



*InformaCast Enabled Outdoor RGB  
(Multi-Color) Strobe  
Operations Guide*

**Part #011489**

Document Part #931649B  
for Firmware Version 20.0.0

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

---

**InformaCast Enabled Outdoor RGB (Multi-Color) Strobe Operations Guide 931649B**  
**Part # 011489**

**COPYRIGHT NOTICE:**

© 2020, CyberData Corporation, ALL RIGHTS RESERVED.

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

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

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

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

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



Technical Support

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

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

Email: [support@cyberdata.net](mailto:support@cyberdata.net)

Fax: (831) 373-4193

Company and product information is at [www.cyberdata.net](http://www.cyberdata.net).

---

## Revision Information

Revision 931649B, which corresponds to firmware version 20.0.0, was released on November 4, 2020, and has the following changes:

- Updates [Figure 1-1, "Model Number Label"](#)
- Updates [Table 1-1, "Specifications"](#)
- Updates [Section 1.3, "Product Features"](#)
- Updates [Section 1.4, "Supported Protocols"](#)
- Updates [Section 1.7, "Compliance"](#)

---


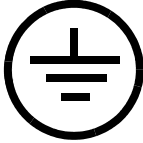
## Browsers Supported

The following browsers have been tested against firmware version 20.0.0:

- Internet Explorer (version: 11)
- Firefox (also called Mozilla Firefox) (version: 62.0)
- Chrome (version: 63.0.3239.132)
- Safari (version: 12)
- Microsoft Edge (version: 42.17134.1.0)

---

## Pictorial Alert Icons

	<p><b>General Alert</b></p> <p>This pictorial alert indicates a potentially hazardous situation. This alert will be followed by a hazard level heading and more specific information about the hazard.</p>
	<p><b>Ground</b></p> <p>This pictorial alert indicates the Earth grounding connection point.</p>

---

## Hazard Levels

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

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




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

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

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

# 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 InformaCast Enabled Outdoor RGB (Multi-Color) Strobe enclosure is not rated for any AC voltages!**

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

---

# Abbreviations and Terms

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

# Contents

---

<b>Chapter 1 Product Overview</b>	<b>1</b>
1.1 How to Identify This Product .....	1
1.2 Typical System Installation .....	2
1.3 Product Features .....	3
1.4 Supported Protocols .....	3
1.5 Supported SIP Servers .....	3
1.6 Specifications .....	4
1.7 Compliance .....	5
1.7.1 CE Statement .....	5
1.7.2 FCC Statement .....	5
1.7.3 Industry Canada (IC) Compliance Statement .....	5
 <b>Chapter 2 Installing the InformaCast Enabled Outdoor RGB (Multi-Color) Strobe</b>	 <b>6</b>
2.1 Parts List .....	6
2.2 InformaCast Enabled Outdoor RGB (Multi-Color) Strobe Setup .....	7
2.2.1 InformaCast Enabled Outdoor RGB (Multi-Color) Strobe Connections .....	7
2.2.2 Connecting the InformaCast Enabled Outdoor RGB (Multi-Color) Strobe to the On-Board Relay .....	9
2.2.3 Identifying the InformaCast Enabled Outdoor RGB (Multi-Color) Strobe Connectors and Jumpers .....	11
2.2.4 Activity and Link LEDs .....	15
2.2.5 Restoring the Factory Default Settings .....	16
2.3 Configure the InformaCast Enabled Outdoor RGB (Multi-Color) Strobe Parameters .....	17
2.3.1 Factory Default Settings .....	17
2.3.2 InformaCast Enabled Outdoor RGB (Multi-Color) Strobe Web Page Navigation .....	18
2.3.3 Using the Toggle Help Button .....	19
2.3.4 Log in to the Configuration Home Page .....	21
2.3.5 Configure the Device .....	25
2.3.6 Configure the Network Parameters .....	28
2.3.7 Configure the SIP (Session Initiation Protocol) Parameters .....	30
2.3.8 Configure the SSL Parameters .....	37
2.3.9 Configure the Multicast Parameters .....	42
2.3.10 Configure the Sensor Configuration Parameters .....	46
2.3.11 Configure the Audio Configuration Parameters .....	50
2.3.12 Configure the Events Parameters .....	53
2.3.13 Configure the Autoprovisioning Parameters .....	59
2.4 Upgrade the Firmware .....	70
2.5 Reboot the Device .....	73
2.6 Command Interface .....	74
2.6.1 Command Interface Post Commands .....	74
 <b>Appendix A Mounting the InformaCast Enabled Outdoor RGB (Multi-Color) Strobe</b>	 <b>75</b>
A.1 Mount the InformaCast Enabled Outdoor RGB (Multi-Color) Strobe .....	75
 <b>Appendix B Troubleshooting/Technical Support</b>	 <b>80</b>
B.1 Frequently Asked Questions (FAQ) .....	80
B.2 Documentation .....	80
B.3 Contact Information .....	81
B.4 Warranty and RMA Information .....	81

## Index

82



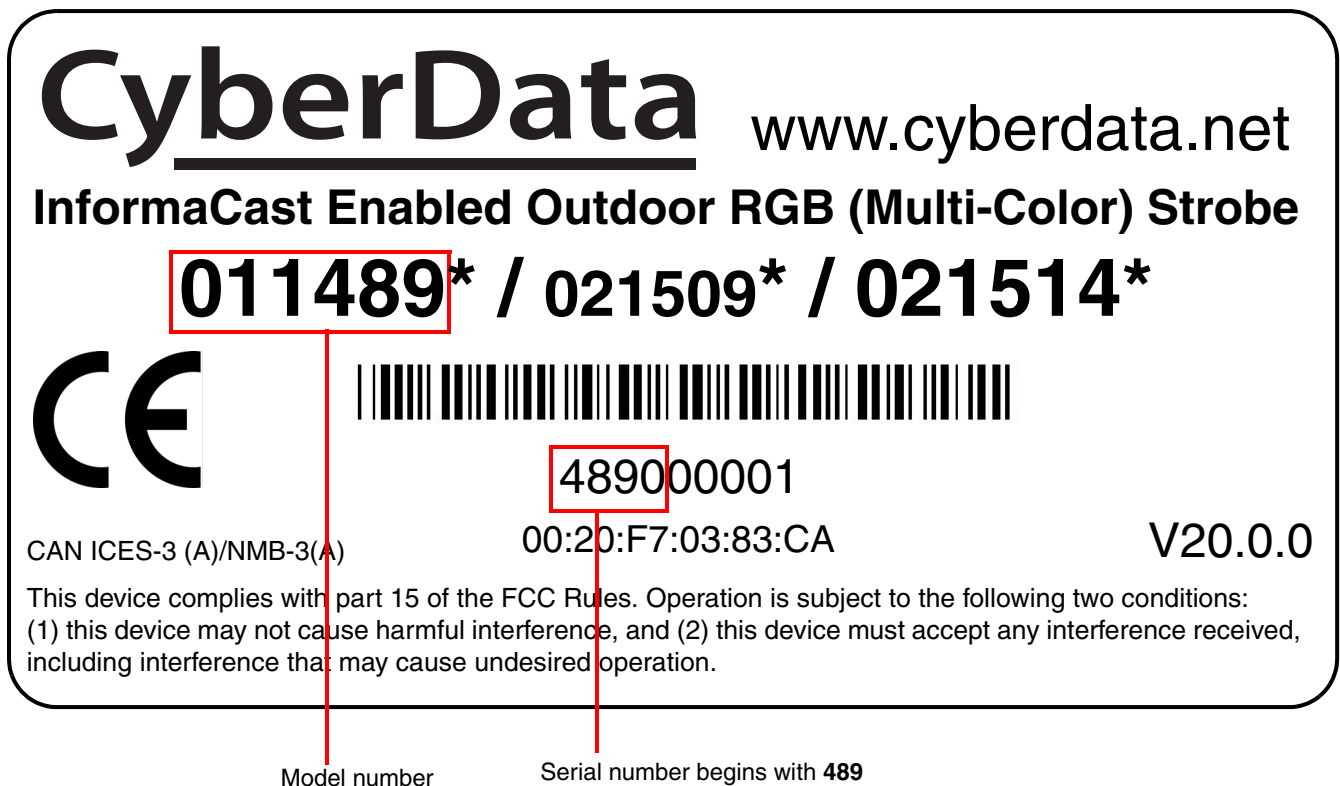
# 1 Product Overview

## 1.1 How to Identify This Product

To identify the InformaCast Enabled Outdoor RGB (Multi-Color) 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 **011489**.
- The serial number on the label should begin with **489**.

Figure 1-1. Model Number Label

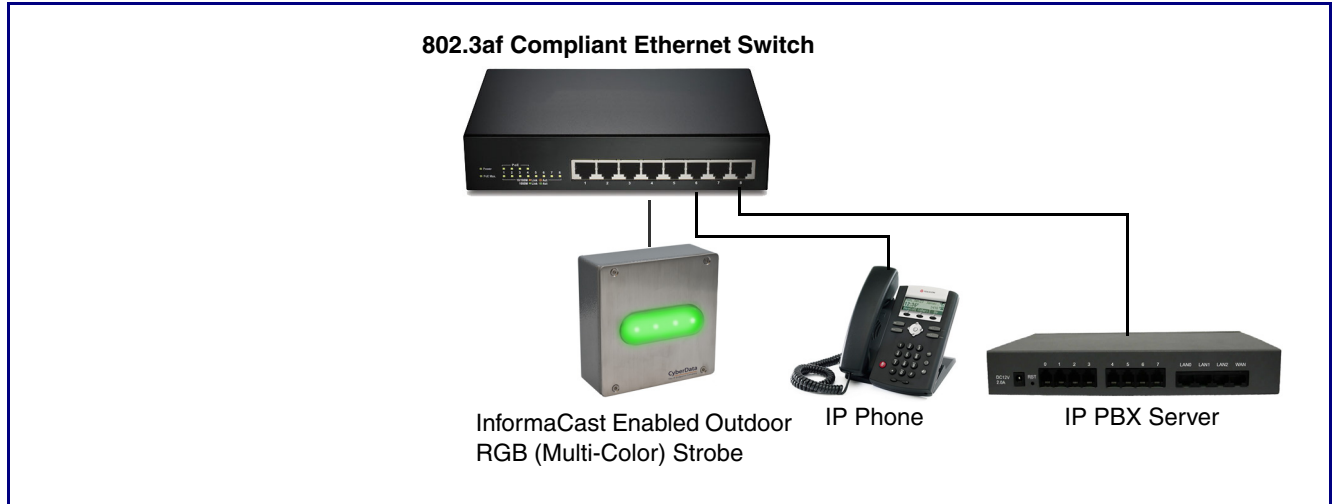


## 1.2 Typical System Installation

The InformaCast Enabled Outdoor RGB (Multi-Color) Strobe is a Session Initiation Protocol (SIP) endpoint designed to provide VoIP phone connectivity in a tamper proof and secure package.

Figure 1-2 illustrate how the InformaCast Enabled Outdoor RGB (Multi-Color) Strobes can be installed as part of a VoIP phone system.

**Figure 1-2. Typical Installation**



---

## 1.3 Product Features

- Compatible with Singlewire InformaCast v12.1, including support for downloading SIP credentials from InformaCast
- Compatible with Cisco Call Manager
- Meets ADA requirements for telephony signaling and notification
- SIP and multicast activation
- For each activation, the user can choose among multiple colors, blink rates, and brightness levels
- Event-controlled relay
- Tamper sensor
- Autoprovisioning via HTTPS, HTTP or TFTP
- Configurable event generation for device health and status monitoring
- 802.11q VLAN tagging
- HTTP Command Interface
- Support for Cisco SRST resiliency

---

## 1.4 Supported Protocols

The InformaCast Enabled Outdoor RGB (Multi-Color) Strobe supports:

- SIP
- Singlewire InformaCast
- Singlewire Failover
- HTTPS or HTTP web-based configuration. HTTPS is enabled by default.

Provides an intuitive user interface for easy system configuration and verification of InformaCast Enabled Outdoor RGB (Multi-Color) Strobe operations.

- DHCP Client  
Dynamically assigns IP addresses in addition to the option to use static addressing.
- RTP
- TLS 1.2

---

## 1.5 Supported SIP Servers

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

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

## 1.6 Specifications

**Table 1-1. Specifications**

Specifications	
Ethernet I/F	10/100 Mbps
Protocol	SIP RFC 3261 Compatible
Notification Software	Singlewire InformaCast v4.0 and above
Power Input	PoE 802.3af compliant or +8 to +12VDC @ 1000mA Regulated Power Supply (not included) <sup>a</sup>
Flash rate	5 user-defined scenes
LED MTBF	100,000 Hours
Brightness	366 Lux (white color)
On-Board Relay	1A at 30 VDC
Network Security	TLS/SSL 1.2
IP Rating	IP66
Operating Range	Temperature: -40° C to 55° C (-40° F to 131° F) Humidity: 5-95%, non-condensing
Storage Temperature	-40° C to 70° C (-40° F to 158° F)
Storage Altitude	Up to 15,000 ft. (4573 m)
Dimensions <sup>b</sup>	5.1 inches [129.5 mm] Length 2.9 inches [73.66 mm] Width 5.1 inches [129.5 mm] Height
Weight	2.0 lbs [0.90 kg]
Boxed Weight	3.0 lbs [1.35 kg]
Compliance	CE; EMC Directive – Class A EN 55032 & EN 55024, LV Safety Directive –EN 60950-1 and EN 62368-1, RoHS Compliant, FCC; Part 15 Class A, Industry Canada; ICES-3 Class A, IEEE 802.3 Compliant
Part Number	011489

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

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

---

## 1.7 Compliance

---

### 1.7.1 CE Statement



As of the date of manufacture, this equipment has been tested and found to comply with the specifications for CE marking and standards per EMC and Radiocommunications Compliance.

EMC Directive - Class A Emissions, Immunity, and LV Safety Directive, RoHS Compliant.  
Flammability rating on all components is 94V-0.

---

### 1.7.2 FCC Statement



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

**CAUTION:** Changes or modifications not expressly approved by the manufacturer responsible for compliance could void the user's authority to operate the equipment.

---

### 1.7.3 Industry Canada (IC) Compliance Statement

Operation is subject to the following two conditions:

1. This device may not cause interference, and
2. This device must accept any interference, including interference that may cause undesired operations of the device.




ICES-3 Class A

## 2 Installing the InformaCast Enabled Outdoor RGB (Multi-Color) Strobe

### 2.1 Parts List

Table 2-2 illustrates the InformaCast Enabled Outdoor RGB (Multi-Color) Strobe parts.

**Table 2-2. Parts List**

Quantity	Part Name	Illustration
1	InformaCast Enabled Outdoor RGB (Multi-Color) Strobe Assembly	
1	Installation Quick Reference Guide	
1	InformaCast Enabled Outdoor RGB (Multi-Color) Strobe Mounting Accessory Kit	

## 2.2 InformaCast Enabled Outdoor RGB (Multi-Color) Strobe Setup

### 2.2.1 InformaCast Enabled Outdoor RGB (Multi-Color) Strobe Connections

Figure 2-3 shows the pin connections on the terminal block. This terminal block can accept 16 AWG gauge wire.

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


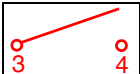
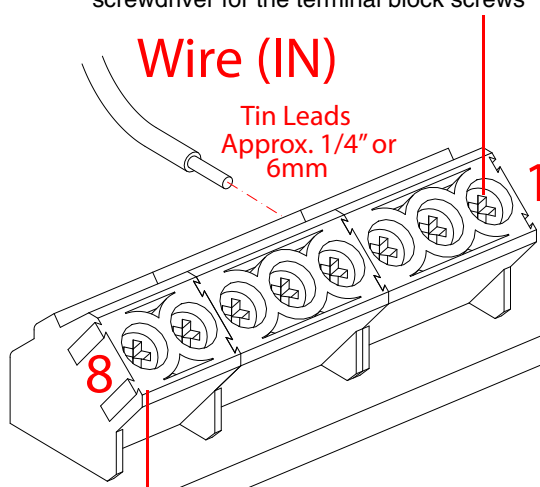
 <p>GENERAL ALERT</p>	<p><b>Caution</b></p> <p><i>Equipment Hazard:</i> Contacts 1 and 2 on the terminal block are only for powering the device from a non-PoE 12 VDC power source as an alternative to Network PoE power. Use of these contacts for any other purpose will damage the device and void the product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

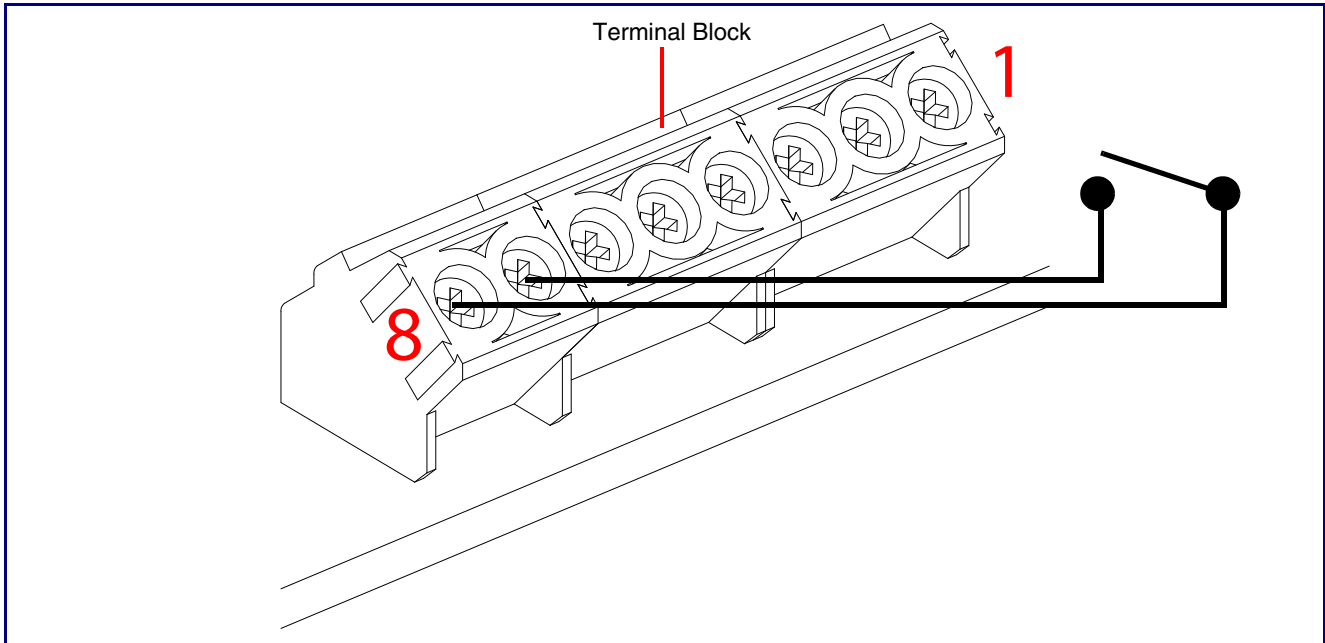
Figure 2-3. Connections and Alternate Power Input

<p>Alternate Power Input: 1 = +8 to +12VDC @ 1000mA Regulated Power Supply* 2 = Power Ground*</p>  <p>Relay Contact: (1 A at 30 VDC for continuous loads) 3 = Relay Common 4 = Relay Normally Open Contact 5 = Sense Input 6 = Sense Ground 7 = Remote Switch "A" 8 = Remote Switch "B"</p> <p>*Contacts 1 and 2 on the terminal block are only for powering the device from a non-PoE 12VDC power source as an alternative to Network PoE power. Use of these contacts for any other purpose will damage the device and void the product warranty.</p>	<p>Use a 3.17 mm (1/8-inch) flat blade screwdriver for the terminal block screws</p> <p><b>Wire (IN)</b></p> <p>Tin Leads Approx. 1/4" or 6mm</p>  <p>Terminal Block can accept 16 AWG wire</p>
--	--

### 2.2.1.1 Remote Switch Connection






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

**Figure 2-4. Remote Switch Connection**





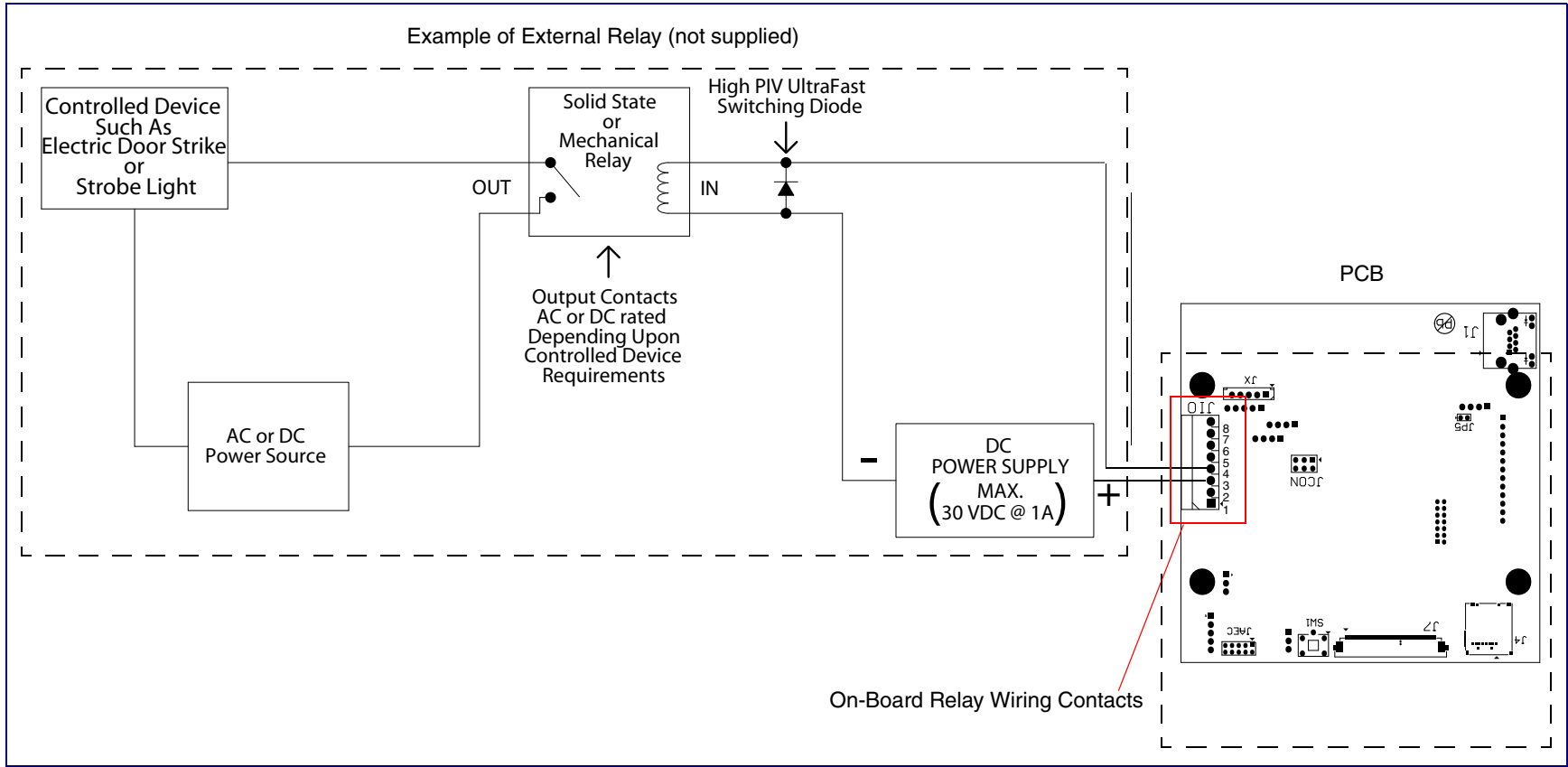
## 2.2.2 Connecting the InformaCast Enabled Outdoor RGB (Multi-Color) Strobe to the On-Board Relay

 GENERAL ALERT	<b>Warning</b> <i>Electrical Hazard:</i> The device enclosure is not rated for any AC voltages.
 GENERAL ALERT	<b>Warning</b> <i>Electrical Hazard:</i> This product should be installed by a licensed electrician according to all local electrical and building codes.
 GENERAL ALERT	<b>Warning</b> <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	<b>Warning</b> <i>Electrical Hazard:</i> The relay contacts are dry and provided for a normally open and momentarily closed configuration. Neither the alternate power input nor PoE power can be used to drive a door strike.
 GENERAL ALERT	<b>Warning</b> 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 2.2.3, "Identifying the InformaCast Enabled Outdoor RGB \(Multi-Color\) Strobe Connectors and Jumpers"](#)).

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.

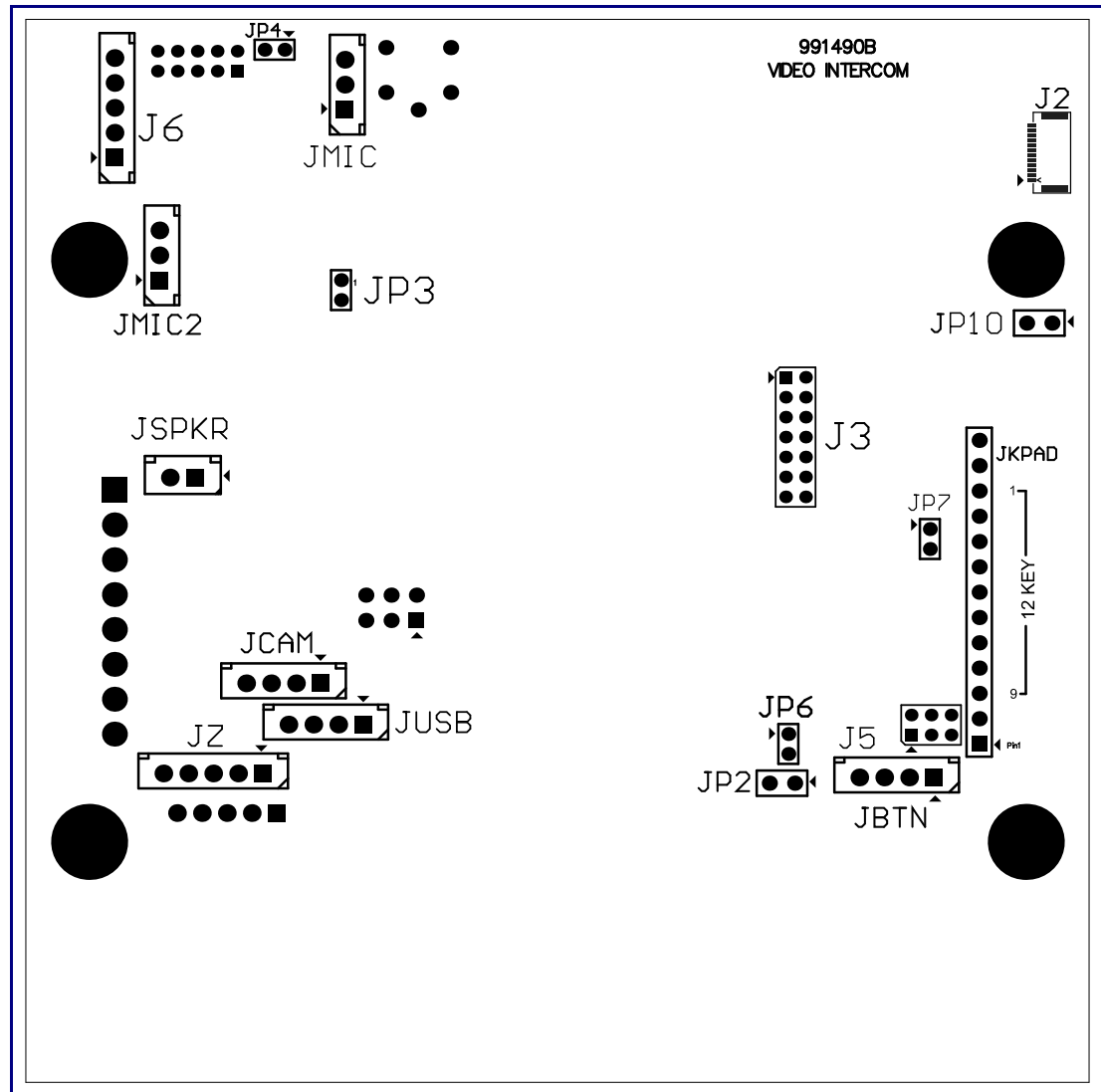
Figure 2-5. Wiring Diagram



## 2.2.3 Identifying the InformaCast Enabled Outdoor RGB (Multi-Color) Strobe Connectors and Jumpers

See the following figures and tables to identify the InformaCast Enabled Outdoor RGB (Multi-Color) Strobe connector locations and functions.

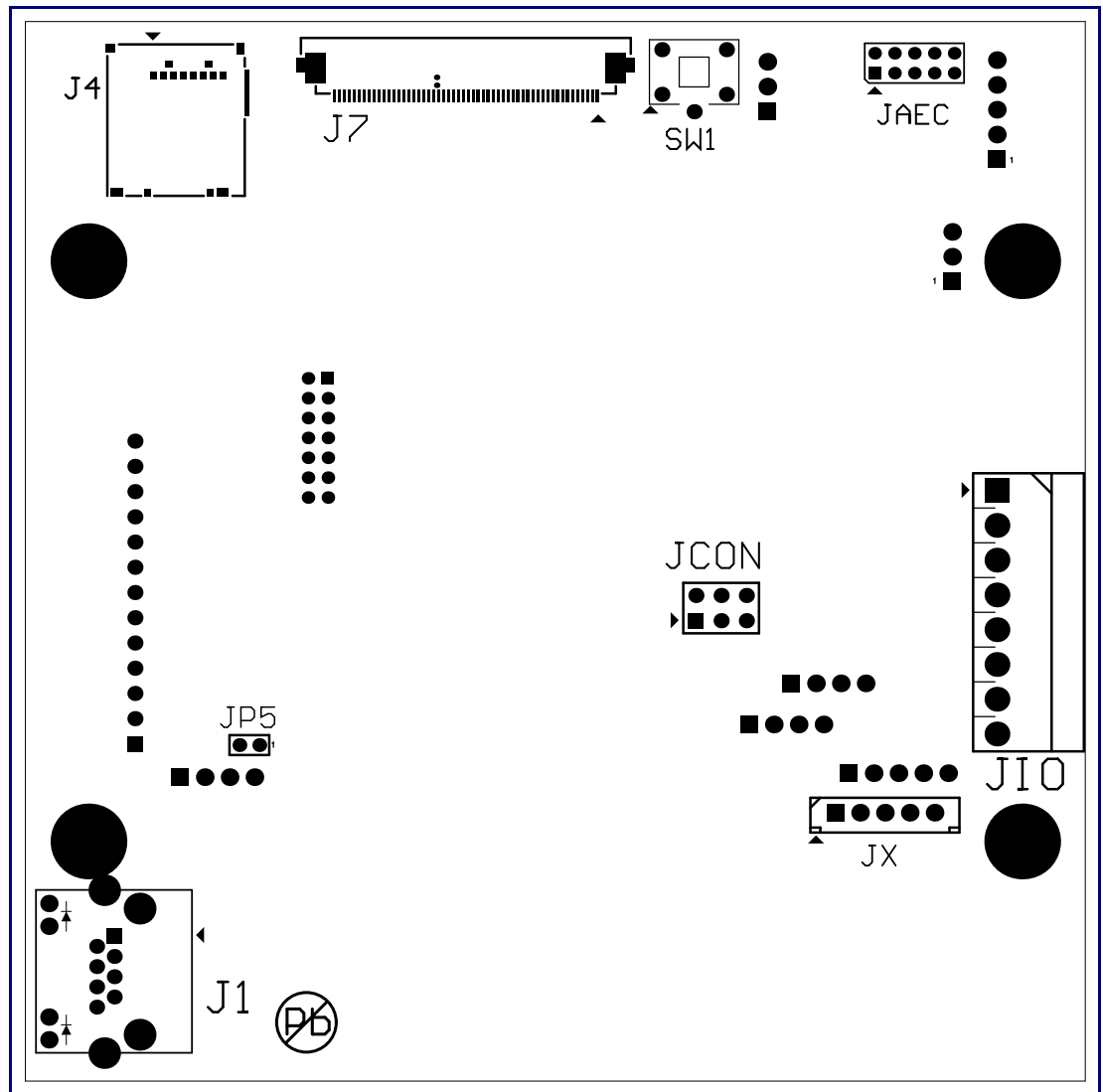
**Figure 2-6. Connector Locations—Board Top**



**Table 2-3. Connector Functions—Board Top**

Connector	Function
JBTN	Call Button LED Interface (Not Used)
JMIC	Microphone Interface (Not Used)
JMIC2	Second Microphone Interface (Not Used)
JSPKR	Speaker Interface (Not Used)
JKPAD	Keypad Interface (Not Used)
JUSB	USB Interface (Not Used)
JZ	I <sup>2</sup> C 5V Peripheral Bus
J2	Biometric Interface (Not Used)
J3	JTAG Interface (Not Used)
J5	ISP AT-Tiny Interface (Factory Only)
J6	Digital Microphone Interface (Not Used)
JP3	Mute Disable Jumper—Jumper should be removed
JP6	Enable AT-Tiny—Jumper should be installed
JP7	Enable Write to EEPROM (Factory Only)
JP10	Disables the intrusion sensor when installed.

**Figure 2-7. Connector Locations—Board Bottom**

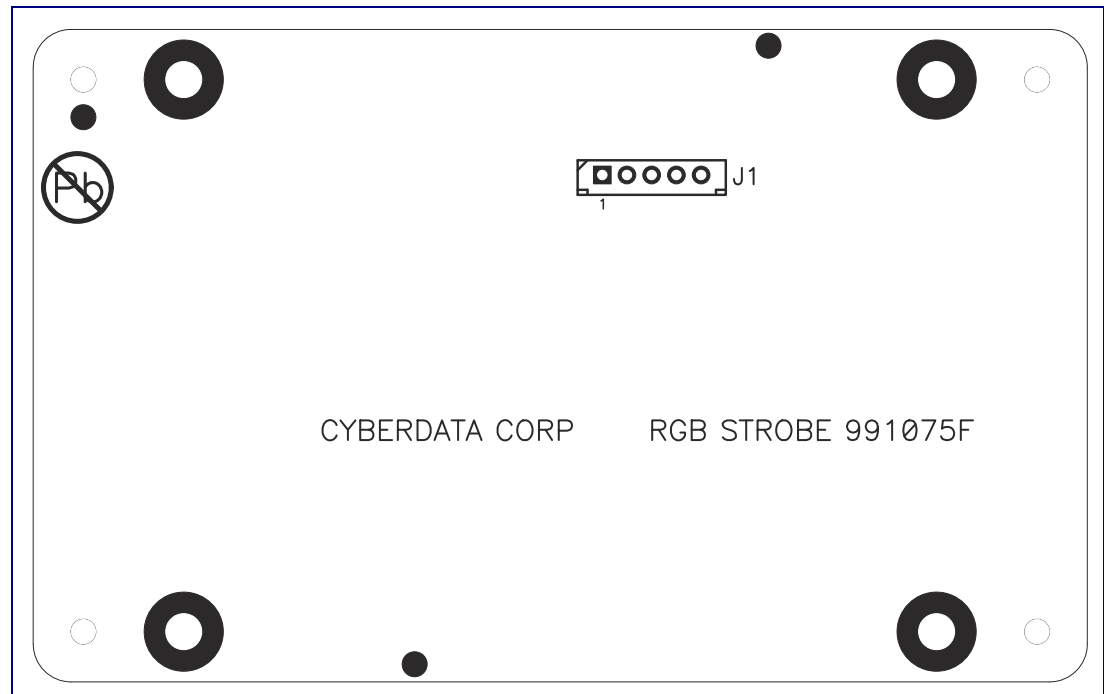


**Table 2-4. Connector Functions—Board Bottom**

Connector	Function
J1	PoE Network Connection (RJ-45 ethernet)
J4	SD Card Slot
JAEC	AEC Configuration Interface (Factory Use Only)
JCON	Console Port (Factory Use Only)
JIO	Terminal Block (see <a href="#">Figure 2-3</a> )
JP5	Reset jumper <sup>a</sup>
JX	Strobe Connector
SW1	See <a href="#">Section 2.2.5, "Restoring the Factory Default Settings"</a>

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

**Figure 2-8. Connector Locations for the 021509 Board**



**Table 2-5. Connector Functions**

Connector	Function
J1	Ethernet Connector

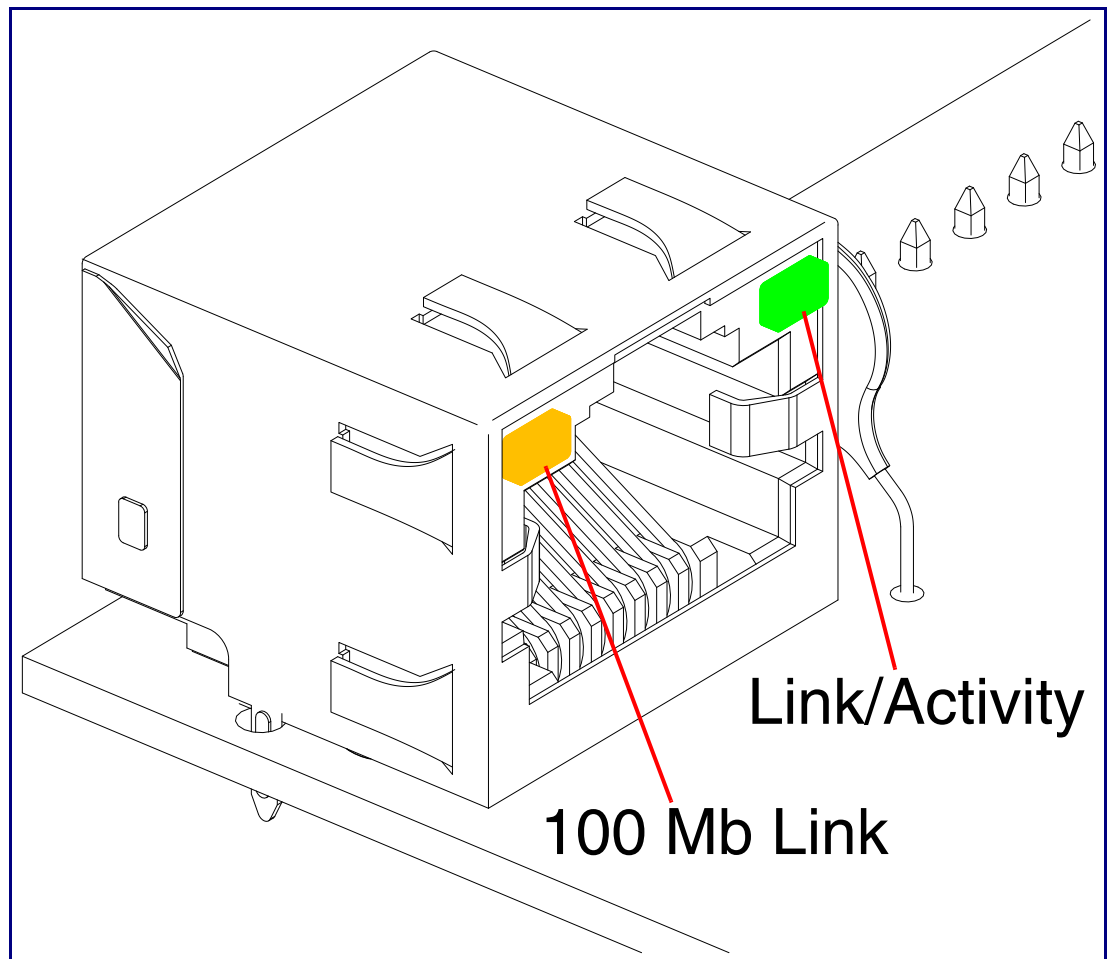
## 2.2.4 Activity and Link LEDs

### 2.2.4.1 Verifying the Network Connectivity and Data Rate

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

- The square, **GREEN Link/Activity** LED blinks when there is network activity (see [Figure 2-9](#)).
- The square, **AMBER 100 Mb Link** LED above the Ethernet port indicates that the network 100 Mb connection has been established (see [Figure 2-9](#)).

**Figure 2-9. Activity and Link LED**



## 2.2.5 Restoring the Factory Default Settings

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

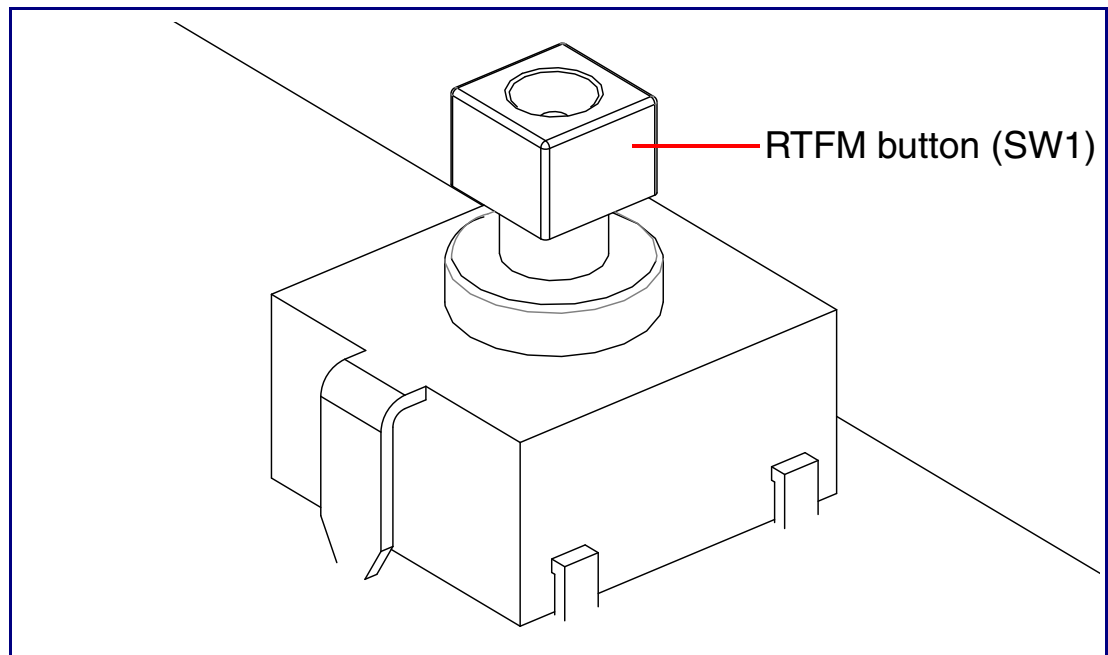
**Note** Each InformaCast Enabled Outdoor RGB (Multi-Color) Strobe is delivered with factory set default values.

To restore the factory default settings:

1. Press and hold the **RTFM button** (see **SW1** in [Figure 2-10](#)) for more than five seconds.

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

**Figure 2-10. RTFM Button (SW1)**





---

## 2.3 Configure the InformaCast Enabled Outdoor RGB (Multi-Color) Strobe Parameters

To configure the InformaCast Enabled Outdoor RGB (Multi-Color) Strobe online, use a standard web browser.

Configure each InformaCast Enabled Outdoor RGB (Multi-Color) Strobe and verify its operation *before* you mount it. When you are ready to mount an InformaCast Enabled Outdoor RGB (Multi-Color) Strobe, refer to [Appendix A, "Mounting the InformaCast Enabled Outdoor RGB \(Multi-Color\) Strobe"](#) for instructions.

---

### 2.3.1 Factory Default Settings

All InformaCast Enabled Outdoor RGB (Multi-Color) Strobes are initially configured with the following default IP settings:

When configuring more than one InformaCast Enabled Outdoor RGB (Multi-Color) Strobe, attach the InformaCast Enabled Outdoor RGB (Multi-Color) Strobes to the network and configure one at a time to avoid IP address conflicts.

**Table 2-6. Factory Default Settings**

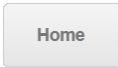





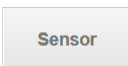
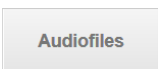
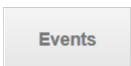
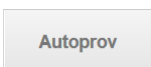
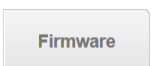
Parameter	Factory Default Setting
IP Addressing	DHCP
IP Address <sup>a</sup>	10.10.10.10
Web Access Username	admin
Web Access Password	admin
Subnet Mask <sup>a</sup>	255.0.0.0
Default Gateway <sup>a</sup>	10.0.0.1

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

## 2.3.2 InformaCast Enabled Outdoor RGB (Multi-Color) Strobe Web Page Navigation

[Table 2-7](#) shows the navigation buttons that you will see on every InformaCast Enabled Outdoor RGB (Multi-Color) Strobe web page.

**Table 2-7. Web Page Navigation**

Web Page Item	Description
	Link to the <b>Home</b> page.
	Link to the <b>Device</b> page.
	Link to the <b>Network</b> page.
	Link to go to the <b>SIP</b> page.
	Link to the <b>SSL</b> page.
	Link to the <b>Multicast</b> page.
	Link to the <b>Sensor</b> page.
	Link to the <b>Audiofiles</b> page.
	Link to the <b>Events</b> page.
	Link to the <b>Autoprovisioning</b> page.
	Link to the <b>Firmware</b> page.

### 2.3.3 Using the Toggle Help Button

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

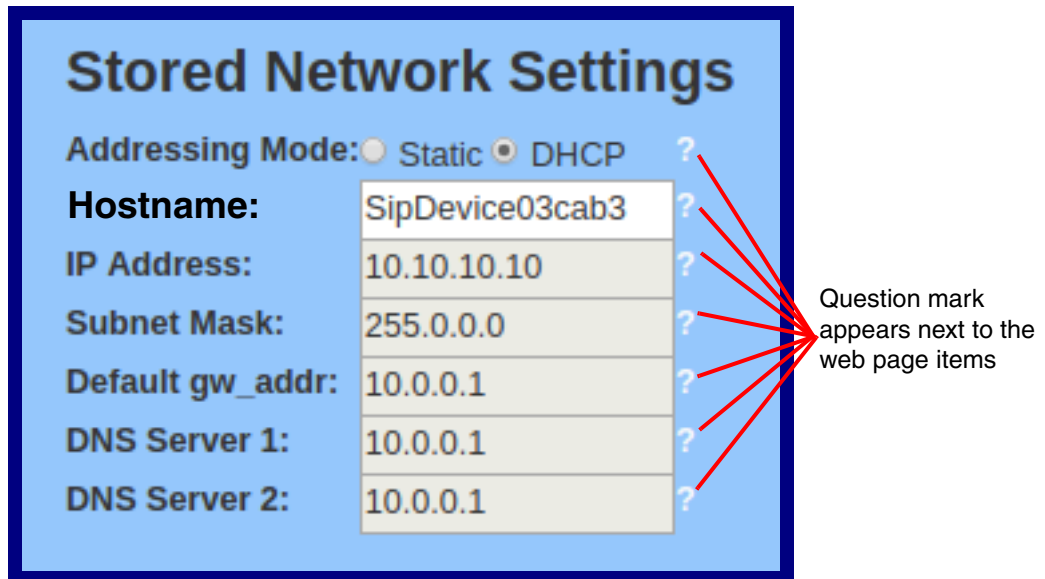
1. Click on the **Toggle Help** button that is on the UI webpage. See [Figure 2-11](#) and [Figure 2-12](#).

**Figure 2-11. Toggle/Help Button**



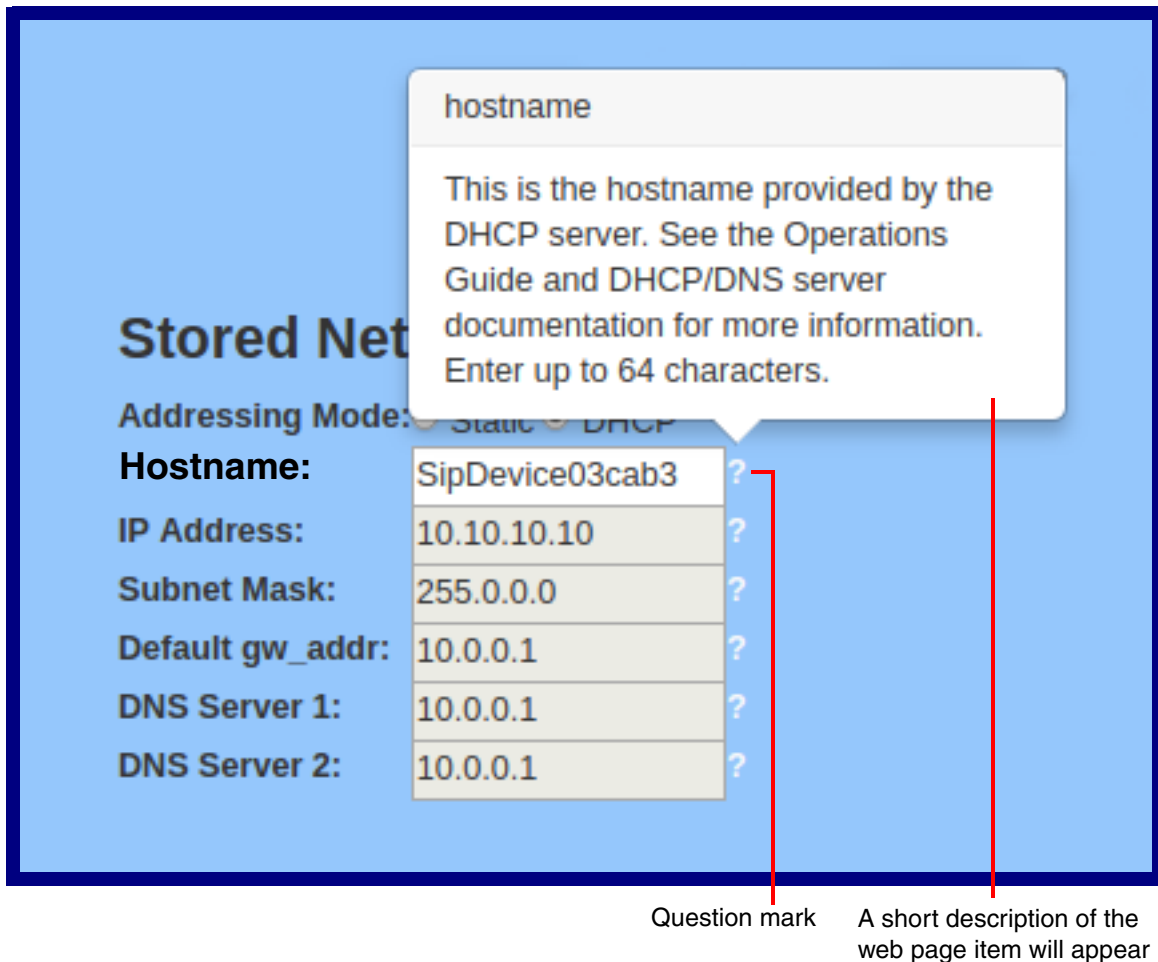
2. You will see a question mark (?) appear next to each web page item that has been provided with a short description by the Help feature. See [Figure 2-12](#).

**Figure 2-12. Toggle Help Button and Question Marks**



3. Move the mouse pointer to hover over the question mark (?), and a short description of the web page item will appear. See [Figure 2-13](#).

**Figure 2-13. Short Description Provided by the Help Feature**



---

## 2.3.4 Log in to the Configuration Home Page

1. Open your browser to the InformaCast Enabled Outdoor RGB (Multi-Color) 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 InformaCast Enabled Outdoor RGB (Multi-Color) 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:

<https://www.cyberdata.net/pages/discovery>

**Note** The Intercom 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 2-14):

Web Access Username: **admin**

Web Access Password: **admin**

Figure 2-14. Home Page

HomeDeviceNetworkSIPSSLMulticastSensorAudiofilesEventsAutoprovFirmware

Singlewire Multicolor Strobe

Current Status

Serial Number:489000001  
Mac Address:00:20:f7:04:04:8a  
Firmware Version:v20.0.0  
Partition 2:v20.0.0  
Partition 3:v20.0.0  
Bootling From:partition 2  

Boot From Other Partition

  
IP Addressing:DHCP  
IP Address:10.10.1.106  
Subnet Mask:255.0.0.0  
Default Gateway:10.0.0.1  
DNS Server 1:10.0.1.56  
DNS Server 2:  
  
SIP Mode:Enabled  
Multicast Mode:Disabled  
Event Reporting:Disabled  
Nightringer:Disabled  
  
Primary SIP Server:**Not registered**  
Backup Server 1:Not registered  
Backup Server 2:Not registered  
Nightringer Server:Not registered  
  
Intrusion Sensor:Inactive

Admin Settings

Username:admin  
Password:\*\*\*\*\*  
Confirm Password:\*\*\*\*\*  

Save

Reboot

Toggle Help

Import Settings

Browse...

No file chosen  

Import Config

Export Settings

Export Config

Operations Guide


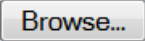

931649B

CyberData Corporation





3. On the **Home** page, review the setup details and navigation buttons described in [Table 2-8](#).

**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 2-8. Home Page Overview**

Web Page Item	Description
<b>Admin Settings</b>	
Username ?	The username to access the web interface. Enter up to 25 characters.
Password ?	The password to access the web interface. Enter up to 25 characters.
Confirm Password ?	Confirm the web interface password.
<b>Current Status</b>	
Serial Number	Shows the device serial number.
Mac Address	Shows the device Mac address.
Firmware Version	Shows the current firmware version.
Partition 2	Contains a complete copy of bootable software.
Partition 3	Contains an alternate, complete copy of bootable software.
Bootting From	Indicates the partition currently used for boot.
	Allows the user to boot from the alternate partition.
IP Addressing	Shows the current IP addressing setting ( <b>DHCP</b> or <b>static</b> ).
IP Address	Shows the current IP address.
Subnet Mask	Shows the current subnet mask address.
Default Gateway	Shows the current default gateway address.
DNS Server 1	Shows the current DNS Server 1 address.
DNS Server 2	Shows the current DNS Server 2 address.
SIP Mode	Shows the current status of the SIP mode.
Multicast Mode	Shows the current status of the Multicast mode.
Event Reporting	Shows the current status of the Event Reporting mode.
Nightringer	Shows the current status of the Nightringer mode.
Primary SIP Server	Shows the current status of the Primary SIP Server.
Backup Server 1	Shows the current status of Backup Server 1.
Backup Server 2	Shows the current status of Backup Server 2.
Nightringer Server	Shows the current status of Nightringer Server.
Intrusion Sensor	Shows the current status of the intrusion sensor when the Home Page is refreshed.
<b>Import Settings</b>	
	Use this button to select a configuration file to import.
	After selecting a configuration file, click Import to import the configuration from the selected file.

**Table 2-8. Home Page Overview (continued)**

Web Page Item	Description
<b>Export Settings</b>	
	Click Export to export the current configuration to a file.
	Click the <b>Save</b> button to save your configuration settings.
	Click on the <b>Reboot</b> button to reboot the system.
	Click on the <b>Toggle Help</b> button to see a short description of some of the web page items. First click on the <b>Toggle Help</b> button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.



## 2.3.5 Configure the Device

1. Click the **Device** menu button to open the **Device** page. See [Figure 2-15](#).

**Figure 2-15. Device Configuration Page**

Home
Device
Network
SIP
SSL
Multicast
Sensor
Audiofiles
Events
Autoprov
Firmware

# Singlewire Multicolor Strobe

### Clock Settings

Enable NTP: ☒

NTP Server:

Timezone:

Current Time: Sun, 10 Mar 2019 10:59:00

### Misc Settings

Device Name:

Disable HTTPS (NOT recommended): ☐

### InformaCast Settings

InformaCast Address:

### Relay Settings

Activate Relay During Ring: ☐

Activate Relay During Night Ring: ☐

Activate Relay on InformaCast: ☐

### InformaCast Strobe Settings

Priority	Scene	Brightness	Color	Red	Green	Blue	
1	ADA	255	Color	255	255	255	Preview
2	Fast Blink	255	Color	255	255	255	Preview
3	Fast Fade	180	White			0	Preview
4	Slow Blink	25	Yellow			60	Preview
5	Off	255	Orange			255	Preview
6	Fast Fade	75	Red			0	Preview
7	Slow Fade	120	Pink			100	Preview
8	Slow Blink	140	Purple			128	Preview
9	Fast Blink	255	Blue			0	Preview
10	Slow Fade	40	Teal			0	Preview
			Green			0	Preview
			Lime			0	Preview

Save
Reboot
Toggle Help

Test Relay





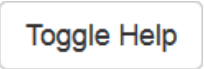
2. On the **Device** page, you may enter values for the parameters indicated in [Table 2-9](#).

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

**Table 2-9. Device Configuration Parameters**

Web Page Item	Description
<b>Clock Settings</b>	
Enable NTP ?	Sync device's local time with the specified NTP Server.
NTP Server ?	Use this field to set the address (in IPv4 dotted decimal notation or as a canonical name) for the NTP Server. This field can accept canonical names of up to 64 characters in length.
Timezone	Enter the tz database string of your timezone.  Examples: America/Los_Angeles America/New_York Europe/London America/Toronto  See <a href="https://en.wikipedia.org/wiki/List_of_tz_database_time_zones">https://en.wikipedia.org/wiki/List_of_tz_database_time_zones</a> for a full list of valid strings.
Current Time	Displays the current time.
<b>InformaCast Settings</b>	
InformaCast Address ?	Use this field to set the address of your InformaCast server. This will override any InformaCast server addresses received via SLP or DHCP.  If using TFTP for configuration, simply enter an IP address (eg. 10.0.1.195) If using HTTP for configuration, enter the full URL to the path that contains the configuration file.  Do not input the file name (e.g.http://10.0.1.195:8081/InformaCast/resources/).If the HTTP protocol is not specified with <b>http://</b> , then TFTP will be used.
<b>Misc Settings</b>	
Device Name ?	Type the device name. Enter up to 25 characters.
Disable HTTPS (NOT recommended) ?	Disables the encrypted connection to the webpage. We do not recommend disabling HTTPS for security reasons.  <b>Note</b> This setting requires a reboot for the changes to take effect.
<b>Relay Settings</b>	
Activate Relay During Ring ?	When selected, the relay will be activated for as long as the device is ringing.
Activate Relay During Night Ring ?	When selected, the relay will be activated as long as the Nightringer extension is ringing.

Table 2-9. Device Configuration Parameters (continued)

Web Page Item	Description
<b>Singlewire Broadcast Strobe Settings</b>	For up to 10 Singlewire pages, when a priority is specified for the page, a corresponding strobe scene will be activated. The color may be selected from the drop down menu, or customized by the user with the 0-255 scale. Brightness is specified with a value between 0 and 255.  <b>The following strobe settings will only appear if a CyberData Strobe product is connected to your device. If a CyberData Strobe product is not connected to your device, you will not see the strobe settings.</b>
Priority ?	Indicates the priority of the Singlewire broadcast, with 1 the highest priority and 10 the lowest.
Scene ?	Use this section to select the strobe flashing behavior for the Singlewire Broadcast.
ADA Compliant ?	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.
Slow Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink ?	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.
Fast Blink ?	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.
Color ?	Select the desired color (only one may be chosen).
Brightness ?	How bright the strobe will blink when there is a Singlewire Broadcast. This is the maximum brightness for “fade” type scenes.
Red ?	The red LED value for the Singlewire Broadcast.
Green ?	The green LED value for the Singlewire Broadcast.
Blue ?	The blue LED value for the Singlewire Broadcast.
	Use this button to preview the strobe flashing behavior for the <b>Sensor Strobe Settings</b> .
	Click on the <b>Test Relay</b> button to do a relay test.
	Click the <b>Save</b> button to save your configuration settings.
	Click on the <b>Reboot</b> button to reboot the system.
	Click on the <b>Toggle Help</b> button to see a short description of some of the web page items. First click on the <b>Toggle Help</b> button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

## 2.3.6 Configure the Network Parameters

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

Figure 2-16. Network Configuration Page

Home Device Network SIP SSL Multicast Sensor Audiofiles Events Autopro Firmware

# Singlewire Multicolor Strobe

### Stored Network Settings

Addressing Mode: ☐ Static ☒ DHCP

Hostname: SipDevice04048a

IP Address: 10.10.10.10

Subnet Mask: 255.0.0.0

Default Gateway: 10.0.0.1

DNS Server 1: 10.0.0.1

DNS Server 2: 10.0.0.1

### VLAN Settings

VLAN ID (0-4095): 0

VLAN Priority (0-7): 0

### Current Network Settings

IP Address: 10.10.1.106

Subnet Mask: 255.0.0.0

Default Gateway: 10.0.0.1

DNS Server 1: 10.0.1.56




DNS Server 2:

Save Reboot Toggle Help

2. On the **Network** page, enter values for the parameters indicated in [Table 2-10](#).

**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 2-10. Network Configuration Parameters**

Web Page Item	Description
<b>Stored Network Settings</b>	
Addressing Mode ?	Select either DHCP IP Addressing or Static Addressing by marking the appropriate radio button. DHCP Addressing mode is enabled on default and the device will attempt to resolve network addressing with the local DHCP server upon boot. If DHCP Addressing fails, the device will revert to the last known IP address or the factory default address if no prior DHCP lease was established. See <a href="#">Section 2.3.1, "Factory Default Settings"</a> for factory default settings. Be sure to click <b>Save</b> and <b>Reboot</b> to store changes when configuring a Static address.
Hostname ?	This is the hostname provided by the DHCP server. See the DHCP/DNS server documentation for more information. Enter up to 64 characters.
IP Address ?	Enter the Static IPv4 network address in dotted decimal notation.
Subnet Mask ?	Enter the Subnet Mask in dotted decimal notation.
Default Gateway ?	Enter the Default Gateway IPv4 address in dotted decimal notation.
DNS Server 1 ?	Enter the primary DNS Server IPv4 address in dotted decimal notation.
DNS Server 2 ?	Enter the secondary DNS Server IPv4 address in dotted decimal notation.
<b>Current Network Settings</b>	
IP Address	Shows the current Static IP address.
Subnet Mask	Shows the current Subnet Mask address.
Default Gateway	Shows the current Default Gateway address.
DNS Server 1	Shows the current DNS Server 1 address.
DNS Server 2	Shows the current DNS Server 2 address.
<b>VLAN Settings</b>	
VLAN ID (0-4095) ?	Specify the IEEE 802.1Q VLAN ID number. Enter up to 4 digits. A value of 0 disables vlan. <b>Note:</b> The device supports 802.1Q VLAN tagging support. The switch port connected to the device will need to be in "trunking mode" for the VLAN tags to propagate.
VLAN Priority (0-7) ?	Specify the IEEE 802.1p VLAN priority level. Enter 1 digit. A value of 0 may cause the VLAN ID tag to be ignored.
	Click the <b>Save</b> button to save your configuration settings.
	Click on the <b>Reboot</b> button to reboot the system.
	Click on the <b>Toggle Help</b> button to see a short description of some of the web page items. First click on the <b>Toggle Help</b> button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

## 2.3.7 Configure the SIP (Session Initiation Protocol) Parameters

1. Click on the **SIP** menu button to open the **SIP** page (Figure 2-17).

Figure 2-17. SIP Configuration Page

**SIP Settings**

Enable SIP operation: ☒  
 Register with a SIP Server: ☒  
 Primary SIP Server: 10.0.0.253  
 Primary SIP User ID: 199  
 Primary SIP Auth ID: 199  
 Primary SIP Auth Password: \*\*\*\*\*  
 Re-registration Interval (in seconds): 360

Backup SIP Server 1:  
 Backup SIP User ID:  
 Backup SIP Auth ID:  
 Backup SIP Auth Password:  
 Re-registration Interval (in seconds): 360

Backup SIP Server 2:  
 Backup SIP User ID:  
 Backup SIP Auth ID:  
 Backup SIP Auth Password:  
 Re-registration Interval (in seconds): 360

Remote SIP Port: 5060  
 Local SIP Port: 5060

SIP Transport Protocol: UDP  
 TLS Version: 1.2 only (recommended)  
 Verify Server Certificate: ☐

Outbound Proxy:  
 Outbound Proxy Port: 0

Use Cisco SRST: ☐  
 Disable rport Discovery: ☐  
 Unregister on Boot: ☐  
 Keep Alive Period: 10000

**Nightringer Settings**

SIP Server:  
 SIP User ID:  
 SIP Auth ID:  
 SIP Auth Password:  
 Re-registration Interval (in seconds): 360

**SIP Ring Strobe Settings**

Blink Strobe on Ring: ☐  
 Scene BrightnessColor Red Green Blue  
 ADA 255 Color 255 255 255 Preview

**SIP Call Strobe Settings**

Blink Strobe during Call: ☐  
 Scene BrightnessColor Red Green Blue  
 ADA 255 Color 255 255 255 Preview

**MWI Strobe Settings**

Blink Strobe on MWI: ☐  
 Scene BrightnessColor Red Green Blue  
 ADA 255 Color 255 255 255 Preview

**Nightringer Strobe Settings**

Blink Strobe on Nightring: ☐  
 Scene BrightnessColor Red Green Blue  
 ADA 255 Color 255 255 255 Preview

**Call Disconnection**

Terminate Call after delay: 0

**Audio Codec Selection**

Codec: Auto Select

**RTP Settings**

RTP Port (even): 10500  
 Jitter Buffer: 50

Save Reboot Toggle Help

2. On the **SIP** page, enter values for the parameters indicated in [Table 2-11](#).

**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 2-11. SIP Configuration Parameters**

Web Page Item	Description
<b>SIP Settings</b>	
Enable SIP Operation ?	When enabled, the device will transmit, receive, and process SIP messages according to the configured SIP settings below.
Register with a SIP Server ?	When enabled, the device will attempt to register to the configured SIP Server(s) on this page. To configure the device to send and receive point-to-point SIP calls, enable <b>SIP Operation</b> and disable <b>Register with a SIP Server</b> (see <a href="#">Section 2.3.7.1, "Point-to-Point Configuration"</a> ).
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.
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.
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 ?	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 ?	Specify the Authenticate Password for the first backup 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.
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 ?	Specify the SIP User ID for the second backup SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the second backup SIP server. Enter up to 64 alphanumeric characters.
Backup SIP Auth ID ?	Specify the Authenticate ID for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.




**Table 2-11. SIP Configuration Parameters (continued)**



Web Page Item	Description
Backup SIP Auth Password ?	Specify the Authenticate Password for the second backup 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.
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.
SIP Transport Protocol ?	Choose the transport protocol for SIP signaling. This will affect all extensions, including the Nightringer. Default is UDP.
TLS Version ?	Choose the TLS version for SIP over TLS. Modern security standards strongly recommend using TLS 1.2.
Verify Server Certificate ?	When enabled, the device will verify the authenticity of the server during the TLS handshake by its certificate and common name. The TLS handshake will be aborted if the server is deemed to be inauthentic and SIP registration will not proceed.
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.
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.
Disable rport Discovery ?	Disabling rport Discovery will prevent the device from including the public WAN IP address and port number in the contact information that is sent to the remote SIP servers. This will generally only need to be enabled when using an SBC or SIP ALG in conjunction with a remote SIP server.
Unregister on Boot ?	When enabled, the device will send one registration with an expiry of 0 on boot.
Keep Alive Period ?	The minimum time in milliseconds between keep-alive packets sent for nat traversal. A value of 0 will disable keep alive packets.
<b>Nightringer Settings</b>	
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.
SIP 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.
SIP Auth ID ?	Specify the Authenticate ID for the SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.







**Table 2-11. SIP Configuration Parameters (continued)**

Web Page Item	Description
SIP Auth Password ?	Specify the Authenticate Password for the SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Re-registration Interval (in seconds) ?	The SIP Re-registration Interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
<b>SIP Ring Strobe Settings</b>	
Blink Strobe on Ring ?	When selected, the Strobe will blink a scene when ringing.
Scene ?	Select desired scene (only one may be chosen).
ADA Compliant ?	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.
Slow Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink ?	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.
Fast Blink ?	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.
Color ?	Select desired color (only one may be chosen).
Brightness ?	How bright the strobe will blink when there is a SIP Ring. This is the maximum brightness for “fade” type scenes.
Red ?	The red LED value for SIP Ring.
Green ?	The green LED value for SIP Ring.
Blue ?	The blue LED value for SIP Ring.
	Use this button to preview the strobe flashing behavior for the <b>SIP Ring Strobe Settings</b> .
<b>SIP Call Strobe Settings</b>	
Blink Strobe during Call ?	When selected, the Strobe will blink a scene during a call.
Scene ?	Select desired scene (only one may be chosen).
ADA Compliant ?	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.
Slow Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink ?	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.
Fast Blink ?	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.
Color ?	Select desired color (only one may be chosen).
Brightness ?	How bright the strobe will blink when there is a SIP Call. This is the maximum brightness for “fade” type scenes.

**Table 2-11. SIP Configuration Parameters (continued)**

Web Page Item	Description
Red ?	The red LED value for SIP Call.
Green ?	The green LED value for SIP Call.
Blue ?	The blue LED value for SIP Call.
	Use this button to preview the strobe flashing behavior for the <b>SIP Call Strobe Settings</b> .
<b>MWI Strobe Settings</b>	
Blink Strobe on MWI ?	When selected, the strobe will blink a scene when a voicemail is waiting for its extension.
Scene ?	Select desired scene (only one may be chosen).
ADA Compliant ?	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.
Slow Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink ?	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.
Fast Blink ?	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.
MWI Call Color ?	Select desired color (only one may be chosen).
Brightness ?	How bright the strobe will blink when there is a message waiting. This is the maximum brightness for “fade” type scenes.
Red ?	The red LED value for MWI.
Green ?	The green LED value for MWI.
Blue ?	The blue LED value for MWI.
	Use this button to preview the strobe flashing behavior for the <b>MWI Strobe Settings</b> .
<b>Nightringer Strobe Settings</b>	
Blink Strobe on Nightring ?	When selected, the Strobe will blink a scene when the Nightringer is ringing.
Scene ?	Select desired scene (only one may be chosen).
ADA Compliant ?	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.
Slow Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink ?	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.
Fast Blink ?	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.

**Table 2-11. SIP Configuration Parameters (continued)**

Web Page Item	Description
Color ?	Select desired color (only one may be chosen).
Brightness ?	How bright the strobe will blink when the Nightringer is ringing. This is the maximum brightness for “fade” type scenes.
Red ?	The red LED value for Nightringer.
Green ?	The green LED value for Nightringer.
Blue ?	The blue LED value for Nightringer.
	Use this button to preview the strobe flashing behavior for the <b>Nightringer Strobe Settings</b> .
<b>Call Disconnection</b>	
Terminate Call After Delay ?	Automatically terminate an active call after a given delay in seconds. A value of 0 will disable this function. Enter up to 8 digits.
<b>Audio Codec Selection</b>	
Codec ?	Select the desired codec (only one may be chosen).
<b>RTP Settings</b>	
RTP Port (even) ?	Specify the port number used for the RTP stream after establishing a SIP call. This port number must be an even number and defaults to 10500. The supported range is 0-65536. Enter up to 5 digits.
Jitter Buffer ?	Specify the size of the jitter buffer (in milliseconds) used for SIP calls. Valid values are 50-1000.
	Click the <b>Save</b> button to save your configuration settings.
	Click on the <b>Reboot</b> button to reboot the system.
	Click on the <b>Toggle Help</b> button to see a short description of some of the web page items. First click on the <b>Toggle Help</b> button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

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

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

### 2.3.7.1 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**

The screenshot shows the 'SIP' configuration page for a 'Singlewire Multicolor Strobe'. The page has a navigation bar at the top with tabs: Home, Device, Network, SIP, SSL, Multicast, Sensor, Audiofiles, Events, Autopro, and Firmware. The main title is 'Singlewire Multicolor Strobe'. Below the title, there are two sections: 'SIP Settings' and 'Nightringer Settings'. In the 'SIP Settings' section, the 'Enable SIP operation:' checkbox is checked. The 'Register with a SIP Server:' checkbox is unchecked, which is highlighted by a red arrow. Below this, there are input fields for 'Primary SIP Server' (0.0.0.253), 'Primary SIP User ID' (99), 'Primary SIP Auth ID' (99), 'Primary SIP Auth Password' (masked with asterisks), and 'Re-registration Interval (in seconds):' (60). The 'Nightringer Settings' section includes input fields for 'SIP Server', 'SIP User ID', 'SIP Auth ID', 'SIP Auth Password', and 'Re-registration Interval (in seconds):' (360).

Device is set to NOT register with a SIP server

## 2.3.8 Configure the SSL Parameters

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

Figure 2-19. SSL Configuration Page

**Singlewire Multicolor Strobe**

**Server CAs**

Browse... No file chosen

Import CA Certificate

Restore Defaults Remove All

Toggle Help

**Client Certificate**

```

subject=
countryName      = US
stateOrProvinceName = California
localityName     = Monterey
organizationName  = Cyberdata
commonName       = Cyberdata_Dev
notBefore=Mar 22 16:50:02 2017 GMT
notAfter=Mar 20 16:50:02 2027 GMT
  
```

Client CA

**Test SSL Connection**

Server: 10.0.0.253

Port: 5060

Test TLS Connection

**List of Trusted CAs**

1	CyberData_CA.pem	Info	Remove
2	DST_ACES_CA_X6.crt	Info	Remove
3	DST_Root_CA_X3.crt	Info	Remove
4	Deutsche_Telekom_Root_CA_2.crt	Info	Remove
5	DigiCert_Assured_ID_Root_CA.crt	Info	Remove
6	DigiCert_Assured_ID_Root_G2.crt	Info	Remove
7	DigiCert_Assured_ID_Root_G3.crt	Info	Remove
8	DigiCert_Global_Root_CA.crt	Info	Remove
9	DigiCert_Global_Root_G2.crt	Info	Remove
10	DigiCert_Global_Root_G3.crt	Info	Remove
11	DigiCert_High_Assurance_EV_Root_CA.crt	Info	Remove
12	DigiCert Trusted Root G4.crt	Info	Remove

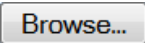
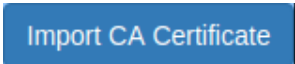
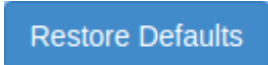




**Figure 2-20. SSL Configuration Page**

12	DigiCert_Trusted_Root_G4.crt	Info	Remove
13	Equifax_Secure_CA.crt	Info	Remove
14	Equifax_Secure_Global_eBusiness_CA.crt	Info	Remove
15	Equifax_Secure_eBusiness_CA_1.crt	Info	Remove
16	GeoTrust_Global_CA.crt	Info	Remove
17	GeoTrust_Global_CA_2.crt	Info	Remove
18	GeoTrust_Primary_Certification_Authority.crt	Info	Remove
19	GeoTrust_Primary_Certification_Authority_-_G2.crt	Info	Remove
20	GeoTrust_Primary_Certification_Authority_-_G3.crt	Info	Remove
21	GeoTrust_Universal_CA.crt	Info	Remove
22	GeoTrust_Universal_CA_2.crt	Info	Remove
23	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G4.crt	Info	Remove
24	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5.crt	Info	Remove
25	VeriSign_Universal_Root_Certification_Authority.crt	Info	Remove
26	Verisign_Class_1_Public_Primary_Certification_Authority.crt	Info	Remove
27	Verisign_Class_1_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
28	Verisign_Class_2_Public_Primary_Certification_Authority_-_G2.crt	Info	Remove
29	Verisign_Class_2_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
30	Verisign_Class_3_Public_Primary_Certification_Authority.crt	Info	Remove
31	Verisign_Class_3_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
32	thawte_Primary_Root_CA.crt	Info	Remove
33	thawte_Primary_Root_CA_-_G2.crt	Info	Remove
34	thawte_Primary_Root_CA_-_G3.crt	Info	Remove

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

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

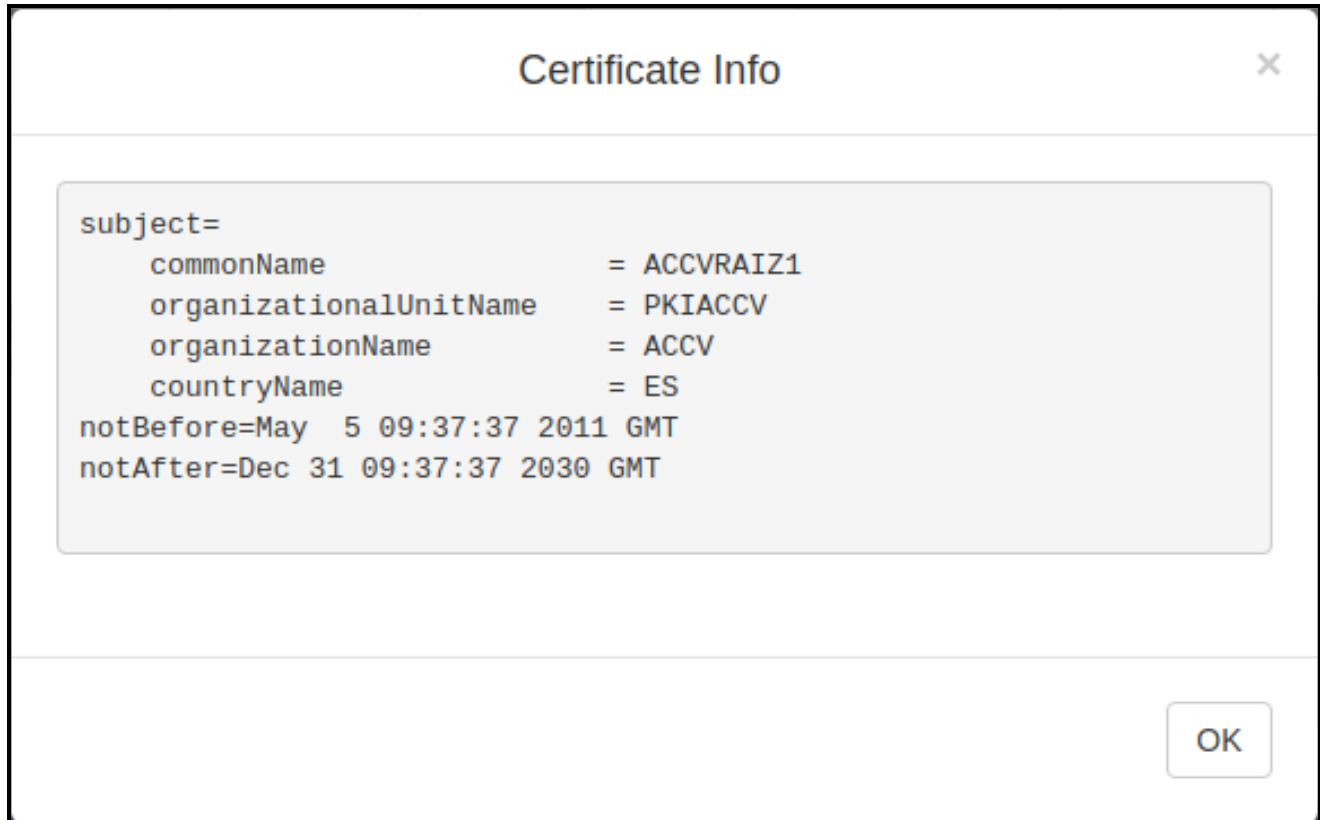
**Table 2-12. SSL Configuration Parameters**

Web Page Item	Description
<b>Server CAs</b>	
	Use this button to select a configuration file to import.
	Click <b>Browse</b> to select a CA certificate to import. After selecting a server certificate authority (CA), click <b>Import CA Certificate</b> to import it to the list of trusted CAs. CAs are used to validate the certificate presented by the server when establishing a TLS connection.
	<b>Restore Defaults</b> will restore the default list of registered CAs and <b>Remove All</b> will remove all registered CAs.
	<b>Restore Defaults</b> will restore the default list of registered CAs and <b>Remove All</b> will remove all registered CAs.
<b>Client Certificate</b>	
Client CA ?	When doing mutual authentication this device will present a client certificate with these parameters. Right click and <b>Save Link As...</b> to get the Cyberdata CA used to sign this client certificate.
<b>Test SSL Connection</b>	
Server ?	The ssl test server address as a fully qualified domain name or in IPv4 dotted decimal notation.
Port ?	The ssl test server port. The supported range is 0-65536. SIP connections over TLS to port 5060 will do the same.
	Use this button to test a TLS connection to a remote server. This will attempt to make a socket connection to the configured test server and port and report the success or failure. This can be used to debug TLS connection issues separate from SIP registration issues.
<b>List of Trusted CAs</b>	
	Provides details of the certificate. After clicking on this button, the <b>Certificate Info Window</b> appears. See <a href="#">Section 2.3.8.1, "Certificate Info Window"</a> .
	Removes this certificate from the list of trusted certificates. After clicking on this button, the <b>Remove Server Certificate Window</b> appears. See <a href="#">Section 2.3.8.2, "Remove Server Certificate Window"</a> .

### 2.3.8.1 Certificate Info Window

The **Certificate Info Window** provides details of the certificate. This window appears after clicking on the **Info** button. See [Figure 2-21](#).

**Figure 2-21. Certificate Info Window**

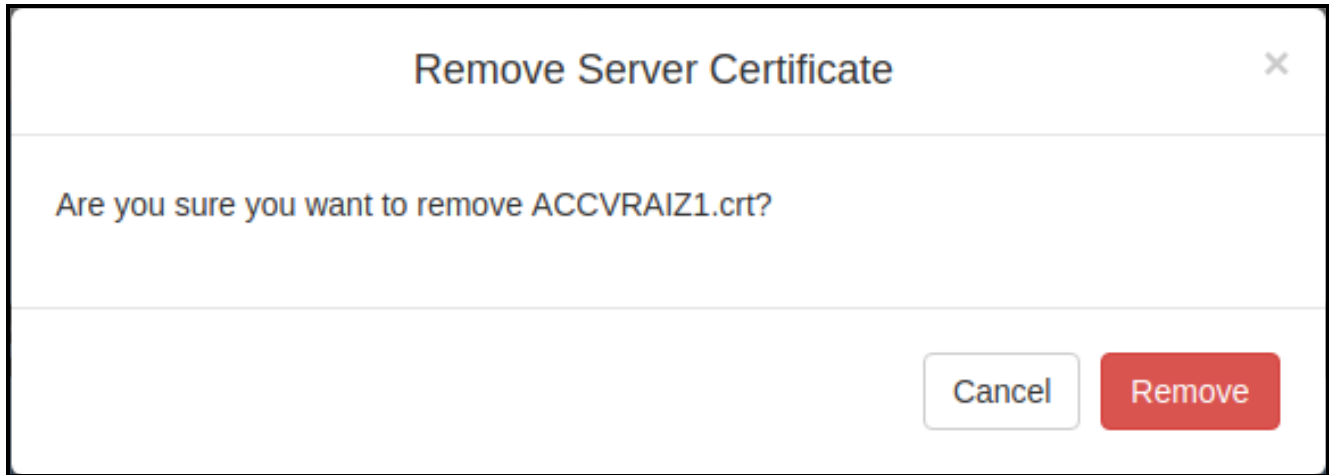




### 2.3.8.2 Remove Server Certificate Window

The **Remove Server Certificate Window** will ask if the user wants to remove a certificate from the list of trusted certificates. This window appears after clicking on the **Remove** button. See [Figure 2-22](#).

**Figure 2-22. Remove Server Certificate Window**



---

## 2.3.9 Configure the Multicast Parameters

The **Multicast** page allows the device to join up to ten paging zones that will activate the strobe when a stream is sent to its address.

A paging zone can consist of one or many CyberData multicast group-enabled products. There is no limit to how many endpoints 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** menu button to open the **Multicast** page. See [Figure 2-23](#).

**Figure 2-23. Multicast Configuration Page**

Home

Device

Network

SIP

SSL

Multicast

Sensor

Audiofiles

Events

Autoprov

Firmware

# Singlewire Multicolor Strobe

## Multicast Settings

Enable Multicast Operation: ☒

Priority	Address	Port	Name	Relay	Scene	Brightness	Color	Red	Green	Blue	
0	239.168.3.1	2000	Background Music	<input type="checkbox"/>	Slow Fade ▾	40	Color ▾	255	200	0	Preview
1	239.168.3.2	3000	MG1	<input type="checkbox"/>	Fast Fade ▾	255	<div>                     White                      Yellow                      Orange                      Red                      Pink                      Purple                      Blue                      Teal                      Green                      Lime                 </div>			0	Preview
2	239.168.3.3	4000	MG2	<input type="checkbox"/>	Slow Blink ▾	180				128	Preview
3	239.168.3.4	5000	MG3	<input type="checkbox"/>	Fast Blink ▾	75				128	Preview
4	239.168.3.5	6000	MG4	<input type="checkbox"/>	ADA ▾	255				255	Preview
5	239.168.3.6	7000	MG5	<input type="checkbox"/>	Off ▾	255				255	Preview
6	239.168.3.7	8000	MG6	<input type="checkbox"/>	Slow Fade ▾	220				0	Preview
7	239.168.3.8	9000	MG7	<input type="checkbox"/>	Fast Fade ▾	140				255	Preview
8	239.168.3.9	10000	MG8	<input type="checkbox"/>	Fast Blink ▾	255				0	Preview
9	239.168.3.10	11000	Emergency	<input type="checkbox"/>	ADA ▾	255	Color ▾	255	255	255	Preview

Polycom Default Channel

1 ▾

Polycom Priority Channel

24 ▾

Polycom Emergency Channel

25 ▾

SIP calls are considered priority 4.5

Port range can be from 2000-65535

Priority 9 is the highest and 0 is the lowest

A higher priority audio stream will always supersede a lower one

Save

Reboot




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

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

**Table 2-13. Multicast Page Parameters**

Web Page Item	Description
Enable Multicast Operation	Enables or disables multicast operation.
Priority	Indicates the priority for the multicast group. Priority <b>9</b> is the highest (emergency streams). <b>0</b> is the lowest (background music). SIP calls are considered priority <b>4.5</b> . See <a href="#">Section 2.3.10, "Configure the Sensor Configuration Parameters"</a> 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]).  <b>Note:</b> 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).
Relay	When selected, the device will activate a relay before the strobe is triggered by the multicast stream.
Scene ?	Select desired scene (only one may be chosen).
ADA Compliant ?	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.
Slow Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink ?	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.
Fast Blink ?	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.
Color ?	Select desired color (only one may be chosen).
Brightness ?	How bright the strobe will blink on a multicast page. This is the maximum brightness for "fade" type scenes.
Red ?	The red LED value for Multicast.
Green ?	The green LED value for Multicast.
Blue ?	The blue LED value for Multicast.
Polycom Default Channel	When a default Polycom channel/group number is selected, the device will subscribe to the default channel for one-way group pages. Group Numbers 1-25 are supported. Or, select <b>Disabled</b> to disable this channel.
Polycom Priority Channel	When a priority Polycom channel/group number is selected, the device will subscribe to the priority channel for one-way group pages. Group Numbers 1-25 are supported. Or, select <b>Disabled</b> to disable this channel.
Polycom Emergency Channel	When an emergency Polycom channel/group number is selected, the device will subscribe to the default channel for one-way group pages. Group Numbers 1-25 are supported. Or, select <b>Disabled</b> to disable this channel.

**Table 2-13. Multicast Page Parameters (continued)**

Web Page Item	Description
	Use this button to preview the strobe flashing behavior for the <b>Multicast Strobe Settings</b> .
	Click the <b>Save</b> button to save your configuration settings.
	Click on the <b>Reboot</b> button to reboot the system.

## 2.3.10 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 Intercom board and will be activated when the Intercom is removed from the case.

Each sensor can trigger up to four different actions:

- Activate the relay until the sensor is deactivated
- Call an extension and play a pre-recorded audio file
- Flash a strobe scene

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

1. Click **Sensor** menu button to open the **Sensor** page ([Figure 2-24](#)).

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

The screenshot shows the 'Sensor' configuration page for a 'Singlewire Multicolor Strobe'. The page features a navigation bar at the top with tabs for Home, Device, Network, SIP, SSL, Multicast, **Sensor**, Audiofiles, Events, Autopro, and Firmware. The main heading is 'Singlewire Multicolor Strobe'. Below this, there are four distinct settings sections:

- Door Sensor Settings:** Includes options for 'Door Sensor Normally Closed' (Yes/No), 'Door Open Timeout (in seconds)' (0), 'Activate Relay' (checkbox), 'Make call to extension' (checkbox), 'Dial Out Extension' (204), 'Dial Out ID' (id204), and 'Repeat Sensor Message' (0).
- Intrusion Sensor Settings:** Includes 'Activate Relay' (checkbox), 'Make call to extension' (checkbox), 'Dial Out Extension' (204), 'Dial Out ID' (id204), and 'Repeat Intrusion Message' (0).
- Sensor Strobe Settings:** Includes 'Blink Strobe on Sensor' (checkbox), a table for 'Scene', 'Color', and 'Brightness' (Red, Green, Blue) with values set to 255, and a 'Preview' button.
- Intrusion Strobe Settings:** Includes 'Blink Strobe on Intrusion' (checkbox), a table for 'Scene', 'Brightness', and 'Color' (Red, Green, Blue) with values set to 255, and a 'Preview' button.

At the bottom of the page, there are buttons for 'Save', 'Reboot', 'Toggle Help', 'Test Door Sensor', and 'Test Intrusion Sensor'.



- On the **Sensor** page, enter values for the parameters indicated in [Table 2-14](#).

**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 2-14. Sensor Configuration Parameters**






Web Page Item	Description
<b>Door Sensor Settings</b>	
Door Sensor Normally Closed ?	Select the inactive state of the door sensor. The door sensor is also known as the Sense Input on the device's terminal block.
Door Open Timeout (in seconds) ?	The time (in seconds) the device will wait before it performs an action when the on-board door sensor is activated. The action(s) performed are based on the configured Door Sensor Settings below. Enter up to 5 digits.
Activate Relay ?	When selected, the device's on-board relay will be activated until the on-board door sensor is deactivated.
Make call to extension ?	When selected, the device will call an extension when the on-board door sensor is activated. Use the <b>Dial Out Extension</b> field below to specify the extension the device will call.
Dial Out Extension ?	Specify the extension the device will call when the on-board door sensor is activated. Enter up to 64 alphanumeric characters.
Dial Out ID ?	An additional Caller identification string added to outbound calls. Enter up to 64 alphanumeric characters.
Repeat Sensor Message ?	The number of times to repeat the audio message to the remote endpoint. A value of 0 will repeat forever. Enter a value from 0-65536.
<b>Sensor Strobe Settings</b>	
Blink Strobe on Sensor ?	When selected, the Strobe will blink a scene when the sensor is triggered for both door and intrusion sensors.
Scene ?	Select desired scene (only one may be chosen).
ADA Compliant ?	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.
Slow Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink ?	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.
Fast Blink ?	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.
Color ?	Select desired color (only one may be chosen).
Brightness ?	How bright the strobe will blink when the sensor is triggered. This is the maximum brightness for "fade" type scenes.
Red ?	The red LED value for the Sensor.
Green ?	The green LED value for the Sensor.

Table 2-14. Sensor Configuration Parameters (continued)

Web Page Item	Description
Blue ?	The blue LED value for the Sensor.
	Use this button to preview the strobe flashing behavior for the <b>Sensor Strobe Settings</b> .
<b>Intrusion Sensor Settings</b>	
Activate Relay ?	When selected, the device's on-board relay will be activated until the intrusion sensor is deactivated.
Make call to extension ?	When selected, the device will call an extension when the intrusion sensor is activated. Use the <b>Dial Out Extension</b> field below to specify the extension the device will call.
Dial Out Extension ?	Specify the extension the device will call when the intrusion sensor is activated. Enter up to 64 alphanumeric characters.
Dial Out ID ?	An additional Caller identification string added to outbound calls. Enter up to 64 alphanumeric characters.
Repeat Intrusion Message ?	The number of times to repeat the audio message to the remote endpoint. A value of 0 will repeat forever. Enter a value from 0-65536.
<b>Intrusion Sensor Strobe Settings</b>	
Blink Strobe on Intrusion Sensor ?	When selected, the Strobe will blink a scene when the intrusion sensor is triggered.
Scene ?	Select desired scene (only one may be chosen).
ADA Compliant ?	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.
Slow Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink ?	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.
Fast Blink ?	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.
Color ?	Select desired color (only one may be chosen).
Brightness ?	How bright the strobe will blink when the intrusion sensor is triggered. This is the maximum brightness for "fade" type scenes.
Red ?	The red LED value for the Intrusion Sensor.
Green ?	The green LED value for the Intrusion Sensor.
Blue ?	The blue LED value for the Intrusion Sensor.
	Use this button to preview the strobe flashing behavior for the <b>Intrusion Sensor Strobe Settings</b> .



**Table 2-14. Sensor Configuration Parameters (continued)**

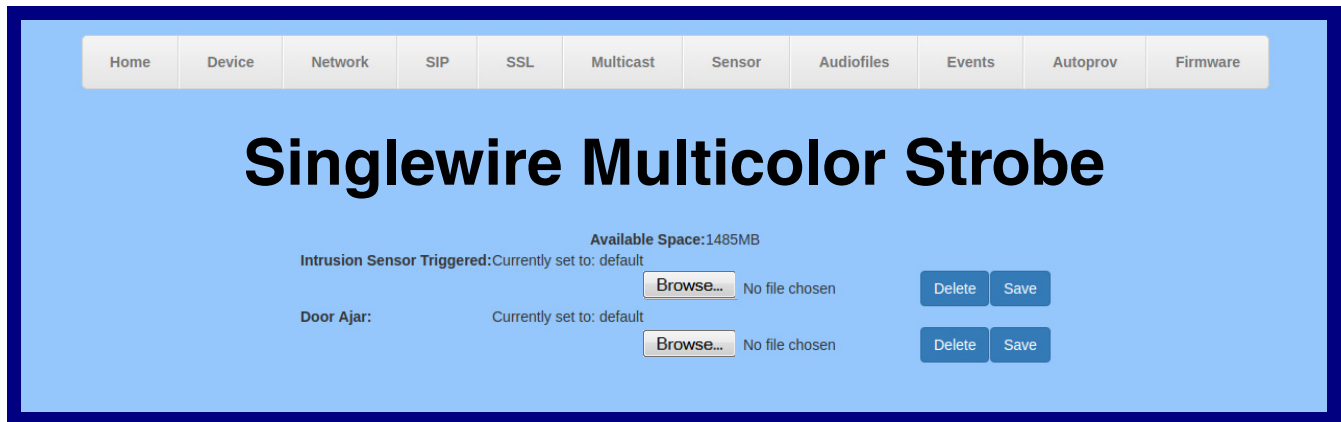
Web Page Item	Description
	Click the <b>Test Door Sensor</b> button to test the door sensor.
	Click the <b>Test Intrusion Sensor</b> button to test the Intrusion sensor.
	Click the <b>Save</b> button to save your configuration settings.
	Click on the <b>Reboot</b> button to reboot the system.
	Click on the <b>Toggle Help</b> button to see a short description of some of the web page items. First click on the <b>Toggle Help</b> button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

## 2.3.11 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 Intercom.

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

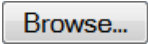
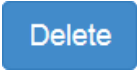

**Figure 2-25. Audiofiles Configuration Page**



2. On the **Audiofiles** 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.

**Table 2-15. Audiofiles Configuration Parameters**

Web Page Item	Description
Available Space	Shows the space available for the user to save custom audio files if they want to change the message when the door or sensor is triggered.
Intrusion Sensor Triggered	Corresponds to the message "Intrusion Sensor Triggered" (24 character limit).
Door Ajar	Corresponds to the message "Door Ajar" (24 character limit).
	Click on the <b>Browse</b> button to navigate to and select an audio file.
	The <b>Delete</b> button will delete any user uploaded audio and restore the stock audio file.
	The <b>Save</b> button will download a new user audio file to the board once you've selected the file by using the <b>Browse</b> button. The <b>Save</b> button will delete any pre-existing user-uploaded audio files.

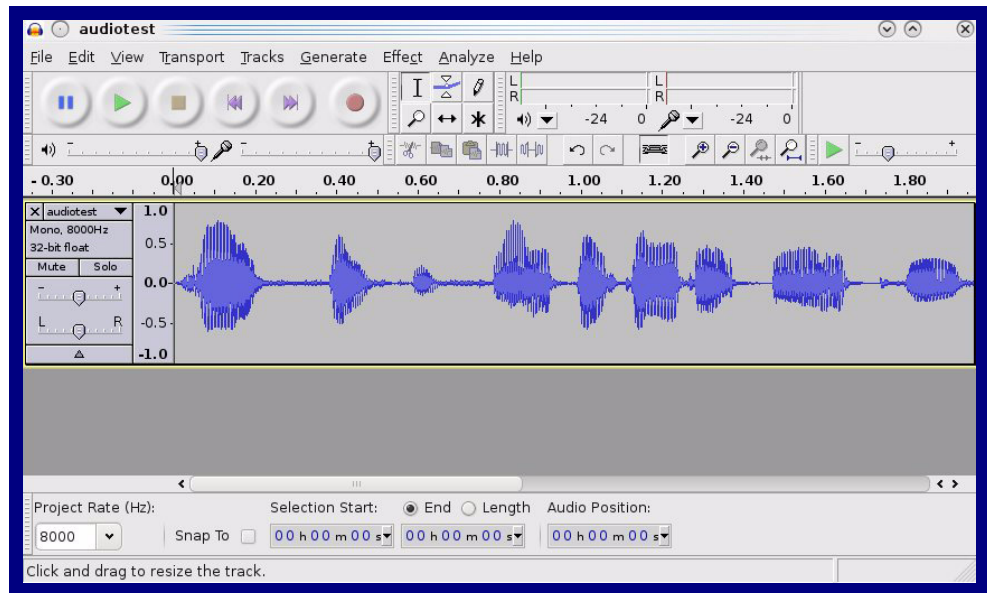
### 2.3.11.1 User-created Audio Files

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

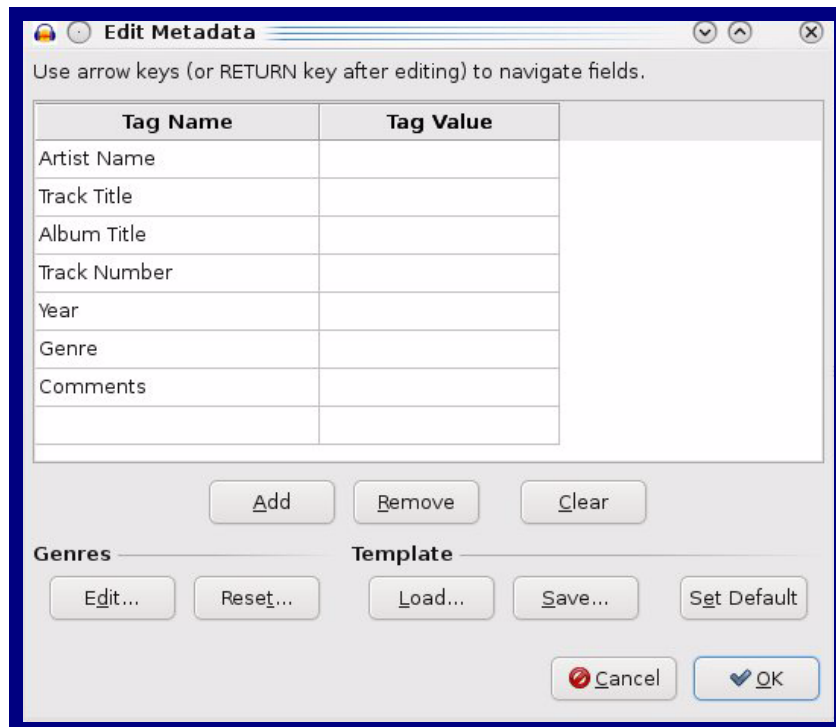
RIFF (little-endian) data, WAVE audio, Microsoft PCM, 16 bit, mono 8000 Hz

You can use the free utility *Audacity* to convert audio files into this format. See [Figure 2-26](#) through [Figure 2-28](#).

**Figure 2-26. Audacity 1**



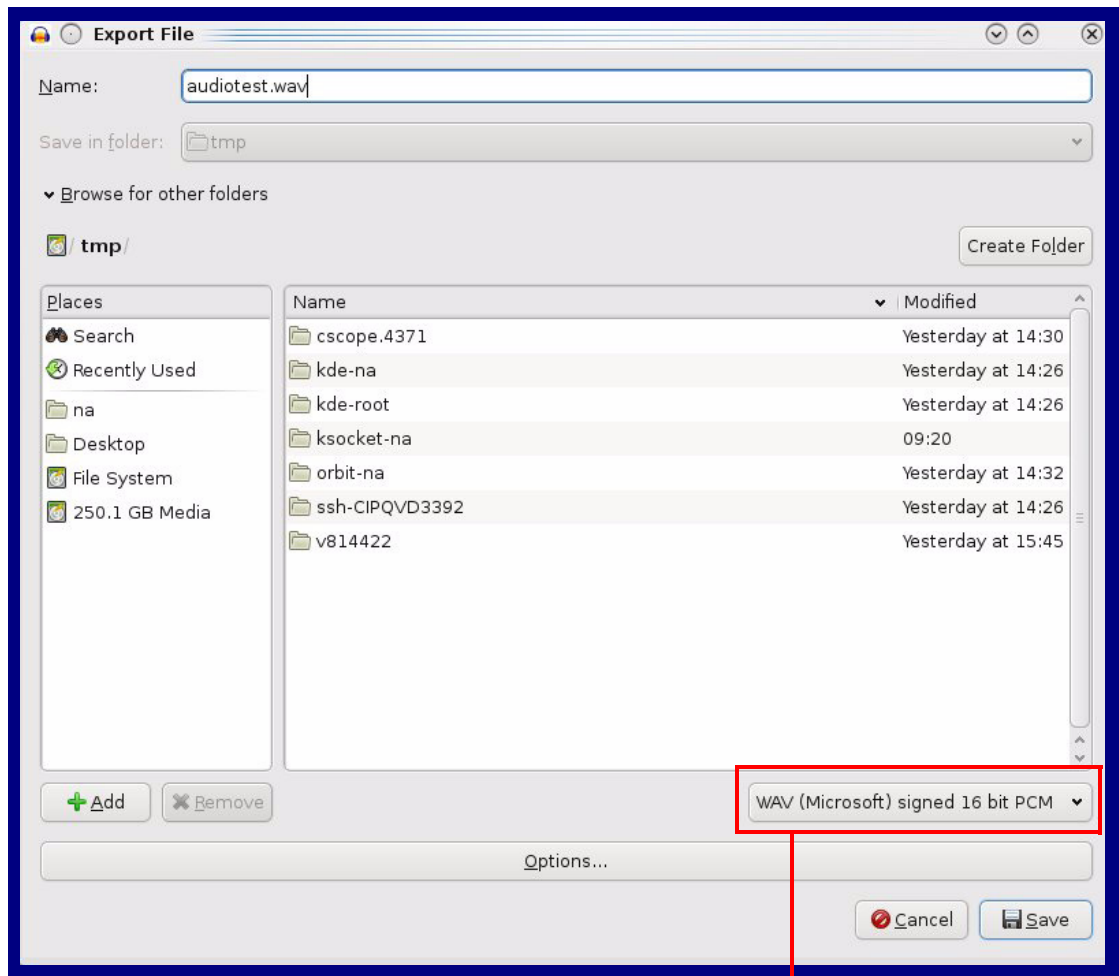
**Figure 2-27. Audacity 2**



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

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

**Figure 2-28. WAV (Microsoft) signed 16 bit PCM**



WAV (Microsoft) signed 16 bit PCM

## 2.3.12 Configure the Events 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 2-29](#)).

**Figure 2-29. Event Configuration Page**

Home Device Network SIP SSL Multicast Sensor Audiofiles **Events** Autopro Firmware

# Singlewire Multicolor Strobe

Enable Event Generation: ☐

## Events

Enable Relay Activated Events: ☐

Enable Relay Deactivated Events: ☐

Enable Ring Events: ☐

Enable Night Ring Events: ☐

Enable Multicast Start Events: ☐

Enable Multicast Stop Events: ☐

Enable Power On Events: ☐

Enable Sensor Events: ☐

Enable 60 Second Heartbeat: ☐

Enable InformaCast Start Events: ☐

Enable InformaCast Stop Events: ☐

## Event Server

Server IP Address: 10.0.0.250

Server Port: 8080

Server URL: xmlparse\_engine

Save Reboot Toggle Help


2. On the **Events** 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. Events Configuration Parameters**

Web Page Item	Description
Enable Event Generation ?	The device will send HTTP POST events to the specified remote server and port number whenever a certain action takes place. Select an event type below to generate an HTTP POST event.
<b>Events</b>	
Enable 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.
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 a strobe scene when the device receives a multicast.
Enable Multicast Stop Events ?	When selected, the device will report when the device stops a strobe scene when the multicast stream ends.
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 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.
Enable Informacast Start Events ?	When selected, the device will report when a Start event has been received from the Singlewire server.
Enable Informacast Stop Events ?	When selected, the device will report when a Stop event has been received from the Singlewire server.
Check All	Click on <b>Check All</b> to select all of the events on the page.
Uncheck All	Click on <b>Uncheck All</b> to de-select all of the events on the page.
<b>Event Server</b>	
Server IP Address ?	The IPv4 address of the event server in dotted decimal notation.
Server Port ?	Specify the event server port number. The supported range is 0-65536. Enter up to 5 digits.
Server URL ?	Generally, the destination URL is the name of the application that receives the events and the string in the HTTP POST command. It can be a script used to parse and process the HTTP POST events. Enter up to 127 characters.
<b>Save</b>	Click the <b>Save</b> button to save your configuration settings.
<b>Reboot</b>	Click on the <b>Reboot</b> button to reboot the system.

**Table 2-16. Events Configuration Parameters(continued)**

Web Page Item	Description
	Click on the <b>Toggle Help</b> button to see a short description of some of the web page items. First click on the <b>Toggle Help</b> button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

### 2.3.12.1 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 VoIP 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 VoIP 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 VoIP 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 VoIP 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 VoIP 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 VoIP 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 VoIP 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 VoIP 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 VoIP 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 VoIP 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 VoIP Device' MAC='0020f70015b6'>
<event>NIGHTRINGING</event>
</cyberdata>
```

## 2.3.13 Configure the Autoprovisioning Parameters

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

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

1. Click the **Autoprov** menu button to open the **Autoprovisioning** page. See [Figure 2-30](#).

**Figure 2-30. Autoprovisioning Page**

Home Device Network SIP SSL Multicast Sensor Audiofiles Events Autoprov Firmware

# Singlewire Multicolor Strobe

Enable Autoprovisioning: ☒

Autoprovisioning Server:

Autoprovisioning Filename:

Use tftp: ☐

Verify Server Certificate ☐

Username:

Password:

Autoprovisioning autoupdate (in minutes):

Autoprovision at time (HHMM):

Autoprovision when idle (in minutes > 10):

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

Autoprovisioning happens on boot.

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

If these haven't been configured, it will look for an autoprovisioning server in your list of DHCP options and try to download '0020f704048a.xml' and if this fails, '000000cd.xml'.

Save Reboot Toggle Help

Download Template

Autoprovisioning log

```





2019-01-30 12:06:34 Autoprov: no autoprov triggers. Exiting...
2019-01-30 12:06:36 Autoprovisioning on boot
2019-01-30 12:06:36 Autoprov found server='https://10.0.0.242:4444' in dhcp option 43
2019-01-30 12:06:36 Autoprov looking for https://10.0.0.242:4444/0020f704048a.xml
2019-01-30 12:06:36 Autoprov not verifying server certificate
2019-01-30 12:06:36 Autoprov: download failed
2019-01-30 12:06:36 Autoprov looking for 000000cd.xml at https://10.0.0.242:4444
2019-01-30 12:06:36 Autoprov looking for https://10.0.0.242:4444/000000cd.xml
2019-01-30 12:06:36 Autoprov not verifying server certificate
2019-01-30 12:06:36 Autoprov: download failed

```

2. On the **Autoprovisioning** page, you may enter values for the parameters indicated in [Table 2-17](#).

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

**Table 2-17. Autoprovisioning Page Parameters**

Web Page Item	Description
Enable Autoprovisioning ?	The device will automatically fetch a configuration file, also known as the 'autoprovisioning file', based on the configured settings below.
Autoprovisioning Server ?	Enter the IPv4 address of the provisioning server in dotted decimal notation.
Autoprovisioning Filename ?	<p>The autoprovisioning filename is the configuration filename. The default autoprovisioning filename is in the format of <b>&lt;mac address&gt;.xml</b>.</p> <p>Supported filename extensions are .txt, and .xml. The current filename is denoted by an asterisk at the bottom of the <a href="#">Autoprovisioning Page</a>. Enter up to 256 characters.</p> <p>A file may have any name with an xml extension. If a file name is entered, the device will look for the specified file name, and only that file.</p>
Use tftp ?	The device will use TFTP (instead of http) to download autoprovisioning files.
Verify Server Certificate ?	When using ssl to download autoprovisioning files, reject connections where the server address doesn't match the server certificate's common name.
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.
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.
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.
	Click the <b>Save</b> button to save your configuration settings.
	Click on the <b>Reboot</b> button to reboot the system.
	Click on the <b>Toggle Help</b> button to see a short description of some of the web page items. First click on the <b>Toggle Help</b> button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.
	Press the <b>Download Template</b> button to create an autoprovisioning file for the device. See <a href="#">Section 2.3.13.3, "Download Template Button"</a>
Autoprovisioning log	The autoprovisioning log provides information about the latest autoprovisioning attempt (i.e. dhcp options and server accessed and files parsed or not found).

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

### 2.3.13.1 Autoprovisioning

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

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

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

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

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

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

You can download an autoprovisioning template file from the [Autoprovisioning Page](#) using the **Download Template** button (see [Table 2-17](#)). This file contains every configuration option that can be set on the board.

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

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

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

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

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

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

The file 0020f7123456.xml contains:

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

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

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

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

#### Checking for New Autoprovisioning Files after Boot

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

## The Autoprovisioning Filename

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

**Table 2-18. Autoprovisioning File Name**

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

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

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

For example:

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

The autoprovisioning filename is set to “cyberdata/”

On boot, the device will try to download:

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

...and if this fails:

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

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

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

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

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

The <FirmwareFile> name can contain path elements (i.e. /path/to/firmware/10.3.0-ulmage-[device\_file\_name]).

The device also supports product strings for downloading firmware. If the <FirmwareFile> option is not set, the device will look for its particular product string for a firmware filename. In this way, a generic autoprovisioning file can specify unique firmware for a range of products.

The list of valid product strings:

```
<ProductString>CallButton31</ProductString>
<ProductString>EmergencyIntercom31</ProductString>
<ProductString>EmergencyIntercom31SW</ProductString>
<ProductString>IndoorIntercom31</ProductString>
<ProductString>IndoorIntercom31SW</ProductString>
<ProductString>IndoorKeypad31</ProductString>
<ProductString>IndoorKeypad31SW</ProductString>
<ProductString>OfficeRinger31</ProductString>
<ProductString>OfficeRinger31SW</ProductString>
<ProductString>OutdoorIntercom31</ProductString>
<ProductString>OutdoorIntercom31SW</ProductString>
<ProductString>OutdoorKeypad31</ProductString>
<ProductString>OutdoorKeypad31SW</ProductString>
<ProductString>Strobe31</ProductString>
<ProductString>Strobe31SW</ProductString>
```



Autoprovisioning  
Example 1

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

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

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

**000000cd.xml**

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

**sip\_common.xml**

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

**sip\_0020f7020001.xml**

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

**sip\_0020f7020002.xml**

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

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

1. Device1 changes its device name to **CyberData Autoprovisioned**.
2. Device1 finds an AutoprovFile element containing the filename **sip\_common.xml**. The device downloads **sip\_common.xml** from “https://autoprovtest.server.net,” and imports this configuration, setting the sip server to **10.0.0.253** and the remote port to **5060.3**.
3. Device1 finds another AutoprovFile element containing the filename **sip\_[macaddress].xml**. The device replaces the **[macaddress]** with its own mac address value creating **sip\_0020f7020001.xml**, downloads this file from “https://autoprovtest.server.net,” and imports this configuration. This sets the user ID to **198**, the password to **ext198**, and the dialout extension to **204**. Device1 is now finished with autoprovisioning.

Device2 goes through the same steps by setting its device name to **CyberData Autoprovisioned**, its SIP server to **10.0.0.253**, and its port to **5060**. When Device2 “sees” **sip\_[macaddress].xml**, Device2 replaces it with its own mac address and downloads **sip\_0020f7020002.xml** from “https://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 **10.0.0.253**, and the port is set to **5060**.

## XML Files

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

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

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

From the device specific xml, a pointer to a sip\_common file

From the device specific xml, a pointer to the device specific sip\_[macaddress].xml

From the common file, a pointer to sip\_common.xml

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

## Autoprovisioned Audio Files

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

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

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

## 2.3.13.2 Sample dhcpd.conf

```

#
# Sample configuration file for ISC dhcpd for Debian
#

ddns-update-style none;

option domain-name "voiplab";
option domain-name-servers 10.0.0.252;
option option-150 code 150 = ip-address;
option ntp-servers north-america.pool.ntp.org;
option space VendorInfo;
option VendorInfo.text code 10 = { text };
authoritative;
log-facility local7;

subnet 10.0.0.0 netmask 255.0.0.0 {
    max-lease-time 3600;
    default-lease-time 3600;

    option routers                10.0.0.1;
    option subnet-mask            255.0.0.0;

    option domain-name            "voiplab";
    option domain-name-servers    10.0.0.252;

    option time-offset            -8;                # Pacific Standard Time

#    option www-server            99.99.99.99;        # OPTION 72

#    option tftp-server-name      "10.0.1.52";        # OPTION 66
#    option tftp-server-name      "http://test.cyberdata.net"; # OPTION 66

#    option option-150            10.0.0.252;        # OPTION 150

# These two lines are needed for option 43
#    vendor-option-space VendorInfo;                # OPTION 43
#    option VendorInfo.text "http://test.cyberdata.net"; # OPTION 43

    range 10.10.0.1 10.10.2.1; }

```

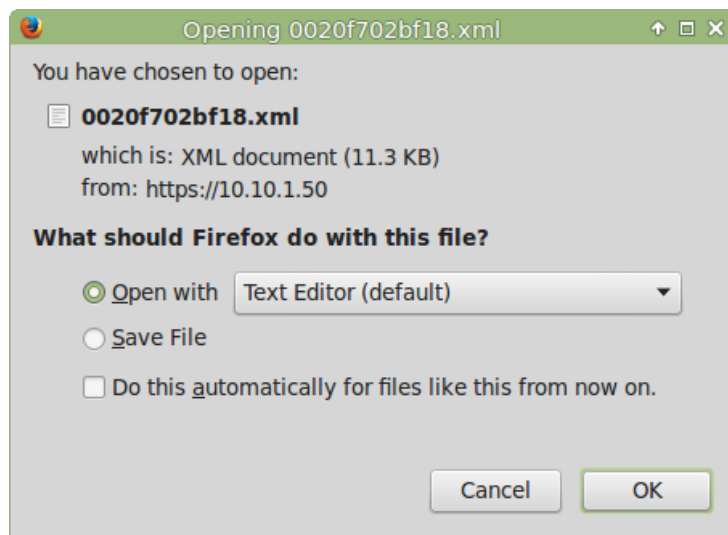
### 2.3.13.3 Download Template Button

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

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

1. On the **Autoprovisioning** page, click on the **Download Template** button.
2. You will see a window prompting you to save a configuration file (**.xml**) to a location on your computer ([Figure 2-31](#)). 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 2-31](#).

**Figure 2-31. Configuration File**



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

## 2.4 Upgrade the Firmware

**Note** CyberData strongly recommends that you do not upgrade the firmware when the device is likely to be in use.

To upgrade the firmware of your device:

1. Download the latest firmware file from the **Downloads** tab at the following webpage:  
<https://www.cyberdata.net/products/011489>
2. Unzip the firmware version file. This file may contain the following:
  - Firmware file
  - Release notes
  - Autoprovisioning template
3. Log in to the **Home** page as instructed in [Section 2.3.4, "Log in to the Configuration Home Page"](#).
4. Click on the **Firmware** menu button to open the **Firmware** page ([Figure 2-32](#)).

**Figure 2-32. Firmware Page**



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

6. Select the firmware file. This reveals the **Upload** button (Figure 2-33).

Figure 2-33. Upload Button



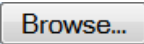

7. Click on the **Upload** button. After selecting the **Upload** button, you will see the progress of the upload in the **Upload Progress** bar.
8. When the upload is complete, you will see the words **Upload finished** under **Status Messages**.
9. At this point, you will see the progress of the upload's post processing in the **Upload Post Processing** bar.

**Note** Do not reboot the device before the upgrading process is complete.

10. When the process is complete, you will see the words **SWUPDATE Successful** under **Status Messages**.
11. The device will reboot automatically.
12. The **Home** page will display the version number of the firmware and indicate which boot partition is active.

Table 2-19 shows the web page items on the **Firmware** page.

**Table 2-19. Firmware Page Parameters**

Web Page Item	Description
	Use the <b>Browse</b> button to navigate to the location of the firmware file that you want to upload.
	Click on the <b>Upload</b> button to automatically upload the selected firmware and reboot the system.  <b>Note:</b> This button only appears after the user has selected a firmware file.
Upload progress	Status bar indicates the progress in uploading the file.
Upload Post Processing	Status bar indicates the progress of the software installation.
Status Messages	Messages relevant to the firmware update process appear here.

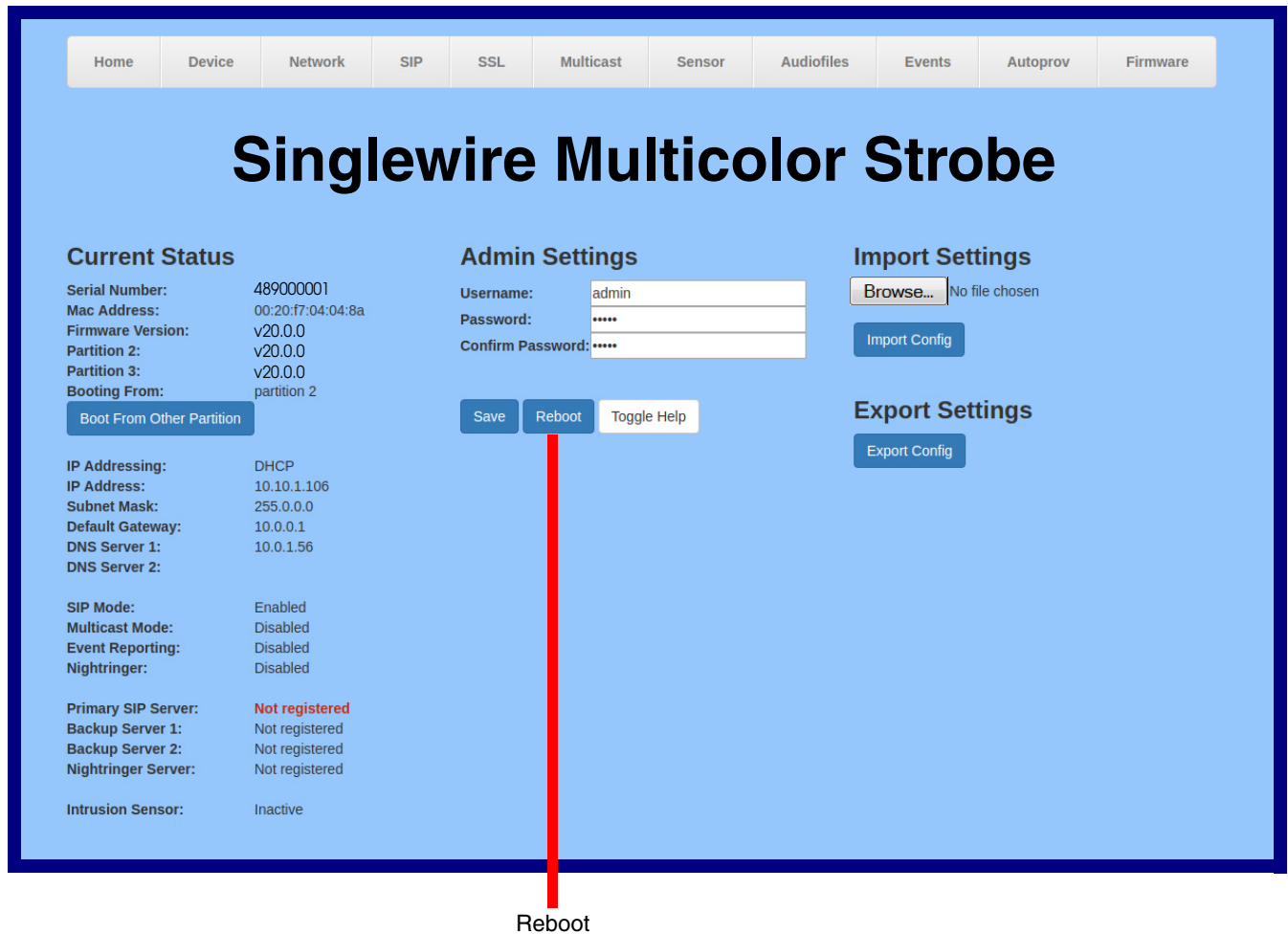


## 2.5 Reboot the Device

To reboot the device, complete the following steps:

1. Log in to the **Home** page as instructed in [Section 2.3.4, "Log in to the Configuration Home Page"](#).
2. Click on the **Reboot** button on the **Home** page ([Figure 2-34](#)). A normal restart will occur.

**Figure 2-34. Home Page**



---

## 2.6 Command Interface

Some functions on the device can be activated using simple POST commands to the web interface. The examples in [Table 2-20](#) use the free unix utility, **wget** **commands**. However, any program that can send HTTP POST commands to the device should work.

---

### 2.6.1 Command Interface Post Commands

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

**Table 2-20. Command Interface Post Commands**

Device Action	HTTP Post Command <sup>a</sup>
Test relay	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.154/command" --post-data "request=test_relay"
Place call to extension (example: extension 600)	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.154/command" --post-data "request=call&extension=600"
Terminate call	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.10.0.40/command" --post-data "terminate=yes"
Reboot	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.154/command" --post-data "request=reboot"
Swap boot partitions	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.154/command" --post-data "request=swap_boot_partition"


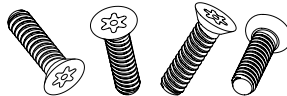
a. Type and enter all of each http POST command on one line.

# Appendix A: Mounting the InformaCast Enabled Outdoor RGB (Multi-Color) Strobe

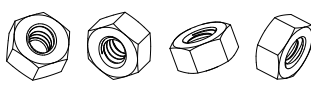
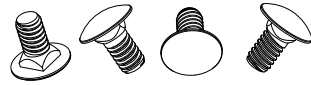
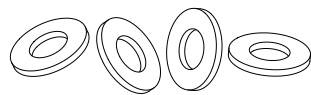
## A.1 Mount the InformaCast Enabled Outdoor RGB (Multi-Color) Strobe

Before you mount the InformaCast Enabled Outdoor RGB (Multi-Color) Strobe, make sure that you have received all of the parts. Refer to the following tables.

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

Quantity	Part Name	Illustration
1	T-15H Torx Key	
4	Security Torx Screw	

**Table A-2. Optional Accessories (for gooseneck mounting)**

Quantity	Part Name	Illustration
4	Carriage bolt nuts	
4	Carriage bolts	
4	Carriage bolt washers	

**Table A-3. Optional Accessories**

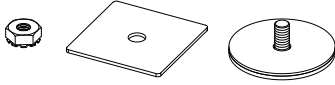
Quantity	Part Name	Illustration
1	531085* hole plug assembly	

Figure A-1 shows how to connect and seal the InformaCast Enabled Outdoor RGB (Multi-Color) Strobe.

Figure A-1. Connecting and Sealing the RGB Strobe

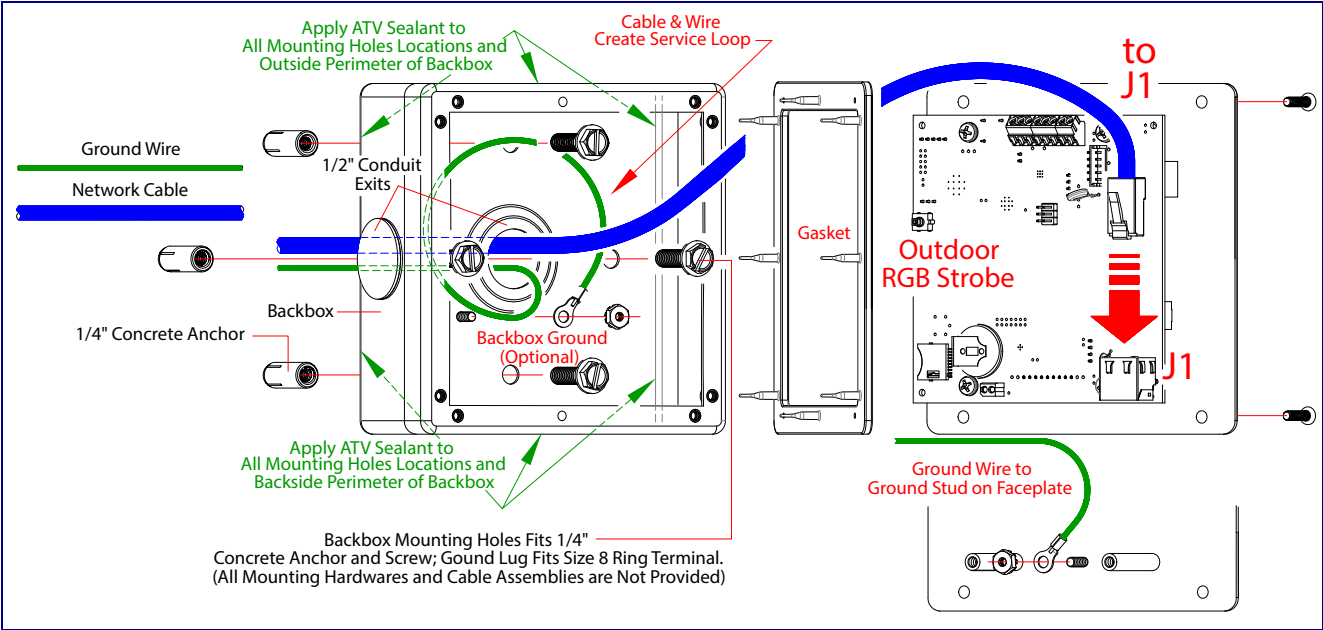


Figure A-2 shows how to install the ground cable to the InformaCast Enabled Outdoor RGB (Multi-Color) Strobe.

**Figure A-2. Installing the Ground Cable**

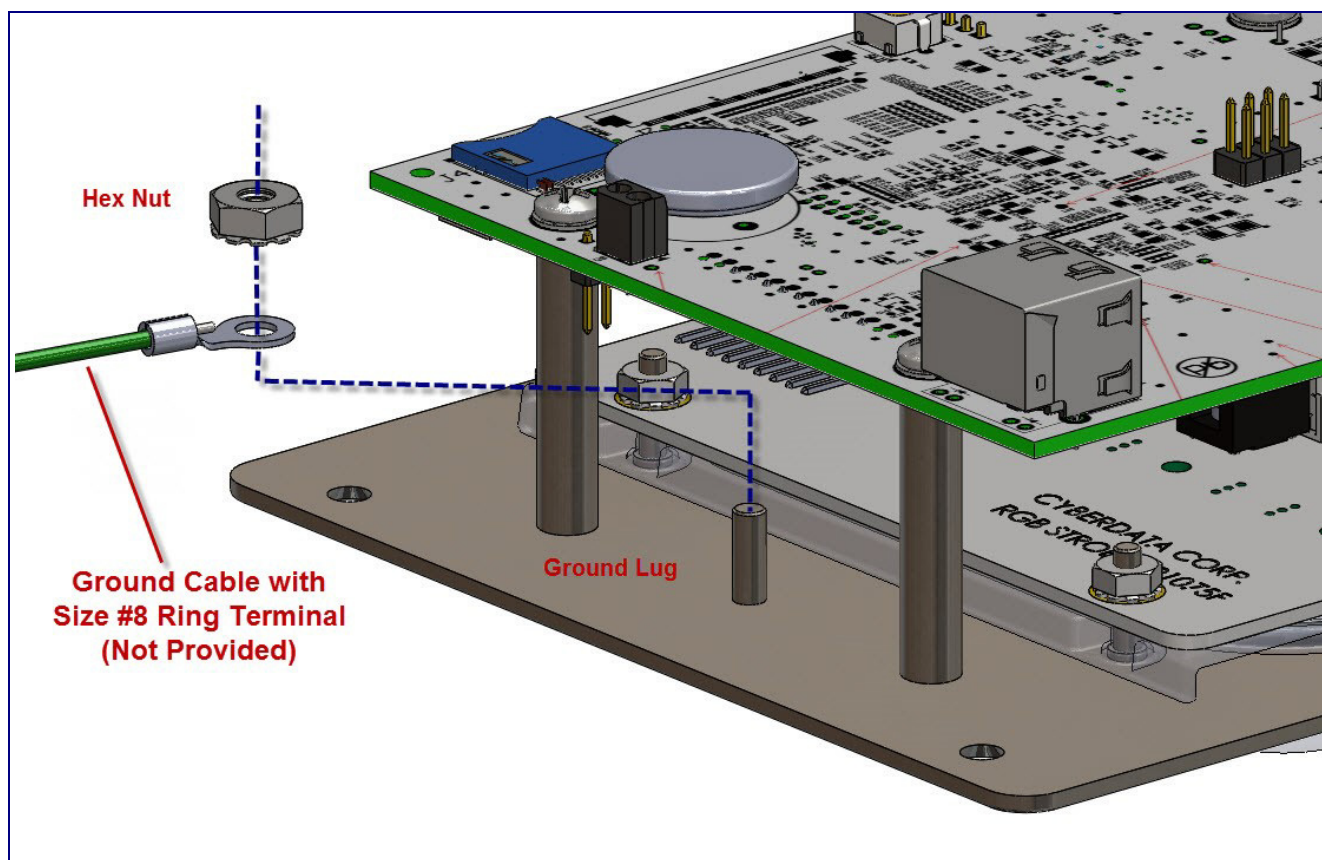


Figure A-3 shows the dimensions and rear view with mounting holes.

**Figure A-3. Dimensions and Rear View with Mounting Holes**

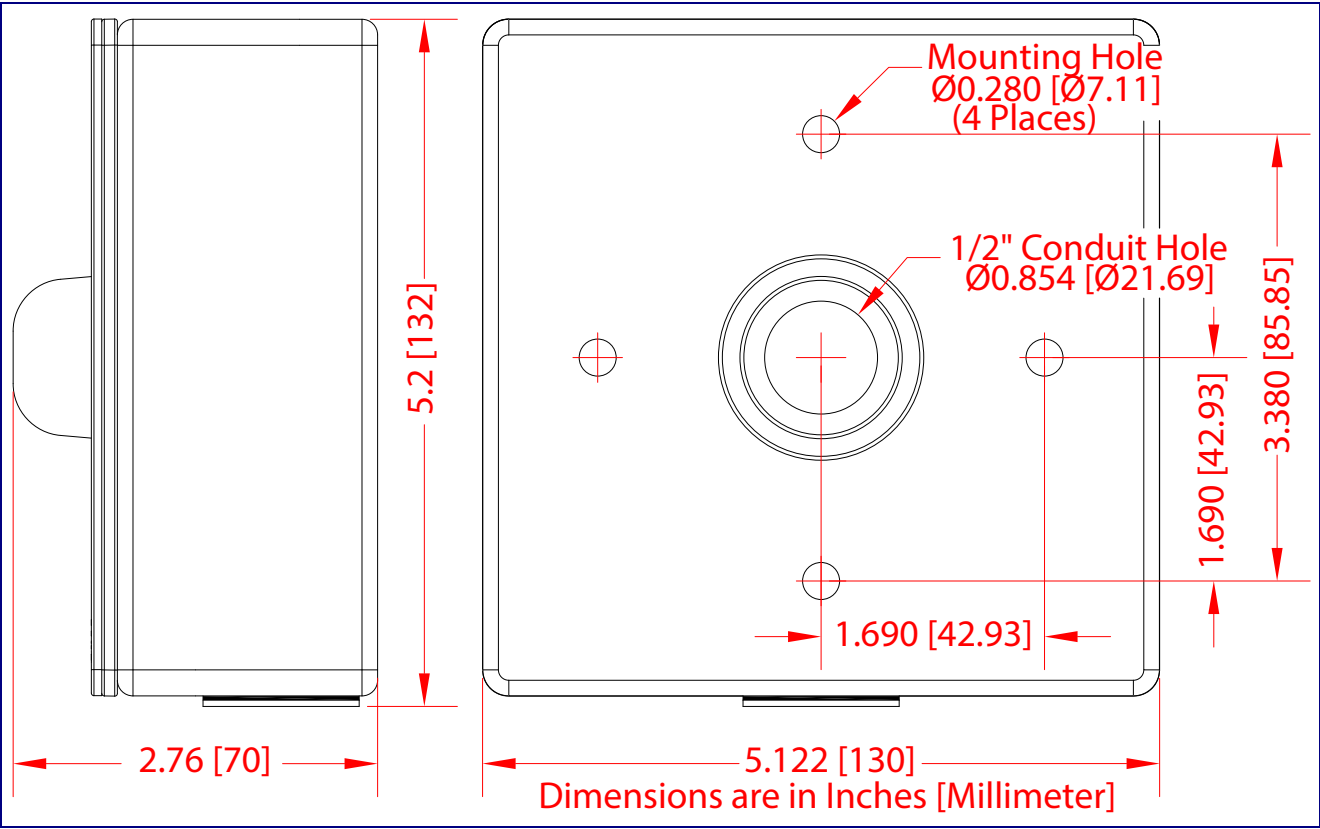
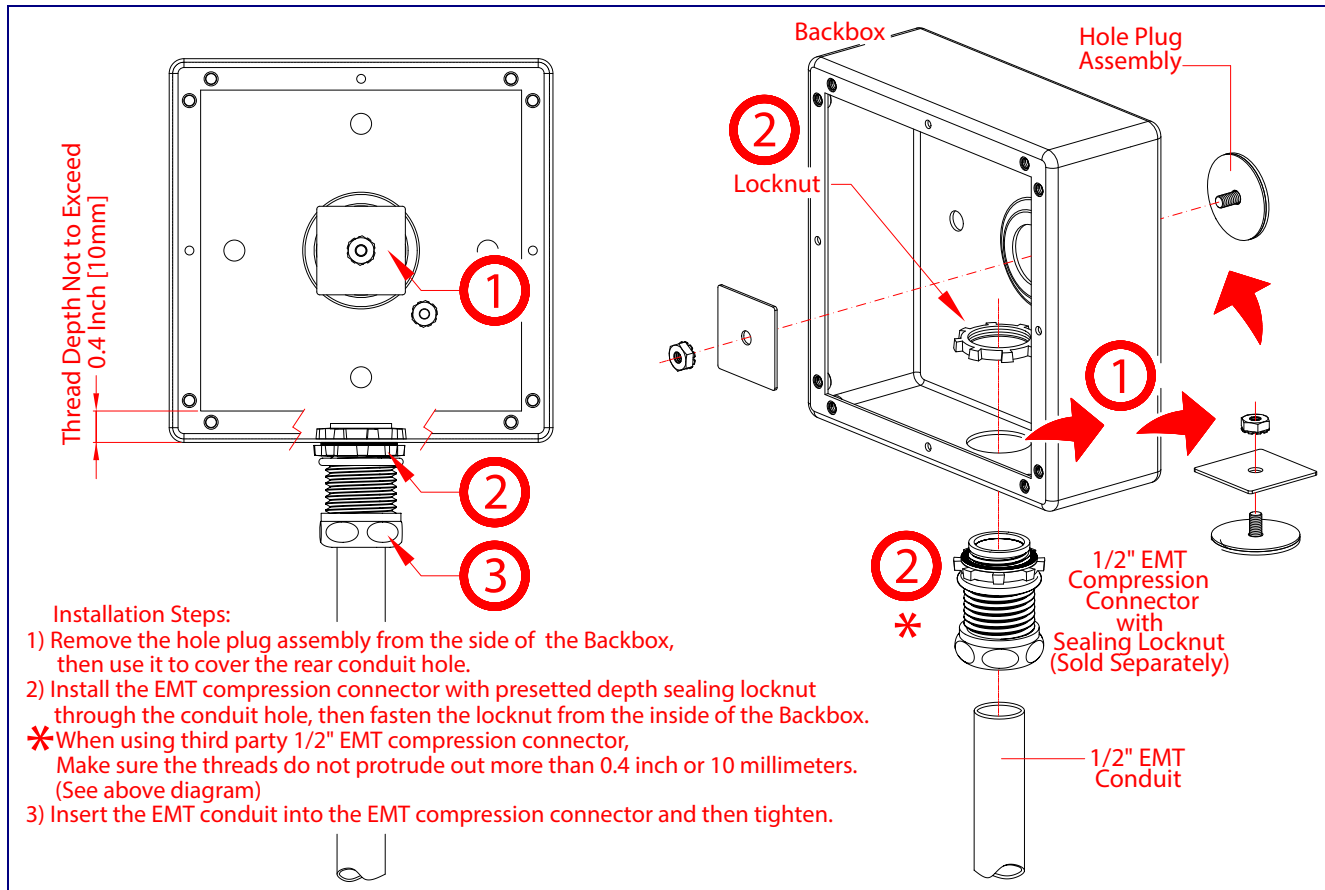


Figure A-4 shows the Side Conduit Mounting for the InformaCast Enabled Outdoor RGB (Multi-Color) Strobe.

Figure A-4. Side Conduit Mounting



# Appendix B: Troubleshooting/Technical Support

---

## B.1 Frequently Asked Questions (FAQ)

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

<https://www.cyberdata.net/products/011489>

---

## B.2 Documentation

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

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

<https://www.cyberdata.net/products/011489>



---

## B.3 Contact Information

Contact	<p>CyberData Corporation 3 Justin Court Monterey, CA 93940 USA <a href="http://www.CyberData.net">www.CyberData.net</a> Phone: 800-CYBERDATA (800-292-3732) Fax: 831-373-4193</p>
Sales	<p>Sales 831-373-2601, Extension 334</p>
Technical Support	<p>The fastest way to get technical support for your VoIP product is to submit a VoIP Technical Support form at the following website:</p> <p><a href="http://support.cyberdata.net/">http://support.cyberdata.net/</a></p> <p>The Support Form initiates a ticket which CyberData uses for tracking customer requests. Most importantly, the Support Form tells us which PBX system and software version that you are using, the make and model of the switch, and other important information. This information is essential for troubleshooting. Please also include as much detail as possible in the <b>Comments</b> section of the Support Form.</p> <p>Phone: (831) 373-2601, Extension 333</p>

---

## 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 7

## A

AC voltages, enclosure is not rated 9  
 activate relay (door sensor) 47  
 activate relay (intrusion sensor) 48  
 activity LED 15  
 address, configuration login 21  
 alternative power input 4  
 audio configuration 50  
 audio configuration page 50  
 audio files, user-created 51  
 autoprovision at time (HHMMSS) 60  
 autoprovision when idle (in minutes > 10) 60  
 autoprovisioning 60, 61  
   download template button 60  
 autoprovisioning autoupdate (in minutes) 60  
 autoprovisioning configuration 59, 60  
 autoprovisioning filename 60  
 autoprovisioning server (IP Address) 60  
 auxiliary relay wiring diagram 10

## B

backup SIP server 1 31  
 backup SIP server 2 31  
 backup SIP servers, SIP server  
   backups 31

## C

changing  
   the web access password 25  
 Cisco SRST 32  
 command interface 74  
 commands 74  
 configurable parameters 26, 29, 31  
 configuration  
   audio 50  
   default IP settings 17  
   door sensor 37, 46  
   intrusion sensor 37, 46  
   network 28

SIP 30  
   using Web interface 17  
 configuration home page 21  
 configuration page  
   configurable parameters 26, 29  
 contact information 81  
 contact information for CyberData 81  
 current network settings 29  
 CyberData contact information 81

## D

default  
   device settings 82  
   gateway 17  
   IP address 17  
   subnet mask 17  
   username and password 17  
   web login username and password 21  
 default gateway 17, 29  
 default intercom settings 16  
 default IP settings 17  
 default login address 21  
 device configuration 25  
   device configuration parameters 60  
   the device configuration page 59  
 device configuration page 25  
 device configuration parameters 26  
 device configuration password  
   changing for web configuration access 25  
 DHCP Client 3  
 dial out extension (door sensor) 47  
 dial out extension (intrusion sensor) 48  
 dial out extension strings 36  
 dimensions 4  
 discovery utility program 21  
 DNS server 29  
 door sensor 46, 47  
   activate relay 47  
   dial out extension 47  
   door open timeout 47  
   door sensor normally closed 47  
 download autoprovisioning template button 60  
 DTMF tones (using rfc2833) 36

## E

enable night ring events 54

- ethernet I/F 4
- event configuration
  - enable night ring events 54
- expiration time for SIP server lease 31, 32, 33
- export settings 23, 24

## F

- factory default settings 16
- firmware
  - where to get the latest firmware 70

## G

- gauge wire (terminal block) 7
- get autoprovisioning template 60

## H

- home page 21
- http POST command 74
- http web-based configuration 3

## I

- identifying your product 1
- illustration of device mounting process 75
- import settings 23, 24
- import/export settings 23, 24
- installation, typical device system 2
- intercom configuration page
  - configurable parameters 31
- intrusion sensor 46, 48
  - activate relay 48
  - dial out extension 48
- IP address 17, 29
- IP addressing
  - default
    - IP addressing setting 17

## L

- lease, SIP server expiration time 31, 32, 33
- LED
  - yellow activity LED 15
- local SIP port 32
- log in address 21

## M

- MGROUP
  - MGROUP Name 44
- mounting
  - optional accessories 75
- mounting the device 75
- multicast configuration 50
- Multicast IP Address 44

## N

- navigation (web page) 18
- navigation table 18
- network configuration 28
- Nightringer 7, 69
- nightringer settings 32
- NTP server 26

## O

- on-board relay 4, 9

## P

- part number 4
- parts list 6
- password
  - for SIP server login 31
  - login 21
  - restoring the default 17
- point-to-point configuration 36
- polycom default channel 44
- polycom emergency channel 44
- polycom priority channel 44
- port
  - local SIP 32
  - remote SIP 32
- POST command 74
- power input 4
  - alternative 4
- product
  - configuring 17
  - mounting 75
  - parts list 6
- product features 3
- product overview
  - product features 3
  - product specifications 4
  - supported protocols 3

- supported SIP servers 3
- typical system installation 2
- product specifications 4
- protocol 4
- protocols supported 3

## R

- reboot 72
- remote SIP port 32
- resetting the IP address to the default 75, 80
- restoring factory default settings 16, 82
- RJ-45 14
- rport discovery setting, disabling 32
- RTFM jumper 16
- RTP/AVP 3

## S

- sales 81
- sensor setup page 37, 46
- sensor setup parameters 37, 46
- sensors 47
- server address, SIP 31
- service 81
- setting up the device 7
- settings, default 16
- SIP
  - enable SIP operation 31
  - local SIP port 32
  - user ID 31
- SIP (session initiation protocol) 3
- SIP configuration 30
- SIP configuration parameters
  - outbound proxy 32
  - registration and expiration, SIP server lease 31, 32, 33
  - unregister on reboot 32
  - user ID, SIP 31
- SIP registration 31
- SIP remote SIP port 32
- SIP server 31
  - password for login 31
  - SIP servers supported 3
  - unregister from 32
  - user ID for login 31
- SIP server configuration 31
- SRST 32
- subnet mask 17, 29
- supported protocols 3

## T

- tech support 81
- technical support, contact information 81
- terminal block connections 7

## U

- user ID
  - for SIP server login 31
- username
  - changing for web configuration access 25
  - default for web configuration access 21
  - restoring the default 17

## V

- VLAN ID 29
- VLAN Priority 29
- VLAN tagging support 29
- VLAN tags 29

## W

- warranty policy at CyberData 81
- web access password 17
- web access username 17
- web configuration log in address 21
- web page
  - navigation 18
- web page navigation 18
- web-based configuration 17
- weight 4
- wget, free unix utility 74
- wire gauge (terminal block) 7