

# *RGB Strobe Operations Guide*

**Part #011376**

Document Part #931212C  
for Firmware Version 11.6.0

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

---

**RGB Strobe Operations Guide 931212C**  
**Part # 011376**

**COPYRIGHT NOTICE:**

© 2016, 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 931212C, which corresponds to firmware version 11.6.0, was released on January 11, 2017, and has the following changes:

- Updates the description for the [Terminate Call After Delay](#) setting in [Table 2-15, "SIP Configuration Parameters"](#) to the following:  
“Automatically terminate an active call after a given delay in seconds. A value of 0 will disable this function. Enter up to 8 digits. This feature only affects outbound calls initiated by sensor events.”

---

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

---

# 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
 <b>Chapter 2 Installing the RGB Strobe</b>	 <b>5</b>
2.1 Parts List .....	5
2.2 RGB Strobe Setup .....	6
2.2.1 RGB Strobe Connections .....	6
2.2.2 Connecting the RGB Strobe to the On-Board Relay .....	7
2.2.3 Identifying the RGB Strobe Connectors and Jumpers .....	9
2.2.4 Link and Activity LEDs .....	12
2.2.5 Restore the Factory Default Settings .....	13
2.3.1 Factory Default Settings .....	14
2.3.2 RGB Strobe Web Page Navigation .....	15
2.3.3 Using the Toggle Help Button .....	16
2.3.4 Log in to the Configuration Home Page .....	18
2.3.5 Configure the Device .....	22
2.3.6 Configure the Network Parameters .....	27
2.3.7 Configure the SIP Parameters .....	30
2.3.8 Configure the Multicast Parameters .....	39
2.3.9 Configure the Sensor Parameters .....	43
2.3.10 Configure the Audiofiles Parameters .....	47
2.3.11 Configure the Event Parameters .....	48
2.3.12 Configure the Autoprovisioning Parameters .....	53
2.4.1 Reboot the Device .....	67
2.5.1 Command Interface Post Commands .....	68
 <b>Appendix A Mounting the RGB Strobe</b>	 <b>69</b>
A.1 Mount the RGB Strobe .....	69
 <b>Appendix B Troubleshooting/Technical Support</b>	 <b>74</b>
B.1 Frequently Asked Questions (FAQ) .....	74
B.2 Documentation .....	74
B.3 Contact Information .....	75
B.4 Warranty and RMA Information .....	75
 <b>Index</b>	 <b>76</b>

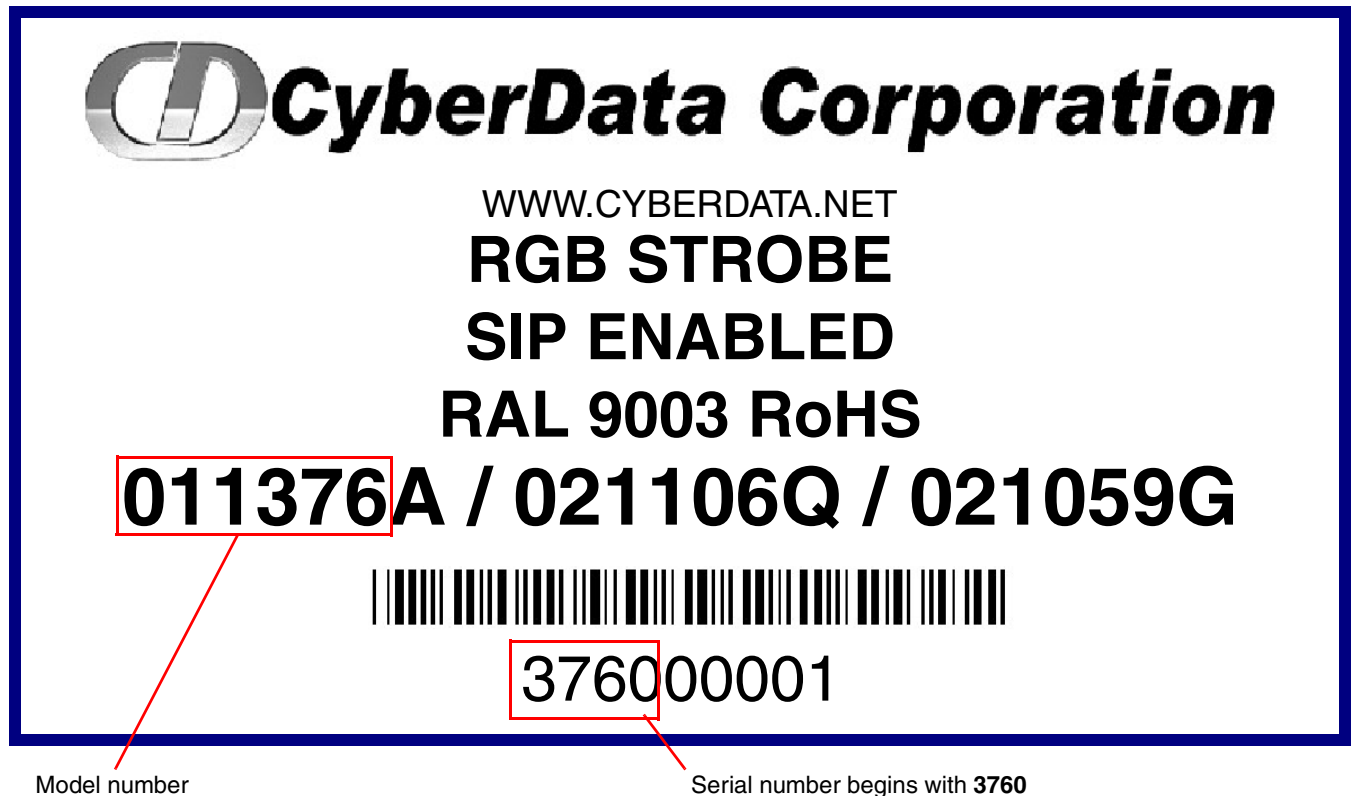
# 1 Product Overview

## 1.1 How to Identify This Product

To identify the RGB 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 011376.
- The serial number on the label should begin with **3760**.

Figure 1-1. Model Number Label



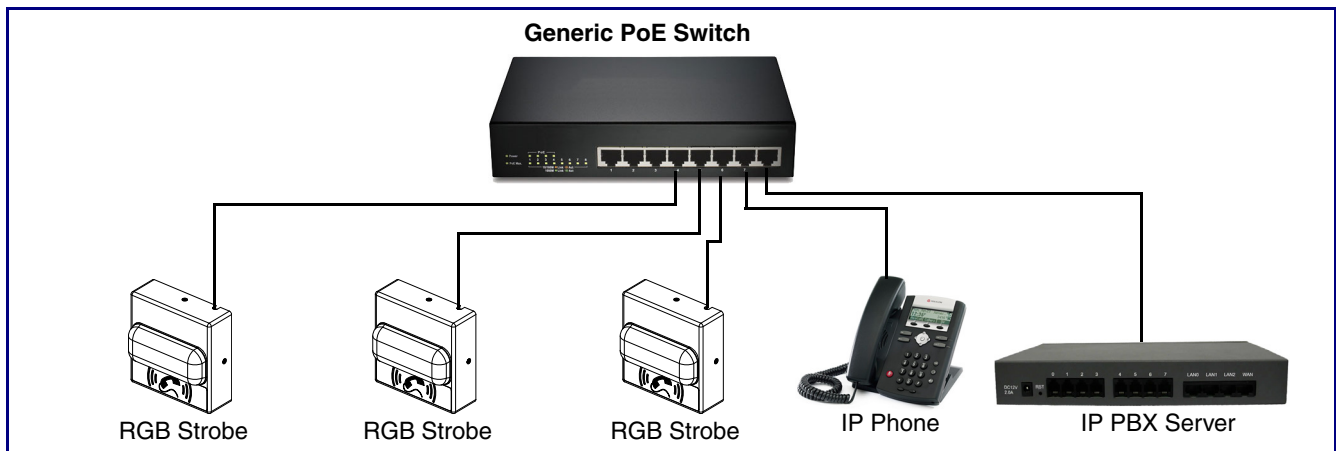


## 1.2 Typical System Installation

The RGB 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 RGB Strobes can be installed as part of a VoIP phone system.

**Figure 1-2. Typical Installation**



---

## 1.3 Product Features

- Meets ADA requirements for telephony signaling and notification
- Five "scenes" with adjustable brightness for each strobe trigger
- Support for 10 multicast addresses
- SIP activation
- Mailbox message waiting indication
- Multicast activation
- Cisco SRST support
- Event-controlled relay
- Tamper sensor
- Web-based setup
- PoE-powered

---

## 1.4 Supported Protocols

The RGB Strobe supports:

- SIP
- HTTP Web-based configuration  
Provides an intuitive user interface for easy system configuration and verification of RGB Strobe operations.
- DHCP Client  
Dynamically assigns IP addresses in addition to the option to use static addressing.
- RTP

---

## 1.5 Supported SIP Servers

Go to the following link to find the RGB Strobe product page which will have information on how to configure the RGB Strobe for various supported SIP servers:

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

## 1.6 Specifications

**Table 1-1. Specifications**

Specifications	
Ethernet I/F	10/100 Mbps
Protocol	SIP RFC 3261 Compatible
Power Input	PoE 802.3af compliant or +8 to +12VDC @ 1000mA Regulated Power Supply <sup>a</sup>
Light power	Up to 90 candela (user-selectable)
Flash rate	5 user-defined scenes
LED MTBF	100,000 Hours
On-Board Relay	1A at 30 VDC
Operating Temperature	-10° C to 50° C (14° F to 122° F)
Dimensions	4.5 inches [115 mm] Length
	2.1 inches [55 mm] Width
	4.5 inches [115 mm] Height
Weight	1.0 lbs. (0.45 kg)
Boxed Weight	2.0 lbs. (0.90 kg)
Part Number	011376

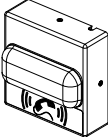


a. Contacts 1 and 2 on the terminal block are only for powering the device from a non-PoE 12VDC power source as an alternative to Network PoE power. Use of these contacts for any other purpose will damage the device and void the product warranty.

# 2 Installing the RGB Strobe

## 2.1 Parts List

Table 2-2 illustrates the RGB Strobe parts.

Table 2-2. Parts List


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

## 2.2 RGB Strobe Setup

### 2.2.1 RGB Strobe Connections

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

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

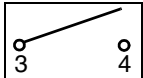
 GENERAL ALERT	<p><b>Caution</b></p> <p><i>Equipment Hazard:</i> Contacts 1 and 2 on the terminal block are only for powering the device from a non-PoE 12 VDC power source as an alternative to Network PoE power. Use of these contacts for any other purpose will damage the device and void the product warranty.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

**Figure 2-1. Connections**

Alternate Power Input:

1 = +8 to +12VDC @ 1000mA Regulated Power Supply\*

2 = Power Ground\*



Relay Contact:

(1 A at 30 VDC for continuous loads)

3 = Relay Common

4 = Relay Normally Open Contact

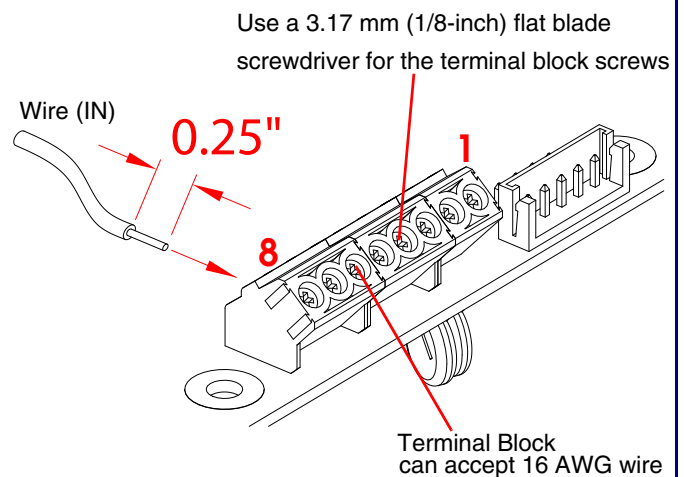
5 = Sense Input

6 = Sense Ground






7 = Reserved for Future Use

8 = Reserved for Future Use

\*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.



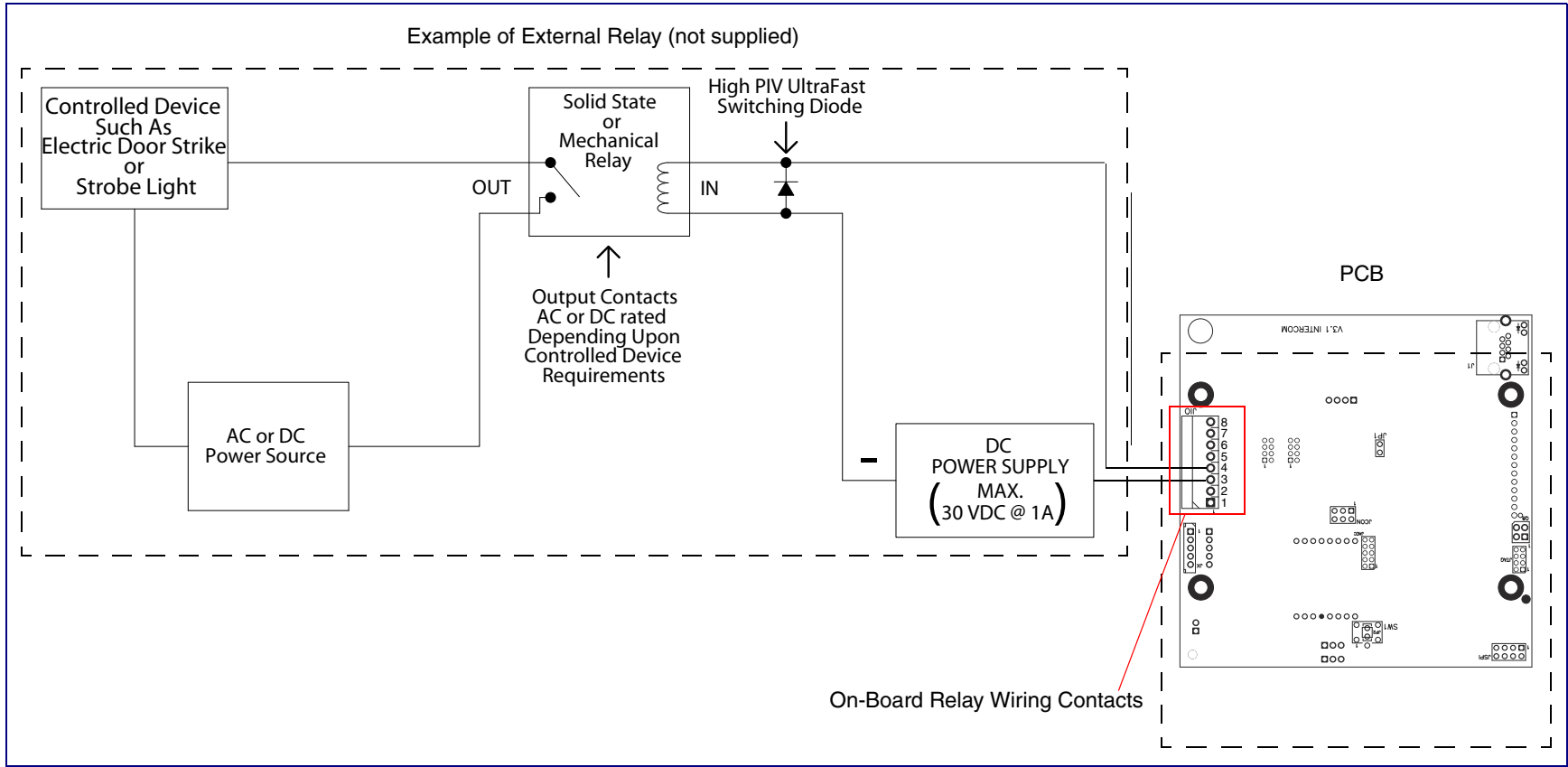
## 2.2.2 Connecting the RGB Strobe to the On-Board Relay

 GENERAL ALERT	<p><b>Warning</b></p> <p><i>Electrical Hazard:</i> The device enclosure is not rated for any AC voltages.</p>
 GENERAL ALERT	<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>
 GENERAL ALERT	<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>
 GENERAL ALERT	<p><b>Warning</b></p> <p><i>Electrical Hazard:</i> The relay contacts are dry and provided for a normally open and momentarily closed configuration. Neither the alternate power input nor PoE power can be used to drive a door strike.</p>
 GENERAL ALERT	<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>

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 RGB 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.

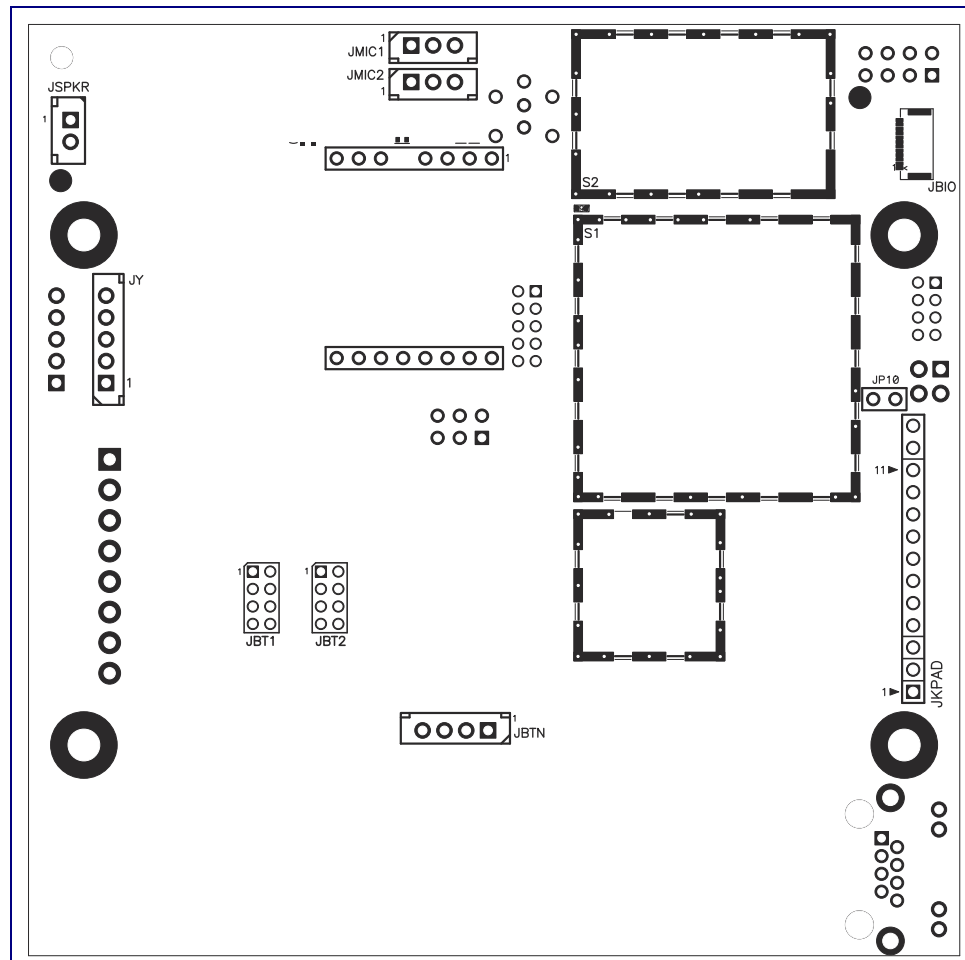
Figure 2-2. Wiring Diagram



## 2.2.3 Identifying the RGB Strobe Connectors and Jumpers

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

**Figure 2-3. Connector Locations**

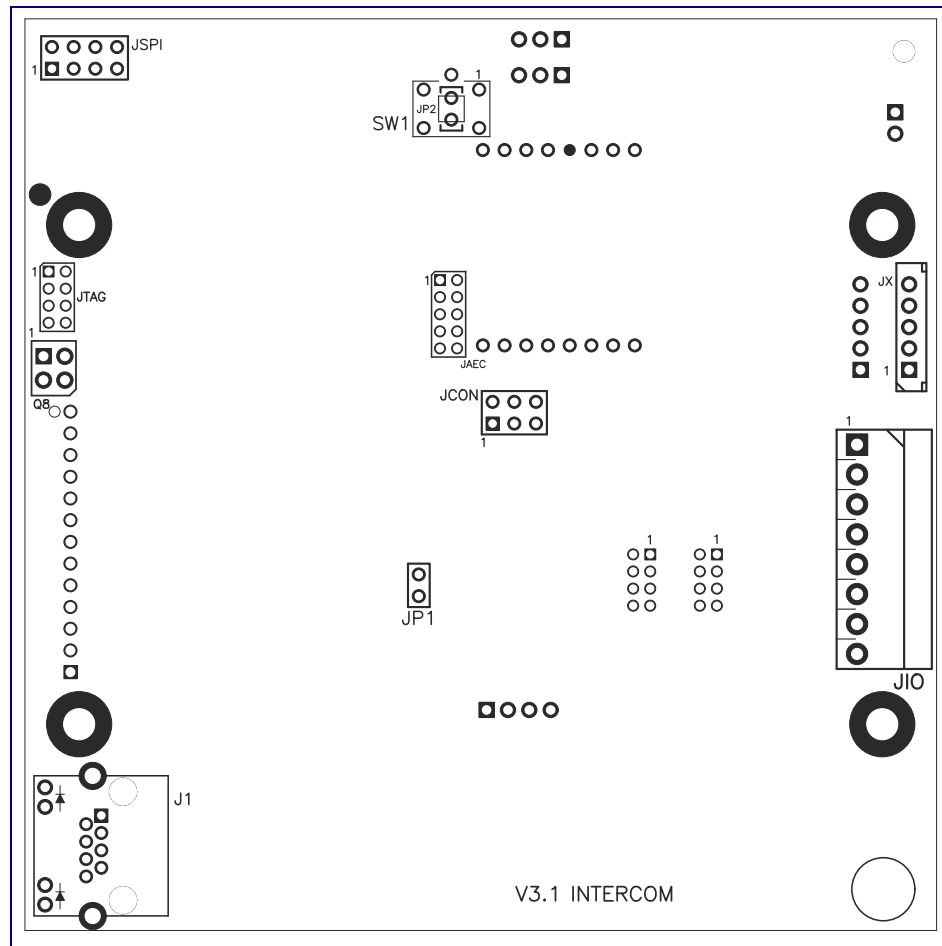


**Table 2-3. Connector Functions**

Connector	Function
JBTN	Call Button LED Interface — Not Used
JM1C1	Microphone Interface — Not Used
JSPKR	Speaker Interface — Not Used
JKPAD	Keypad Interface — Not Used
JX	Auxiliary Strobe Connector — Not Used
JY	Proximity Sensor Interface — Not Used
JP10	Disables the intrusion sensor when installed.
JBT1	Touch Button -1 Interface — Not Used
JBT2	Touch Button -2 Interface — Not Used



**Figure 2-4. Connector Locations**

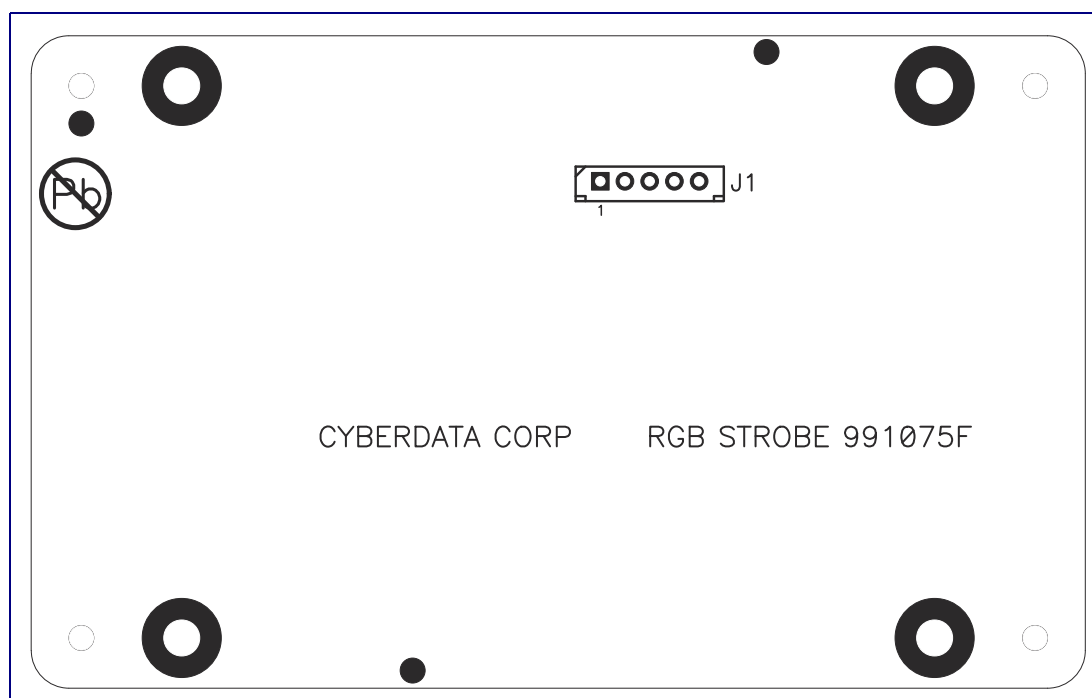


**Table 2-4. Connector Functions**

Connector	Function
JP1	Reset jumper <sup>a</sup>
J1	PoE Network Connection (RJ-45 ethernet)
JAEC	AEC Configuration Interface (Factory Use Only)
JIO	Terminal Block (see <a href="#">Figure 2-1</a> )
JCON	Console Port (Factory Use Only)
JTAG	JTAG (Factory Use Only)
JSPI	Reserved (Factory Use Only)
SW1	See <a href="#">Section 2.2.5.1, "RTFM Button"</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 2-5. Connector Locations for the 021509 Board**



**Table 2-5. Connector Functions**

Connector	Function
J1	Ethernet Connector

---

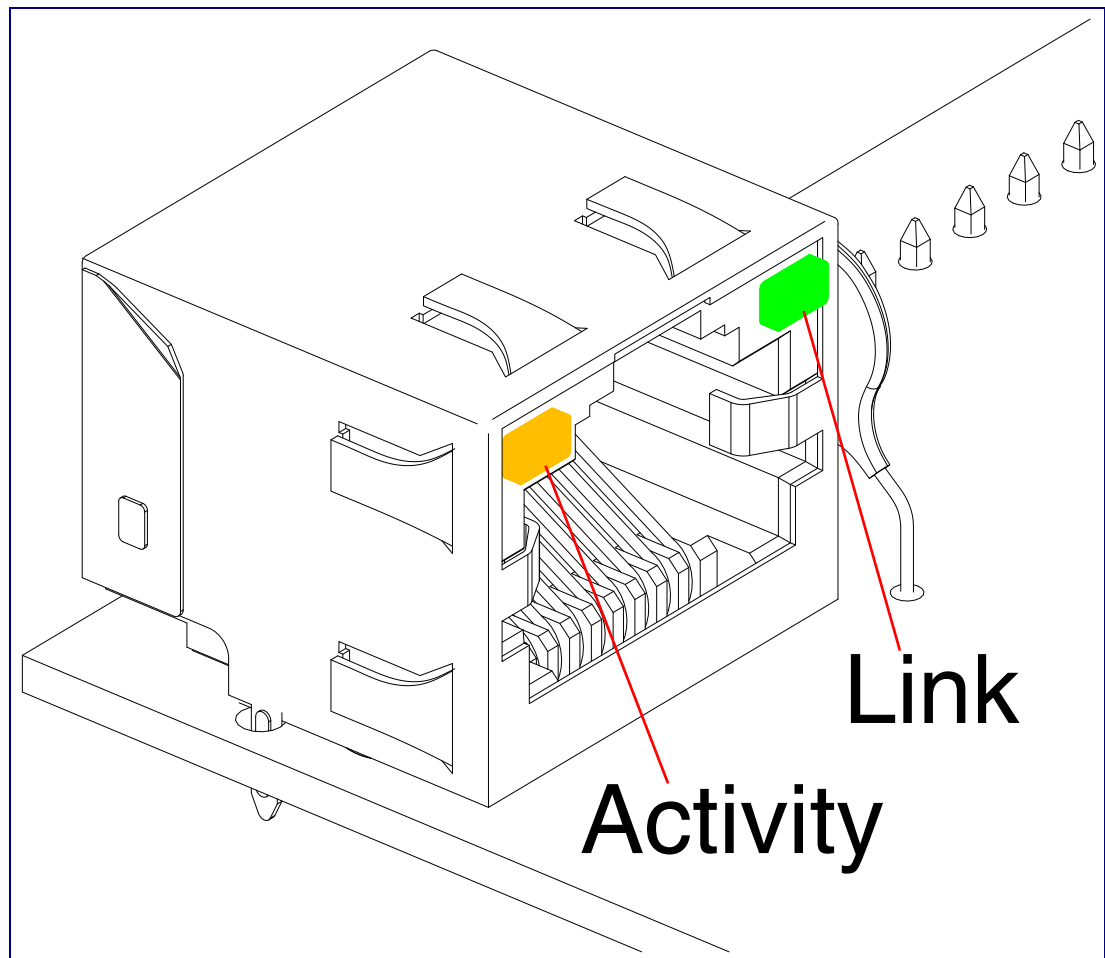
## 2.2.4 Link and Activity LEDs

### 2.2.4.1 Verifying the Network Connectivity and Data Rate

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

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

**Figure 2-6. Link and Activity LEDs**



---

## 2.2.5 Restore the Factory Default Settings

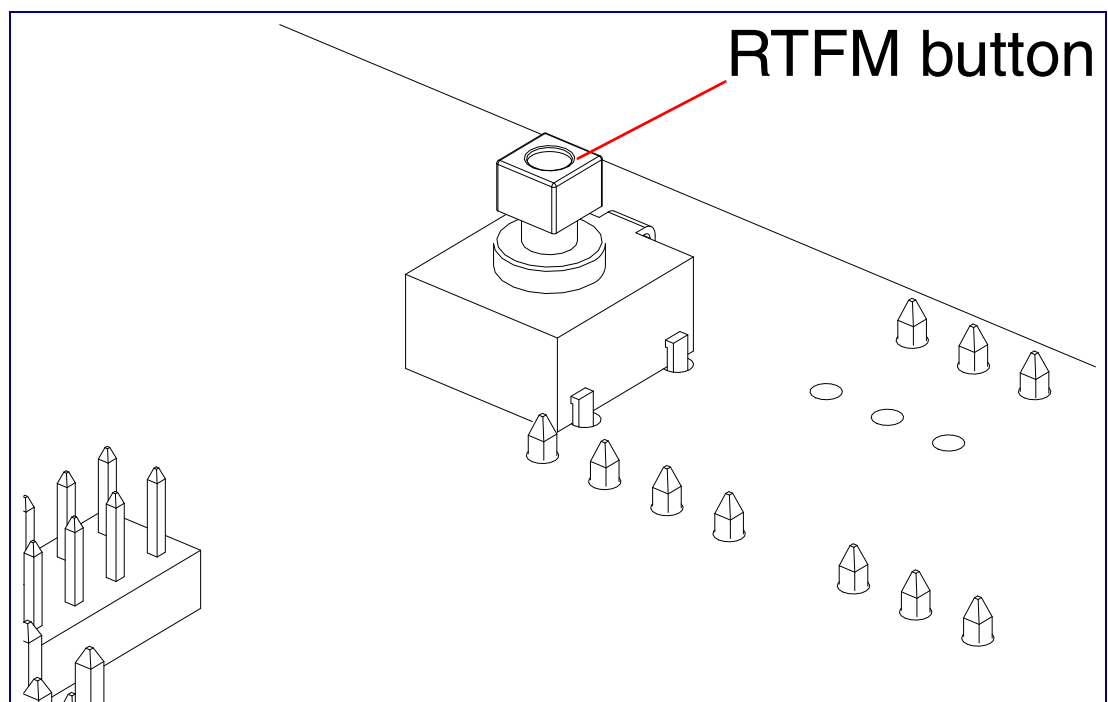
### 2.2.5.1 RTFM Button

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

**Note** Each device is delivered with factory set default values.

**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 2-7. RTFM Button**



To set the factory default settings:

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

---

## 2.3 Configure the RGB Strobe Parameters

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

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

---

### 2.3.1 Factory Default Settings

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

When configuring more than one RGB Strobe, attach the RGB 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

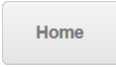
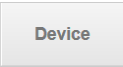
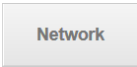



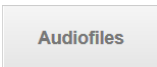
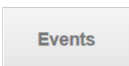
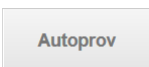
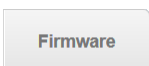
a. Default if there is not a DHCP server present.

---

## 2.3.2 RGB Strobe Web Page Navigation

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

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

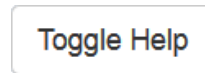
Web Page Item	Description
	Link to the <b>Home</b> page.
	Link to the <b>Device</b> page.
	Link to the <b>Network</b> page.
	Link to go to the <b>SIP</b> page.
	Link to the <b>Multicast</b> page.
	Link to the <b>Sensor</b> page.
	Link to the <b>Audiofiles</b> page.
	Link to the <b>Events</b> page.
	Link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

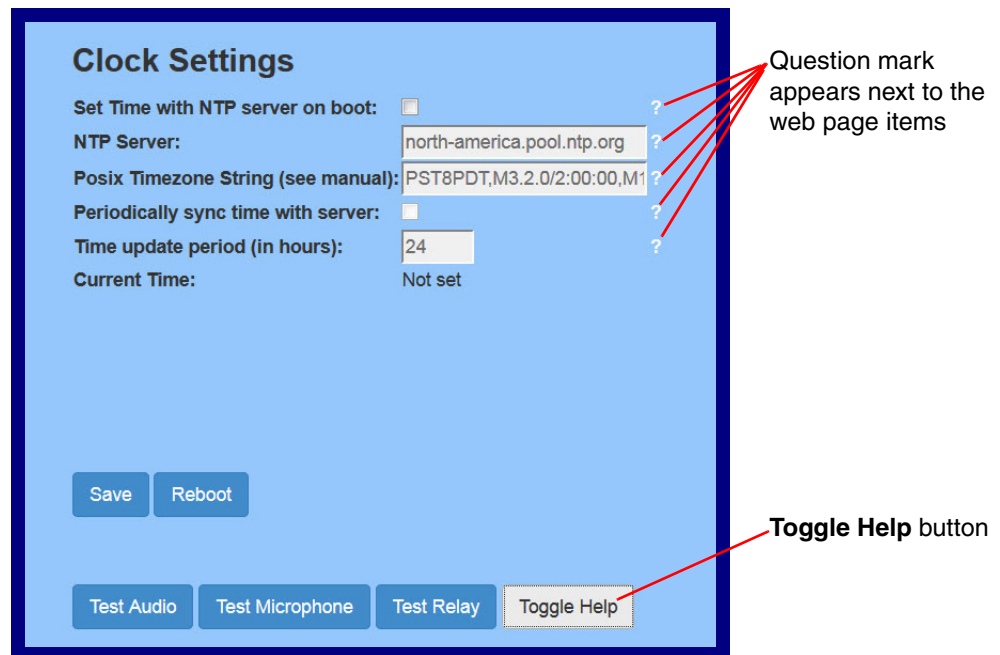
1. Click on the **Toggle Help** button that is on the UI webpage. See [Figure 2-8](#) and [Figure 2-9](#).

**Figure 2-8. Toggle/Help Button**



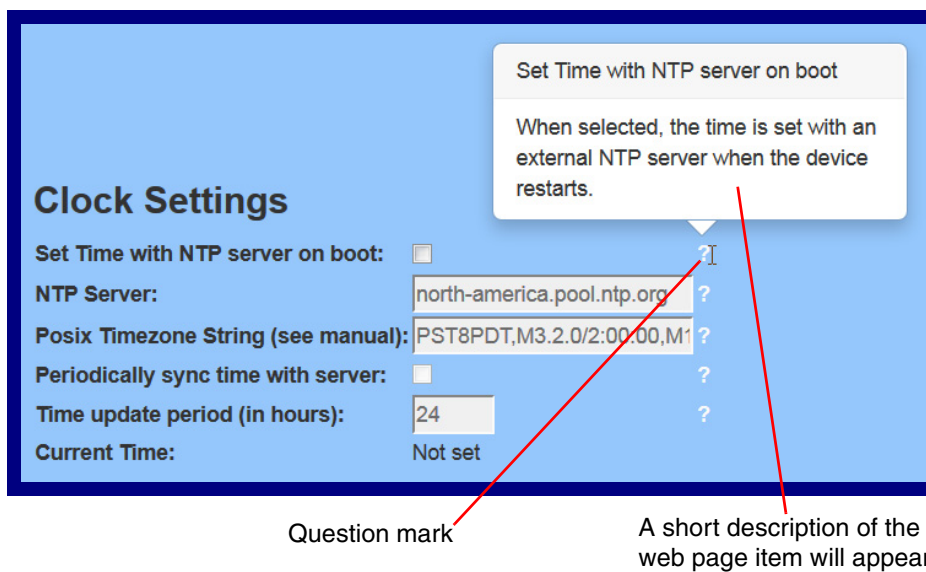
2. You will see a question mark (?) appear next to each web page item that has been provided with a short description by the Help feature. See [Figure 2-9](#).

**Figure 2-9. 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 2-10](#).

**Figure 2-10. Short Description Provided by the Help Feature**





---

## 2.3.4 Log in to the Configuration Home Page

1. Open your browser to the RGB 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 RGB 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 **Downloads** tab on the following webpage:

<http://www.cyberdata.net/voip/011376/>

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

- When prompted, use the following default **Web Access Username** and **Web Access Password** to access the **Home Page** (Figure 2-11):

Web Access Username: **admin**

Web Access Password: **admin**

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

**Figure 2-11. Home Page**

**Home** Device Network SIP Multicast Sensor Audiofiles Events Autoprov Firmware

# CyberData RGB Strobe

### Current Status

Serial Number: 376000001  
Mac Address: 00:20:f7:03:76:9d  
Firmware Version: v11.6.0

IP Addressing: DHCP  
IP Address: 10.10.1.231  
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

### Admin Settings

Username: admin  
Password:  
Confirm Password:

Save Reboot Toggle Help

### Import Settings

Browse... No file chosen  
Import Config

### Export Settings

Export Config

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

**Table 2-8. Home Page Overview**




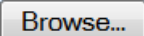







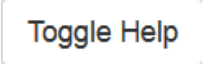
Web Page Item	Description
<b>Admin Settings</b>	
Username 	The username to access the web interface. Enter up to 25 characters.
Password 	The password to access the web interface. Enter up to 25 characters.
Confirm Password 	Confirm the web interface password.
<b>Current Status</b>	
Serial Number	Shows the device serial number.
Mac Address	Shows the device Mac address.
Firmware Version	Shows the current firmware version.
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.
<b>Import Settings</b>	
 	Click <b>Browse</b> to select a configuration file to import.
 	After selecting a configuration file, click <b>Import</b> to import the configuration from the selected file. Then, click Save and Reboot to store changes.
<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. <b>Note:</b> You need to reboot for changes to take effect.
	Click on the <b>Reboot</b> button to reboot the system.

Table 2-8. Home Page Overview (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.

## 2.3.5 Configure the Device

1. Click the **Device Configuration** button to open the **Device Configuration** page. See [Figure 2-12](#).

**Figure 2-12. Device Configuration Page**

Home Device Network SIP Multicast Sensor Audiofiles Events Autoprov Firmware

# CyberData RGB Strobe

### Misc Settings

Device Name: CyberData VoIP RGB Strobe

Disable HTTPS (NOT recommended): ☐

### Relay Settings

Activate Relay During Ring: ☐

Activate Relay During Night Ring: ☐

### Clock Settings

Set Time with NTP server on boot: ☐

NTP Server: north-america.pool.ntp.org

Posix Timezone String (see manual): PST8PDT,M3.2.0/2:00:00,M11.

Periodically sync time with server: ☐

Time update period (in hours): 24

Current Time: 16:11:38

Save Reboot

Test Relay Toggle Help

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

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

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

Web Page Item	Description
<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>Clock Settings</b>	
Set Time with NTP Server on boot ?	When selected, the time is set with an external NTP server when the device restarts.
NTP Server ?	Use this field to set the address (in IPv4 dotted decimal notation or as a canonical name) for the NTP Server. This field can accept canonical names of up to 64 characters in length.
Posix Timezone String ?	See <a href="#">Section 2.3.5.1, "Time Zone Strings"</a> for information about how to use the Posix Timezone String to specify time zone and daylight savings time where applicable. Enter up to 63 characters.
Periodically sync time with server ?	When selected, the time is periodically updated with the NTP server at the configured interval below.
Time update period (in hours) ?	The time interval after which the device will contact the NTP server to update the time. Enter up to 4 digits.
Current Time	Allows you to input the current time. (6 character limit)

**Table 2-9. Device Configuration Parameters (continued)**

Web Page Item	Description
<b>Relay Settings</b>	
Activate Relay During Ring ?	When selected, the relay will be activated for as long as the device is ringing. When Auto-Answer Incoming Calls is enabled, the device will not ring and this option does nothing.
Activate Relay During Night Ring ?	When selected, the relay will be activated as long as the Nightringer extension is ringing.
<b>Save</b>	Click the <b>Save</b> button to save your configuration settings. <b>Note:</b> You need to reboot for changes to take effect.
<b>Reboot</b>	Click on the <b>Reboot</b> button to reboot the system.
<b>Test Relay</b>	Click on the <b>Test Relay</b> button to do a relay test.
<b>Toggle Help</b>	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** You must click on the **Save** button and then the **Reboot** button for the changes to take effect.

### 2.3.5.1 Time Zone Strings

The posix time zone string tells the internal date and time utilities how to handle daylight savings time for different time zones. Table 2-10 shows some common strings.

**Table 2-10. Common Time Zone Strings**

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

<sup>a</sup>.Phoenix, Arizona does not use daylight savings time.

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

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

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

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

Time Zone String Examples

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

**Table 2-12. Time Zone String Examples**

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

a.Tokyo does not use daylight savings time.

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

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

**Figure 2-13. Three or Four Character Time Zone Identifier**

You can also use the following URL when a certain time zone applies daylight savings time:

<http://www.timeanddate.com/time/dst/2011.html>



World GMT Table [Table 2-13](#) has information about the GMT time in various time zones.

**Table 2-13. World GMT Table**

<b>Time Zone</b>	<b>City or Area Zone Crosses</b>
GMT-12	Eniwetok
GMT-11	Samoa
GMT-10	Hawaii
GMT-9	Alaska
GMT-8	PST, Pacific US
GMT-7	MST, Mountain US
GMT-6	CST, Central US
GMT-5	EST, Eastern US
GMT-4	Atlantic, Canada
GMT-3	Brazilia, Buenos Aries
GMT-2	Mid-Atlantic
GMT-1	Cape Verdes
GMT	Greenwich Mean Time, Dublin
GMT+1	Berlin, Rome
GMT+2	Israel, Cairo
GMT+3	Moscow, Kuwait
GMT+4	Abu Dhabi, Muscat
GMT+5	Islamabad, Karachi
GMT+6	Almaty, Dhaka
GMT+7	Bangkok, Jakarta
GMT+8	Hong Kong, Beijing
GMT+9	Tokyo, Osaka
GMT+10	Sydney, Melbourne, Guam
GMT+11	Magadan, Soloman Is.
GMT+12	Fiji, Wellington, Auckland

## 2.3.6 Configure the Network Parameters

1. Click the **Networking** button to open the **Network Configuration** page (Figure 2-14).

Figure 2-14. Network Configuration Page

**CyberData RGB Strobe**

**Stored Network Settings**

Addressing Mode: ☒ Static ☐ DHCP

Hostname:

IP Address:

Subnet Mask:

Default Gateway:

DNS Server 1:

DNS Server 2:

DHCP Timeout in seconds\*:

\* A value of -1 will retry forever

**VLAN Settings**

VLAN ID (0-4095):

VLAN Priority (0-7):

**Current Network Settings**

IP Address: 10.10.1.252

Subnet Mask: 255.0.0.0

Default Gateway: 10.0.0.1

DNS Server 1: 10.0.1.56

DNS Server 2:



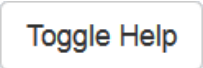
2. On the **Network Configuration** page, enter values for the parameters indicated in [Table 2-14](#).

**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. 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.
DHCP Timeout in seconds ?	Specify the desired time-out duration (in seconds) that the device will wait for a response from the DHCP server before reverting back to the stored static IP address. The stored static IP address may be the last known IP address or the factory default address if no prior DHCP lease was established. Enter up to 8 characters. A value of -1 will retry forever.
<b>VLAN Settings</b>	
VLAN ID (0-4095) ?	Specify the IEEE 802.1Q VLAN ID number. Enter up to 4 digits.  <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.
<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.

Table 2-14. Network Configuration Parameters (continued)

Web Page Item	Description
	Click the <b>Save</b> button to save your configuration settings. <b>Note:</b> You need to reboot for changes to take effect.
	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** You must click on the **Save** button and then the **Reboot** button for the changes to take effect.

## 2.3.7 Configure the SIP Parameters

1. Click **SIP Config** to open the **SIP Configuration** page (Figure 2-15).

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

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

Figure 2-15. SIP Configuration Page

**SIP Settings**

Enable SIP operation: ☒  
Register with a SIP Server: ☒  
Use Cisco SRST: ☐  
Primary SIP Server: 10.0.0.253  
Primary SIP User ID: 199  
Primary SIP Auth ID: 199  
Primary SIP Auth Password: \*\*\*\*\*  
Backup SIP Server 1:   
Backup SIP User ID 1:   
Backup SIP Auth ID 1:   
Backup SIP Auth Password 1:   
Backup SIP Server 2:   
Backup SIP User ID 2:   
Backup SIP Auth ID 2:   
Backup SIP Auth Password 2:   
Remote SIP Port: 5060  
Local SIP Port: 5060  
Outbound Proxy:   
Outbound Proxy Port: 0  
Disable rport Discovery: ☐  
Re-registration Interval (in seconds): 360  
Unregister on Boot: ☐  
Keep Alive Period: 10000

**SIP Strobe Settings**

Blink Strobe on Ring: ☐  
Scene Color Brightness Red Green Blue  
ADA White 100 0 0 0 Preview

**MWI Strobe Settings**

Blink Strobe on MWI: ☐  
Scene Color Brightness Red Green Blue  
ADA White 100 0 0 0 Preview

**Nightringer Settings**

Enable Nightringer: ☐  
SIP Server: 10.0.0.253  
Remote SIP Port: 5060  
Local SIP Port: 5061  
Outbound Proxy:   
Outbound Proxy Port: 0  
User ID: 241  
Authenticate ID: 241  
Authenticate Password: \*\*\*\*\*  
Re-registration Interval (in seconds): 360

**Nightringer Strobe Settings**

Blink Strobe on Nightring: ☐  
Scene Color Brightness Red Green Blue  
ADA White 100 0 0 0 Preview

**Call Disconnection**

Terminate Call after delay: 0

**Codec Selection**

Force Selected Codec: ☐  
Codec: PCMU (G.711, u-law)

**RTP Settings**

RTP Port (even): 10500

Save Reboot Toggle Help

2. On the **SIP Configuration** page, enter values for the parameters indicated in [Table 2-15](#).

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



**Table 2-15. 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 2.3.7.2, "Point-to-Point Configuration"</a> ).
Use Cisco SRST ?	When enabled, the backup servers are handled according to Cisco SRST (Survivable Remote Site Telephony). It is required for use in clustered Cisco Unified Communications Manager topologies.
Primary SIP Server ?	Enter the SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the primary SIP server. This field can accept entries of up to 255 characters in length.
Primary SIP User ID ?	Specify the SIP User ID for the Primary SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the primary SIP server. Enter up to 64 alphanumeric characters.
Primary SIP Auth ID ?	Specify the Authenticate ID for the Primary SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Primary SIP Auth Password ?	Specify the Authenticate Password for the Primary SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Server 1 ?	Enter the backup SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the backup SIP server. This field can accept entries of up to 255 characters in length.
Backup SIP User ID 1 ?	Specify the SIP User ID for the first backup SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the first backup SIP server. Enter up to 64 alphanumeric characters.
Backup SIP Auth ID 1 ?	Specify the Authenticate ID for the first backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Auth Password 1 ?	Specify the Authenticate Password for the first backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Server 2 ?	Enter a second backup SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the second backup SIP server. This field can accept entries of up to 255 characters in length.
Backup SIP User ID 2 ?	Specify the SIP User ID for the second backup SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the second backup SIP server. Enter up to 64 alphanumeric characters.

**Table 2-15. SIP Configuration Parameters (continued)**

Web Page Item	Description
Backup SIP Auth ID 2 ?	Specify the Authenticate ID for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Auth Password 2 ?	Specify the Authenticate Password for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Remote SIP Port ?	The Remote SIP Port is the port number the device will use as the destination port when sending SIP messages. The default Remote SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
Local SIP Port ?	The Local SIP Port is the port number the device will use to receive SIP messages. The default Local SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
Outbound Proxy ?	Enter the Outbound Proxy address as an IPv4 address in dotted decimal notation or a fully qualified domain name (FQDN). When an IP address is configured, the device will send all SIP messages to this IP address. When an FQDN is configured, the device will run DNS NAPTR, SRV, and A queries on the FQDN to resolve an IP address to which it will send all SIP messages. This field can accept entries of up to 255 characters in length.
Outbound Proxy Port ?	The Outbound Proxy Port is port number used as the destination port when sending SIP messages to the outbound proxy. A value of 0 will default to 5060. The supported range is 0-65536. Enter up to 5 digits.
Disable rport Discovery ?	Disabling rport Discovery will prevent the device from including the public WAN IP address and port number in the contact information that is sent to the remote SIP servers. This will generally only need to be enabled when using an SBC or SIP ALG in conjunction with a remote SIP server.
Re-registration Interval (in seconds) ?	The SIP Re-registration interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
Unregister on Boot ?	When enabled, the device will send one registration with an expiry of 0 on boot.
Keep Alive Period ?	The minimum time in milliseconds between keep-alive packets sent for nat traversal. A value of 0 will disable keep alive packets.
<b>SIP Strobe Settings</b>	
Blink Strobe on Ring ?	When selected, the Strobe will blink a scene when ringing.
Scene ?	Use this setting to choose a scene (strobe flashing behavior).
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.
Off ?	The strobe will not blink.

Table 2-15. SIP Configuration Parameters (continued)








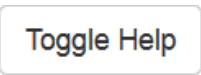

Web Page Item	Description
Color ?	Select desired color for SIP (only one may be chosen).
Brightness ?	How bright the strobe will blink when there is a SIP Call. This is the maximum brightness for “fade” type scenes.
Red ?	The red LED value for SIP Call.
Green ?	The green LED value for SIP Call.
Blue ?	The blue LED value for SIP Call.
	Use this button to preview the strobe flashing behavior for the <b>SIP 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 ?	Use this setting to choose a scene (strobe flashing behavior).
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.
Off ?	The strobe will not blink.
Color	Select desired color (only one may be chosen).
Brightness	How bright the strobe will blink when a message is waiting [0 - 100]. 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.
	Click on the Preview button to see the strobe blink the selected scene.
<b>Nightringer Settings</b>	
Enable Nightringer ?	When Nightringer is enabled, the device will attempt to register a second extension with the SIP server. Any calls made to this extension will play a ringtone (corresponds to <b>Night Ring</b> on the <b>Audiofiles</b> page). By design, it is not possible to answer a call to the Nightringer extension.
SIP Server ?	Enter the SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's Nightringer extension on the SIP server. This field can accept entries of up to 255 characters in length.



**Table 2-15. SIP Configuration Parameters (continued)**

Web Page Item	Description
Remote SIP Port ?	The Remote SIP Port is the port number the device will use as the destination port when sending SIP messages for the Nightringer extension. The default Remote SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
Local SIP Port ?	The Local SIP Port is the port number the device will use to receive SIP messages for the Nightringer extension. This value cannot be the same as the <b>Local SIP Port</b> for the primary extension. The default Local SIP Port is 5061. The supported range is 0-65536. Enter up to 5 digits.
Outbound Proxy ?	Enter the Outbound Proxy address as an IPv4 address in dotted decimal notation or a fully qualified domain name (FQDN). When an IP address is configured, the device will send all SIP messages to this IP address for the Nightringer extension. When an FQDN is configured, the device will run DNS NAPTR, SRV, and A queries on the FQDN to resolve an IP address to which it will send all SIP messages for the Nightringer extension. This field can accept entries of up to 255 characters in length.
Outbound Proxy Port ?	The Outbound Proxy Port is port number used as the destination port when sending SIP messages to the outbound proxy for the Nightringer extension. A value of 0 will default to 5060. The supported range is 0-65536. Enter up to 5 digits.
User ID ?	Specify the SIP User ID for the SIP server. This parameter becomes the user portion of the SIP-URI for the device's Nightringer extension. Enter up to 64 alphanumeric characters.
Authenticate ID ?	Specify the Authenticate ID for the SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Authenticate Password ?	Specify the Authenticate Password for the SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Re-registration Interval (in seconds) ?	The SIP Re-registration Interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
<b>Nightringer Strobe Settings</b>	Use this section to select the strobe flashing behavior for the <b>Nightringer</b> event.
Blink Strobe on Nightring ?	When selected, the Strobe will blink a scene when the Nightringer is ringing.
Scene ?	Use this setting to choose a scene (strobe flashing behavior).
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.
Off ?	The strobe will not blink.
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.

**Table 2-15. SIP Configuration Parameters (continued)**

Web Page Item	Description
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. This feature only affects outbound calls initiated by sensor events.
<b>Codec Selection</b>	
Force Selected Codec	When configured, this option will allow you to force the device to negotiate for the selected codec. Otherwise, the device will perform codec negotiation using the default list of supported codecs.
Codec	Select 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.
	Click the <b>Save</b> button to save your configuration settings. <b>Note:</b> You need to reboot for changes to take effect.
	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** You must click on the **Save** button and then the **Reboot** button for the changes to take effect.

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

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

### 2.3.7.1 Dial Out Extension Strings and DTMF Tones (using rfc2833)

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

**Table 2-16. Examples of Dial-Out Extension Strings**

Extension String	Resulting Action
302	Dial out extension 302 and establish a call

**Table 2-16. Examples of Dial-Out Extension Strings**

<b>Extension String</b>	<b>Resulting Action</b>
302,2	Dial out extension 302 and establish a call, wait 3 seconds then send the DTMF tone '2'
302,25,,,4,,1	Dial out extension 302 and establish a call, wait 3 seconds then send the DTMF tone '2', send out DTMF tone 5, wait 6 seconds, send out DTMF tone 4, wait 4 seconds, send out DTMF tone 1

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

### 2.3.7.2 Point-to-Point Configuration

When the device is set to not register with a SIP server (see [Figure 2-16](#)), 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 2-16. SIP Page Set to Point-to-Point Mode**

Home Device Network **SIP** Multicast Sensor Audiofiles Events Autoprovisioning Firmware

## CyberData RGB Strobe

### SIP Settings

Enable SIP operation: ☒

Register with a SIP Server: ☐

Use Cisco SRST: ☐

Primary SIP Server: 10.0.0.253

Primary SIP User ID: 199

Primary SIP Auth ID: 199

Primary SIP Auth Password: \*\*\*\*\*

Backup SIP Server 1:

Backup SIP User ID 1:

Backup SIP Auth ID 1:

Backup SIP Auth Password 1:

Backup SIP Server 2:

Backup SIP User ID 2:

Backup SIP Auth ID 2:

Backup SIP Auth Password 2:

Remote SIP Port: 5060

Local SIP Port: 5060

Outbound Proxy:

Outbound Proxy Port: 0

Disable rport Discovery: ☐

Re-registration Interval (in seconds): 360

Unregister on Boot: ☐

Keep Alive Period: 10000

### SIP Strobe Settings

Blink Strobe on Ring: ☐

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

Preview

### MWI Strobe Settings

Blink Strobe on MWI: ☐

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

Preview

### Nightringer Settings

Enable Nightringer: ☐

SIP Server: 10.0.0.253

Remote SIP Port: 5060

Local SIP Port: 5061

Outbound Proxy:

Outbound Proxy Port: 0

User ID: 241

Authenticate ID: 241

Authenticate Password: \*\*\*\*\*

Re-registration Interval (in seconds): 360

### Nightringer Strobe Settings

Blink Strobe on Nightringer: ☐

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

Preview

### Call Disconnection

Terminate Call after delay: 0

### Codec Selection

Force Selected Codec: ☐

Codec: PCMU (G.711, u-law)

### RTP Settings

RTP Port (even): 10500

Save Reboot Toggle Help

Device is set to NOT register with a SIP server

### 2.3.7.3 Delayed DTMF

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

**Table 2-17. Examples of Dial-Out Extension Strings**

Extension String	Resulting Action
302	Dial out extension 302 and establish a call
302,2	Dial out extension 302 and establish a call, wait 3 seconds then send the DTMF tone '2'
302,25,,,4,,1	Dial out extension 302 and establish a call, wait 3 seconds then send the DTMF tone '2', send out DTMF tone 5, wait 6 seconds, send out DTMF tone 4, wait 4 seconds, send out DTMF tone 1

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

---

## 2.3.8 Configure the Multicast Parameters

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

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

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

**Note** The RGB Strobe does not play audio, but the Strobe LED will light up in whatever pattern is selected in the [Multicast Strobe Settings](#) on the [Multicast Configuration Page](#).

1. Click on the **Multicast** menu button to open the **Multicast** page. See [Figure 2-17](#).

**Figure 2-17. Multicast Configuration Page**

Home
Device
Network
SIP
Multicast
Sensor
Audiofiles
Events
Autoprov
Firmware

# CyberData RGB Strobe

## Multicast Settings

Enable Multicast Operation: ☒

Priority	Address	Port	Name	Relay	Scene	Color	Brightness	Red	Green	Blue	
9	239.168.3.10	11000	Emergency	<input type="checkbox"/>	ADA	White	100	0	0	0	Preview
8	239.168.3.9	10000	MG8	<input type="checkbox"/>	Slow Fade	Red	60	255	0	0	Preview
7	239.168.3.8	9000	MG7	<input type="checkbox"/>	Fast Fade	Green	100	0	255	0	Preview
6	239.168.3.7	8000	MG6	<input type="checkbox"/>	Slow Blink	Blue	40	0	0	255	Preview
5	239.168.3.6	7000	MG5	<input type="checkbox"/>	Fast Fade	Yellow	80	255	255	0	Preview
4	239.168.3.5	6000	MG4	<input type="checkbox"/>	Fast Blink	Violet	75	255	0	255	Preview
3	239.168.3.4	5000	MG3	<input type="checkbox"/>	Off	White	100	0	255	255	Preview
2	239.168.3.3	4000	MG2	<input type="checkbox"/>	Fast Fade	Cyan	10	0	255	255	Preview
1	239.168.3.2	3000	MG1	<input type="checkbox"/>	Slow Fade	Custom	35	50	75	50	Preview
0	239.168.3.1	2000	Background Music	<input type="checkbox"/>	Slow Blink	White	90	0	0	0	Preview

Polycorn Default Channel  
Polycorn Priority Channel  
Polycorn Emergency Channel

1  
24  
25

Blue  
Yellow  
Violet  
Cyan  
Custom  
White

SIP calls are considered priority 4.5

Port range can be from 2000-65535

Ports must be even numbers

Priority 9 is the highest and 0 is the lowest

A higher priority stream will always supersede a lower one

\* You need to reboot for changes to take effect

Save
Reboot
Toggle Help

2. On the **Multicast** page, enter values for the parameters indicated in [Table 2-18](#).




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

**Table 2-18. Multicast Configuration 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 2.3.8.1, "Assigning Priority"</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 multicast audio is sent.
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.
<b>Multicast Strobe Settings</b>	Use this section to select the strobe flashing behavior for the <b>Multicast</b> event.
Scene ?	Use this setting to choose a scene (strobe flashing behavior).
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.
Off ?	The strobe will not blink.
Color ?	Select desired color (only one may be chosen).
Brightness ?	How bright the strobe will blink for the multicast event. This is the maximum brightness for "fade" type scenes.
Red ?	The red LED value for the multicast event.
Green ?	The green LED value for the multicast event.
Blue ?	The blue LED value for the multicast event.



Table 2-18. Multicast Configuration Parameters (continued)

Web Page Item	Description
	Click on the <b>Preview</b> button to see the strobe blink the selected scene.
	Click the <b>Save</b> button to save your configuration settings. <b>Note:</b> You need to reboot for changes to take effect.
	Click on the <b>Reboot</b> button to reboot the system.

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

### 2.3.8.1 Assigning Priority

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

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

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

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

Ringtones and  
Nightringtones

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

## 2.3.9 Configure the Sensor 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 RGB Strobe board and will be activated when the RGB Strobe is removed from the case.

Each sensor can trigger the following actions:

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

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

1. Click the **Sensor** menu button to open the **Sensor** page (Figure 2-18).

Figure 2-18. Sensor Configuration Page

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

# CyberData RGB Strobe

### Door Sensor Settings

Door Sensor Normally Closed: ☒ Yes ☐ No  
Door Open Timeout (in seconds):   
Activate Relay: ☐  
Make call to extension: ☐  
Dial Out Extension:   
Dial Out ID:

### Intrusion Sensor Settings

Activate Relay: ☐  
Make call to extension: ☐  
Dial Out Extension:   
Dial Out ID:

### Sensor Strobe Settings

Blink Strobe on Sensor: ☐

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

Preview

Save Reboot Toggle Help

Test Door Sensor Test Intrusion Sensor

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

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

**Table 2-19. 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.
<b>Sensor Strobe Settings</b>	
Blink Strobe on Sensor ?	When selected, the Strobe will blink a scene when the sensor is triggered.
Scene ?	Use this setting to choose a scene (strobe flashing behavior).
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.
Off ?	The strobe will not blink.
Color ?	Select desired color (only one may be chosen).
Brightness ?	How bright the strobe will blink for the sensor event. This is the maximum brightness for "fade" type scenes.
Red ?	The red LED value for the sensor event.
Green ?	The green LED value for the sensor event.

Table 2-19. Sensor Configuration Parameters (continued)








Web Page Item	Description
Blue ?	The blue LED value for the sensor event.
	Click on the <b>Preview</b> button to see the strobe blink the selected scene.
<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.
<b>Intrusion Sensor Strobe Settings</b>	Use this section to select the strobe flashing behavior for the <b>Intrusion Sensor</b> event.
Blink Strobe on Intrusion Sensor ?	When selected, the Strobe will blink a scene when the intrusion sensor is triggered.
Scene ?	Use this setting to choose a scene (strobe flashing behavior).
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.
Off ?	The strobe will not blink.
Color ?	Select desired color (only one may be chosen).
Brightness ?	How bright the strobe will blink for the intrusion sensor event. This is the maximum brightness for "fade" type scenes.
Red ?	The red LED value for the intrusion sensor event.
Green ?	The green LED value for the intrusion sensor event.
Blue ?	The blue LED value for the intrusion sensor event.
	Click on the <b>Preview</b> button to see the strobe blink the selected scene.

Table 2-19. 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. <b>Note:</b> You need to reboot for changes to take effect.
	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.

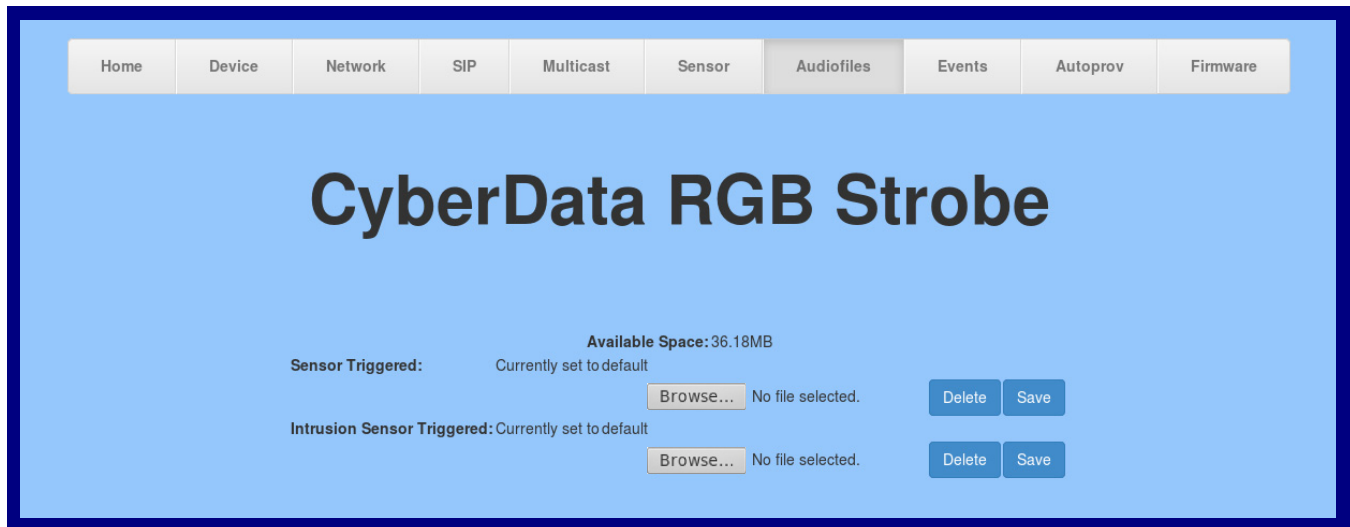
**Note** You must click on the **Save** button and then the **Reboot** button for the changes to take effect.

## 2.3.10 Configure the Audiofiles Parameters

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

1. Click on the **Audiofiles** menu button to open the **Audiofiles** page (Figure 2-19).




Figure 2-19. Audiofiles Configuration Page



2. On the **Audiofiles** page, enter values for the parameters indicated in Table 2-20.

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

Table 2-20. 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.
Sensor Triggered	Corresponds to the message "Sensor Triggered" (24 character limit).
Intrusion Sensor Triggered	Corresponds to the message "Intrusion Sensor Triggered" (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 Configure the Event Parameters

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

1. Click on the **Events** menu button to open the **Events** page (Figure 2-20).

Figure 2-20. Event Configuration Page

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

# CyberData RGB 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 Security Events: ☒  
Enable 60 Second Heartbeat: ☒  
[Check All](#) [Uncheck All](#)

## 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 2-21](#).



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

**Table 2-21. 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. A Ring Event will not be generated when <b>Auto-Answer Incoming Calls</b> is enabled on the <b>Device</b> page.
Enable Night Ring Events ?	When selected, the device will report when it starts ringing upon an incoming SIP call to the Nightringer extension. As a reminder, the Nightringer extension always rings upon an incoming SIP call and it is not possible to alter this behavior.
Enable Multicast Start Events ?	When selected, the device will report when the device starts playing a multicast audio stream.
Enable Multicast Stop Events ?	When selected, the device will report when the device stops playing a multicast audio stream.
Enable Power On Events ?	When selected, the device will report when it boots.
Enable Sensor Events ?	When selected, the device will report when the on-board sensor is activated.
Enable Security Events ?	When enabled, the device will report when the intrusion sensor is activated.
Enable 60 Second Heartbeat Events ?	When enabled, the device will report a Heartbeat event every 60 seconds. SIP registration is not required to generate Heartbeat events.
Check All	Click on <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>Note:</b> You need to reboot for changes to take effect.



Table 2-21. Events Configuration Parameters (continued)

Web Page Item	Description
	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** You must click on the **Save** button and then the **Reboot** button for the changes to take effect.

### 2.3.11.1 Example Packets for Events

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

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

Here are example packets for every event:

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

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

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

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

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

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

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

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

```
POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 205
Content-Type: application/x-www-form-urlencoded
```

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

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

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

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

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

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

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

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

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

## 2.3.12 Configure the Autoprovisioning Parameters

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

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

1. Click the **Autoprov** menu button to open the **Autoprovisioning** page. See [Figure 2-21](#).

**Figure 2-21. Autoprovisioning Page**

Home Device Network SIP Multicast Sensor Audiofiles Events Autoprov Firmware

# CyberData RGB Strobe

Disable Autoprovisioning: ☐

Autoprovisioning Server:

Autoprovisioning Filename:

Use tftp: ☐

Username:

Password:

Autoprovisioning autoupdate (in minutes): 0

Autoprovision at time (HHMMSS):

Autoprovision when idle (in minutes > 10): 0

See the manual to learn how to use autoprovisioning to configure your device.  
Autoprovisioning happens on boot.  
The device will first look for a configured server address and filename.  
If these haven't been configured, it will look for an autoprovisioning server in your list of DHCP options and try to download '0020f70353cf.xml' and if this fails, '000000cd.xml'.

Save Reboot Toggle Help

Download Template


### Autoprovisioning log

```
00:00 Autoprovisioning Device...
00:00 Autoprov found option 43 in DHCP server="http://chalmers.cyberdata.net"
00:00 Autoprov looking for 0020f70353cf.xml at http://chalmers.cyberdata.net
00:00 Autoprov looking for 000000cd.xml at http://chalmers.cyberdata.net
00:00 Failed to fetch autoprov file
00:00 Autoprov found option 72 in DHCP server="10.0.1.118"
00:00 Autoprov looking for 0020f70353cf.xml at 10.0.1.118
00:00 Autoprov looking for 000000cd.xml at 10.0.1.118
00:00 Failed to fetch autoprov file
00:00 Autoprov found option 150 in DHCP server="10.0.5.120"
```




2. On the **Autoprovisioning** page, you may enter values for the parameters indicated in [Table 2-22](#).

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

**Table 2-22. Autoprovisioning Configuration Parameters**

Web Page Item	Description
Disable Autoprovisioning ?	Prevent the device from automatically trying to download a configuration file. See <a href="#">Section 2.3.12.1, "Autoprovisioning"</a> for more information.
Autoprovisioning Server ?	Enter the IPv4 address of the provisioning server in dotted decimal notation.
Autoprovisioning Filename ?	<p>The autoprovisioning filename is the configuration filename. The default autoprovisioning filename is in the format of <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.
Username ?	The username used to authenticate with an autoprovisioning server. Leave this field blank to disable authentication.
Password ?	The password used to authenticate with an autoprovisioning server. Leave this field blank to disable authentication.
Autoprovisioning Autoupdate (in minutes) ?	<p>The reoccurring time (in minutes) the device will wait before checking for new autoprovisioning files. Enter up to 6 digits. A value of 0 will disable this option.</p> <p><b>Note:</b> To use the auto update options, enable the <a href="#">Set Time with NTP Server on boot</a> setting on the <a href="#">Device Configuration Page</a> (see <a href="#">Table 2-9</a>).</p>
Autoprovision at time (HHMMSS) ?	<p>The time of day the device will check for a new autoprovisioning file. The time must be 6 characters in length and in HHMMSS format. An empty value will disable this option.</p> <p><b>Note:</b> To use the auto update options, enable the <a href="#">Set Time with NTP Server on boot</a> setting on the <a href="#">Device Configuration Page</a> (see <a href="#">Table 2-9</a>).</p>
Autoprovision when idle (in minutes > 10) ?	<p>The idle time (in minutes greater than 10) after which the device will check for a new autoprovisioning file. Enter up to 6 digits. A value of 0 will disable this option.</p> <p><b>Note:</b> To use the auto update options, enable the <a href="#">Set Time with NTP Server on boot</a> setting on the <a href="#">Device Configuration Page</a> (see <a href="#">Table 2-9</a>).</p>
	<p>Click the <b>Save</b> button to save your configuration settings.</p> <p><b>Note:</b> You need to reboot for changes to take effect.</p>

**Table 2-22. Autoprovisioning Configuration Parameters (continued)**

Web Page Item	Description
	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 2.3.12.3, "Download Template Button"</a>
Autoprovisioning Log	The autoprovisioning log reflects the steps the device takes with autoprovisioning, relaying information about the server, DHCP options, configuration file names, and success or failure of finding and parsing the files.

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

### 2.3.12.1 Autoprovisioning

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

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

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

By default, the device will get its autoprovisioning server from the DHCP options. See [Section 2.3.12.2, "Sample dhcpd.conf"](#) for an example of how to configure dhcpd to offer autoprovisioning server addresses. If multiple options are set, the device will attempt to download autoprovisioning files from every server.

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

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

You can download an autoprovisioning template file from the [Autoprovisioning Page](#) using the **Download Template** button (see [Table 2-22](#)). 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](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 2-23. 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  
Firmware Updates

```
<FirmwareSettings>  
  <FirmwareFile>505-ulmage-ceiling-speaker</FirmwareFile>  
  <FirmwareServer>10.0.1.3</FirmwareServer>  
  <OutdoorIntercom30>firmware_file_v9.3.0</OutdoorIntercom30>  
  <OutdoorIntercom31>firmware_file_v10.3.0</OutdoorIntercom31>  
  <CallButton31>firmware_file_v10.3.0</CallButton31>  
</FirmwareSettings>
```

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

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

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

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

The list of valid product strings:

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

Autoprovisioning  
Example 1

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

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

The devices are set to use DHCP and that server provides an autoprovisioning server address with option 43. The address is "https://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 Configuration** page or by changing the autoprovisioning file with “**default**” set as the file name.

### 2.3.12.2 Sample dhcpd.conf

```
#
# Sample configuration file for ISC dhcpd for Debian
#

ddns-update-style none;

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

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

    option routers                10.0.0.1;
    option subnet-mask            255.0.0.0;

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

    option time-offset            -8;          # Pacific Standard Time

#    option www-server            99.99.99.99;          # OPTION 72

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

#    option option-150            10.0.0.252;          # OPTION 150

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

    range 10.10.0.1 10.10.2.1; }
```

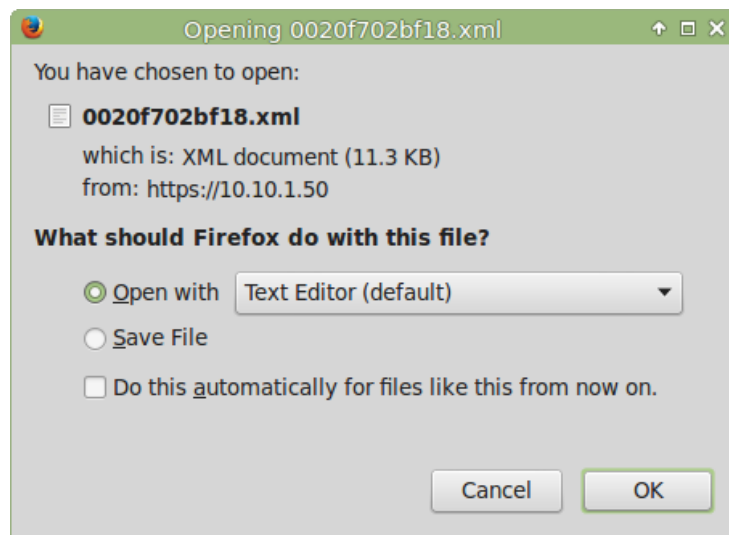
### 2.3.12.3 Download Template Button

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 2-22](#)). 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 2-22](#).

**Figure 2-22. 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 and Reboot the RGB Strobe

 GENERAL ALERT	<b>Caution</b> <b>Equipment Hazard:</b> Devices with a serial number that begins with 3760xxxxx can only run firmware versions 10.0.0 or later.
--	--

To download the firmware to your computer:

1. Download the latest firmware file from the **Downloads** tab at the following webpage:  
<http://www.cyberdata.net/voip/011376/>
2. Unzip the firmware version file. This file may contain the following:
  - Firmware file
  - Release notes
3. Log in to the RGB Strobe home page as instructed in [Section 2.3.4, "Log in to the Configuration Home Page"](#).
4. Click on the **Firmware** button to open the **Firmware** page. See [Figure 2-23](#).


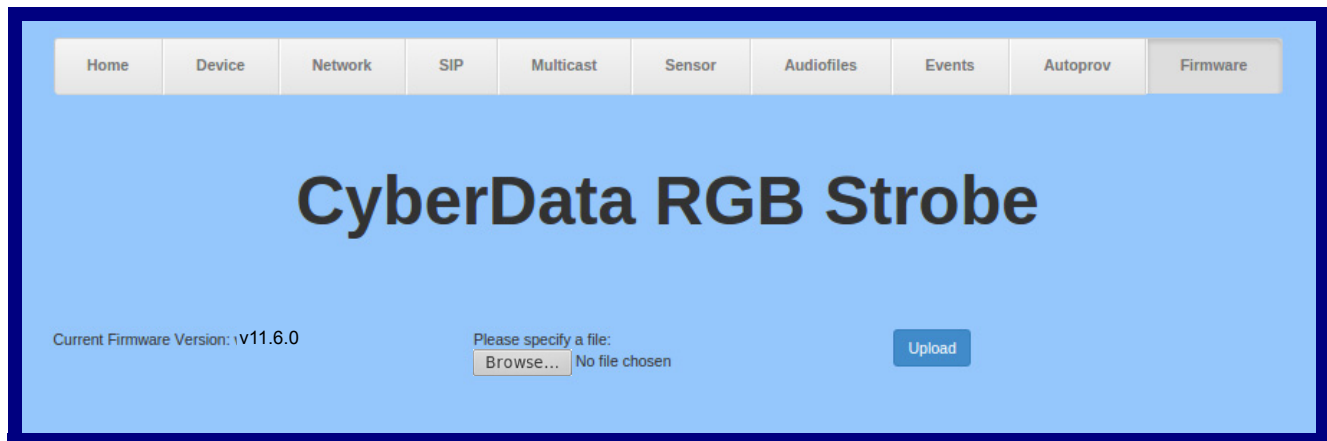
 GENERAL ALERT	<b>Caution</b> <b>Equipment Hazard:</b> CyberData strongly recommends that you first reboot the device before attempting to upgrade the firmware of the device. See <a href="#">Section 2.4.1, "Reboot the Device"</a> .
---	---

Figure 2-23. Firmware Page



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



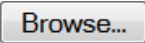

- Click on the **Upload** button.

**Note** Do not reboot the device after clicking on the **Upload** button.

**Note** This starts the upgrade process. Once the RGB Strobe has uploaded the file, the **Uploading Firmware** countdown page appears, indicating that the firmware is being written to flash. The RGB Strobe will automatically reboot when the upload is complete. When the countdown finishes, the **Firmware** page will refresh. The uploaded firmware filename should be displayed in the system configuration (indicating successful upload and reboot).

- Table 2-24 shows the web page items on the **Firmware** page.

**Table 2-24. Firmware Parameters**

Web Page Item	Description
Current Firmware Version	Shows the current firmware version.
	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.

## 2.4.1 Reboot the Device

To reboot a RGB Strobe, log in to the web page as instructed in [Section 2.3.4, "Log in to the Configuration Home Page"](#).

1. Click on the **Reboot** button on the **Home** page ([Figure 2-24](#)). A normal restart will occur.

Figure 2-24. Home Page

Home Device Network SIP Multicast Sensor Audiofiles Events Autoprov Firmware

# CyberData RGB Strobe

### Current Status

Serial Number: 376000001  
Mac Address: 00:20:f7:03:76:9d  
Firmware Version: v11.6.0

IP Addressing: DHCP  
IP Address: 10.10.1.231  
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

### Admin Settings

Username: admin  
Password:  
Confirm Password:

Save Reboot Toggle Help

### Import Settings

Browse... No file chosen

Import Config

### Export Settings

Export Config

Reboot

## 2.5 Command Interface

Some functions on the device can be activated using simple POST commands to the web interface. The examples in [Table 2-25](#) use the free unix utility, **wget** commands. However, any program that can send HTTP POST commands to the device should work.

### 2.5.1 Command Interface Post Commands

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

**Table 2-25. Command Interface Post Commands**

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

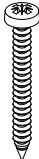
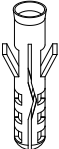
a. Type and enter all of each http POST command on one line.

# Appendix A: Mounting the RGB Strobe

## A.1 Mount the RGB Strobe

Before you mount the RGB Strobe, make sure that you have received all the parts for each RGB Strobe. Refer to [Table A-1](#).

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

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

**Table A-2. Gang Box Mounting Components**

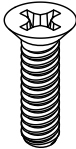
Quantity	Part Name	Illustration
4	#6-32 x 0.625-inch Flat-Head Machine Screw.	

Figure A-1 shows the wall mounting option for the RGB Strobe.

**Note** Be sure to connect the RGB Strobe to the Earth Ground.

**Figure A-1. Wall Mounting Options**

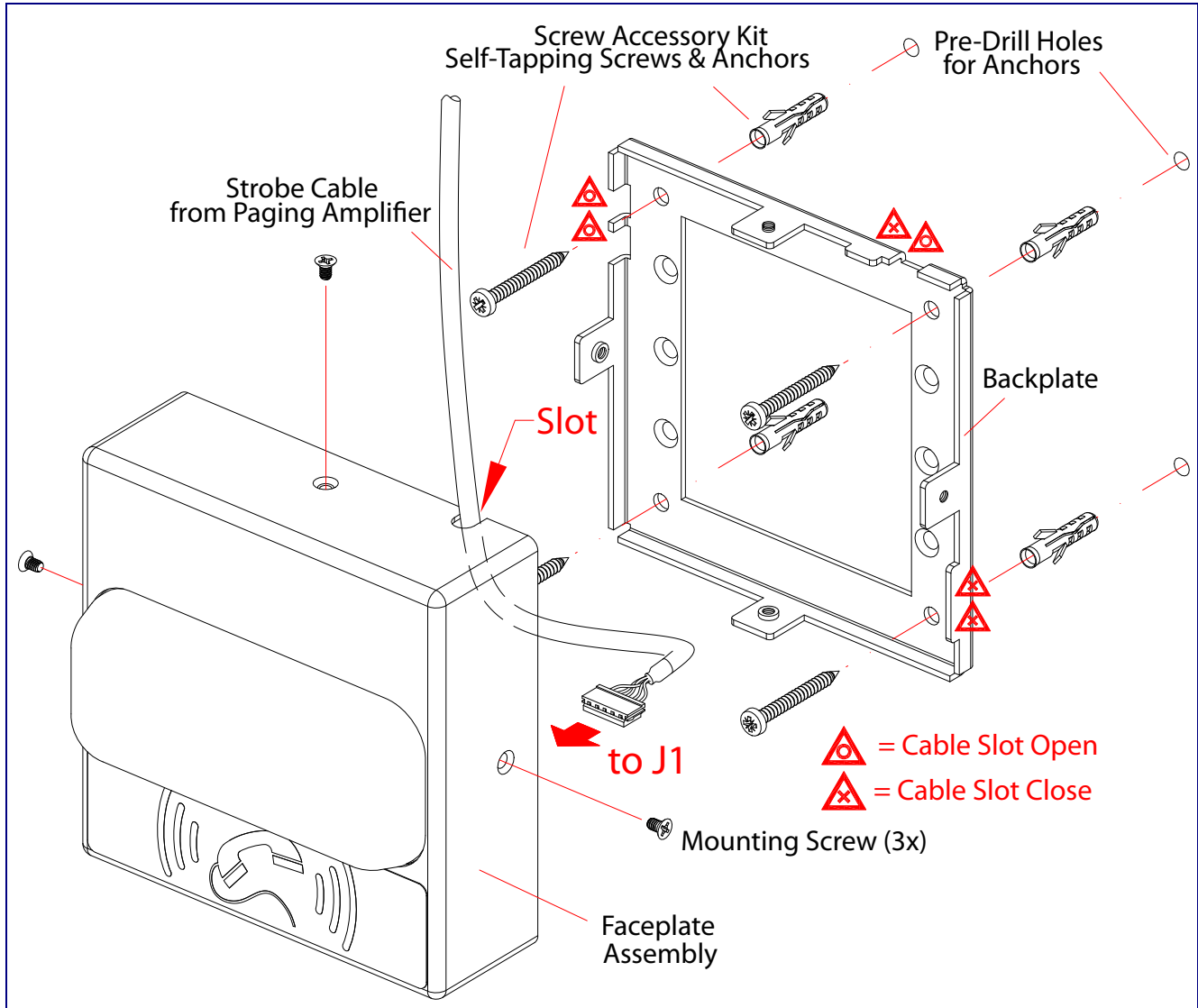


Figure A-2 shows the gang box mounting options for the RGB Strobe.

**Note** Be sure to connect the RGB Strobe to the Earth Ground.

**Figure A-2. Gang Box Mounting Options**

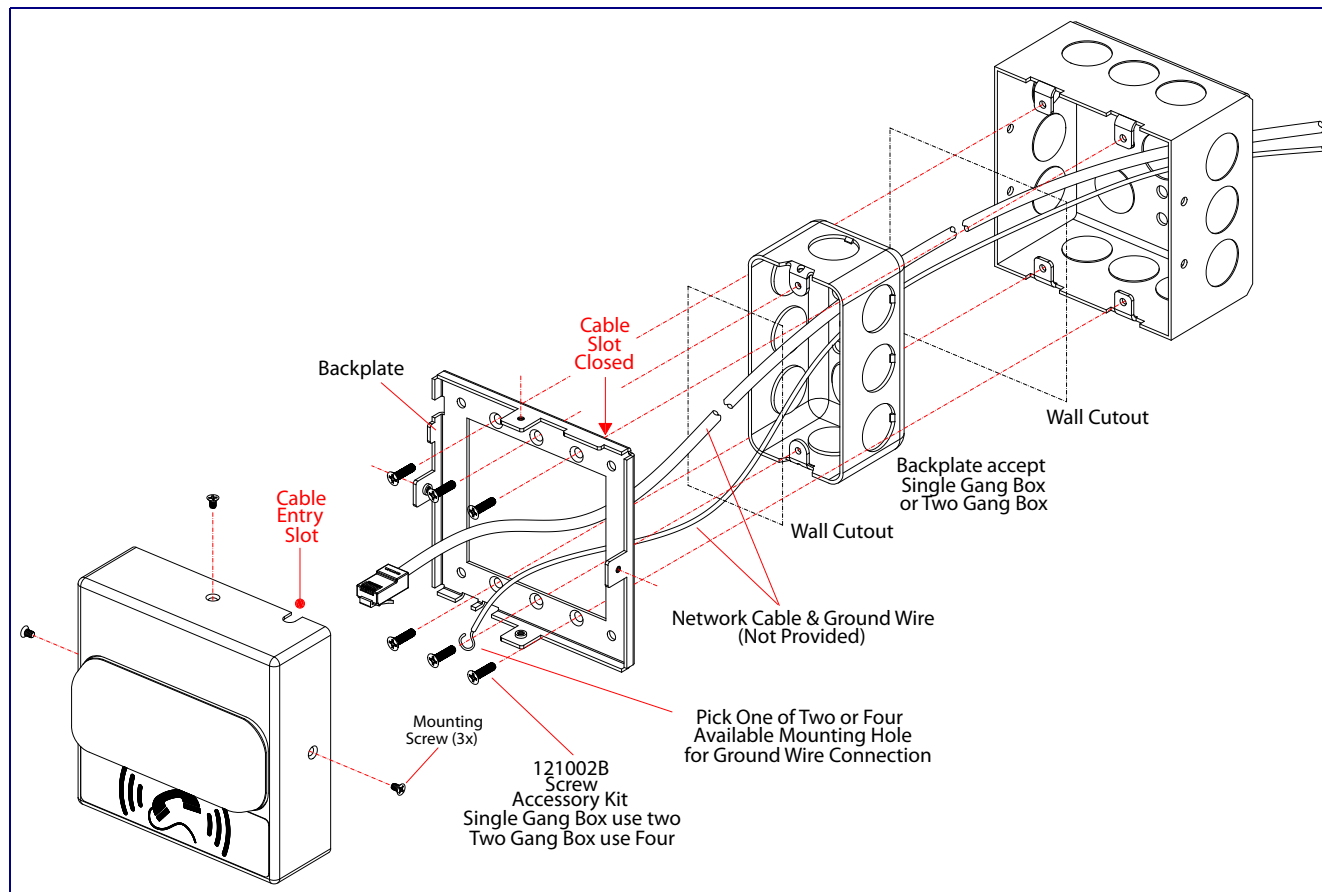
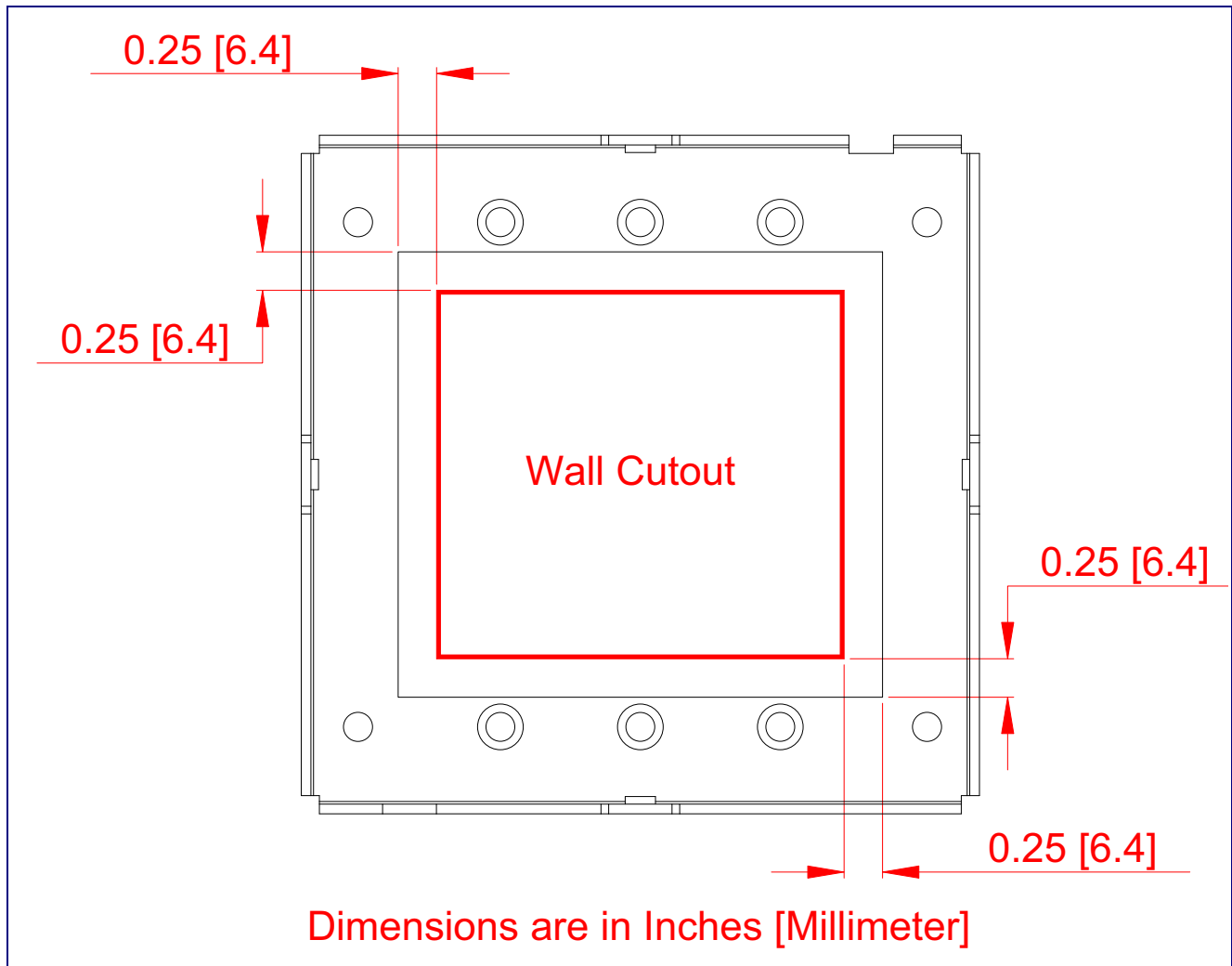


Figure A-3 shows the wall mounting with either a single or two gang box.

**Figure A-3. Wall Mounting with Single or Two Gang Box**





# Appendix B: Troubleshooting/Technical Support

---

## B.1 Frequently Asked Questions (FAQ)

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

<http://www.cyberdata.net/voip/011376/>

---

## B.2 Documentation

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

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

<http://www.cyberdata.net/voip/011376/>

---

## 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 6

## A

AC voltages, enclosure is not rated 7  
 activate relay (door sensor) 44  
 activate relay (intrusion sensor) 45  
 activity LED 12  
 address, configuration login 18  
 alternative power input 4  
 audio configuration 47  
 audio configuration page 47  
 Autoprovision at time (HHMMSS) 54  
 autoprovision at time (HHMMSS) 54  
 autoprovision when idle (in minutes > 10) 54  
 autoprovisioning 55  
     download template button 55  
 autoprovisioning autoupdate (in minutes) 54  
 autoprovisioning configuration 53, 54  
 autoprovisioning filename 54  
 autoprovisioning server (IP Address) 54  
 auxiliary relay wiring diagram 8

## B

backup SIP server 1 31  
 backup SIP server 2 31  
 backup SIP servers, SIP server  
     backups 31  
 baud rate  
     verifying 12

## C

changing  
     the web access password 22  
 Cisco SRST 31  
 command interface 68  
 commands 68  
 configurable parameters 20, 23, 28  
 configuration  
     audio 47  
     default IP settings 14  
     door sensor 43

intrusion sensor 43  
 network 27  
 SIP 30  
     using Web interface 14  
 configuration home page 19  
 configuration page  
     configurable parameters 20, 23, 28  
 contact information 75  
 contact information for CyberData 75  
 Current Network Settings 28  
 current network settings 28  
 CyberData contact information 75

## D

default  
     device settings 76  
     gateway 14  
     IP address 14  
     subnet mask 14  
     username and password 14  
     web login username and password 19  
 default device settings 13  
 default gateway 14, 28  
 default IP settings 14  
 default login address 18  
 device configuration 22  
     device configuration parameters 54  
     the device configuration page 53  
 device configuration page 22  
 device configuration parameters 23  
 device configuration password  
     changing for web configuration access 22  
 DHCP Client 3  
 dial out extension (door sensor) 44  
 dial out extension (intrusion sensor) 45  
 dial out extension strings 35  
 dial-out extension strings 38  
 dimensions 4  
 discovery utility program 18  
 DNS server 28  
 door sensor 43, 44  
     activate relay 44  
     dial out extension 44  
     door open timeout 44  
     door sensor normally closed 44  
 download autoprovisioning template button 55  
 DTMF tones 35, 38  
 DTMF tones (using rfc2833) 35

## E

- earth ground 70, 71
- enable night ring events 49
- ethernet I/F 4
- event configuration
  - enable night ring events 49
- expiration time for SIP server lease 32, 34
- export settings 20

## F

- factory default settings 13
  - how to set 13
- firmware
  - where to get the latest firmware 65

## G

- gang box mounting 70, 71
- get autoprovisioning template 55
- GMT table 26
- GMT time 26

## H

- home page 19
- http POST command 68
- http web-based configuration 3

## I

- identifier names (PST, EDT, IST, MUT) 25
- identifying your product 1
- illustration of device mounting process 69
- import settings 20
- import/export settings 20
- installation, typical device system 2
- intrusion sensor 43, 45
  - activate relay 45
  - dial out extension 45
- IP address 14, 28
- IP addressing
  - default
    - IP addressing setting 14

## L

- lease, SIP server expiration time 32, 34
- LED
  - green link LED 12
  - yellow activity LED 12
- lengthy pages 42
- link LED 12
- local SIP port 32
- log in address 18

## M

- MGROUP
  - MGROUP Name 41
- mounting the device 69
- Multicast IP Address 41

## N

- navigation (web page) 15
- navigation table 15
- network configuration 27
- Network Setup 27
- nightring tones 42
- Nightringer 6, 64, 65
- nightringer settings 33
- NTP server 23

## O

- on-board relay 4, 7
- operating temperature 4

## P

- pages (lengthy) 42
- part number 4
- parts list 5
- password
  - for SIP server login 31
  - login 19
  - restoring the default 14
- point-to-point configuration 37
- polycom default channel 41
- polycom emergency channel 41
- polycom priority channel 41
- port

- local SIP 32
- remote SIP 32
- posix timezone string
  - timezone string 23
- POST command 68
- power input 4
  - alternative 4
- priority
  - assigning 42
- product
  - configuring 14
  - mounting 69
  - parts list 5
- product features 3
- product overview
  - product features 3
  - product specifications 4
  - supported protocols 3
  - supported SIP servers 3
  - typical system installation 2
- product specifications 4
- protocol 4
- protocols supported 3

## R

- reboot 66, 67
- remote SIP port 32
- Reset Test Function Management (RTFM) switch 13
- resetting the IP address to the default 69, 74
- restoring factory default settings 13, 76
- restoring the factory default settings 13
- ringtones 42
  - lengthy pages 42
- RJ-45 10
- rport discovery setting, disabling 32
- RTFM switch 13
- RTP/AVP 3

## S

- sales 75
- sensor setup page 43
- sensor setup parameters 43
- sensors 44
- server address, SIP 31
- service 75
- set time with external NTP server on boot 23
- setting up the device 6
- settings, default 13
- SIP
  - enable SIP operation 31

- local SIP port 32
- user ID 31
- SIP (session initiation protocol) 3
- SIP configuration 30
  - SIP Server 31
- SIP configuration parameters
  - outbound proxy 32, 34
  - registration and expiration, SIP server lease 32, 34
  - 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
- SRST 31
- subnet mask 14, 28
- supported protocols 3

## T

- tech support 75
- technical support, contact information 75
- terminal block, 16 AWG gauge wire 6
- time zone string examples 25

## U

- user ID
  - for SIP server login 31
- username
  - changing for web configuration access 22
  - default for web configuration access 19
  - restoring the default 14

## V

- verifying
  - baud rate 12
  - network connectivity 12
- VLAN ID 28
- VLAN Priority 28
- VLAN tagging support 28
- VLAN tags 28

## W

- warranty policy at CyberData 75
- web access password 14
- web access username 14
- web configuration log in address 18
- web page
  - navigation 15
- web page navigation 15
- web-based configuration 14
- weight 4
- wget, free unix utility 68