	
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 Dial Out Extension 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 Dial Out Extension and play an audio file to the phone answering the SIP call (corresponds to Door Ajar on the Audiofiles page).
Sensor Strobe Settings	
The following strobe settings will only appear if a CyberData Strobe product is connected to your device. If a CyberData Strobe product is not connected to your device, you will not see the strobe settings.	
Blink Strobe on Sensor ?	When selected, the Strobe will blink a scene when the sensor is triggered.
Scene ?	Select desired scene (only one may be chosen).
ADA Compliant ?	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.
Slow Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink ?	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.
Fast Blink ?	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.
Color ?	Select desired color (only one may be chosen).

Table 2-16. Sensor Configuration Parameters (continued)













Web Page Item	Description
Brightness ?	How bright the strobe will blink when the sensor is triggered. This is the maximum brightness for “fade” type scenes.
Red ?	The red LED value for the Sensor.
Green ?	The green LED value for the Sensor.
Blue ?	The blue LED value for the Sensor.
	Use this button to preview the strobe flashing behavior for the Sensor Strobe Settings .
Intrusion Sensor Settings	
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 Dial Out Extension 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 Dial Out Extension and play an audio file (corresponds to Intrusion Sensor Triggered on the Audiofiles page) to the phone answering the SIP call when the intrusion sensor is activated.
Intrusion Sensor Strobe Settings	
The following strobe settings will only appear if a CyberData Strobe product is connected to your device. If a CyberData Strobe product is not connected to your device, you will not see the strobe settings.	
Blink Strobe on Intrusion Sensor ?	When selected, the Strobe will blink a scene when the intrusion sensor is triggered.
Scene ?	Select desired scene (only one may be chosen).
ADA Compliant ?	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.
Slow Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink ?	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.
Fast Blink ?	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.
Color ?	Select desired color (only one may be chosen).

Table 2-16. Sensor Configuration Parameters (continued)

Web Page Item	Description
Brightness 	How bright the strobe will blink when the intrusion sensor is triggered. This is the maximum brightness for “fade” type scenes.
Red 	The red LED value for the Intrusion Sensor.
Green 	The green LED value for the Intrusion Sensor.
Blue 	The blue LED value for the Intrusion Sensor.
	Use this button to preview the strobe flashing behavior for the Intrusion Sensor Strobe Settings .
	Click the Test Door Sensor button to test the door sensor.
	Click the Test Intrusion Sensor button to test the Intrusion sensor.
	Click the Save button to save your configuration settings. Note: You need to reboot for changes to take effect.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark () appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

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

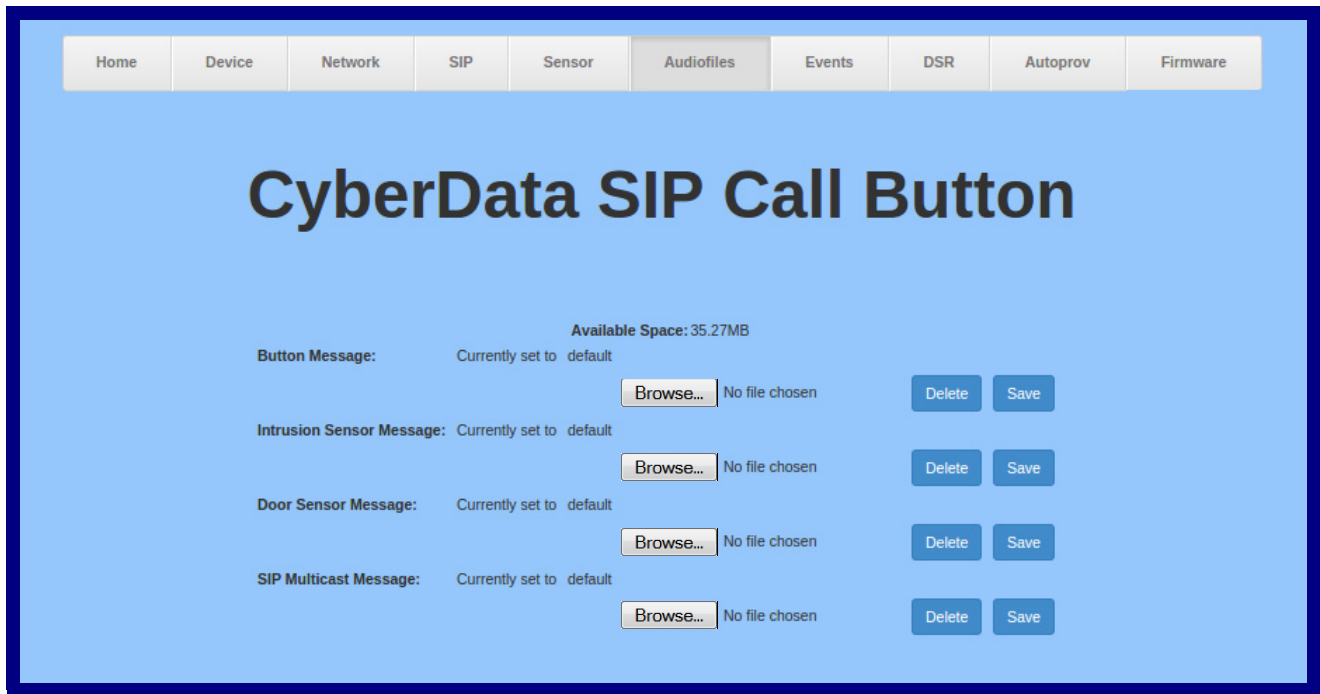
Note None of the **Sensor Configuration Page** settings require a reboot for the changes to take effect.

2.5.9 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 2-26).

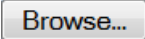


Figure 2-26. Audio Configuration Page



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.
Button Message	Corresponds to the message "Customer Service Needed" when a call is initiated from the call button.
Intrusion Sensor Message	Corresponds to the message "Intrusion Sensor Triggered."
Door Sensor Message	Corresponds to the message "Door Ajar."
SIP Multicast Message	This is the message that plays when multicast audio is initiated by the call button.
	Click on the Browse button to navigate to and select an audio file.
	The Delete button will delete any user uploaded audio and restore the stock audio file.
	The Save button will download a new user audio file to the board once you've selected the file by using the Browse button. The Save button will delete any pre-existing user-uploaded audio files.

2.5.9.1 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 2-27](#) through [Figure 2-29](#).

Figure 2-27. Audacity 1

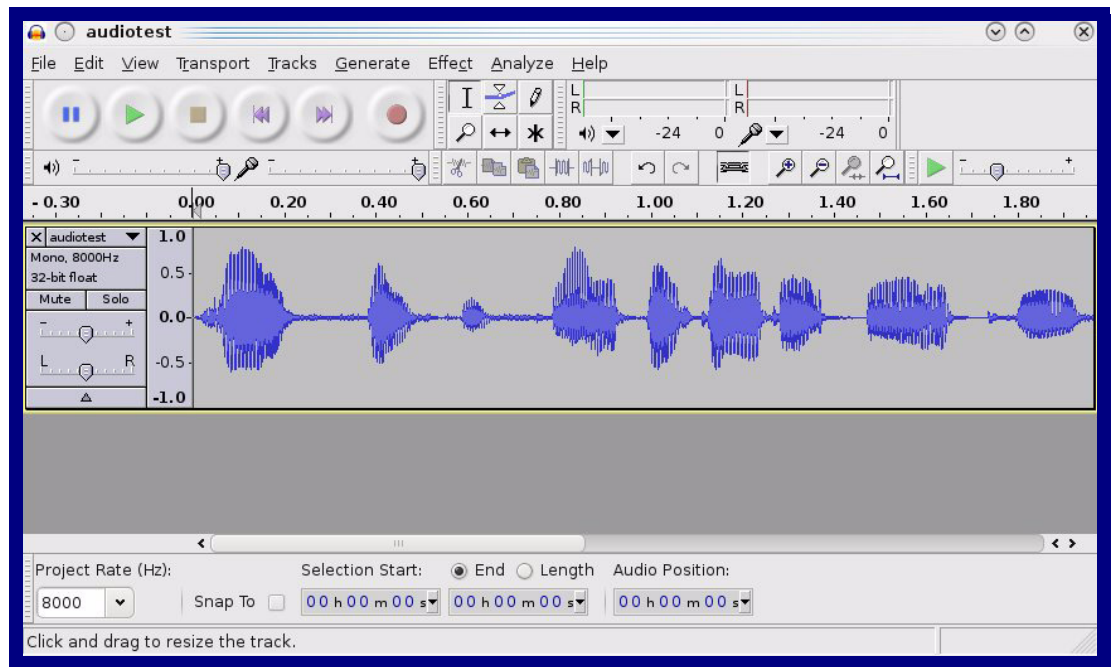
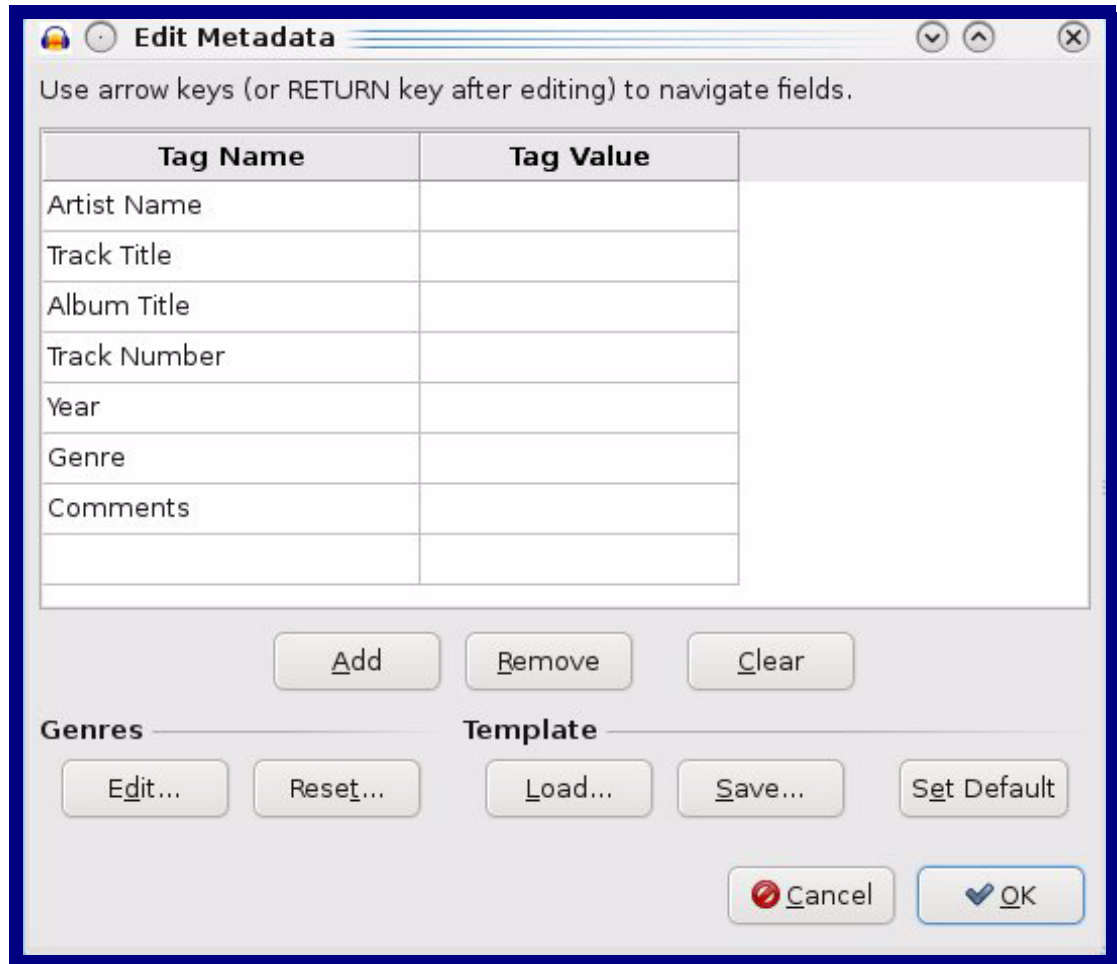


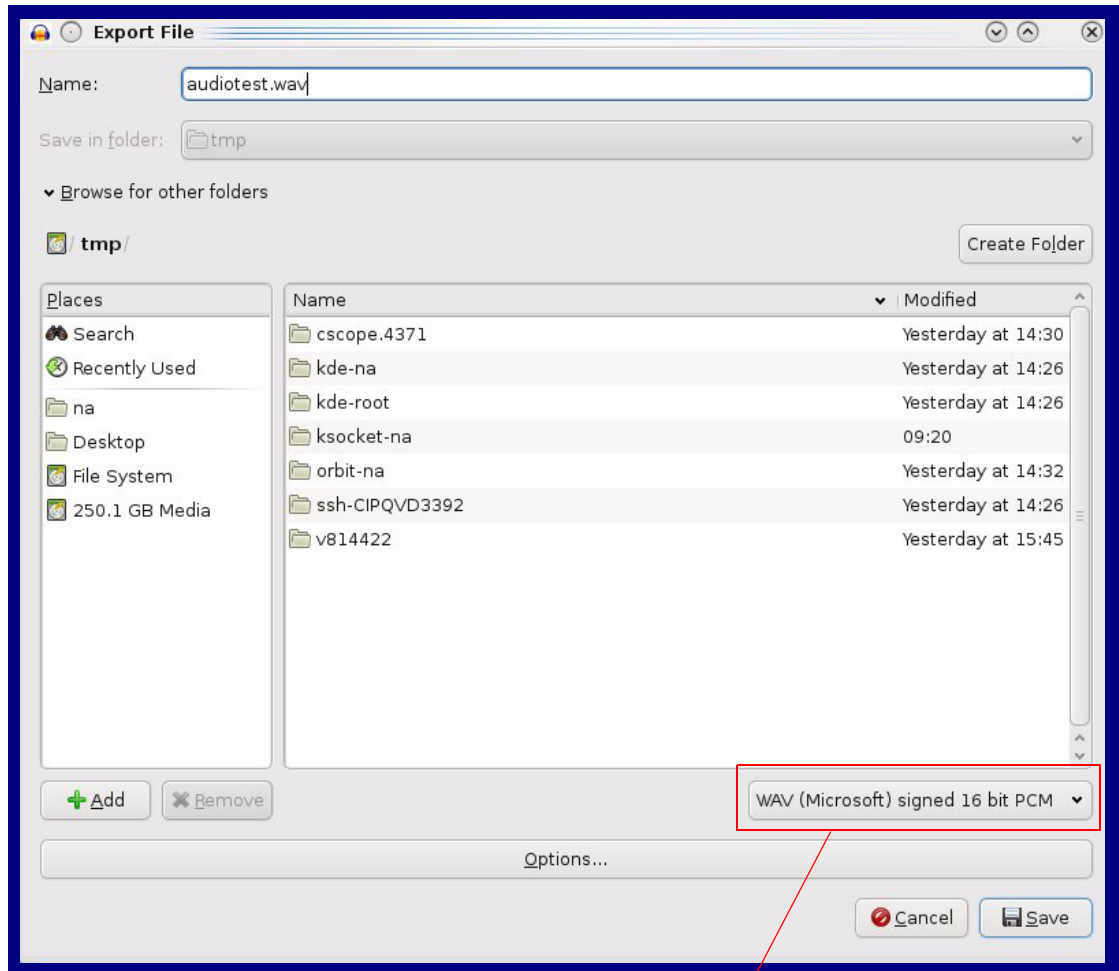
Figure 2-28. Audacity 2



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

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

Figure 2-29. WAV (Microsoft) signed 16 bit PCM



WAV (Microsoft) signed 16 bit PCM

2.5.10 Configure the Event Parameters

1. Click the **Event Config** button to open the **Event Configuration** page (Figure 2-30). 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 2-30. 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:



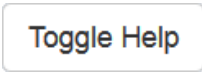
Server Port:

Server URL:

- 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.
Events	
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 Check All to select all of the events on the page.
Uncheck All	Click on Uncheck All to de-select all of the events on the page.
Event Server	
Server IP Address ?	The IPv4 address of the event server in dotted decimal notation.
Server Port ?	Specify the event server port number. The supported range is 0-65536. Enter up to 5 digits.
Server URL ?	Generally, the destination URL is the name of the application that receives the events and the string in the HTTP POST command. It can be a script used to parse and process the HTTP POST events. Enter up to 127 characters.
	Click the Save button to save your configuration settings. Note: You need to reboot for changes to take effect.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help 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.

2.5.10.1 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>
```

2.5.11 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, manually through the web interface, or by using a Windows application.

This section describes operations for running firmware version 4.8 or later of the Dual Door Strike Relay. If you have an older version of the firmware, then please contact CyberData Technical Support. The version number appears in the **Discovered Remote Relays** section on the **DSR** page (Figure 2-31).

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

Figure 2-31. DSR Page (not associated with any DSRs)

Remote Relay Settings
 Not associated with any DSRs

Save Reboot Toggle Help

Discovered Remote Relays

Product Type	IP Address	MAC Address	Serial Number	Name	Version		
DoorLock	10.10.1.45	00:20:F7:02:A7:9A	270000004	LOCK270000004	V2.2AM	View	Associate
DoorLock	10.10.1.179	00:20:F7:02:A7:E2	270000078	LOCK270000078	V2.0A	View	Associate
DoorLock	10.10.1.19	00:20:F7:03:54:BE	375000016	LOCK375000016	V4.8T	View	Associate

Cache age: 00:09



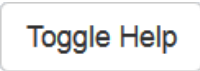




Discover

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

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

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

Table 2-19. DSR Configuration Parameters (not associated with any DSRs)

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

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

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

2.5.12 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 2-32](#).

Figure 2-32. 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): 0

Autoprovision at time (HHMMSS):

Autoprovision when idle (in minutes > 10): 0

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

Autoprovisioning happens on boot.

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

If these haven't been configured, it will look for an autoprovisioning server in your list of DHCP options and try to download '0020f7036ecf.xml' and if this fails, '00000cd.xml'.

Save Reboot Toggle Help

Download Template

Autoprovisioning log

```
00:00 Autoprovisioning Device...
00:00 Autoprov found option 43 in DHCP server="http://chalmers.cyberdata.net"
00:00 Autoprov looking for 0020f7036ecf.xml at http://chalmers.cyberdata.net
00:00 Autoprov looking for 00000cd.xml at http://chalmers.cyberdata.net
00:00 Failed to fetch autoprov file
00:00 Autoprov found option 72 in DHCP server="10.0.1.118"
00:00 Autoprov looking for 0020f7036ecf.xml at 10.0.1.118
00:00 Autoprov looking for 00000cd.xml at 10.0.1.118
00:00 Failed to fetch autoprov file
00:00 Autoprov found option 150 in DHCP server="10.0.5.120"
00:00 Autoprov looking for 0020f7036ecf.xml at 10.0.5.120
```

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

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

Table 2-20. Autoprovisioning Configuration Parameters





Web Page Item	Description
Disable Autoprovisioning ?	Prevent the device from automatically trying to download a configuration file. See Section 2.5.12.1, "Autoprovisioning" 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 <mac address>.xml.</p> <p>Supported filename extensions are .txt, and .xml. The current filename is denoted by an asterisk at the bottom of the Autoprovisioning Page. 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>Note: To use the auto update options, enable the Set Time with NTP Server on boot setting on the Device Configuration Page page (see Table 2-7).</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>Note: To use the auto update options, enable the Set Time with NTP Server on boot setting on the Device Configuration Page page (see Table 2-7).</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>Note: To use the auto update options, enable the Set Time with NTP Server on boot setting on the Device Configuration Page page (see Table 2-7).</p>
	<p>Click the Save button to save your configuration settings.</p> <p>Note: You need to reboot for changes to take effect.</p>

Table 2-20. Autoprovisioning Configuration Parameters (continued)

Web Page Item	Description
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help 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 Download Template button to create an autoprovisioning file for the device. See Section 2.5.12.3, "Download Template Button"
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.

2.5.12.1 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 2.5.12.2, "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 auto provisioning template file from the [Auto provisioning Page](#) using the **Download Template** button (see [Table 2-20](#)). This file contains every configuration option that can be set on the board.

Auto provisioning files can contain the whole configuration or a subset of this file. The first auto provisioning file can also contain links to other auto provisioning files.

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

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

After downloading the first auto provisioning file, the device will step through up to twenty additional <AutoproFile> 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 its name to 'Newname'.
2. It will try to download <http://example.com/common.xml>.
3. It will try to download http://example.com/sip_reg0020f7123456.xml.
4. It will try to download <http://example.com/audio0020f7123456>.
5. It will try to download <http://example.com/device.xml>.

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

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

Checking for New
Autoprovisioning
Files after Boot

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

The
 Autoprovisioning
 Filename

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

Table 2-21. 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-ceiling-speaker</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://autoprovttest.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://autoprovttest.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://autoprovttest.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://autoprovttest.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://autoprovttest.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 auto provisioning 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 auto provisioning 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 auto provisioned 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 auto provisioning 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 auto provisioning 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 auto provisioning file with “**default**” set as the file name.

2.5.12.2 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; }
}
```

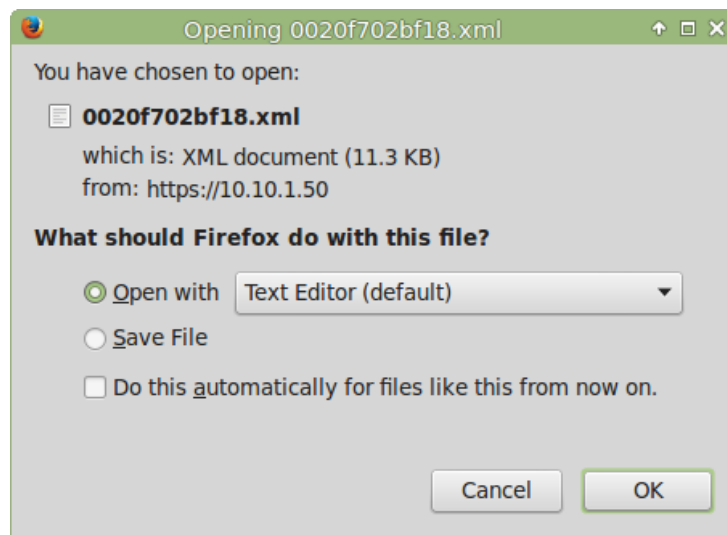
2.5.12.3 Download Template Button

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

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

1. On the **Auto provisioning** 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 2-33). 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 2-33.

Figure 2-33. Configuration File



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

2.5.13 Downloading the Firmware

To download the firmware to your computer:

1. Download the latest firmware file from the **Downloads** tab at the following webpage:
<http://www.cyberdata.net/voip/011049/>
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 2.5.4, "Log in to the Configuration Home Page"](#).
4. Click on the **Firmware** menu button to open the **Firmware** page. See [Figure 2-34](#).

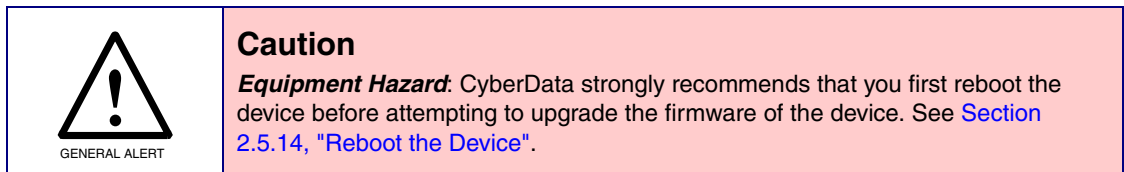
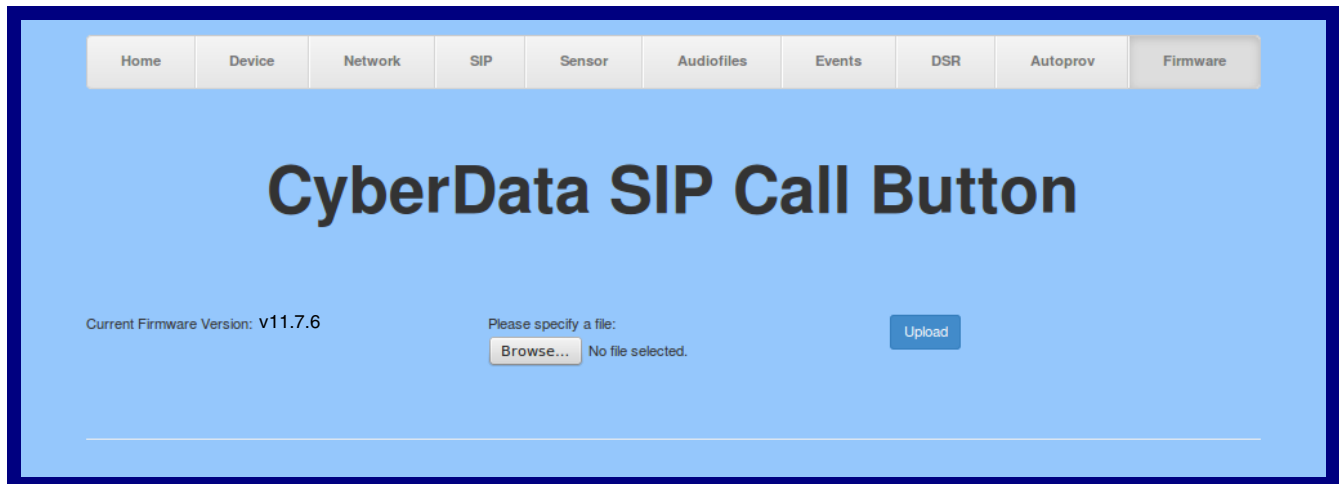


Figure 2-34. Firmware Page



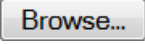

5. Click on the **Browse** button, and then navigate to the location of the firmware file.
6. Select the firmware file.
7. Click on the **Upload** button.

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

Table 2-22. Firmware Parameters

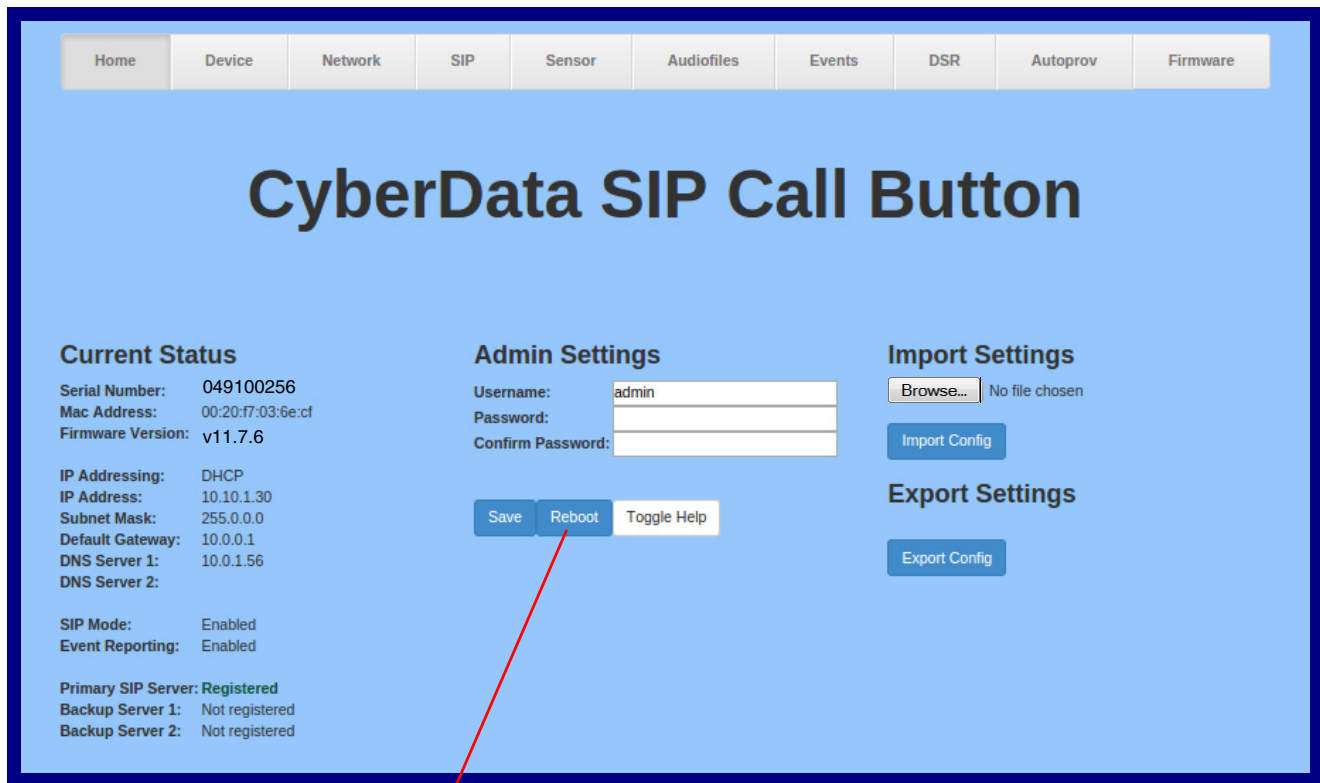
Web Page Item	Description
Current Firmware Version	Shows the current firmware version.
	Use the Browse button to navigate to the location of the firmware file that you want to upload.
	Click on the Upload button to automatically upload the selected firmware and reboot the system.

2.5.14 Reboot the Device

To reboot a SIP Call Button, log in to the web page as instructed in [Section 2.5.4, "Log in to the Configuration Home Page"](#).

1. Click on the **Reboot** button on the **Home** page ([Figure 2-35](#)). A normal restart will occur.

Figure 2-35. Home Page



Reboot

2.6 Command Interface

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

2.6.1 Command Interface Post Commands

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

Table 2-23. Command Interface Post Commands

Device Action	HTTP Post Command ^a
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/sensor.cgi" --post-data "doortest=yes"
Trigger the Intrusion Sensor Test (Sensor Config page)	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/sensor.cgi" --post-data "intrusiontest=yes"

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

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)

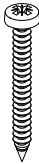
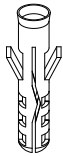
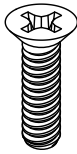
Quantity	Part Name	Illustration
4	#6 x 1.25 inches Sheet Metal Screw	
4	#6 Ribbed Plastic Anchor	

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

Figure A-1. Network Connector Prior to Installation

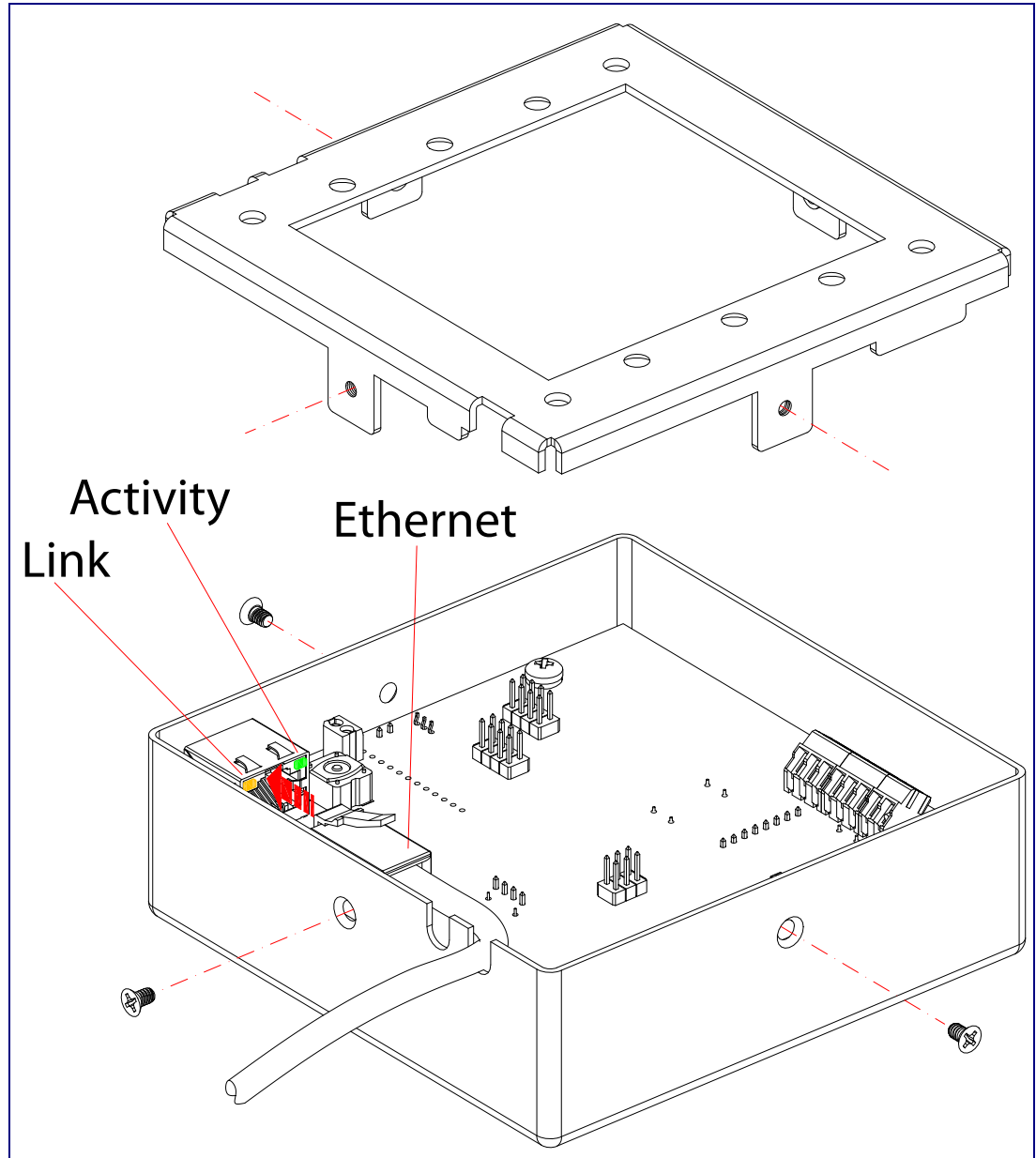


Figure A-3 shows the wall mounting options for the SIP Call Button.

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

Figure A-2. Wall Mounting Options

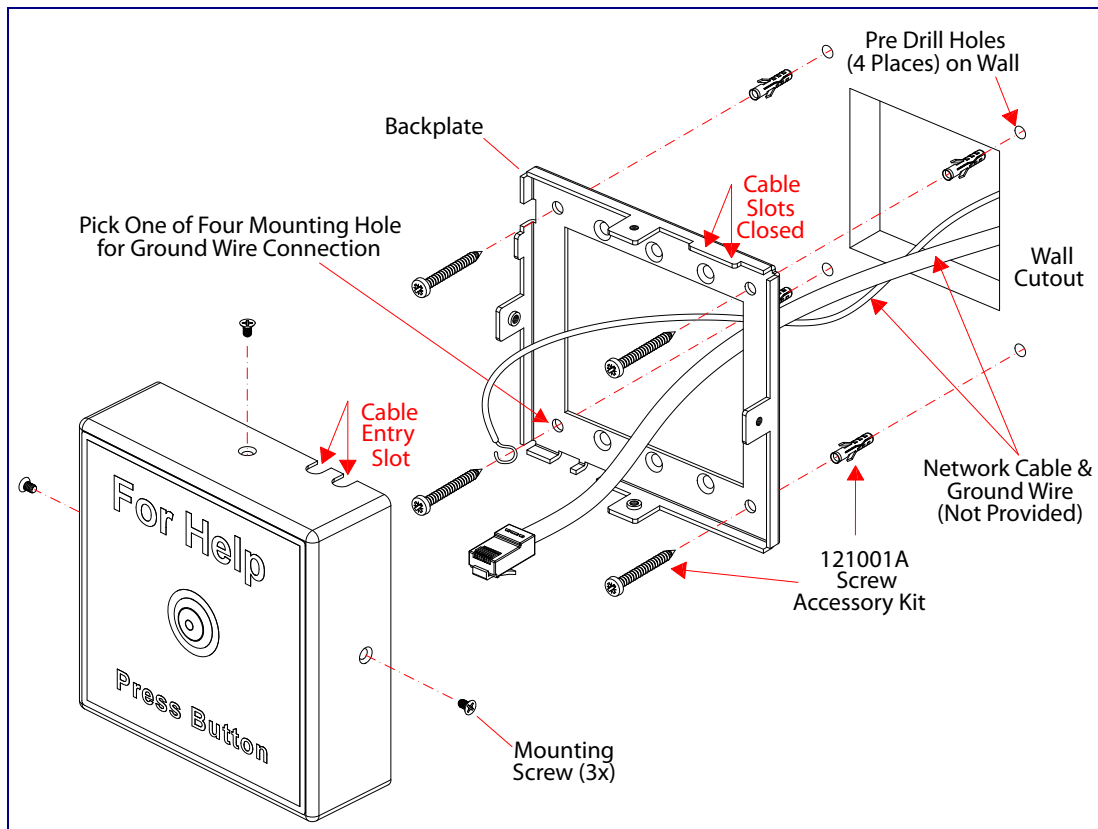


Figure A-3 shows the gang box mounting options for the SIP Call Button.

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

Figure A-3. Mounting Options

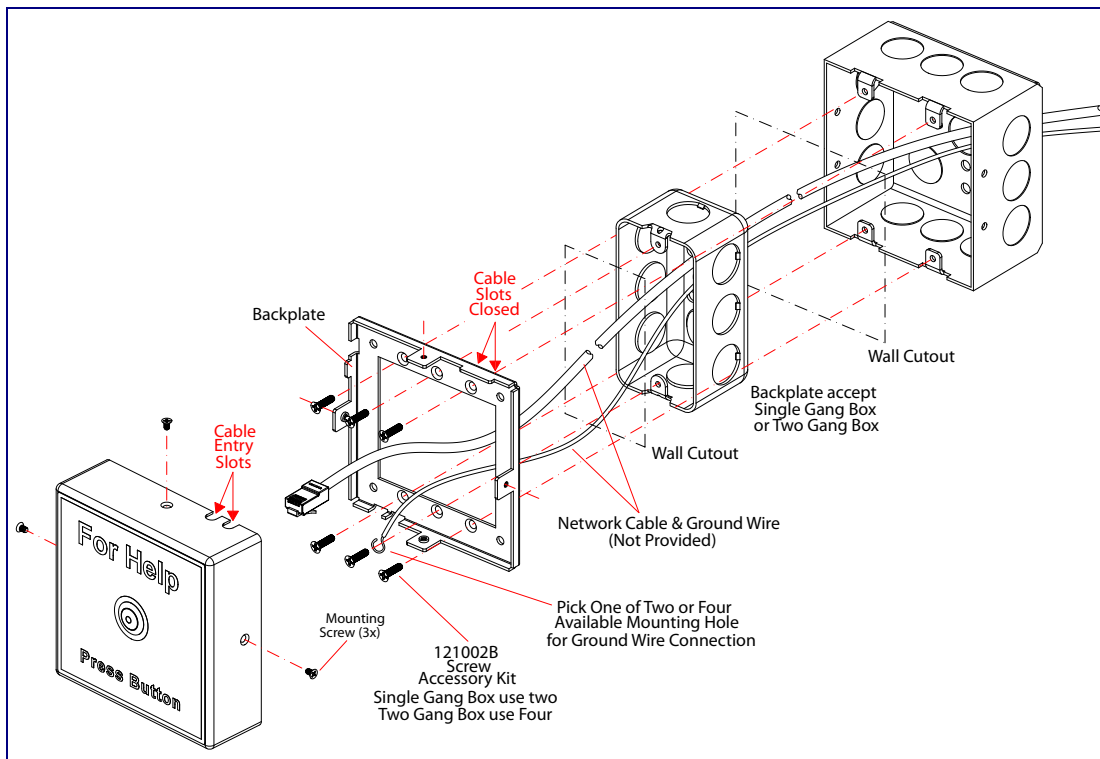
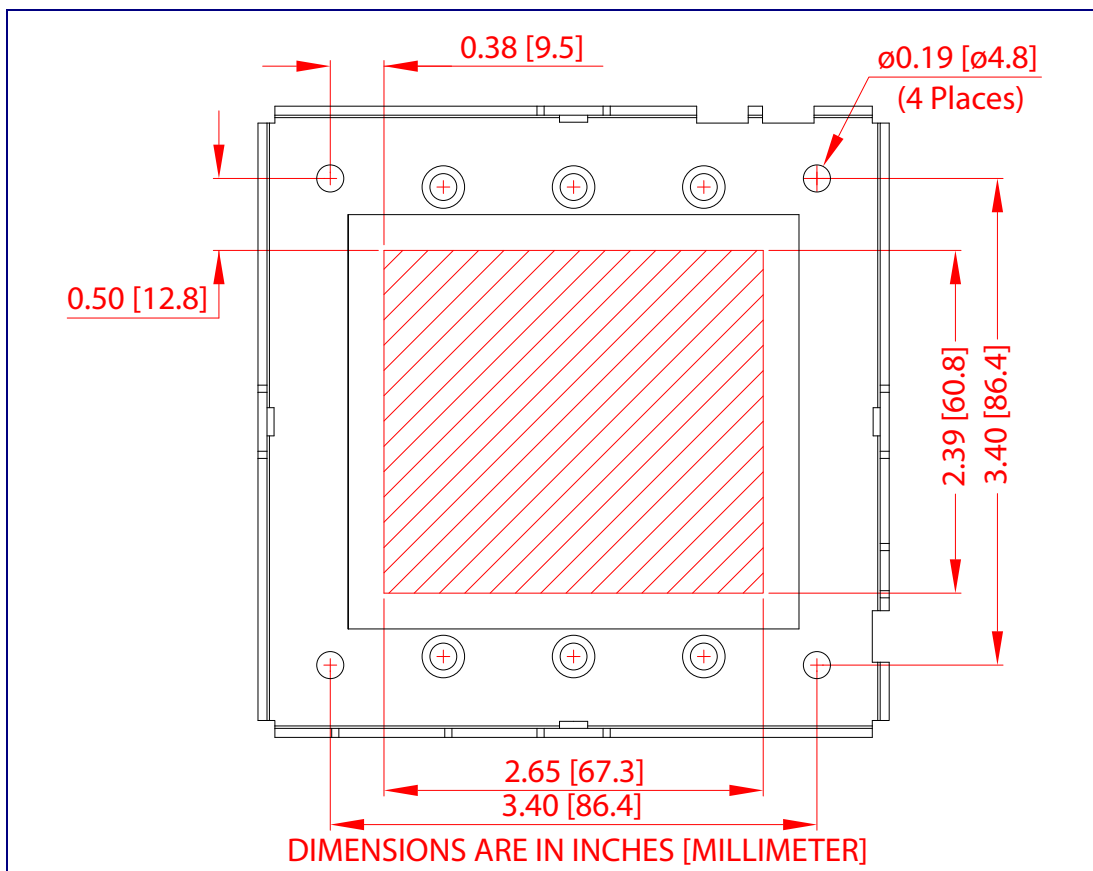


Figure A-4 shows the maximum recommended wall cutout dimensions for mounting the SIP Call Button.

Figure A-4. Maximum Recommended Wall Cutout Dimensions



Appendix B: Troubleshooting/Technical Support

B.1 Frequently Asked Questions (FAQ)

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

<http://www.cyberdata.net/voip/011049/>

B.2 Documentation

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

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

<http://www.cyberdata.net/voip/011049/>

B.3 Contact Information

Contact CyberData Corporation
 3 Justin Court
 Monterey, CA 93940 USA
 www.CyberData.net
 Phone: 800-CYBERDATA (800-292-3732)
 Fax: 831-373-4193

Sales Sales 831-373-2601, Extension 334

Technical The fastest way to get technical support for your VoIP product is to submit a VoIP Technical
Support Support form at the following website:

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

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 **Comments** section of the Support Form.

Phone: (831) 373-2601, Extension 333

B.4 Warranty and RMA Information

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

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

Index

Numerics

16 AWG gauge wire 9

A

activate relay (door sensor) 49
 activate relay (intrusion sensor) 50
 activity LED 19
 address, configuration login 28
 alternative power input 6
 announcing a device's IP address 21
 audio configuration 52
 audio configuration page 52
 audio encodings 5
 audio files, user-created 54
 autoprovision at time (HHMMSS) 64
 autoprovision when idle (in minutes > 10) 64
 autoprovisioning 65
 download template button 65
 autoprovisioning autoupdate (in minutes) 64
 autoprovisioning configuration 63, 64
 autoprovisioning filename 64
 autoprovisioning server (IP Address) 64

B

backup SIP server 1 42
 backup SIP server 2 42
 backup SIP servers, SIP server
 backups 42
 browsers supported 4

C

call button configuration
 default IP settings 24
 call button LED 23
 call termination 33
 changing
 the web access password 32
 Cisco SRST 42
 command interface 78
 commands 78
 configurable parameters 33, 39
 configuration
 audio 52
 default IP settings 24

 door sensor 47
 intrusion sensor 47
 network 38
 SIP 41
 using Web interface 24
 configuration home page 28
 configuration page
 configurable parameters 33, 39
 contact information 85
 contact information for CyberData 85
 Current Network Settings 39
 current network settings 39
 CyberData contact information 85

D

default
 device settings 86
 gateway 24
 IP address 24
 subnet mask 24
 username and password 24
 web login username and password 28
 default gateway 24, 39
 default IP settings 24
 default login address 28
 default settings 22
 device configuration 32
 device configuration parameters 64
 the device configuration page 63
 device configuration page 32
 device configuration parameters 33
 device configuration password
 changing for web configuration access 32
 DHCP Client 5
 dial out extension (door sensor) 49
 dial out extension (intrusion sensor) 50
 dial out extension strings 45, 46
 dimensions 6
 discovery utility program 28
 DNS server 39
 door sensor 47, 49
 activate relay 49
 dial out extension 49
 door open timeout 49
 door sensor normally closed 49
 flash button LED 49
 download autoprovisioning template button 65
 DTMF tones 45, 46
 DTMF tones (using rfc2833) 45

E

earth ground 81, 82
 ethernet cable 80
 ethernet I/F 6
 expiration time for SIP server lease 43
 export settings 30

F

factory default settings 22
 firmware
 where to get the latest firmware 75
 flash button LED (door sensor) 49
 flash button LED (intrusion sensor) 50

G

gang box mounting 81, 82
 get autoprovisioning template 65
 GMT table 36
 GMT time 36

H

home page 28
 http POST command 78
 http web-based configuration 5

I

identifier names (PST, EDT, IST, MUT) 36
 identifying your product 1
 illustration of device mounting process 79
 import settings 30
 import/export settings 30
 installation, typical intercom system 2
 intrusion sensor 47, 50
 activate relay 50
 dial out extension 50
 flash button LED 50
 IP address 24, 39
 IP addressing
 default
 IP addressing setting 24

J

J3 terminal block, 16 AWG gauge wire 9

L

lease, SIP server expiration time 43
 LED
 green link LED 19
 yellow activity LED 19
 link LED 19, 80
 local SIP port 43
 log in address 28

M

mounting the device 79

N

navigation (web page) 25
 navigation table 25
 network configuration 38
 Network Setup 38
 Nightringer 9, 74
 NTP server 33

O

on-board relay 6, 11
 operating temperature 6

P

packet time 5
 part number 6
 parts list 8
 password
 for SIP server login 42
 login 28
 restoring the default 24
 payload types 6
 point-to-point configuration 46
 port
 local SIP 43
 remote SIP 43

- posix timezone string
 - timezone string 33
- POST command 78
- power input 6
 - alternative 6
- product
 - configuring 24
 - mounting 79
 - parts list 8
- product features 4
- product overview
 - product features 4
 - product specifications 6
 - supported protocols 5
 - supported SIP servers 5
 - typical system installation 2
- product specifications 6
- protocol 6
- protocols supported 5

R

- reboot 76, 77
- remote SIP port 43
- reset test function management button 20
- resetting the IP address to the default 79, 84
- restoring factory default settings 22, 86
- RJ-45 18
- rport discovery setting, disabling 43
- RTFM button 20
- RTFM jumper 20, 21, 22
- RTP/AVP 5

S

- sales 85
- sensor setup page 48, 61
- sensor setup parameters 47
- sensors 49
- server address, SIP 42
- service 85
- set time with external NTP server on boot 33
- setting up the device 9
- settings, default 22
- SIP
 - enable SIP operation 42
 - local SIP port 43
 - user ID 42
- SIP configuration 41
- SIP configuration parameters
 - outbound proxy 43
 - registration and expiration, SIP server lease 43

- unregister on reboot 43
 - user ID, SIP 42
- SIP registration 42
- SIP remote SIP port 43
- SIP server 42
 - password for login 42
 - SIP servers supported 5
 - unregister from 43
 - user ID for login 42
- SIP server configuration 42
- SRST 42
- status LED 80
- subnet mask 24, 39
- supported protocols 5

T

- tech support 85
- technical support, contact information 85
- terminal block, 16 AWG gauge wire 9
- TFTP server 5
- time zone string examples 36

U

- user ID
 - for SIP server login 42
- username
 - changing for web configuration access 32
 - default for web configuration access 28
 - restoring the default 24

V

- VLAN ID 39
- VLAN Priority 39
- VLAN tagging support 39
- VLAN tags 39

W

- warranty policy at CyberData 85
- web access password 24
- web access username 24
- web browsers supported 4
- web configuration log in address 28
- web page
 - navigation 25
- web page navigation 25

web-based configuration 24
wget, free unix utility 78
wiring the circuit 12
 devices less than 1A at 30 VDC 12