



SIP Call Button Operations Guide

Part #011049

Document Part #930801L for Firmware Version 11.3.1

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

SIP Call Button Operations Guide 930801L Part # 011049

COPYRIGHT NOTICE: © 2015, CyberData Corporation, ALL RIGHTS RESERVED.

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

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

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

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

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

CyberData	Technical Support
The IP Endpoint Company	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 930801L, which corresponds to firmware version 11.3.1, was released on November 15, 2016, and has the following changes:

- Updates Figure 1-2, "Typical Installation"
- Updates Figure 2-1, "Connections"
- Adds Section 2.2.1.1, "Remote Switch Connection"

Browsers Supported

The following browsers have been tested against firmware version 11.3.1:

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

Important Safety Instructions

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

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

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

Pictorial Alert Icons

GENERAL ALERT	General Alert 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.
	Ground This pictorial alert indicates the Earth grounding connection point.

Hazard Levels

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

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

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

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

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

Abbreviations and Terms

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

Chapter 1 Product Overview	1
1.1 How to Identify This Product	1
1.2 Typical System Installation	2
1.3 Product Features	3
1.4 Supported Protocols	3
1.5 Supported SIP Servers	3
1.6 Specifications	4
Chapter 2 Installing the SIP Call Button	5

Chapter 2 Installing the SIP Call Button	5
2.1 Parts List	5
2.2 SIP Call Button Setup	6
2.2.1 SIP Call Button Connections	6
2.2.2 Using the On-Board Relay	8
2.2.3 Wiring the Circuit	9
2.2.4 Identifying the SIP Call Button Connectors and Jumpers	10
2.2.5 Activity and Link LEDs	12
2.2.6 Restore the Factory Default Settings	13
2.2.7 Call Button and the Call Button LED	14
2.3.1 Factory Default Settings	15
2.3.2 SIP Call Button Web Page Navigation	16
2.3.3 Using the Toggle Help Button	17
2.3.4 Log in to the Configuration Home Page	19
2.3.5 Configure the Device	23
2.3.6 Configure the Network Parameters	29
2.3.7 Configure the SIP Parameters	32
2.3.8 Configure the Sensor Configuration Parameters	38
2.3.9 Configure the Audio Configuration Parameters	42
2.3.10 Configure the Event Parameters	46
2.3.11 Configure the Door Strike Relay	51
2.3.12 Configure the Device (on the DSR page)	55
2.3.13 Configure the Autoprovisioning Parameters	58
2.3.14 Downloading the Firmware	70
2.3.15 Reboot the Device	72
2.4.1 Command Interface Post Commands	73

Appendix A Mounting the SIP Call Button	74
A.1 Mount the SIP Call Button	74
Appendix B Troubleshooting/Technical Support	79
B.1 Frequently Asked Questions (FAQ)	79
B.2 Documentation	
B.3 Contact Information	
B.4 Warranty and RMA Information	
Index	81

Index

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



Model number

Serial number begins with 0491

1.2 Typical System Installation

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

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

Figure 1-2. Typical Installation



1.3 Product Features

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

1.4 Supported Protocols

The SIP Call Button supports:

- SIP
- HTTP Web-based configuration

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

DHCP Client

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

- RTP
- RTP/AVP Audio Video Profile
- Audio Encodings
 PCMU (G.711 mu-law)
 PCMA (G.711 A-law)

Packet Time 20 ms

1.5 Supported SIP Servers

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

SIP RFC 3261 Compatible	
PoE 802.3af compliant or +8 to +12VDC @ 1000mA Regulated Power Supply ^a	
1A at 30 VDC	
-	

Table 1-1. Specifications

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.

2 Installing the SIP Call Button

2.1 Parts List

Table 2-1 illustrates the SIP Call Button parts.

Table 2-1. Pa	arts List
---------------	-----------

Quantity	Part Name	Illustration
1	SIP Call Button Assembly	For Help
1	Installation Quick Reference Guide	Water
1	SIP Call Button Mounting Accessory Kit	

2.2 SIP Call Button Setup

2.2.1 SIP Call Button Connections

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

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



Caution

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

Figure 2-1. Connections



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.





2.2.2 Using the On-Board Relay

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

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.

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 CyberData Door Strike Intermediate Relay Module (CD# 011269) (see Section 2.2.4, "Identifying the SIP Call Button Connectors and Jumpers").



Figure 2-3. Wiring Diagram

2.2.4 Identifying the SIP Call Button Connectors and Jumpers

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



Figure 2-4. Connector Locations

Table	2-2.	Connector	Functions
-------	------	-----------	-----------

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





Table 2-3. Connector Functions

Connector	Function			
J1	PoE Network Connection (RJ-45 ethernet)			
J3	Terminal Block (see Figure 2-1)			
J4	Console Port (Factory Use Only)			
J5	JTAG (Factory Use Only)			
J9	Auxiliary Strobe Connector — Not Used			
J12	Reserved (Factory Use Only)			

2.2.5 Activity and Link LEDs

2.2.5.1 Verifying the Network Connectivity and Data Rate

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

- The square, YELLOW Activity LED blinks when there is network activity (see Figure 2-6).
- The square, **GREEN Link** LED above the Ethernet port indicates that the network connection has been established (see Figure 2-6).



Figure 2-6. Activity and Link LED

2.2.6 Restore the Factory Default Settings

2.2.6.1 RTFM Switch

When the SIP Call Button is operational and linked to the network, use the Reset Test Function Management (RTFM) switch (Figure 2-7) to set the factory default settings.

- **Note** Each SIP Call Button is delivered with factory set default values.
- **Note** The SIP Call Button will use DHCP to obtain the new IP address (DHCP-assigned address or default to 10.10.10.10 if a DHCP server is not present).



Figure 2-7. RTFM Switch

To set the factory default settings:

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

2.2.7 Call Button and the Call Button LED

2.2.7.1 Calling with the The Call Button

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

2.2.7.2 Call Button LED Function

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



Figure 2-8. Call Button and Call Button LED

2.3 Configure the SIP Call Button Parameters

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

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

2.3.1 Factory Default Settings

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

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

Table 2-4. Factory Default Settings

Parameter	Factory Default Setting	
IP Addressing	DHCP	
IP Address ^a	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.

2.3.2 SIP Call Button Web Page Navigation

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

Web Page Item	Description
Home	Link to the Home page.
Device	Link to the Device page.
Network	Link to the Network page.
SIP	Link to go to the SIP page.
Sensor	Link to the Sensor page.
Audiofiles	Link to the Audiofiles page.
Events	Link to the Events page.
DSR	Link to the Door Strike Relay page.
Autoprov	Link to the Autoprovisioning page.
Firmware	Link to the Firmware page.

Table 2-5. Web Page Navigation

2.3.3 Using the Toggle Help Button

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

1. Click on the Toggle Help button that is on the UI webpage. See Figure 2-9 and Figure 2-10.

Figure 2-9. Toggle/Help Button

Тод	igle I	Help
log	gle i	Help

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 2-10.

Figure 2-10. Toggle Help Button and Question Marks

Clock Settings Set Time with NTP server on boot:		Question mark appears next to the web page items
NTP Server:	north-america.pool.ntp.org ?	web page items
Posix Timezone String (see manual):	PST8PDT,M3.2.0/2:00:00,M1 ?	
Periodically sync time with server:		
Time update period (in hours):	24 ?	
Current Time:	Not set	
Save Reboot		Toggle Help button
Test Audio Test Microphone	Test Relay Toggle Help	

3. Move the mouse pointer to hover over the question mark (?), and a short description of the web page item will appear. See Figure 2-11.



Figure 2-11. Short Description Provided by the Help Feature

2.3.4 Log in to the Configuration Home Page

- 1. Open your browser to the SIP Call Button IP address.
- **Note** If the network does not have access to a DHCP server, the device will default to an IP address of 10.10.10.10.
- Note Make sure that the PC is on the same IP network as the SIP Call Button.
- **Note** You may also download CyberData's VoIP Discovery Utility program which allows you to easily find and configure the default web address of the CyberData VoIP products.

CyberData's VoIP Discovery Utility program is available at the following website address: http://www.cyberdata.net/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 2-12):

Web Access Username: admin

Web Access Password: admin

Figure 2-12. Home Page

	Cybe	rData SIP Ca	all Button
Current Sta	tus	Admin Settings	Import Settings
Serial Number:	049100256	Username: admin	Browse No file selected
Mac Address:	00:20:f7:02:56:f6	Password:	
irmware Version:	v11.3.1	Confirm Password:	Import Confin
P Addressing:	DHCP		mport comy
P Address:	10.10.1.46		Export Settings
Subnet Mask:	255.0.0.0	Save Reboot Toggle Help	Export oottingo
Default Gateway:	10.0.0.1		
ONS Server 1:	10.0.0.252		Export Config
ONS Server 2:			
SIP Volume:	0		
Multicast Volume:	0		
Ring Volume:	0		
Sensor Volume:	0		
/olume Boost:	Off		
Microphone Gain:	0		
SIP Mode:	Enabled		
Multicast Mode:	Disabled		
Event Reporting:	Disabled		
lightringer:	Disabled		
Primary SIP Server:	Registered		
Backup Server 1:	Not registered		
Backup Server 2:	Not registered		
	Not registered		

- 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.

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 Volume	Shows the current SIP volume level.				
Multicast Volume	Shows the current Multicast volume level.				
Ring Volume	Shows the current Ring volume level.				
Sensor Volume	Shows the current Sensor volume level.				
Volume Boost	Shows the current Volume Boost level.				
Microphone Gain	Shows the current microphone gain level.				
SIP Mode	Shows the current status of the SIP mode.				
Multicast Mode	Shows the current status of the Multicast mode.				
Event Reporting	Shows the current status of the Event Reporting mode.				
Nightringer	Shows the current status of the Nightringer mode.				
Primary SIP Server	Shows the current status of the Primary SIP Server.				
Backup Server 1	Shows the current status of Backup Server 1.				
Backup Server 2	Shows the current status of Backup Server 2.				
Nightringer Server	Shows the current status of Nightringer Server.				
Import Settings					
Browse	Use this button to select a configuration file to import.				
Import Config After selecting a configuration file, click Import to import the configuration from the selected file. Then, click Save and Rebord store changes.					

Table 2-6. Home Page Overview

Web Page Item	Description				
Export Settings					
Export Config	Click Export to export the current configuration to a file.				
	Click the Save button to save your configuration settings.				
Save	Note: You need to reboot for changes to take effect.				
Reboot	Click on the Reboot button to reboot the system.				
Toggle Help	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.				

Table 2-6. Home Page Overview (continued)

2.3.5 Configure the Device

1. Click the **Device Configuration** button to open the **Device Configuration** page. See Figure 2-13.

	Fig	ure 2-13. Devi	ce Configurati	on Page			
Home Device	Network S	IP Sensor	Audiofiles	Events	DSR	Autoprov	Firmware
C	vberF)ata S		all F	Rutt	on	
U,							
Relay Settings			Clock Se	ttings			
Activate Relay with DTMF code:			Set Time with N	TP server on bo	oot:		
DTMF Activation Code:	321		NTP Server:		north-an	nerica.pool.ntp.org	
DTMF Activation Duration (in secon	ds): 2		Posix Timezone	e String (see ma	nual): PST8PD	DT,M3.2.0/2:00:00,M1	1.1.0
Activate Relay While Call Active:			Periodically syr	nc time with serv	/er:		
Activate Relay On Button Press:			Time update pe	riod (in hours):	24		
Relay On Button Press Duration:	3		Current Time:		NULSEL		
Misc Settings							
Device Name:	CyberData SIP Call B	utton					
Button Lit when Idle:	×						
Button Brightness (0-255):	255						
Disable HTTPS (NOT recommended	I): 🗌						
Save Reboot							
Tost Polay Tassia Liala							
rest Relay roggle 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.

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.				
DTMF Activation Code ?	Activation code used to activate the relay when entered on a phone during a SIP call with the device. Activate Relay with DTMF Code must be enabled. Enter up to 25 digits (* and # are supported).				
DTMF Activation Duration (in seconds) 🛜	The length of time (in seconds) during which the relay will be activated when the DTMF Activation Code is detected. Enter up to 5 digits.				
	NOTE : A DTMF activation duration of 0 will toggle the relay indefinitely or until the activation code is sent again				
Activate Relay While Call Active 🛜	When selected, the relay will be activated as long as the SIP call is active.				
Activate Relay on Button Press 🛜	When selected, the relay will be activated when the Call button is pressed.				
Relay on Button Press Duration ?	The length of time (in seconds) during which the relay will be activated when the Call button is pressed. Enter up to 5 digits. A Relay on Button Press Duration value of 0 will pulse the relay once when the Call button is pressed.				
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.				
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 2.3.5.1, "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.				

Web Page Item	Description When selected, the time is periodically updated with the NTP server at the configured interval below.				
Periodically sync time with server ?					
Time update period (in hours) ?	The time interval after which the device will contact the NTP server to update the time. Enter up to 4 digits.				
Current Time	Allows you to input the current time. (6 character limit)				
	Click the Save button to save your configuration settings.				
Save	Note: You need to reboot for changes to take effect.				
Reboot	Click on the Reboot button to reboot the system.				
Test Relay	Click on the Test Relay button to do a relay test.				
Toggle Help	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.				

Table 2-7. Device Configuration Parameters (continued)

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

2.3.5.1 Time Zone Strings

The posix time zone string tells the internal date and time utilities how to handle daylight savings time for different time zones. Table 2-8 shows some common strings.

	6
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

Table 2-8. Common Time Zone Strings

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

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.
МЗ	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

Table 2-9. Time Zone String Parts

Time Zone String Examples Table 2-10 has some more examples of time zone strings.

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

Table 2-10. Time Zone String Examples

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 2-14. 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			

2.3.6 Configure the Network Parameters

1. Click the Networking button to open the Network Configuration page (Figure 2-15).

Figure 2-15	. Network	Configuration	Page
-------------	-----------	---------------	------

Home Device	Network	SIP	Sensor	Audiofiles	Events	DSR	Autoprov	Firmware
CyberData SIP Call Button								
Stored Network S	ettings			VLAN Se	ettings			
Addrossing Modo:				VI AN ID (0-40	95): 0			
Hostname:	Static UDHCP			VLAN Priority	(0-7): 0			
IP Address:	0.10.10.10			,	(•••)]=			
Subnet Mask: 2	55.0.0.0							
Default Gateway:	0.0.0.1							
DNS Server 1: 1	0.0.0.1							
DNS Server 2: 1	0.0.0.1							
DHCP Timeout in seconds*: 6	i0							
* A value of -1 will retry forever								
Current Network	Settings			Save Re	boot Toggle I	Help		
IP Address: 10.10.0.16 Subnet Mask: 255.00.0 Default Gateway: 10.0.0.11 DNS Server 1: 10.0.0.252 DNS Server 2: 10.0.11	-							
- 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.

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 2.3.1, "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	Shows the 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

Web Page Item	Description			
	Click the Save button to save your configuration settings.			
Save	Note: You need to reboot for changes to take effect.			
Reboot	Click on the Reboot button to reboot the system.			
Toggle Help	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.			

Table 2-12. Network Configuration Parameters (continued)

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

2.3.7 Configure the SIP Parameters

1. Click SIP Config to open the SIP Configuration page (Figure 2-16).

Figure 2-16. SIF	P Configuration Page
------------------	----------------------

Home Dev	ice Network	SIP Sensor	Audiofiles	Events DSR	Autoprov	Firmware
	Cvber	Data S	SIP C	all But	tton	
SIP Settings			Dial Out	t Settings		
Enable SIP eneration:			Dial out Exter	sion: 204		
Degleter with a OID O			Extension ID	id204		
Hegister with a SIP Serve			Literatori ID			
Die Cisco SRST:	10.0.052					
Primary SIP Server:	199		Call Dis	connection		
Primary SIP Auth ID:	199		Terminate Ca	ll after delay: 0		
Primary SIP Auth Passwo	rd: •••••					
Backup SIP Server 1:						
Backup SIP User ID 1:						
Backup SIP Auth ID 1:						
Backup SIP Auth Passwo	rd 1:					
Backup SIP Server 2:						
Backup SIP User ID 2:						
Backup SIP Auth ID 2:						
Backup SIP Auth Passwo	rd 2:					
Remote SIP Port:	5060					
Local SIP Port:	5060					
Outbound Proxy:						
Outbound Proxy Port:	0					
Disable roort Discovery						
Re-registration Interval (i	n seconds): 360					
Unregister on Boot:						
Keep Alive Period:	10000					
	I					
RTP Settings			Save Re	poot Toggle Help		
RTP Port (even): 10500						

- 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 2.3.7.3, "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 <mark>?</mark>	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.

Web Page Item	Description
Backup SIP User ID 2 ?	Specify the SIP User ID for the second backup SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the second backup SIP server. Enter up to 64 alphanumeric characters.
Backup SIP Auth ID 2 ?	Specify the Authenticate ID for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Auth Password 2 🛜	Specify the Authenticate Password for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Remote SIP Port ?	The Remote SIP Port is the port number the device will use as the destination port when sending SIP messages. The default Remote SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
Local SIP Port ?	The Local SIP Port is the port number the device will use to receive SIP messages. The default Local SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
Outbound Proxy ?	Enter the Outbound Proxy address as an IPv4 address in dotted decimal notation or a fully qualified domain name (FQDN). When an IP address is configured, the device will send all SIP messages to this IP address. When an FQDN is configured, the device will run DNS NAPTR, SRV, and A queries on the FQDN to resolve an IP address to which it will send all SIP messages. This field can accept entries of up to 255 characters in length.
Outbound Proxy Port ?	The Outbound Proxy Port is port number used as the destination port when sending SIP messages to the outbound proxy. A value of 0 will default to 5060. The supported range is 0-65536. Enter up to 5 digits.
Disable rport Discovery ?	Disabling rport Discovery will prevent the device from including the public WAN IP address and port number in the contact information that is sent to the remote SIP servers. This will generally only need to be enabled when using an SBC or SIP ALG in conjunction with a remote SIP server.
Re-registration Interval (in seconds) ?	The SIP Re-registration interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
Unregister on Boot ?	When enabled, the device will send one registration with an expiry of 0 on boot.
Keep Alive Period 🛜	The minimum time in milliseconds between keep-alive packets sent for nat traversal. A value of 0 will disable keep alive packets.
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.
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 2.3.7.2, "Dial Out Extension Strings and DTMF Tones (using rfc2833)".

Table 2-13. SIP Configuration Parameters (continued)

Web Page Item	Description
Extension ID ?	A Caller identification string added to outbound calls. Enter up to 64 alphanumeric characters.
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.
	Click the Save button to save your configuration settings.
Save	Note: You need to reboot for changes to take effect.
Reboot	Click on the Reboot button to reboot the system.
Toggle Help	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.

Table 2-13. SIP Configuration Parameters (continued)

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

2.3.7.1 Server Configurations

For specific server configurations, go to the following webpage:

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

2.3.7.2 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.

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		

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

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

2.3.7.3 Point-to-Point Configuration

When the board is set to not register with a SIP server (see Figure 2-17), 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 2-17. SIP Configuration Page Set to Point-to-Point Mode

Home Device	Network SIP Sensor	Audiofiles Events DSR Autoprov Firmware	
С	yberData S	SIP Call Button	
SIP Settings		Dial Out Settings	
Enable SIP operation:		Dial out Extension: 10.0.1.40	
Begister with a SIP Server		Extension ID: id204	
Use Cisco SRST	A		
Primary SIP Server:	10.00.253	Call Disconnection	
Primary SIP User ID:	199		
Primary SIP Auth ID:	199	Terminate Call after delay: 0	
Primary SIP Auth Password:	•••••		
Backup SIP Server 1:			
Backup SIP User ID 1:			
Backup SIP Auth Password 1:			
Backup SIP Server 2:			
Backup SIP User ID 2:			
Backup SIP Auth ID 2:			
Backup SIP Auth Password 2:			
Remote SIP Port:	5060		
Local SIP Port:	5060		
Outbound Proxy:			
Outbound Proxy Port:	0		
Disable roort Discovery:			
Re-registration Interval (in secon	ds): 360		
Unregister on Boot:			
Keep Alive Period:	10000		
RTP Settings		Sive Rebot Toggle Help	
RTP Port (even): 10500			

Device is set to NOT register with a SIP server

2.3.7.4 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.

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		

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

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

2.3.8 Configure the Sensor Configuration Parameters

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

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

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

- Flash the LED until the sensor is deactivated (roughly 10 times/second)
- · Activate the relay until the sensor is deactivated
- Call a preset extension and play a pre-recorded audio file (once)
- **Note** Calling a preset extension can be set up as a point-to-point call, but currently can't send delayed DTMF tones.

1. Click Sensor Config to open the Sensor Configuration page (Figure 2-18).

Figure 2-18. Sensor Configuration Page

Home Device	Network SIP	Sensor Audiofiles	Events	DSR	Autoprov	Firmware
C	yberD a	ata SIP C	all E	Butto	on	
Door Sensor Settin	ngs	Intrusi	on Sensor S	ettings		
Door Sensor Normally Closed: Door Open Timeout (in second Flash Button LED: Activate Relay: Make call to extension: Dial Out Extension: Dial Out ID: Play recorded audio:	Yes No s): 0 204 1d204	Flash Butte Activate Re Make call t Dial Out Ex Dial Out ID Play record	n LED: lay: extension: 204 id204 ed audio:			
Save Reboot Toggle H Test Door Sensor Test Intru	elp sion Sensor					

- 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.

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).	
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.	
Save	Click the Save button to save your configuration settings. Note : You need to reboot for changes to take effect.	

Table 2-16. Sensor Configuration Parameters

Web Page Item Description			
Reboot	Click on the Reboot button to reboot the system.		
Toggle Help	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.		
Test Door Sensor	Click the Test Door Sensor button to test the door sensor.		
Test Intrusion Sensor	Click the T est Intrusion Sensor button to test the Intrusion sensor.		

 Table 2-16. Sensor Configuration Parameters (continued)

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

2.3.9 Configure the Audio Configuration Parameters

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

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

Figure 2-19. Audio Configuration Page

CyberData SIP Call Button cualabe space: 8: 0.18% Mater Message: Currently set to default Entraisen Sensor Message: Currently set to default Creaser Message: Currently set to default Corsensor Message: Currently set to default Corsensor Message: Currently set to default Corsensor Message: Currently set to default	Available Space: 36.19MB nty set to default Browse No file selected.
CyberData SIP Call Button cualabe space:36.19MB Button Message: Currently setto default Intrusion Sensor Message: Currently setto default Browse No file selected. Delete Save Dor Sensor Message: Currently setto default Erowse No file selected. Delete Save Save	Available Space: 36.19MB ntly set to default Browse No file selected. Delete Save
Available Space: 36.19MB Button Message: Currently set to default Browse No file selected. Intrusion Sensor Message: Currently set to default Browse No file selected. Delete Save Door Sensor Message: Currently set to default	Available Space:36.19MB ntly set to default Browse No file selected. Delete Save
Available Space: 36.19MB Button Message: Currently set to default Browse No file selected. Delete Save Intrusion Sensor Message: Currently set to default Browse No file selected. Delete Save Door Sensor Message: Currently set to default Browse No file selected. Delete Save	Available Space:36.19MB ntly set to default Browse No file selected. Delete Save
Button Message: Currentiy set to default Browse No file selected. Delete Save Intrusion Sensor Message: Currentiy set to default Browse No file selected. Delete Save Door Sensor Message: Currentiy set to default	Infly set to default Browse No file selected. Delete Save
Browse No file selected. Delete Save Intrusion Sensor Message: Currently set to default Browse No file selected. Delete Save Door Sensor Message: Currently set to default	Browse No file selected. Delete Save
Intrusion Sensor Message: Currently set to default Browse No file selected. Delete Save Currently set to default	
Browse No file selected. Delete Save Door Sensor Message: Currently set to default Currently	ntiy set to default
Door Sensor Message: Currentily set to default	Browse No file selected. Delete Save
Prowso No file colorized Delate Save	ntiy set to default Prowson No file selected Delete Save
DIOWSE No lie selecieu. Delete Save	

- 2. On the Audiofiles page, enter values for the parameters indicated in Table 2-17.
- **Note** The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

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."				
Browse	Click on the Browse button to navigate to and select an audio file.				
Delete	The Delete button will delete any user uploaded audio and restore the stock audio file.				

Table 2-17. Audiofiles Configuration Parameters

Web Page Item	Description
Save	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.

Table 2-17. Audiofiles Configuration Parameters (continued)

2.3.9.1 User-created Audio Files

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

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

You can use the free utility *Audacity* to convert audio files into this format. See Figure 2-20 through Figure 2-22.



Figure 2-20. Audacity 1

Tag Name	Tag Value	
Artist Name		
Track Title		
Album Title		
Track Number		
Year		
Genre		
Comments		
<u>A</u> dd	<u>B</u> emove <u>G</u> Template	Clear
E <u>d</u> it Rese <u>t</u>	Load	ave S <u>e</u> t Default

Figure 2-21. Audacity 2

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

• WAV (Microsoft) signed 16 bit PCM.

🔒 💽 Export File		$\odot \odot \otimes$
Name: audiotest.v	vav	
Save in folder:		
✓ Browse for other folders		
🛃/ tmp/		Create Folder
Places	Name	✓ Modified
🆚 Search	🛅 cscope.4371	Yesterday at 14:30
🛞 Recently Used	🛅 kde-na	Yesterday at 14:26
🛅 na	🛅 kde-root	Yesterday at 14:26
🛅 Desktop	🛅 ksocket-na	09:20
🐻 File System	🛅 orbit-na	Yesterday at 14:32
👩 250.1 GB Media	ssh-CIPQVD3392	Yesterday at 14:26
	► v814422	Yesterday at 15:45
) \$
₽ Add ≋ <u>R</u> emove		WAV (Microsoft) signed 16 bit PCM 👻
	<u>O</u> ptions	

Figure 2-22. WAV (Microsoft) signed 16 bit PCM

WAV (Microsoft) signed 16 bit PCM

2.3.10 Configure the Event Parameters

1. Click the **Event Config** button to open the **Event Configuration** page (Figure 2-23). The **Event Configuration** page specifies a remote server that can be used to receive HTTP POST events when actions take place on the board.

<section-header> cost Cost Co</section-header>	Home Device Network	SIP Sensor	Audiofiles	Events	DSR	Autoprov	Firmware
Enable Event Generation: Events Enable Button Events: Enable Call Start Events: Enable Call Terminated Events: Enable Relay Activated Events: Enable Relay Deactivated Events: Enable Relay Events: Enable Socord Heartbeat: Check All Venteck All Togle Help	Cyber	Data S	SIP C	all E	Butt	on	
Events Server IP Address: 10.0.250 Enable Button Events: Server Port: Enable Call Start Events: Server URL: Enable Call Terminated Events: Server URL: Enable Relay Deactivated Events: Server URL: Enable Relay Deactivated Events: Server URL: Enable Sensor Events: Server URL: Enable Go Second Heartbeat: Server URL: Check All Vincheck All	Enable Event Generation:		Event Se	erver			
Enable Button Events: bddd Enable Call Start Events: Server VRL: Enable Relay Activated Events: Enable Relay Deactivated Events: Enable Relay Deactivated Events: Enable Relay Events: Enable Sensor Events: Enable Relay Events: Enable Gol Second Heartbeat: Check All	Events		Server IP Add	ress: 10.0.0.250			
Enable Call Start Events: Enable Call Terminated Events: Enable Relay Activated Events: Enable Relay Deactivated Events: Enable Sensor Events: Enable Relay Events: Enable Security Events: Enable 60 Second Heartbeat: Check All	Enable Button Events:		Server Port:	xminarse e	ingine		
Enable Call Terminated Events: Enable Relay Activated Events: Enable Relay Deactivated Events: Enable Power On Events: Enable Sensor Events: Enable Relay Events: Enable Relay Events: Enable Go Second Heartbeat: Check All Save Reboot Toggle Help	Enable Call Start Events:		our offer	Tumperso_o			
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	Enable Call Terminated Events:						
Enable Heiay Deactivated Events: Enable Power On Events: Enable Sensor Events: Enable Remote Relay Events: Enable Security Events: Enable 60 Second Heartbeat: Check All Uncheck All Save Reboot Toggle Help	Enable Relay Activated Events:						
Enable Power On Events: Enable Sensor Events: Enable Remote Relay Events: Enable 60 Second Heartbeat: Check All Uncheck All Save Reboot Toggle Help	Enable Relay Deactivated Events:						
Enable Sensor Events: Enable Remote Relay Events: Enable Security Events: Enable 60 Second Heartbeat: Check All Uncheck All Save Reboot Toggle Help							
Enable Security Events: Enable 60 Second Heartbeat: Check All Uncheck All Save Reboot Toggle Help	Enable Sensor Events:						
Enable 60 Second Heartbeat: Check All Uncheck All Save Reboot Toggle Help	Enable Security Events						
Check All Uncheck All Save Reboot Toggle Help	Enable 60 Second Heartheat						
Save Reboot Toggle Help	Check All Uncheck All						
Save Reboot Toggle Help							
Save Reboot Toggle Help							
Save Reboot Toggle Help							
Save Reboot Toggie Heip							
	Save Reboot Toggle Help						

Figure 2-23. Event Configuration Page

- 2. On the Events page, enter values for the parameters indicated in Table 2-18.
- **Note** The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

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.			
Save	Note: You need to reboot for changes to take effect.			
Reboot	Click on the Reboot button to reboot the system.			

Web Page Item	Description
Toggle Help	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.

2.3.10.1 Example Packets for Events

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

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

Here are example packets for every event:

```
POST xmlparse engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 197
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData SIP Device' MAC='0020f70015b6'>
<event>POWERON</event>
</cyberdata>
POST xmlparse engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 199
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData SIP Device' MAC='0020f70015b6'>
<event>HEARTBEAT
</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>
```

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

```
</cyberdata>
```

```
POST xmlparse engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 201
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData SIP Device' MAC='0020f70015b6'>
<event>CALL ACTIVE</event>
</cyberdata>
POST xmlparse engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 205
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData SIP Device' MAC='0020f70015b6'>
<event>CALL TERMINATED</event>
</cyberdata>
POST xmlparse engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 197
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData SIP Device' MAC='0020f70015b6'>
<event>RINGING</event>
</cyberdata>
POST xmlparse engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData SIP Device' MAC='0020f70015b6'>
<event>RELAY_ACTIVATED</event>
</cyberdata>
POST xmlparse engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData SIP Device' MAC='0020f70015b6'>
<event>RELAY DEACTIVATED</event>
</cyberdata>
POST xmlparse engine HTTP/1.1
Host: 10.0.3.79
```

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

2.3.11 Configure the Door Strike Relay

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

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

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

Remote Relay Settings Dor Open Timeout (in seconds): [0 Activate Remote Relay with DTMF code: 321 DTMF Activation Code: 321 DTMF Activation Code: 321 Activate Remote Relay With Call Active: 4ctivate Local Relay: DTMF Activation Duration (in seconds): 2 Activate Remote Relay While Call Active: Make call to extension: Activate Remote Relay On Button Press: Dal Out Extension: Remote Relay On Button Press Duration (in second) 3 Seconds): Image: Status: Listen Port for Remote Relay Status: 49999 Save Rebot Toggle Help Discovered Remote Relays Play recorde Relays Extended Type IP Address MAC Address Serial Number Name Version Volta I.010.1102 0020:F7:02:47:E2 27000078 V2.0A Version Volta I.010.1102 Version Volta I.	Home Device Network SIP Sensor Audiofiles Events DSR Autoprov Firmware											
Discovered Remote Relays Product Type IP Address MAC Address Serial Number Name Version Discover DoorLock 10.10.1.102 00:20:F7:02:A7:E2 270000078 LOCK270000078 V2.0A View Associate	Remote Not associated Activate Remo DTMF Activati DTMF Activati Activate Remo Activate Remo Remote Relay seconds): Listen Port for Save Re	Relay S d with any DS the Relay with on Code: on Duration (the Relay Whi the Relay On On Button P Remote Relay Doot Togg	Settings SRs In DTMF code: (In seconds): Ille Call Active: Button Press: tress Duration (In ay Status: gle Help	321 2 3 3 49999			Remo Door Oper Flash Butt Activate Le Make call t Play recor Dial Out E Dial Out ID	te Door S n Timeout (in s ion LED: ocal Relay: io extension: ded audio: xtension: :	Sens(or Setti :0 	ngs	
Cache age: 00:10	Product Type DoorLock Cache age: 00:	IP Address 10.10.1.102 10	MAC Address 00:20:F7:02:A7:E2	Serial Number 270000078	Discover Name LOCK270000078	ed Re Version V2.0A	mote F	Relays Associate	D	iscover		

Figure 2-24. DSR Page

- 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.

Web Page Item	Description			
Remote Relay Settings	The settings in this section will activate an associated door strike relay.			
Activate Relay with DTMF Code 🛜	Activates the remote relay (DSR) when the DTMF Activation Code is entered on the phone during a SIP call with the device. RFC2833 DTMF payload types are supported.			
DTMF Activation Code ?	Activation code used to activate the remote relay (DSR) when entered on a phone during a SIP call with the device. Activate Remote Relay with DTMF Code must be enabled. Enter up to 25 digits (* and # are supported).			
DTMF Activation Duration (in seconds) 🛜	The length of time (in seconds) during which the remote relay (DSR) will be activated when the DTMF Activation Code is detected. Enter up to 5 digits.			
Activate Remote Relay While Call Active ?	When selected, the remote relay (DSR) will be activated as long as the call is active.			
Activate Remote Relay on Button Press ?	When selected, the remote relay (DSR) will be activated when the Call Button is pressed.			
Remote Relay on Button Press Duration ?? (in seconds)	The length of time (in seconds) during which the remote relay (DSR) will be activated when the Call button is pressed. Enter up to 5 digits. A Remote Relay on Button Press Duration value of 0 will pulse the remote relay (DSR) once when the Call button is pressed.			
Listen Port for Remote Relay Status ?	Specify the port to listen for remote relay (DSR) status packets.			
Remote Door Sensor Settings				
Door Open Timeout (in seconds) ?	The time (in seconds) the device will wait before it performs an action when the remote (DSR) door sensor is activated. The action(s) performed are based on the configured Remote Door Sensor Settings below.			
Flash Button LED 🛜	When selected, the Call button LED will flash until the remote (DSR) door sensor is deactivated (roughly 10 times/second).			
Activate Local Relay 🛜	When selected, the device's on-board relay will be activated until the remote (DSR) door sensor is deactivated.			
Make call to extension ?	When selected, the device will call an extension when the remote (DSR) door sensor is activated. Use the 'Dial Out Extension' field below to specify the extension the device will call.			
Play recorded audio ?	When selected, the device will call the Dial Out Extension and play an audio file to the phone answering the SIP call (corresponds to Door Ajar on the Audiofiles page) when the remote (DSR) door sensor is activated.			
Dial Out Extension ?	Specify the extension the device will call when the remote (DSR) door sensor is activated. Enter up to 64 alphanumeric characters.			

Table 2-19. DSR Configuration Parameters

Web Page Item	Description
Dial Out ID 🛜	An additional Caller identification string added to outbound calls. Enter up to 64 alphanumeric characters.
	Click the Save button to save your configuration settings.
Save	Note: You need to reboot for changes to take effect.
Reboot	Click on the Reboot button to reboot the system.
Toggle Help	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.
Discover	Use this button to search for and find any remote relays that are available on the network.
View	Use this button to view the settings of a remote relay that has been "discovered" after pressing the Discover button.
Associate	Use this button to associate the remote relay with the device. Only one relay may be associated with a device.

Table 2-19. DSR Configuration Parameters (continued)

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

Table 2-19. DSR Configuration Parameters (continued)



Relay Status						
Door: open Relay: inactive						
Kick Remote Relay	Activate Remote Relay	Deactivate Remote Relay	Refresh			

2.3.12 Configure the Device (on the DSR page)

1. Click the View button on the DSR page to open the Configure Device page (Figure 2-26).

Figure 2-26. DSR Page Configure Device Page

Configure Device					
Serial Number	27000002	Refresh			
MAC Address	00:20:F7:02:6C:F8	Get Log			
Version	V1.2A				
Device Name	LOCK27000003	Clear Log			
Addressing Mode	Static OHCP	Reboot			
IP Address:	192.168.70.74	Set Time			
Subnet Mask:	255.255.240.0	Save Changes			
Default Gateway:	192.168.64.1				
Command Port:	59999	Cancel			
Send Events	◎ Off ○ On				
Event IP Address:	192.168.79.255				
Event Port:	49999				
Energize Time:					
DST	◎ Off ○ On				
DST Start:	M3.2.0/02.00.00				
DST End:	M11.1.0/02.00.00				
Current Time:	Current Time: 17:45:26 08182014				
Encryption:	Encryption: None AES-256				
Encryption Key:					
Door State	opon	-			
Door State					
Relay State					
Button State	inactive				
LED	red				
Alarm State	Alarm State alarm				
JP4, 6, 9, 10	0000				
Browse No file selected. Upgrade					

- 2. On the **Configure Device** page, enter values for the parameters indicated in Table 2-20.
- **Note** The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

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

Table 2-20. DSR Page Configure Device Parameters

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

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

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

2.3.13 Configure the Autoprovisioning Parameters

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

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

1. Click the Autoprov menu button to open the Autoprovisioning page. See Figure 2-27.

Figure 2-27. Autoprovisioning Page

Home	Device	Network	SIP	Sensor	Audiofiles	Events	DSR	Autoprov	Firmware
	C	vhei	rDa [·]	ta S	SIP C	all F	Rutt	on	
	$\mathbf{\vee}$	ybci	Du				Juli		
)isable Autopro	visionina:								
Autoprovisionin	g Server:								
Autoprovisionin	g Filename:								
Use tftp:									
Username:									
Password:									
Autoprovisionin	g autoupdate (in	minutes): 0							
Autoprovision a	t time (HHMMSS):	:							
Autoprovision w	hen idle (in minu	tes > 10): 0							
See the manual to	learn how to use a	autoprovisioning to a	onfigure your de	vice.					
Autoprovisioning I	happens on boot.								
The device will first look for a configured server address and filename.									
f these haven't be	een configured, it w	ill look for an autopr	ovisioning serve	r in your list of L	DHCP options and try	to download '0020f7	702b41d.xml' and	if this fails, '000000c	d.xml'.
Save Rebo	ot Toggle Help								
Download Tem	plate								
Autoprovision	ing log								
00:00 Autoprovi	isioning Device								Π
00:00 Autoprov	found option 43 in I	DHCP server="http	://chalmers.cybe	rdata.net"					
00:00 Autoprov looking for 0020f702b41d.xml at http://chalmers.cyberdata.net 00:00 Autoprov looking for 000000cd.xml at http://chalmers.cyberdata.net									
00:00 Failed to f	fetch autoprov file								
00:00 Autoprov	found option 72 in I	DHCP server="10.0).1.2"						
00:00 Autoprov	looking for 0020170	cd.xml at 10.0.1.2	1.2						
	fetch autoprov file								
00:00 Failed to f									
00:00 Failed to t 00:00 Autoprov 00:00 Autoprov	found option 150 in looking for 0020f70	DHCP server="10 2b41d.xml at 10.0.	.0.5.120" 5.120						

- 2. On the **Autoprovisioning** page, you may enter values for the parameters indicated in Table 2-21.
- **Note** The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Web Page Item	Description
Disable Autoprovisioning ?	Prevent the device from automatically trying to download a configuration file. See Section 2.3.13.1, "Autoprovisioning" for more information.
Autoprovisioning Server ?	Enter the IPv4 address of the provisioning server in dotted decimal notation.
Autoprovisioning Filename ?	The autoprovisioning filename is the configuration filename. The default autoprovisioning filename is in the format of <mac address="">.xml.</mac>
	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.
	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.
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) ?	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.
	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).
Autoprovision at time (HHMMSS) ?	The time of day the device will check for a new autoprovisioning file. The time must be 6 characters in length and in HHMMSS format. An empty value will disable this option.
	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).
Autoprovision when idle (in minutes > 10) ?	The idle time (in minutes greater than 10) after which the device will check for a new autoprovisioning file. Enter up to 6 digits. A value of 0 will disable this option.
	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).
Save	Click the Save button to save your configuration settings. Note : You need to reboot for changes to take effect.

Table 2-21. Autoprovisioning Configuration Parameters

Web Page Item	Description
Reboot	Click on the Reboot button to reboot the system.
Toggle Help	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.
Download Template	Press the Download Template button to create an autoprovisioning file for the device. See Section 2.3.13.3, "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).

Table 2-21. Autoprovisioning Configuration Parameters (continued)

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

2.3.13.1 Autoprovisioning

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

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

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

By default, the device will get its autoprovisioning server from the DHCP options. See Section 2.3.13.2, "Sample dhcpd.conf" for an example of how to configure dhcpd to offer autoprovisioning server addresses. If multiple options are set, the device will attempt to download autoprovisioning files from every server.

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

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

You can download an autoprovisioning template file from the Autoprovisioning Page using the **Download Template** button (see Table 2-21). This file contains every configuration option that can be set on the board.

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

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

<mi< th=""><th>.scSettings></th></mi<>	.scSettings>	
	<devicename>CyberData VoIP Intercom</devicename>	
</td <td colspan="2"><autoprovfile>common.xml</autoprovfile>></td>	<autoprovfile>common.xml</autoprovfile> >	
</td <td colspan="2"><autoprovfile>sip_reg[macaddress].xml</autoprovfile>></td>	<autoprovfile>sip_reg[macaddress].xml</autoprovfile> >	
</td <td colspan="2"><autoprovfile>audio[macaddress]</autoprovfile>></td>	<autoprovfile>audio[macaddress]</autoprovfile> >	
</td <td><autoprovfile>device[macaddress].xml</autoprovfile>></td>	<autoprovfile>device[macaddress].xml</autoprovfile> >	
<td>MiscSettings></td>	MiscSettings>	

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

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

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

The file 0020f7123456.xml contains:

- 1. The device will first set it's name to 'Newname'.
- 2. It will try to download http://example.com/common.xml.
- 3. It will try to download http://example.com/sip_reg0020f7123456.xml.
- 4. It will try to download http://example.com/audio0020f7123456.
- 5. It will try to download http://example.com/device.xml.

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

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

Checking for New Autoprovisioning files 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.

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

Table 2-22. Autoprovisioning File Name

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

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

For example:

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

The autoprovisioning filename is set to "cyberdata/"

On boot, the device will try to download:

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

...and if this fails:

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

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

Autoprovisioning <FirmwareSettings>

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

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

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

The <FirmwareFile> name can contain path elements (i.e. /path/to/firmware/10.3.0-uImage-[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>IndoorIntercom31SW</ProductString> <ProductString>IndoorIntercom31SW</ProductString> <ProductString>IndoorKeypad31</ProductString> <ProductString>OfficeRinger31</ProductString> <ProductString>OfficeRinger31SW</ProductString> <ProductString>OutdoorIntercom31SW</ProductString> <ProductString>OutdoorIntercom31</productString> <ProductString>OutdoorIntercom31</productString> <ProductString>OutdoorIntercom31</productString> <ProductString>OutdoorIntercom31SW</ProductString> <ProductString>OutdoorKeypad31</ProductString> <ProductString>OutdoorKeypad31</ProductString> <ProductString>Strobe31</ProductString> <ProductString>Strobe31</ProductString></productString></productString></productString></productString></productString></productString></productString></productString></productString></productString></productString></productString></productString></productString></productString></productString></productString></productString></productString></productString></productString></productString></productString> Autoprovisioning Example 1

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

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

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

00000cd.xml

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

sip_common.xml

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

sip_0020f7020001.xml

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

sip_0020f7020002.xml

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

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

- 1. Device1 changes its device name to CyberData Autoprovisioned.
- Device1 finds an AutoprovFile element containing the filename sip_common.xml. The device downloads sip_common.xml from "https://autoprovtest.server.net," and imports this configuration, setting the sip server to 10.0.0.253 and the remote port to 5060.3.
- 3. Device1 finds another AutoprovFile element containing the filename sip_[macaddress].xml. The device replaces the [macaddress] with its own mac address value creating sip_0020f7020001.xml, downloads this file from "https://autoprovtest.server.net," and imports this configuration. This sets the user ID to 198, the password to ext198, and the dialout extension to 204. Device1 is now finished with autoprovisioning.
Device2 goes through the same steps by setting its device name to **CyberData Autoprovisioned**, its SIP server to **10.0.0.253**, and its port to **5060**. When Device2 "sees" **sip_[macaddress].xml**, Device2 replaces it with its own mac address and downloads **sip_0020f7020002.xml** from "https:// autoprovtest.server.net." Device2 sets the SIP User ID to **500**, the password to **ext500**, and the dialout extension to **555**.

Autoprovisioning Example 2

Here is another example of setting up your autoprovisioning files:

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

0020f7020001.xml

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

0020f7020002.xml

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

common_settings.xml

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

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

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

Device2 does the same except it downloads **0020f7020002.xml** on boot and imports these values instead. The Sip User ID is **500**, password is **ext500**, and dialout extension is **555**. Device2 then downloads the **common_settings.xml** file and imports those values. The device name is set to **CyberData Autoprovisioned**, the SIP server is set to **10.0.253**, and the port is set to **5060**.

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

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

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

From the device specific xml, a pointer to a sip_common file

From the device specific xml, a pointer to the device specific sip_[macaddress].xml

From the common file, a pointer to sip_common.xml

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

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

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

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

2.3.13.2 Sample dhcpd.conf

```
#
# Sample configuration file for ISC dhcpd for Debian
#
ddns-update-style none;
option domain-name "voiplab";
option domain-name-servers 10.0.0.252;
option option-150 code 150 = ip-address;
option ntp-servers north-america.pool.ntp.org;
option space VendorInfo;
option VendorInfo.text code 10 = { text };
authoritative;
log-facility local7;
subnet 10.0.0.0 netmask 255.0.0.0 {
    max-lease-time 3600;
   default-lease-time 3600;
   option routers
                                   10.0.0.1;
    option subnet-mask
                                   255.0.0.0;
                                   "voiplab";
   option domain-name
    option domain-name-servers
                                  10.0.0.252;
    option time-offset
                                   -8;
                                                   # Pacific Standard Time
                                                                     # OPTION 72
#
     option www-server
                                    99.99.99.99;
                                      "10.0.1.52";
                                                                     # OPTION 66
#
     option tftp-server-name
#
      option tftp-server-name
                                     "http://test.cyberdata.net";
                                                                     # OPTION 66
                                                                     # OPTION 150
#
      option option-150
                                      10.0.0.252;
# These two lines are needed for option 43
     vendor-option-space VendorInfo;
                                                                     # OPTION 43
#
#
     option VendorInfo.text "http://test.cyberdata.net";
                                                                     # OPTION 43
```

range 10.10.0.1 10.10.2.1; }

2.3.13.3 Download Template Button

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

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

- 1. On the Autoprovisioning page, click on the Download Template button.
- 2. You will see a window prompting you to save a configuration file (**.xml**) to a location on your computer (Figure 2-28). 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 2-28.

🖲 Opening 0020f702bf18.xml 🔹 🕈 🗖 🗙					
You have chosen to open:					
O020f702bf18.xml which is: XML document (11.3 KB) from: https://10.10.1.50					
What should Firefox do with this file?					
Open with Text Editor (default)					
○ Save File					
Do this <u>a</u> utomatically for files like this from now on.					
Cancel OK					

Figure 2-28. Configuration File

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

2.3.14 Downloading the Firmware

To download the firmware to your computer:

- Download the latest firmware file from the **Downloads** tab at the following webpage: <u>http://www.cyberdata.net/voip/011049/</u>
- 2. Unzip the firmware version file. This file may contain the following:
- Firmware file
- Release notes
- 3. Log in to the SIP Call Button home page as instructed in Section 2.3.4, "Log in to the Configuration Home Page".
- 4. Click on the **Firmware** menu button to open the **Firmware** page. See Figure 2-29.



Figure 2-29. Firmware Page



- 5. Click on the Browse button, and then navigate to the location of the firmware file.
- 6. Select the firmware file.
- 7. Click on the **Upload** button.
- Note Do not reboot the device after clicking on the Upload button.
- **Note** This starts the upgrade process. Once the SIP Call Button has uploaded the file, the **Uploading Firmware** countdown page appears, indicating that the firmware is being written to flash. The SIP Call Button will automatically reboot when the upload is complete. When the countdown finishes, the **Firmware** page will refresh. The uploaded firmware filename should be displayed in the system configuration (indicating a successful upload and reboot).

8. Table 2-23 shows the web page items on the **Firmware** page.

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

Table	2-23.	Firmware	Parameters
10010			i araniotoro

2.3.15 Reboot the Device

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

1. Click on the **Reboot** button on the **Home** page (Figure 2-30). A normal restart will occur.

Figure 2-30. Home Page

Home	Device	Network	SIP	Sensor	Audiofiles	Events	DSR	Autoprov	Firmware
		_							
	C	ybe	rDa	ata S	SIP C	all	Butt	on	
Current Sta	tus		٨d	lmin Settir	as		Import S	ettinas	
	040100056		~~		igs		importo	cungs	
Serial Number:	00:20:17:02:56	f6	User	rname: a	idmin		Browse	No file selected.	
Firmware Version:	v11.3.1	10	Pase	sword:				_	
en anna e veraroll.			Con	firm Password:			Import Config		
IP Addressing:	DHCP								
IP Address:	10.10.1.46			Debust.	Tanala Uala		Export S	ettings	
Subnet Mask:	255.0.0.0		Sa	Reboot	i oggle Help			J	
Default Gateway:	10.0.0.1								
DNS Server 1:	10.0.0.252						Export Config		
DNS Server 2:									
SIP Volume:	0			/					
Multicast Volume:	0								
Ring Volume:	0								
Sensor Volume:	0								
Volume Boost:	Off								
Microphone Gain:	0								
SIP Mode:	Enabled								
Multicast Mode:	Disabled								
Event Reporting:	Disabled		/						
Nightringer:	Disabled								
Primary SIP Server	Begistered	/							
Backup Server 1:	Not registered								
Backup Server 2:	Not registered								
Nightringer Server	:Not registered								
		/							
	_								
	/								
	Rebo	ot							

2.4 Command Interface

Some functions on the device can be activated using simple POST commands to the web interface. The examples in Table 2-24 use the free unix utility, **wget commands**. However, any program that can send HTTP POST commands to the device should work.

2.4.1 Command Interface Post Commands

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

Device Action	HTTP Post Command ^a
Trigger relay (for configured delay)	wgetuser adminpassword adminauth-no-challengeno- check-certificatequiet -O /dev/null "https://10.0.3.71/cgi-bin/ command.cgi"post-data "test_relay=yes"
Place call to extension (example: extension 130)	wgetuser adminpassword adminauth-no-challengeno- check-certificatequiet -O /dev/null "https://10.0.3.71/cgi-bin/ command.cgi"post-data "call=130"
Terminate active call	wgetuser adminpassword adminauth-no-challengeno- check-certificatequiet -O /dev/null "https://10.0.3.71/cgi-bin/ command.cgi"post-data "terminate=yes"
Force reboot	wgetuser adminpassword adminauth-no-challengeno- check-certificatequiet -O /dev/null "https://10.0.3.71/cgi-bin/ command.cgi"post-data "reboot=yes"
Trigger the Door Sensor Test (Sensor Config page)	wgetuser adminpassword adminauth-no-challengeno- check-certificatequiet -O /dev/null "https://10.0.3.71/cgi-bin/ sensor.cgi"post-data "doortest=yes"
Trigger the Intrusion Sensor Test (Sensor Config page)	wgetuser adminpassword adminauth-no-challengeno- check-certificatequiet -O /dev/null "https://10.0.3.71/cgi-bin/ sensor.cgi"post-data "intrusiontest=yes"

Table 2-24. Command Interface Post Commands

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.

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

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

Table A-2. Gang Box Mounting Components

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

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

Section 2.2.5, "Activity and Link LEDs" explains how the Link and Status LEDs work.





Figure A-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 <u>www.CyberData.net</u> Phone: 800-CYBERDATA (800-292-3732) Fax: 831-373-4193

Sales Sales 831-373-2601, Extension 334

TechnicalThe fastest way to get technical support for your VoIP product is to submit a VoIP TechnicalSupportSupport 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 6

A

activate local relay (door sensor) 52 activate relay (door sensor) 40 activate relay (intrusion sensor) 40 activity LED 12 address, configuration login 19 alternative power input 4 announcing a speaker's IP address 13 audio configuration 42 audio configuration page 42 audio encodings 3 audio files, user-created 43 autoprovision at time (HHMMSS) 59 autoprovision when idle (in minutes > 10) 59 autoprovisioning 60 download template button 60 autoprovisioning autoupdate (in minutes) 59, 60 autoprovisioning configuration 58, 59 autoprovisioning filename 59 autoprovisioning server (IP Address) 59

B

backup SIP server 1 33 backup SIP server 2 33 backup SIP servers, SIP server backups 33 browsers supported 3

С

call button 12 call button configuration default IP settings 15 call button LED 14 changing the web access password 23 Chrome (web browser) 3 Cisco SRST 33 command interface 73 commands 73 configurable parameters 24, 30, 33, 56 configuration audio 42 default IP settings 15 door sensor 38 intrusion sensor 38 network 29, 55 SIP 32 using Web interface 15 configuration home page 19 configuration page configurable parameters 24, 30, 56 contact information 80 contact information for CyberData 80 Current Network Settings 30 current network settings 30 CyberData contact information 80

D

default device settings 81 gateway 15 IP address 15 subnet mask 15 username and password 15 web login username and password 19 default device settings 13 default gateway 15, 30 default IP settings 15 default login address 19 device configuration 23 device configuration parameters 59 the device configuration page 58 device configuration page 23 device configuration parameters 24 device configuration password changing for web configuration access 23 **DHCP Client 3** dial out extension (door sensor) 40, 52 dial out extension (intrusion sensor) 40 dial out extension strings 35, 37 dimensions 4 discovery utility program 19 DNS server 30 door sensor 38, 40, 52 activate local relay 52 activate relay 40 dial out extension 40, 52 door open timeout 40, 52 door sensor normally closed 40 flash button LED 40, 52 download autoprovisioning template button 60 DTMF tones 35, 37

DTMF tones (using rfc2833) 35

E

earth ground 76, 77 ethernet cable 75 ethernet I/F 4 expiration time for SIP server lease 34 export settings 21, 22

F

factory default settings 13 how to set 13 Firefox (web browser) 3 firmware where to get the latest firmware 70 flash button LED (door sensor) 40, 52 flash button LED (intrusion sensor) 40

G

gang box mounting 76, 77 get autoprovisioning template 60 GMT table 27 GMT time 27

Η

home page 19 http POST command 73 http web-based configuration 3

identifier names (PST, EDT, IST, MUT) 27 identifying your product 1 illustration of device mounting process 74 import settings 21, 22 installation, typical device system 2 intercom configuration page configurable parameters 33 Internet Explorer (web browser) 3 intrusion sensor 38, 40 activate relay 40 dial out extension 40 flash button LED 40 IP address 15, 30 IP addressing default IP addressing setting 15

J

J3 terminal block, 16 AWG gauge wire 6

L

lease, SIP server expiration time 34 LED green link LED 12 yellow activity LED 12 link LED 12, 75 local SIP port 34 log in address 19

Μ

mounting the device 74 Mozilla Firefox (web browser) 3

Ν

navigation (web page) 16 navigation table 16 network configuration 29 network configuration of intercom 55 Network Setup 29, 55 Nightringer 6, 69 NTP server 24

0

on-board relay 4, 8 operating temperature 4

Ρ

packet time 3 part number 4 parts list 5 82

password for SIP server login 33 login 19 restoring the default 15 payload types 4 point-to-point configuration 36 port local SIP 34 remote SIP 34 posix timezone string timezone string 24 POST command 73 power input 4 alternative 4 product configuring 15 mounting 74 parts list 5 product features 3 product overview product features 3 product specifications 4 supported protocols 3 supported SIP servers 3 typical system installation 2 product specifications 4 protocol 4 protocols supported 3

R

reboot 71, 72 remote SIP port 34 Reset Test Function Management (RTFM) switch 13 resetting the IP address to the default 74, 79 restoring factory default settings 13, 81 restoring the factory default settings 13 rport discovery setting, disabling 34 RTFM switch 13 RTP/AVP 3

S

Safari (web browser) 3 sales 80 sensor setup page 39, 51 sensor setup parameters 38 sensors 40, 52 server address, SIP 33 service 80 set time with external NTP server on boot 24 setting up the device 6 settings, default 13 SIP enable SIP operation 33 local SIP port 34 user ID 33 SIP (session initiation protocol) 3 SIP configuration 32 SIP Server 33 SIP configuration parameters outbound proxy 34 registration and expiration, SIP server lease 34 unregister on reboot 34 user ID. SIP 33 SIP registration 33 SIP remote SIP port 34 SIP server 33 password for login 33 SIP servers supported 3 unregister from 34 user ID for login 33 SRST 33 status LED 75 subnet mask 15, 30 supported protocols 3

T

tech support 80 technical support, contact information 80 terminal block, 16 AWG gauge wire 6 time zone string examples 27

U

user ID for SIP server login 33 username changing for web configuration access 23 default for web configuration access 19 restoring the default 15

V

VLAN ID 30 VLAN Priority 30 VLAN tagging support 30 VLAN tags 30

W

warranty policy at CyberData 80 web access password 15 web access username 15 web browsers supported 3 web configuration log in address 19 web page navigation 16 web page navigation 16 web-based configuration 15 weight 4 wget, free unix utility 73 wiring the circuit 9 devices less than 1A at 30 VDC 9