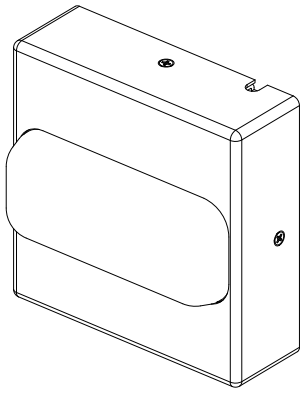
CyberData

The IP Endpoint Company



Singlewire Strobe Operations Guide

Part #*011244*

Document Part #*930829C*
for Firmware Version *10.4.0*

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

Singlewire Strobe Operations Guide 930829C
Part # 011244

CyberData
The IP Endpoint Company

Technical Support

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

Phone: (831) 373-2601, Ext. 333
Email: support@cyberdata.net
Fax: (831) 373-4193
Company and product information is at **www.cyberdata.net**.

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!**

Warning

Electrical Hazard: This product should be installed by a licensed electrician according to all local electrical and building codes.

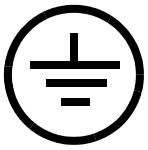
Warning

Electrical Hazard: To prevent injury, this apparatus must be securely attached to the floor/wall in accordance with the installation instructions.

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

Revision Information

Revision 930829C, which corresponds to firmware version 10.4.0, and was released on October 1, 2014, has the following changes:

- Updates Figure 2-12, "Home Page"
- Adds Figure 2-13, "Device Configuration Page"
- Adds Section 2.2.3, "Configure the Device"
- Adds Figure 2-14, "Strobe Configuration Page"
- Adds Section 2.2.4, "Configure the Strobe"
- Adds Figure 2-15, "Network Configuration Page"
- Adds Section 2.2.5, "Configure the Network Parameters"
- Adds Figure 2-16, "SIP Configuration Page"
- Adds Section 2.2.6, "Configure the SIP Parameters"
- Adds Figure 2-17, "Nightringer Configuration Setup"
- Adds Section 2.2.7, "Configure the Night Ringer Parameters"
- Adds Figure 2-18, "Sensor Configuration Page"
- Adds Section 2.2.8, "Configure the Sensor Configuration Parameters"
- Adds Figure 2-19, "Multicast Configuration Page"
- Adds Section 2.2.9, "Configure the Multicast Parameters"
- Adds Figure 2-20, "Audio Configuration Page"
- Adds Section 2.2.10, "Configure the Audio Configuration Parameters"
- Adds Figure 2-24, "Event Configuration Page"
- Adds Section 2.2.11, "Configure the Event Parameters"
- Adds Figure 2-25, "Autoprovisioning Configuration Page"
- Adds Section 2.2.12, "Configure the Autoprovisioning Parameters"
- Updates Figure 2-28, "Upgrade Firmware Page"
- Updates Figure 2-29, "Reboot Button"

Browsers Supported

The following browsers have been tested against firmware version 10.4.0:

- 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)

Contents

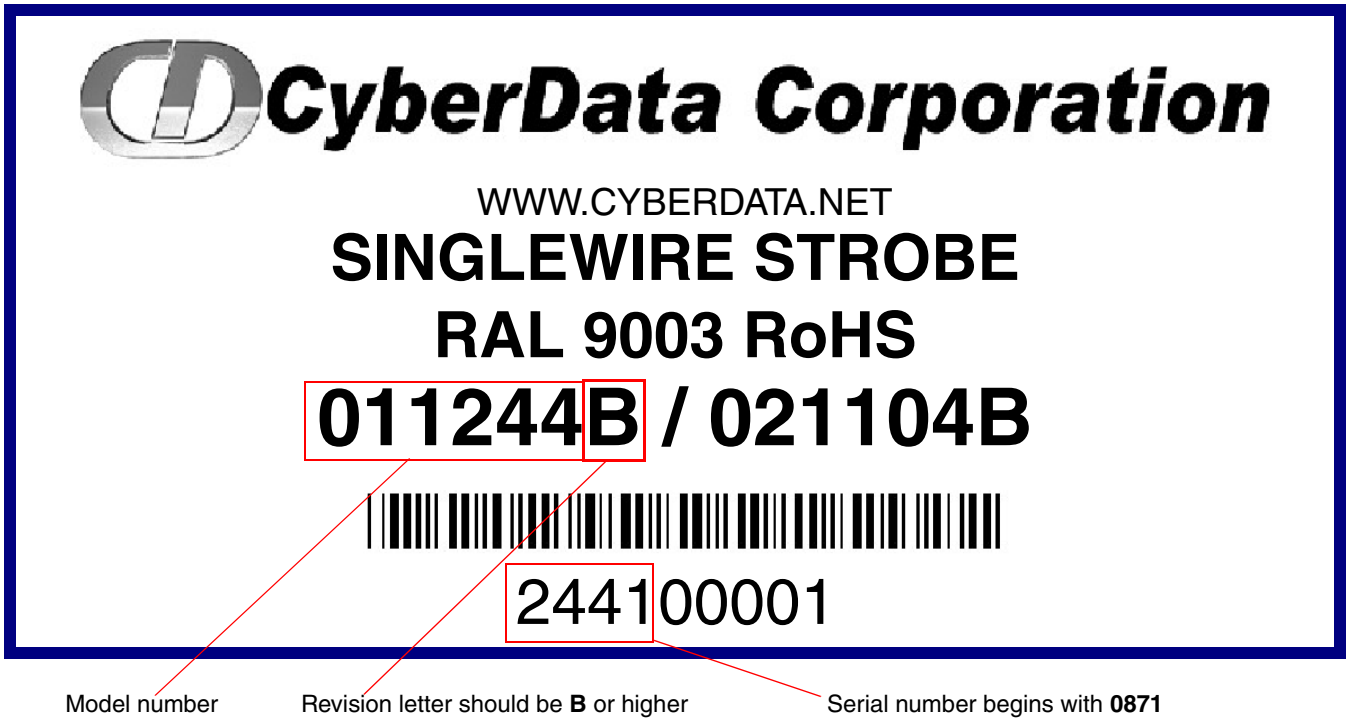
1 Product Overview

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**.

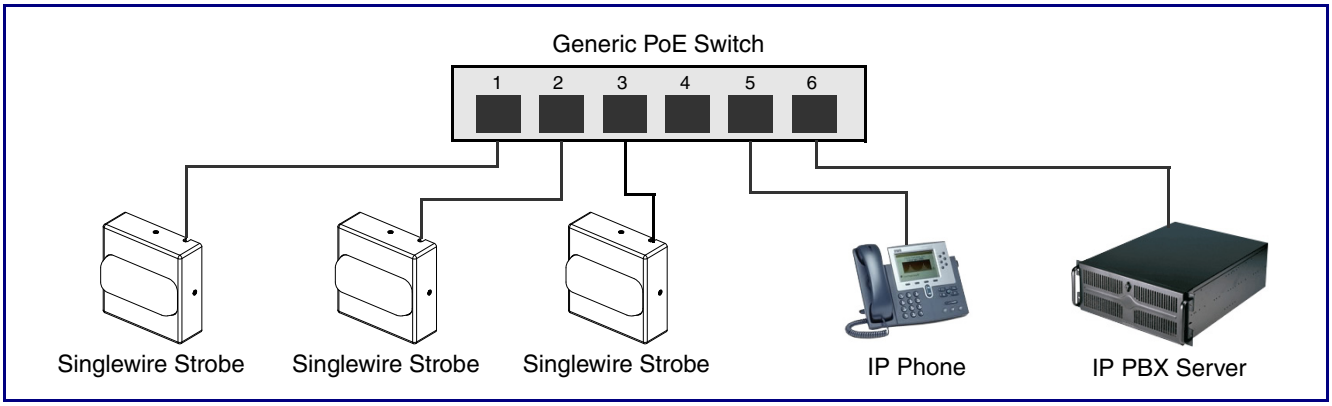
Figure 1-1. Model Number Label



1.2 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



Warning

Electrical Hazard: The Singlewire Strobe enclosure is not rated for any AC voltages.

Warning

Electrical Hazard: This product should be installed by a licensed electrician according to all local electrical and building codes.

Warning

Electrical Hazard: To prevent injury, this apparatus must be securely attached to the floor/wall in accordance with the installation instructions.

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

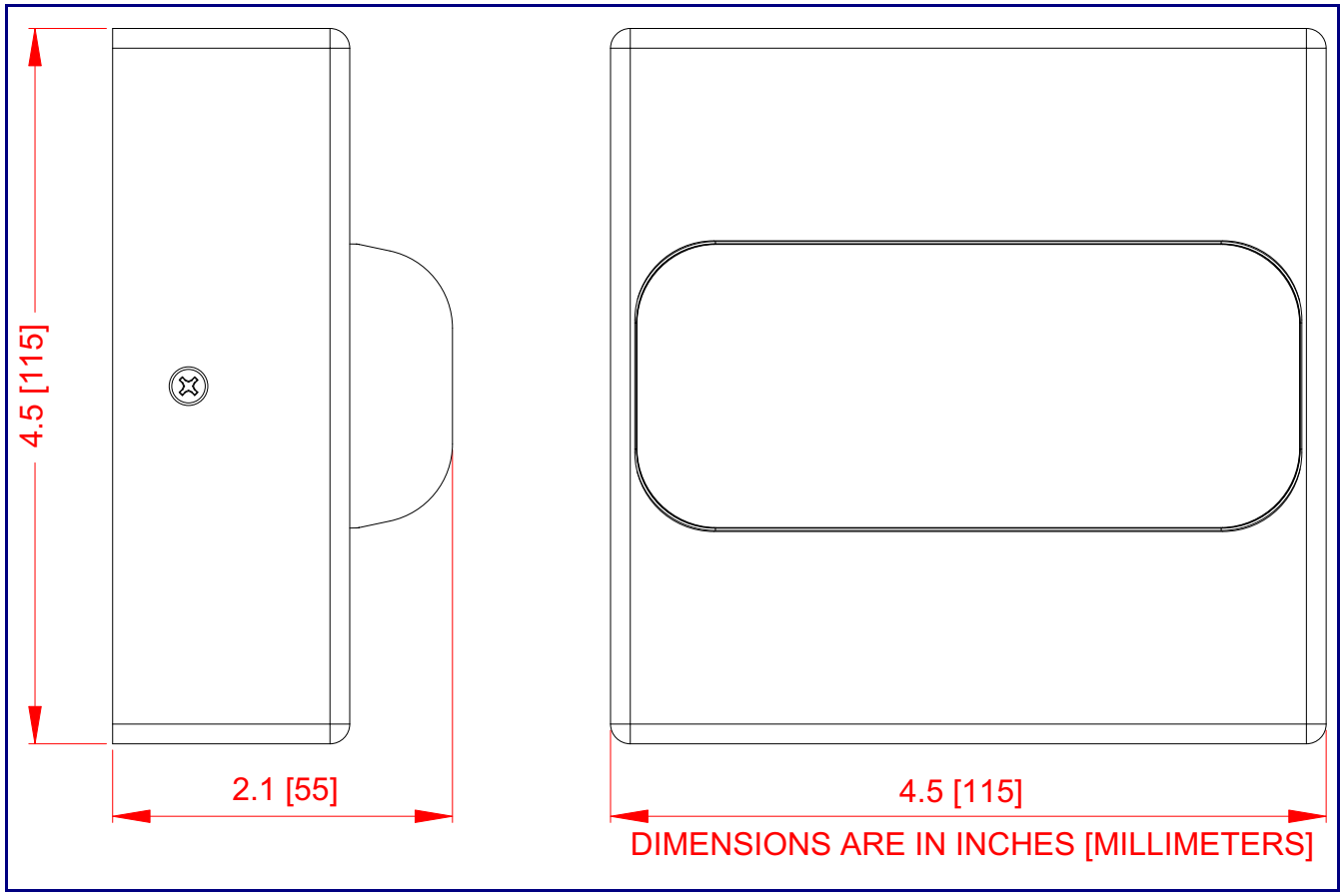
1.5 Product Specifications

Table 1-1. Specifications

Category	Specification
Ethernet I/F	10/100 Mbps
Power Input	PoE 802.3af compliant or 8 to 12 VDC at 1000 mA
Protocol	InformaCast v4.0 and later
Light power	90 candela (5-Watt LEDs)
Flash rate	2 per second
LED MTBF	100,000 Hours
Operating Temperature	-10° C to 50° C (14° F to 122° F)
Dimensions	4.5” x 4.5” x 1.5” (H x W x D)
Warranty	2 years limited
Power Requirement	802.3af compliant or 8 to 12 VDC at 1000 mA
Auxiliary Relay	1A at 30 VDC
Weight	1.6 lbs./shipping weight of 2.2 lbs. (0.7 kg/shipping weight of 1.0kg)
Part Number	011244

1.6 Dimensions

Figure 1-3. Dimensions—Size of Unit with Case

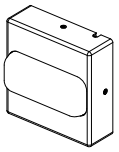


2 Installing the Singlewire Strobe

2.1 Parts List

Table 2-2 illustrates the Singlewire Strobe parts.

Table 2-2. Parts List

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

2.1 Singlewire Strobe Setup

2.1.1 Singlewire Strobe Connections

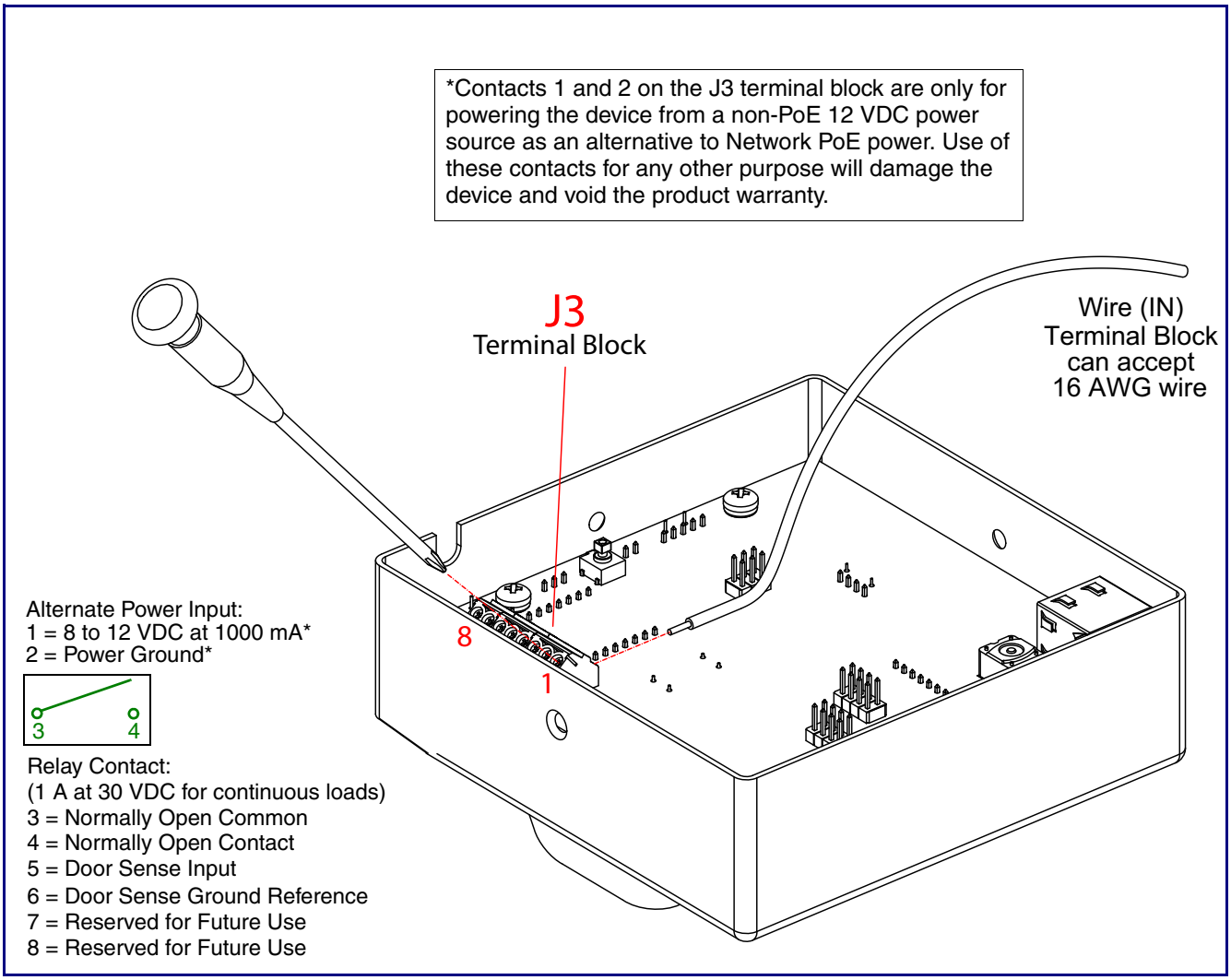
Figure 2-4 shows the pin connections on the J3 (terminal block). This terminal block can accept 16 AWG gauge wire.

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

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 2-4. Singlewire Strobe Connections



2.1.2 Connecting the Singlewire Strobe to the Auxiliary Relay

Warning

Electrical Hazard: The Singlewire Strobe enclosure is not rated for any AC voltages.

Warning

Electrical Hazard: This product should be installed by a licensed electrician according to all local electrical and building codes.

Warning

Electrical Hazard: To prevent injury, this apparatus must be securely attached to the floor/wall in accordance with the installation instructions.

Warning

Electrical Hazard: 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.

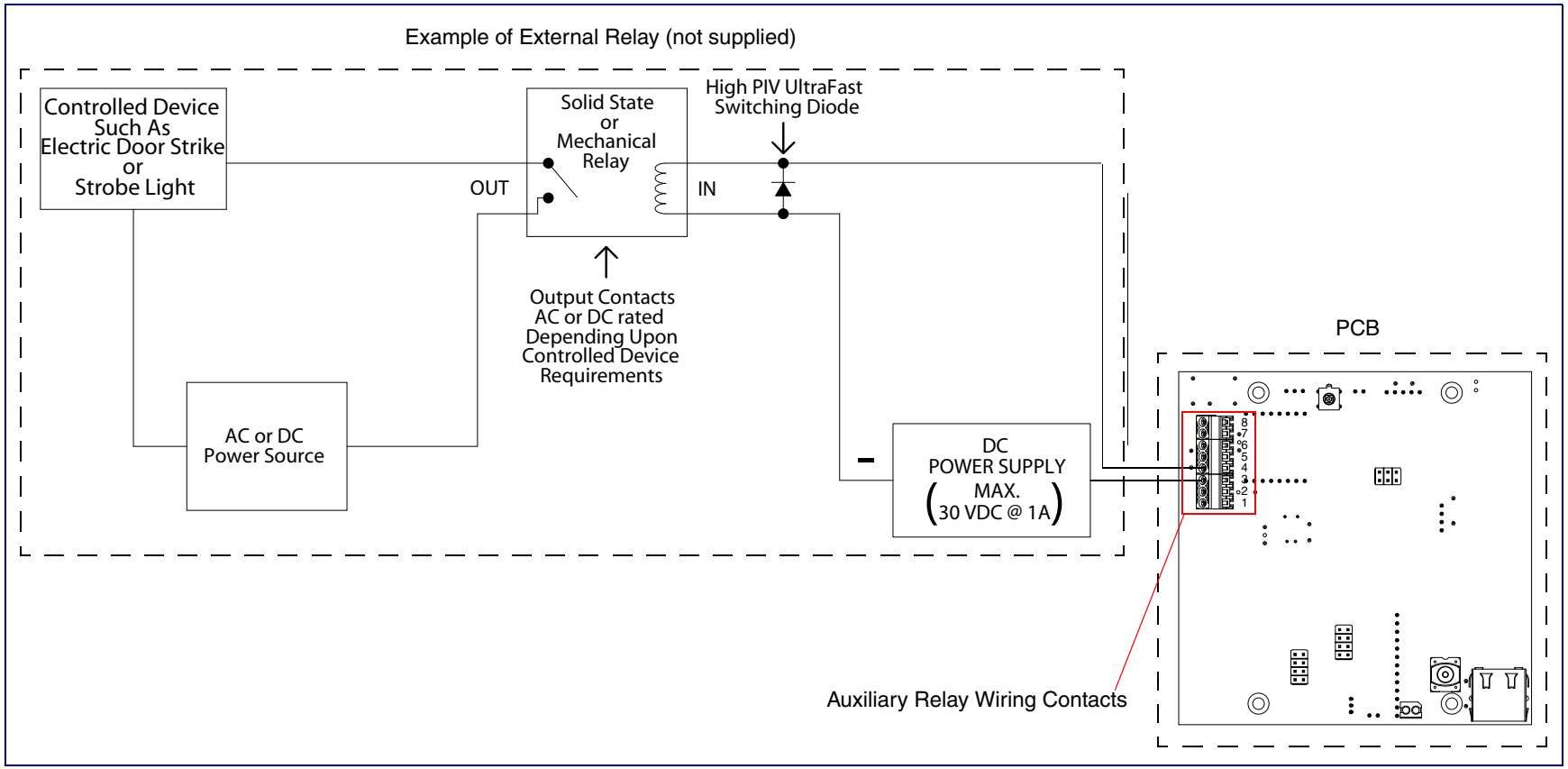
Warning

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 2-5, "Auxiliary Relay 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.

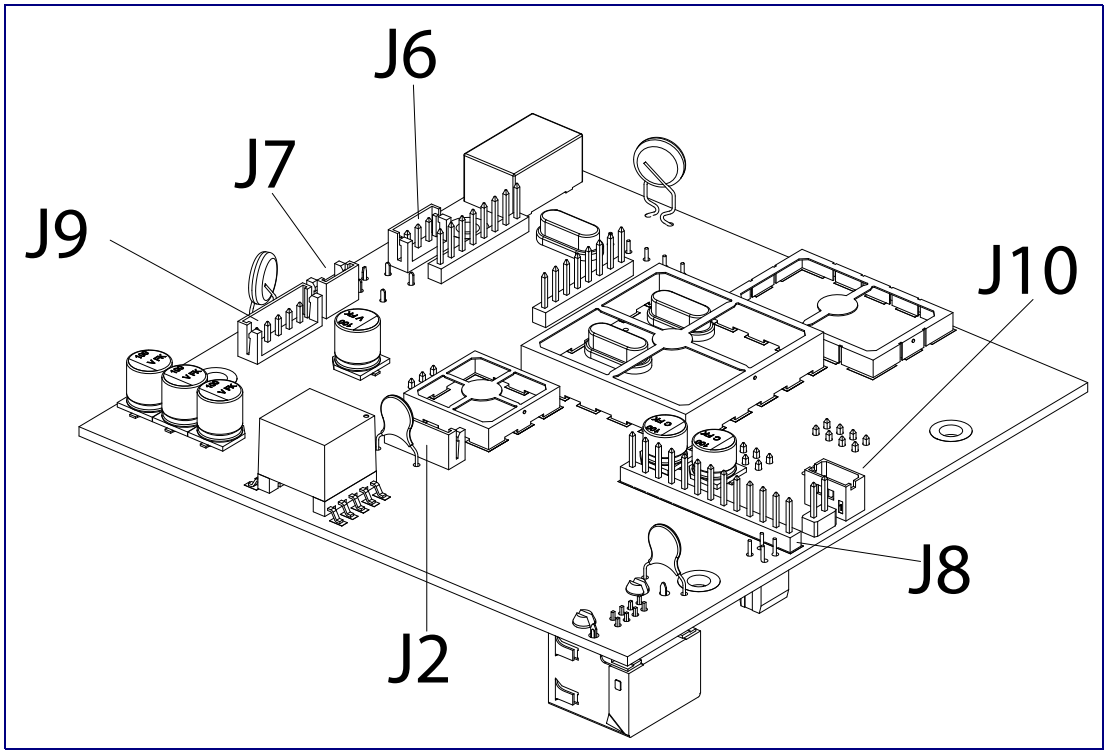
Figure 2-5. Auxiliary Relay Wiring Diagram



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.

Figure 2-6. Connector Locations for the 021084 Board



.

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 2-7. Connector Locations for the 021084 Board

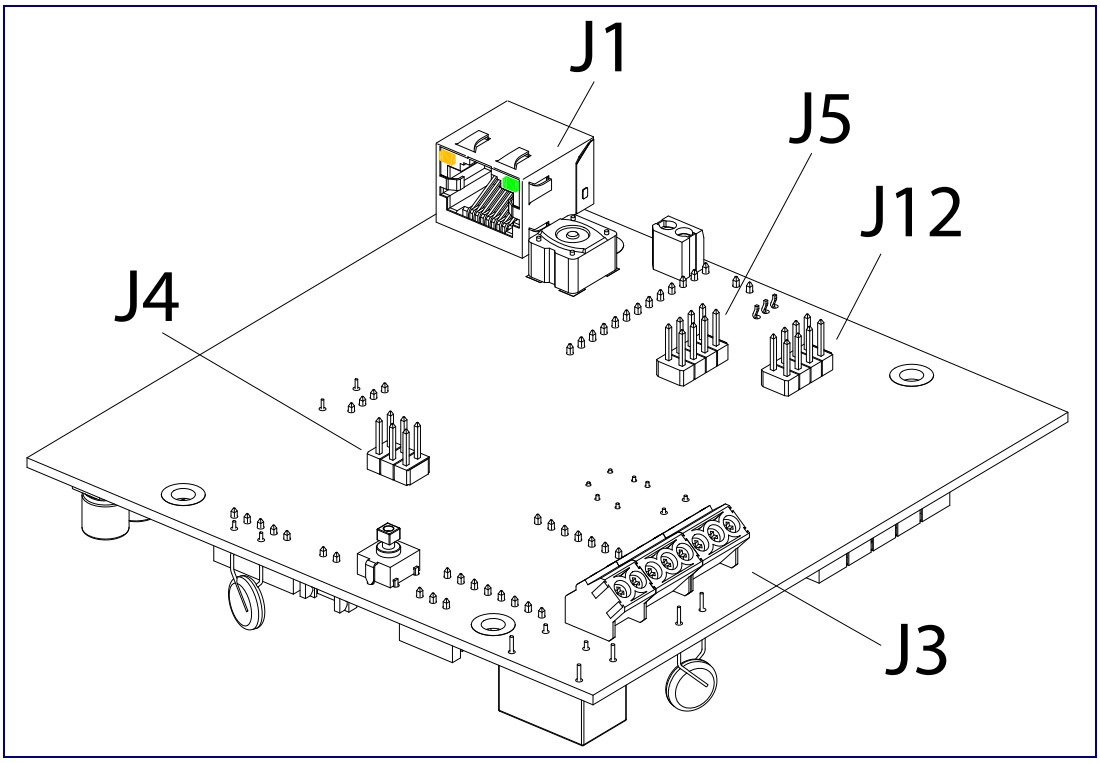
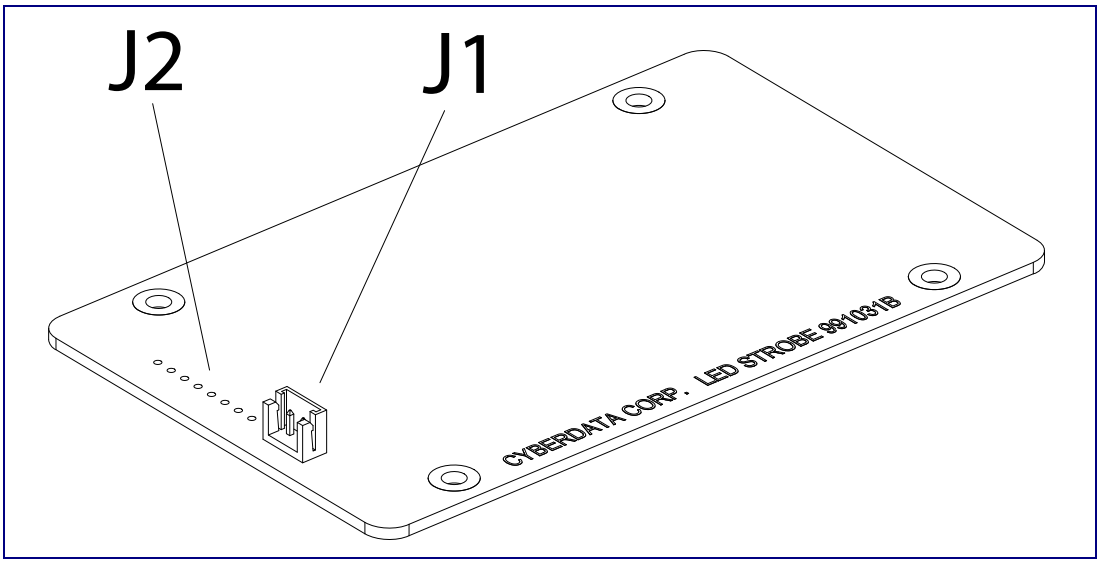


Table 2-4. Connector Functions

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

Figure 2-8. Connector Locations for the 021054 Board



.

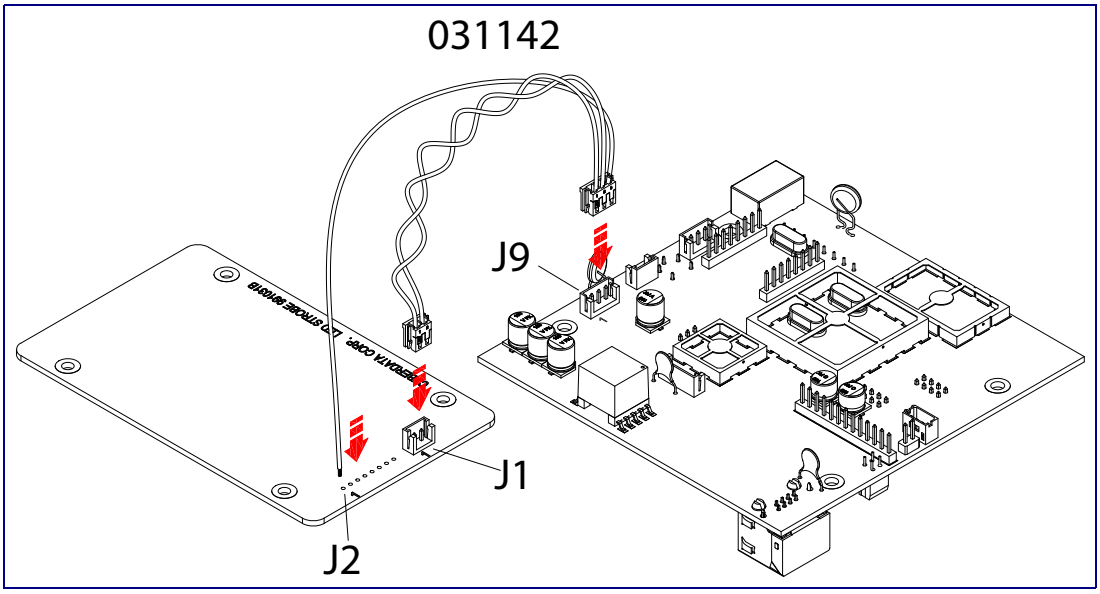
Table 2-5. Connector Functions

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 2-9 to see how the 021054 and 021084 boards are connected with the 031142 cable assembly.

Figure 2-9. 021054 and 021084 Boards Connected with the 031142 Cable Assembly

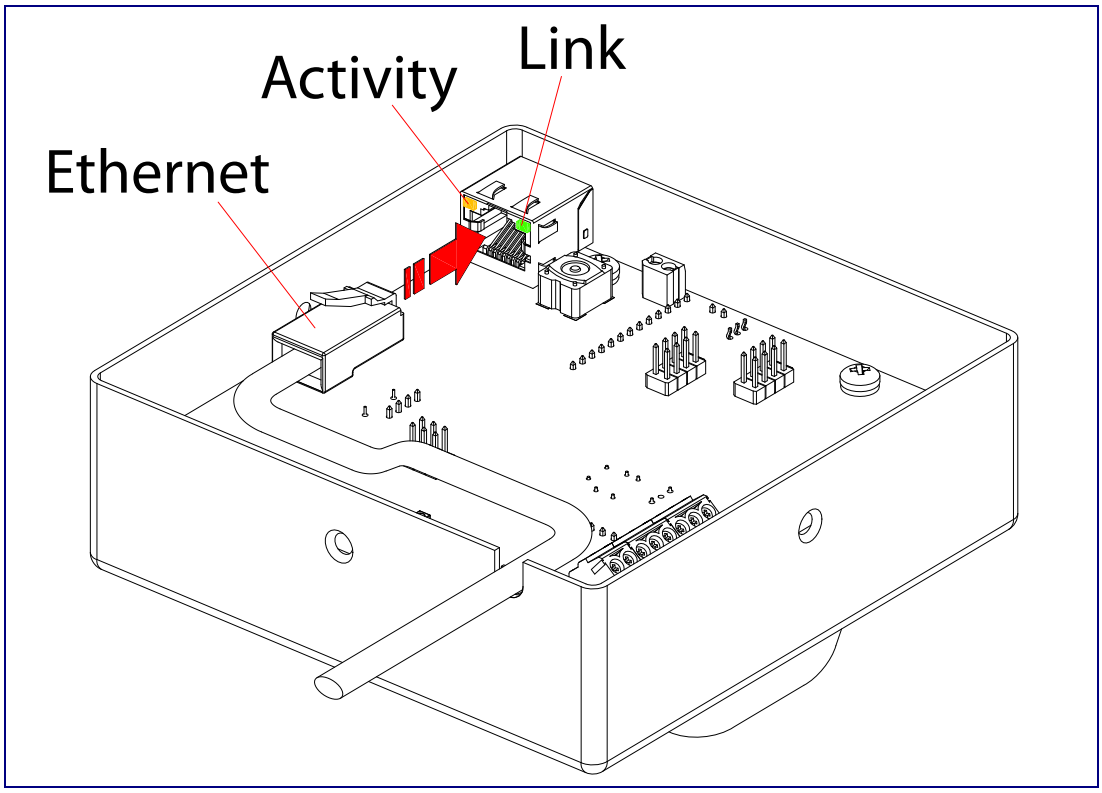


2.1.4 Network Connectivity

When you plug in the Ethernet cable (Figure 2-10) or power supply:

- The square, **GREEN Link** LED (Figure 2-10) above the Ethernet port indicates that the network connection has been established.
- The square, **YELLOW Activity** LED (Figure 2-10) blinks when there is network activity.

Figure 2-10. Network LEDs



2.1.5 Restore the Factory Default Settings

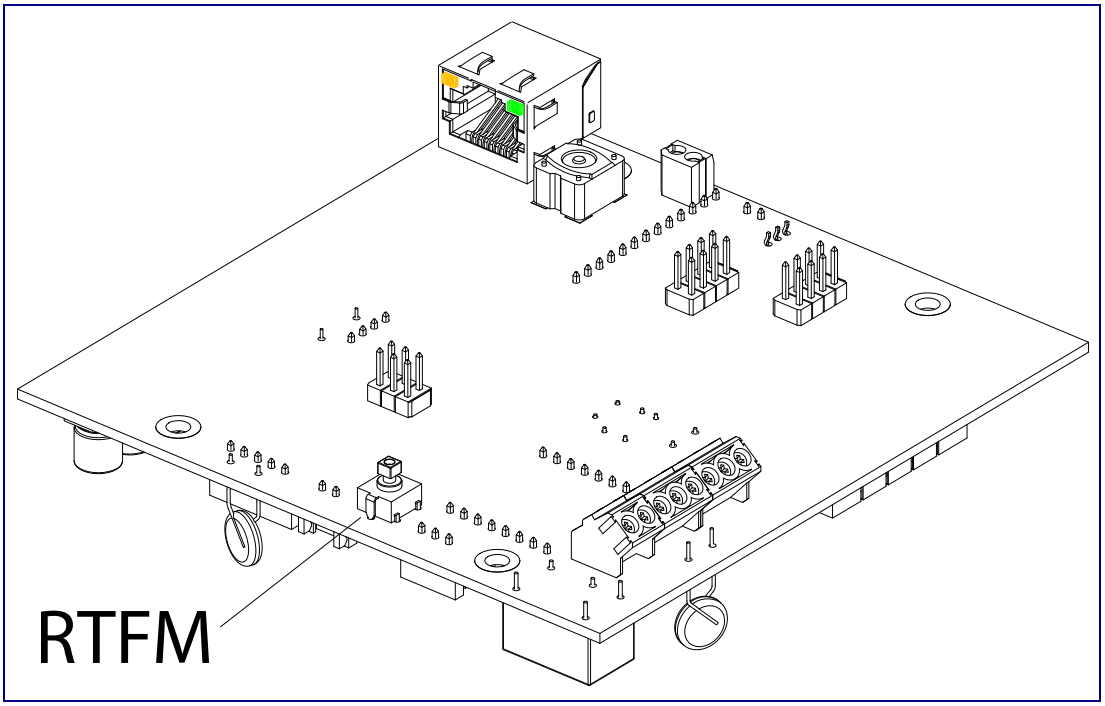
2.1.5.1 RTFM Switch

When the Singlewire Strobe is operational and linked to the network, use the Reset Test Function Management (RTFM) switch (Figure 2-11) 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 2-11. 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.

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]	10.10.10.10
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.

2.2.1 Singlewire Strobe Web Page Navigation

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

Table 2-7. Web Page Navigation

Web Page Item	Description
	Link to the **Home** page.
	Link to the **Device Configuration** page.
	Link to the **Strobe Configuration** page.
	Link to the **Networking** page.
	Link to go to the **SIP Configuration** page.
	Link to go to the **Nightringer** page.
	Link to the **Sensor Configuration** page.
	Link to the **Multicast Configuration** page.
	Link to the **Audio Configuration** page.
	Link to the **Event Configuration** page.
	Link to the **Autoprovisioning Configuration** page.
	Link to the **Update Firmware** page.

2.2.2 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:

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

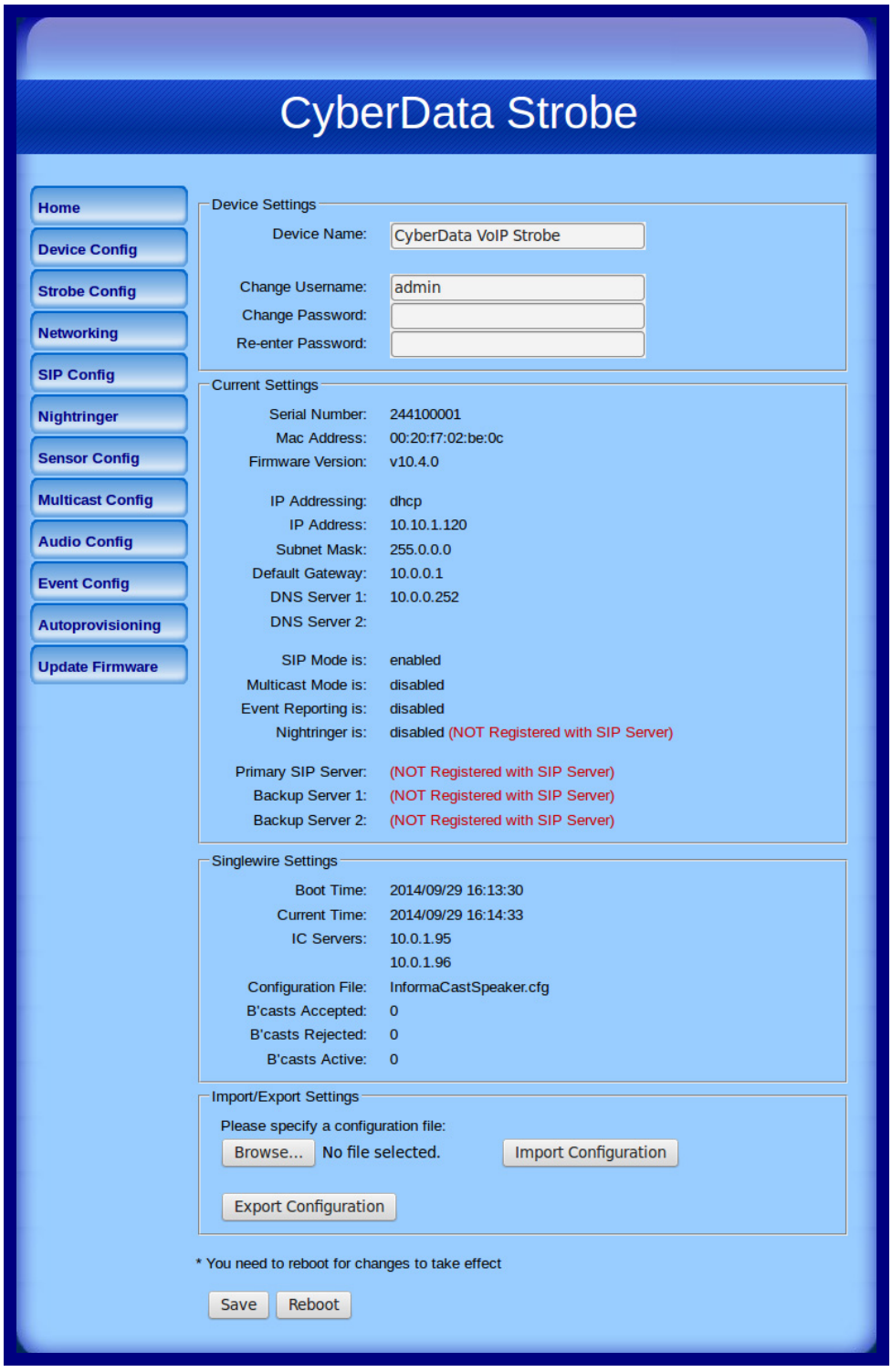
Note The Singlewire Strobe ships in DHCP mode. To get to the **Home** page, use the discovery utility to scan for the device on the network and open your browser from there.

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**

Figure 2-12. Home Page



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

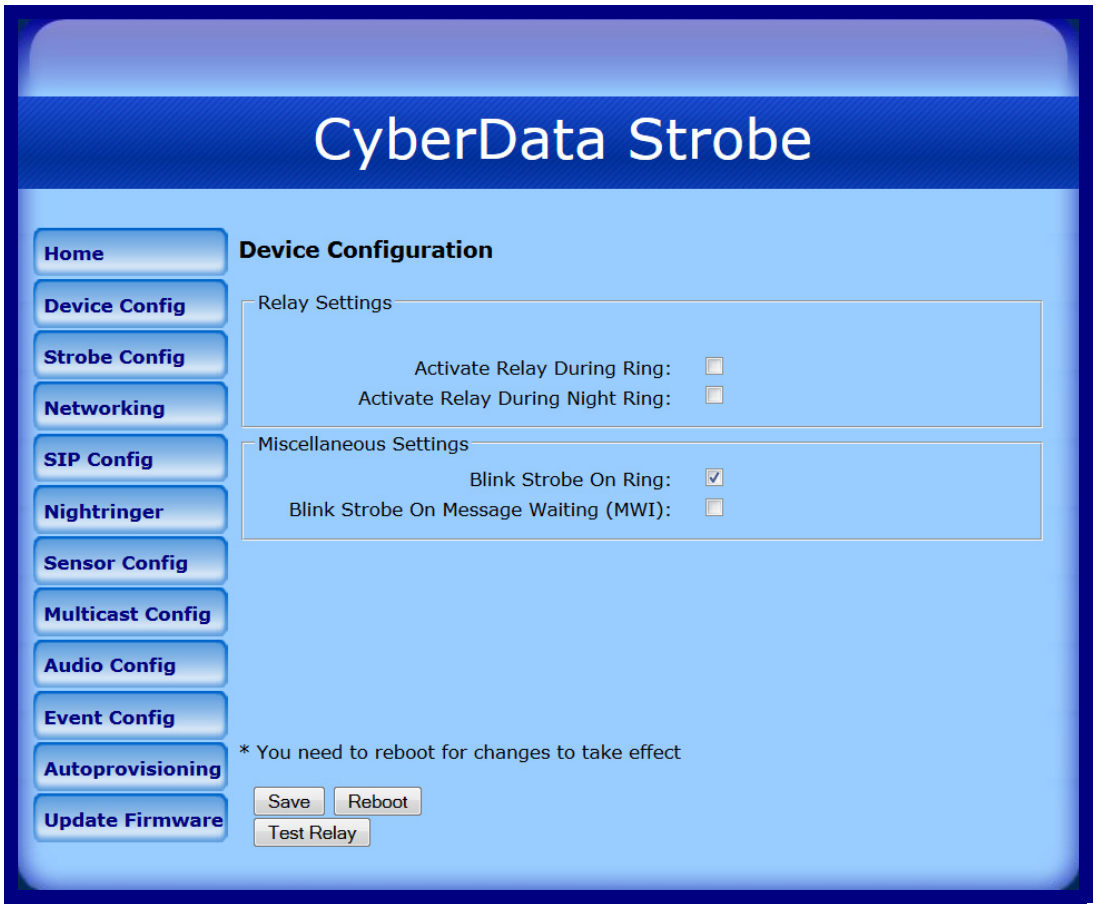
Table 2-8. Home Page Overview

Web Page Item	Description
Device Settings	
Device Name	Shows the device name.
Change Username	Type in this field to change the username.
Change Password	Type in this field to change the password.
Re-enter Password	Type the password again in this field to confirm the new password.
Current Settings	
Serial Number	Shows the device serial number.
Mac Address	Shows the device Mac address.
Firmware Version	Shows the current firmware version.
IP Addressing	Shows the current IP addressing setting (**DHCP** or **static**).
IP Address	Shows the current IP address.
Subnet Mask	Shows the current subnet mask address.
Default Gateway	Shows the current default gateway address.
DNS Server 1	Shows the current DNS Server 1 address.
DNS Server 2	Shows the current DNS Server 2 address.
SIP Mode is	Shows the current status of the SIP mode.
Multicast Mode is	Shows the current status of the Multicast mode.
Event Reporting is	Shows the current status of the Event Reporting mode.
Nightringer is	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.
Import/Export Settings	
Browse...	Press the **Browse** button to select a configuration file to import.
Import Configuration	IPress the **Import Configuration** button to save a board configuration to the board. **Note**: The board will have to be reset before changes will take effect.
Export Configuration	Press the **Export Configuration** button to download the current board configuration.
Save	Click on the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.

2.2.3 Configure the Device

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

Figure 2-13. Device Configuration Page



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

Table 2-9. Device Configuration Parameters

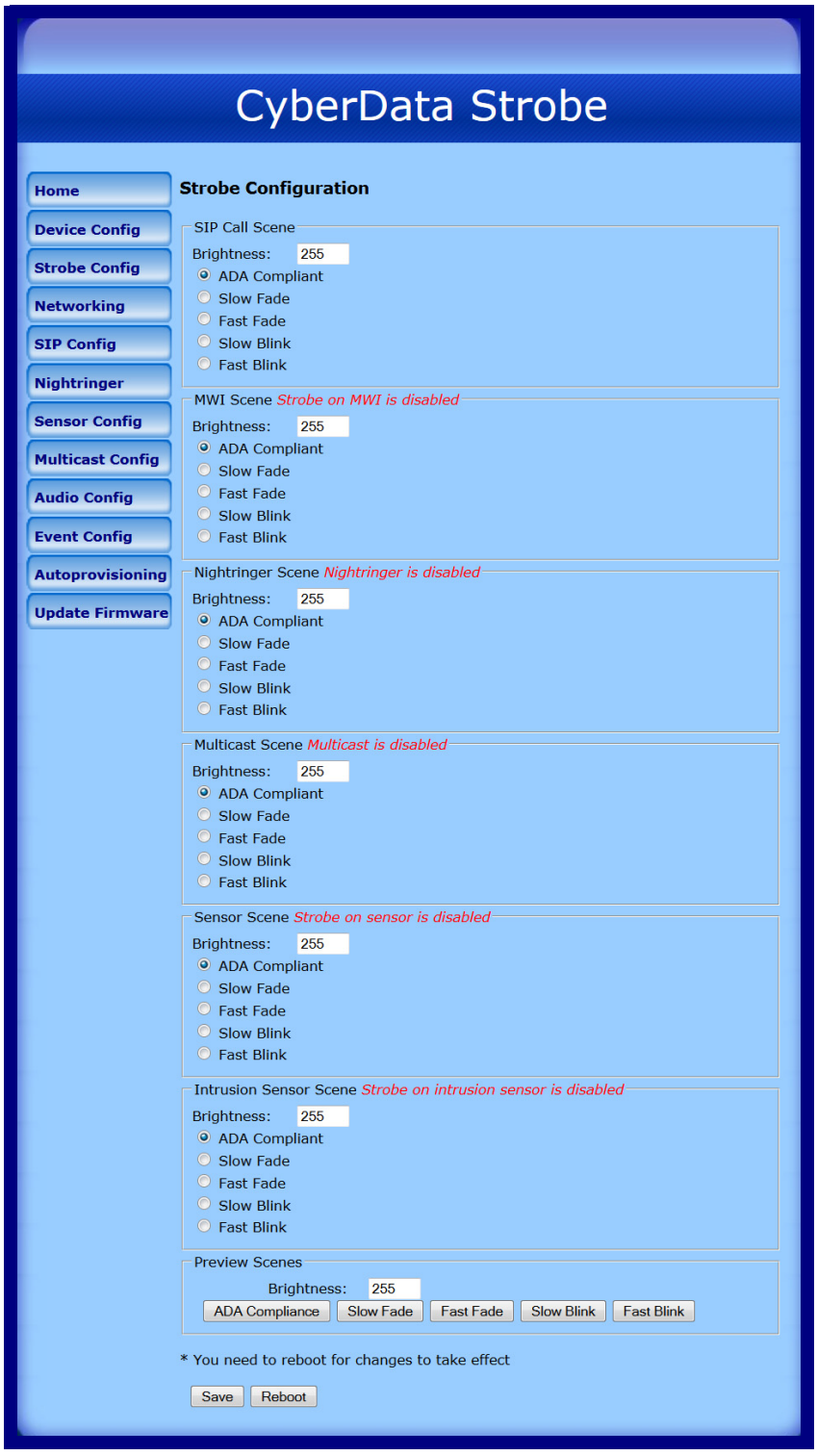
Web Page Item	Description
Relay Settings	
Activate Relay During Ring	When selected, the relay will be activated for as long as the call is ringing.
Activate Relay During Night Ring	Check this box to activate the relay for as long as a Night Ring tone is ringing.
Miscellaneous Settings	
Blink Strobe on Ring	When selected, the strobe light will blink during an incoming call.
Blink Strobe on Message Waiting (MWI)	When selected, the strobe light will blink if there is a message waiting.
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.
Test Relay	Click on the **Test Relay** button to do a relay test.

3. After changing the parameters, click the **Save** button.

2.2.4 Configure the Strobe

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

Figure 2-14. Strobe Configuration Page



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

2.2.4.1 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**.

Table 2-10. Device Configuration Parameters

Web Page Item	Description
SIP Call Scene	Use this section to select the strobe flashing behavior for the **SIP Call** event.
Brightness	Enter the desired strobe brightness level for the **SIP Call** event. (default is 255) (3 character limit [values from 1 to 255])
ADA Compliant	When selected, the **ADA Compliant** strobe flashing mode is enabled for the **SIP Call** event.
Slow Fade	When selected, the **Slow Fade** strobe flashing mode is enabled for the **SIP Call** event.
Fast Fade	When selected, the **Fast Fade** strobe flashing mode is enabled for the **SIP Call** event.
Slow Blink	When selected, the **Slow Blink** strobe flashing mode is enabled for the **SIP Call** event.
Fast Blink	When selected, the **Fast Blink** strobe flashing mode is enabled for the **SIP Call** event.
MWI Scene	Use this section to select the strobe flashing behavior for the **Message Waiting (MWI)** event.
Brightness	Enter the desired strobe brightness level for the **MWI** event. (default is 255) (3 character limit [values from 1 to 255])
ADA Compliant	When selected, the **ADA Compliant** strobe flashing mode is enabled for the **MWI** event.
Slow Fade	When selected, the **Slow Fade** strobe flashing mode is enabled for the **MWI** event.
Fast Fade	When selected, the **Fast Fade** strobe flashing mode is enabled for the **MWI** event.
Slow Blink	When selected, the **Slow Blink** strobe flashing mode is enabled for the **MWI** event.
Fast Blink	When selected, the **Fast Blink** strobe flashing mode is enabled for the **MWI** event.
Nightringer Scene	Use this section to select the strobe flashing behavior for the **Nightringer** event.
Brightness	Enter the desired strobe brightness level for the **Nightringer** event. (default is 255) (3 character limit [values from 1 to 255])
ADA Compliant	When selected, the **ADA Compliant** strobe flashing mode is enabled for the **Nightringer** event.
Slow Fade	When selected, the **Slow Fade** strobe flashing mode is enabled for the **Nightringer** event.
Fast Fade	When selected, the **Fast Fade** strobe flashing mode is enabled for the **Nightringer** event.
Slow Blink	When selected, the **Slow Blink** strobe flashing mode is enabled for the **Nightringer** event.
Fast Blink	When selected, the **Fast Blink** strobe flashing mode is enabled for the **Nightringer** event.

Table 2-10. Device Configuration Parameters (continued)

Web Page Item	Description
Multicast Scene	Use this section to select the strobe flashing behavior for the **Multicast** event.
Brightness	Enter the desired strobe brightness level for the **Multicast** event. (default is 255) (3 character limit [values from 1 to 255])
ADA Compliant	When selected, the **ADA Compliant** strobe flashing mode is enabled for the **Multicast** event.
Slow Fade	When selected, the **Slow Fade** strobe flashing mode is enabled for the **Multicast** event.
Fast Fade	When selected, the **Fast Fade** strobe flashing mode is enabled for the **Multicast** event.
Slow Blink	When selected, the **Slow Blink** strobe flashing mode is enabled for the **Multicast** event.
Fast Blink	When selected, the **Fast Blink** strobe flashing mode is enabled for the **Multicast** event.
Sensor Scene	Use this section to select the strobe flashing behavior for the **Sensor** event.
Brightness	Enter the desired strobe brightness level for the **Sensor** event. (default is 255) (3 character limit [values from 1 to 255])
ADA Compliant	When selected, the **ADA Compliant** strobe flashing mode is enabled for the **Sensor** event.
Slow Fade	When selected, the **Slow Fade** strobe flashing mode is enabled for the **Sensor** event.
Fast Fade	When selected, the **Fast Fade** strobe flashing mode is enabled for the **Sensor** event.
Slow Blink	When selected, the **Slow Blink** strobe flashing mode is enabled for the **Sensor** event.
Fast Blink	When selected, the **Fast Blink** strobe flashing mode is enabled for the **Sensor** event.
Intrusion Sensor Scene	Use this section to select the strobe flashing behavior for the **Intrusion Sensor** event.
Brightness	Enter the desired strobe brightness level for the **Intrusion Sensor** event. (default is 255) (3 character limit [values from 1 to 255])
ADA Compliant	When selected, the **ADA Compliant** strobe flashing mode is enabled for the **Intrusion Sensor** event.
Slow Fade	When selected, the **Slow Fade** strobe flashing mode is enabled for the **Intrusion Sensor** event.
Fast Fade	When selected, the **Fast Fade** strobe flashing mode is enabled for the **Intrusion Sensor** event.
Slow Blink	When selected, the **Slow Blink** strobe flashing mode is enabled for the **Intrusion Sensor** event.
Fast Blink	When selected, the **Fast Blink** strobe flashing mode is enabled for the **Intrusion Sensor** event.
Preview Scenes	Use this section to preview the strobe flashing behavior for the **Scene** button that is pressed.
Brightness	Enter the desired strobe brightness level for the scene that you want to preview. (default is 255) (3 character limit [values from 1 to 255])
ADA Compliance	Click on the **ADA Compliance** button to preview the **ADA Compliance** strobe flashing mode.
Slow Fade	Click on the **Slow Fade** button to preview the **Slow Fade** strobe flashing mode.
Fast Fade	Click on the **Fast Fade** button to preview the **Fast Fade** strobe flashing mode.
Slow Blink	Click on the **Slow Blink** button to preview the **Slow Blink** strobe flashing mode.
Fast Blink	Click on the **Fast Blink** button to preview the **Fast Blink** strobe flashing mode.

Table 2-10. Device Configuration Parameters (continued)

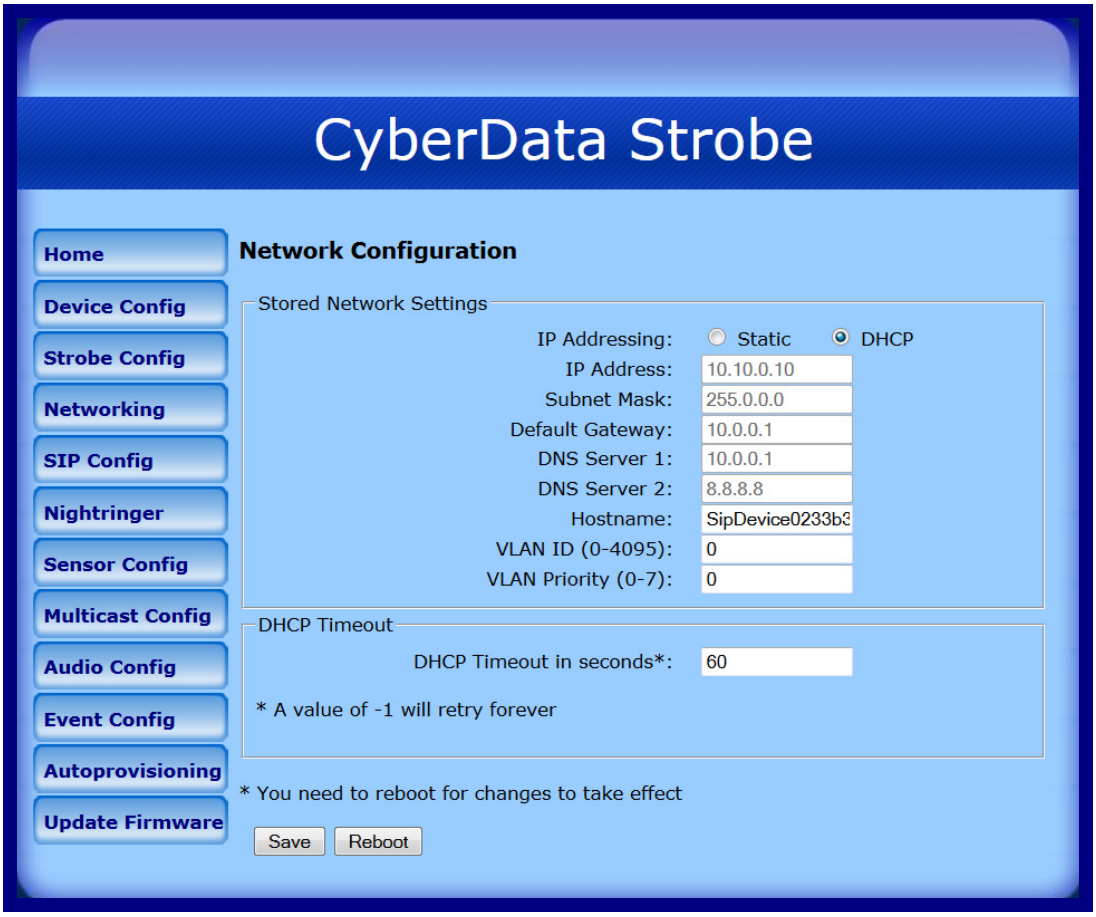
Web Page Item	Description
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.

3. After changing the parameters, click the **Save** button.

2.2.5 Configure the Network Parameters

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

Figure 2-15. Network Configuration Page



2. On the **Network Configuration** page, enter values for the parameters indicated in Table 2-11.

Table 2-11. Network Configuration Parameters

Web Page Item	Description
Stored Network Settings	
IP Addressing	Select either **DHCP IP Addressing** or **Static IP Addressing** by marking the appropriate radio button. If you select **Static**, configure the remaining parameters indicated in Table 2-11. If you select **DHCP**, go to Step 3.
IP Address	Enter the Static IP address.
Subnet Mask	Enter the Subnet Mask address.
Default Gateway	Enter the Default Gateway address.
DNS Server 1	Enter the DNS Server 1 address.
DNS Server 2	Enter the DNS Server 2 address.
Hostname	This is the hostname provided to the DHCP server. This can be used in conjunction with a DNS server to address the device by host name instead of by IP address. Check your DHCP server and DNS server documentation for more information.
VLAN ID (0-4095)	Enter the VLAN ID number. **Note**: The device supports 802.11Q VLAN tagging support. The switch port connected to the device will need to be in “trunking mode” for the VLAN tags to propagate.
VLAN Priority (0-7)	Enter the VLAN priority number.
DHCP Timeout	
DHCP Timeout in seconds	Enter the desired timeout duration (in seconds) that the device will wait for a response from the DHCP server before defaulting back to the stored static IP address. **Note**: A value of **-1** will cause the device to retry indefinitely and a value of **0** will cause the device to reset to a default of 60 seconds.
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.

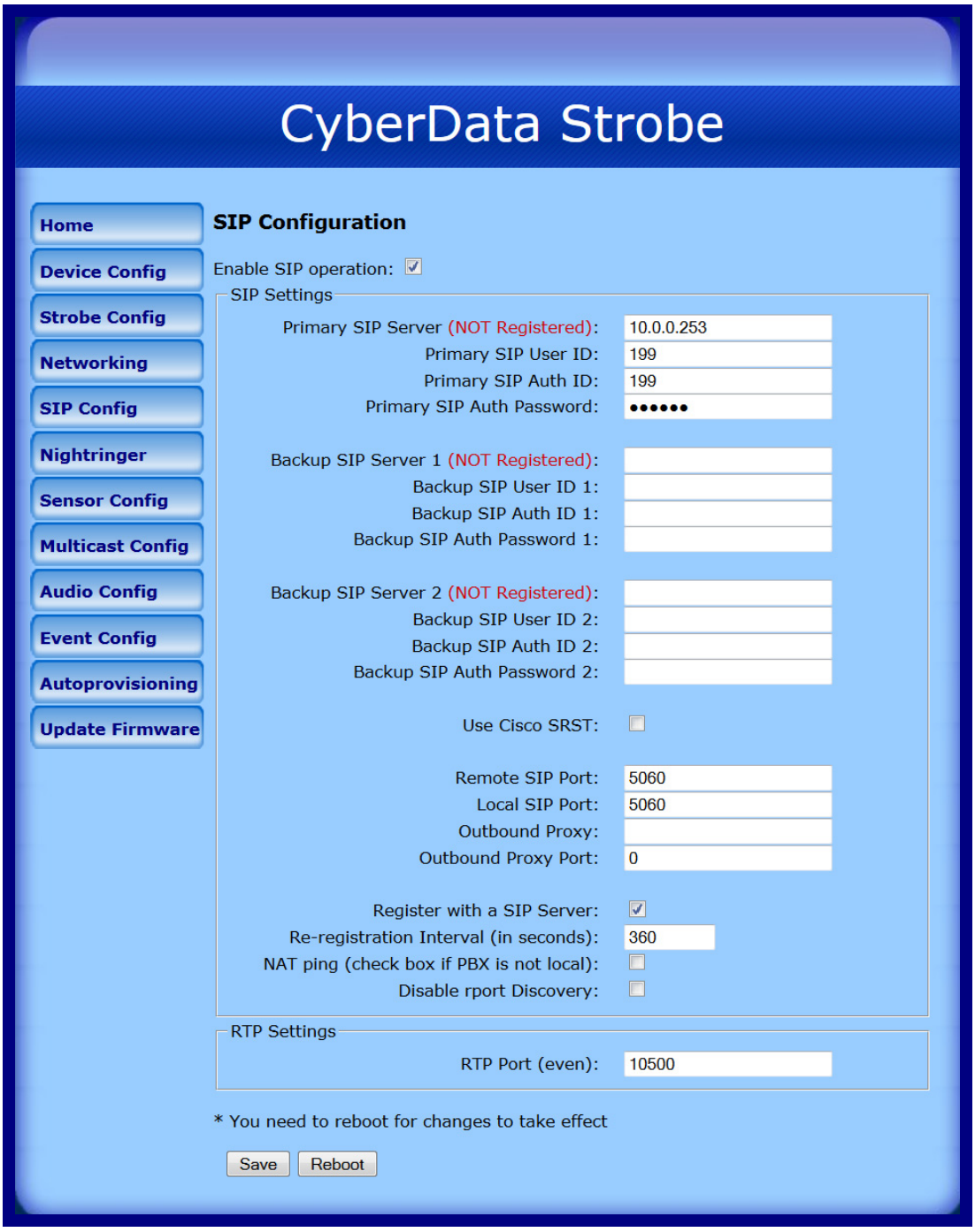
3. After changing the parameters, click **Save Settings**. This updates the changed parameters and reboots the Singlewire Strobe if appropriate.
4. Connect the Singlewire Strobe to the target network.
5. From a system on the same network as the Singlewire Strobe, open a browser with the new IP address of the Singlewire Strobe.

2.2.6 Configure the SIP Parameters

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

Note For specific server configurations, go to the following website address: http://www.cyberdata.net/support/server/index.html

Figure 2-16. SIP Configuration Page



2. On the **SIP Configuration** page, enter values for the parameters indicated in Table 2-12.

Table 2-12. SIP Configuration Parameters

Web Page Item	Description
Enable SIP Operation	Enables or disables SIP operation.
SIP Settings	
Primary SIP Server [registration status]	Type the SIP server represented as either a numeric IP address in dotted decimal notation or the fully qualified host name (255 character limit [FQDN]).
Primary SIP User ID	Type the **SIP User ID** for the Primary SIP Server (up to 64 alphanumeric characters).
Primary SIP Auth ID	Type the **SIP Authenticate ID** for the Primary SIP Server (up to 64 alphanumeric characters).
Primary SIP Auth Password	Type the **SIP Authenticate Password** for the Primary SIP Server (up to 64 alphanumeric characters).
Backup SIP Server 1 Backup SIP Server 2	• If all of the **SIP Server** and **Backup SIP Server** fields are populated, the device will attempt to stay registered with all three servers all of the time. You can leave the **Backup SIP Server 1** and **Backup SIP Server 2** fields blank if they are not needed. • In the event of a registration failure on the **Primary SIP Server**, the device will use the next highest priority server for outbound calls (**Backup SIP Server 1**). If **Backup SIP Server 1** fails, the device will use **Backup SIP Server 2**. • If a higher priority SIP Server comes back online, the device will switch back to this server.
Backup SIP User ID 1 Backup SIP User ID 2	Type the **SIP User ID** for the Backup SIP Server (up to 64 alphanumeric characters).
Backup SIP Auth ID 1 Backup SIP Auth ID 2	Type the **SIP Authenticate ID** for the Backup SIP Server (up to 64 alphanumeric characters).
Backup SIP Auth Password 1 Backup SIP Auth Password 2	Type the **SIP Authenticate Password** for the Backup SIP Server (up to 64 alphanumeric characters).
Use Cisco SRST	When selected, the backup servers are handled according to Cisco SRST (Survivable Remote Site Telephony).
Remote SIP Port	Type the **Remote SIP Port** number (default 5060) (5 character limit [values from 1 to 65535]).
Local SIP Port	Type the **Local SIP Port** number (default 5060) (5 character limit [values from 2000 to 65535]).
Outbound Proxy	Type the Outbound Proxy as either a numeric IP address in dotted decimal notation or the fully qualified host name (255 character limit [FQDN]).
Outbound Proxy Port	Type the Outbound Proxy Port number (5 character limit [values from 1 to 65535]).
Register with a SIP Server	Check this box to enable SIP Registration.
Re-registration Interval (in seconds)	Type the SIP registration lease time (in seconds).

Table 2-12. SIP Configuration Parameters (continued)

Web Page Item	Description
NAT ping (check box if PBX is not local)	Check this box if the PBX server is remote and you are experiencing problems establishing calls with the PBX.
Disable rport Discovery	Check this box prevent the device from including the public WAN IP address in the contact information that is sent to the remote SIP servers. This will generally only need to be enabled when using an SBC in conjunction with a remote SIP server.
RTP Settings	
RTP Port (even)	Specify the port number used for the RTP stream after establishing a SIP call. This port number has to be an even number and defaults to 10500.
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.

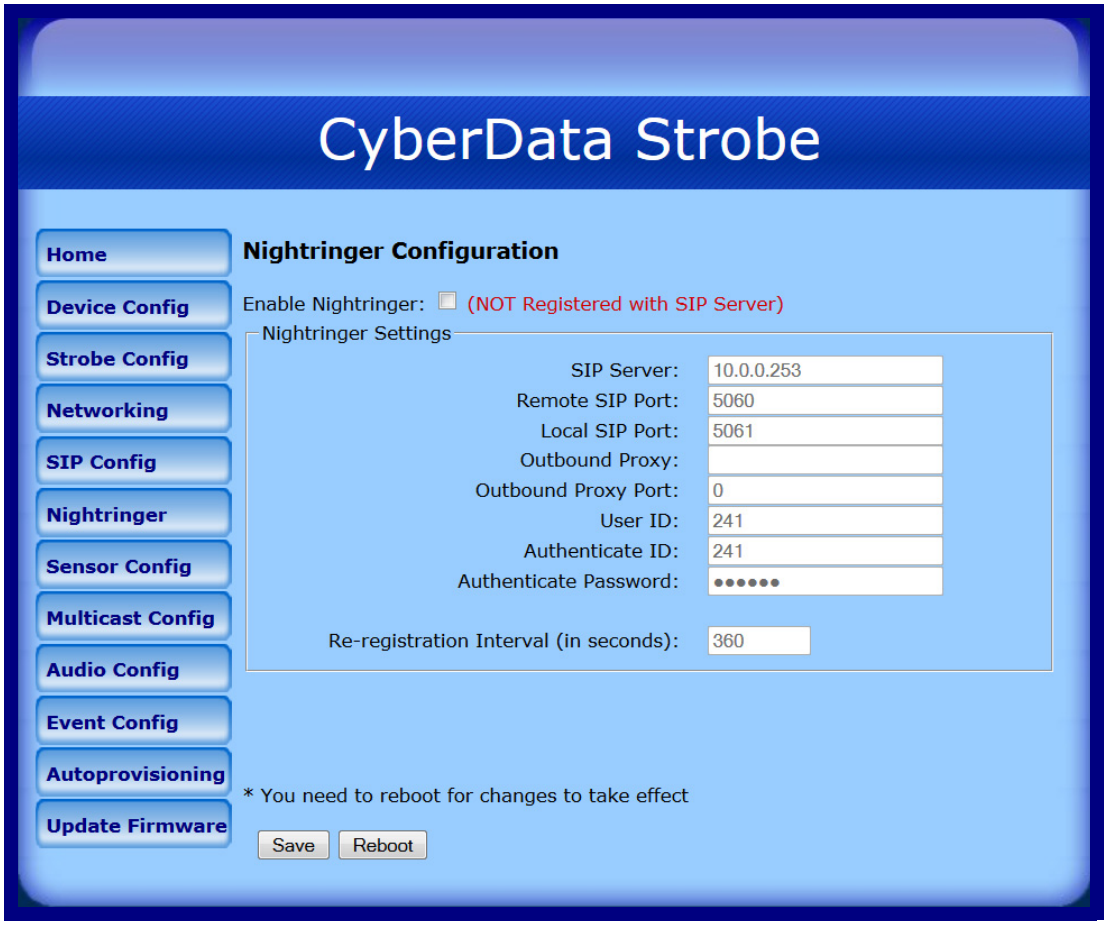
3. After changing the parameters, click **Save Settings**.

2.2.7 Configure the Night Ringer Parameters

When the Nightringer is enabled, the device will register as a second SIP extension. Registration does not have to be to the same server as the primary SIP registration. Any calls made to the Nightringer extension will cause the device to play a ring tone. There is no way to answer this call. The Nightringer is designed to be used in buildings where calls made after hours are directed to a ring group.

1. Click on the **Nightringer** button to open the **Nightringer Configuration** page. See Figure 2-17.

Figure 2-17. Nightringer Configuration Setup



2. On the **Nightringer Configuration** page, enter values for the parameters indicated in Table 2-13.

Table 2-13. Nightringer Configuration Parameters

Web Page Item	Description
Enable Nightringer	When the nightringer is enabled, the SIP Strobe will attempt to register a second extension with the SIP server. Any calls made to this extension will cause the strobe to flash.
Nightringer Settings	
SIP Server	Type the SIP server represented as either a numeric IP address in dotted decimal notation.
Remote SIP Port	Type the Remote SIP Port number (default 5060) (8 character limit).
Local SIP Port	Type the Local SIP Port number (default 5060) (8 character limit). **Note**: This value cannot be the same as the **Local SIP Port** found on the **SIP Configuration Page**.
Outbound Proxy	Type the Outbound Proxy as either a numeric IP address in dotted decimal notation or the fully qualified host name (255 character limit [FQDN]).
Outbound Proxy Port	Type the Outbound Proxy Port number (8 character limit).
User ID	Type the **User ID** (up to 64 alphanumeric characters).
Authenticate ID	Type the **Authenticate ID** (up to 64 alphanumeric characters).
Authenticate Password	Type the **Authenticate Password** (up to 64 alphanumeric characters).
Re-registration Interval (in seconds)	Type the SIP Registration lease time (in seconds).
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.

3. After changing the parameters, click on the **Save** button.

2.2.8 Configure the Sensor Configuration Parameters

The sensor (pins 5 and 6) on the header can be used to monitor the open or closed state of a switch. There is an option on the **Sensor Configuration** page to trigger on an open or short condition on these pins.

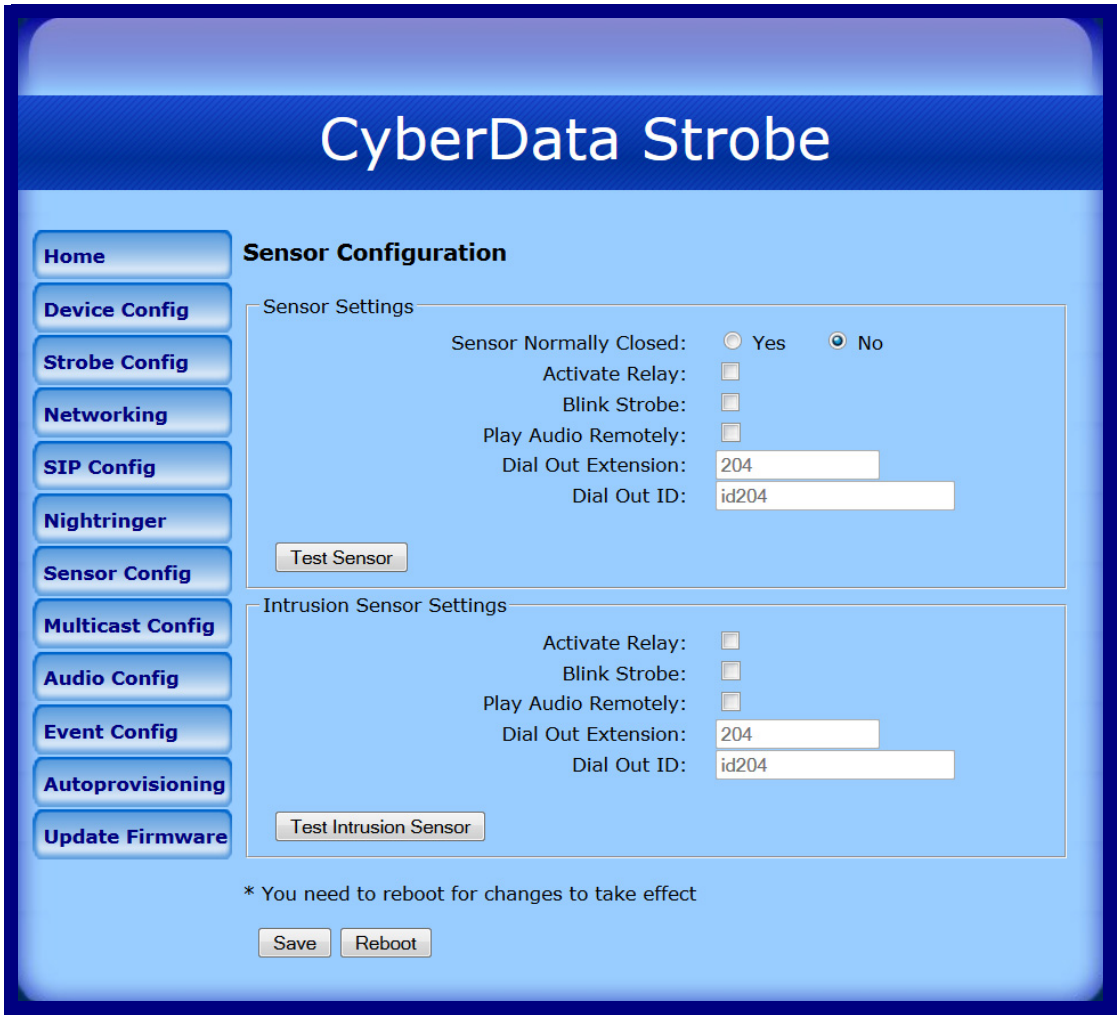
The intrusion sensor is an optical sensor installed on the Singlewire Strobe board and will be activated when the Singlewire Strobe is removed from the case.

For each sensor there are two actions the Singlewire Strobe can take:

- Flash the LED until the sensor is deactivated (roughly 10 times/second)
- Activate the relay until the sensor is deactivated

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

Figure 2-18. Sensor Configuration Page



2. On the **Sensor Configuration** page, enter values for the parameters indicated in Table 2-14.

Table 2-14. Sensor Configuration Parameters

Web Page Item	Description
Sensor Settings	
Sensor Normally Closed	Select the inactive state of the sensors.
Activate Relay	Check this box to blink the strobe light until the sensor is deactivated.
Blink Strobe	Check this box to activate the blinking strobe until the sensor is deactivated.
Play Audio Remotely	Check this box to loop an audio file out of a remote speaker until the sensor is deactivated.
Dial Out Extension	Enter the desired dial-out extension number.
Dial Out ID	Type the desired Extension ID (64 character limit).
Test Sensor	Use this button to test the sensor.
Intrusion Sensor Settings	
Activate Relay	Check this box to activate the relay until the sensor is deactivated.
Blink Strobe	Check this box to blink the strobe light until the sensor is deactivated.
Play Audio Remotely	Check this box to loop an audio file out of a remote speaker until the sensor is deactivated.
Dial Out Extension	Enter the desired dial-out extension number.
Dial Out ID	Type the desired Extension ID (64 character limit).
Test Intrusion Sensor	Use this button to test the Intrusion sensor.
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.

3. After changing the parameters, click **Save Settings**.

2.2.9 Configure the Multicast Parameters

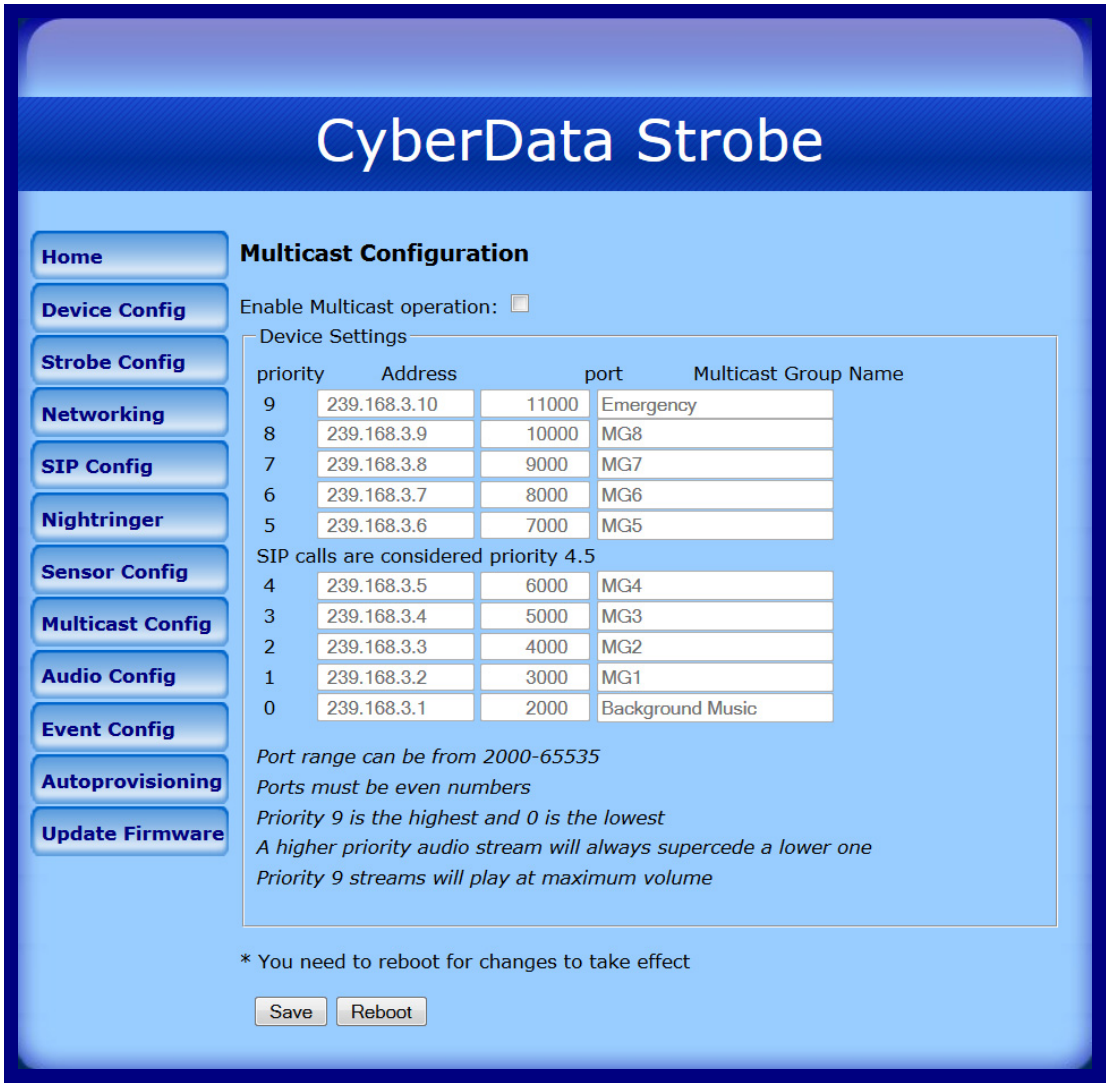
The **Multicast Configuration** page allows the device to join up to ten paging zones for receiving ulaw/alaw encoded RTP audio streams.

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.

1. Click on the **Multicast Configuration** button to open the **Multicast Configuration** page. See Figure 2-19.

Figure 2-19. Multicast Configuration Page



2. On the **Multicast Configuration** page, enter values for the parameters indicated in Table 2-15.

Table 2-15. Multicast Configuration Parameters

Web Page Item	Description
Enable Multicast Operation	Enables or disables multicast operation.
Device Settings	
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 (range can be from 2000 to 65535)	Enter the port number for this multicast group (5 character limit). **Note**: The multicast ports have to be even values. The webpage will enforce this restriction.
Multicast Group Name	Assign a descriptive name for this multicast group (25 character limit).
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.

3. After changing the parameters, click on the **Save** button.

2.2.9.1 Assigning Priority

When playing multicast streams, audio on different streams will preempt each other according to their priority in the list. An audio stream with a higher priority will interrupt a stream with a lower priority.

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 level is set to maximum.

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

Ringtones and Nightringtones

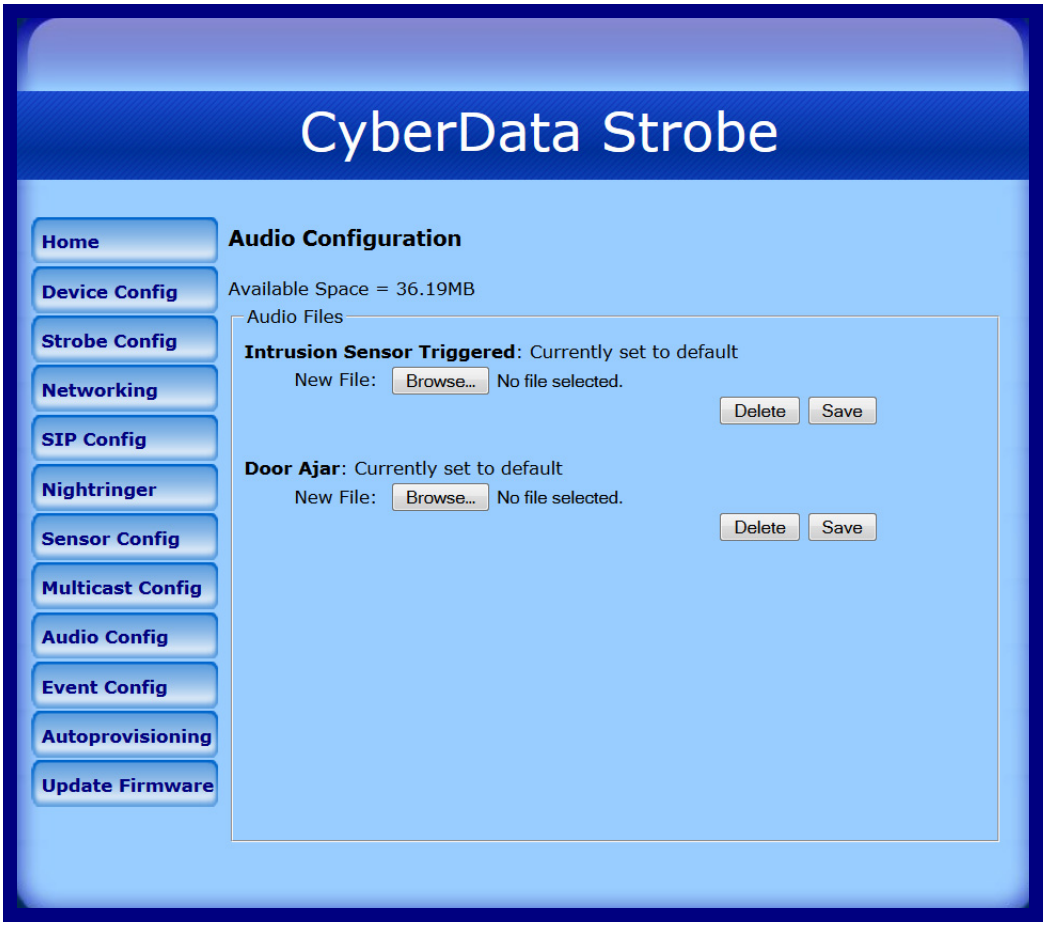
Ringtones all play at the same priority level. This means that it is possible to have a nightring tone and a normal ringtone playing at the same time.

2.2.10 Configure the Audio Configuration Parameters

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

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

Figure 2-20. Audio Configuration Page



2. On the **Audio Configuration** page, enter values for the parameters indicated in Table 2-16.

Table 2-16. Audio Configuration Parameters

Web Page Item	Description
Audio Files	
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...	The **Browse** button will allow you to navigate to and select an 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.

2.2.10.1 User-created Audio Files

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

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

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

Figure 2-21. Audacity 1

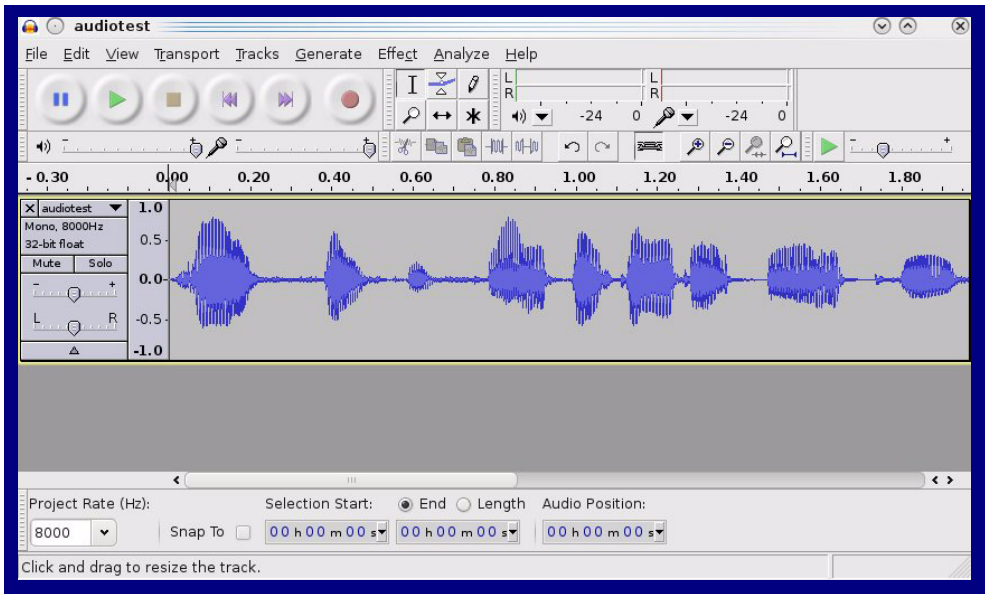
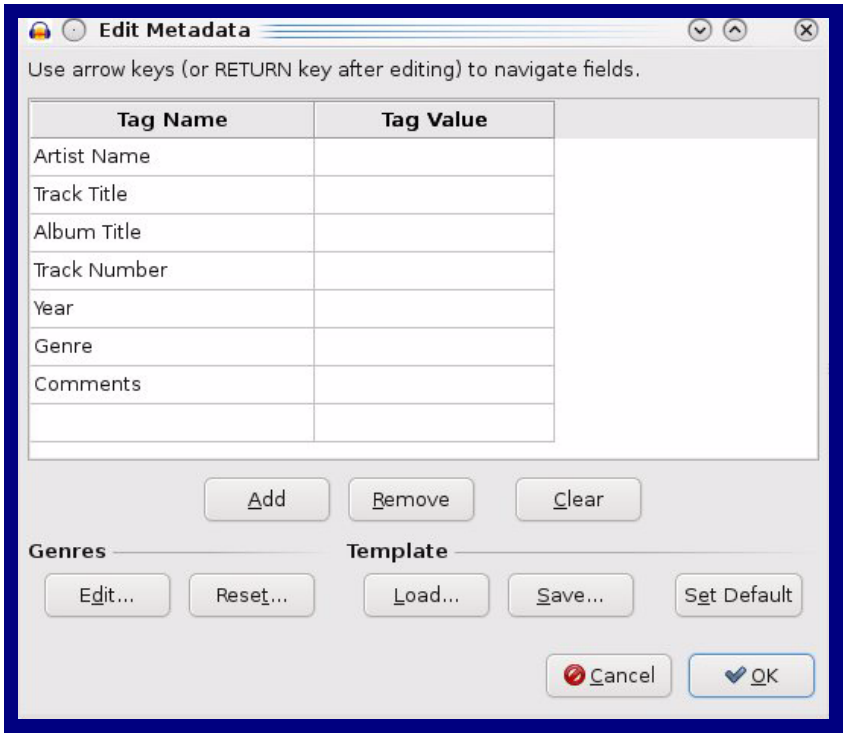


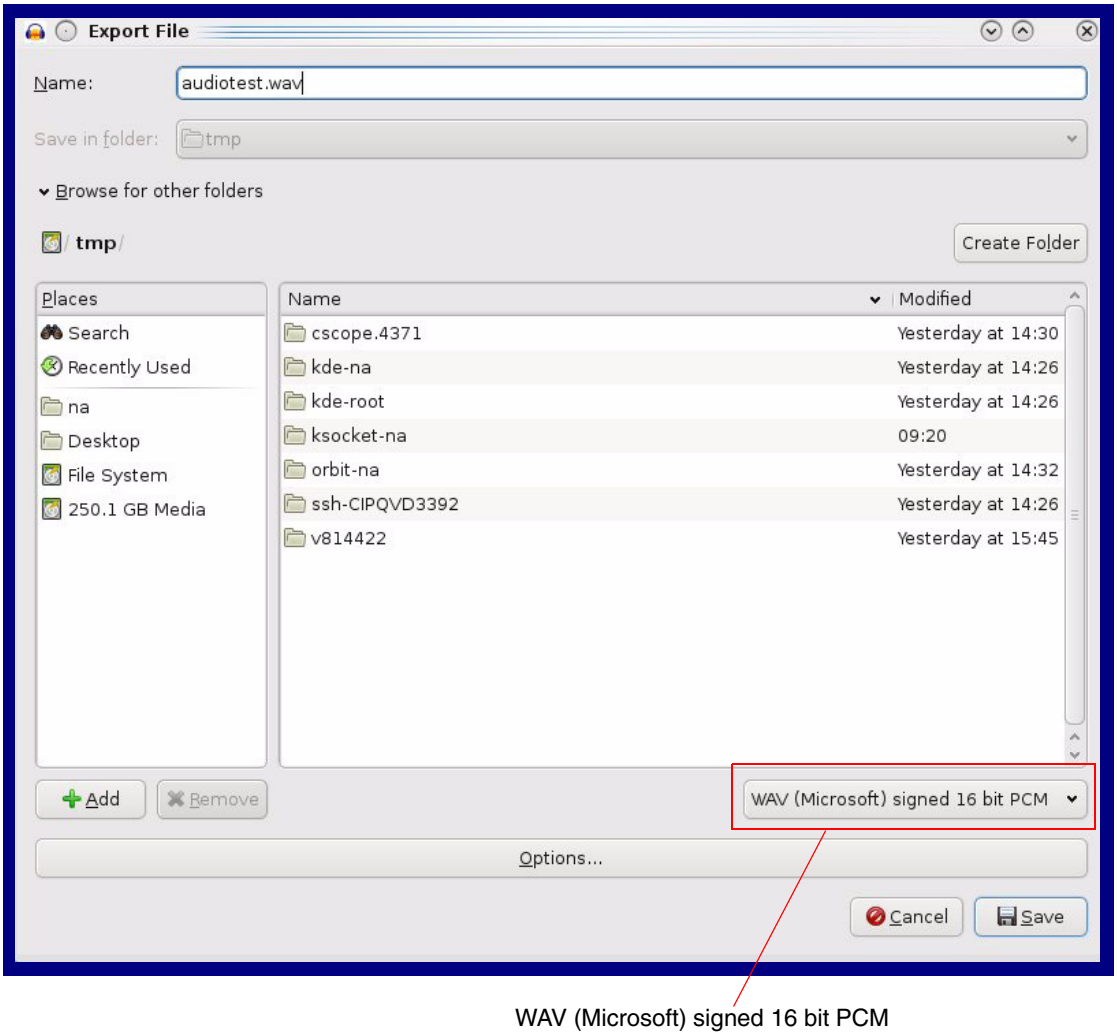
Figure 2-22. Audacity 2



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

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

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



2.2.11 Configure the Event Parameters

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

Figure 2-24. Event Configuration Page

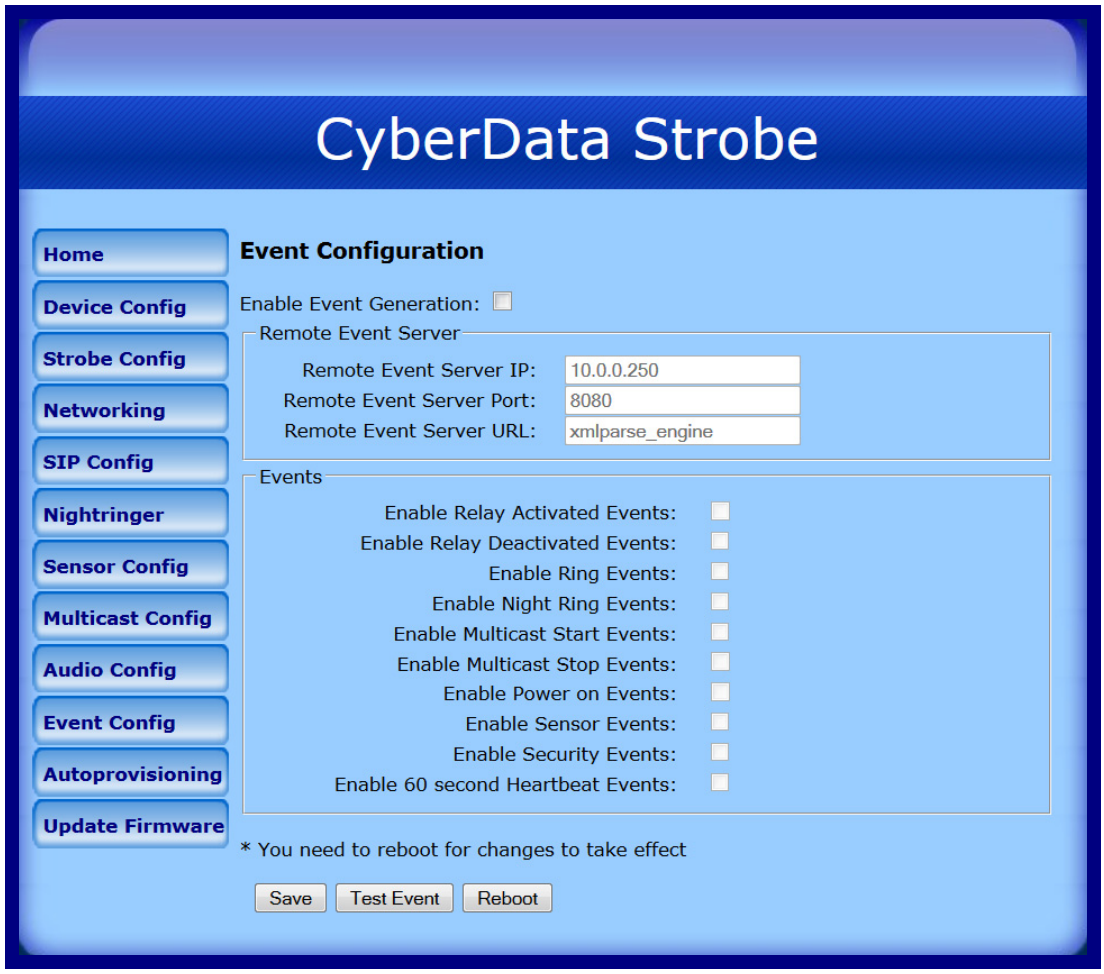


Table 2-17 shows the web page items on the **Event Configuration** page.

Table 2-17. Event Configuration

Web Page Item	Description
Enable Event Generation	When selected, Event Generation is enabled.
Remote Event Server	
Remote Event Server IP	Type the Remote Event Server IP address. (64 character limit)
Remote Event Server Port	Type the Remote Event Server port number. (8 character limit)
Remote Event Server URL	Type the Remote Event Server URL. (127 character limit)
Events	
Enable Relay Activated Events	When selected, Relay Activated Events are enabled.
Enable Relay Deactivated Events	When selected, Relay Deactivated Events are enabled.
Enable Ring Events	When selected, Ring Events are enabled.
Enable Night Ring Events	When selected, there is a notification when the device receives a night ring.
Enable Multicast Start Events	When selected, Multicast Start Events are enabled.
Enable Multicast Stop Events	When selected, Multicast Stop Events are enabled.
Enable Power On Events	When selected, Power On Events are enabled.
Enable Sensor Events	When selected, Sensor Events are enabled.
Enable Security Events	When selected, Security Events are enabled.
Enable 60 Second Heartbeat Events	When selected, 60 Second Heartbeat Events are enabled.
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Test Event	Click on the **Test Event** button to test an event.
Reboot	Click on the **Reboot** button to reboot the system.

2.2.11.1 Example Packets for Events

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

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

Here are example packets for every event:

```
POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 197
Content-Type: application/x-www-form-urlencoded

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


POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 199
Content-Type: application/x-www-form-urlencoded

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


POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 196
Content-Type: application/x-www-form-urlencoded

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

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 201
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData SIP Device' MAC='0020f70015b6'>
<event>CALL_ACTIVE</event>
</cyberdata>
POST xmlparse_engine HTTP/1.1
```

```
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 205
Content-Type: application/x-www-form-urlencoded

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


POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 197
Content-Type: application/x-www-form-urlencoded

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


POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded

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

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 233
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData 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</event>
</cyberdata>
POST xmlparse_engine HTTP/1.1
```

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

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

2.2.12 Configure the Autoprovisioning Parameters

Autoprovisioning can be used to configure your device automatically on boot, after a periodic delay, after sitting idle for a period of time, or at a specified time.

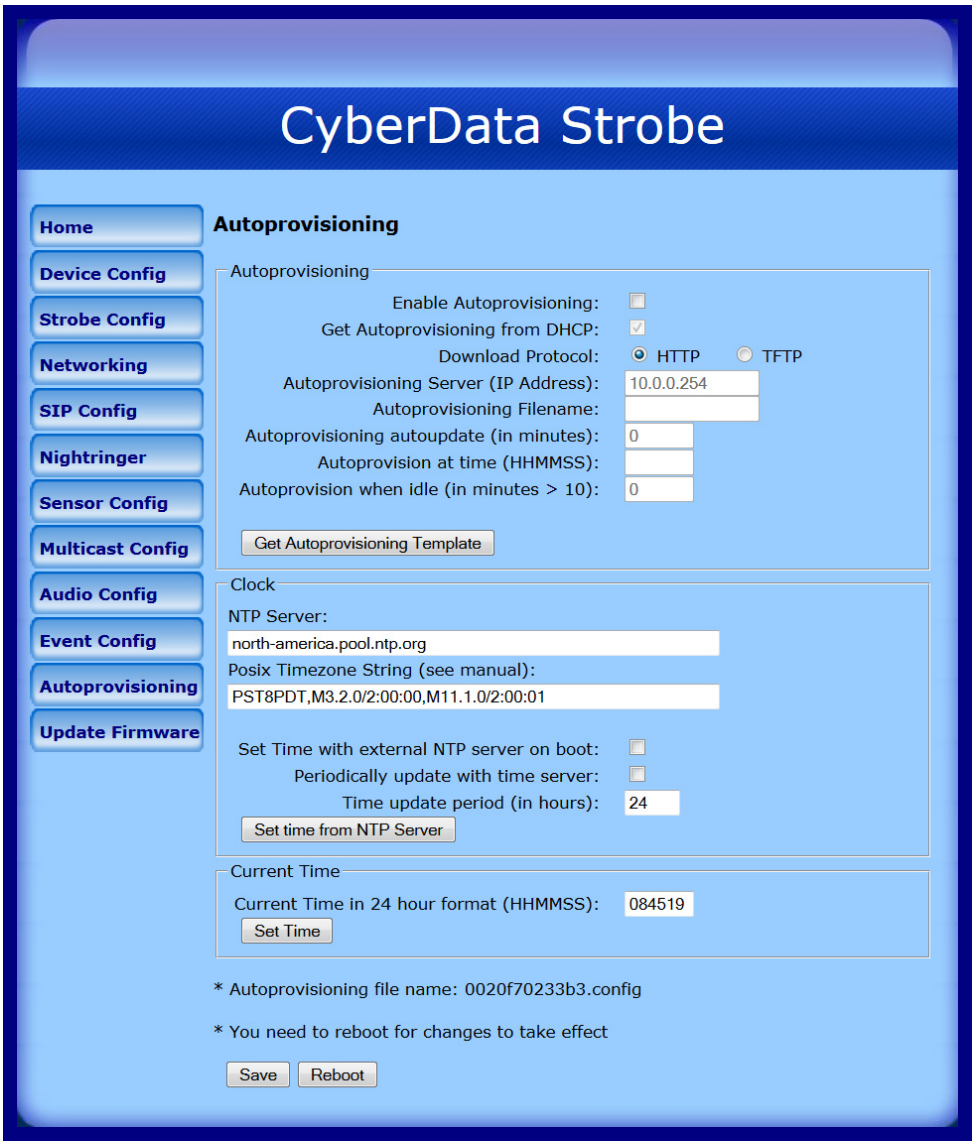
The autoprovisioning file contains the board configuration in xml format. Autoprovisioned values in this file will override values stored in on-board memory.

The autoprovisioning file can be hosted with a tftp or a web server and by default is named according to the MAC address of the device (for example: 0020f7350058.config). The autoprovisioning filename can also be specified.

The device does not have a real time clock but can sync with a network time server on boot.

1. Click the **Autoprovisioning** button to open the **Autoprovisioning Configuration** page. See Figure 2-25.

Figure 2-25. Autoprovisioning Configuration Page



2. On the **Autoprovisioning Configuration** page, you may enter values for the parameters indicated in Table 2-18.

Table 2-18. Autoprovisioning Configuration Parameters

Web Page Item	Description
Autoprovisioning	
Enable Autoprovisioning	See Section 2.2.12.1, "Autoprovisioning".
Get Autoprovisioning from DHCP	See Section 2.2.12.1, "Autoprovisioning".
Download Protocol	Allows you to select whether the autoprovisioning file is acquired via **TFTP** or **HTTP**.
Autoprovisioning Server (IP Address)	See Section 2.2.12.1, "Autoprovisioning" (15 character limit).
Autoprovisioning Filename	Type the desired name for the autoprovisioning file.
Autoprovisioning Autoupdate (in minutes)	Type the desired time (in minutes) that you want the Autoprovisioning feature to update (6 character limit).
Autoprovision at time (HHMMSS)	Type the desired time of day that you want the Autoprovisioning feature to update (must be 6 characters).
Autoprovision when idle (in minutes > 10)	Type the desired time (in minutes greater than 10) that you want the Autoprovisioning feature to update after a certain amount of idle time (6 character limit).
Get Autoprovisioning Template	Press the **Get Autoprovisioning Template** button to create an autoprovisioning file for this unit. See Section 2.2.12.2, "Get Autoprovisioning Template Button"
Clock	
NTP Server	Allows you to select the NTP server (64 character limit).
Posix Timezone String	See Section 2.2.12.3, "Time Zone Strings" (43 character limit).
Set Time with External NTP Server on boot	When selected, the time is set with an external NTP server when the device restarts.
Periodically update with time server	When selected, the time is periodically updated with a time server.
Time update period (in hours)	Allows you to select the time updated period (in hours) (4 character limit).
Set time from NTP Server	Allows you to set the time from the NTP server.
Current Time	
Current Time (UTC) in 24 hour format (**HHMMSS**)	Allows you to input the current time in the 24 hour format. (6 character limit)
Set Time	Click on this button to set the clock after entering the current time.
Save	Click on the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.

2.2.12.1 Autoprovisioning

Autoprovisioning File

It is not necessary to set every option found in the autoprovisioning template. As long as the XML is valid, the file can contain any subset. Options not autoprovisioned will default to the values stored in the on board memory. For example if you only wanted to modify the device name, the following would be a valid autoprovisioning file:

```
<?xml version="1.0" encoding="utf-8" ?>
<specific>
    <MiscSettings>
        <DeviceName>auto Strobe</DeviceName>
    </MiscSettings>

</specific>
```

Get Autoprovisioning from DHCP

When this option is checked, the device will automatically fetch its autoprovisioning server address from the DHCP server. The device will use the address specified in **OPTION 150** (TFTP-server-name) or **OPTION 66**. If both options are set, the device will use **OPTION 150**.

Refer to the documentation of your DHCP server for setting up **OPTION 150**.

To set up a Linux DHCPD server to serve autoprovisioning information (in this case using both option 66 and 150), here's an example dhcpd.conf:

```
# dhcpd.conf
#
# Configuration file for ISC dhcpd (see 'man dhcpd.conf')
#
ddns-update-style ad-hoc;

option option-150 code 150 = ip-address;

subnet 10.0.0.0 netmask 255.0.0.0 {
        max-lease-time 120;
        default-lease-time 120;

        option routers                  10.0.0.1;
        option subnet-mask              255.0.0.0;

        option domain-name              "voiplab";
        option domain-name-servers       10.0.0.1;

        option time-offset              -8;     # Pacific Standard Time

        option tftp-server-name         "10.0.0.254";

        option option-150               10.0.0.254;

        range 10.10.0.1 10.10.2.1;}
```

Autoprovisioning Server (IP Address)

Instead of using DHCP to provide the autoprovisioning tftp server address, you can specify an address manually.

Autoprovisioning Autoupdate

When the device is set to autoprovision either after a period of time, or when idle, or at a time of day, the device will do the following:

- Re-download the autoprovisioning file.
- Compare this new file to the one downloaded on boot, and if it finds differences, force a system reset.
- After rebooting, the board will configure itself according to this new file.

Autoprovisioned Firmware Upgrades

An Autoprovisioned firmware upgrade only happens after a reboot, will take roughly three minutes, and the web page will be unresponsive during this time.

The '**FirmwareVersion**' value in the xml file *must* match the version stored in the '**FirmwareFile**'.

```
<FirmwareVersion>v10.0.1</FirmwareVersion>
<FirmwareFile>1001-strobe-uImage</FirmwareFile>
```

If these values are mismatched, the board can get stuck in a loop where it goes through the following sequence of actions:

1. The board downloads and writes a new firmware file.
2. After the next reboot, the board recognizes that the firmware version does not match.
3. The board downloads and writes the firmware file again.

CyberData has timed a firmware upgrade at 140 seconds. Therefore, if you suspect the board is stuck in a loop, either remove or comment out the **FirmwareVersion** line in the XML file and let the board boot as it normally does.

Autoprovisioned Audio Files

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

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

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

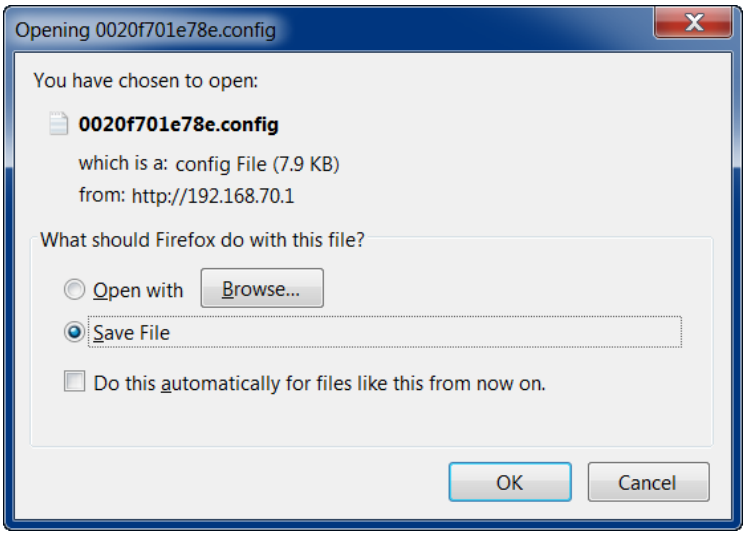
2.2.12.2 Get Autoprovisioning Template Button

The **Get Autoprovisioning 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 **Get Autoprovisioning Template** button.
2. You will see a window prompting you to save a configuration file (**.config**) to a location on your computer (Figure 2-26). 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 2-26.

Figure 2-26. 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.

2.2.12.3 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 2-19 shows some common strings.

Table 2-19. Common Time Zone Strings

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

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

Table 2-20 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 2-20. Time Zone String Parts

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

Time Zone String Examples

Table 2-21 has some more examples of time zone strings.

Table 2-21. Time Zone String Examples

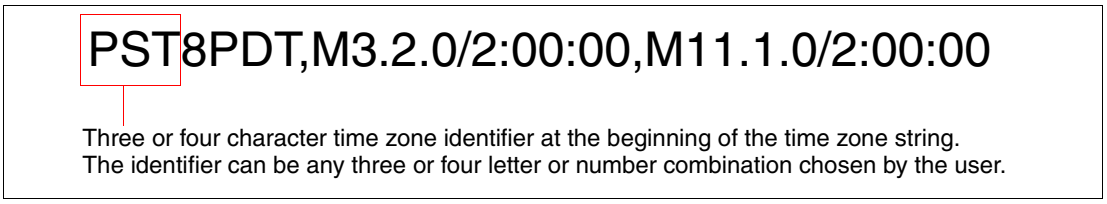
Time Zone	Time Zone String
Tokyo[a]	IST-9
Berlin[b]	CET-1MET,M3.5.0/1:00,M10.5.0/1:00

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 2-27. 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 2-22 has information about the GMT time in various time zones.

Table 2-22. World GMT Table

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

Table 2-22. World GMT Table (continued)

Time Zone	City or Area Zone Crosses
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

2.3 Upgrade the Firmware and Reboot the Singlewire Strobe

Caution

Equipment Hazard: Devices with a serial number that begins with 0871xxxxx 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

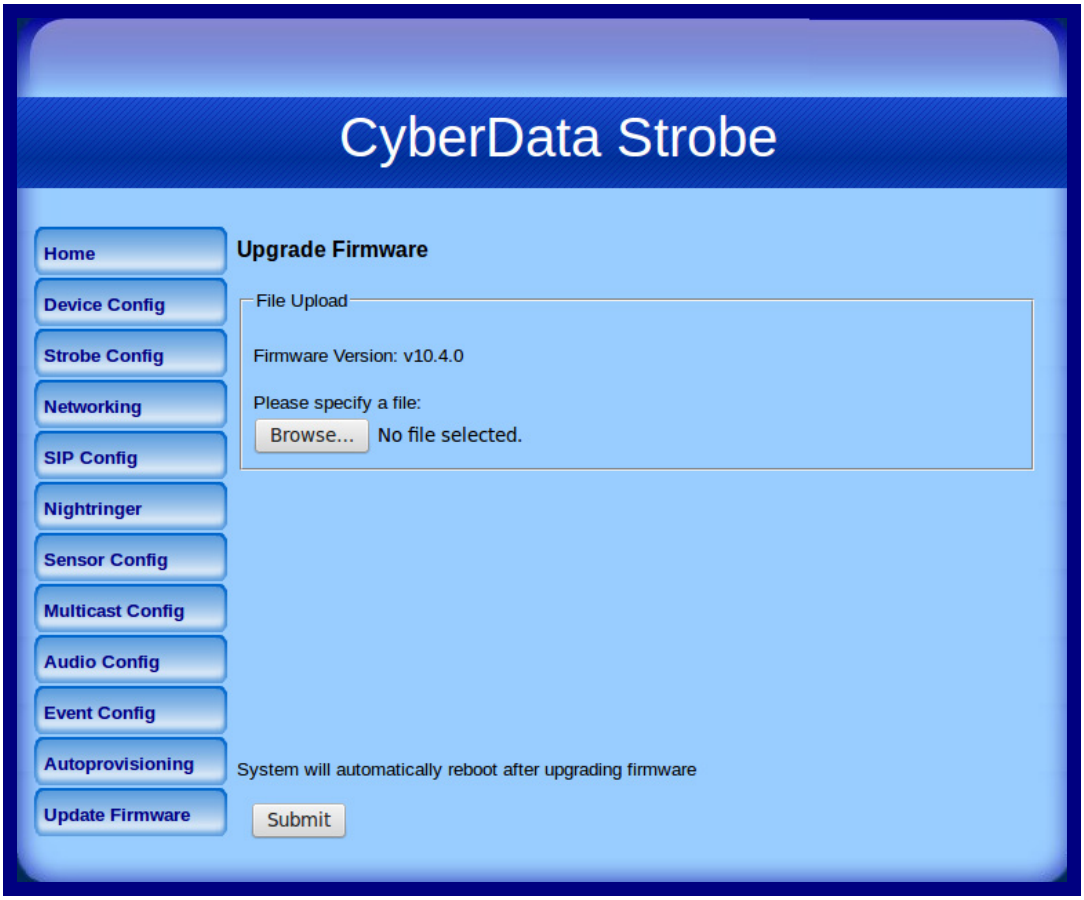
2. Unzip the firmware version file. This file may contain the following:

- Firmware file
- Release notes

3. Log in to the Singlewire Strobe home page as instructed in Section 2.2.2, "Log in to the Configuration Home Page".

4. Click the **Update Firmware** button to open the **Upgrade Firmware** page. See Figure 2-28.

Figure 2-28. Upgrade Firmware Page



5. Select **Browse**, and then navigate to the location of the Singlewire Strobe firmware file.
6. Click **Submit**.

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 **Upgrade Firmware** page will refresh. The uploaded firmware filename should be displayed in the system configuration (indicating successful upload and reboot).

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

Table 2-23. Firmware Upgrade Parameters

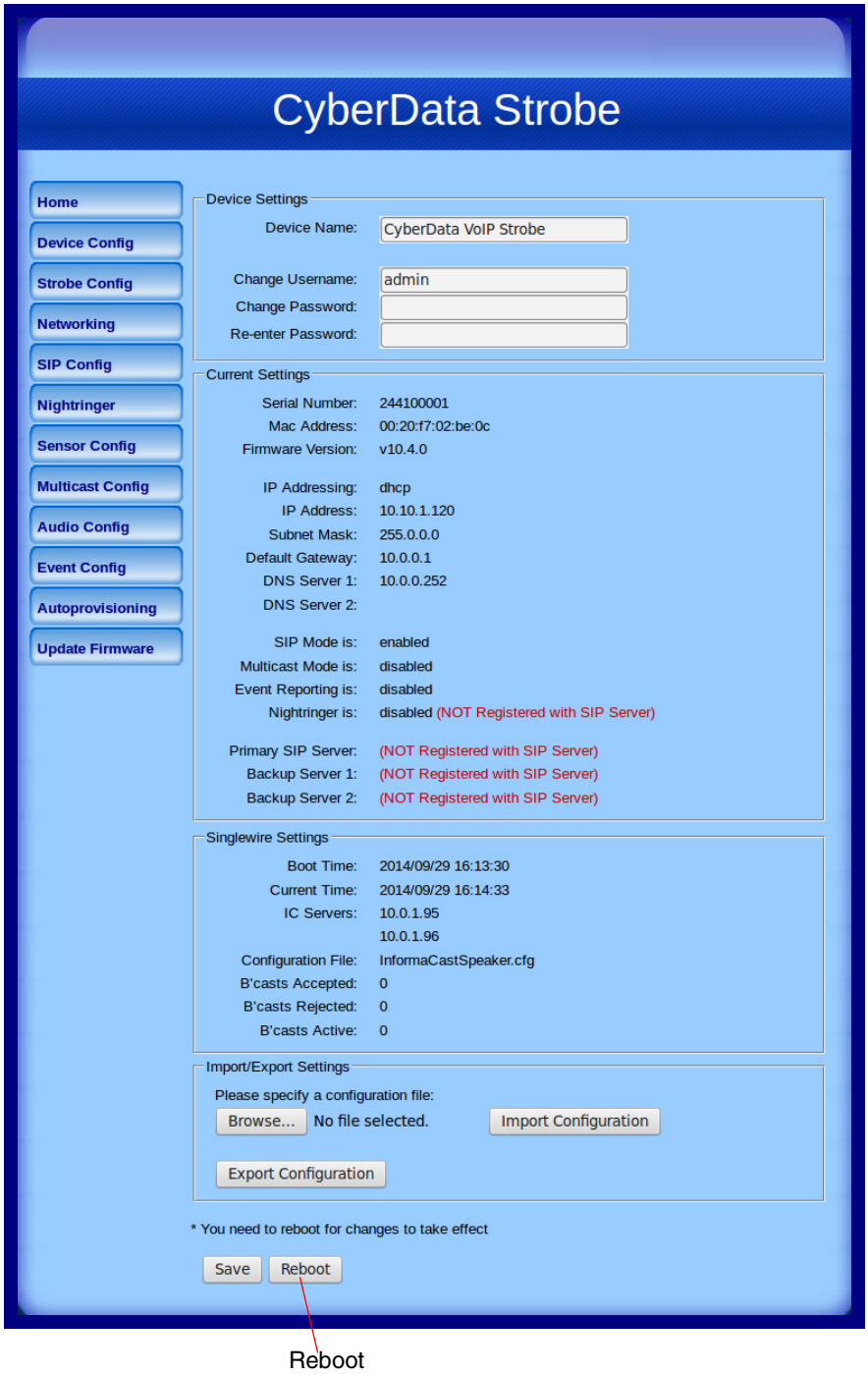
Web Page Item	Description
File Upload	
Firmware Version	Shows the current firmware version.
Browse...	Use the **Browse** button to navigate to the location of the firmware file that you want to upload.
Submit	Click on the **Submit** button to automatically upload the selected firmware and reboot the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

2.3.1 Reboot the Singlewire Strobe

To reboot a Singlewire Strobe:

1. Log in to the web page as instructed in Section 2.2.2, "Log in to the Configuration Home Page".
2. Click the **Reboot** button (Figure 2-29). A normal restart will occur.

Figure 2-29. Reboot Button



2.4 Command Interface

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

2.4.1 Command Interface Post Commands

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

Table 2-24. Command Interface Post Commands

Device Action	HTTP Post Command[a]
Trigger relay (for configured delay)	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/command.cgi" --post-data "test_relay=yes"
Place call to extension (example: extension 130)	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/command.cgi" --post-data "call=130"
Terminate active call	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/command.cgi" --post-data "terminate=yes"
Force reboot	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/command.cgi" --post-data "reboot=yes"
Trigger the Door Sensor Test (Sensor Config page)	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/sensorconfig.cgi" --post-data "doortest=yes"
Trigger the Intrusion Sensor Test (Sensor Config page)	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/sensorconfig.cgi" --post-data "intrusiontest=yes"

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

Appendix A: Mounting the Singlewire Strobe

A.1 Important Safety Instructions

Warning

Electrical Hazard: The Singlewire Strobe enclosure is not rated for any AC voltages.

Warning

Electrical Hazard: This product should be installed by a licensed electrician according to all local electrical and building codes.

Warning

Electrical Hazard: To prevent injury, this apparatus must be securely attached to the floor/wall in accordance with the installation instructions.

Warning

The PoE connector is intended for intra-building connections only and does not route to the outside plant.

A.2 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.

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

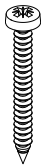
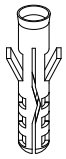
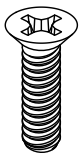
Quantity	Part Name	Illustration
4	#6 x 1.5 inches Sheet Metal Screw	
4	#6 Ribbed Plastic Anchor	

Table A-2. Gang Box Mounting Components

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

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

Section 2.1.4, "Network Connectivity" explains how the **Link** and **Status** LEDs work.

Figure A-1. Network Connector Prior to Installation

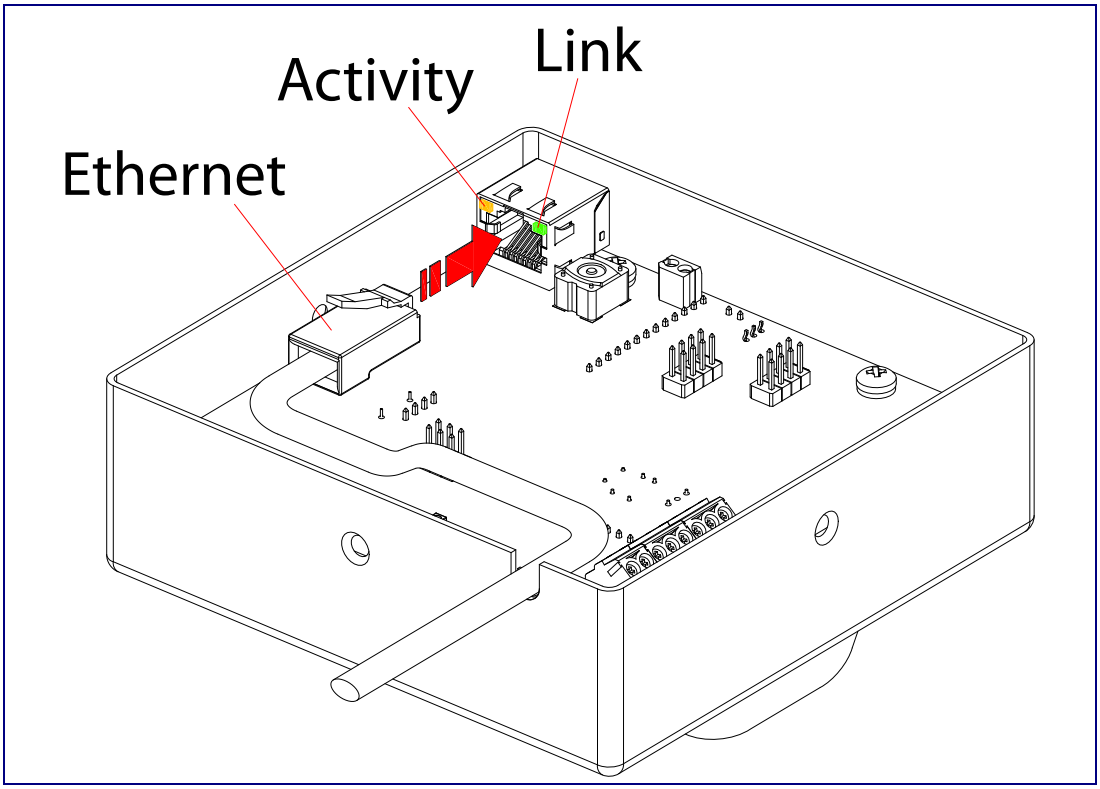


Figure A-2 shows the wall mounting options for the Singlewire Strobe.

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

Figure A-2. Wall Mounting Options

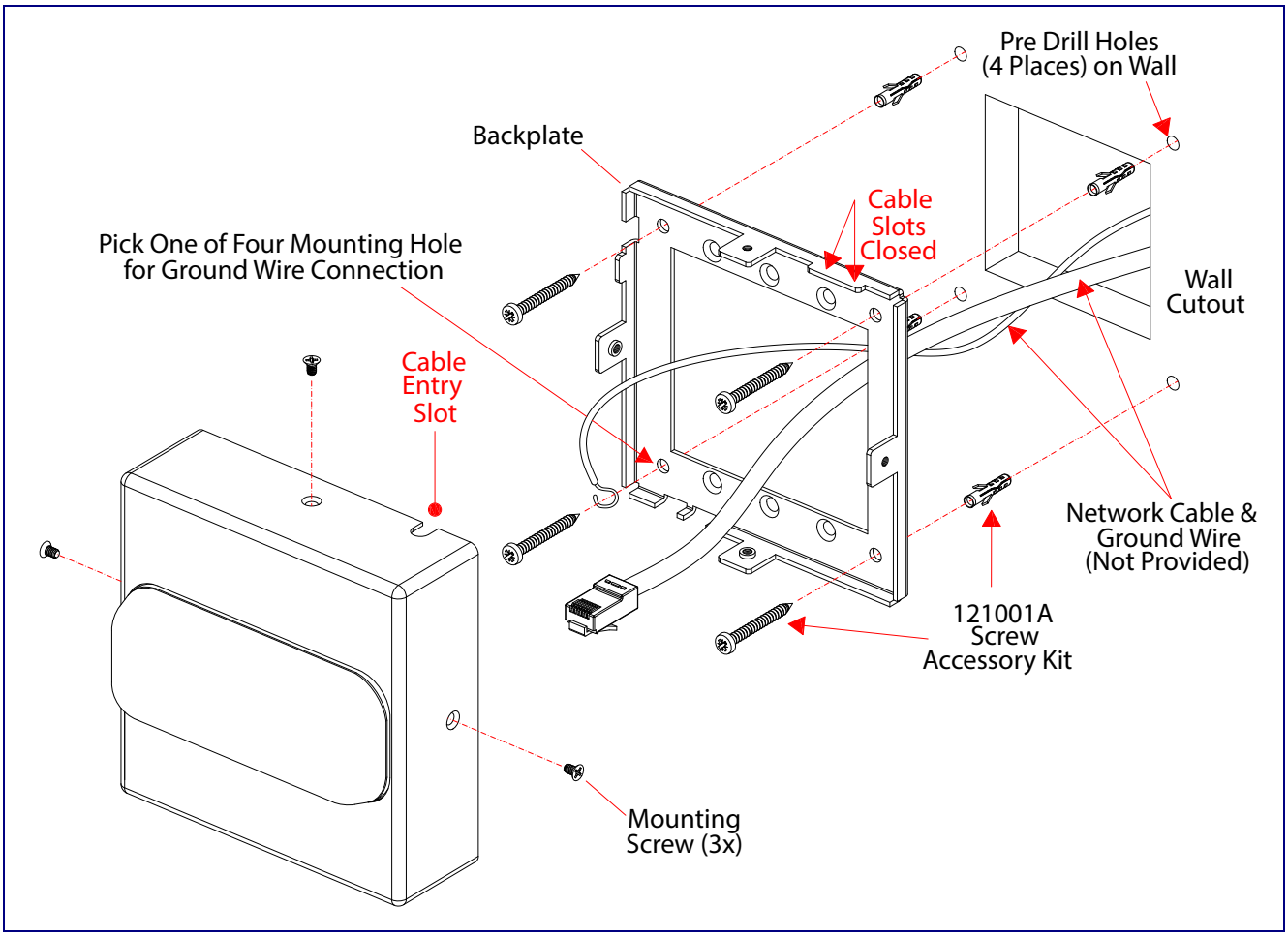


Figure A-3 shows the gang box mounting options for the Singlewire Strobe.

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

Figure A-3. Gang Box Mounting Options

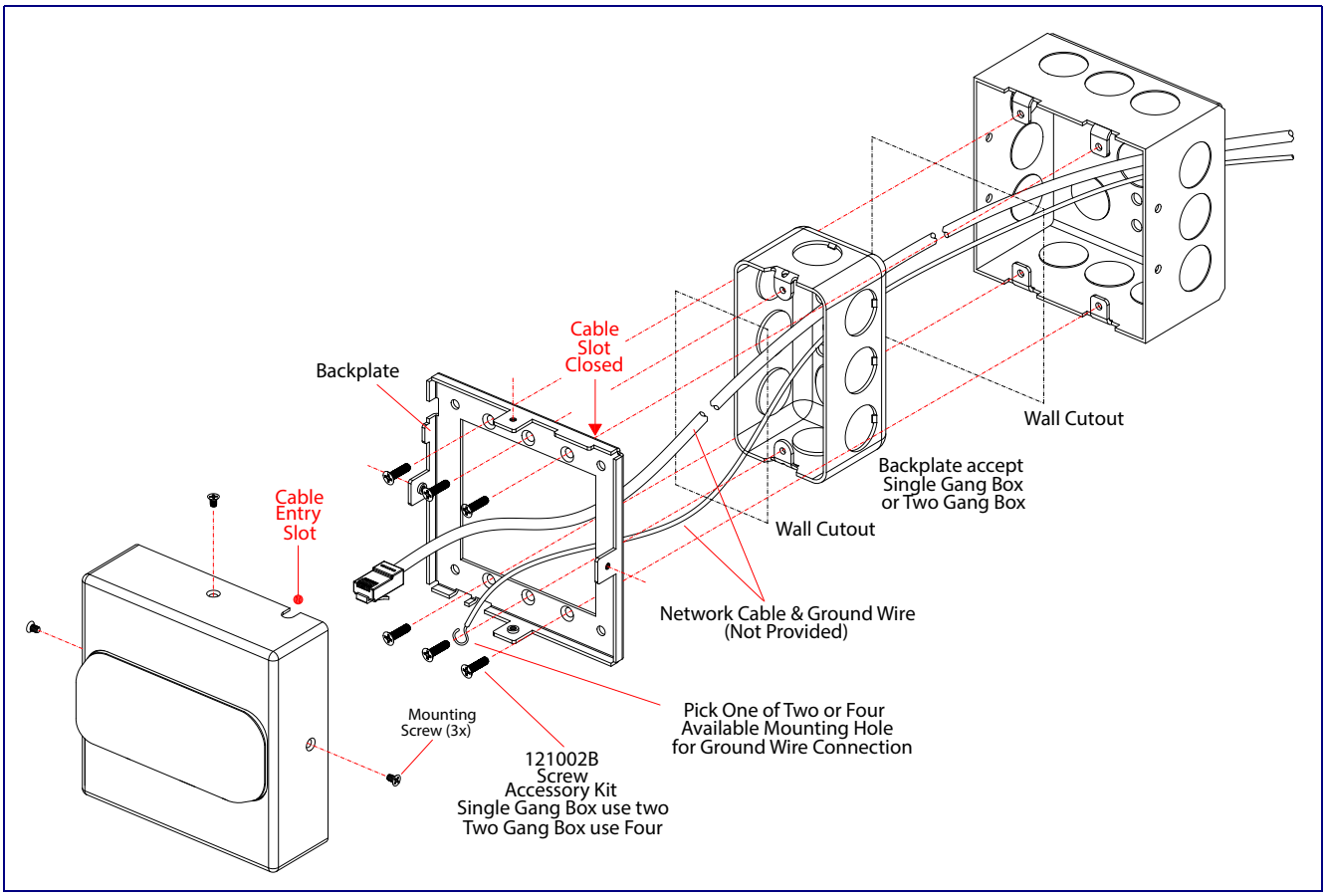
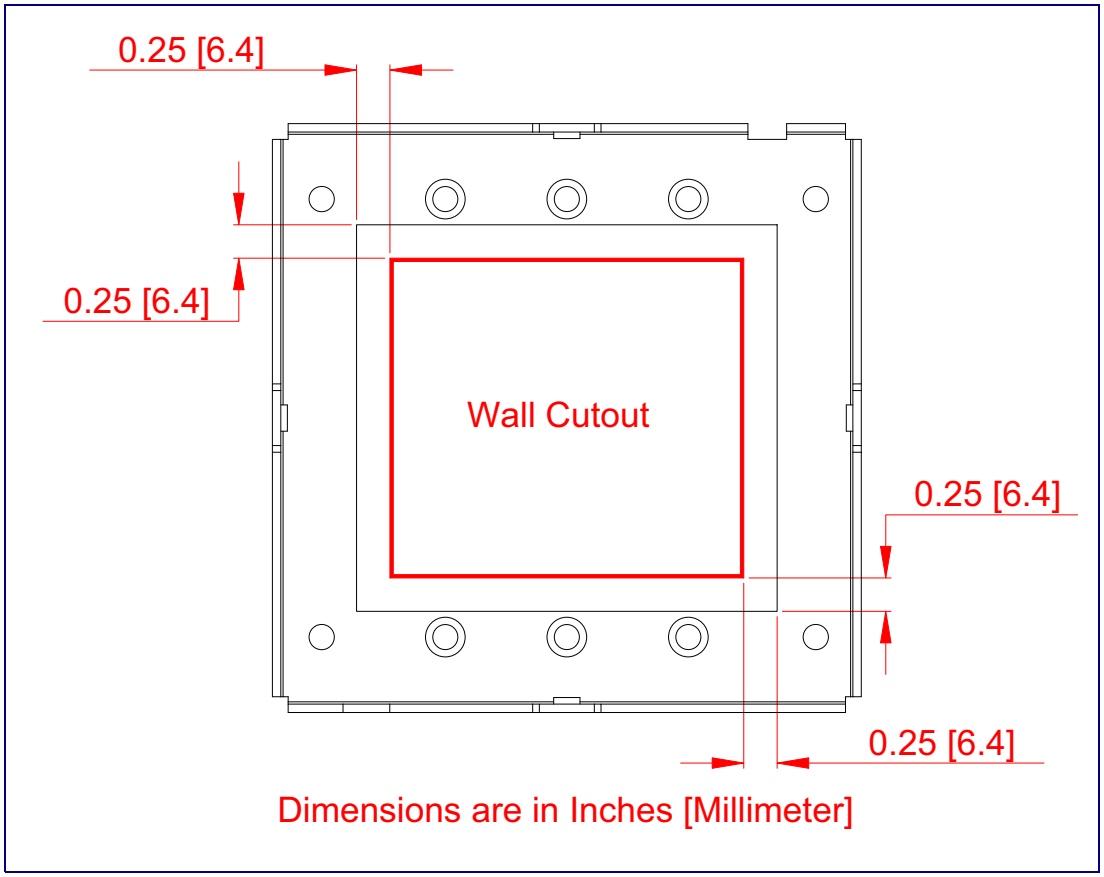


Figure A-4 shows the maximum recommended wall cutout dimensions for mounting the Singlewire Strobe.

Figure A-4. Maximum Recommended Wall Cutout Dimensions



Appendix B: Troubleshooting/Technical Support

B.1 Frequently Asked Questions (FAQ)

A list of frequently asked questions (FAQs) are available on the 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 www.CyberData.net 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://www.cyberdata.net/support/contactsupportvoip.php** Phone: (831) 373-2601, Ext. 333 Email: support@cyberdata.net
Returned Materials Authorization	To return the product, contact the Returned Materials Authorization (RMA) department: 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. No product will 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://www.cyberdata.net/support/rmastatus.html**

B.4 Warranty

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

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

End of Life Devices are included under this policy. End of Life devices are devices that are no longer produced or sold. Technical support is still available for these devices. However, no firmware revisions or updates will be provided. If an End of Life device cannot be repaired, the replacement offered may be the current version of the device.

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

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

B.4.1 Warranty & RMA Returns within the United States

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

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

CyberData Corporation

3 Justin Court.

Monterey, CA 93940

Attn: RMA "xxxxxx"

B.4.2 Warranty & RMA Returns Outside of the United States

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

B.4.3 Spare in the Air Policy

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

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

B.4.4 Return and Restocking Policy

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

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

B.4.5 Warranty and RMA Returns Page

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

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

Index

Numerics

A

B

C

D

E

F

G

H

I

J

L

M

N

P

R

S

T

U

V

W

Y