

Singlewire Strobe Operations Guide

Part #011244

Document Part #930829F for Firmware Version 11.3.0

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

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 930829F, which corresponds to firmware version 11.3.0, and was released on October 30, 2015, has the following changes:

- Updates the following specifications in Table 1-1, "Specifications"
 - Power Input: PoE 802.3af compliant or +8 to +12VDC @ 1000mA Regulated Power Supply
 - Speaker Output: 1 Watt Peak Power
 - On-Board Relay: 1A at 30 VDC
 - Dimensions: 5.118 inches [130 mm] Length, 2.252 inches [57.21 mm] Width, 5.118 inches [130 mm] Height
 - Weight: 1.0 lbs. (0.45 kg)
 - Boxed Weight: 2.0 lbs. (0.90 kg)
- Updates Figure 2-1, "Singlewire Strobe Connections"

Browsers Supported

The following browsers have been tested against firmware version 11.3.0:

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

Important Safety Instructions

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

14. WARNING: The Singlewire Strobe 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

Contents

Chapter 1 Product Overview	1
1.1 How to Identify This Product	
1.2 Typical System Installation	
1.3 Product Features	
1.4 Supported Protocols	
1.5 Specifications	4
Chapter 2 Installing the Singlewire Strobe	5
2.1 Parts List	
2.1 Singlewire Strobe Setup	
2.1.1 Singlewire Strobe Connections	
2.1.2 Connecting the Singlewire Strobe to the On-Board Relay	
2.1.3 Identifying the Singlewire Strobe Connectors and Jumpers	
2.1.4 Link and Activity LEDs	
2.1.5 Restore the Factory Default Settings	
2.2.1 Factory Default Settings	
2.2.2 Singlewire Strobe Web Page Navigation	
2.2.3 Using the Toggle Help Button	
2.2.4 Log in to the Configuration Home Page	
2.2.5 Configure the Device	
2.2.6 Configure the Strobe	
2.2.7 Configure the Network Parameters	
2.2.8 Configure the SIP Parameters	
2.2.9 Configure the Sensor Configuration Parameters	
2.2.10 Configure the Audio Configuration Parameters	
2.2.12 Configure the Event Parameters	
2.2.12 Configure the Autoprovisioning Parameters	
2.3.1 Reboot the Device	
2.4.1 Command Interface Post Commands	
	09
Appendix A Mounting the Singlewire Strobe	70
A.1 Mount the Singlewire Strobe	70
Appendix B Troubleshooting/Technical Support	75
B.1 Frequently Asked Questions (FAQ)	75
B.2 Documentation	
B.3 Contact Information	
B.4 Warranty and RMA Information	
Index	77

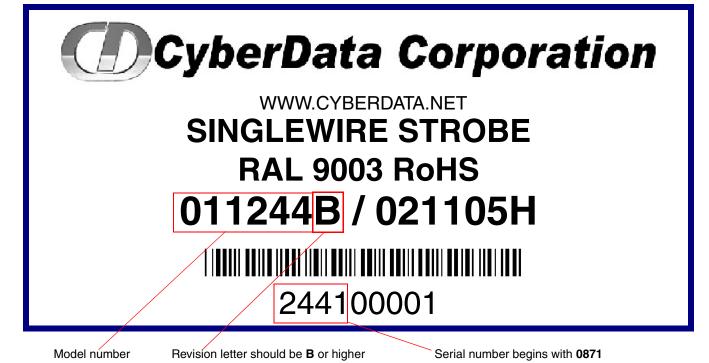
1 Product Overview

1.1 How to Identify This Product

To identify the Singlewire Strobe, 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 011244.
- The revision letter of the model number should be **B** or higher.
- The serial number on the label should begin with 2441.

Figure 1-1. Model Number Label

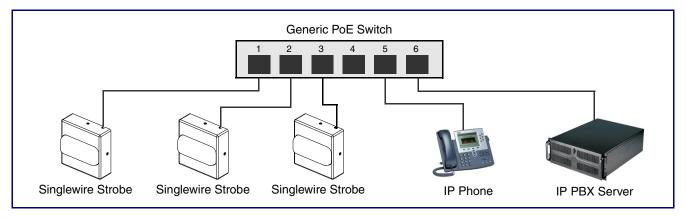


1

1.2 Typical System Installation

Figure 1-2 illustrate how the Singlewire Strobes can be installed as part of a VoIP phone system.

Figure 1-2. Typical Installation



GENERAL ALERT	Warning <i>Electrical Hazard:</i> The Singlewire Strobe 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.

1.3 Product Features

- Compatible with Singlewire InformaCast
- Meets ADA requirements for telephony signalling and notification
- Web-based setup
- PoE-powered

1.4 Supported Protocols

The Singlewire Strobe supports:

• HTTP Web-based configuration

Provides an intuitive user interface for easy system configuration and verification of Singlewire Strobe 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 Specifications

10/100 Mbps SIP RFC 3261 Compatible and InformCast v4.0 and later
SIP RFC 3261 Compatible and InformCast v4.0 and later
PoE 802.3af compliant or +8 to +12VDC @ 1000mA Regulated Power Supply ^a
Up to 90 candela (user-selectable)
5 user-defined scenes
100,000 Hours
1A at 30 VDC
-10° C to 50° C (14° F to 122° F)
G711, A-law and μ-law
4.5 inches [115 mm] Length
2.1 inches [55 mm] Width
4.5 inches [115 mm] Height
1.0 lbs. (0.45 kg)
2.0 lbs. (0.90 kg)
011244

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 Singlewire Strobe

2.1 Parts List

Table 2-2 illustrates the Singlewire Strobe parts.

Quantity	Part Name	Illustration
1	Singlewire Strobe Assembly	·
1	Installation Quick Reference Guide	
1	Singlewire Strobe Mounting Accessory Kit	

Table 2-2. Parts List

2.1 Singlewire Strobe Setup

2.1.1 Singlewire Strobe Connections

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

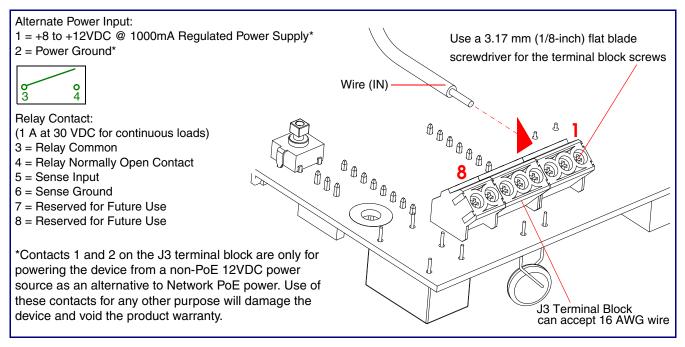
Note As an alternative to using PoE power, you can supply +8 to +12VDC @ 1000mA Regulated Power Supply into the terminal block.



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. Singlewire Strobe Connections



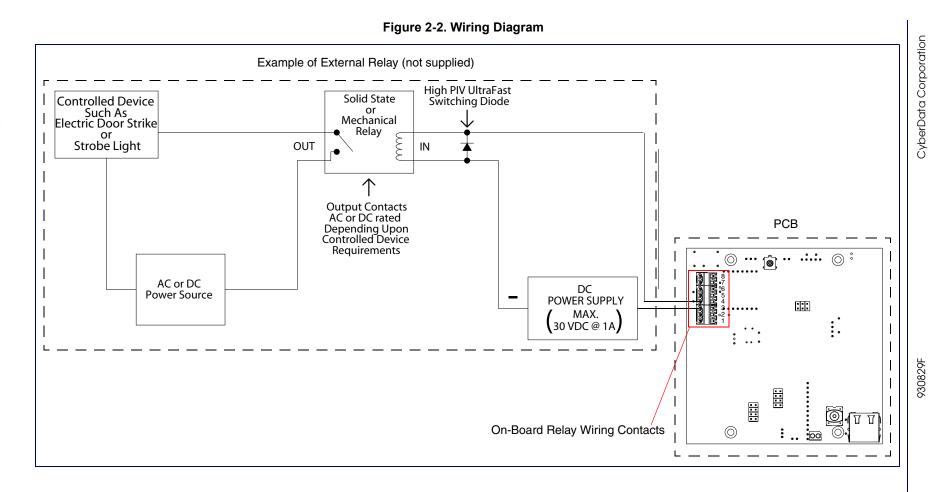
2.1.2 Connecting the Singlewire Strobe to the On-Board Relay

GENERAL ALERT	Warning <i>Electrical Hazard:</i> The device 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 <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.
	Warning The PoE connector is intended for intra-building connections only and does not route to the outside plant.

The device incorporates an on-board relay which enables users to control an external relay for activating an auxiliary device such as an electric door strike (see Figure 2-2, "Wiring Diagram").

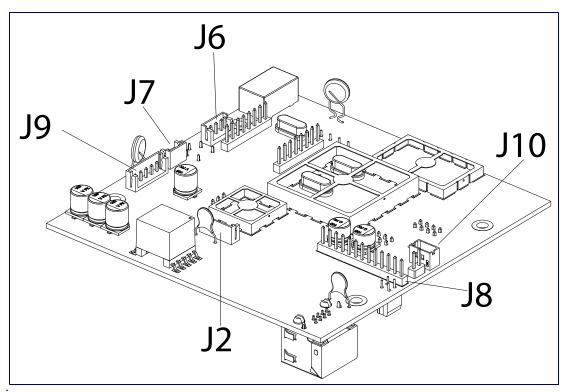
The relay contacts are limited to 1A at 30 VDC. The relay activation time is selectable through the web interface and is controlled by DTMF tones generated from the phone being called. The DTMF tones are selectable from the web interface as well.

GENERAL ALERT



2.1.3 Identifying the Singlewire Strobe Connectors and Jumpers

See the following figures and tables to identify the Singlewire Strobe connector locations and functions.



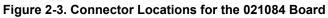


Table 2-3.	Connector	Functions
------------	-----------	-----------

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

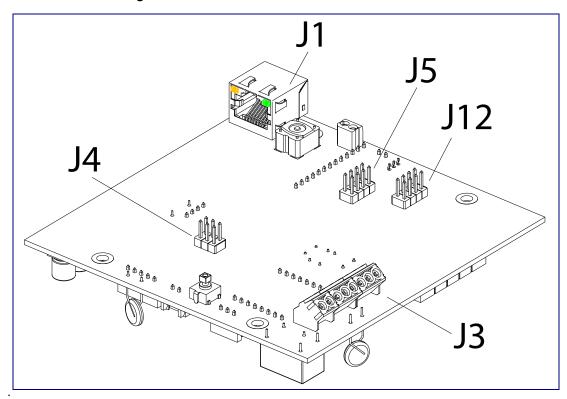


Figure 2-4. Connector Locations for the 021084 Board

Table 2-4. Connector Functions

J4 Reserved (Factory Use Only J5 Reserved (Factory Use Only	Connector Function		
J4 Reserved (Factory Use Only J5 Reserved (Factory Use Only	J1	Ethernet Connector	
J5 Reserved (Factory Use Only	J3	User Terminal Block Interface	
	J4	Reserved (Factory Use Only)	
J12 Reserved (Factory Use Only	J5	Reserved (Factory Use Only)	
	J12	Reserved (Factory Use Only)	

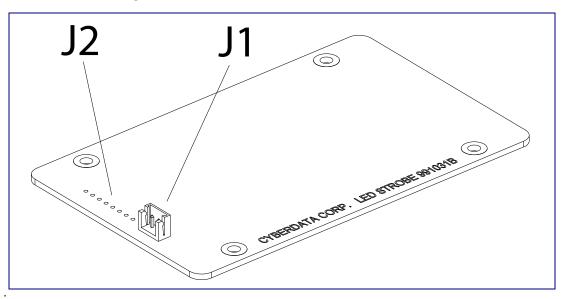


Figure 2-5. Connector Locations for the 021054 Board



Connector	Function
J1	Ethernet Connector
J2	Call Button Interface — Not Used

2.1.3.1 Connecting the 021054 and 021084 Boards with the 031142 Cable Assembly

Use Figure 2-6 to see how the 021054 and 021084 boards are connected with the 031142 cable assembly.

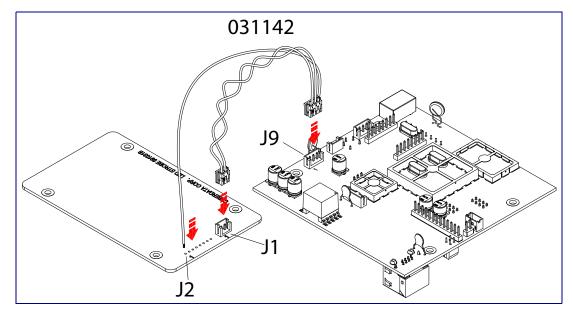


Figure 2-6. 021054 and 021084 Boards Connected with the 031142 Cable Assembly

2.1.4 Link and Activity LEDs

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

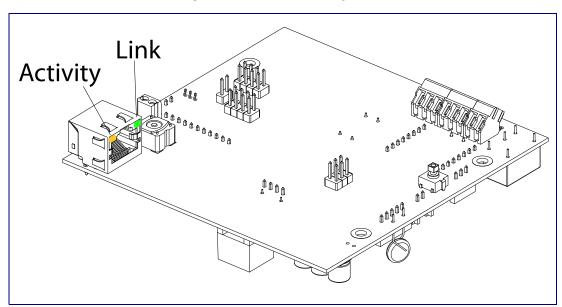


Figure 2-7. Link and Activity LEDs

2.1.5 Restore the Factory Default Settings

2.1.5.1 RTFM Switch

When the Singlewire Strobe is operational and linked to the network, use the Reset Test Function Management (RTFM) switch (Figure 2-8) to set the factory default settings.

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

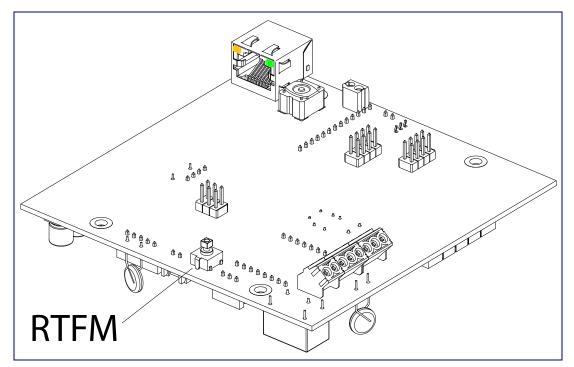


Figure 2-8. RTFM Switch

To set the factory default settings:

1. Press and hold the RTFM switch for seven seconds, and then release the RTFM switch.

2.2 Configure the Singlewire Strobe Parameters

To configure the Singlewire Strobe online, use a standard web browser.

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

2.2.1 Factory Default Settings

All Singlewire Strobes are initially configured with the following default IP settings:

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

Table 2-6. 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.

2.2.2 Singlewire Strobe Web Page Navigation

Table 2-7 shows the navigation buttons that you will see on every Singlewire Strobe web page.

Web Page Item	Description
Home	Link to the Home page.
Device	Link to the Device page.
Strobe	Link to the Strobe page.
Network	Link to the Network page.
SIP	Link to go to the SIP page.
Multicast	Link to the Multicast page.
Sensor	Link to the Sensor page.
Audiofiles	Link to the Audiofiles page.
Events	Link to the Events page.
Autoprov	Link to the Autoprovisioning page.
Firmware	Link to the Firmware page.

Table 2-7. Web Page Navigation

2.2.3 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

Toggle H	lelp

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	• 3	Question mark appears next to the
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

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.

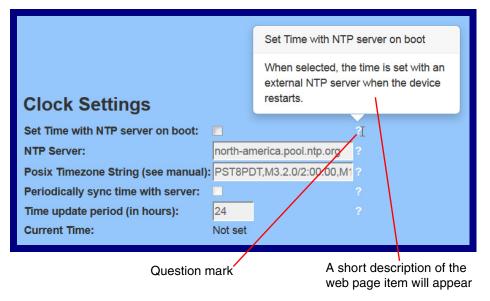


Figure 2-11. Short Description Provided by the Help Feature

2.2.4 Log in to the Configuration Home Page

- 1. Open your browser to the Singlewire Strobe 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 Singlewire Strobe.
- **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: <u>http://www.cyberdata.net/support/voip/discovery.html</u>

Note The Singlewire Strobe 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

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

	Home Device Strobe Network SIP Multicast Sensor Audiofiles Events Autoprov Firmware					
Admin Settings	Import Settings					
	Browse No file selected.					
Confirm Password:	Import Config					
Singlowire Status	Export Settings					
Singlewire Status						
Boot Time: 2015/01/08 12:50:22						
Current Time: 2015/01/08 13:31:41	Export Config					
B'casts Active: 0						
Save Reboot Toggle Help						
	Singlewire Status Boot Time: 2015/01/08 12:50:22 Current Time: 2015/01/08 13:31:41 IC Servers: 10.0.1.95 Do.0.1.96 Configuration File: InformaCastSpeaker.cfg B'casts Accepted: 0 B'casts Rejected: 0 B'casts Active: 0					

Figure 2-12. Home Page

3. On the Home Page, review the setup details and navigation buttons described in Table 2-8.

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.

Table 2-8. Home Page Overview

Web Page Item	Description
Singlewire Settings	
Boot Time	Shows the boot time.
Current Time	Shows the current time.
IC Servers	Shows the InformaCast server IP addresses.
Configuration File	Shows the configuration file.
B'casts Accepted	Shows the number of B'casts accepted.
B'casts Rejected	Shows the number of B'casts rejected.
B'casts Active	Shows the number of active B'casts.
Import Settings	
Browse	Click Browse 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 Reboot to store changes.
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 2-8. Home Page Overview (continued)

2.2.5 Configure the Device

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

			U		. Device e	0	5			
Home	Device	Strobe	Network	SIP	Multicast	Sensor	Audiofiles	Events	Autoprov	Firmware
			Cv		·Nat	2 6	troh	0		
			Cy	JEI	υαι	aJ	trob	C		
Misc Set	tings					Relay Se	ttings			
Device Name:		Cyber	Data VoIP Strobe			Activate Relay	During Ring:			
Blink Strobe o	n Ring:						During Night Ring			
Blink Strobe o						Activate Relay	While Call Active:			
Disable HTTP:	S (NOT recomme	ended): 🔲								
Clock Se	ettings									
Set Time with	NTP server on b	oot: 🔳								
NTP Server:		north-a	merica.pool.ntp.c	org						
Posix Timezor	ne String (see ma	anual): PST8P	DT,M3.2.0/2:00:0	0 0,M 1						
	nc time with ser		_							
	eriod (in hours):									
Current Time:		Not set								
Save Rel	poot									
Test Relay	Toggle Help									

Figure 2-13. Device Configuration Page

- 2. On the **Device Configuration** page, you may enter values for the parameters indicated in Table 2-9.
- **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				
Misc Settings					
Device Name ?	Type the device name. Enter up to 25 characters.				
Blink Strobe on Ring ?	When selected, the Strobe will blink a scene when ringing (including when the Nightringer is ringing, if enabled). Scenes can be selected on the Strobe Configuration Page .				
Blink Strobe on MWI ?	When selected, the strobe will blink a scene when a voicemail is waiting for its extension. Scenes can be selected on the Strobe Configuration Page .				
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 <mark>?</mark>	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 2.2.5.1, "Time Zone Strings" for information about how to use the Posix Timezone String to specify time zone and daylight savings time where applicable. Enter up to 63 characters.				
Periodically sync time with server ?	When selected, the time is periodically updated with the NTP server at the configured interval below.				
Time update period (in hours) ?	The time interval after which the device will contact the NTP server to update the time. Enter up to 4 digits.				
Current Time	Allows you to input the current time. (6 character limit)				

Table 2-9. Device Configuration Parameters

Web Page Item	Description				
Relay Settings					
Activate Relay During Ring 🛜	When selected, the relay will be activated for as long as the device is ringing. When Auto-Answer Incoming Calls is enabled, the device will not ring and this option does nothing.				
Activate Relay During Night Ring ?	When selected, the relay will be activated as long as the Nightringer extension is ringing.				
Activate Relay While Call Active 🛜	When selected, the relay will be activated as long as the SIP call is active.				
Test Relay	Click on the Test Relay button to do a relay test.				
	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 2-9. Device Configuration Parameters (continued)

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

2.2.5.1 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 2-10 shows some common strings.

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

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

Table 2-11 shows a breakdown of the parts that constitute the following time zone string:

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

Table 2-11	. Time Zone	String Parts
------------	-------------	--------------

Time Zone String Part	Meaning
CST6CDT	The time zone offset from GMT and three character identifiers for the time zone.
CST	Central Standard Time
6	The (hour) offset from GMT/UTC
CDT	Central Daylight Time
M3.2.0/2:00:00	The date and time when daylight savings begins.
М3	The third month (March)
.2	The 2nd occurrence of the day (next item) in the month
.0	Sunday
/2:00:00	Time of day to change
M11.1.0/2:00:00	The date and time when daylight savings ends.
M11	The eleventh month (November)
.1	The 1st occurrence of the day (next item) in the month
.0	Sunday
/2:00:00	Time of day to change

Time Zone String Examples

Table 2-12 has some more examples of time zone strings.

Table 2-12. Time Zone String Examples

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

a.Tokyo does not use daylight savings time.

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

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

Figure 2-14. 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 2-13 has information about the GMT time in various time zones.

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	
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	

Table 2-13. World GMT Table

2.2.6 Configure the Strobe

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

	CyberData S	Strobe
SIP Call Scene	MWI Scene	Nightringer Scene
Brightness: 255	Brightness: 255	Brightness: 255
ADA Compliant	ADA Compliant	 ADA Compliant
Slow Fade	◯ Slow Fade	Slow Fade
⊃ Fast Fade	◯ Fast Fade	○ Fast Fade
Slow Blink	O Slow Blink	◯ Slow Blink
◯ Fast Blink	◯ Fast Blink	Fast Blink
Multicast Scene	Sensor Scene	Intrusion Sensor Scene
Brightness: 255	Brightness: 255	Brightness: 255
ADA Compliant	ADA Compliant	ADA Compliant
○ Slow Fade	Slow Fade	◯ Slow Fade
◯ Fast Fade	◯ Fast Fade	○ Fast Fade
Slow Blink	O Slow Blink	O Slow Blink
⊃ Fast Blink	Fast Blink Save Reboot Toggle Help	○ Fast Blink
Preview Scenes		
Brightness: 255		
Fast Fade Slow Fade		
Fast Blink Slow Blink		
ADA Compliance		

2. On the **Device Configuration** page, you may enter values for the parameters indicated in Table 2-9.

2.2.6.1 Scenes

You can select one of five strobe flashing behaviors (called "scenes") and adjust the brightness for each event that would trigger the strobe (such as SIP ring, night ring, multicast, message waiting, sensor triggered, intrusion sensor triggered). The scenes are **ADA Compliance**, **Fast Fade**, **Slow Fade**, **Fast Blin**k, and **Slow Blink**.

Web Page Item	Description
SIP Call Scene	Use this section to select the strobe flashing behavior for the SIP Call event.
Brightness	How bright the strobe will blink on a SIP call. This is the maximum brightness for "fade" type scenes.
ADA Compliant	Strobe will blink on at the specified brightness for 150ms then off for 350ms during the duration of the event.
Slow Fade	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink	Strobe will blink on at the specified brightness for one second then off for one second during the duration of the event.
Fast Blink	Strobe will blink on at the specified brightness then off five times per second during the duration of the event.
MWI Scene	Use this section to select the strobe flashing behavior for the Message Waiting (MWI) event.
Brightness	How bright the strobe will blink when a message is waiting. This is the maximum brightness for "fade" type scenes.
ADA Compliant	Strobe will blink on at the specified brightness for 150ms then off for 350ms during the duration of the event.
Slow Fade	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink	Strobe will blink on at the specified brightness for one second then off for one second during the duration of the event.
Fast Blink	Strobe will blink on at the specified brightness then off five times per second during the duration of the event.
Nightringer Scene	Use this section to select the strobe flashing behavior for the Nightringer event.
Brightness	How bright the strobe will blink when the Nightringer is ringing. This is the maximum brightness for "fade" type scenes.
ADA Compliant	Strobe will blink on at the specified brightness for 150ms then off for 350ms during the duration of the event.
Slow Fade	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.

Table 2-14. Device Configuration Parameters

Web Page Item	Description
Fast Fade	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink	Strobe will blink on at the specified brightness for one second then off for one second during the duration of the event.
Fast Blink	Strobe will blink on at the specified brightness then off five times per second during the duration of the event.
Multicast Scene	Use this section to select the strobe flashing behavior for the Multicast event.
Brightness	How bright the strobe will blink on a multicast page. This is the maximum brightness for "fade" type scenes.
ADA Compliant	Strobe will blink on at the specified brightness for 150ms then off for 350ms during the duration of the event.
Slow Fade	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink	Strobe will blink on at the specified brightness for one second then off for one second during the duration of the event.
Fast Blink	Strobe will blink on at the specified brightness then off five times per second during the duration of the event.
Sensor Scene	Use this section to select the strobe flashing behavior for the Sensor event.
Brightness	How bright the strobe will blink when the sensor is triggered. This is the maximum brightness for "fade" type scenes.
ADA Compliant	Strobe will blink on at the specified brightness for 150ms then off for 350ms during the duration of the event.
Slow Fade	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink	Strobe will blink on at the specified brightness for one second then off for one second during the duration of the event.
Fast Blink	Strobe will blink on at the specified brightness then off five times per second during the duration of the event.
ntrusion Sensor Scene	Use this section to select the strobe flashing behavior for the Intrusion Sensor event.
Brightness	How bright the strobe will blink when the intrusion sensor is triggered. This is the maximum brightness for "fade" type scenes.
ADA Compliant	Strobe will blink on at the specified brightness for 150ms then off for 350ms during the duration of the event.
Slow Fade	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink	Strobe will blink on at the specified brightness for one second then off for one second during the duration of the event.

Table 2-14. Device Configuration Parameters (continued)

Web Page Item	Description
Fast Blink	Strobe will blink on at the specified brightness then off five times per second during the duration of the event.
Preview Scenes	Use this section to preview the strobe flashing behavior for the Scene button that is pressed.
Brightness	How bright the strobe will blink when previewing scenes.
Fast Fade	Click on the Fast Fade button to preview the Fast Fade strobe flashing mode.
Slow Fade	Click on the Slow Fade button to preview the Slow Fade strobe flashing mode.
Fast Blink	Click on the Fast Blink button to preview the Fast Blink strobe flashing mode.
Slow Blink	Click on the Slow Blink button to preview the Slow Blink strobe flashing mode.
ADA Compliance	Click on the ADA Compliance button to preview the ADA Compliance strobe flashing mode.
	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.
Note	• You must click on the Save button and then the Reboot button for the changes to take effect.

Table 2-14. Device Configuration	Parameters (continued)
----------------------------------	------------------------

2.2.7 Configure the Network Parameters

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

Figure 2-16. Network Configuration Page

DNS Server 2: 10.0.0.1 DHCP Timeout in seconds*: 60 * A value of -1 will retry forever Current Network Settings IP Address: 10.10.0.76 Subnet Mask: 255.0.0.0 Default Gateway: 10.0.1	Home	Device	Strobe	Network	SIP	Multicast	Sensor	Audiofiles	Events	Autoprov	Firmware
Stored Network Settings Addressing Mode: Static Static SpDevice023300 IP Address: SpDevice023300 IP Address: Stonet Mask: 255.000 Default Gateway: 10.0.1 DNS Server 1: 10.0.1 DNS Server 2: 10.0.1 DNS Server 1: 10.0.1 DNS Server 2: 10.0.1 DHOP Timeout in seconds*: *A value of -1 will retry torever Subret Mask: 255.000 Default Gateway: 10.00.1 Dis Server 1: Paddress: Paddress: 10.0.0.1 DNS Server 2: 10.0.1 DNS Server 2: 10.0.1 Drep Timeout in seconds*: 60 - - A value of -1 will retry torever Subret 1: 10.0.0.1 Dis Server 1: 10.0.0.252				Cvl	bei	Dat	a Si	trob	е		
Addressing Mode: Static DHCP VLAN ID (0-4095): 0 Hostname: SipDevice0233c0 VLAN Priority (0-7): 0 IP Address: 101.01.01 ULAN Priority (0-7): 0 Subnet Mask: 255.0.0.0 Default Gateway: 100.0.1 DNS Server 1: 100.0.1 DNS Server 2: 100.0.1 DHCP Timeout in seconds*: 60 - - * A value of -1 will retry forever Save Toggle Help IP Address: 10.10.76 Subnet Mask: 255.0.0 Default Gateway: 10.0.0.1 DNS Server 1: 10.00.252											
Addressing Mode: Static DHCP VLAN ID (0-4095): 0 Hostname: SipDevice0233c0 VLAN Priority (0-7): 0 IP Address: 10.0.0.10 0 0 Subnet Mask: 255.0.0.0 0 0 Default Gateway: 10.0.0.1 0 0 DNS Server 1: 10.0.0.1 0 0 DHCP Timeout in seconds*: 60 0 0 * A value of -1 will retry forever Toggle Help Toggle Help IP Address: 10.10.0.76 Subnet Mask: 255.0.0.0 Default Gateway: 10.0.0.1 Toggle Help Toggle Help	Stored N	letwork 9	Settings				VLAN Se	ttings			
Hostname: SpDevice0233c0 IP Address: 10.10.10 Subnet Mask: 255.0.0 Default Gateway: 10.0.1 DNS Server 1: 10.0.1 DNS Server 2: 10.0.1 DHCP Timeout in seconds*: 60 * A value of -1 will retry forever Save Reboot Toggle Help IP Address: 10.10.76 Subnet Mask: 255.0.0 Default Gateway: 10.0.1 DNS Server 1: 10.0.252											
IP Address: 10.10.10.10 Subnet Mask: 255.0.0.0 Default Gateway: 10.0.1 DNS Server 1: 10.0.1 DNS Server 2: 10.0.1 DHCP Timeout in seconds*: 60 * A value of -1 will retry forever Save Reboot Toggle Help IP Address: 10.10.76 Subnet Mask: 255.0.0 Default Gateway: 10.0.1 DNS Server 1: DNS Server 1: 10.0.252		_							_		
Subnet Mask: 255.0.0 Default Gateway: 100.0.1 DNS Server 1: 10.0.1 DNS Server 2: 10.0.1 DHCP Timeout in seconds*: 60 * A value of -1 will retry forever Save Toggle Help Save Reboot Toggle Help IP Address: 10.10.76 Subnet Mask: 255.0.0 Default Gateway: 10.0.1 Untercolspan="2">Toggle Help				-			(
Default Gateway: 10.0.1 DNS Server 1: 10.0.1 DNS Server 2: 10.0.1 DHCP Timeout in seconds*: 60 * A value of -1 will retry forever Save Reboot Toggle Help Save Reboot Toggle Help Default Gateway: 10.0.76 Subnet Mask: 255.0.0 Default Gateway: 10.0.252		-		-							
DNS Server 1: 10.0.0.1 DNS Server 2: 10.0.0.1 DHCP Timeout in seconds*: 60 * A value of -1 will retry forever Current Network Settings IP Address: 10.10.0.76 Subnet Mask: 255.0.0 Default Gateway: 10.0.1 DNS Server 1: 10.0.252				-							
DNS Server 2: 10.0.0.1 DHCP Timeout in seconds*: 60 * A value of -1 will retry forever Current Network Settings IP Address: 10.10.0.76 Subnet Mask: 255.0.0 Default Gateway: 10.0.1 DNS Server 1: 10.0.252	DNS Server 1:			-							
DHCP Timeout in seconds*: 60 * A value of -1 will retry forever Current Network Settings IP Address: 10.10.0.76 Subnet Mask: 255.0.0 Default Gateway: 10.0.1 DNS Server 1: 10.0.252	DNS Server 2:										
* A value of -1 will retry forever Current Network Settings IP Address: 10.10.0.76 Subnet Mask: 255.0.0 Default Gateway: 10.0.1 DNS Server 1: 10.0.252											
Current Network Settings IP Address: 10.10.0.76 Subnet Mask: 255.0.00 Default Gateway: 10.0.01 DNS Server 1: 10.0.252			1								
Current Network Settings IP Address: 10.10.0.76 Subnet Mask: 255.0.00 Default Gateway: 10.0.01 DNS Server 1: 10.0.252											
Current Network Settings IP Address: 10.10.0.76 Subnet Mask: 255.0.00 Default Gateway: 10.0.01 DNS Server 1: 10.0.252								-			
IP Address: 10.10.0.76 Subnet Mask: 255.0.0 Default Gateway: 10.0.0.1 DNS Server 1: 10.0.252	Current	Network	Settings				Save Reb	Toggle Help			
Subnet Mask: 255.0.0 Default Gateway: 10.0.0.1 DNS Server 1: 10.0.0.252											
Default Gateway: 10.0.0.1 DNS Server 1: 10.0.0.252	Subnet Mask:										
DNS Server 2:	DNS Server 1:										
	DNS Server 2:										

- 2. On the Network Configuration page, enter values for the parameters indicated in Table 2-15.
- **Note** The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Description
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 2.2.1, "Factory Default Settings" for factory default settings. Be sure to click Save and Reboot to store changes when configuring a Static address.
This is the hostname provided by the DHCP server. See the DHCP/ DNS server documentation for more information. Enter up to 64 characters.
Enter the Static IPv4 network address in dotted decimal notation.
Enter the Subnet Mask in dotted decimal notation.
Enter the Default Gateway IPv4 address in dotted decimal notation.
Enter the primary DNS Server IPv4 address in dotted decimal notation.
Enter the secondary DNS Server IPv4 address in dotted decimal notation.
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.
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.
Specify the IEEE 802.1p VLAN priority level. Enter 1 digit. A value of 0 may cause the VLAN ID tag to be ignored.
Shows the current network settings.
Shows the current Static IP address.
Shows the current Subnet Mask address.
Shows the current Default Gateway address.
Shows the current DNS Server 1 address.
Shows the current DNS Server 2 address.

Table 2-15. 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 2-15. Network Configuration Parameters (continued)

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

2.2.8 Configure the SIP Parameters

- 1. Click SIP Config to open the SIP Configuration page (Figure 2-17).
- Note For specific server configurations, go to the following website address: http://www.cyberdata.net/support/server/index.html

Figure 2-17. SIP Configuration Page

		ho	Dat	a Ci	roh			
	U y	DCI	υαι					
SIP Settings				Nightring	er Setting	5		
Enable SIP operation:				Enable Nightring	ger:			
Register with a SIP Server:	×			SIP Server:		10.0.0.253		
Use Cisco SRST:				Remote SIP Port	:	5060		
Primary SIP Server:	10.0.0.253			Local SIP Port:		5061		
Primary SIP User ID:	199			Outbound Proxy	<i>r</i> :			
Primary SIP Auth ID:	199			Outbound Proxy	Port:	0		
Primary SIP Auth Password:	•••••			User ID:		241		_
				Authenticate ID:		241		_
Backup SIP Server 1:				Authenticate Pa			_	
Backup SIP User ID 1:				Re-registration I	nterval (in secon	is): 360		
Backup SIP Auth ID 1:								
Backup SIP Auth Password 1:		_		Dial Out S	Settings			
Backup SIP Server 2:				Dial out Extensi	on: 204		-	
Backup SIP User ID 2:				Extension ID:	id204		-	
Backup SIP Auth ID 2:								
Backup SIP Auth Password 2:				Call Disc	onnection			
Remote SIP Port:	5060			Terminate Call a	fter delay: 0			
Local SIP Port:	5060							
Outbound Proxy:								
Outbound Proxy Port:	0	_						
RTP Settings				Save Rebo	ot Toggle Help			
RTP Port (even): 10500					- oggio Holp			

- 2. On the SIP Configuration page, enter values for the parameters indicated in Table 2-16.
- **Note** The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-16. SIP Configuration Parameters	
Description	

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

Web Page Item	Description
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.
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.
Nightringer Settings	
Enable Nightringer 🛜	When Nightringer is enabled, the device will attempt to register a second extension with the SIP server. Any calls made to this extension will play a ringtone (corresponds to Night Ring on the Audiofiles page). By design, it is not possible to answer a call to the Nightringer extension.
SIP Server 🛜	Enter the SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's Nightringer extension on the SIP server. This field can accept entries of up to 255 characters in length.
Remote SIP Port ?	The Remote SIP Port is the port number the device will use as the destination port when sending SIP messages for the Nightringer extension. The default Remote SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
Local SIP Port ?	The Local SIP Port is the port number the device will use to receive SIP messages for the Nightringer extension. This value cannot be the same as the Local SIP Port for the primary extension. The default Local SIP Port is 5061. The supported range is 0-65536. Enter up to 5 digits.
Outbound Proxy 🛜	Enter the Outbound Proxy address as an IPv4 address in dotted decimal notation or a fully qualified domain name (FQDN). When an IP address is configured, the device will send all SIP messages to this IP address for the Nightringer extension. When an FQDN is configured, the device will run DNS NAPTR, SRV, and A queries on the FQDN to resolve an IP address to which it will send all SIP messages for the Nightringer extension. This field can accept entries of up to 255 characters in length.

Table 2-16. SIP Configuration Parameters (continued)

Web Page Item	Description
Outbound Proxy Port ?	The Outbound Proxy Port is port number used as the destination port when sending SIP messages to the outbound proxy for the Nightringer extension. A value of 0 will default to 5060. The supported range is 0-65536. Enter up to 5 digits.
User ID ?	Specify the SIP User ID for the SIP server. This parameter becomes the user portion of the SIP-URI for the device's Nightringer extension. Enter up to 64 alphanumeric characters.
Authenticate ID ?	Specify the Authenticate ID for the SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Authenticate Password ?	Specify the Authenticate Password for the SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Re-registration Interval (in seconds)	The SIP Re-registration Interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
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 2.2.8.1, "Dial Out Extension Strings and DTMF Tones (using rfc2833)".
Extension ID ?	A Caller identification string added to outbound calls. Enter up to 64 alphanumeric characters.
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.
Note You mus effect.	st click on the Save button and then the Reboot button for the changes to take
Note For spec	ific server configurations, go to the following website address:
http://wv	/w.cyberdata.net/support/server/index.html

Table 2-16. SIP Configuration Parameters (continued)

2.2.8.1 Dial Out Extension Strings and DTMF Tones (using rfc2833)

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

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 2-17. Examples of Dial-Out Extension Strings

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

2.2.8.2 Point-to-Point Configuration

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

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

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

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

SIP Settings Enable SIP operation:	-	Enable Nightrir	er Settings	•	
Enable SIP operation:	-	Nightring Enable Nightrin			
Enable SIP operation:]	Enable Nightrir	er Settings		
Enable SIP operation:]	Enable Nightrir	er Settings		
Register with a SIP Server: Use Cisco SRST:)]				
Use Cisco SRST:			ger:		
_		SIP Server:		10.0.0.253	
_		Remote SIP Po	t:	5060	
Primary SIP Server: 10	.0.0.253	Local SIP Port:		5061	
Primary SIP User ID: 19		Outbound Prop	y:		
Primary SIP Auth ID: 19		Outbound Prop	y Port:	0	
Primary SIP Auth Password:		User ID:		241	 _
		Authenticate IE		241	 _
Backup SIP Server 1:		Authenticate P		•••••	
Backup SIP User ID 1:		Re-registration	Interval (in seconds): 360	
Backup SIP Auth ID 1:					
Backup SIP Auth Password 1:		Dial Out	Settings		
Backup SIP Server 2:		Dial out Extens	ion: 204		
Backup SIP User ID 2:		Extension ID:	id204		
Backup SIP Auth ID 2:					
Backup SIP Auth Password 2:		Call Disc	onnection		
Demote OID Dest:	20	Terminate Call			
Remote SIP Port: 50 Local SIP Port: 50	60	reminate Call	and delay.		
Outbound Proxy:					
Outbound Proxy: 0					
RTP Settings		Cours Date	Tanala Mala		
RTP Port (even): 10500		Save Reb	oot Toggle Help		

Device is set to NOT register with a SiP server

2.2.8.3 Delayed DTMF

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

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 2-18. Examples of Dial-Out Extension Strings

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

2.2.9 Configure the Multicast Parameters

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

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

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

- **Note** The Singlewire Strobe does not play audio, but the Strobe LED will light up in whatever pattern is selected in the **Multicast Scene** on the **Strobe Configuration Page**.
- 1. Click on the Multicast menu button to open the Multicast page. See Figure 2-19.

Figure 2-19. Multicast Configuration Page

Home Device Strobe N	letwork	SIP	Multicast	Sensor	Audiofiles	Events	Autoprov	Firmware	
					_				
C	Cy	ber	Dat	a St	rob	e			
Multicast Settings									
		Er	nable Multicast (Operation:					
	Priority	Address	Port	Name	Веер				
	9	239.168.3.10	11000	Emergency					
	8	239.168.3.9	10000	MG8					
	7	239.168.3.8	9000	MG7					
	6	239.168.3.7	8000	MG6					
	5	239.168.3.6	7000	MG5					
	4	239.168.3.5	6000	MG4					
	3	239.168.3.4	5000	MG3					
	2	239.168.3.3	4000	MG2					
	1	239.168.3.2	3000	MG1					
	0	239.168.3.1	2000	Background Mu	usic				
		c 11	^o calls are consid	ered priority 4.5					
			rt range can be fr						
			Ports must be ev						
	A			and 0 is the lowes www.ssupersede					
		Priority S	9 streams will play	at maximum volu	ime				
		* You ne		hanges to take ef	fect				
			Save	Reboot					

- 2. On the Multicast 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
Enable Multicast Operation	Enables or disables multicast operation.
Priority	Indicates the priority for the multicast group. Priority 9 is the highest (emergency streams). 0 is the lowest (background music). SIP calls are considered priority 4.5 . See Section 2.2.9.1 , "Assigning Priority" for more details.
Address	Enter the multicast IP Address for this multicast group (15 character limit).
Port	Enter the port number for this multicast group (5 character limit [range can be from 2000 to 65535]).
	Note : The multicast ports have to be even values. The webpage will enforce this restriction.
Name	Assign a descriptive name for this multicast group (25 character limit).
Веер	When selected, the device will play a beep before multicast audio is sent.
	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.

Table 2-19. Multicast Configuration Parameters

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

2.2.9.1 Assigning Priority

The device will prioritize simultaneous audio streams according to their priority in the list.

If both SIP and Multicast is enabled, SIP audio streams are considered priority **4.5**. SIP audio will interrupt multicast streams with priority **0** through **4** and will be interrupted by multicast streams with priority **5** through **9**.

During priority **9** multicast streams, the volume is set to maximum.

Note SIP calls, multicast streams, ring tones, ringback tones, and nightring tones are all prioritized.

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

2.2.10 Configure the Sensor Configuration Parameters

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

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

Each sensor can trigger the following actions:

- Flash the LED until the sensor is deactivated (roughly 10 times/second)
- · Activate the relay until the sensor is deactivated
- **Note** Calling a preset extension can be set up as a point-to-point call, but currently cannot send delayed DTMF tones.
- 1. Click the Sensor menu button to open the Sensor page (Figure 2-20).

Figure 2-20. Sensor Configuration Page

Home	Device	Strobe	Network	SIP	Multicast	Sensor	Audiofiles	Events	Autoprov	Firmware
			C	ha			tue b			
			Cy	bei	Dal	a 5	trob	e		
Door Se	nsor Set	ttings				Intrusion	Sensor Se	ettings		
Door Sensor	Normally Clos	sed: O _{Yes}	O No			Blink Strobe:				
Door Open Ti	imeout (in sec	onds): 0				Activate Relay:				
Blink Strobe:						Make call to ex	tension:			
Activate Relay	y:					Dial Out Extens	sion: 204			
Make call to e	extension:					Dial Out ID:	id204			
Dial Out Exter	nsion:	204				Play recorded	audio:			
Dial Out ID:		id204								
Play recorded	audio:									
	_									
Save Re	aboot Toggi	le Help								
Test Door S	ensor Test	Intrusion Senso	or							

- 2. On the Sensor 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
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.
Blink Strobe 🛜	When selected, the Strobe will blink a scene until the on-board door sensor is deactivated. Scenes can be selected on the Strobe Configuration Page .
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	
Blink Strobe ?	When selected, the Strobe will blink a scene until the on-board door sensor is deactivated. Scenes can be selected on the Strobe Configuration Page .
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.

Table 2-20. Sensor Configuration Parameters

Web Page Item	Description
Test Door Sensor	Click the Test Door Sensor button to test the door sensor.
Test Intrusion Sensor	Click the Test Intrusion Sensor button to test the Intrusion sensor.
	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 2-20. Sensor Configuration Parameters (continued)

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

2.2.11 Configure the Audio Configuration Parameters

The **Audiofiles** page is used to add custom audio to the board. User uploaded audio will take precedence over the audio files shipped with the device.

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

Figure 2-21. Audiofiles Configuration Page

Home	Device	Strobe	Network	SIP	Multicast	Sensor	Audiofiles	Events	Autoprov	Firmware
			Cyl	oer	Dat	a Si	trob	e		
		ntrusion Sense	or Triggered: Cur	rently set too	Available Spac	e: 36.18MB				
	ı	Door Ajar:	Cur	rently set too	Browse	. No file selecte	ed. Pla	y Delete	Save	
					Browse	. No file selecte	ed. Pla	y Delete	Save	

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

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.
Intrusion Sensor Triggered	Corresponds to the message "Intrusion Sensor Triggered" (24 character limit).
Door Ajar	Corresponds to the message "Door Ajar" (24 character limit).
Browse	Click on the Browse button to navigate to and select an audio file.
Play	The Play button will play that audio file.
Delete	The Delete button will delete any user uploaded audio and restore the stock audio file.
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 2-21. Audiofiles Configuration Parameters

2.2.11.1 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 2-22 through Figure 2-24.

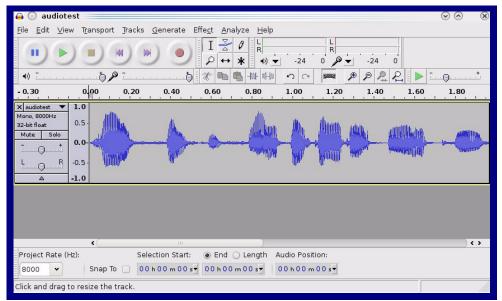


Figure 2-22. Audacity 1

Figure	2-23.	Audacity	2
--------	-------	----------	---

🔒 💽 Edit Metadata 🚃		\odot \odot \otimes
Use arrow keys (or RETURN ke	ey after editing) to navigate fi	elds.
Tag Name	Tag Value	
Artist Name		
Track Title		
Album Title		
Track Number		
Year		
Genre		
Comments		
Add	<u>R</u> emove <u>C</u> lea	r
Genres	Template	
E <u>d</u> it Rese <u>t</u>	Load Save	. S <u>e</u> t Default
		⊇ancel ♥ <u>0</u> K

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	.wav	
Save in <u>f</u> older: 📄 tmp		~ \
✓ Browse for other folders		
🙋/ tmp/		Create Fo <u>l</u> der
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
		<u>^</u>
		×
<u>A</u> dd		WAV (Microsoft) signed 16 bit PCM 👻
	Options	

Figure 2-24. WAV (Microsoft) signed 16 bit PCM

WAV (Microsoft) signed 16 bit PCM

2.2.12 Configure the Event Parameters

The **Events** page specifies a remote server that can be used to receive HTTP POST events when actions take place on the board.

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

Figure 2-25. Event Configuration Page

Event Server Event Server IP Address: Inable Relay Activated Events: Inable Relay Deactivated Events: Inable Ring Events: Inable Multicast Start Events: Inable Multicast Stop Events: Inable Power On Events: Inable Sensor Events: Inable Security Events:		Cy	berDa	ia Ji			
Event Server Event Server IP Address: Inable Relay Activated Events: Inable Relay Deactivated Events: Inable Ring Events: Inable Multicast Start Events: Inable Multicast Stop Events: Inable Power On Events: Inable Sensor Events: Inable Security Events:							
Server IP Address: 10.0.250 nable Relay Activated Events: Server Port: nable Relay Deactivated Events: Server URL: mable Ring Events: Server URL: nable Night Ring Events: Server URL: nable Multicast Start Events: Server URL: nable Multicast Stop Events: Server URL: nable Sensor Events: Server URL:	Enable Event Generation:			Event Ser	ver		
hable Relay Activated Events: server URL: xmiparse_engine hable Relay Deactivated Events: nable Multicast Start Events: nable Multicast Stop Events: nable Power On Events: nable Sensor Events: nable Security Events:	Events						
nable Relay Deactivated Events: nable Ring Events: nable Night Ring Events: nable Multicast Start Events: nable Multicast Stop Events: nable Power On Events: nable Sensor Events: nable Security Events:	Enable Relay Activated Events:			Server Port:	8080		
nable Night Ring Events: nable Multicast Start Events: nable Multicast Stop Events: nable Power On Events: nable Sensor Events: nable Security Events:	Enable Relay Deactivated Event	ts:		Server URL:	xmlparse_engine	e	
nable Multicast Start Events: nable Multicast Stop Events: nable Power On Events: nable Sensor Events: nable Security Events:	Enable Ring Events:						
nable Multicast Stop Events: nable Power On Events: nable Sensor Events: nable Security Events:	Enable Night Ring Events:						
nable Power On Events:	Enable Multicast Start Events:						
nable Sensor Events:	Enable Multicast Stop Events:						
nable Security Events:	Enable Power On Events:						
	Enable Sensor Events:						
nable 60 Second Heartbeat:	Enable Security Events:						
	Enable 60 Second Heartbeat:						
heck All Uncheck All	Check All	Uncheck All					

- 2. On the Events page, enter values for the parameters indicated in Table 2-22.
- **Note** The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

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 Relay Activated Events ?	When selected, the device will report relay activation.		
Enable Relay Deactivated Events 🛜	When selected, the device will report relay deactivation.		
Enable Ring Events 🛜	When selected, the device will report when it starts ringing upon an incoming SIP call. A Ring Event will not be generated when Auto-Answer Incoming Calls is enabled on the Device page.		
Enable Night Ring Events ?	When selected, the device will report when it starts ringing upon an incoming SIP call to the Nightringer extension. As a reminder, the Nightringer extension always rings upon an incoming SIP call and it is not possible to alter this behavior.		
Enable Multicast Start Events ?	When selected, the device will report when the device starts playing a multicast audio stream.		
Enable Multicast Stop Events ?	When selected, the device will report when the device stops playing a multicast audio stream.		
Enable Power On Events ?	When selected, the device will report when it boots.		
Enable Sensor Events 🛜	When selected, the device will report when the on-board sensor is activated.		
Enable 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 <mark>?</mark>	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.		

s

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.

Table 2-22. Events Configuration Parameters (continued)

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

2.2.12.1 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>
</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
</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>MULTICAST START
<index>8</index>
</cyberdata>
POST xmlparse engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 233
Content-Type: application/x-www-form-urlencoded
```

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData SIP Device' MAC='0020f70015b6'>
<event>MULTICAST_STOP</event>
<index>8</index>
</cyberdata>
```

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

Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>

<cyberdata NAME='CyberData SIP Device' MAC='0020f70015b6'>

User-Agent: CyberData/1.0.0

<event>NIGHTRINGING</event>

Host: 10.0.3.79

</cyberdata>

Content-Length: 234

2.2.13 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 2-26.

Figure 2-26. Autoprovisioning Page

Home	Device	Strobe	Network	SIP	Multicast	Sensor	Audiofiles	Events	Autoprov	Firmware
			Cv	be	rDat	ta S ⁱ	trob	е		
			- ,							
Disable Autop	orovisioning:									
Autoprovision										
Autoprovision	ning Filename:									
Use tftp: Username:										
Password:										
	ning autoupda	te (in minutes):	0							
Autoprovision										
Autoprovision	n when idle (in	minutes > 10):	0							
See the manual	l to learn how to	o use autoprovisi	oning to config	ure your dev	ice.					
Autoprovisionin										
		configured serve								
If these haven't	t been configure	d, it will look for	an autoprovisio	oning server	in your list of DH	CP options and tr	r to download '002	0f70233c0.xml" a	and if this fails, '000	0000cd.xml".
Save Rel	boot Toggle	Help								
Download Te	mplate									
Autoprovisio	oning log									
00:00 Autopro 00:00 Autopro 00:00 Got aut 00:00 Autopro 00:00 Autopro 00:00 Got aut 00:00 Autopro 00:00 Autopro 00:00 Got aut	ov looking for 00 toprov file. Pars ov found option ov looking for 00 toprov file. Pars ov found option ov looking for 00 toprov file. Pars	28 43 in DHCP sen 120170233c0.xml ing "0020170233 72 in DHCP sen 120170233c0.xml ing "0020170233 150 in DHCP sen 120170233c0.xml ing "0020170233 66 in DHCP sen	at http://chaim c0.xml" ver="10.0.0.252 at 10.0.0.252 c0.xml" rver="10.0.0.252 at 10.0.0.252 c0.xml"	ners.cyberda ?" i2"	ta.net					

- 2. On the **Autoprovisioning** page, you may enter values for the parameters indicated in Table 2-23.
- **Note** The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Web Page Item	Description
Disable Autoprovisioning ?	Prevent the device from automatically trying to download a configuration file. See Section 2.2.13.1, "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 2-9).
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 2-9).
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 2-9).
	Click the Save button to save your configuration settings.
Save	Note: You need to reboot for changes to take effect.

Table 2-23. 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 2.2.13.3, "Download Template Button"		
Autoprovisioning Log	The autoprovisioning log reflects the steps the device takes with autoprovisioning, relaying information about the server, DHCP options, configuration file names, and success or failure of finding and parsing the files.		

 Table 2-23. Autoprovisioning Configuration Parameters (continued)

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

2.2.13.1 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 2.2.13.2, "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 2-23). This file contains every configuration option that can be set on the board.

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

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

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

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 2-24. 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>OfficeRinger31SW</ProductString> <ProductString>OutdoorIntercom31SW</ProductString> <ProductString>OutdoorIntercom31</ProductString> <ProductString>OutdoorIntercom31SW</ProductString> <ProductString>OutdoorIntercom31SW</ProductString> <ProductString>OutdoorKeypad31</ProductString> <ProductString>Strobe31</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> Autoprovisioning Example 1

ioning 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.

2.2.13.2 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; }

2.2.13.3 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 2-27). 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 2-27.

😣 Openin	g 0020f702bf18.xml 🔹 🕈 🗆 🗙				
You have chosen to open:					
OO20f702bf18.xml which is: XML document (11.3 KB) from: https://10.10.1.50					
What should Firefox do with this file?					
Open with Te	kt Editor (default) 🔹				
○ <u>S</u> ave File					
Do this <u>a</u> utoma	tically for files like this from now on.				
	Cancel OK				

Figure 2-27. 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 Upgrade the Firmware and Reboot the Singlewire Strobe



Caution

Equipment Hazard: Devices with a serial number that begins with 2441xxxxx can only run firmware versions 10.0.0 or later.

To upload the firmware from your computer:

1. Retrieve the latest Singlewire Strobe firmware file from the Singlewire Strobe **Downloads** page at:

http://www.cyberdata.net/products/voip/digitalanalog/strobev3singlewire/downloads.html

- 2. Unzip the firmware version file. This file may contain the following:
- Firmware file
- Release notes
- 3. Log in to the Singlewire Strobe home page as instructed in Section 2.2.4, "Log in to the Configuration Home Page".
- 4. Click on the Firmware button to open the Firmware page. See Figure 2-28.



Caution

Equipment Hazard: CyberData strongly recommends that you first reboot the device before attempting to upgrade the firmware of the device. See Section 2.3.1, "Reboot the Device".

Figure 2-28. Firmware Page

Home	Device	Strobe	Network	SIP	Multicast	Sensor	Audiofiles	Events	Autoprov	Firmware	
			Cyl	bel	Dat	a Si	trob	е			
Current Firmwa	are Version: v11	.3.0		lease specif Browse	<u> </u>		U	pload			

- 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 Singlewire Strobe has uploaded the file, the **Uploading Firmware** countdown page appears, indicating that the firmware is being written to flash. The Singlewire Strobe 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 successful upload and reboot).
- 8. Table 2-25 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 firmware file that you want to upload.		
Upload	Click on the Upload button to automatically upload the selected firmware and reboot the system.		

Table 2-25.	Firmware	Parameters
-------------	----------	------------

2.3.1 Reboot the Device

To reboot a Singlewire Strobe, log in to the web page as instructed in Section 2.2.4, "Log in to the Configuration Home Page".

1. Click on the **Reboot** button on the **Home** page (Figure 2-29). A normal restart will occur.

Figure 2-29. Home Page

				strobe		
		Cybe.	Dutu C			
Current St	atus	Admin	Settings	Imp	ort Settings	
Serial Number:	087100106					
Mac Address:	00:20:f7:02:33:c0	Username:	admin	Brow	No file selected.	
Firmware Version:		Password:				
		Confirm Pas	ssword:	Impo	rt Config	
IP Addressing:	DHCP			_		
IP Address:	10.10.0.76	Cingle	uiro Statua	Exp	ort Settings	
Subnet Mask:	255.0.0.0	Singlet	wire Status		Ŭ	
Default Gateway:		Boot Time:	2015/01/08 12:50:22			
DNS Server 1:	10.0.252	Current Tim	e: 2015/01/08 13:31:41	Expo	rt Config	
DNS Server 2:		IC Servers:	10.0.1.95			
SIP Volume:	0	Orafianati	10.0.1.96			
Multicast Volume:		B'casts Acc	on File: InformaCastSpeaker.cfg			
Ring Volume:	0	B'casts Reje				
Sensor Volume:	0	B'casts Acti				
Volume Boost:	Off					
Microphone Gain:	: 0	Save	Reboot Toggle Help			
SIP Mode:	Enabled	/				
Multicast Mode:	Disabled					
Event Reporting:	Disabled					
Nightringer:	Disabled					
Primary SIP Serve	r: Registered					
Backup Server 1:	-					
Backup Server 2:	Not registered					
Nightringer Serve	r:Not registered					

Reboot

2.4 Command Interface

Some functions on the device can be activated using simple POST commands to the web interface. The examples in Table 2-26 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 2-26.	Command	Interface	Post	Commands
-------------	---------	-----------	------	----------

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

Appendix A: Mounting the Singlewire Strobe

A.1 Mount the Singlewire Strobe

Before you mount the Singlewire Strobe, make sure that you have received all the parts for each Singlewire Strobe. Refer to Table A-1.

Quantity	Part Name	Illustration
4	#6 x 1.5 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.	×

After the Singlewire Strobe is assembled, plug the Ethernet cable into the Singlewire Strobe Assembly (see Figure A-1).

Section 2.1.4, "Link and Activity LEDs" explains how the Link and Status LEDs work.

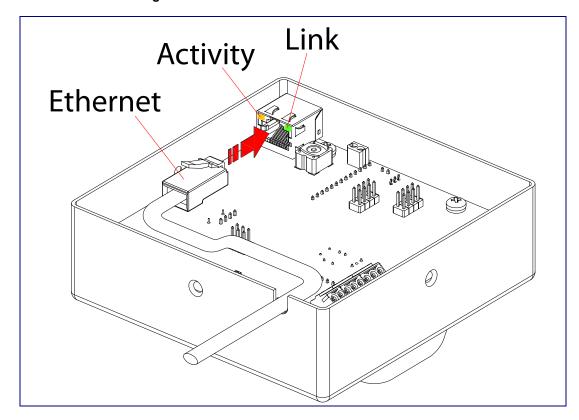


Figure A-1. Network Connector Prior to Installation

Figure A-2 shows the wall mounting options for the Singlewire Strobe.

Note Be sure to connect the Singlewire Strobe to the Earth Ground.

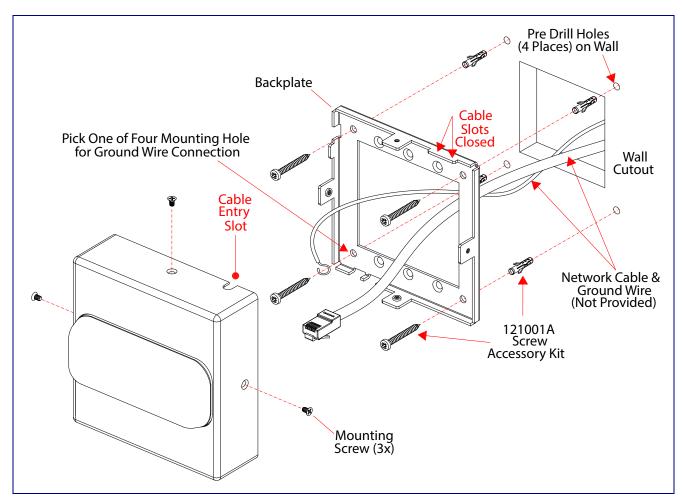


Figure A-2. Wall Mounting Options

Figure A-3 shows the gang box mounting options for the Singlewire Strobe.

Note Be sure to connect the Singlewire Strobe to the Earth Ground.

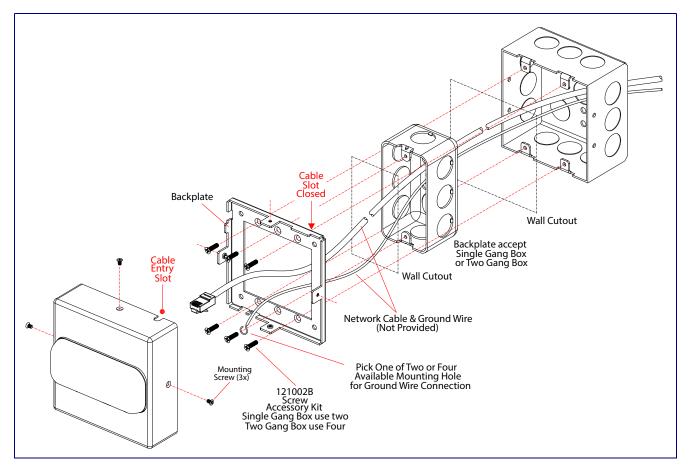
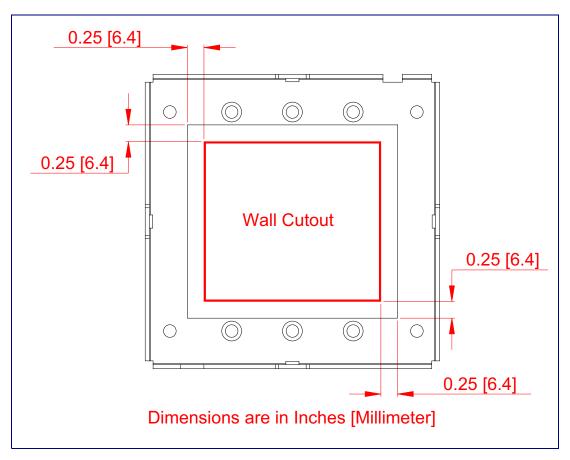


Figure A-3. Gang Box Mounting Options

Figure A-4 shows the maximum recommended wall cutout dimensions for mounting the Singlewire Strobe.





Appendix B: Troubleshooting/Technical Support

B.1 Frequently Asked Questions (FAQ)

A list of frequently asked questions (FAQs) are available on the Singlewire Strobe product page at:

http://www.cyberdata.net/products/voip/digitalanalog/strobev3singlewire/faqs.html

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

B.2 Documentation

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

http://www.cyberdata.net/products/voip/digitalanalog/strobev3singlewire/docs.html

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
Technical Support	The fastest way to get technical support for your VoIP product is to submit a VoIP Technical Support form at the following website:
	http://support.cyberdata.net/
	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, Ext. 333 Email: support@cyberdata.net
Returned	To return the product, contact the Returned Materials Authorization (RMA) department:
Materials Authorization	Phone: 831-373-2601, Extension 136 Email: RMA@CyberData.net
	When returning a product to CyberData, an approved CyberData RMA number must be printed on the outside of the original shipping package. Also, RMA numbers require an active VoIP Technical Support ticket number. A product will not be accepted for return without an approved RMA number. Send the product, in its original package, to the following address:
	CyberData Corporation 3 Justin Court Monterey, CA 93940 Attention: RMA "your RMA number"
RMA Status Form	If you need to inquire about the repair status of your product(s), please use the CyberData RMA Status form at the following web address:

http://support.cyberdata.net/

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

Α

AC voltages 2 AC voltages, enclosure is not rated 7 activate relay (door sensor) 44 activate relay (intrusion sensor) 44 activity LED 12 address, configuration login 18 alternative power input 4 audio configuration 46 audio configuration page 46 audio encodings 3 audio files, user-created 47 Autoprovision at time (HHMMSS) 55 autoprovision at time (HHMMSS) 55 autoprovision when idle (in minutes > 10) 55 autoprovisioning 56 download template button 56

autoprovisioning autoupdate (in minutes) 55 autoprovisioning configuration 54, 55 autoprovisioning filename 55 autoprovisioning server (IP Address) 55 auxiliary relay wiring diagram 8

B

backup SIP server 1 35 backup SIP server 2 35 backup SIP servers, SIP server backups 35 baud rate verifying 12

С

changing the web access password 22 Chrome (web browser) 3 Cisco SRST 35 command interface 69 commands 69 configurable parameters 20, 23, 28, 32

configuration audio 46 default IP settings 14 door sensor 43 intrusion sensor 43 network 31 SIP 34 using Web interface 14 configuration home page 19 configuration page configurable parameters 20, 23, 28, 32 contact information 76 contact information for CyberData 76 **Current Network Settings 32** current network settings 32 CyberData contact information 76

D

default device settings 77 gateway 14 IP address 14 subnet mask 14 username and password 14 web login username and password 19 default device settings 13 default gateway 14, 32 default IP settings 14 default login address 18 device configuration 22 device configuration parameters 55 the device configuration page 54 device configuration page 22, 27 device configuration parameters 23, 28 device configuration password changing for web configuration access 22 **DHCP Client 3** dial out extension (door sensor) 44 dial out extension (intrusion sensor) 44 dial out extension strings 38 dial-out extension strings 40 dimensions 4 discovery utility program 18 DNS server 32 door sensor 43, 44 activate relay 44 dial out extension 44 door open timeout 44 door sensor normally closed 44

flash button LED 44 download autoprovisioning template button 56 DTMF tones 38, 40 DTMF tones (using rfc2833) 38

E

earth ground 72, 73 enable night ring events 50 ethernet cable 71 ethernet I/F 4 event configuration enable night ring events 50 expiration time for SIP server lease 37 export settings 21

F

factory default settings 13 how to set 13 Firefox (web browser) 3 firmware where to get the latest firmware 66 flash button LED (door sensor) 44

G

gang box mounting 72, 73 get autoprovisioning template 56 GMT table 26 GMT time 26

Η

home page 19 http POST command 69 http web-based configuration 3

identifier names (PST, EDT, IST, MUT) 25 identifying your product 1 illustration of device mounting process 70 import settings 21 import/export settings 21 installation, typical device system 2 Internet Explorer (web browser) 3 intrusion sensor 43, 44 activate relay 44 dial out extension 44 IP address 14, 32 IP addressing default IP addressing setting 14

J

J3 terminal block, 16 AWG gauge wire 6

L

lease, SIP server expiration time 37 LED green link LED 12 yellow activity LED 12 lengthy pages 42 link LED 12, 71 local SIP port 36 log in address 18

Μ

MGROUP MGROUP Name 42 mounting the device 70 Mozilla Firefox (web browser) 3 Multicast IP Address 42

Ν

navigation (web page) 15 navigation table 15 network configuration 31 Network Setup 31 nightring tones 42 Nightringer 6, 65, 66 nightringer settings 36 NTP server 23

0

on-board relay 4, 7 operating temperature 4

Ρ

packet time 3 pages (lengthy) 42 part number 4 parts list 5 password for SIP server login 35 login 19 restoring the default 14 payload types 4 point-to-point configuration 39 port local SIP 36 remote SIP 36 posix timezone string timezone string 23 POST command 69 power input 4 alternative 4 priority assigning 42 product configuring 14 mounting 70 parts list 5 product features 3 product overview product features 3 product specifications 4 supported protocols 3 typical system installation 2 product specifications 4 protocol 4 protocols supported 3

R

reboot 67, 68 regulatory compliance 4 remote SIP port 36 Reset Test Function Management (RTFM) switch 13 resetting the IP address to the default 70, 75 restoring factory default settings 13, 77 restoring the factory default settings 13 ringtones 42 lengthy pages 42 RMA returned materials authorization 76 RMA status 76 RTFM switch 13 RTP/AVP 3

S

Safari (web browser) 3 sales 76 sensor setup page 43 sensor setup parameters 43 sensors 44 server address, SIP 35 service 76 set time with external NTP server on boot 23 setting up the device 6 settings, default 13 SIP enable SIP operation 35 local SIP port 36 user ID 35 SIP configuration 34 SIP Server 35 SIP configuration parameters outbound proxy 36, 37 registration and expiration, SIP server lease 37 user ID, SIP 35 SIP registration 35 SIP remote SIP port 36 SIP server 35 password for login 35 user ID for login 35 SRST 35 status LED 71 subnet mask 14, 32 supported protocols 3

T

tech support 76 technical support, contact information 76 terminal block, 16 AWG gauge wire 6 time zone string examples 25

U

user ID for SIP server login 35 username changing for web configuration access 22 default for web configuration access 19 restoring the default 14

V

verifying baud rate 12 network connectivity 12 VLAN ID 32 VLAN Priority 32 VLAN tagging support 32 VLAN tags 32

W

warranty policy at CyberData 76 web access password 14 web access username 14 web configuration log in address 18 web page navigation 15 web page navigation 15 web-based configuration 14 weight 4 wget, free unix utility 69