CyberData
The IP Endpoint Company

SIP RGB (Multi-Color) Strobe Operations Guide

Part #*011376*
Document Part #*931567C*
for Firmware Version *20.2.0*

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

SIP RGB (Multi-Color) Strobe Operations Guide 931567C
Part # 011376

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.

CyberData
The IP Endpoint Company

Technical Support

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

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

Revision Information

Revision 931567C, which corresponds to firmware version 20.2.0, was released on January 17, 2022, and has the following changes:

- Updates Figure 1-2, "Typical Installation"
- Updates Figure 2-17, "SIP Page"
- Updates Figure 2-18, "SIP Page"
- Updates Figure 2-19, "SIP Page"
- Updates Figure 2-20, "SIP Page"
- Updates Table 2-11, "SIP Configuration Parameters"
- Adds Section 2.3.7.2, "Point-to-Point Fault Sense Reporting"
- Updates Figure 2-22, "SSL Configuration Page"
- Updates Figure 2-23, "SSL Configuration Page"
- Updates Figure 2-24, "SSL Configuration Page"
- Updates Table 2-12, "SSL Configuration Parameters"
- Updates Figure 2-33, "Event Configuration Page"

Pictorial Alert Icons

⚠ GENERAL ALERT	General Alert This pictorial alert indicates a potentially hazardous situation. This alert will be followed by a hazard level heading and more specific information about the hazard.
⏚	Ground This pictorial alert indicates the Earth grounding connection point.

Hazard Levels

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

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

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

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

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

Important Safety Instructions

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

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

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

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

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
SRTP	Secure Real Time Protocol
u-law	A companding algorithm, primarily used in the digital telecommunication
UC	Unified Communications
VoIP	Voice over Internet Protocol

Contents

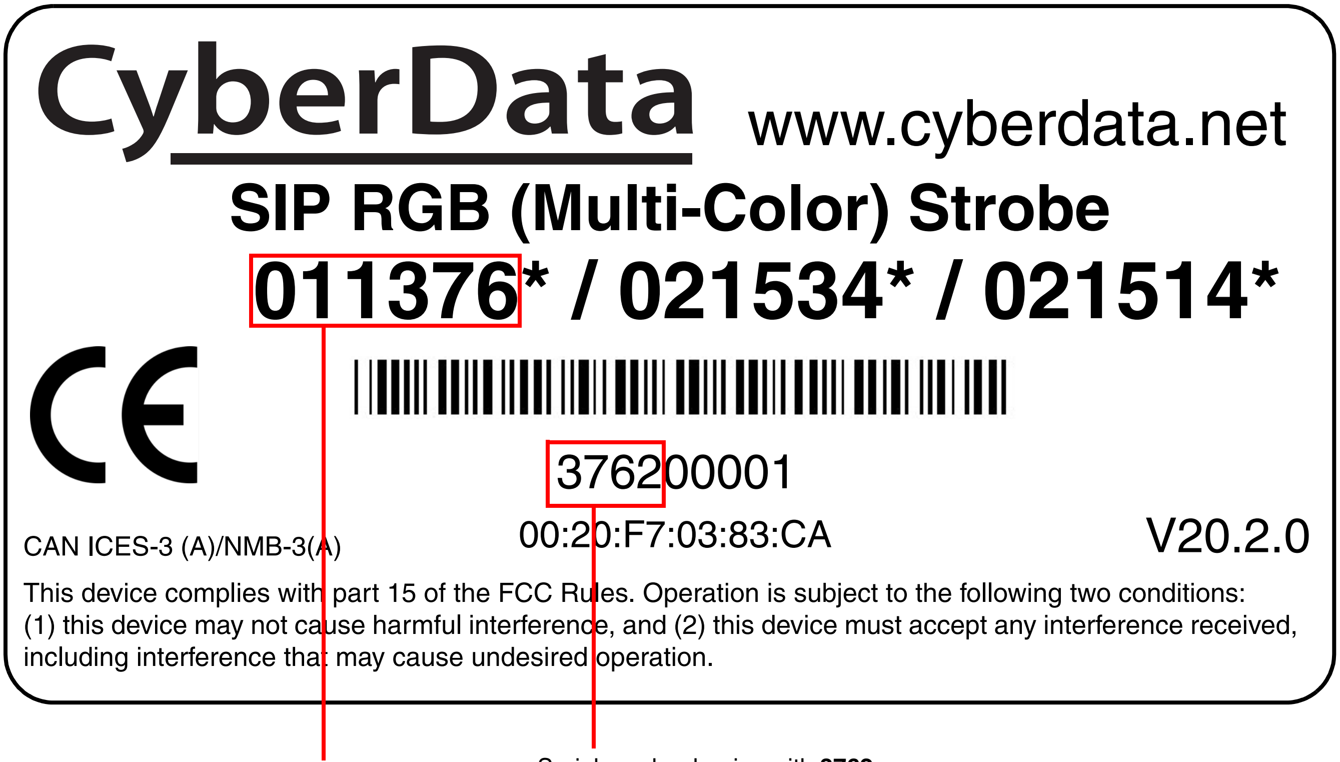
1 Product Overview

1.1 How to Identify This Product

To identify the SIP RGB (Multi-Color) Strobe, look for a model number label similar to the one shown in Figure 1-1. Confirm the following:

- The model number on the label should be 011376.
- The serial number on the label should begin with **3762**.

Figure 1-1. Model Number Label


CyberData
www.cyberdata.net
SIP RGB (Multi-Color) Strobe
011376* / 021534* / 021514*
376200001
CAN ICES-3 (A)/NMB-3(A)
00:20:F7:03:83:CA
V20.2.0
This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Model number

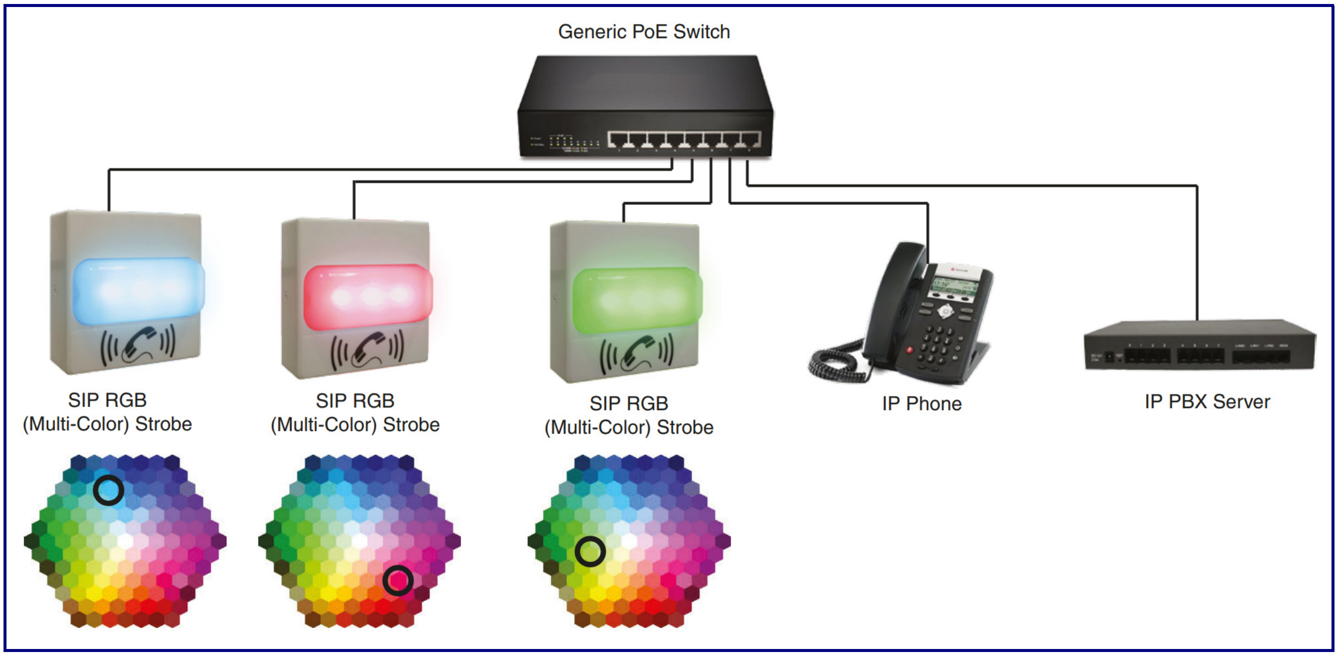
Serial number begins with **3762**

1.2 Typical System Installation

The SIP 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 SIP RGB (Multi-Color) Strobes can be installed as part of a VoIP phone system.

Figure 1-2. Typical Installation


Generic PoE Switch
SIP RGB (Multi-Color) Strobe
SIP RGB (Multi-Color) Strobe
SIP RGB (Multi-Color) Strobe
IP Phone
IP PBX Server

1.3 Product Features

- Meets ADA requirements for telephony signaling and notification
- Simultaneous SIP and multicast
- Night Ringer function - second SIP extension that can be configured with its own strobe scene
- Door closure and tamper alert signals
- TLS 1.2 (including mutual authentication) and SRTP enhanced security for IP Endpoints in a local or cloud-based environment
- Autoprovisioning via HTTP, HTTPS, or TFTP
- HTTPS or HTTP web based configuration. HTTPS is enabled by default.
- Configurable event generation for device health and status monitoring
- 802.11q VLAN tagging
- HTTP command interface
- Support for Cisco SRST resiliency

1.4 Supported SIP Servers

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

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

1.5 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[a]
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
Network Security	TLS 1.2, SRTP, HTTPS
Operating Range	Temperature: -40° C to 55° C (-40° F to 131° F) Humidity: 5-95%, non-condensing
Storage Temperature	-40° C to 70° C (-40° F to 158° F)
Storage Altitude	Up to 15,000 ft. (4573 m)
Dimensions[b]	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]
Compliance	CE: EMC Directive – Class A EN 55032 & EN 55024, LV Safety Directive EN 62368-1; RoHS Compliant; FCC Part 15 Class A; Industry Canada ICES-3 Class A; IEEE 802.3 Compliant; TAA Compliant
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.

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

1.6 Compliance

1.6.1 CE Statement

As of the date of manufacture, the Paging Series has been tested and found to comply with the specifications for CE marking and standards per EMC and Radiocommunications Compliance. This applies to the following products: 011145, 011146, 011233, 011280, 011295, 011314, 011368, and 011372.

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

1.6.2 FCC Statement

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

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

1.6.3 Industry Canada (IC) Compliance Statement

Operation is subject to the following two conditions:

1.This device may not cause interference, and

2.This device must accept any interference, including interference that may cause undesired operations of the device.

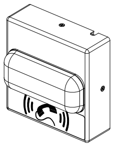
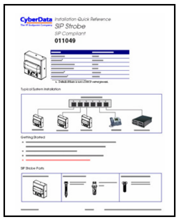
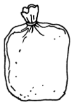
ICES-3 Class A

2 Installing the SIP RGB (Multi-Color) Strobe

2.1 Parts List

Table 2-2 illustrates the SIP RGB Strobe parts.

Table 2-2. Parts List

Quantity	Part Name	Illustration
1	SIP RGB Strobe Assembly	
1	Installation Quick Reference Guide	 CyberData The IP Endpoint Company Installation Quick Reference SIP Strobe SIP Compliant 011049 a. Default if there is not a DHCP server present. Typical System Installation Getting Started SIP Strobe Parts
1	SIP RGB Strobe Mounting Accessory Kit	

2.2 SIP RGB (Multi-Color) Strobe Setup

2.2.1 SIP RGB Strobe Connections

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

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

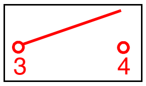
GENERAL ALERT

Caution

Equipment Hazard: 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.

Figure 2-3. Connections and Alternate Power Input

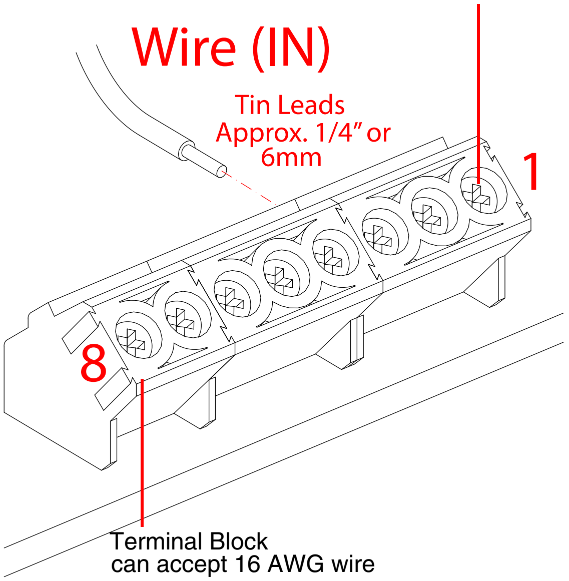
Alternate Power Input:
1 = +8 to +12VDC @ 1000mA Regulated Power Supply*
2 = Power Ground*



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 = Remote Switch "A"
8 = Remote Switch "B"

*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.

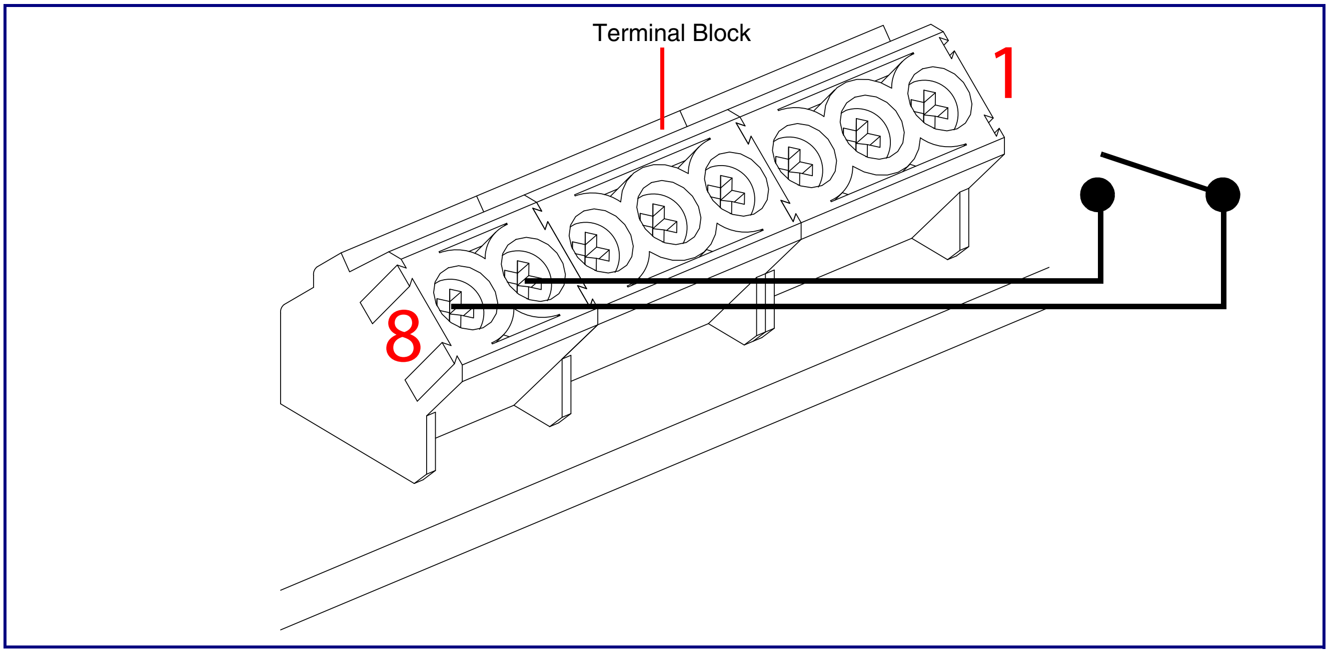
Use a 3.17 mm (1/8-inch) flat blade screwdriver for the terminal block screws



2.2.1.1 Remote Switch Connection

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

Figure 2-4. Remote Switch Connection



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

⚠ GENERAL ALERT	**Warning** *Electrical Hazard:* The device enclosure is not rated for any AC voltages.

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

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

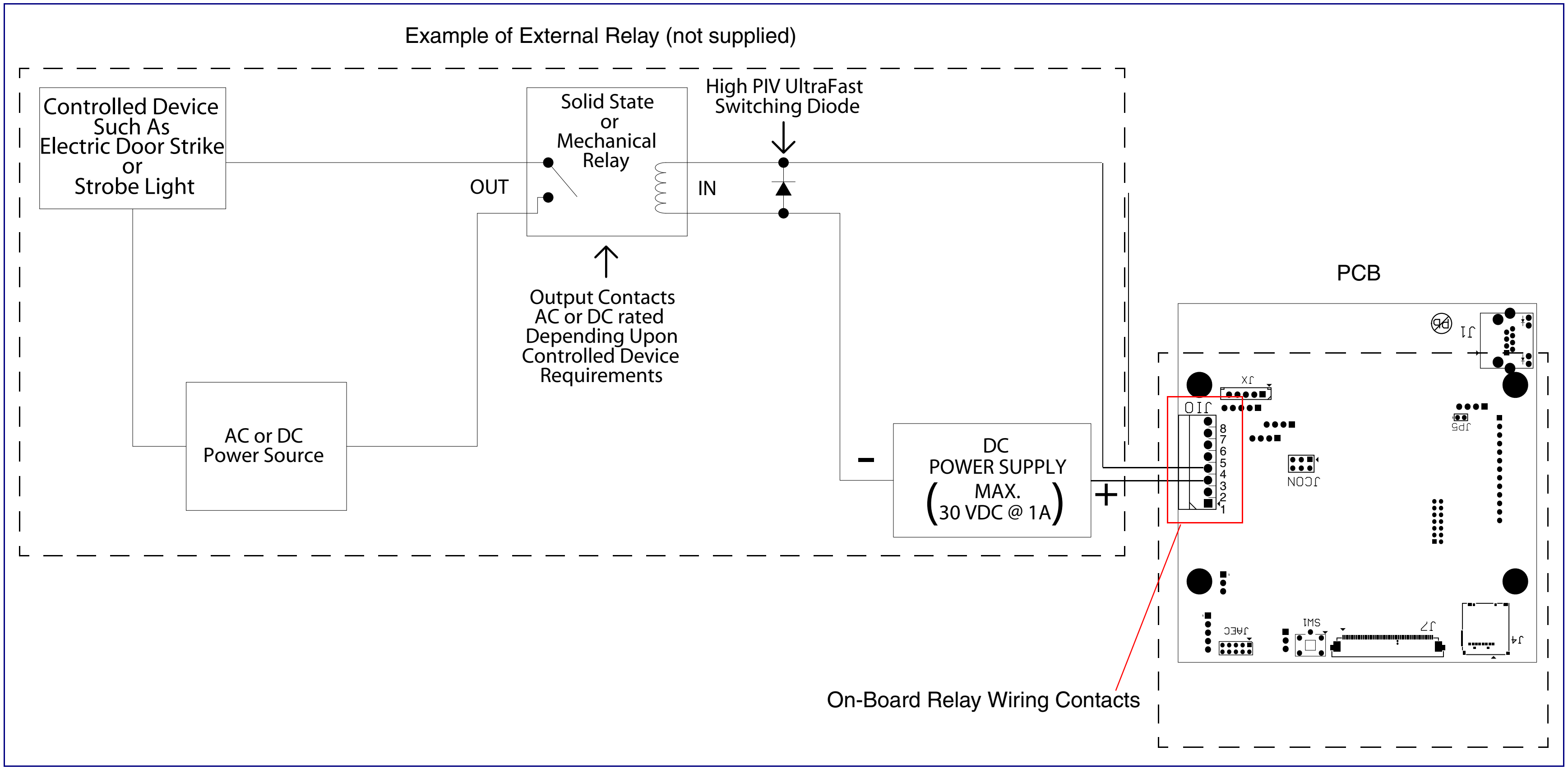
⚠ GENERAL ALERT	**Warning** *Electrical Hazard:* The relay contacts are dry and provided for a normally open and momentarily closed configuration. Neither the alternate power input nor PoE power can be used to drive a door strike.

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

The device incorporates an on-board relay which enables users to control an external relay for activating an auxiliary device such as an electric door strike (see Figure 2.2.3, "Identifying the SIP RGB (Multi-Color) Strobe Connectors and Jumpers").

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

Figure 2-5. Wiring Diagram


Example of External Relay (not supplied)
Controlled Device Such As Electric Door Strike or Strobe Light
Solid State or Mechanical Relay
High PIV UltraFast Switching Diode
OUT
IN
Output Contacts AC or DC rated Depending Upon Controlled Device Requirements
AC or DC Power Source
–
DC POWER SUPPLY (MAX. 30 VDC @ 1A)
+
PCB
J10
8
7
6
5
4
3
2
1
JCON
J1
J5
JX
SW1
J7
J4
JAEC
On-Board Relay Wiring Contacts

2.2.3 Identifying the SIP RGB (Multi-Color) Strobe Connectors and Jumpers

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

Figure 2-6. Connector Locations—Board Top

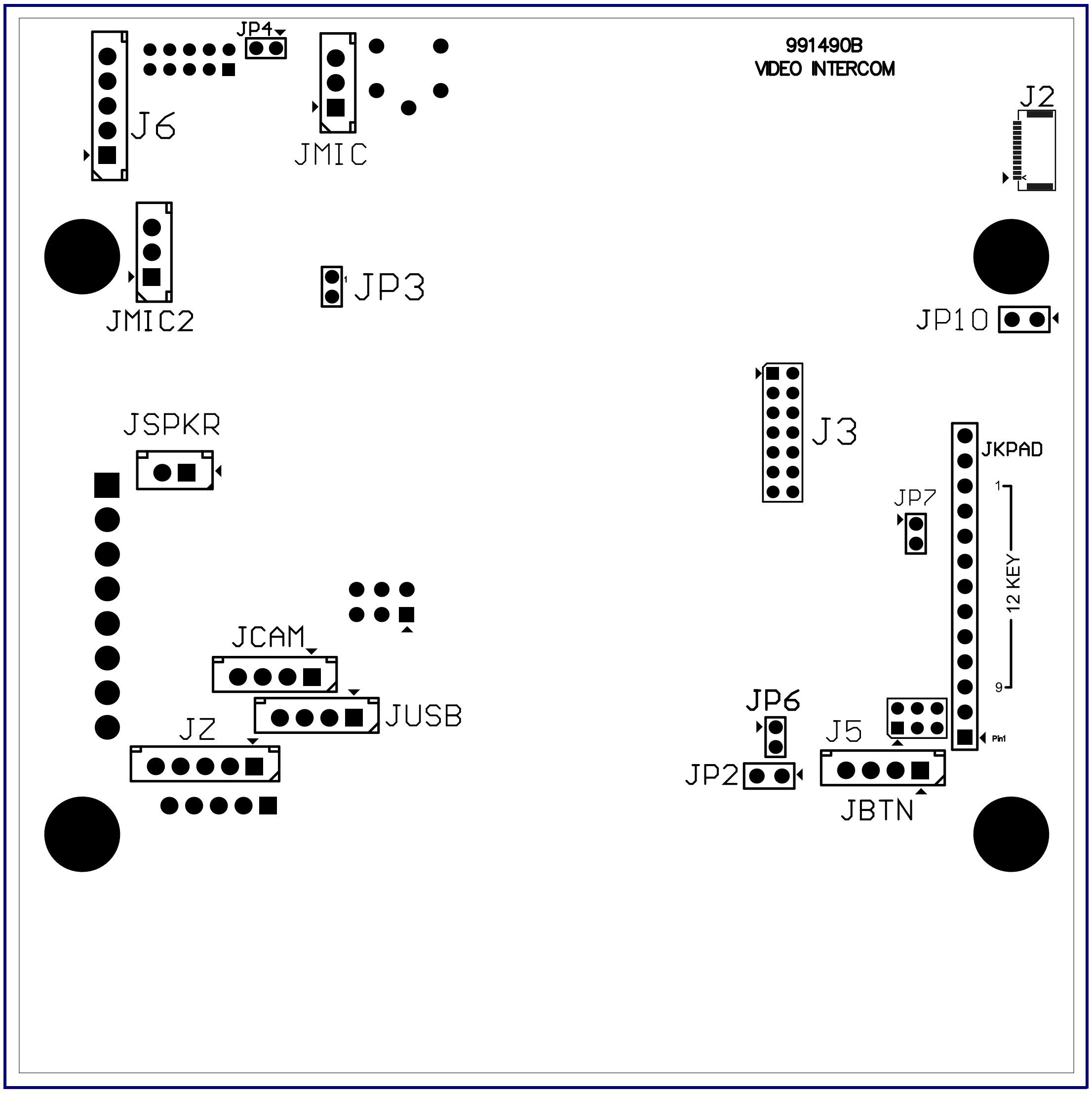


Table 2-3. Connector Functions—Board Top

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

Figure 2-7. Connector Locations—Board Bottom

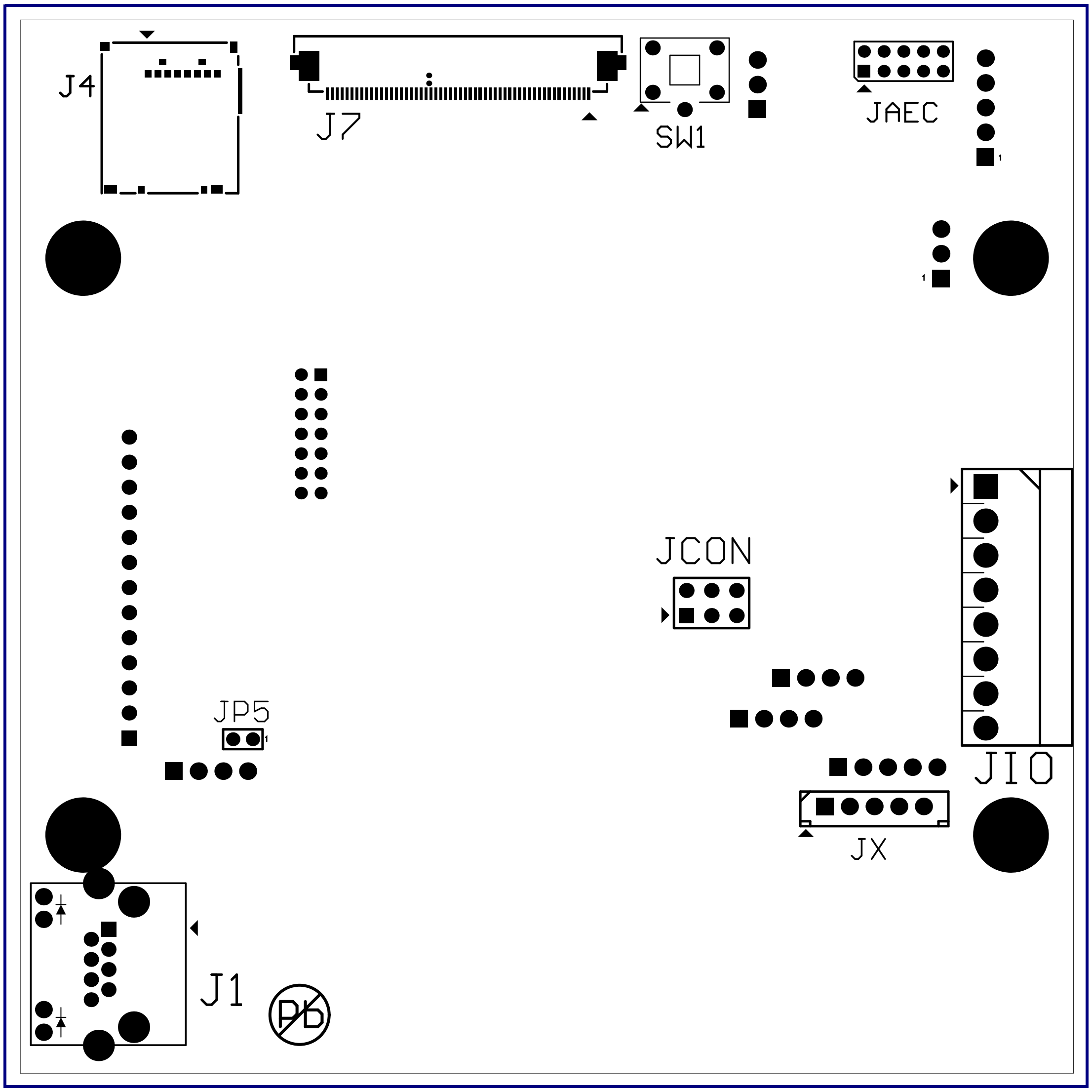
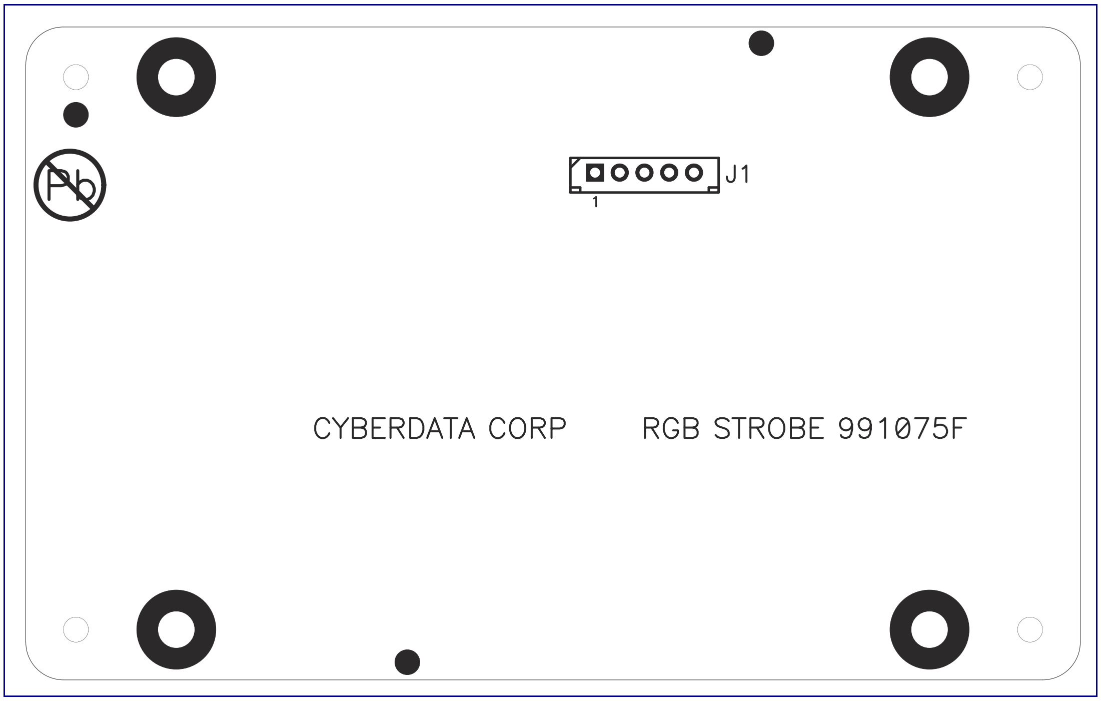


Table 2-4. Connector Functions—Board Bottom

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

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

Figure 2-8. Connector Locations for the 021509 Board



.

Table 2-5. Connector Functions

Connector	Function
J1	Ethernet Connector

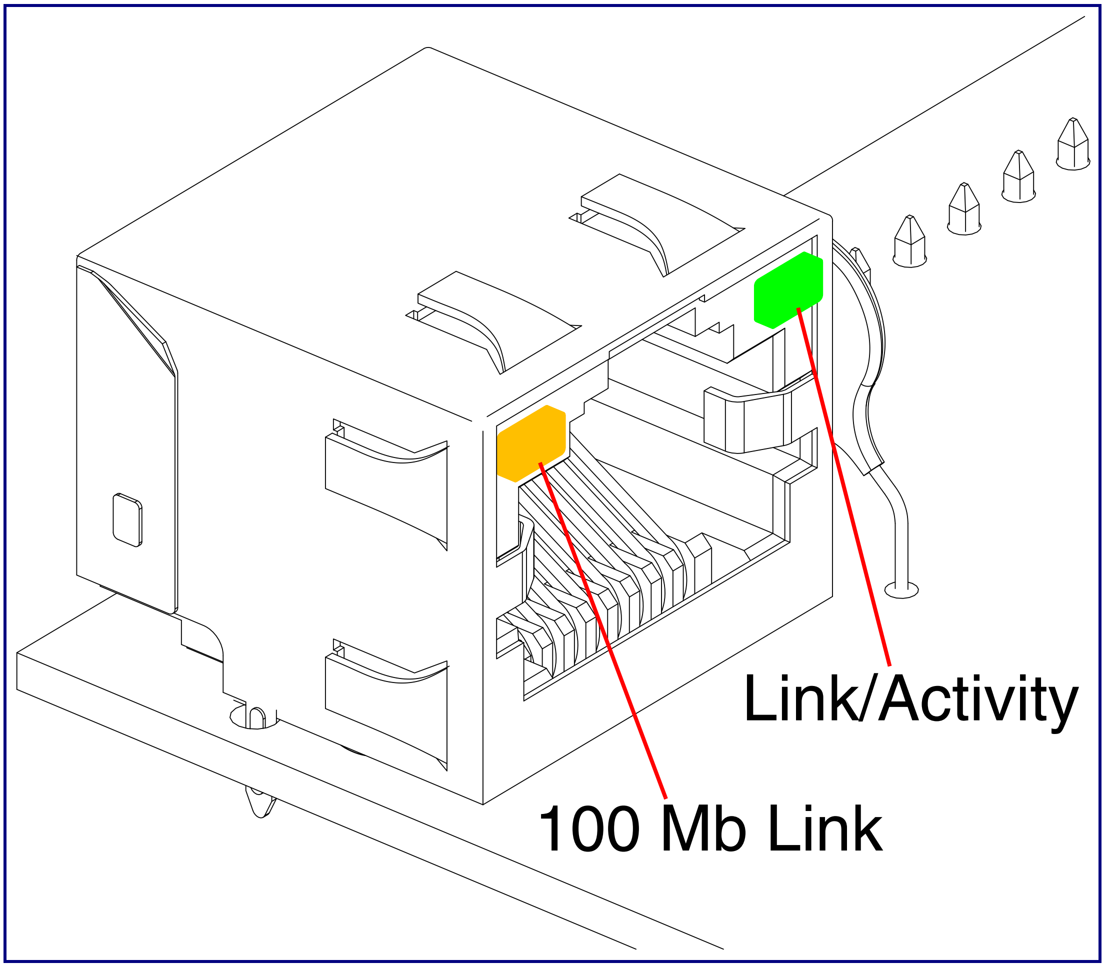
2.2.4 Activity and Link LEDs

2.2.4.1 Verifying the Network Connectivity and Data Rate

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

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

Figure 2-9. Activity and Link LED



2.2.5 Restoring the Factory Default Settings

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

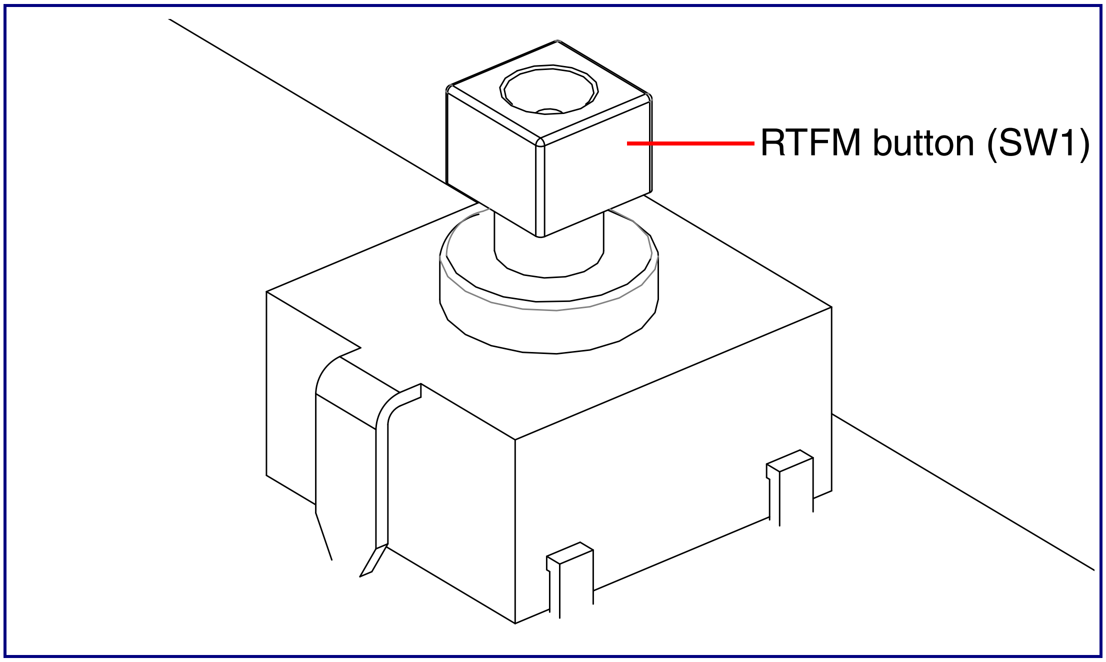
Note Each SIP RGB Strobe is delivered with factory set default values.

To restore the factory default settings:

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

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

Figure 2-10. RTFM Button (SW1)



2.3 Configure the SIP RGB Strobe Parameters

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

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

2.3.1 Factory Default Settings

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

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

Table 2-6. Factory Default Settings

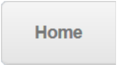
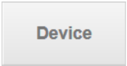
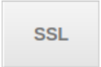
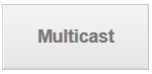
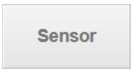
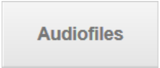
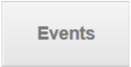
Parameter	Factory Default Setting
IP Addressing	DHCP
IP Address[a]	10.10.10.10
Web Access Username	admin
Web Access Password	admin
Subnet Mask[a]	255.0.0.0
Default Gateway[a]	10.0.0.1

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

2.3.2 SIP RGB Strobe Web Page Navigation

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

Table 2-7. Web Page Navigation

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

2.3.3 Using the Toggle Help Button

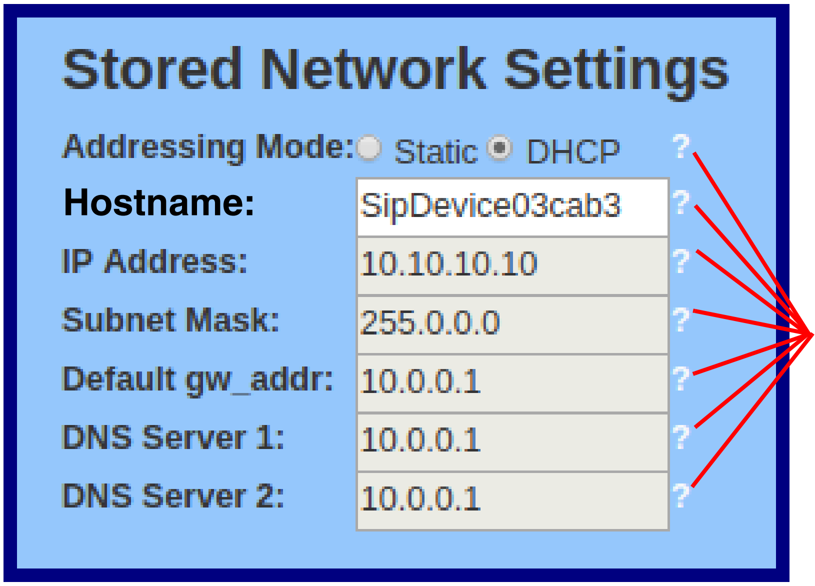
The **Toggle Help** button allows you to see a short description of some of the settings on the webpage. To use the **Toggle Help** button, do the following:

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

Figure 2-11. Toggle/Help Button

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

Figure 2-12. Toggle Help Button and Question Marks



Stored Network Settings

Addressing Mode: ○ Static ● DHCP ?

Hostname: SipDevice03cab3 ?

IP Address: 10.10.10.10 ?

Subnet Mask: 255.0.0.0 ?

Default gw_addr: 10.0.0.1 ?

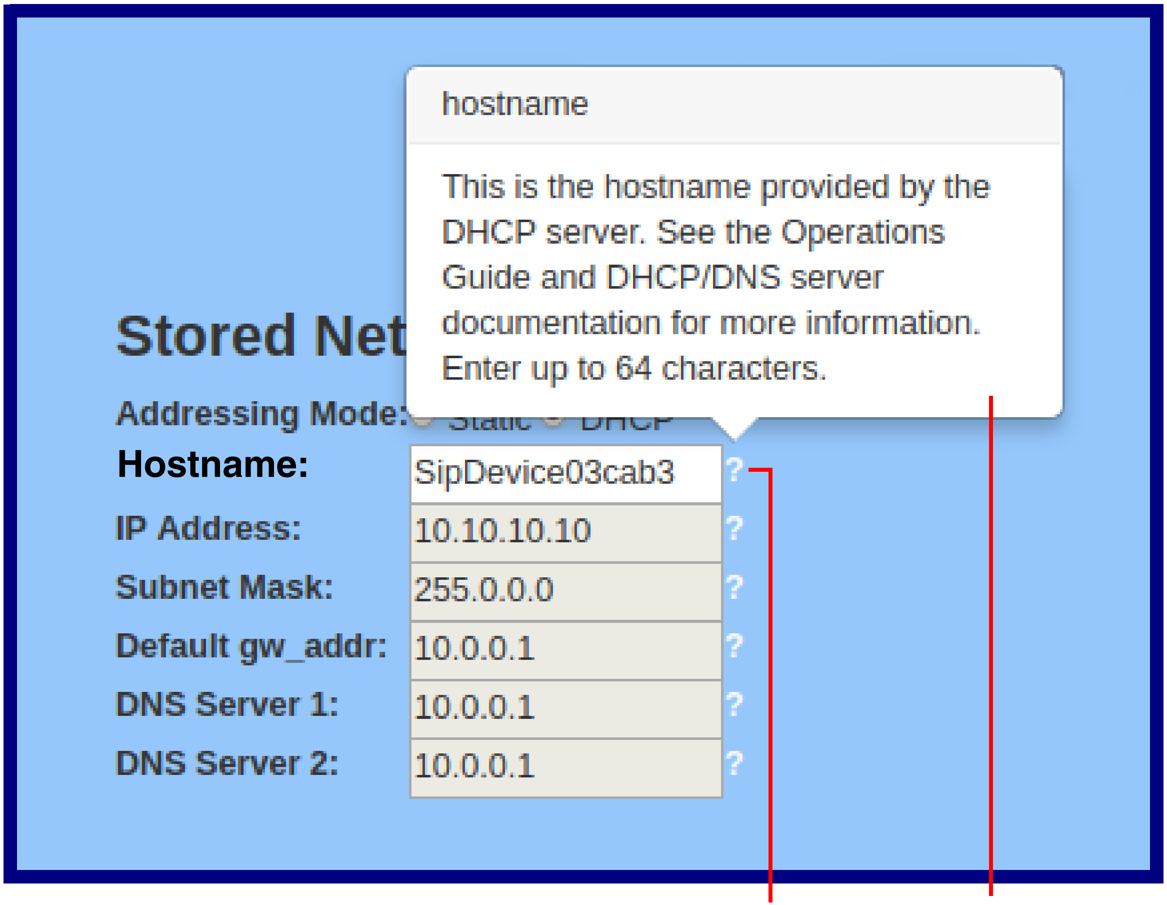
DNS Server 1: 10.0.0.1 ?

DNS Server 2: 10.0.0.1 ?

Question mark
appears next to the
web page items

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

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



hostname

This is the hostname provided by the DHCP server. See the Operations Guide and DHCP/DNS server documentation for more information. Enter up to 64 characters.

Stored Net

Addressing Mode: ○ Static ○ DHCP

Hostname: SipDevice03cab3 ?

IP Address: 10.10.10.10 ?

Subnet Mask: 255.0.0.0 ?

Default gw_addr: 10.0.0.1 ?

DNS Server 1: 10.0.0.1 ?

DNS Server 2: 10.0.0.1 ?

Question mark

A short description of the web page item will appear

2.3.4 Log in to the Configuration Home Page

1. Open your browser to the SIP 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 SIP 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 following website address:

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

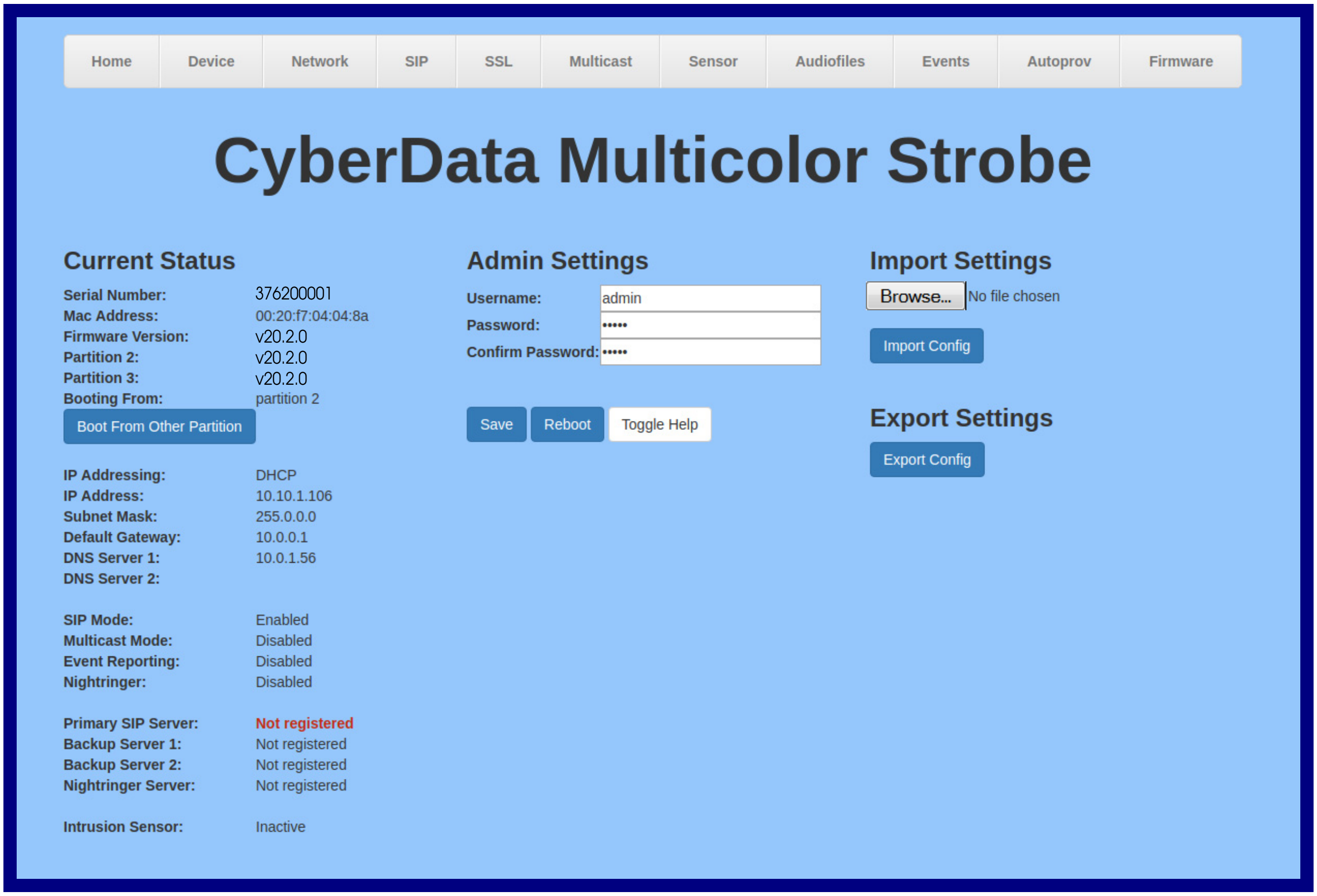
Note The Intercom ships in DHCP mode. To get to the **Home** page, use the discovery utility to scan for the device on the network and open your browser from there.

2. When prompted, use the following default **Web Access Username** and **Web Access Password** to access the **Home Page** (Figure 2-14):

   Web Access Username: **admin**

   Web Access Password: **admin**

Figure 2-14. Home Page



CyberData Multicolor Strobe

Current Status

Serial Number:	376200001
Mac Address:	00:20:f7:04:04:8a
Firmware Version:	v20.2.0
Partition 2:	v20.2.0
Partition 3:	v20.2.0
Booting From:	partition 2
IP Addressing:	DHCP
IP Address:	10.10.1.106
Subnet Mask:	255.0.0.0
Default Gateway:	10.0.0.1
DNS Server 1:	10.0.1.56
DNS Server 2:	
SIP Mode:	Enabled
Multicast Mode:	Disabled
Event Reporting:	Disabled
Nightringer:	Disabled
Primary SIP Server:	Not registered
Backup Server 1:	Not registered
Backup Server 2:	Not registered
Nightringer Server:	Not registered
Intrusion Sensor:	Inactive

Admin Settings

Username: admin
Password: •••••
Confirm Password: •••••

Import Settings

No file chosen

Export Settings

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

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

Table 2-8. Home Page Overview

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

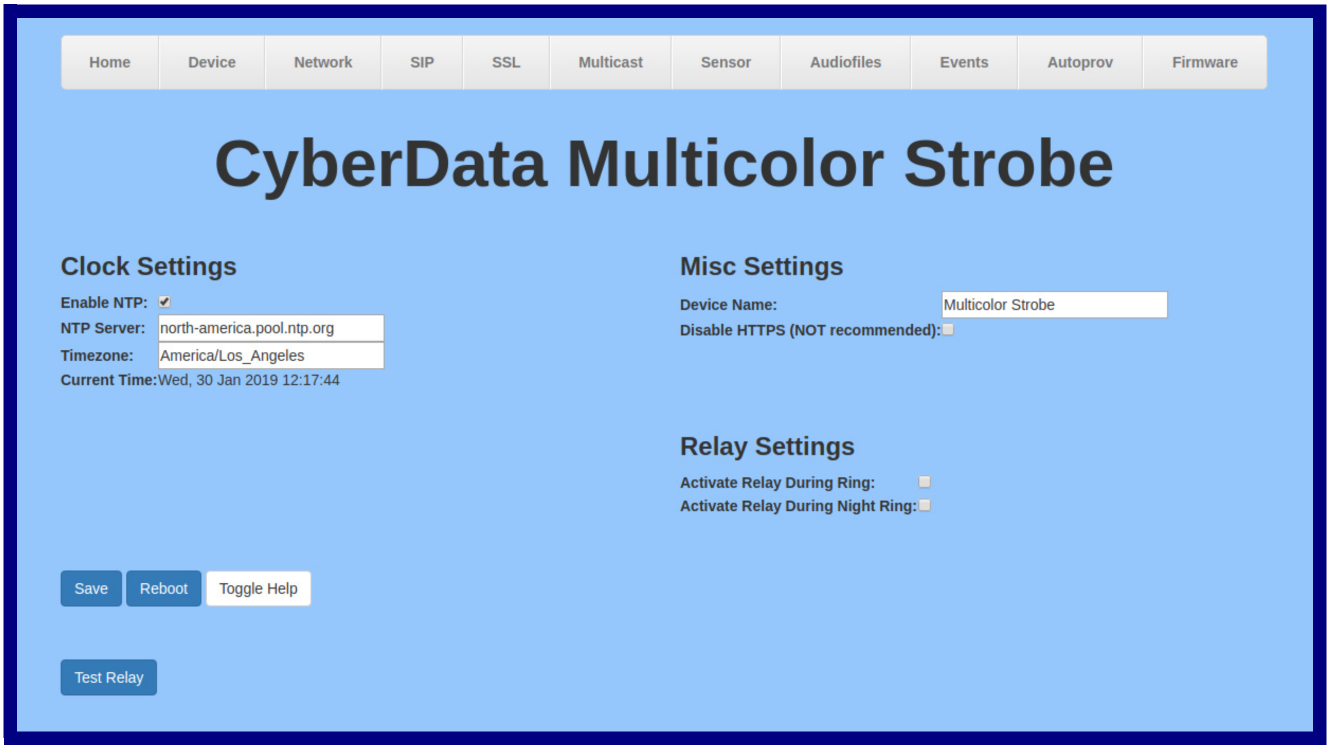
Table 2-8. Home Page Overview (continued)

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

2.3.5 Configure the Device

1. Click the **Device** menu button to open the **Device** page. See Figure 2-15.

Figure 2-15. Device Configuration Page



CyberData Multicolor Strobe

Clock Settings

Enable NTP: ☑

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

Timezone: America/Los_Angeles

Current Time: Wed, 30 Jan 2019 12:17:44

Misc Settings

Device Name: Multicolor Strobe

Disable HTTPS (NOT recommended): □

Relay Settings

Activate Relay During Ring: □

Activate Relay During Night Ring: □

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

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

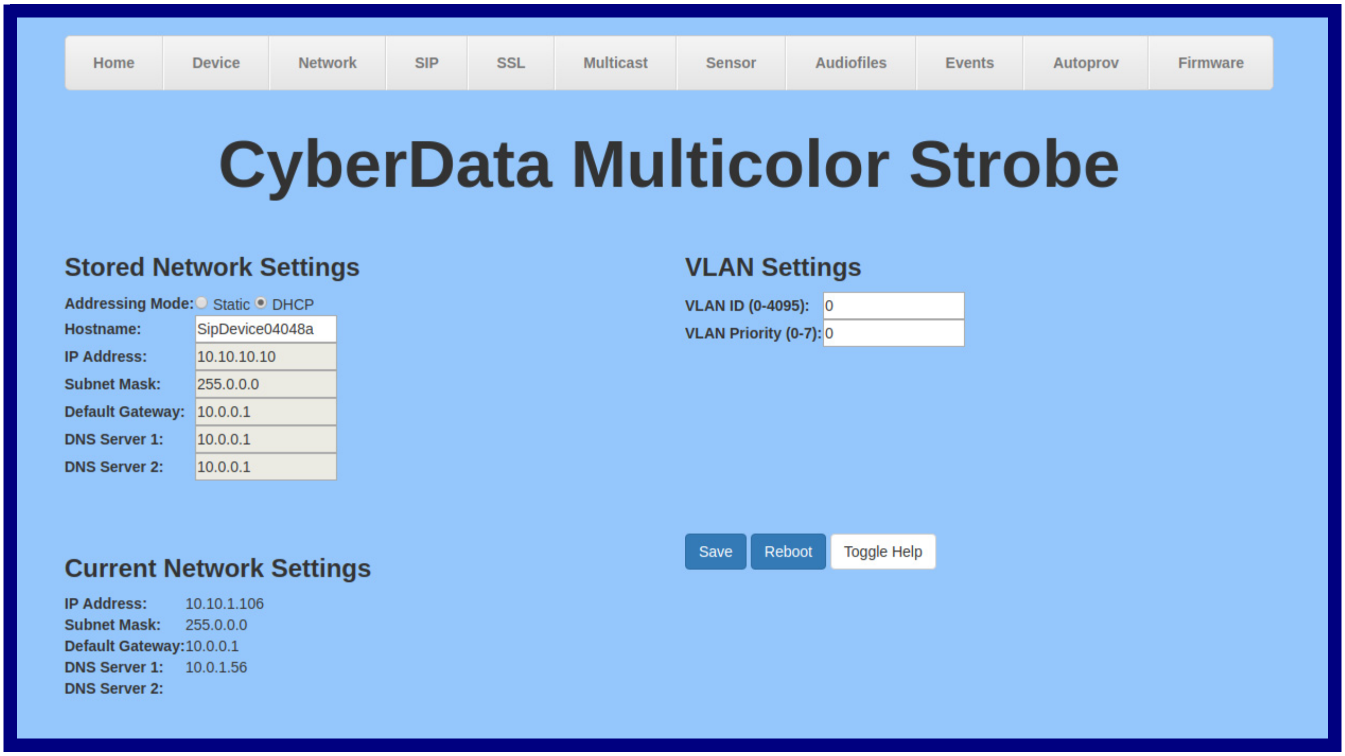
Table 2-9. Device Configuration Parameters

Web Page Item	Description
Clock Settings	
Enable NTP ?	Sync device's local time with the specified NTP Server.
NTP Server ?	Use this field to set the address (in IPv4 dotted decimal notation or as a canonical name) for the NTP Server. This field can accept canonical names of up to 64 characters in length.
Timezone	Enter the tz database string of your timezone. Examples: America/Los_Angeles America/New_York Europe/London America/Toronto See **https://en.wikipedia.org/wiki/List_of_tz_database_time_zones** for a full list of valid strings.
Current Time	Displays the current time.
Misc Settings	
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. **Note** This setting requires a reboot for the changes to take effect.
Relay Settings	
Activate Relay During Ring ?	When selected, the relay will be activated for as long as the device is ringing.
Activate Relay During Night Ring ?	When selected, the relay will be activated as long as the Nightringer extension is ringing.
Test Relay	Click on the **Test Relay** button to do a relay test.
Save	Click the **Save** button to save your configuration settings.
Reboot	Click on the **Reboot** button to reboot the system.
Toggle Help	Click on the **Toggle Help** button to see a short description of some of the web page items. First click on the **Toggle Help** button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

2.3.6 Configure the Network Parameters

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

Figure 2-16. Network Configuration Page



Stored Network Settings

Addressing Mode: ○ Static ● DHCP
Hostname: SipDevice04048a
IP Address: 10.10.10.10
Subnet Mask: 255.0.0.0
Default Gateway: 10.0.0.1
DNS Server 1: 10.0.0.1
DNS Server 2: 10.0.0.1

VLAN Settings

VLAN ID (0-4095): 0
VLAN Priority (0-7): 0

Current Network Settings

IP Address: 10.10.1.106
Subnet Mask: 255.0.0.0
Default Gateway: 10.0.0.1
DNS Server 1: 10.0.1.56
DNS Server 2:

2. On the **Network** page, enter values for the parameters indicated in Table 2-10.

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

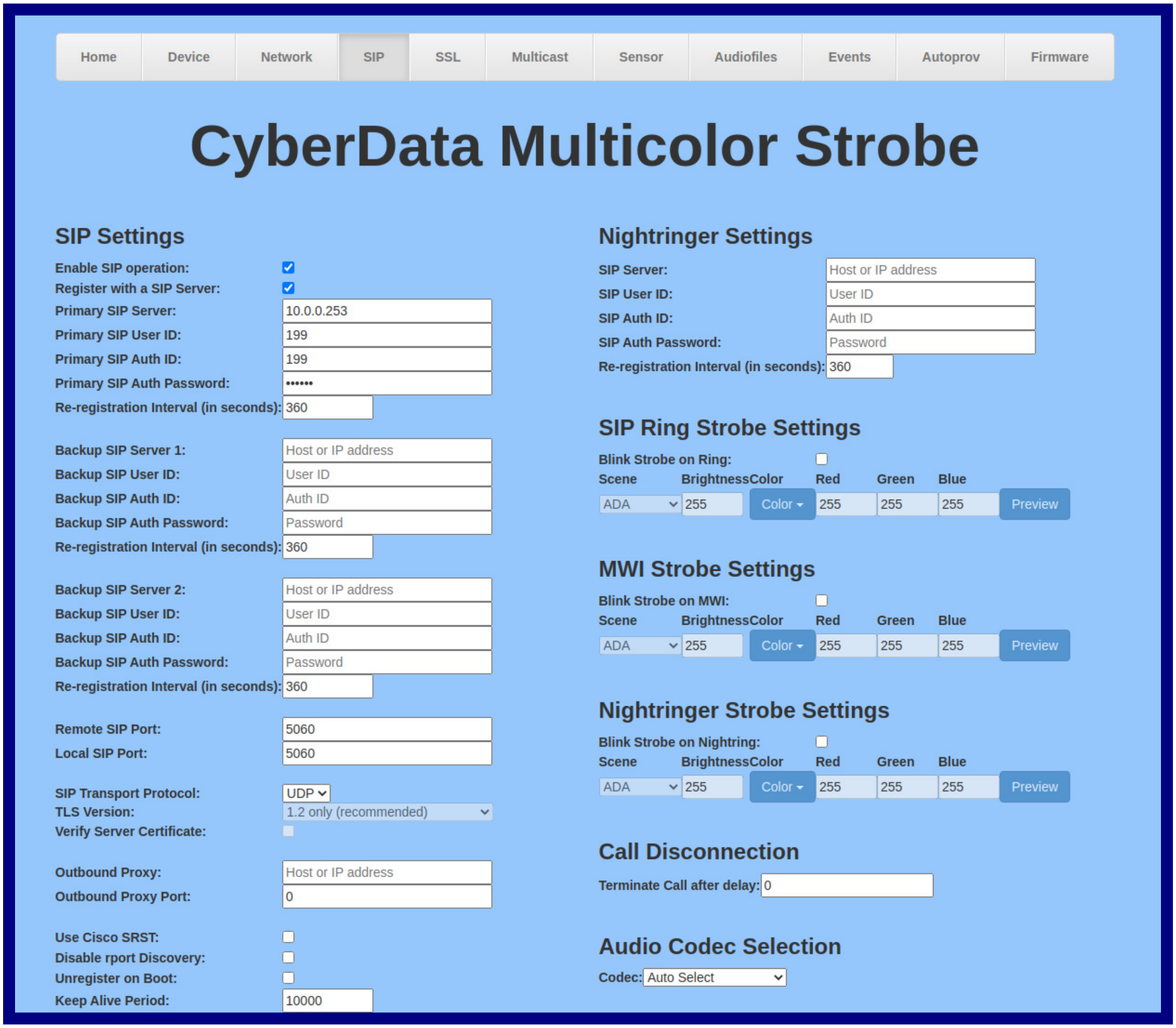
Table 2-10. Network Configuration Parameters

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

2.3.7 Configure the SIP Parameters

The SIP parameters enable the device to contact and register with the SIP server. On the Home page, click **SIP Config** to open the **SIP** page.

Figure 2-17. SIP Page



CyberData Multicolor Strobe

SIP Settings

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

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

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

Remote SIP Port: 5060
Local SIP Port: 5060

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

Outbound Proxy: Host or IP address
Outbound Proxy Port: 0

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

Nightringer Settings

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

SIP Ring Strobe Settings

Blink Strobe on Ring: □

Scene	Brightness	Color	Red	Green	Blue
ADA	255	Color ▾	255	255	255

MWI Strobe Settings

Blink Strobe on MWI: □

Scene	Brightness	Color	Red	Green	Blue
ADA	255	Color ▾	255	255	255

Nightringer Strobe Settings

Blink Strobe on Nightring: □

Scene	Brightness	Color	Red	Green	Blue
ADA	255	Color ▾	255	255	255

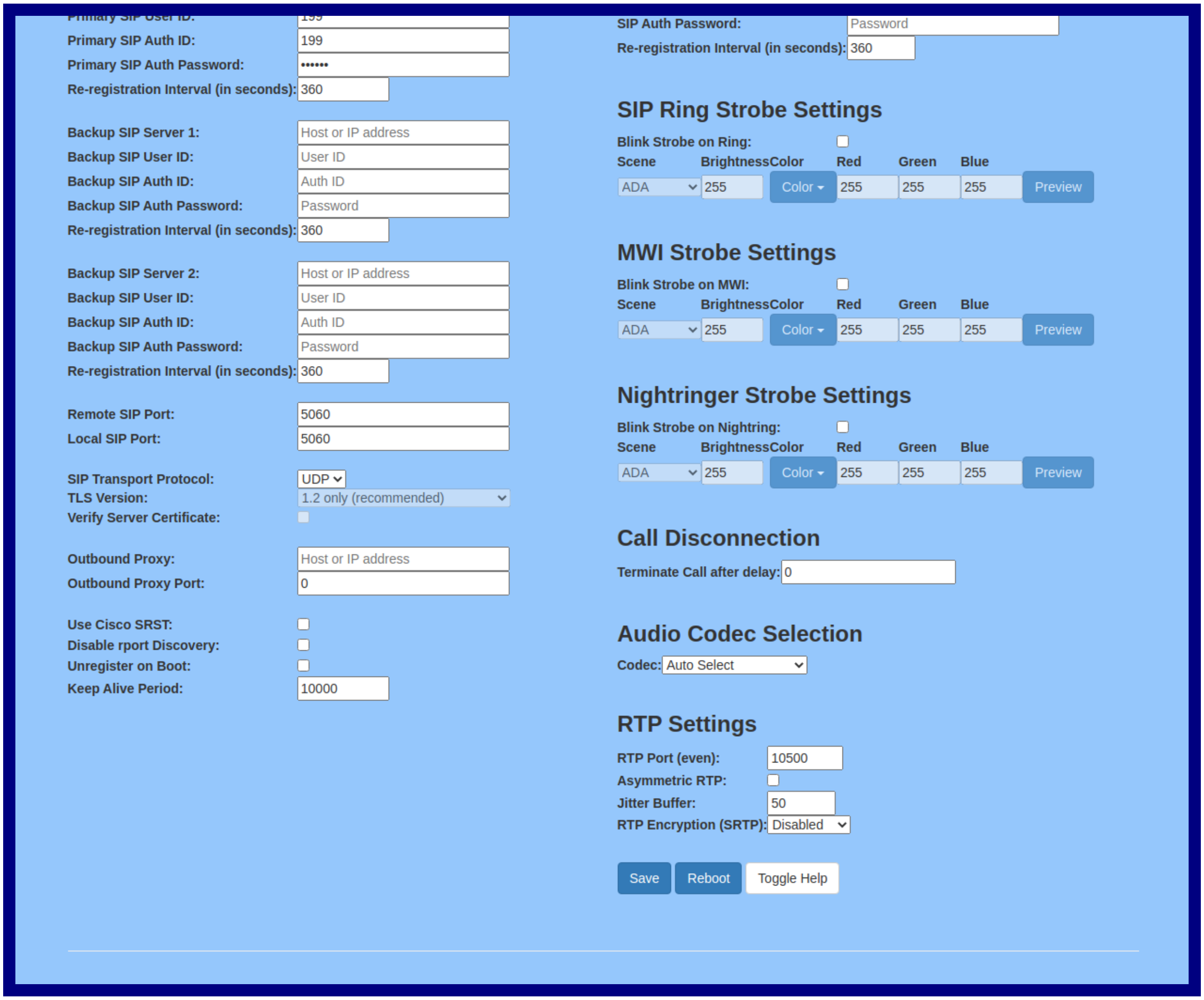
Call Disconnection

Terminate Call after delay: 0

Audio Codec Selection

Codec: Auto Select

Figure 2-18. SIP Page



Primary SIP User ID: 199
Primary SIP Auth ID: 199
Primary SIP Auth Password: ••••••
Re-registration Interval (in seconds): 360

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

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

Remote SIP Port: 5060
Local SIP Port: 5060

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

Outbound Proxy: Host or IP address
Outbound Proxy Port: 0

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

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

SIP Ring Strobe Settings

Blink Strobe on Ring: ☐

Scene	Brightness	Color	Red	Green	Blue	
ADA	255	Color ▾	255	255	255	Preview

MWI Strobe Settings

Blink Strobe on MWI: ☐

Scene	Brightness	Color	Red	Green	Blue	
ADA	255	Color ▾	255	255	255	Preview

Nightringer Strobe Settings

Blink Strobe on Nightring: ☐

Scene	Brightness	Color	Red	Green	Blue	
ADA	255	Color ▾	255	255	255	Preview

Call Disconnection

Terminate Call after delay: 0

Audio Codec Selection

Codec: Auto Select

RTP Settings

RTP Port (even): 10500
Asymmetric RTP: ☐
Jitter Buffer: 50
RTP Encryption (SRTP): Disabled

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

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

Table 2-11. SIP Configuration Parameters

Web Page Item	**Description**
SIP Settings	
Enable SIP Operation ?	When enabled, the device will transmit, receive, and process SIP messages according to the configured SIP settings below.
Register with a SIP Server ?	When enabled, the device will attempt to register to the configured SIP Server(s) on this page. To configure the device to send and receive point-to-point SIP calls, enable **SIP Operation** and disable **Register with a SIP Server** (see Section 2.3.7.1, "Point-to-Point Configuration").
Primary SIP Server ?	Enter the SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the primary SIP server. This field can accept entries of up to 255 characters in length.
Primary SIP User ID ?	Specify the SIP User ID for the Primary SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the primary SIP server. Enter up to 64 alphanumeric characters.
Primary SIP Auth ID ?	Specify the Authenticate ID for the Primary SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Primary SIP Auth Password ?	Specify the Authenticate Password for the Primary SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Re-registration Interval (in seconds) ?	The SIP Re-registration interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
Backup SIP Server 1 ?	Enter the backup SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the backup SIP server. This field can accept entries of up to 255 characters in length.
Backup SIP User ID ?	Specify the SIP User ID for the first backup SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the first backup SIP server. Enter up to 64 alphanumeric characters.
Backup SIP Auth ID ?	Specify the Authenticate ID for the first backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Auth Password ?	Specify the Authenticate Password for the first backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Re-registration Interval (in seconds) ?	The SIP Re-registration interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
Backup SIP Server 2 ?	Enter a second backup SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the second backup SIP server. This field can accept entries of up to 255 characters in length.
Backup SIP User ID ?	Specify the SIP User ID for the second backup SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the second backup SIP server. Enter up to 64 alphanumeric characters.
Backup SIP Auth ID ?	Specify the Authenticate ID for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.

Table 2-11. SIP Configuration Parameters (continued)

Web Page Item	Description
Backup SIP Auth Password ?	Specify the Authenticate Password for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Re-registration Interval (in seconds) ?	The SIP Re-registration interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
Remote SIP Port ?	The Remote SIP Port is the port number the device will use as the destination port when sending SIP messages. The default Remote SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
Local SIP Port ?	The Local SIP Port is the port number the device will use to receive SIP messages. The default Local SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
SIP Transport Protocol ?	Choose the transport protocol for SIP signaling. This will affect all extensions, including the Nightringer. Default is UDP.
TLS Version ?	Choose the TLS version for SIP over TLS. Modern security standards strongly recommend using TLS 1.2.
Verify Server Certificate ?	When enabled, the device will verify the authenticity of the server during the TLS handshake by its certificate and common name. The TLS handshake will be aborted if the server is deemed to be inauthentic and SIP registration will not proceed.
Outbound Proxy ?	Enter the Outbound Proxy address as an IPv4 address in dotted decimal notation or a fully qualified domain name (FQDN). When an IP address is configured, the device will send all SIP messages to this IP address. When an FQDN is configured, the device will run DNS NAPTR, SRV, and A queries on the FQDN to resolve an IP address to which it will send all SIP messages. This field can accept entries of up to 255 characters in length.
Outbound Proxy Port ?	The Outbound Proxy Port is port number used as the destination port when sending SIP messages to the outbound proxy. A value of 0 will default to 5060. The supported range is 0-65536. Enter up to 5 digits.
Use Cisco SRST ?	When enabled, the backup servers are handled according to Cisco SRST (Survivable Remote Site Telephony). It is required for use in clustered Cisco Unified Communications Manager topologies.
Disable rport Discovery ?	Disabling rport Discovery will prevent the device from including the public WAN IP address and port number in the contact information that is sent to the remote SIP servers. This will generally only need to be enabled when using an SBC or SIP ALG in conjunction with a remote SIP server.
Unregister on Boot ?	When enabled, the device will send one registration with an expiry of 0 on boot.
Keep Alive Period ?	The minimum time in milliseconds between keep-alive packets sent for nat traversal. A value of 0 will disable keep alive packets.
Nightringer Settings	
SIP Server ?	Enter the SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's Nightringer extension on the SIP server. This field can accept entries of up to 255 characters in length.
SIP User ID ?	Specify the SIP User ID for the SIP server. This parameter becomes the user portion of the SIP-URI for the device's Nightringer extension. Enter up to 64 alphanumeric characters.
SIP Auth ID ?	Specify the Authenticate ID for the SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.

Table 2-11. SIP Configuration Parameters (continued)

Web Page Item	Description
SIP Auth Password ?	Specify the Authenticate Password for the SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Re-registration Interval (in seconds) ?	The SIP Re-registration Interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
Relay rings to multicast ?	When selected, the device will play ring tones to the specified multicast address and port.
Multicast Address ?	The multicast address used for nightring audio.
Multicast Port ?	The multicast port used for nightring audio.
Call Disconnection	
Terminate Call After Delay ?	Automatically terminate an active call after a given delay in seconds. A value of 0 will disable this function. Enter up to 8 digits.
Audio Codec Selection	
Codec ?	Select desired codec (only one may be chosen).
RTP Settings	
RTP Port (even) ?	Specify the port number used for the RTP stream after establishing a SIP call. This port number must be an even number and defaults to 10500. The supported range is 0-65536. Enter up to 5 digits.
Asymmetric RTP ?	Specify if the remote endpoint will send and receive RTP packets on different ports. If set to false, the device will track the address/port that is sending RTP packets during a SIP call. If the address/port changes mid-stream, the device will disregard the SDP and send all further RTP packets to this new address. If set to true, this device will ignore the sending address/port and send RTP as specified in the SDP. Warning! Enabling asymmetric RTP can cause the RTP stream to be lost. Most installations should not enable asymmetric RTP.
Jitter Buffer ?	Specify the size of the jitter buffer (in milliseconds) used for SIP calls. Valid values are 50-1000.
RTP Encryption (SRTP) ?	When enabled, a SIP call's audio streams are encrypted using SRTP.
Save	Click the **Save** button to save your configuration settings.
Reboot	Click on the **Reboot** button to reboot the system.
Toggle Help	Click on the **Toggle Help** button to see a short description of some of the web page items. First click on the **Toggle Help** button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

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

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

1. Enter the IP address of the **SIP Server.**
2. Enter the port numbers used for SIP signaling:

   a. **Remote SIP Port**
   b. **Local SIP Port**

3. Enter the SIP registration parameters:
   a. **SIP User ID**
   b. **Authenticate ID**
   c. **Authenticate Password**
4. For **SIP Registration**, designate whether you want the VoIP Paging Server to register with your SIP server.
5. At **Unregister on Reboot**:
   a. Select **Yes** to automatically unregister the SIP RGB Strobe when you reboot it.
   b. Select **No** to keep the SIP RGB Strobe registered when you reboot it.
6. In the **Register Expiration** field, enter the number of seconds the SIP RGB Strobe registration lease remains valid with the SIP Server. The SIP RGB Strobe automatically re-registers with the SIP server before the lease expiration timeout.

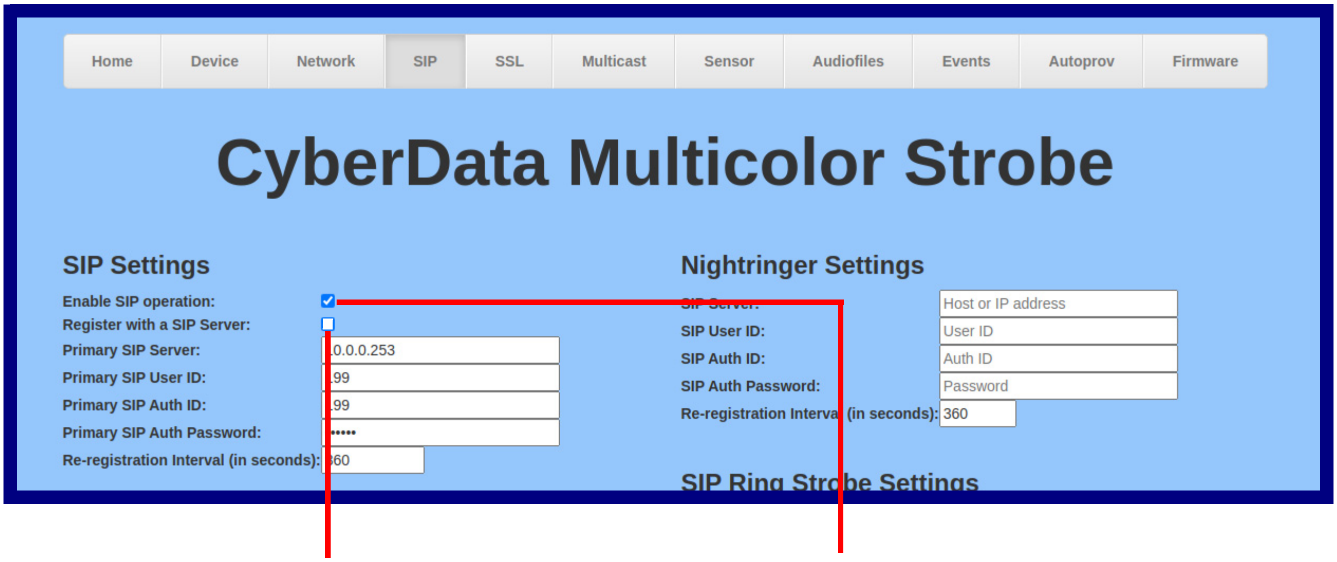
2.3.7.1 Point-to-Point Configuration

It is possible to use the device as a paging endpoint without registering it with a SIP server by configuring it for Point-to-Point paging. To do this, complete the following steps:

1. On the **SIP** page (Figure 2-19), make sure of the following:
   - The **Register with a SIP Server** parameter is not selected.
   - The **Enable SIP Operation** parameter is selected
2. Click on the **Save** button to save the changes.
3. Click on the **Reboot** button to reboot the device.
4. Enter the device's IP address as a “speed dial” (also called “auto-dial”) key on the phone(s) from which you want to page.

Note Establishing point-to-point SIP calls may not work with all phones.

Figure 2-19. SIP Page



SIP Settings

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

Nightringer Settings

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

SIP Ring Strobe Settings

Register with a SIP Server is not selected

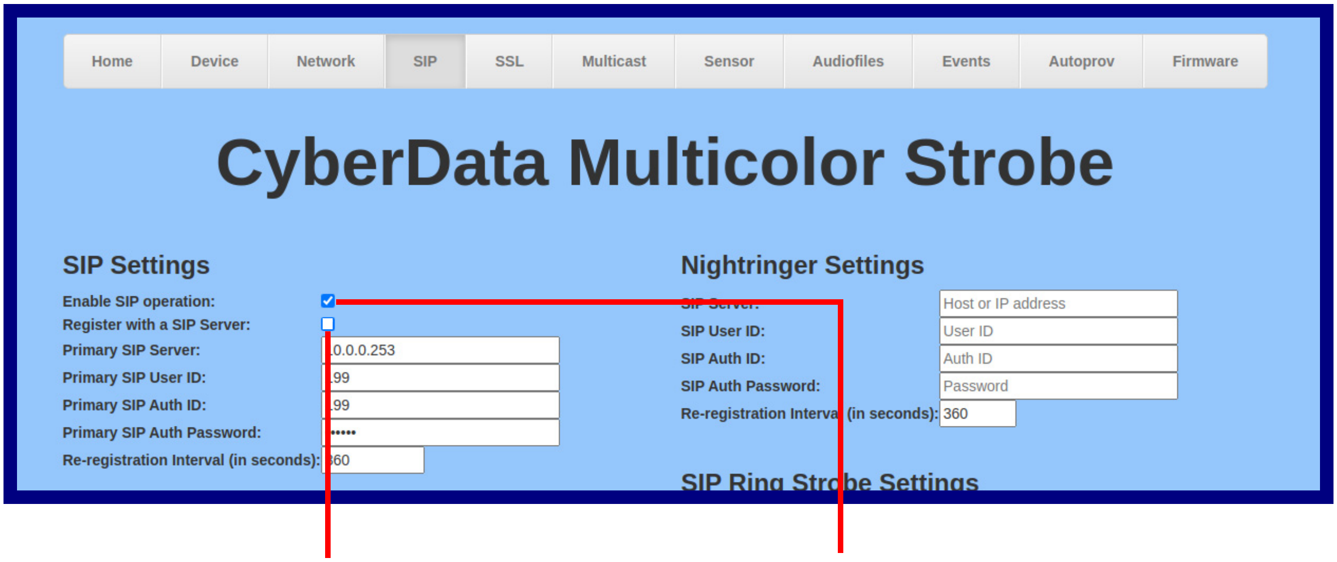
Enable SIP Operation is selected

2.3.7.2 Point-to-Point Fault Sense Reporting

It is possible to use the device to report faults detected at the device's Fault Sense Input without registering it with a SIP server by configuring it for Point-to-Point Fault Sense reporting. To do this, complete the following steps:

1. On the **SIP** page (Figure 2-20), make sure of the following:
   - The **Register with a SIP Server** parameter is not selected.
   - The **Enable SIP Operation** parameter is selected

Figure 2-20. SIP Page



CyberData Multicolor Strobe

SIP Settings

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

Nightringer Settings

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

SIP Ring Strobe Settings

Register with a SIP Server is not selected

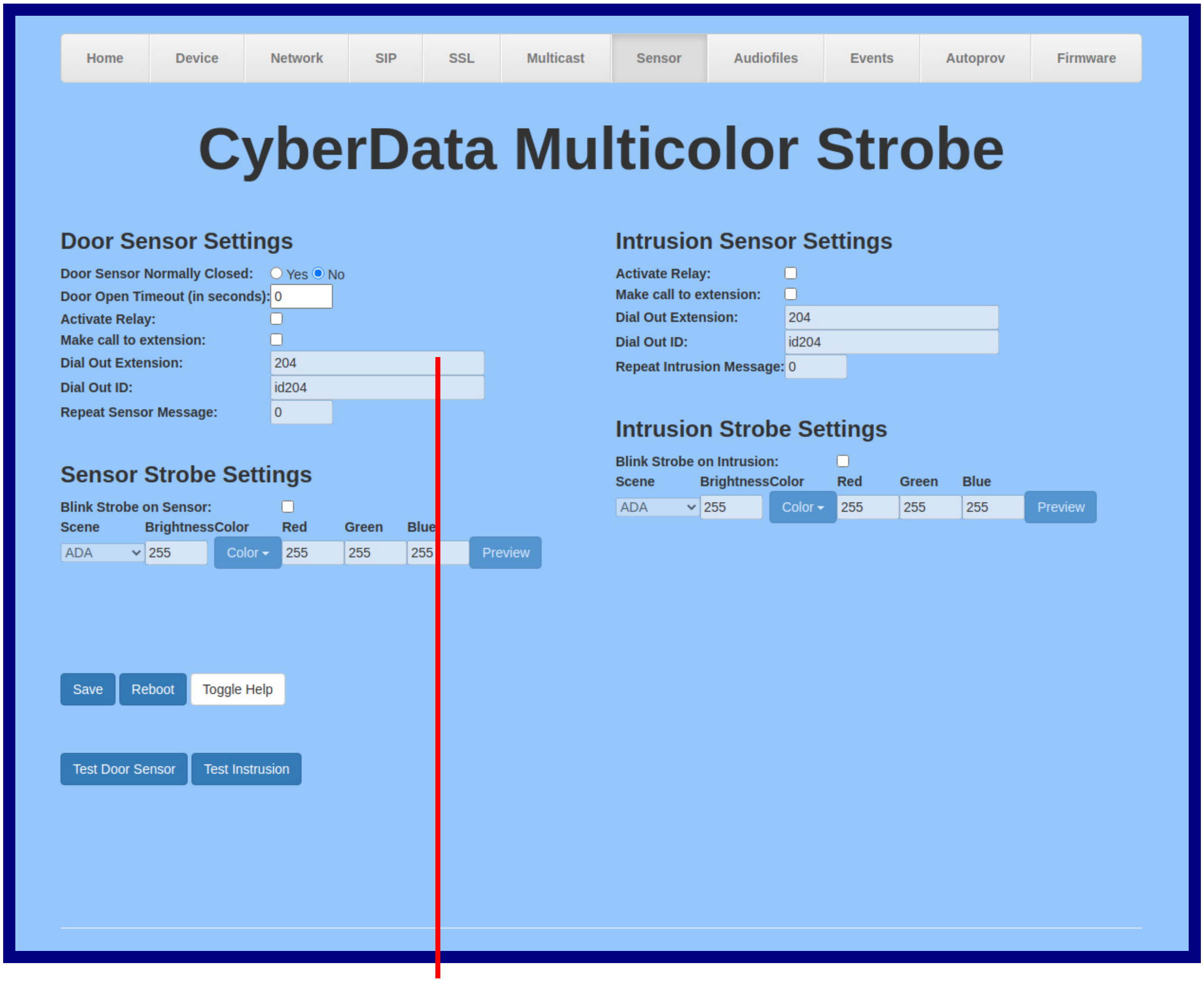
Enable SIP Operation is selected

2. Click on the **Save** button to save the changes.
3. Click on the **Reboot** button to reboot the device.

4. On the **Sensor** page (Figure 2-21) in the **Dial Out Extension** field, enter the IP address of the phone that is to be called when a fault is detected at the Fault Sense Input.

Note Establishing point-to-point SIP calls may not work with all phones.

Figure 2-21. Sensor Page



CyberData Multicolor Strobe

Door Sensor Settings

Door Sensor Normally Closed: ○ Yes ● No
Door Open Timeout (in seconds): 0
Activate Relay: ☐
Make call to extension: ☐
Dial Out Extension: 204
Dial Out ID: id204
Repeat Sensor Message: 0

Sensor Strobe Settings

Blink Strobe on Sensor: ☐

Scene	Brightness	Color	Red	Green	Blue
ADA	255	Color ▾	255	255	255

Intrusion Sensor Settings

Activate Relay: ☐
Make call to extension: ☐
Dial Out Extension: 204
Dial Out ID: id204
Repeat Intrusion Message: 0

Intrusion Strobe Settings

Blink Strobe on Intrusion: ☐

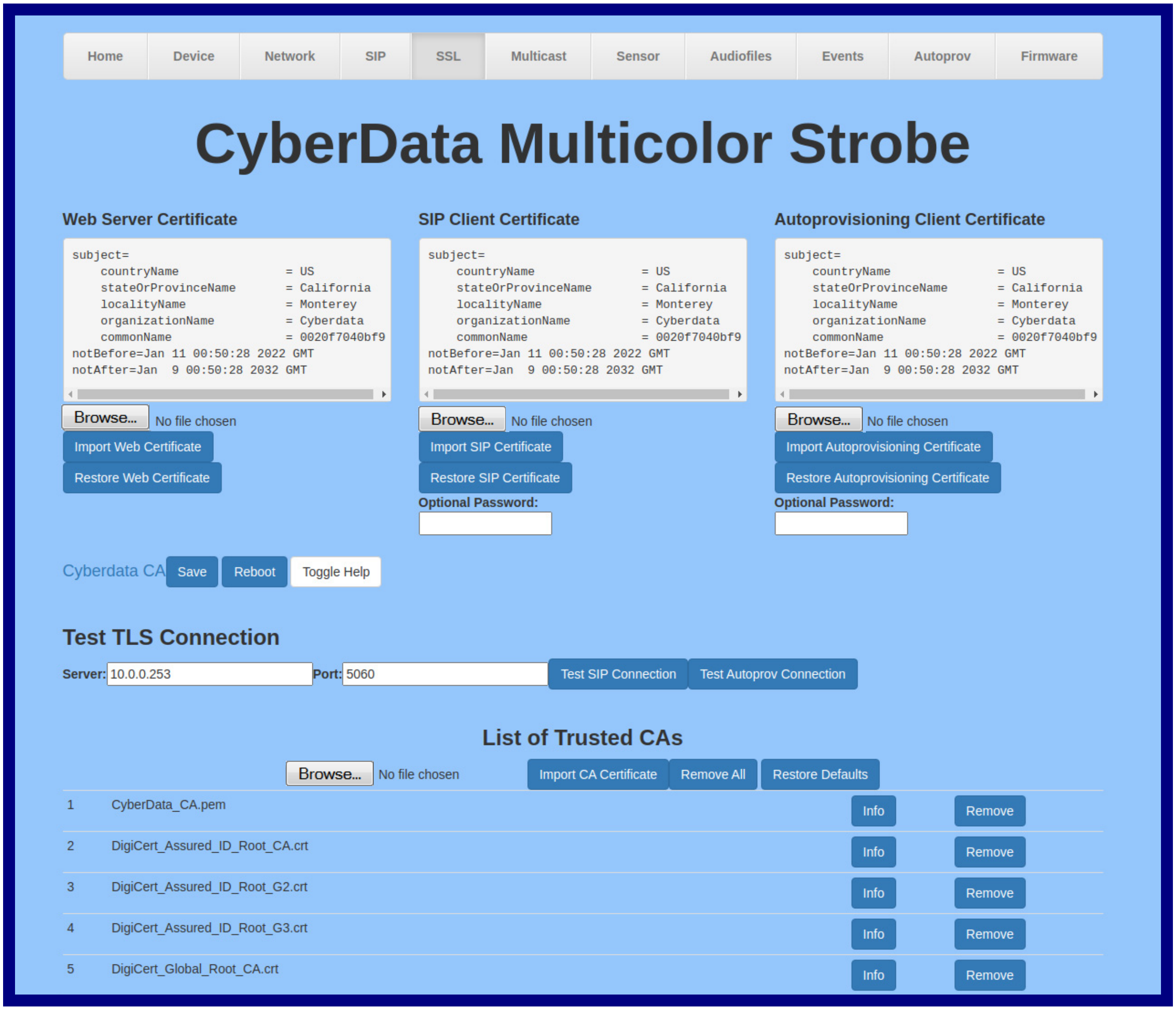
Scene	Brightness	Color	Red	Green	Blue
ADA	255	Color ▾	255	255	255

In the **Dial Out Extension** field, enter the IP address of the phone that is to be called when a fault is detected at the Fault Sense Input.

2.3.8 Configure the SSL Parameters

1. Click **SSL** menu button to open the **SSL** page (Figure 2-22 and Figure 2-23).

Figure 2-22. SSL Configuration Page



CyberData Multicolor Strobe

Web Server Certificate

```
subject=
    countryName               = US
    stateOrProvinceName       = California
    localityName              = Monterey
    organizationName          = Cyberdata
    commonName                = 0020f7040bf9
notBefore=Jan 11 00:50:28 2022 GMT
notAfter=Jan  9 00:50:28 2032 GMT
```

SIP Client Certificate

```
subject=
    countryName               = US
    stateOrProvinceName       = California
    localityName              = Monterey
    organizationName          = Cyberdata
    commonName                = 0020f7040bf9
notBefore=Jan 11 00:50:28 2022 GMT
notAfter=Jan  9 00:50:28 2032 GMT
```

Optional Password:

Autoprovisioning Client Certificate

```
subject=
    countryName               = US
    stateOrProvinceName       = California
    localityName              = Monterey
    organizationName          = Cyberdata
    commonName                = 0020f7040bf9
notBefore=Jan 11 00:50:28 2022 GMT
notAfter=Jan  9 00:50:28 2032 GMT
```

Browse... No file chosen
Import Autoprovisioning Certificate
Restore Autoprovisioning Certificate

Optional Password:

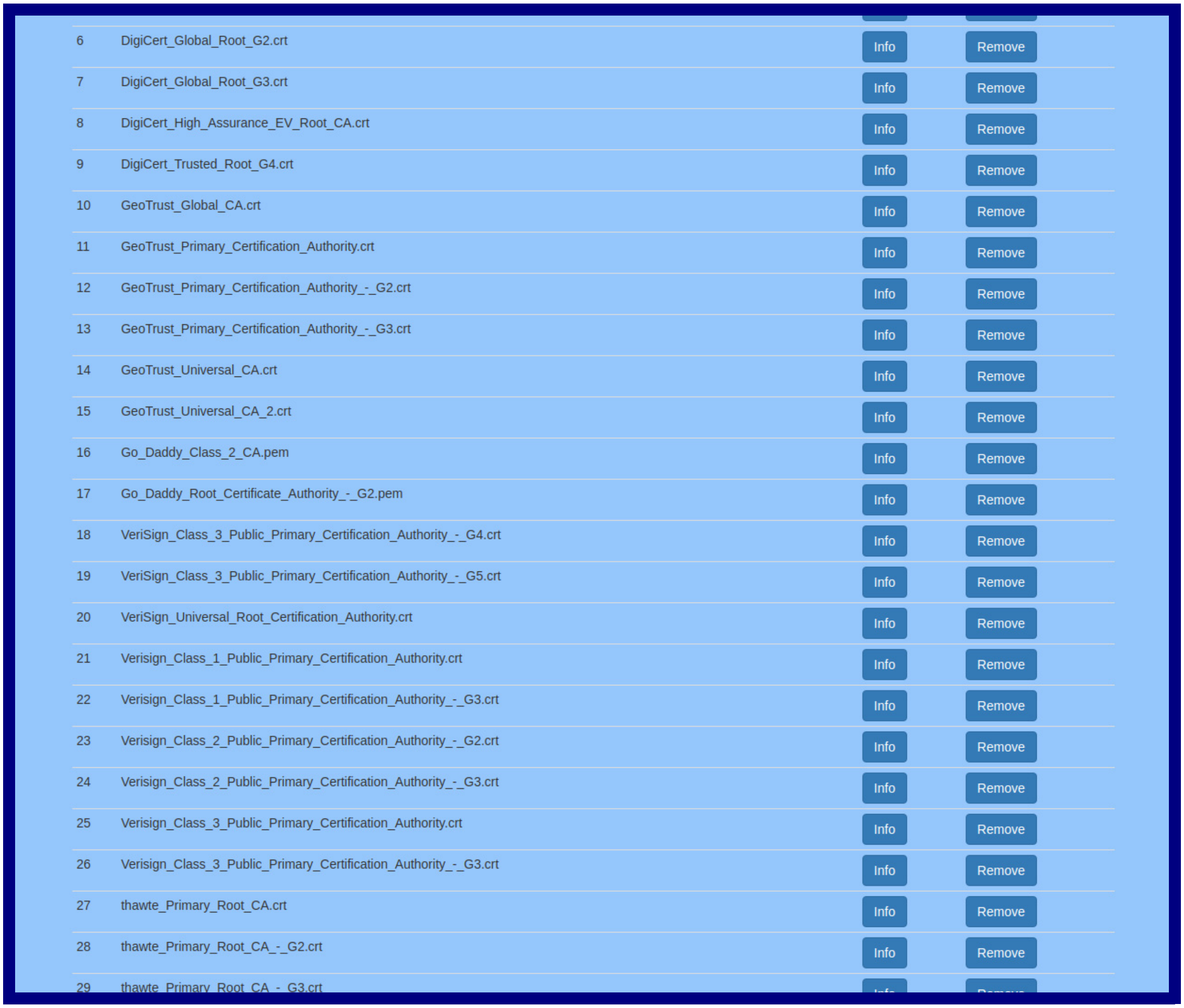
Test TLS Connection

Server: 10.0.0.253 Port: 5060

List of Trusted CAs

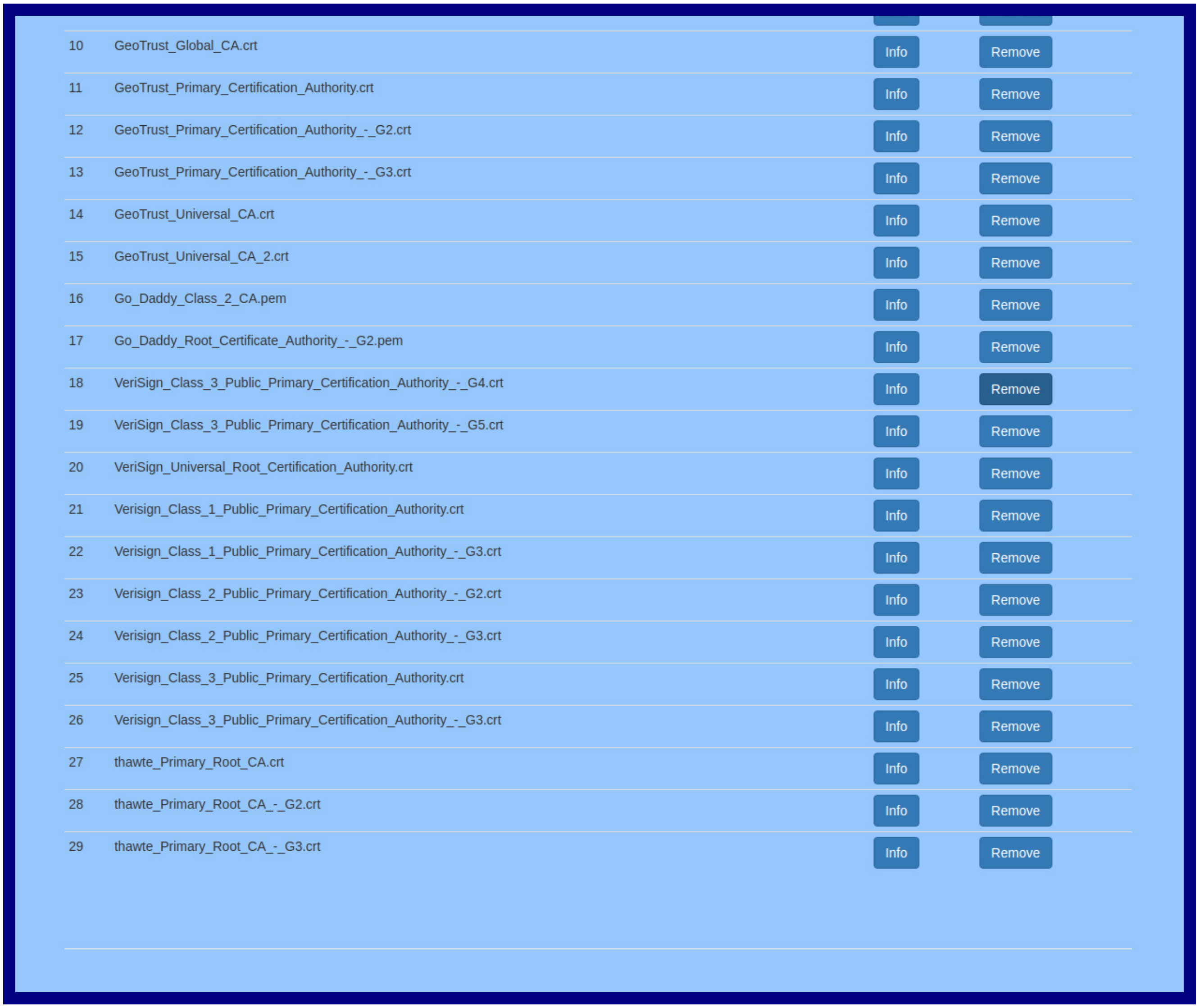
1	CyberData_CA.pem	Info	Remove
2	DigiCert_Assured_ID_Root_CA.crt	Info	Remove
3	DigiCert_Assured_ID_Root_G2.crt	Info	Remove
4	DigiCert_Assured_ID_Root_G3.crt	Info	Remove
5	DigiCert_Global_Root_CA.crt	Info	Remove

Figure 2-23. SSL Configuration Page



6	DigiCert_Global_Root_G2.crt	Info	Remove
7	DigiCert_Global_Root_G3.crt	Info	Remove
8	DigiCert_High_Assurance_EV_Root_CA.crt	Info	Remove
9	DigiCert_Trusted_Root_G4.crt	Info	Remove
10	GeoTrust_Global_CA.crt	Info	Remove
11	GeoTrust_Primary_Certification_Authority.crt	Info	Remove
12	GeoTrust_Primary_Certification_Authority_-_G2.crt	Info	Remove
13	GeoTrust_Primary_Certification_Authority_-_G3.crt	Info	Remove
14	GeoTrust_Universal_CA.crt	Info	Remove
15	GeoTrust_Universal_CA_2.crt	Info	Remove
16	Go_Daddy_Class_2_CA.pem	Info	Remove
17	Go_Daddy_Root_Certificate_Authority_-_G2.pem	Info	Remove
18	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G4.crt	Info	Remove
19	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5.crt	Info	Remove
20	VeriSign_Universal_Root_Certification_Authority.crt	Info	Remove
21	Verisign_Class_1_Public_Primary_Certification_Authority.crt	Info	Remove
22	Verisign_Class_1_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
23	Verisign_Class_2_Public_Primary_Certification_Authority_-_G2.crt	Info	Remove
24	Verisign_Class_2_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
25	Verisign_Class_3_Public_Primary_Certification_Authority.crt	Info	Remove
26	Verisign_Class_3_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
27	thawte_Primary_Root_CA.crt	Info	Remove
28	thawte_Primary_Root_CA_-_G2.crt	Info	Remove
29	thawte_Primary_Root_CA_-_G3.crt	Info	Remove

Figure 2-24. SSL Configuration Page



10	GeoTrust_Global_CA.crt	Info	Remove
11	GeoTrust_Primary_Certification_Authority.crt	Info	Remove
12	GeoTrust_Primary_Certification_Authority_-_G2.crt	Info	Remove
13	GeoTrust_Primary_Certification_Authority_-_G3.crt	Info	Remove
14	GeoTrust_Universal_CA.crt	Info	Remove
15	GeoTrust_Universal_CA_2.crt	Info	Remove
16	Go_Daddy_Class_2_CA.pem	Info	Remove
17	Go_Daddy_Root_Certificate_Authority_-_G2.pem	Info	Remove
18	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G4.crt	Info	Remove
19	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5.crt	Info	Remove
20	VeriSign_Universal_Root_Certification_Authority.crt	Info	Remove
21	Verisign_Class_1_Public_Primary_Certification_Authority.crt	Info	Remove
22	Verisign_Class_1_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
23	Verisign_Class_2_Public_Primary_Certification_Authority_-_G2.crt	Info	Remove
24	Verisign_Class_2_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
25	Verisign_Class_3_Public_Primary_Certification_Authority.crt	Info	Remove
26	Verisign_Class_3_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
27	thawte_Primary_Root_CA.crt	Info	Remove
28	thawte_Primary_Root_CA_-_G2.crt	Info	Remove
29	thawte_Primary_Root_CA_-_G3.crt	Info	Remove

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

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

Table 2-12. SSL Configuration Parameters

Web Page Item	**Description**
Web Server Certificate	Certificate used by the web server.
Browse...	Click **Browse** to select a certificate to import.
Import Web Certificate	After selecting a certificate, click **Import Web Certificate** to import it as the certificate used by this device's web server.
Restore Web Certificate	Restore the device's default web server certificate. This will remove the user-uploaded Web Server Certificate.(Server CAs and Trusted CAs are unaffected).
SIP Client Certificate	When doing mutual authentication this device will present a client certificate with these parameters.
Browse...	Click **Browse** to select a certificate to import.
Import SIP Certificate	After selecting a certificate, click **Import SIP Certificate** to import it as the certificate used by the device during SIP transactions.
Restore SIP Certificate	Restore the device's default sip client certificate. This will remove any user-uploaded sip client certificates (Server CAs and Trusted CAs are unaffected).
Optional Password	Enter the optional password for the SIP certificate's private key. **Note**: When using a password, it must be entered and saved before importing the certificate.
Autoprovisioning Client Certificate	When doing mutual authentication this device will present a client certificate with these parameters.
Browse...	Click **Browse** to select a certificate to import.
Import Autoprovisioning Certificate	After selecting a certificate, click **Import Autoprovisioning Certificate** to import it as this device's certificate. This certificate will be used when requesting files during autoprovisioning.
Restore Autoprovisioning Certificate	Restore the device's default autoprovisioning certificate. This will remove any user-uploaded autoprovisioning certificates. (Server CAs and Trusted CAs are unaffected).
Optional Password ?	Enter the optional password for the Autoprovisioning certificate's private key. **Note**: When using a password, it must be entered and saved before importing the certificate.
Cyberdata CA ?	Right click and **Save Link As...** to get the Cyberdata CA used to sign this client certificate.

Table 2-12. SSL Configuration Parameters (continued)

Web Page Item	Description
Save	Click the **Save** button to save your configuration settings.
Reboot	Click on the **Reboot** button to reboot the system.
Toggle Help	Click on the **Toggle Help** button to see a short description of some of the web page items. First click on the **Toggle Help** button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.
Test TLS Connection	
Server ?	The ssl test server address as a fully qualified domain name or in IPv4 dotted decimal notation.
Port ?	The supported range is 0-65536. SIP connections over TLS to port 5060 are modified to connect to port 5061. This test button will do the same.
Test SIP Connection	Use this button to test a TLS connection to a remote server using the sip client key and password. This will attempt to make a socket connection to the configured test server and port and report the success or failure. This can be used to debug TLS connection issues separate from SIP registration issues.
Test Autoprov Connection	Use this button to test a TLS connection to a remote server using the autoprovisioning client key and password. This will attempt to make a socket connection to the configured test server and port and report the success or failure. This can be used to debug TLS connection issues with secure autoprovisioning.
List of Trusted CAs	
Browse...	Use this button to select a configuration file to import.
Import CA Certificate	Click **Browse** to select a CA certificate to import. After selecting a server certificate authority (CA), click **Import CA Certificate** to import it to the list of trusted CAs. CAs are used to validate the certificate presented by the server when establishing a TLS connection.
Restore Defaults	**Restore Defaults** will restore the default list of registered CAs and **Remove All** will remove all registered CAs.
Remove All	**Restore Defaults** will restore the default list of registered CAs and **Remove All** will remove all registered CAs.
Info	Provides details of the certificate. After clicking on this button, the **Certificate Info Window** appears. See Section 2.3.8.1, "Certificate Info Window".

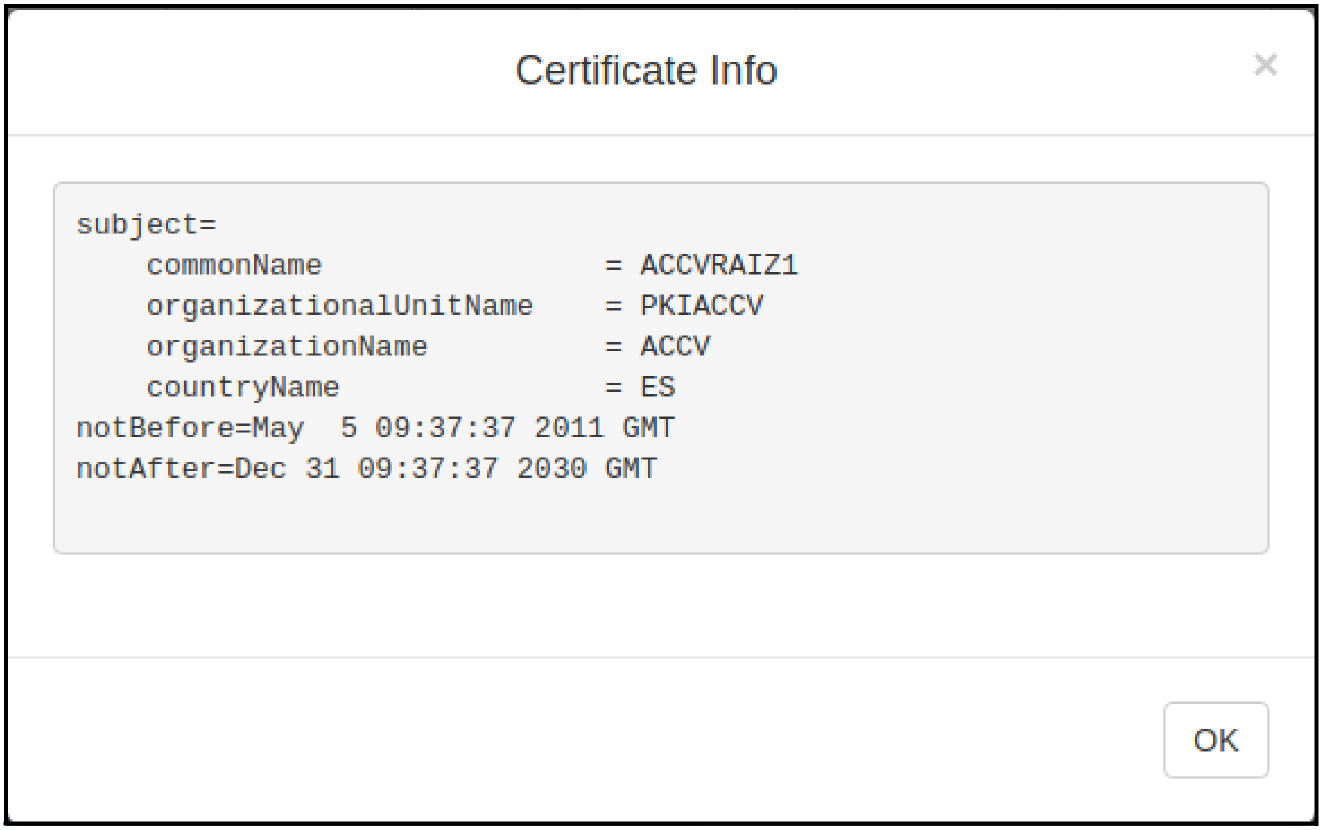
Table 2-12. SSL Configuration Parameters (continued)

Web Page Item	Description
Remove	Removes this certificate from the list of trusted certificates. After clicking on this button, the **Remove Server Certificate Window** appears. See Section 2.3.8.2, "Remove Server Certificate Window".

2.3.8.1 Certificate Info Window

The **Certificate Info Window** provides details of the certificate. This window appears after clicking on the **Info** button. See Figure 2-25.

Figure 2-25. Certificate Info Window

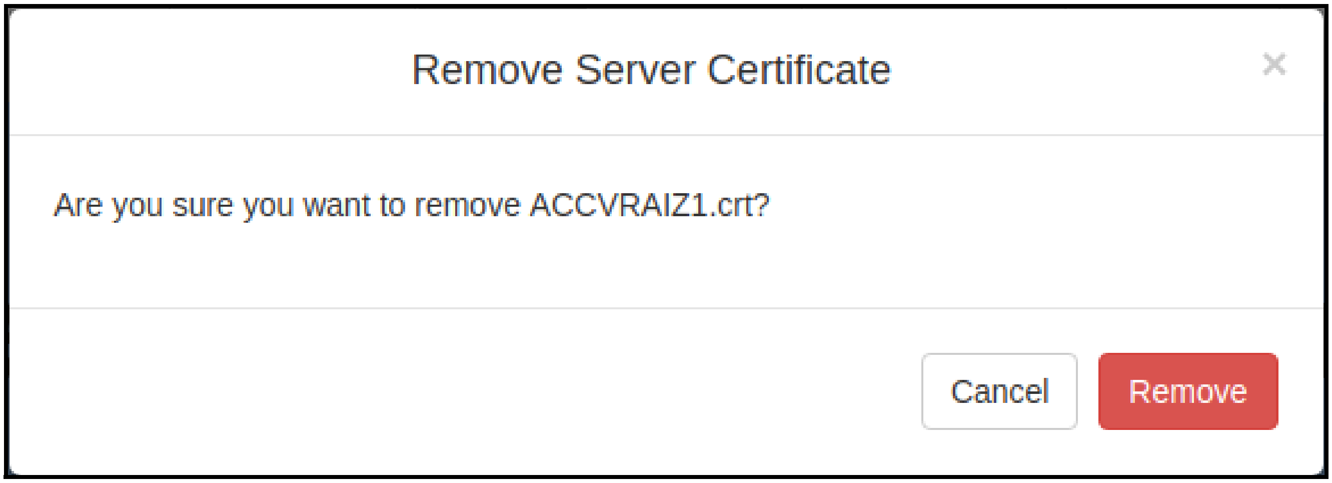


```
subject=
    commonName                = ACCVRAIZ1
    organizationalUnitName    = PKIACCV
    organizationName          = ACCV
    countryName               = ES
notBefore=May  5 09:37:37 2011 GMT
notAfter=Dec 31 09:37:37 2030 GMT
```

2.3.8.2 Remove Server Certificate Window

The **Remove Server Certificate Window** will ask if the user wants to remove a certificate from the list of trusted certificates. This window appears after clicking on the **Remove** button. See Figure 2-26.

Figure 2-26. Remove Server Certificate Window



Remove Server Certificate

Are you sure you want to remove ACCVRAIZ1.crt?

2.3.9 Configure the Multicast Parameters

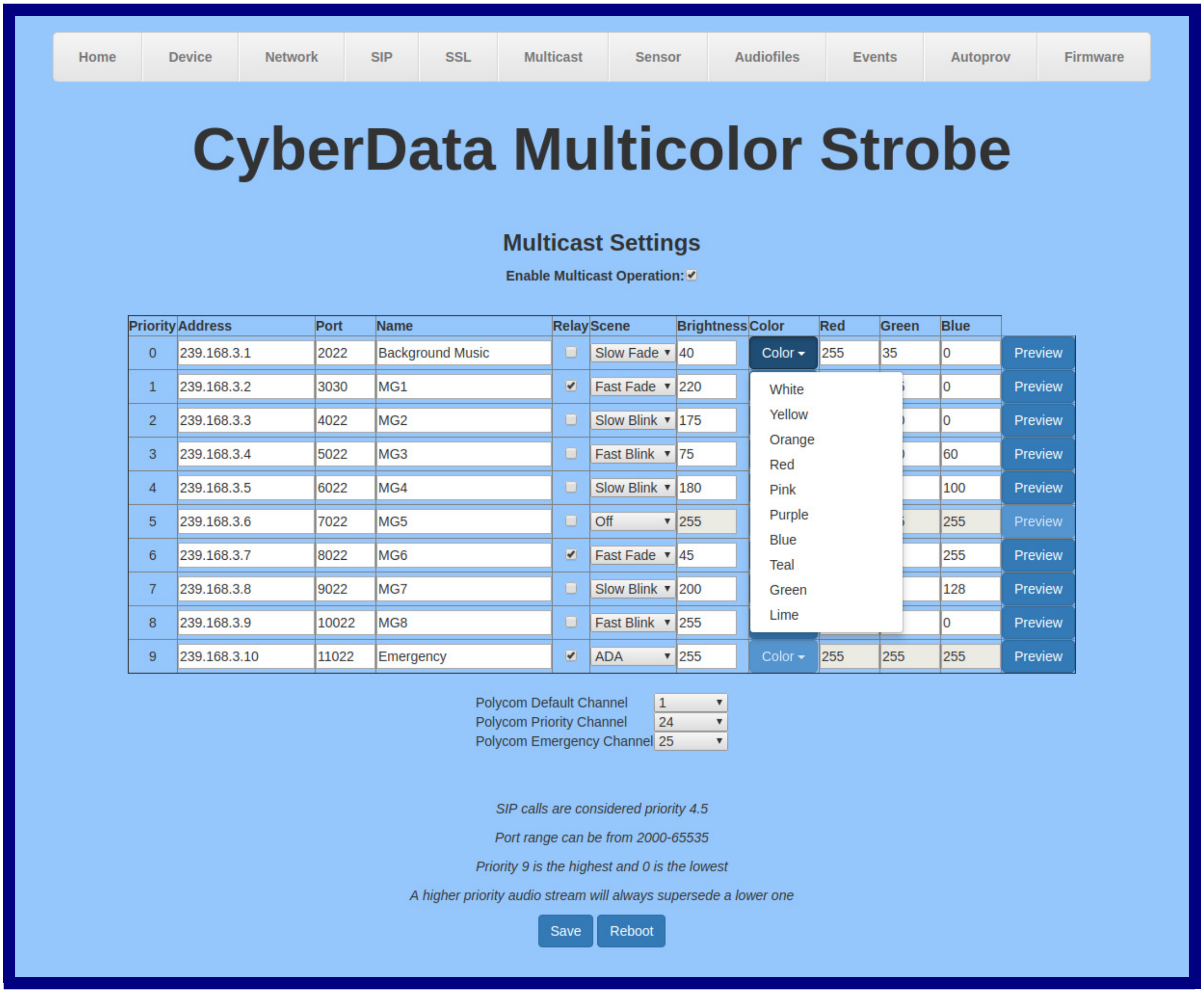
The **Multicast** page allows the device to join up to ten paging zones that will activate the strobe when a stream is sent to its address.

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

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

1. Click on the **Multicast** menu button to open the **Multicast** page. See Figure 2-27.

Figure 2-27. Multicast Configuration Page



CyberData Multicolor Strobe

Multicast Settings

Enable Multicast Operation: ☑

Priority	Address	Port	Name	Relay	Scene	Brightness	Color	Red	Green	Blue	
0	239.168.3.1	2022	Background Music	☐	Slow Fade	40	Color	255	35	0	Preview
1	239.168.3.2	3030	MG1	☑	Fast Fade	220	[illegible]	[illegible]	[illegible]	0	Preview
2	239.168.3.3	4022	MG2	☐	Slow Blink	175	[illegible]	[illegible]	[illegible]	0	Preview
3	239.168.3.4	5022	MG3	☐	Fast Blink	75	[illegible]	[illegible]	[illegible]	60	Preview
4	239.168.3.5	6022	MG4	☐	Slow Blink	180	[illegible]	[illegible]	[illegible]	100	Preview
5	239.168.3.6	7022	MG5	☐	Off	255	[illegible]	[illegible]	[illegible]	255	Preview
6	239.168.3.7	8022	MG6	☑	Fast Fade	45	[illegible]	[illegible]	[illegible]	255	Preview
7	239.168.3.8	9022	MG7	☐	Slow Blink	200	[illegible]	[illegible]	[illegible]	128	Preview
8	239.168.3.9	10022	MG8	☐	Fast Blink	255	[illegible]	[illegible]	[illegible]	0	Preview
9	239.168.3.10	11022	Emergency	☑	ADA	255	Color	255	255	255	Preview

Polycom Default Channel 1
Polycom Priority Channel 24
Polycom Emergency Channel 25

SIP calls are considered priority 4.5

Port range can be from 2000-65535

Priority 9 is the highest and 0 is the lowest

A higher priority audio stream will always supersede a lower one

Save Reboot

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

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

Table 2-13. Multicast Page Parameters

Web Page Item	Description
Enable Multicast Operation	Enables or disables multicast operation.
Priority	Indicates the priority for the multicast group. Priority **9** is the highest (emergency streams). **0** is the lowest (background music). SIP calls are considered priority **4.5**. See Section 2.3.10, "Configure the Sensor Configuration Parameters" for more details.
Address	Enter the multicast IP Address for this multicast group (15 character limit).
Port	Enter the port number for this multicast group (5 character limit [range can be from 2000 to 65535]). **Note**: The multicast ports have to be even values. The webpage will enforce this restriction.
Name	Assign a descriptive name for this multicast group (25 character limit).
Relay	When selected, the device will activate a relay before the strobe is triggered by the multicast stream.
Scene ?	Select desired scene (only one may be chosen).
ADA Compliant ?	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.
Slow Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink ?	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.
Fast Blink ?	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.
Color ?	Select desired color (only one may be chosen).
Brightness ?	How bright the strobe will blink on a multicast page. This is the maximum brightness for “fade” type scenes.
Red ?	The red LED value for Multicast.
Green ?	The green LED value for Multicast.
Blue ?	The blue LED value for Multicast.
Polycom Default Channel	When a default Polycom channel/group number is selected, the device will subscribe to the default channel for one-way group pages. Group Numbers 1-25 are supported. Or, select **Disabled** 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 **Disabled** 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 **Disabled** to disable this channel.

Table 2-13. Multicast Page Parameters (continued)

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

2.3.10 Configure the Sensor Configuration Parameters

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

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

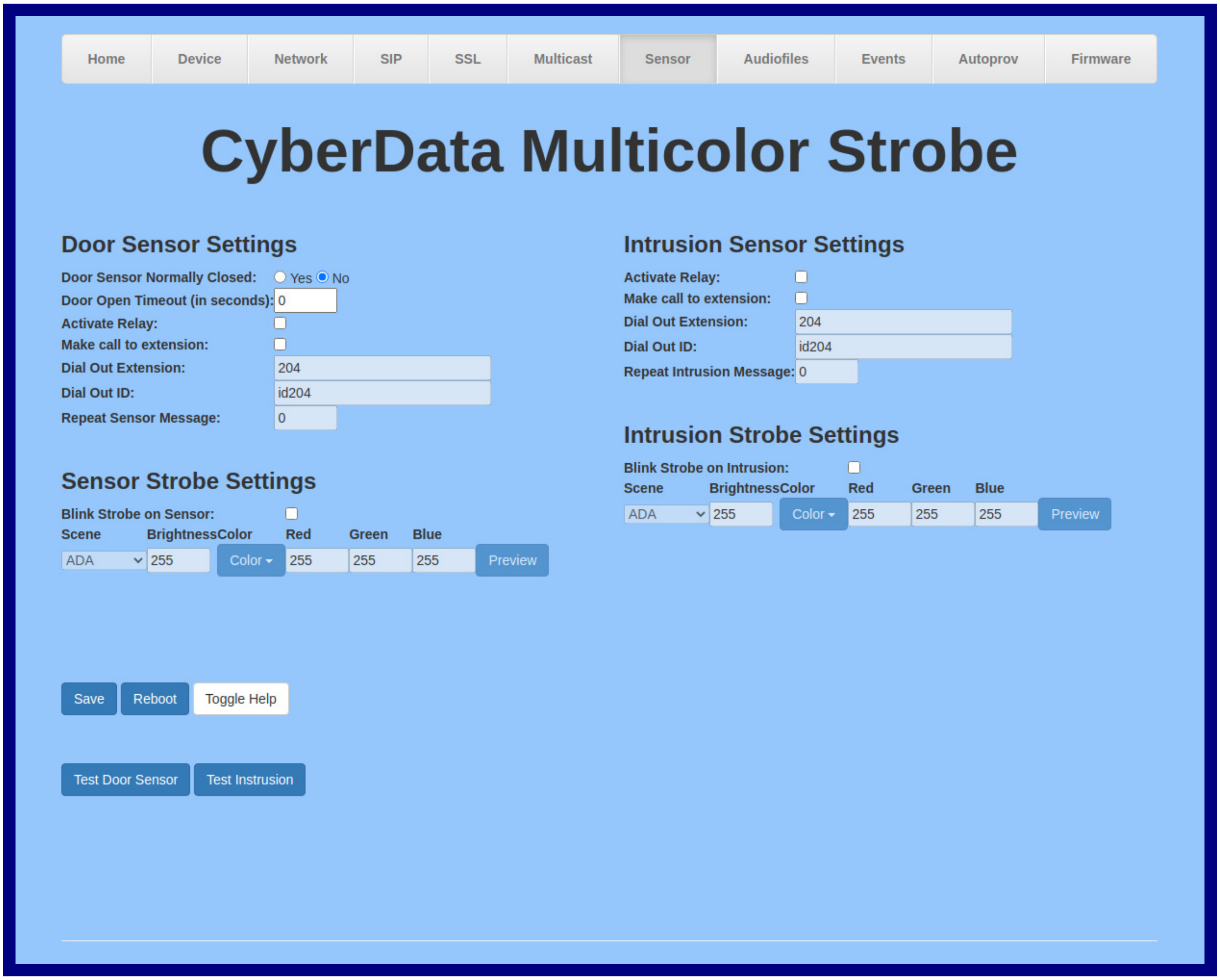
Each sensor can trigger up to four different actions:

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

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

1. Click **Sensor** menu button to open the **Sensor** page (Figure 2-28).

Figure 2-28. Sensor Configuration Page



CyberData Multicolor Strobe

Door Sensor Settings

Door Sensor Normally Closed: ○ Yes ● No
Door Open Timeout (in seconds): 0
Activate Relay: □
Make call to extension: □
Dial Out Extension: 204
Dial Out ID: id204
Repeat Sensor Message: 0

Sensor Strobe Settings

Blink Strobe on Sensor: □

Scene	Brightness	Color	Red	Green	Blue	
ADA	255	Color ▾	255	255	255	Preview

Intrusion Sensor Settings

Activate Relay: □
Make call to extension: □
Dial Out Extension: 204
Dial Out ID: id204
Repeat Intrusion Message: 0

Intrusion Strobe Settings

Blink Strobe on Intrusion: □

Scene	Brightness	Color	Red	Green	Blue	
ADA	255	Color ▾	255	255	255	Preview

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

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

Table 2-14. Sensor Configuration Parameters

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

Table 2-14. Sensor Configuration Parameters (continued)

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

Table 2-14. Sensor Configuration Parameters (continued)

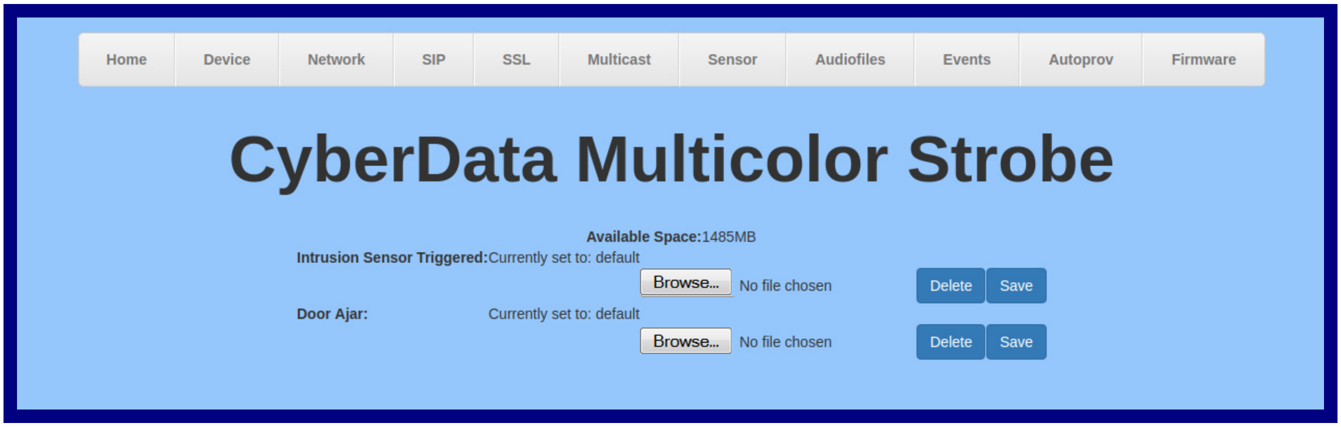
Web Page Item	Description
	Click the **Test Door Sensor** button to test the door sensor.
	Click the **Test Intrusion Sensor** button to test the Intrusion sensor.
	Click the **Save** button to save your configuration settings.
	Click on the **Reboot** button to reboot the system.
	Click on the **Toggle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

2.3.11 Configure the Audio Configuration Parameters

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

1. Click on the **Audiofiles** menu button to open the **Audiofiles** page (Figure 2-29).

Figure 2-29. Audiofiles Configuration Page



CyberData Multicolor Strobe

Available Space:1485MB

Intrusion Sensor Triggered: Currently set to: default

No file chosen

Door Ajar: Currently set to: default

No file chosen

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

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

Table 2-15. Audiofiles Configuration Parameters

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

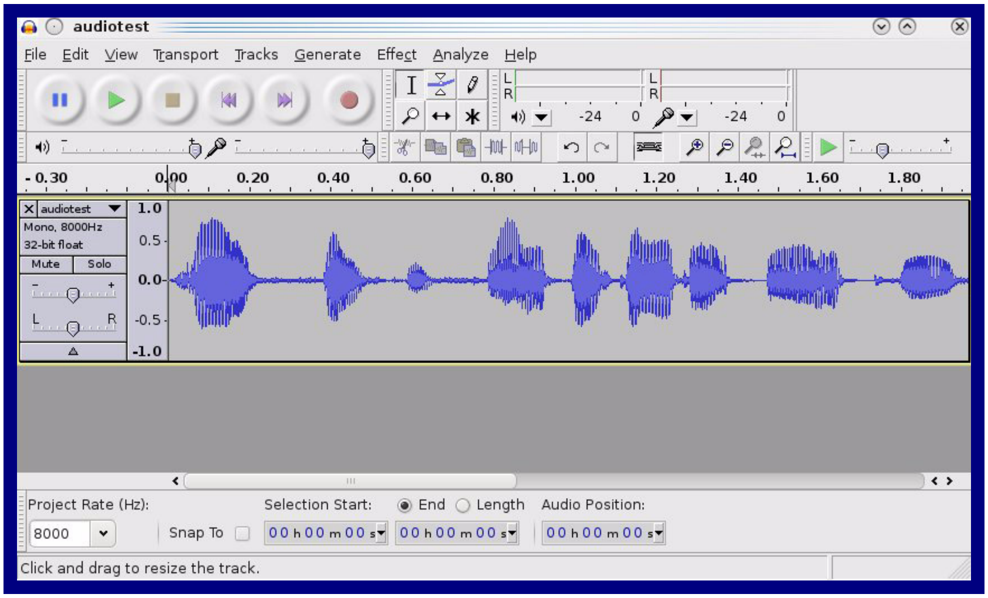
2.3.11.1 User-created Audio Files

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

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

You can use the free utility *Audacity* to convert audio files into this format. See Figure 2-30 through Figure 2-32.

Figure 2-30. Audacity 1



Project Rate (Hz): 8000

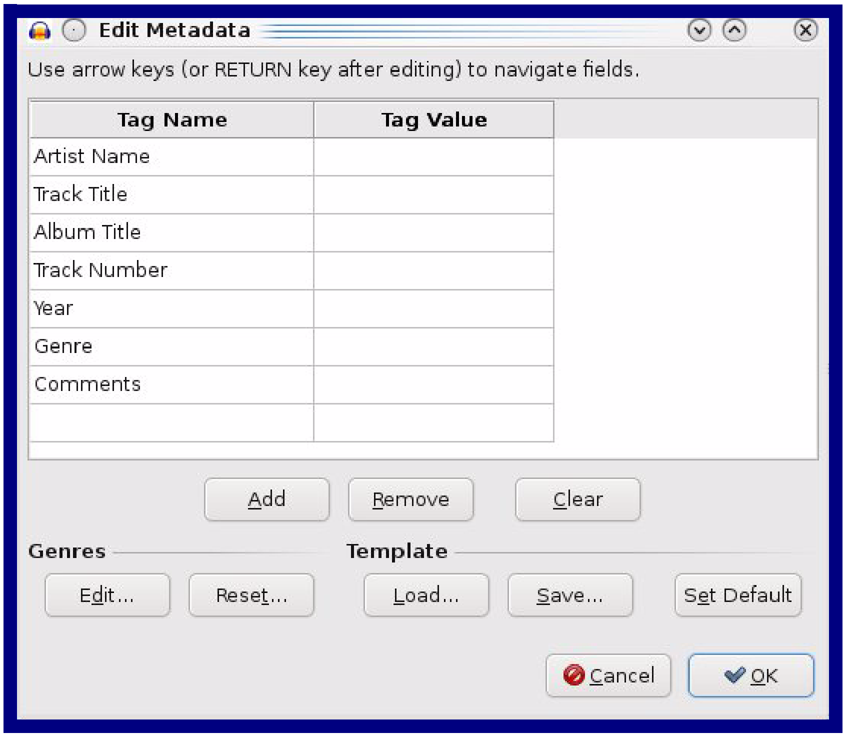
Selection Start: 00 h 00 m 00 s

● End 00 h 00 m 00 s

Audio Position: 00 h 00 m 00 s

Click and drag to resize the track.

Figure 2-31. Audacity 2



Edit Metadata

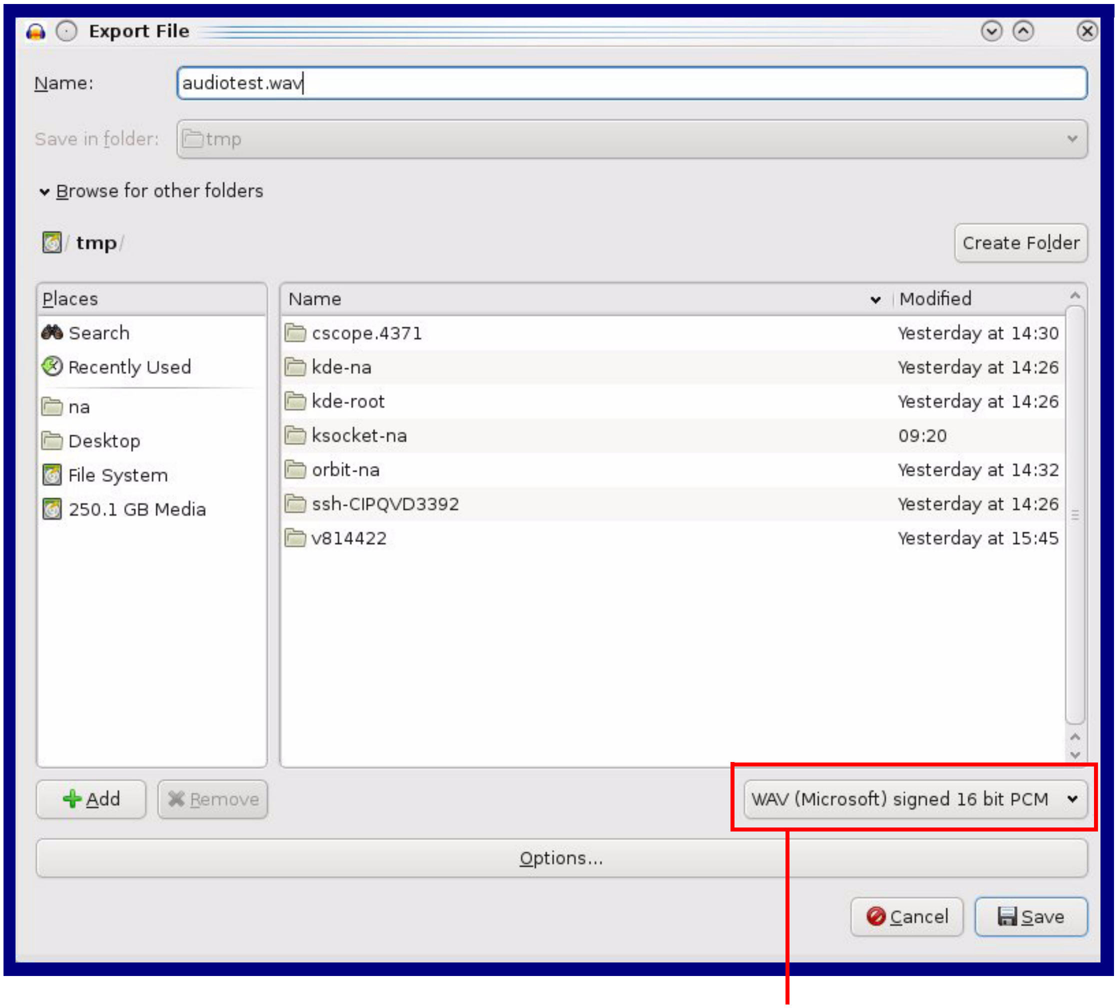
Use arrow keys (or RETURN key after editing) to navigate fields.

Tag Name	Tag Value
Artist Name	
Track Title	
Album Title	
Track Number	
Year	
Genre	
Comments	

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

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

Figure 2-32. WAV (Microsoft) signed 16 bit PCM



Export File

Name: audiotest.wav

Save in folder: tmp

Browse for other folders

/ tmp /

Name	Modified
cscope.4371	Yesterday at 14:30
kde-na	Yesterday at 14:26
kde-root	Yesterday at 14:26
ksocket-na	09:20
orbit-na	Yesterday at 14:32
ssh-CIPQVD3392	Yesterday at 14:26
v814422	Yesterday at 15:45

WAV (Microsoft) signed 16 bit PCM

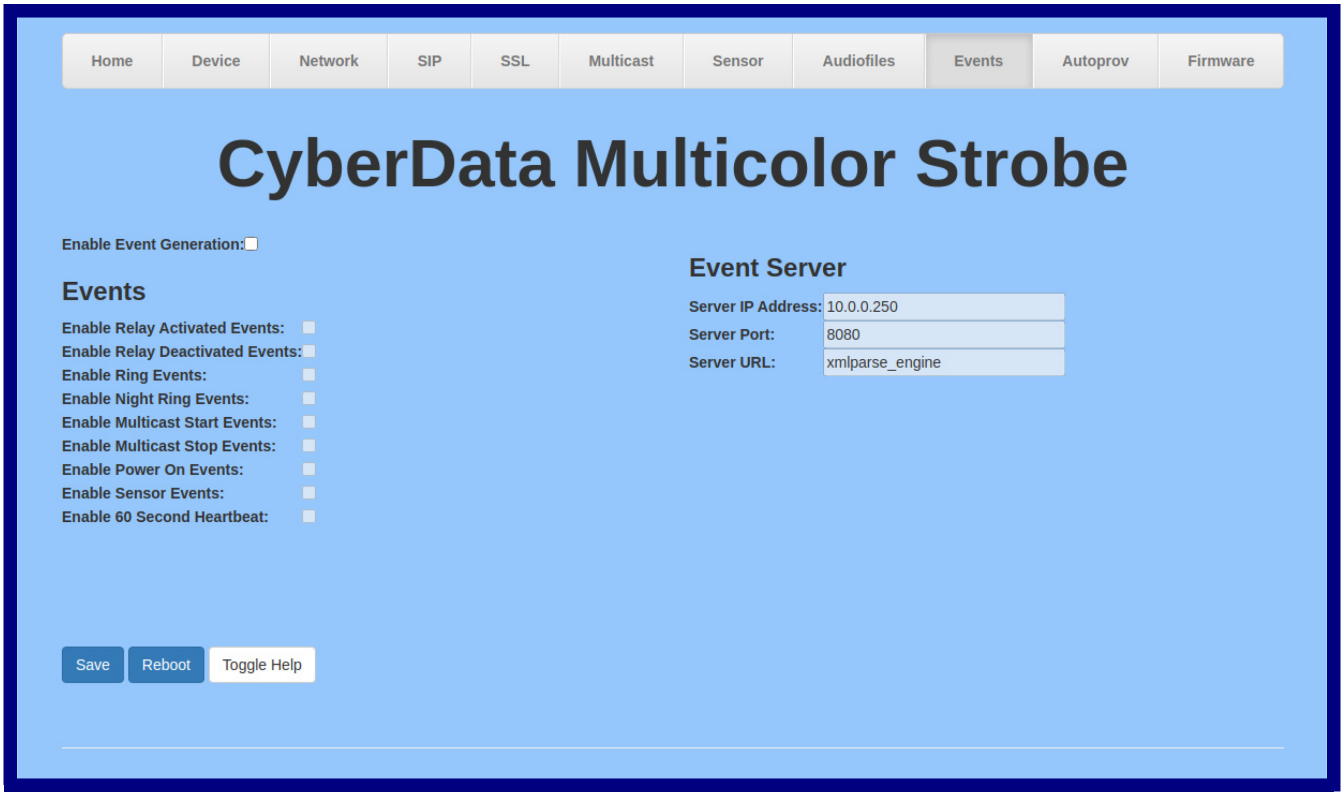
WAV (Microsoft) signed 16 bit PCM

2.3.12 Configure the Events Parameters

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

1. Click on the **Events** menu button to open the **Events** page (Figure 2-33).

Figure 2-33. Event Configuration Page



Enable Event Generation: □

Events

Enable Relay Activated Events: □
Enable Relay Deactivated Events: □
Enable Ring Events: □
Enable Night Ring Events: □
Enable Multicast Start Events: □
Enable Multicast Stop Events: □
Enable Power On Events: □
Enable Sensor Events: □
Enable 60 Second Heartbeat: □

Event Server

Server IP Address: 10.0.0.250
Server Port: 8080
Server URL: xmlparse_engine

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

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

Table 2-16. Events Configuration Parameters

Web Page Item	Description
Enable Event Generation ?	The device will send HTTP POST events to the specified remote server and port number whenever a certain action takes place. Select an event type below to generate an HTTP POST event.
Events	
Enable Relay Activated Events ?	When selected, the device will report relay activation.
Enable Relay Deactivated Events ?	When selected, the device will report relay deactivation.
Enable Ring Events ?	When selected, the device will report when it starts ringing upon an incoming SIP call.
Enable Night Ring Events ?	When selected, the device will report when it starts ringing upon an incoming SIP call to the Nightringer extension. As a reminder, the Nightringer extension always rings upon an incoming SIP call and it is not possible to alter this behavior.
Enable Multicast Start Events ?	When selected, the device will report when the device starts a strobe scene when the device receives a multicast.
Enable Multicast Stop Events ?	When selected, the device will report when the device stops a strobe scene when the multicast stream ends.
Enable Power On Events ?	When selected, the device will report when it boots.
Enable Sensor Events ?	When selected, the device will report when the on-board sensor is activated.
Enable 60 Second Heartbeat Events ?	When enabled, the device will report a Heartbeat event every 60 seconds. SIP registration is not required to generate Heartbeat events.
Check All	Click on **Check All** to select all of the events on the page.
Uncheck All	Click on **Uncheck All** to de-select all of the events on the page.
Event Server	
Server IP Address ?	The IPv4 address of the event server in dotted decimal notation.
Server Port ?	Specify the event server port number. The supported range is 0-65536. Enter up to 5 digits.
Server URL ?	Generally, the destination URL is the name of the application that receives the events and the string in the HTTP POST command. It can be a script used to parse and process the HTTP POST events. Enter up to 127 characters.
Save	Click the **Save** button to save your configuration settings.
Reboot	Click on the **Reboot** button to reboot the system.
Toggle Help	Click on the **Toggle Help** button to see a short description of some of the web page items. First click on the **Toggle Help** button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

2.3.12.1 Example Packets for Events

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

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

Here are example packets for every event:

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

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


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

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


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

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

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

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>CALL_ACTIVE</event>
</cyberdata>
POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
```

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

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


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

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


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

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

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

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

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

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

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

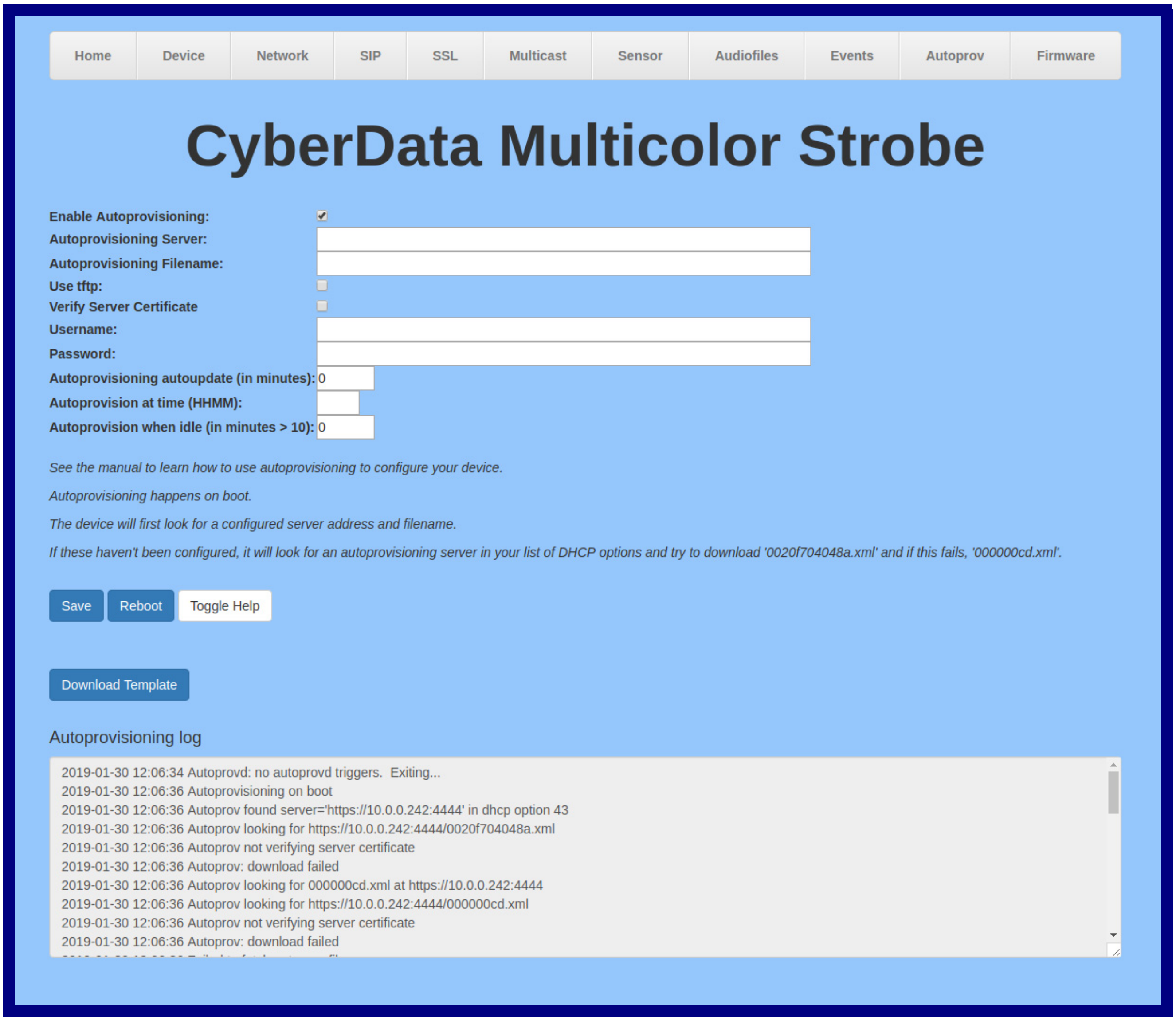
2.3.13 Configure the Autoprovisioning Parameters

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

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

1. Click the **Autoprov** menu button to open the **Autoprovisioning** page. See Figure 2-34.

Figure 2-34. Autoprovisioning Page



CyberData Multicolor Strobe

Enable Autoprovisioning: ☑
Autoprovisioning Server:
Autoprovisioning Filename:
Use tftp: □
Verify Server Certificate □
Username:
Password:
Autoprovisioning autoupdate (in minutes): 0
Autoprovision at time (HHMM):
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 '0020f704048a.xml' and if this fails, '000000cd.xml'.

Autoprovisioning log

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

2. On the **Autoprovisioning** page, you may enter values for the parameters indicated in Table 2-17.

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

Table 2-17. Autoprovisioning Page Parameters

Web Page Item	Description
Enable Autoprovisioning ?	The device will automatically fetch a configuration file, also known as the 'autoprovisioning file', based on the configured settings below.
Autoprovisioning Server ?	Enter the IPv4 address of the provisioning server in dotted decimal notation.
Autoprovisioning Filename ?	The autoprovisioning filename is the configuration filename. The default autoprovisioning filename is in the format of **<mac address>.xml**. Supported filename extensions are .txt, and .xml. The current filename is denoted by an asterisk at the bottom of the **Autoprovisioning Page**. Enter up to 256 characters. A file may have any name with an xml extension. If a file name is entered, the device will look for the specified file name, and only that file.
Use tftp ?	The device will use TFTP (instead of http) to download autoprovisioning files.
Verify Server Certificate ?	When using ssl to download autoprovisioning files, reject connections where the server address doesn't match the server certificate's common name.
Username ?	The username used to authenticate with an autoprovisioning server. Leave this field blank to disable authentication.
Password ?	The password used to authenticate with an autoprovisioning server. Leave this field blank to disable authentication.
Autoprovisioning Autoupdate (in minutes) ?	The reoccurring time (in minutes) the device will wait before checking for new autoprovisioning files. Enter up to 6 digits. A value of 0 will disable this option.
Autoprovision at time (HHMMSS) ?	The time of day the device will check for a new autoprovisioning file. The time must be 6 characters in length and in HHMMSS format. An empty value will disable this option.
Autoprovision when idle (in minutes > 10) ?	The idle time (in minutes greater than 10) after which the device will check for a new autoprovisioning file. Enter up to 6 digits. A value of 0 will disable this option.
Save	Click the **Save** button to save your configuration settings.
Reboot	Click on the **Reboot** button to reboot the system.
Toggle Help	Click on the **Toggle Help** button to see a short description of some of the web page items. First click on the **Toggle Help** button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.
Download Template	Press the **Download Template** button to create an autoprovisioning file for the device. See Section 2.3.13.3, "Download Template Button"
Autoprovisioning log	The autoprovisioning log provides information about the latest autoprovisioning attempt (i.e. dhcp options and server accessed and files parsed or not found).

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

2.3.13.1 Autoprovisioning

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

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

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

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

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

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

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

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

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

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

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

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

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

The file 0020f7123456.xml contains:

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

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

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

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

Checking for New Autoprovisioning Files after Boot

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

The Autoprovisioning Filename

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

Table 2-18. Autoprovisioning File Name

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

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

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

For example:

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

The autoprovisioning filename is set to "cyberdata/"

On boot, the device will try to download:

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

...and if this fails:

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

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

Autoprovisioning Firmware Updates

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

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

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

The <FirmwareFile> name can contain path elements (i.e. /path/to/firmware/10.3.0-uImage-[device_file_name]).

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

The list of valid product strings:

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

Autoprovisioning Example 1

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

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

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

000000cd.xml

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

sip_common.xml

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

sip_0020f7020001.xml

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

sip_0020f7020002.xml

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

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

1. Device1 changes its device name to **CyberData Autoprovisioned**.
2. Device1 finds an AutoprovFile element containing the filename **sip_common.xml**. The device downloads **sip_common.xml** from “https://autoprovtest.server.net,” and imports this configuration, setting the sip server to **10.0.0.253** and the remote port to **5060.3**.
3. Device1 finds another AutoprovFile element containing the filename **sip_[macaddress].xml**. The device replaces the **[macaddress]** with its own mac address value creating **sip_0020f7020001.xml**, downloads this file from “https://autoprovtest.server.net,” and imports this configuration. This sets the user ID to **198**, the password to **ext198**, and the dialout extension to **204**. Device1 is now finished with autoprovisioning.

Device2 goes through the same steps by setting its device name to **CyberData Autoprovisioned**, its SIP server to **10.0.0.253**, and its port to **5060**. When Device2 “sees” **sip_[macaddress].xml**, Device2 replaces it with its own mac address and downloads **sip_0020f7020002.xml** from “https://autoprovtest.server.net.” Device2 sets the SIP User ID to **500**, the password to **ext500**, and the dialout extension to **555**.

Autoprovisioning Example 2

Here is another example of setting up your autoprovisioning files:

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

0020f7020001.xml

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

0020f7020002.xml

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

common_settings.xml

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

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

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

Device2 does the same except it downloads **0020f7020002.xml** on boot and imports these values instead. The Sip User ID is **500**, password is **ext500**, and dialout extension is **555**. Device2 then downloads the **common_settings.xml** file and imports those values. The device name is set to **CyberData Autoprovisioned**, the SIP server is set to **10.0.0.253**, and the port is set to **5060**.

XML Files

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

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

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

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

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

From the common file, a pointer to sip_common.xml

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

Autoprovisioned Audio Files

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

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

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

2.3.13.2 Sample dhcpd.conf

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

ddns-update-style none;

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

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

    option routers                  10.0.0.1;
    option subnet-mask              255.0.0.0;

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

    option time-offset              -8;             # Pacific Standard Time

#     option www-server               99.99.99.99;                    # OPTION 72

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

#     option option-150                10.0.0.252;                    # OPTION 150

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

    range 10.10.0.1 10.10.2.1; }
```

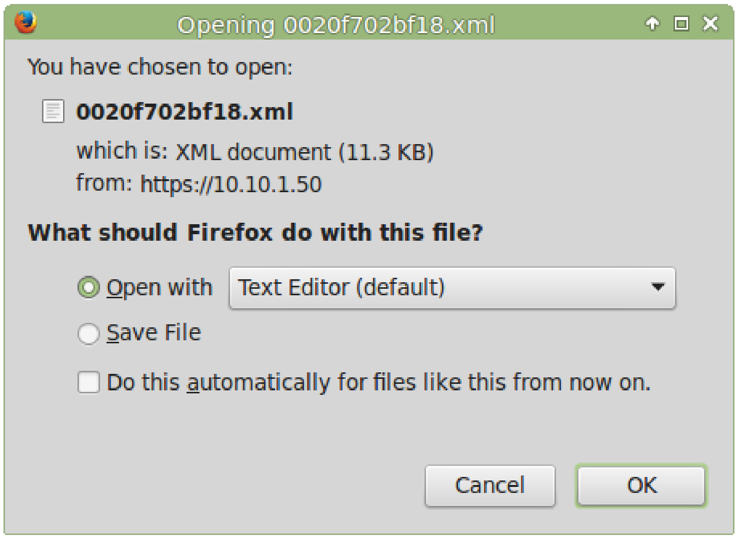
2.3.13.3 Download Template Button

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

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

1. On the **Autoprovisioning** page, click on the **Download Template** button.
2. You will see a window prompting you to save a configuration file (**.xml**) to a location on your computer (Figure 2-35). 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 2-35.

Figure 2-35. Configuration File



Opening 0020f702bf18.xml

You have chosen to open:

0020f702bf18.xml

which is: XML document (11.3 KB)

from: https://10.10.1.50

What should Firefox do with this file?

● Open with Text Editor (default)

○ Save File

□ Do this automatically for files like this from now on.

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

2.4 Upgrade the Firmware

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

To upgrade the firmware of your device:

1. Download the latest firmware file from the **Downloads** tab at the following webpage:

   https://www.cyberdata.net/products/011376

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

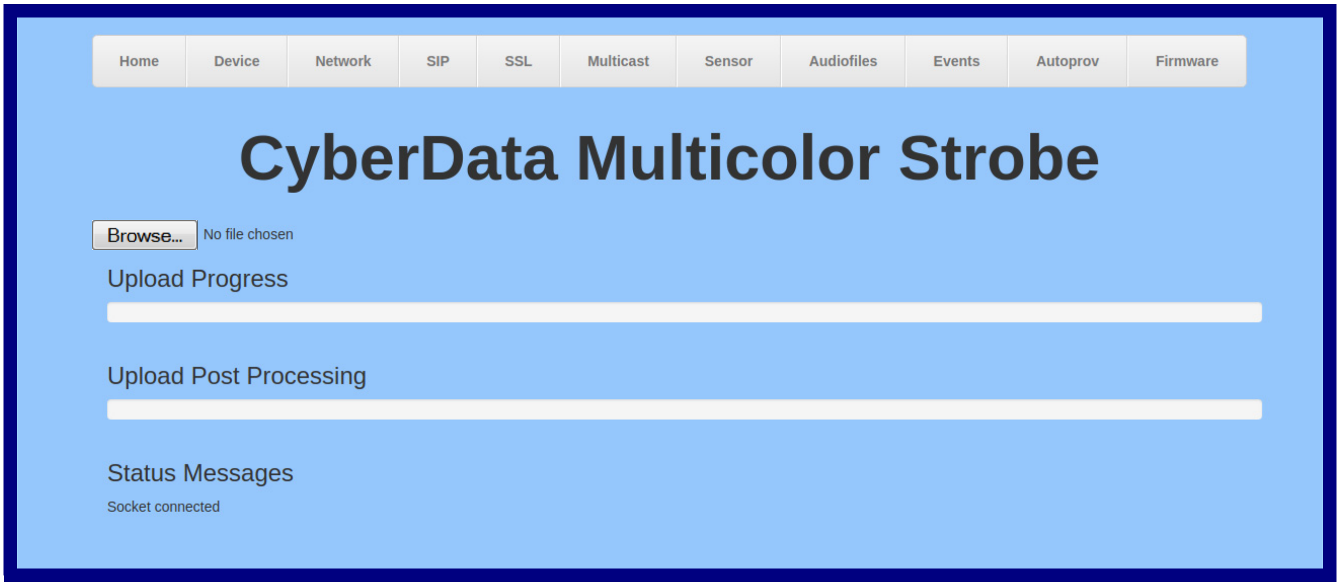
- Firmware file
- Release notes
- Autoprovisioning template

3. Log in to the **Home** page as instructed in Section 2.3.4, "Log in to the Configuration Home Page".

4. Click on the **Firmware** menu button to open the **Firmware** page (Figure 2-36).

GENERAL ALERT	**Caution** ***Equipment Hazard***: CyberData strongly recommends that you first reboot the device before attempting to upgrade the firmware of the device. See Section 2.5, "Reboot the Device".

Figure 2-36. Firmware Page



CyberData Multicolor Strobe

No file chosen

Upload Progress

Upload Post Processing

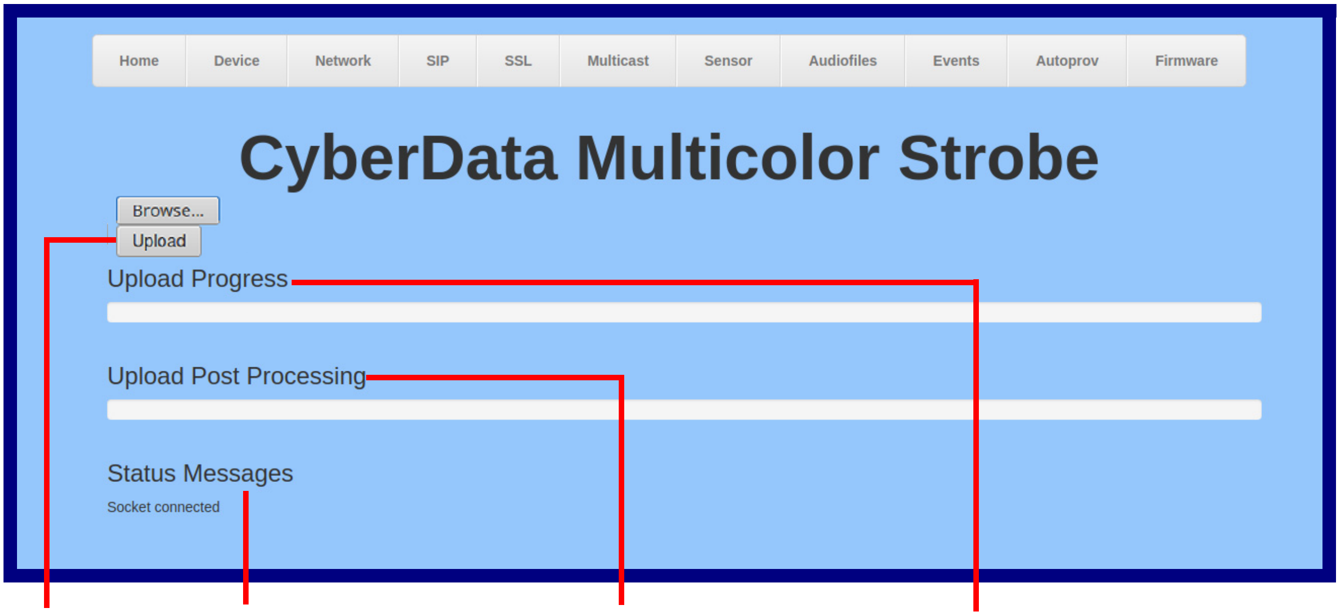
Status Messages

Socket connected

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

6. Select the firmware file. This reveals the **Upload** button (Figure 2-37).

Figure 2-37. Upload Button



Socket connected

Upload button **Status Messages** **Upload Post Processing** bar **Upload Progress** bar

7. Click on the **Upload** button. After selecting the **Upload** button, you will see the progress of the upload in the **Upload Progress** bar.

8. When the upload is complete, you will see the words **Upload finished** under **Status Messages**.

9. At this point, you will see the progress of the upload's post processing in the **Upload Post Processing** bar.

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

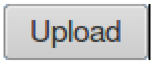
10. When the process is complete, you will see the words **SWUPDATE Successful** under **Status Messages**.

11. The device will reboot automatically.

12. The **Home** page will display the version number of the firmware and indicate which boot partition is active.

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

Table 2-19. Firmware Page Parameters

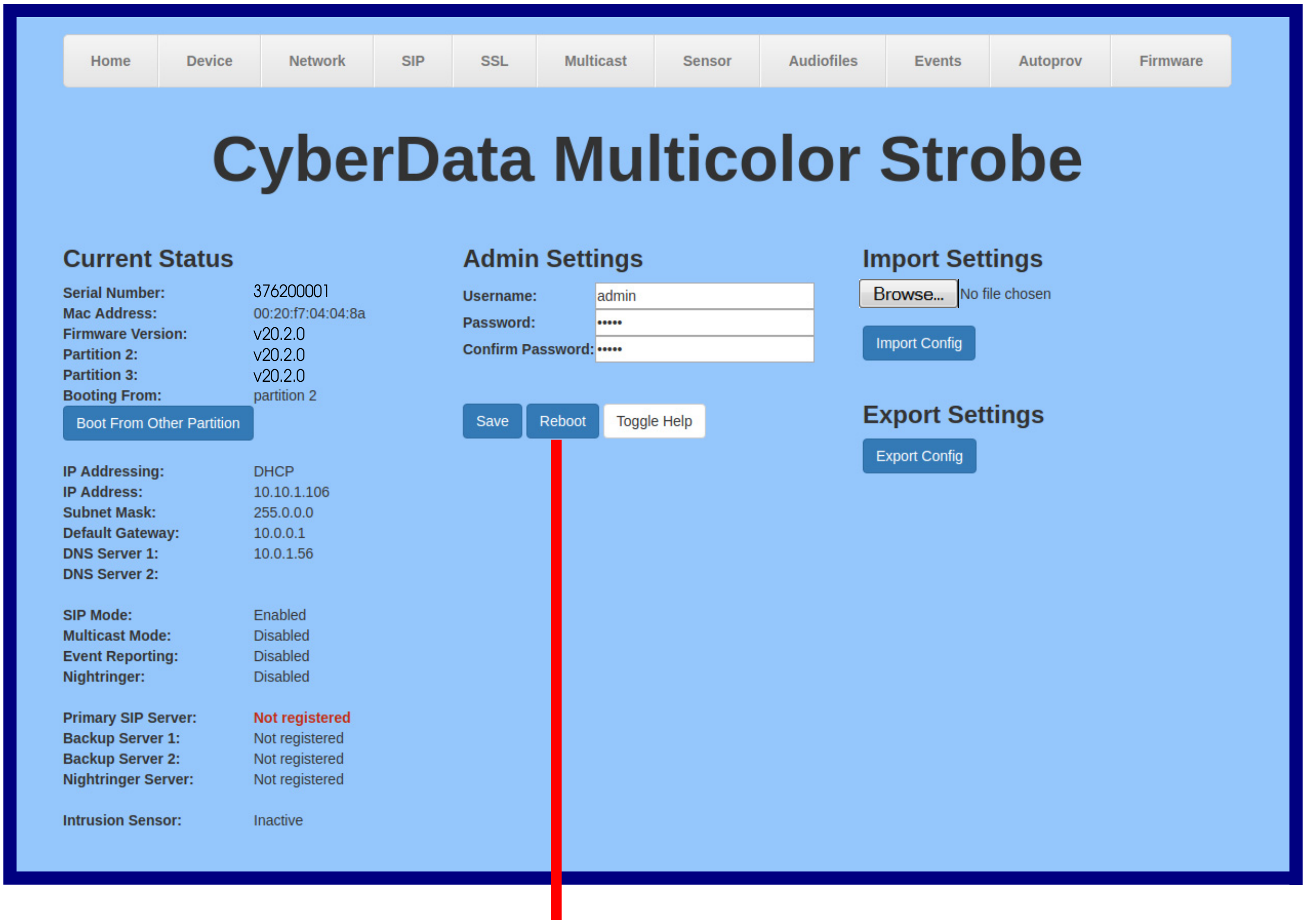
Web Page Item	Description
	Use the **Browse** button to navigate to the location of the firmware file that you want to upload.
	Click on the **Upload** button to automatically upload the selected firmware and reboot the system. **Note**: This button only appears after the user has selected a firmware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

2.5 Reboot the Device

To reboot the device, complete the following steps:

1. Log in to the **Home** page as instructed in Section 2.3.4, "Log in to the Configuration Home Page".
2. Click on the **Reboot** button on the **Home** page (Figure 2-38). A normal restart will occur.

Figure 2-38. Home Page



CyberData Multicolor Strobe

Current Status

Serial Number:	376200001
Mac Address:	00:20:f7:04:04:8a
Firmware Version:	v20.2.0
Partition 2:	v20.2.0
Partition 3:	v20.2.0
Booting From:	partition 2
IP Addressing:	DHCP
IP Address:	10.10.1.106
Subnet Mask:	255.0.0.0
Default Gateway:	10.0.0.1
DNS Server 1:	10.0.1.56
DNS Server 2:	
SIP Mode:	Enabled
Multicast Mode:	Disabled
Event Reporting:	Disabled
Nightringer:	Disabled
Primary SIP Server:	Not registered
Backup Server 1:	Not registered
Backup Server 2:	Not registered
Nightringer Server:	Not registered
Intrusion Sensor:	Inactive

Admin Settings

Username: admin
Password: •••••
Confirm Password: •••••

Import Settings

Export Settings

Reboot

2.6 Command Interface

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

2.6.1 Command Interface Post Commands

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

Table 2-20. Command Interface Post Commands

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

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

Appendix A: Mounting the SIP RGB (Multi-Color) Strobe

A.1 Mount the SIP RGB Strobe

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

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

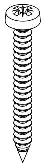
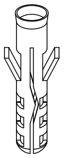
Quantity	Part Name	Illustration
4	#6 x 1.5 inches Sheet Metal Screw	
4	#6 Ribbed Plastic Anchor	

Table A-2. Gang Box Mounting Components

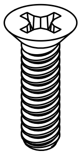
Quantity	Part Name	Illustration
4	#6-32 x 0.625-inch Flat-Head Machine Screw.	

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

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

Figure A-1. Wall Mounting Options

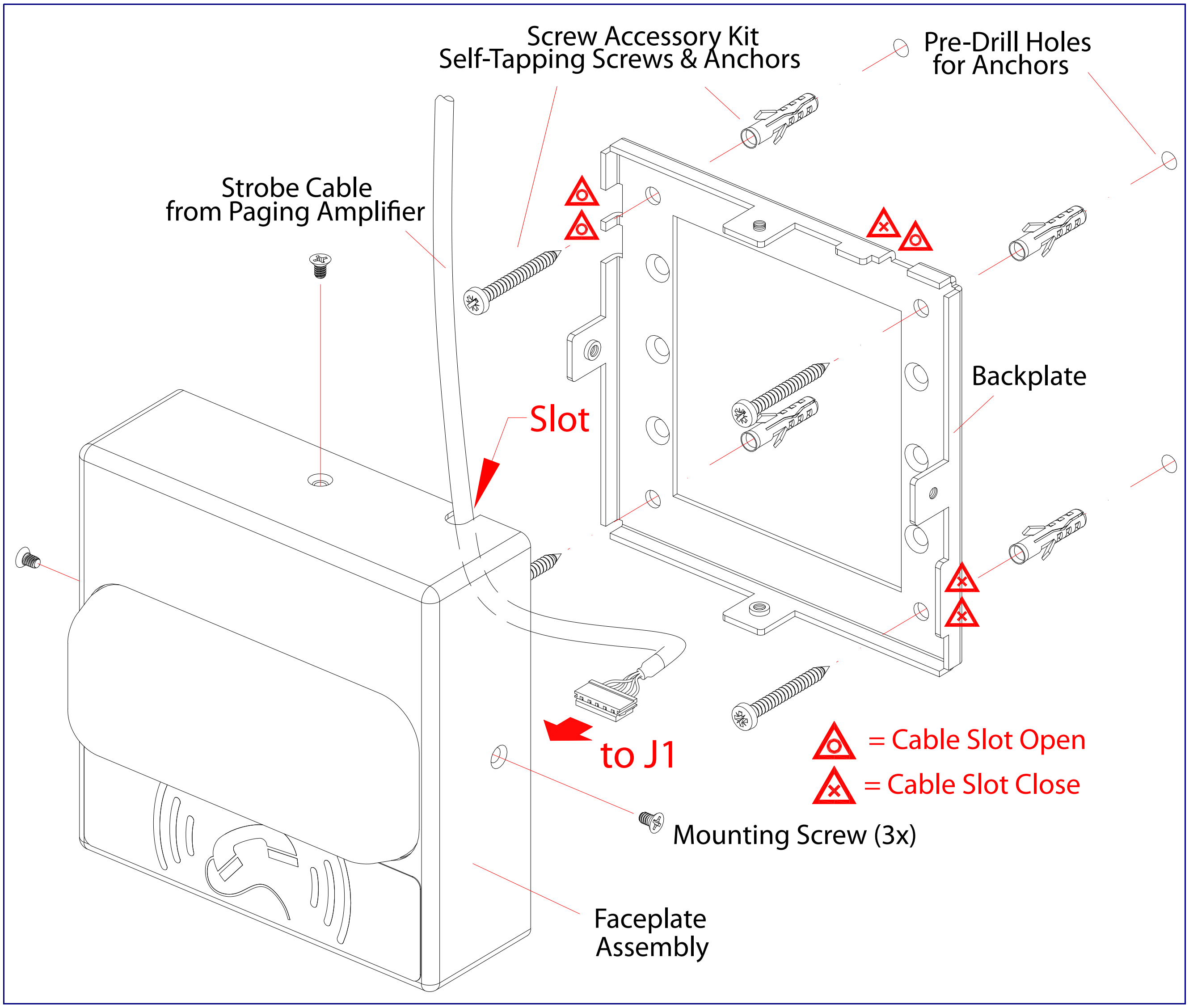


Figure A-2 shows the gang box mounting options for the SIP RGB Strobe.

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

Figure A-2. Gang Box Mounting Options

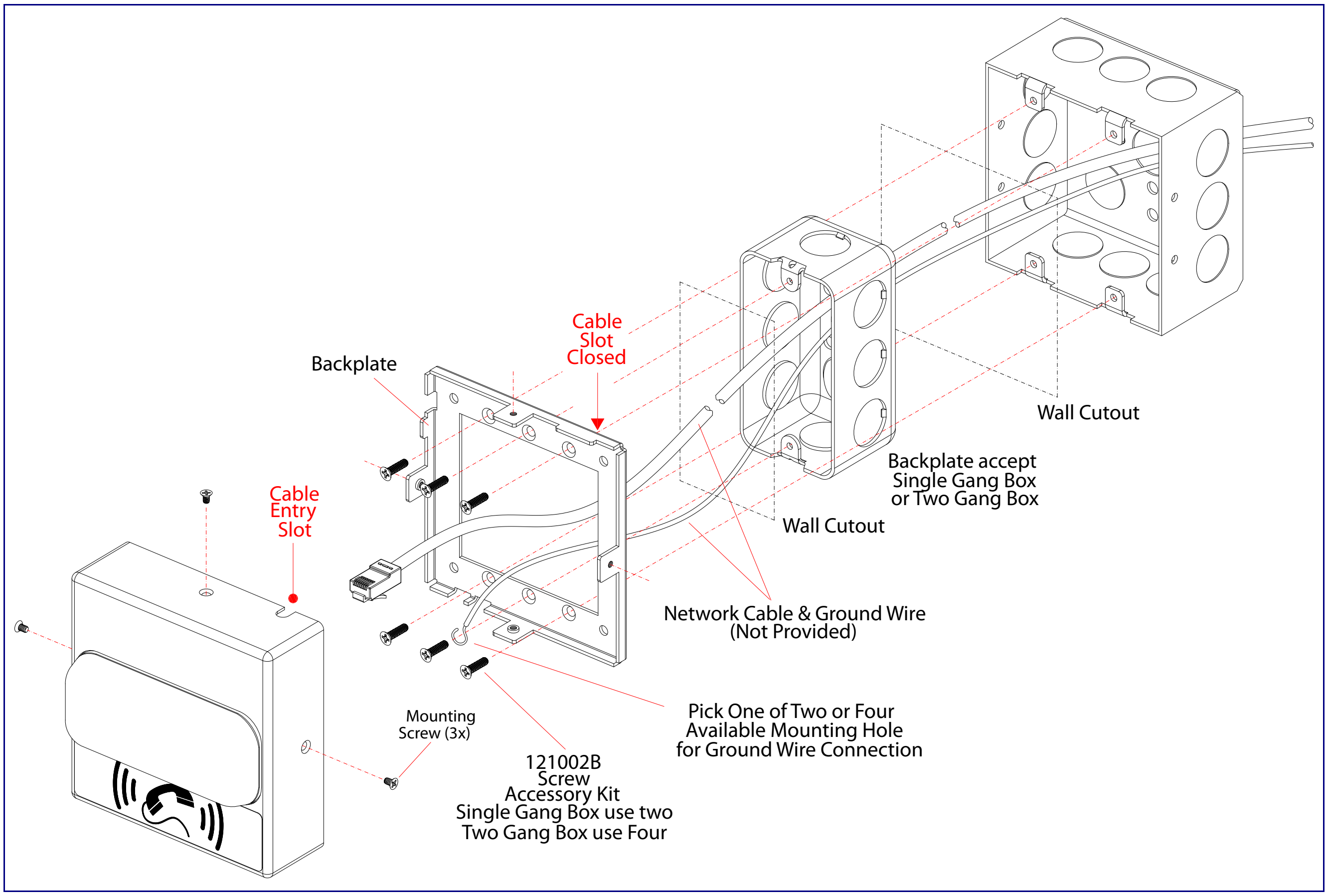
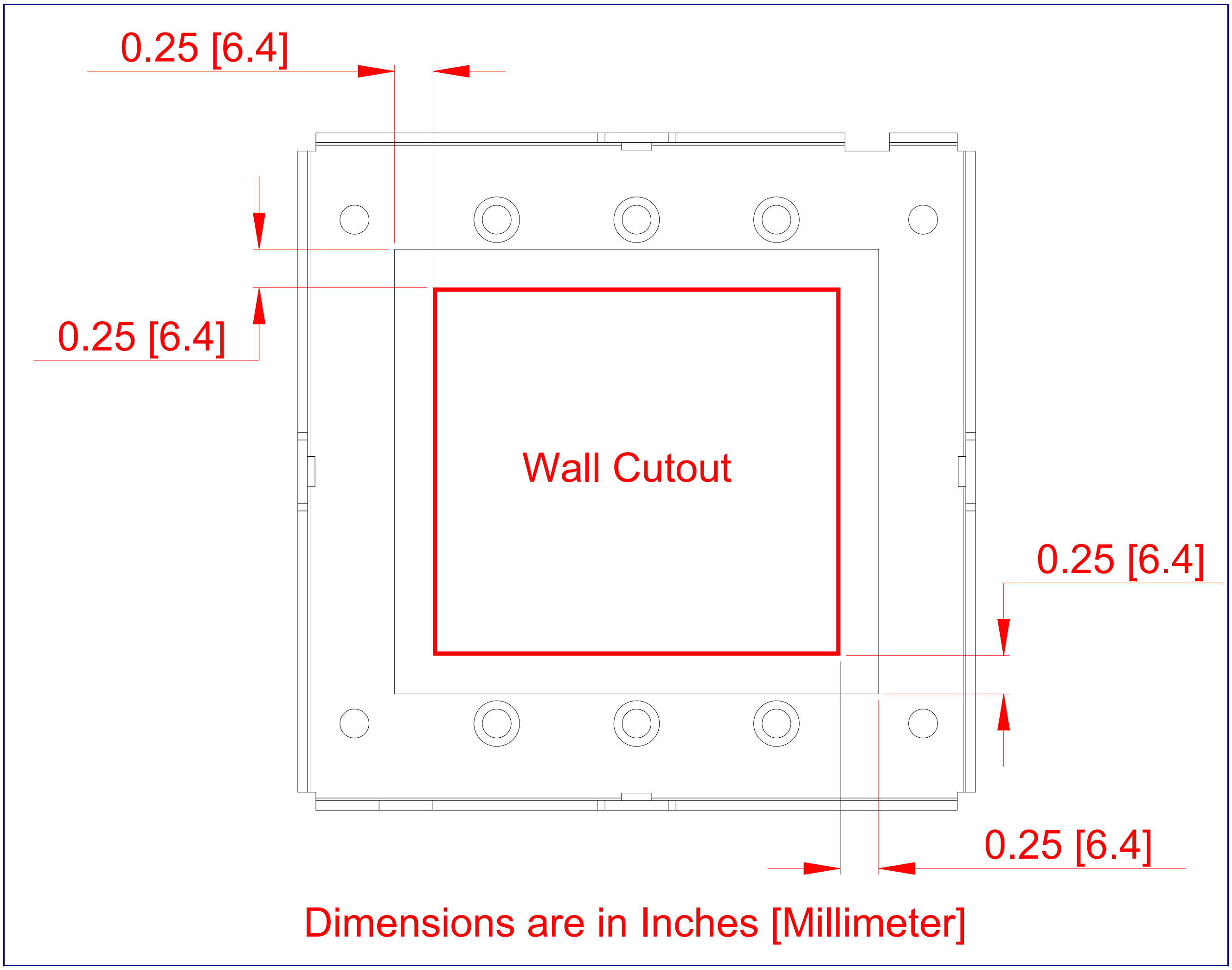


Figure A-3 shows the wall mounting with either a single or two gang box.

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:

https://www.cyberdata.net/products/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:

https://www.cyberdata.net/products/011376

B.3 Contact Information

Contact

CyberData Corporation
3 Justin Court
Monterey, CA 93940 USA
www.CyberData.net
Phone: 800-CYBERDATA (800-292-3732)
Fax: 831-373-4193

Sales

Sales 831-373-2601, Extension 334

Technical Support

The fastest way to get technical support for your VoIP product is to submit a VoIP Technical Support form at the following website:

https://support.cyberdata.net/

The Support Form initiates a ticket which CyberData uses for tracking customer requests. Most importantly, the Support Form tells us which PBX system and software version that you are using, the make and model of the switch, and other important information. This information is essential for troubleshooting. Please also include as much detail as possible in the **Comments** section of the Support Form.

Phone: (831) 373-2601, Extension 333

B.4 Warranty and RMA Information

The most recent warranty and RMA information is available at the following website address:

https://support.cyberdata.net/

Index