



SIP Paging Amplifier Operations Guide

Part #011324
Document Part #931971A
for Firmware Version 20.5.0

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

SIP Paging Amplifier Operations Guide 931971A
Part # 011324

COPYRIGHT NOTICE:

© 2023, CyberData Corporation, ALL RIGHTS RESERVED.

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

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

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

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

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



Technical Support

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

<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 931971A, which corresponds to firmware version 20.5.0, was released on June 15, 2023.

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.



Warning

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



Warning



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



Warning

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

Pictorial Alert Icons

	<p>General Alert</p> <p><i>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.</i></p>
	<p>Ground</p> <p><i>This pictorial alert indicates the Earth grounding connection point.</i></p>

Hazard Levels

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

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

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

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

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

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

Chapter 1 Product Overview	1
1.1 How to Identify This Product	1
1.2 Typical System Installation	2
1.3 Features	3
1.4 Supported Protocols	4
1.5 Supported SIP Servers	4
1.6 Specifications	5
1.7 Typical Coverage	6
1.7.1 Intelligibility Outdoor Field Test	6
1.7.2 Typical Warehouse Paging Setup	7
1.8 Compliance	8
1.8.1 CE Statement	8
1.8.2 FCC Statement	8
1.8.3 Industry Canada (IC) Compliance Statement	8
 Chapter 2 Installing the SIP Paging Amplifier	 9
2.1 Parts List	9
2.2 SIP Paging Amplifier Setup	10
2.2.1 SIP Paging Amplifier Components	11
2.2.2 Connecting the SIP Paging Amplifier	12
2.2.3 SIP Paging Amplifier System Installation and Connection Options	15
2.2.4 Strobe Connections Behind the Port Cover	17
2.2.5 Connecting the 011288 Auxiliary RGB (Multi-Color) Strobe Kit	18
2.2.6 Ethernet Connection	21
2.2.7 Loudspeaker Type	21
2.2.8 Cabling/Wiring	21
2.2.9 Confirm Operation	22
2.2.10 Confirm the IP Address and Test the Audio	23
2.3.1 Factory Default Settings	24
2.3.2 SIP Paging Amplifier Web Page Navigation	25
2.3.3 Using the Toggle Help Button	26
2.3.4 Log in to the Home Page	28
2.3.5 Configure the Device	32
2.3.6 Configure the Audio	35
2.3.7 Configure the Network Parameters	37
2.3.8 Configure the SIP (Session Initiation Protocol) Parameters	40
2.3.9 Configure the SSL Parameters	50
2.3.10 Configure the Multicast Parameters	56
2.3.11 Configure the Sensor Page Parameters	60
2.3.12 Configure the Audiofiles Page Parameters	64
2.3.13 Configure the Events Parameters	70
2.3.14 Configure the Autoprovisioning Parameters	75
2.4.1 Downloading the Firmware	87
2.4.2 Reboot the Device	90
2.5.1 Command Interface Post Commands	91
 Appendix A Mounting the Amplifier	 92
A.1 Mount the Amplifier	92
A.2 Dimensions	93
 Appendix B Troubleshooting/Technical Support	 94
B.1 Frequently Asked Questions (FAQ)	94
B.2 Documentation	94
B.3 Contact Information	95
B.4 Warranty and RMA Information	95
 Index	 96

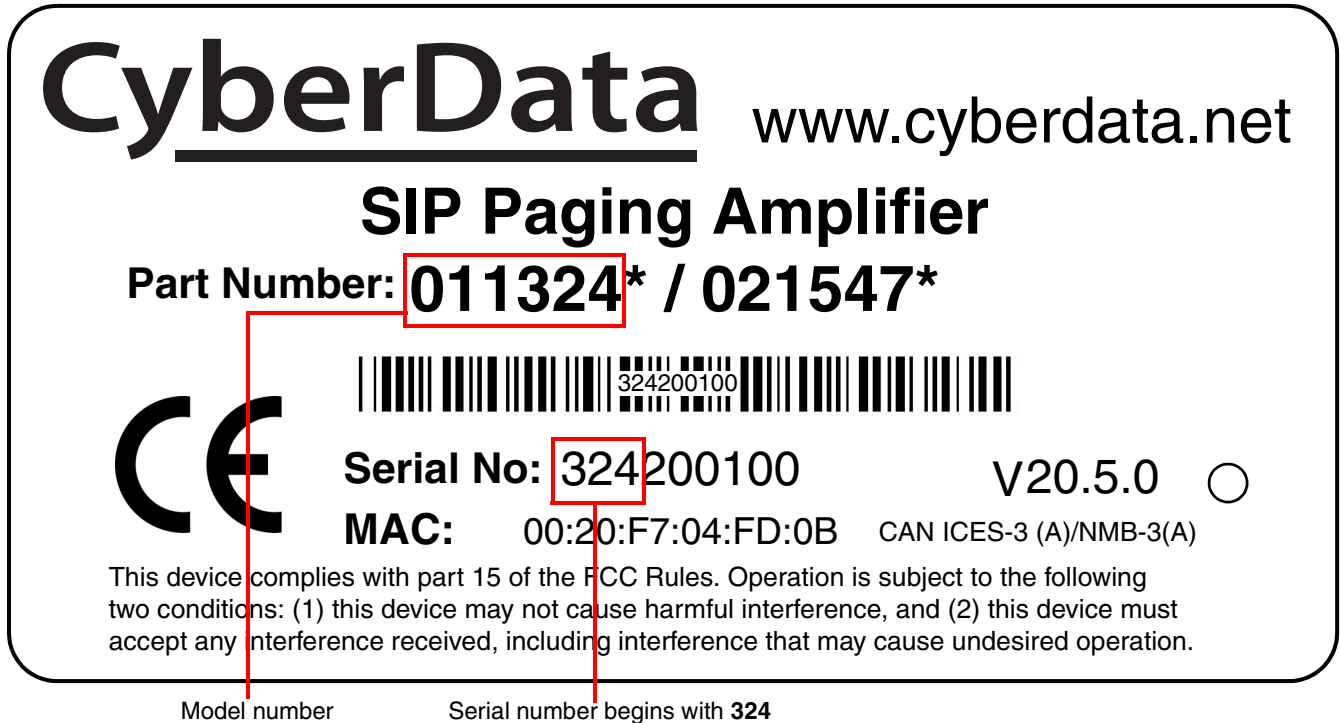
1 Product Overview

1.1 How to Identify This Product

To identify the SIP Paging Amplifier (PoE), 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 **011324**.

Figure 1-1. Model Number Label¹

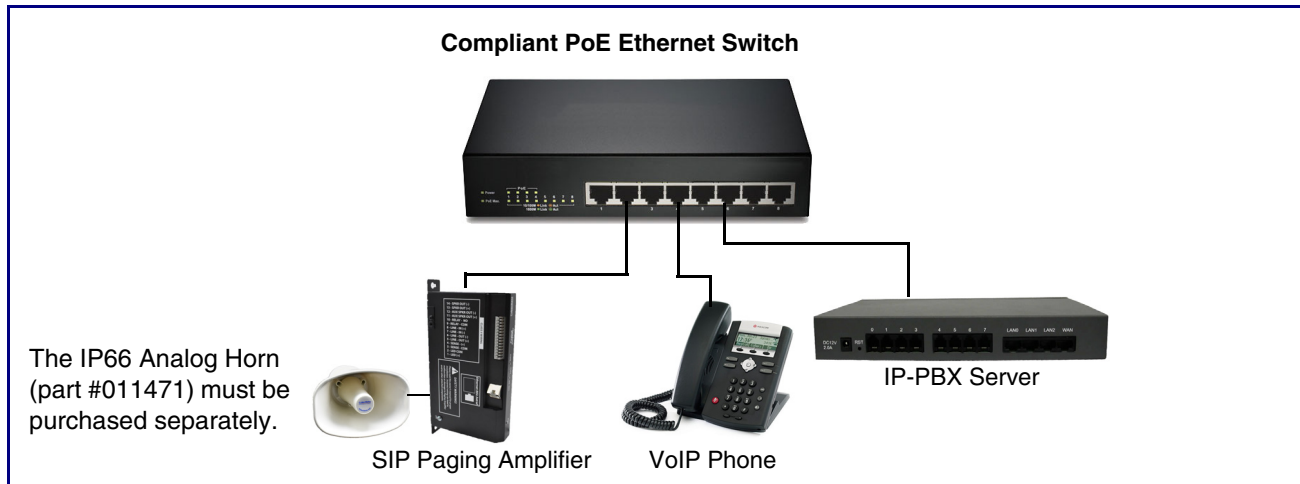


1. This figure is just an example. The revision and version information in this figure may be different than the label on your product.

1.2 Typical System Installation

Figure 1-2 illustrates how the SIP Paging Amplifier is normally installed as part of a public address system.

Figure 1-2. Typical Installation



1.3 Features

- Concurrent SIP and multicast paging
 - Loud/Night Ringer function - second SIP extension
 - Paging Prioritization
 - Support for 10 multicast paging groups
 - 9 user-uploadable page messages
 - Can receive pages directly from Poly phones as well as other devices that can send standard multicast
 - Sense input capable of generating events or SIP calls
 - Supports delayed pages, i.e. call buffering
 - Support for security code to prevent unwanted SIP calls
-
- Support for auxiliary strobe
 - Line-in for background music
 - Line-out connector
 - DTMF controlled relay
 - Supports up to two 011471 IP66 Analog Horns or other 8 Ohm speaker
 - Network volume control
-
- TLS 1.2 and SRTP enhanced security for IP Endpoints in a local or cloud-based environment
 - Autoprovisioning via HTTPS, HTTP or TFTP
 - HTTPS web based configuration
 - Configurable event generation for device health and status monitoring
 - 802.11q VLAN tagging
 - HTTPS command interface
 - Support for Cisco SRST resiliency

1.4 Supported Protocols

The SIP Paging Amplifier supports:

- SIP
- Multicast
- HTTPS web-based configuration

Provides an intuitive user interface for easy system configuration and verification of SIP Paging Amplifier operations.

- TLS 1.2
- DHCP Client

Dynamically assigns IP addresses in addition to the option to use static addressing.

- TFTP Client

Facilitates hosting for the configuration file for Autoprovisioning.

- RTP
- SRTP
- RTP/AVP - Audio Video Profile
- SPEEX
- Audio Encodings

PCMU (G.711 mu-law)

PCMA (G.711 A-law)

G.722

G.729

Packet Time 20 ms

1.5 Supported SIP Servers

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

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

1.6 Specifications

Table 1-1. Specifications

Specifications	
Ethernet I/F	10/100 Mbps
Protocol	SIP RFC 3261 Compatible
Power Input	PoE 802.3at or 802.3af
Audio Output	802.3at: 117.9 (+/- 0.2) dBC @ 1M and 1kHz ^a 802.3af: 115.1 (+/- 0.2) dBC @ 1M and 1kHz ^a
Line In:	
Input Signal Amplitudes	2.0 VPP maximum
Input Impedance	10k Ohm
Line Out:	
Output Signal Amplitudes	2.0 VPP maximum
Output Level	+2dBm nominal
Total Harmonic Distortion	0.5% maximum
Output Impedance	10k Ohm
On-Board Relay	1A @ 30 VDC
Payload Types	G.711 a-law, G.711μ-law, G.722, and G.729
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	1.10 in. [29.0 mm] Length 4.20 in. [107.0 mm] Width 8.50 in. [215.0 mm] Height
Weight	1.27 lbs. [0.57 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
Warranty	2 Years Limited
Part Number	011324

a. When used with the 011471 Horn (sold separately).

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

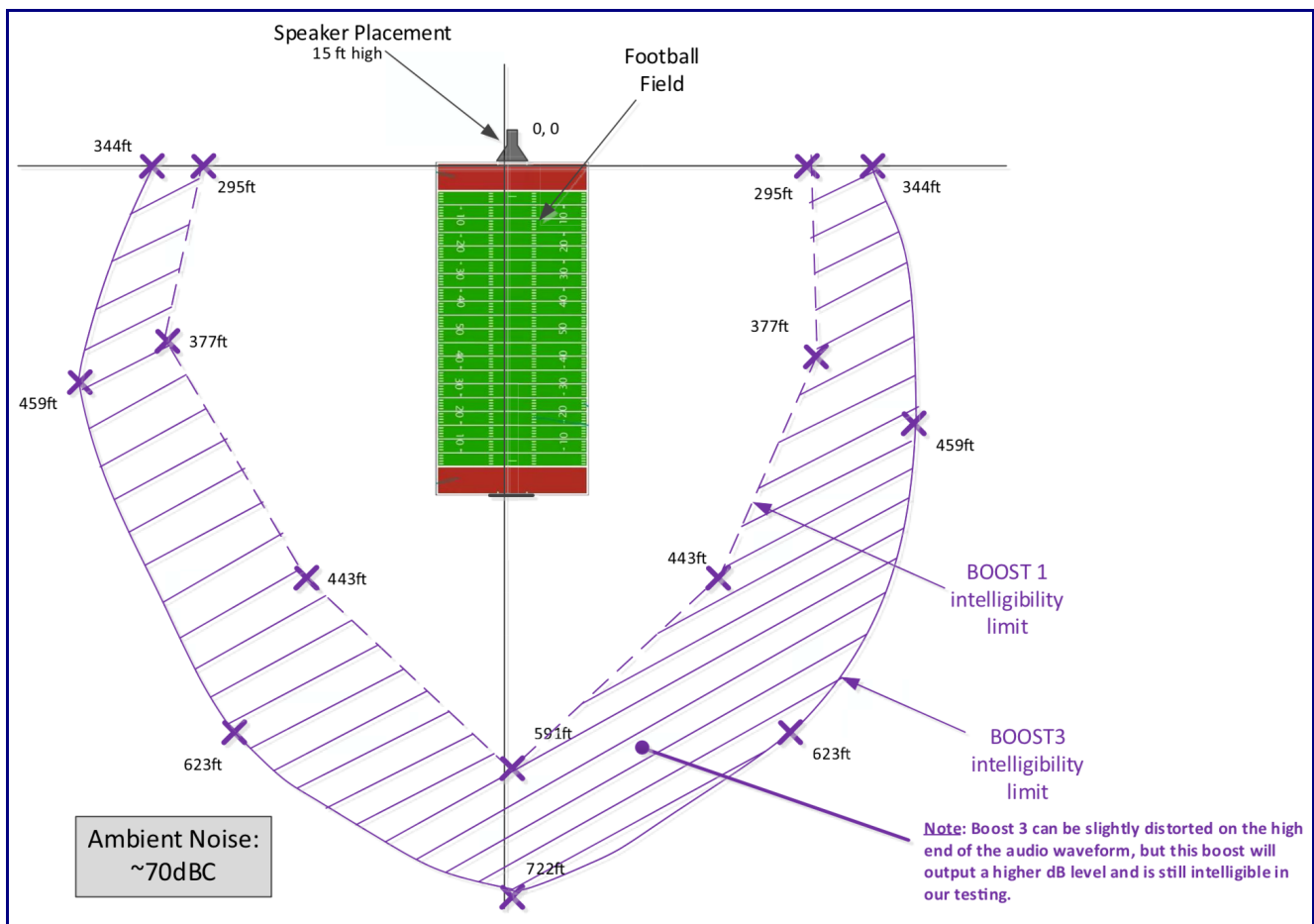
1.7 Typical Coverage

With one horn attached to the Paging Amplifier under standard 802.3af PoE power, coverage is up to 5,000 square feet. With two horns attached to the Paging Amplifier under 802.3at PoE (high power), coverage is up to 10,000 square feet depending on ambient background noise levels.

1.7.1 Intelligibility Outdoor Field Test

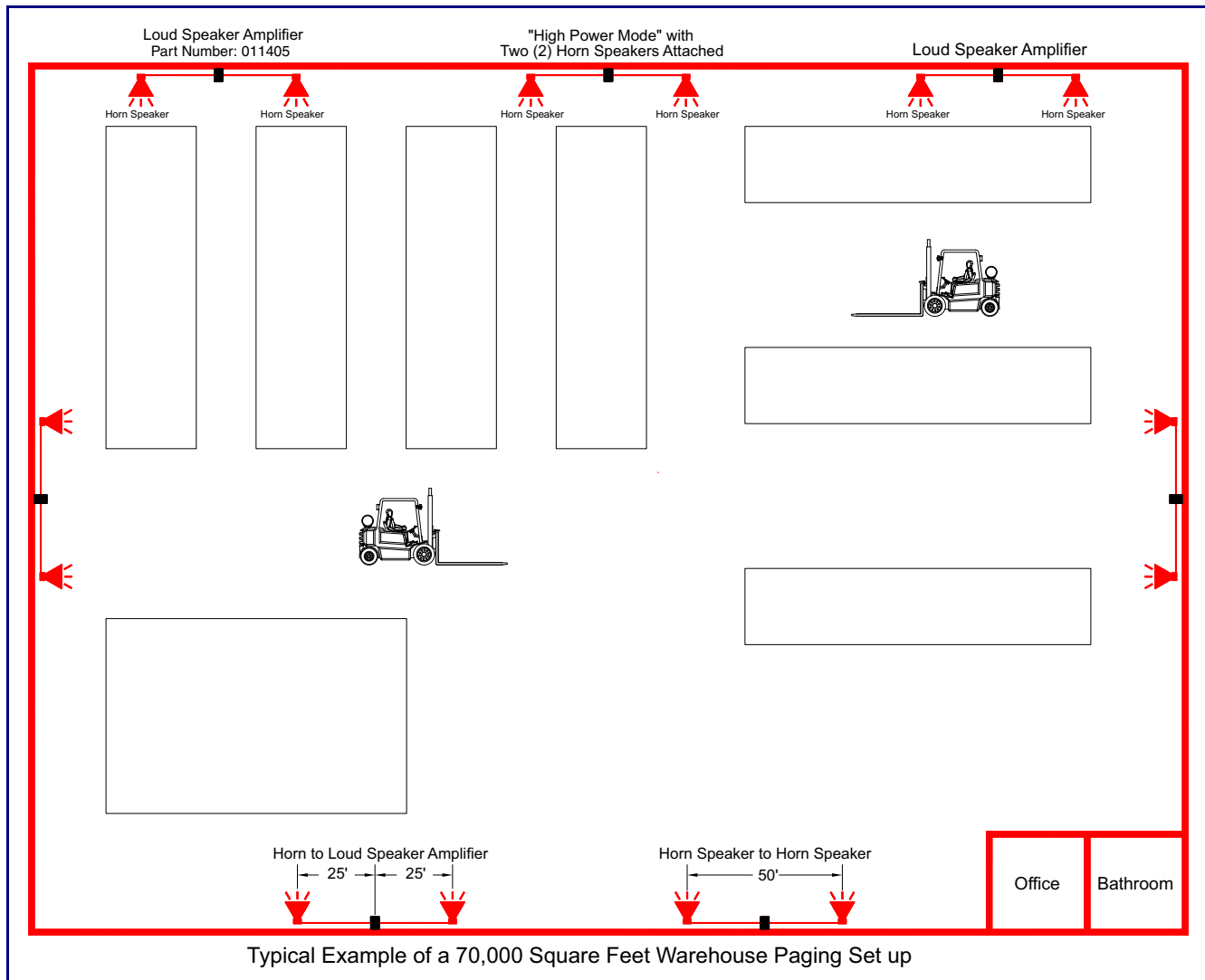
The figure below shows the intelligibility outdoor field test of the device when it is used with the 011471 IP66 Outdoor Analog Horn.

Figure 1-3. Intelligibility Outdoor Field Test



1.7.2 Typical Warehouse Paging Setup

Figure 1-4. Typical Warehouse Paging Setup



1.8 Compliance



1.8.1 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 Radio communications Compliance.

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



1.8.2 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.

1.8.3 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.

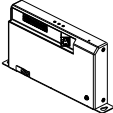


ICES-3 Class A

2 Installing the SIP Paging Amplifier

2.1 Parts List

Table 2-2 illustrates the parts for each SIP Paging Amplifier and includes a kit for mounting.

Table 2-2. Parts List

Quantity	Part Name	Illustration
1	SIP Paging Amplifier Assembly	
1	Installation Quick Reference Guide	
1	SIP Paging Amplifier Accessory Kit	

2.2 SIP Paging Amplifier Setup

Set up and configure each SIP Paging Amplifier *before* you mount it.

CyberData delivers each SIP Paging Amplifier with the factory default values indicated in [Table 2-3](#):

Table 2-3. Factory Default Settings—Default of Network

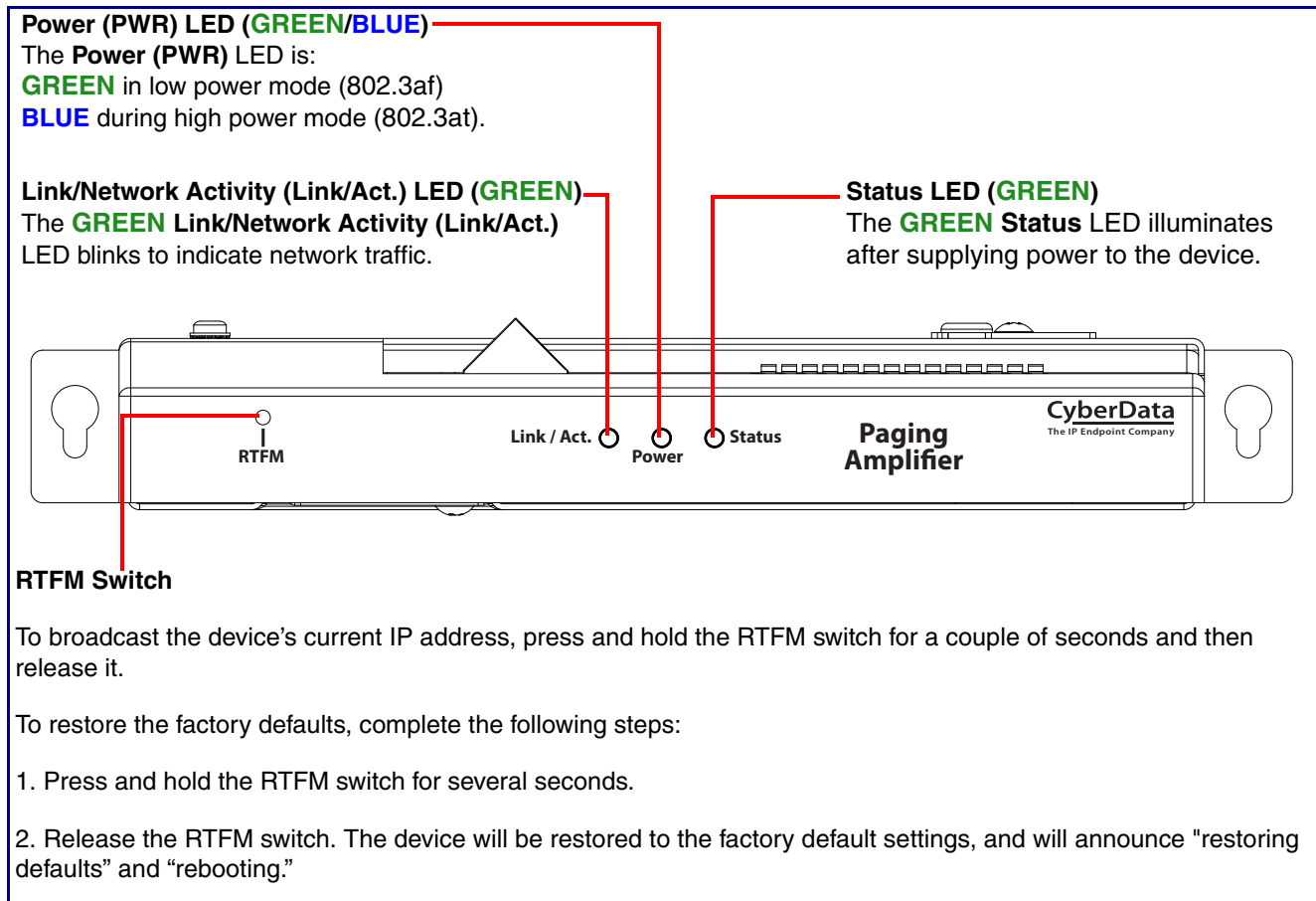
Parameter	Factory Default Setting
IP Addressing	DHCP
IP Address ^a	192.168.1.23
Web Access Username	admin
Web Access Password	admin
Subnet Mask ^a	255.255.255.0
Default Gateway ^a	192.168.1.1

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

2.2.1 SIP Paging Amplifier Components

Figure 2-5 shows the components of the SIP Paging Amplifier.

Figure 2-5. SIP Paging Amplifier Components

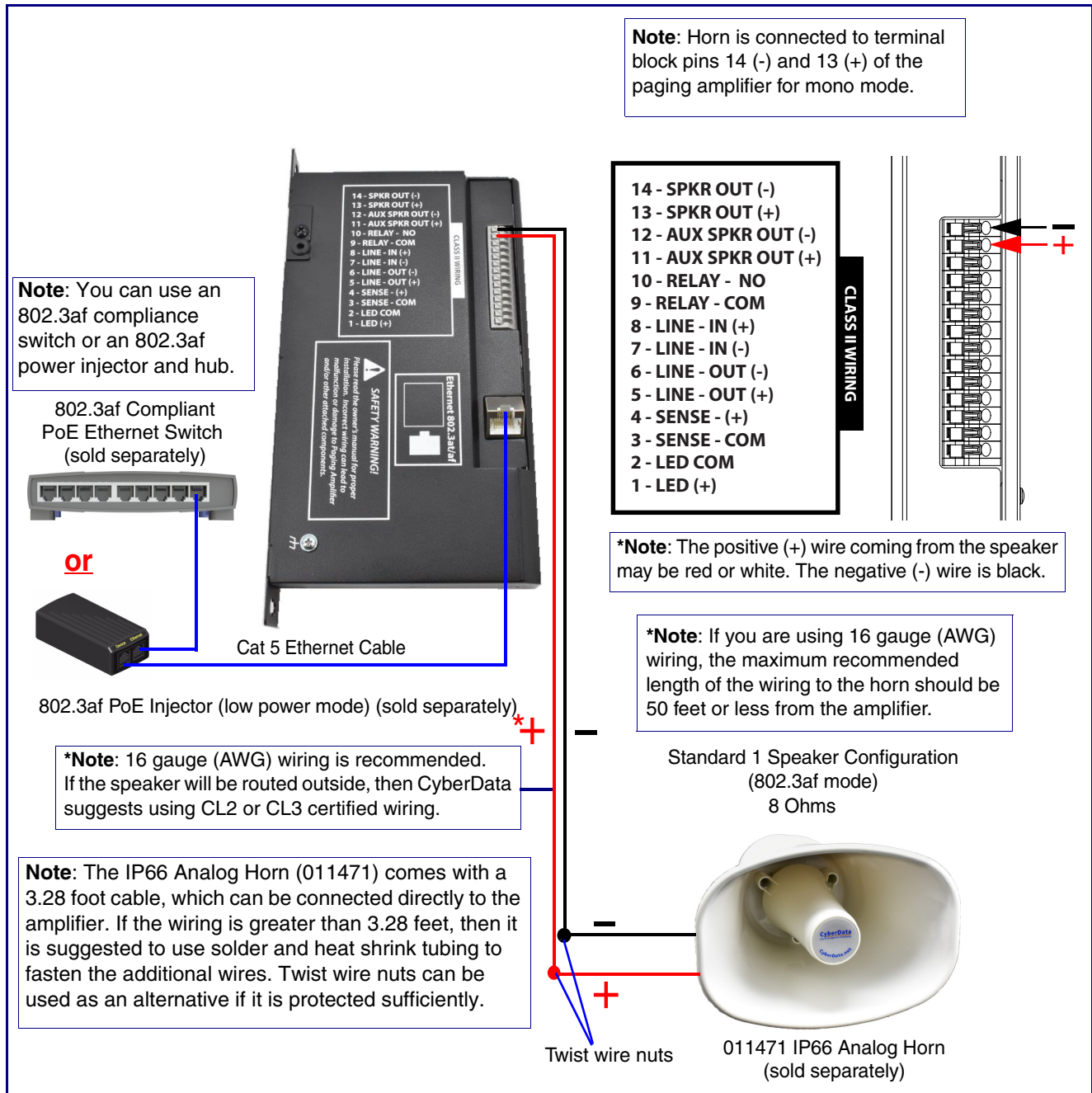


2.2.2 Connecting the SIP Paging Amplifier

2.2.2.1 Using the Amplified Outputs

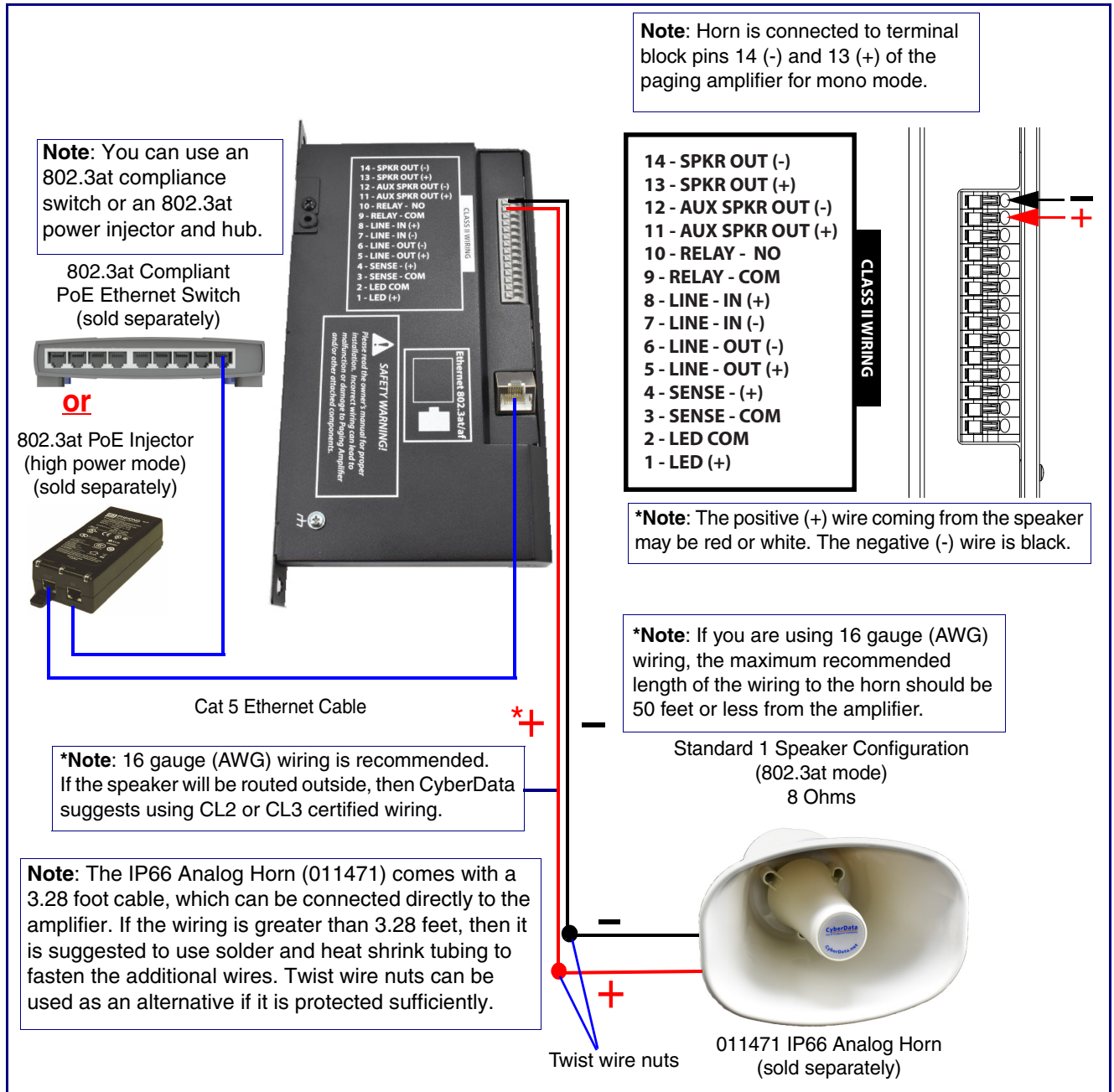
Low Power Mode (One Speaker) The following figure illustrates how to connect the SIP Paging Amplifier and use the amplified outputs in low power mode to one speaker or horn.

Figure 2-6. Using the Amplified Outputs—Low Power Mode with One Speaker



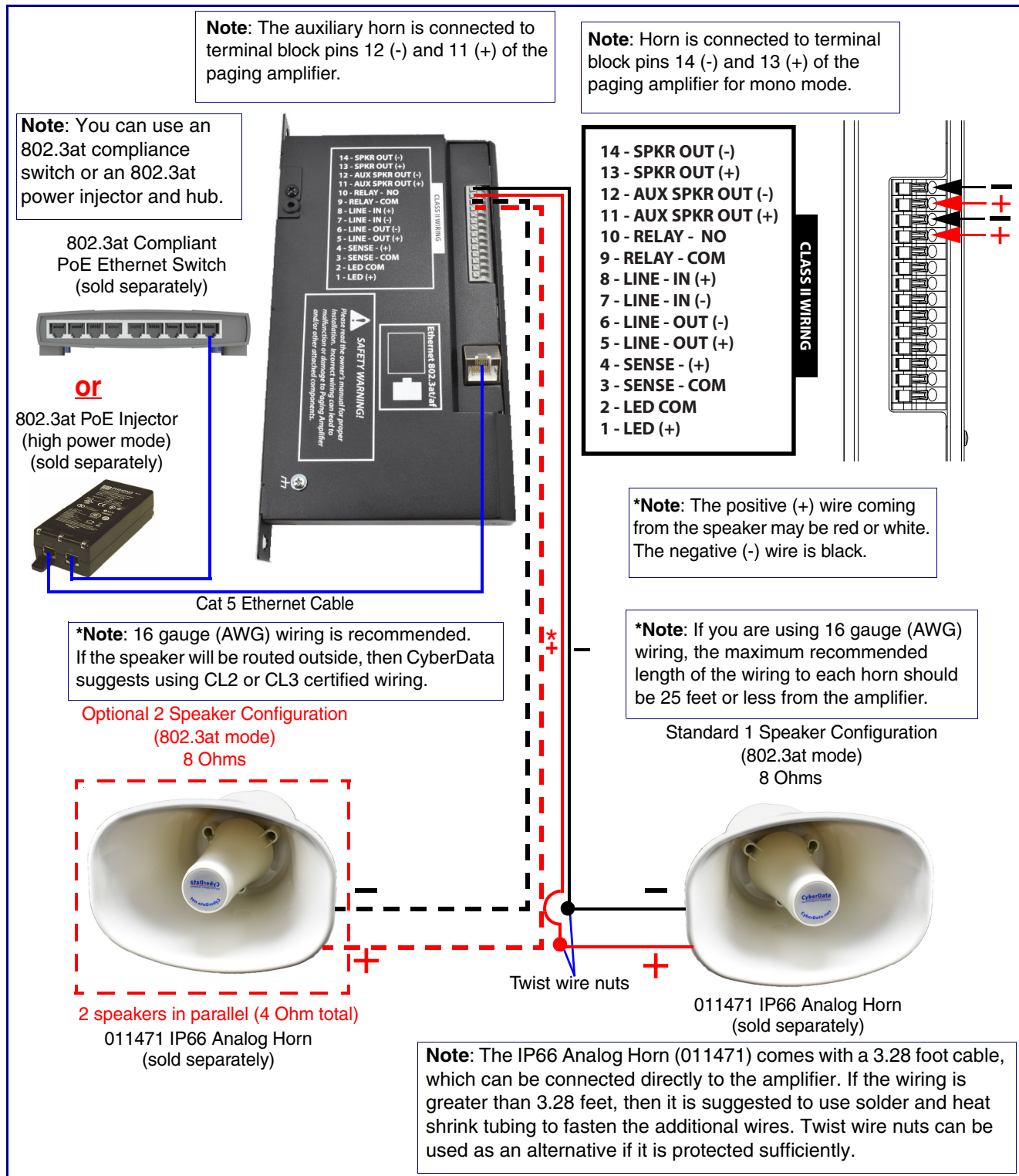
High Power Mode (One Speaker) The following figure illustrates how to connect the SIP Paging Amplifier and use the amplified outputs in high power mode to one speaker or horn.

Figure 2-7. Using the Amplified Outputs—High Power Mode with One Speaker



High Power Mode (Two Speakers) The following figure illustrates how to connect the SIP Paging Amplifier and use the amplified outputs in high power mode to two speakers or horns.

Figure 2-8. Using the Amplified Outputs—High Power Mode with Two Speakers



2.2.3 SIP Paging Amplifier System Installation and Connection Options

The following figures show the connection options for the SIP Paging Amplifier.

Figure 2-9. SIP Paging Amplifier Connections

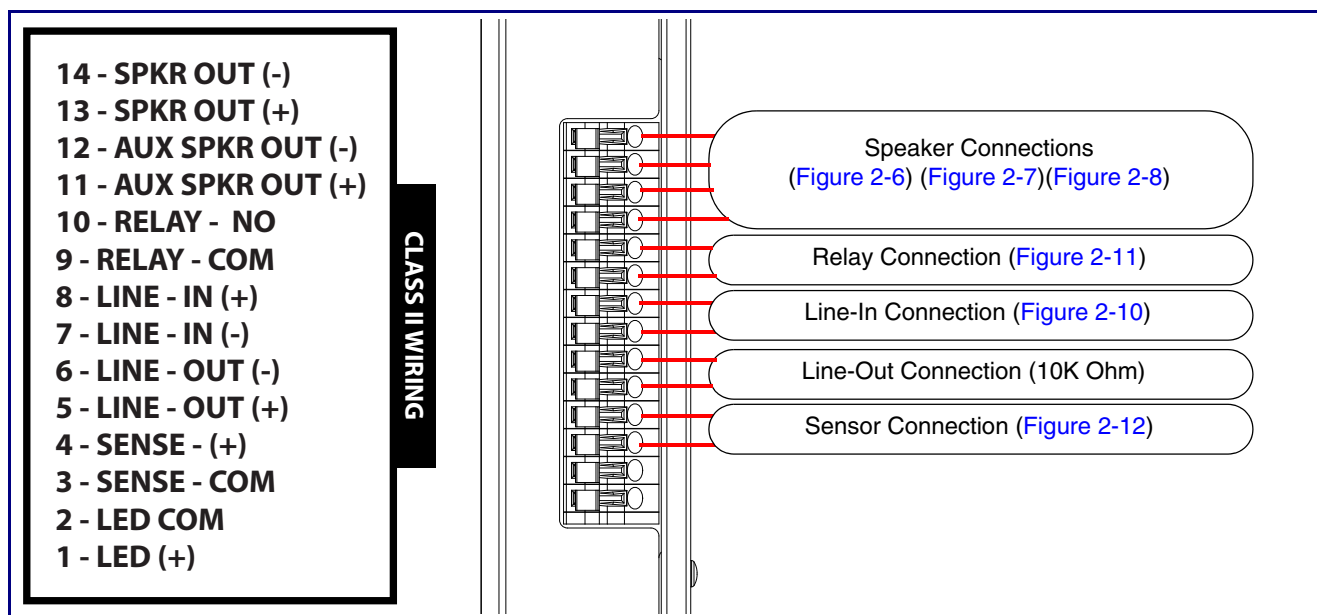


Figure 2-10. Line-In Connection

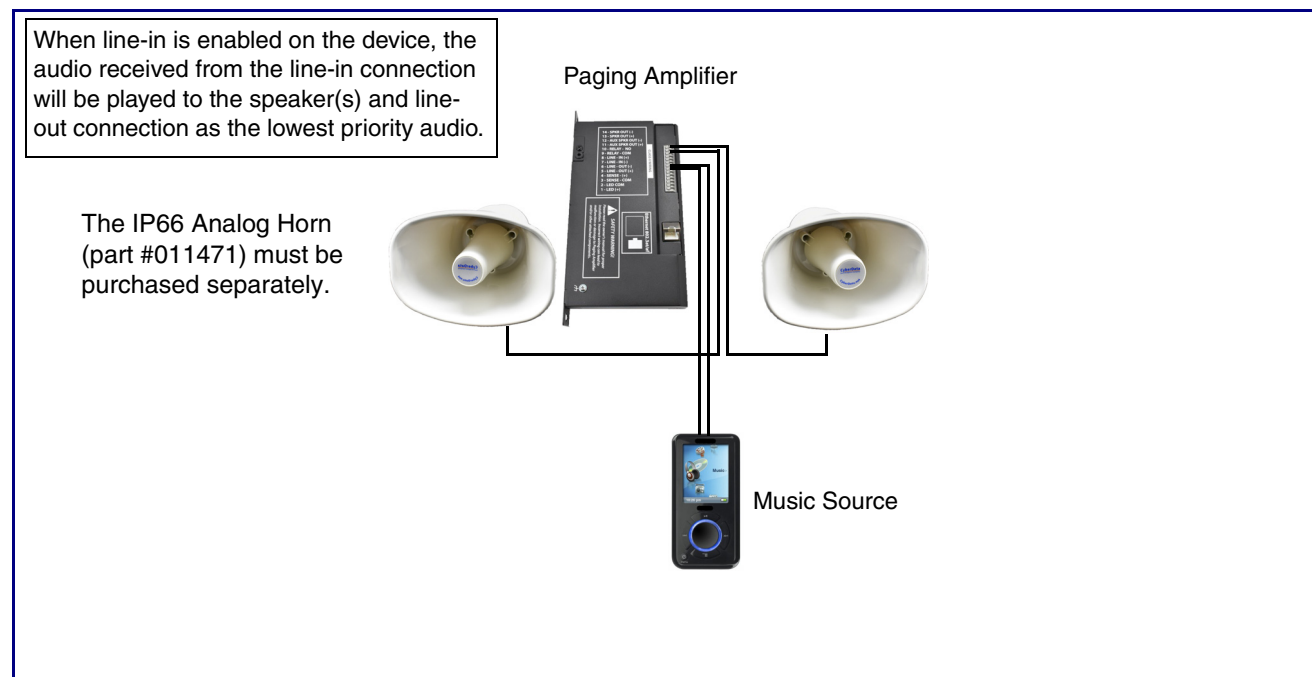


Figure 2-11. Relay or LED Strobe Connection

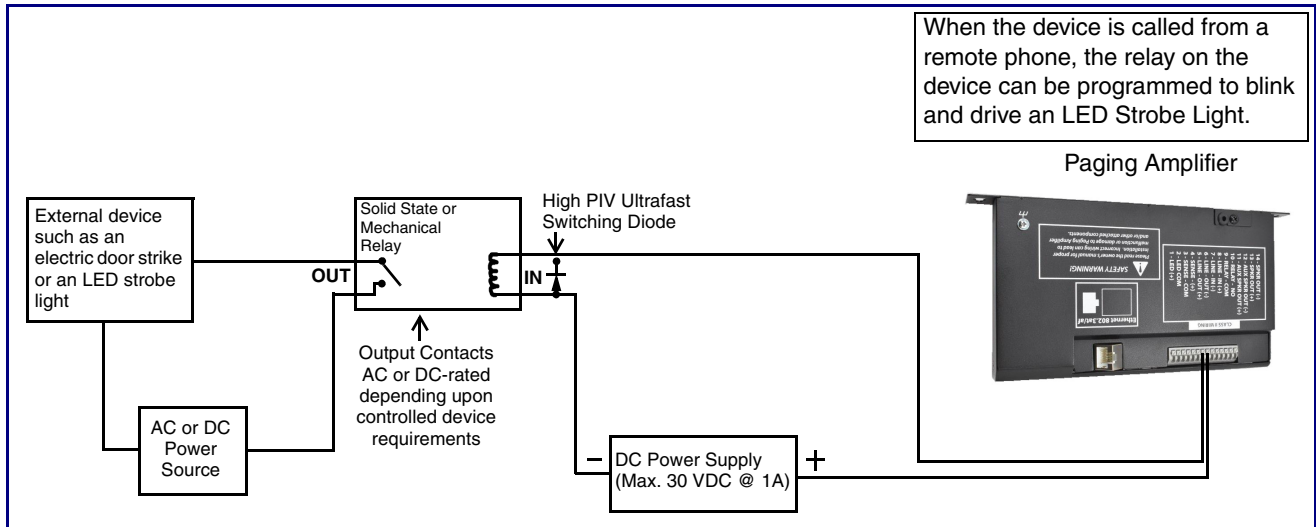
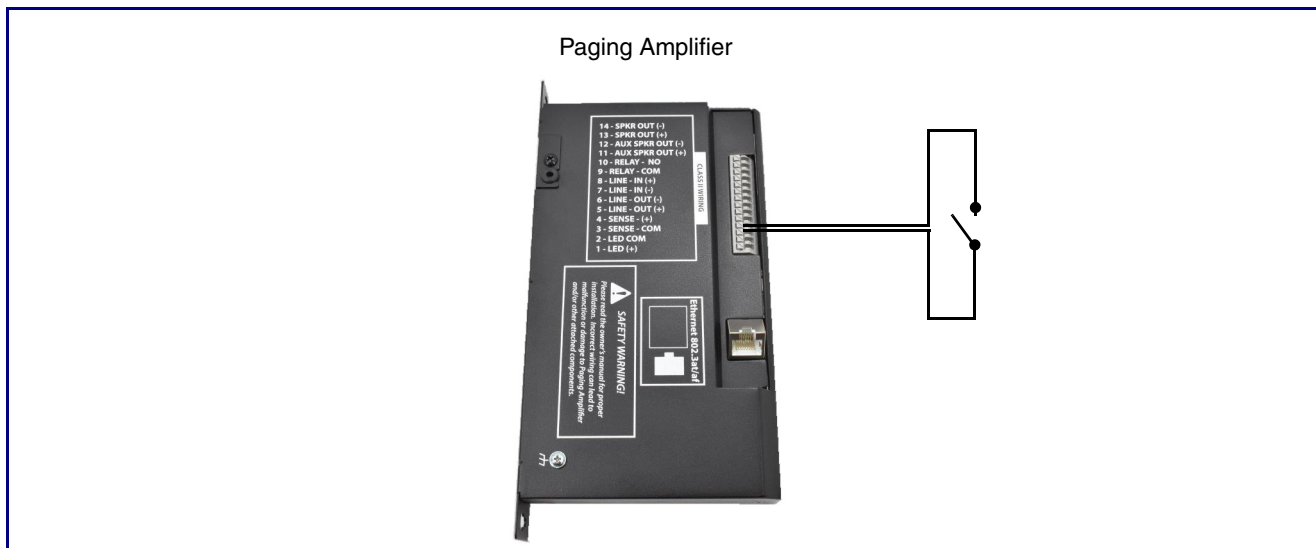


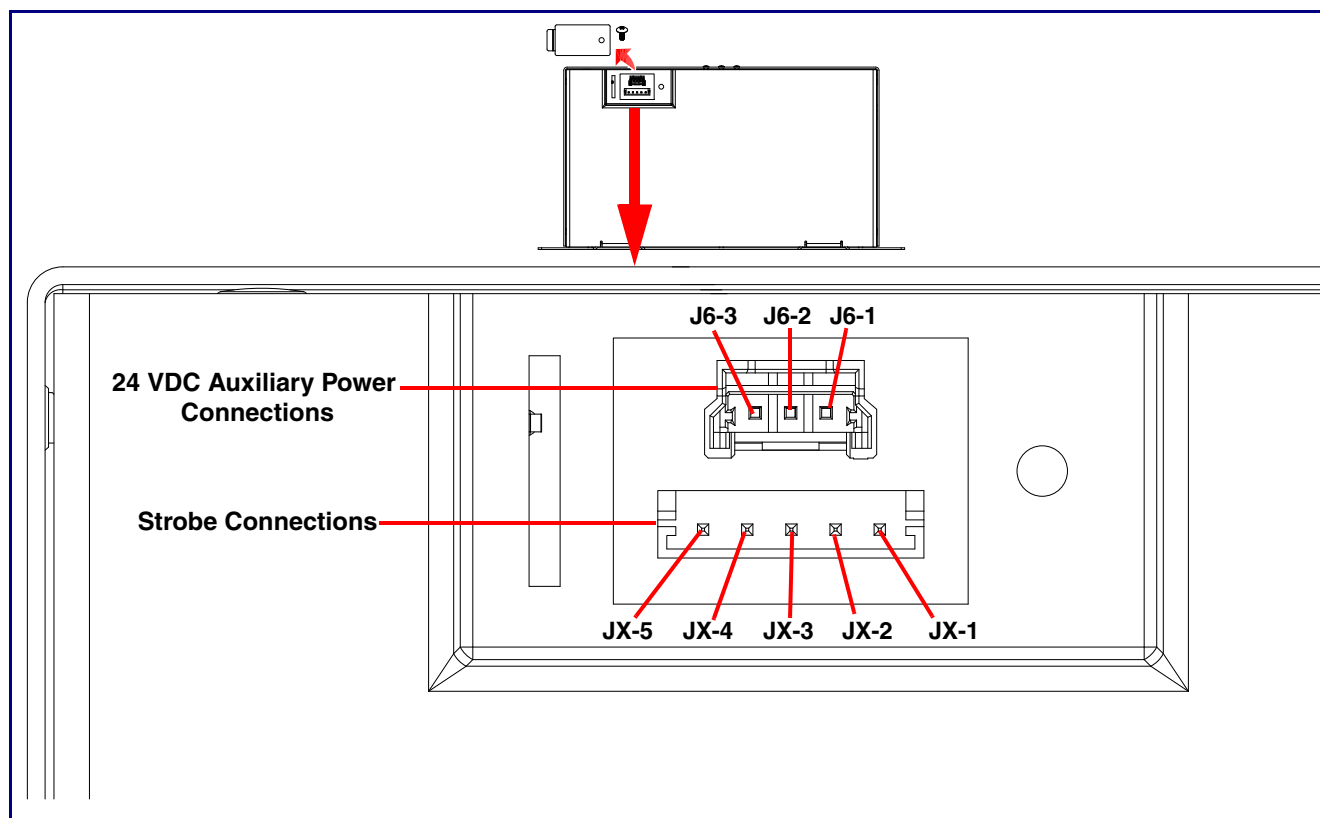
Figure 2-12. Sensor Connection



2.2.4 Strobe Connections Behind the Port Cover

See [Figure 2-13](#) for the additional connection options for the SIP Paging Amplifier.

Figure 2-13. Connections Behind the Port Cover



See [Table 2-4](#) for the descriptions of the connections behind the port cover.

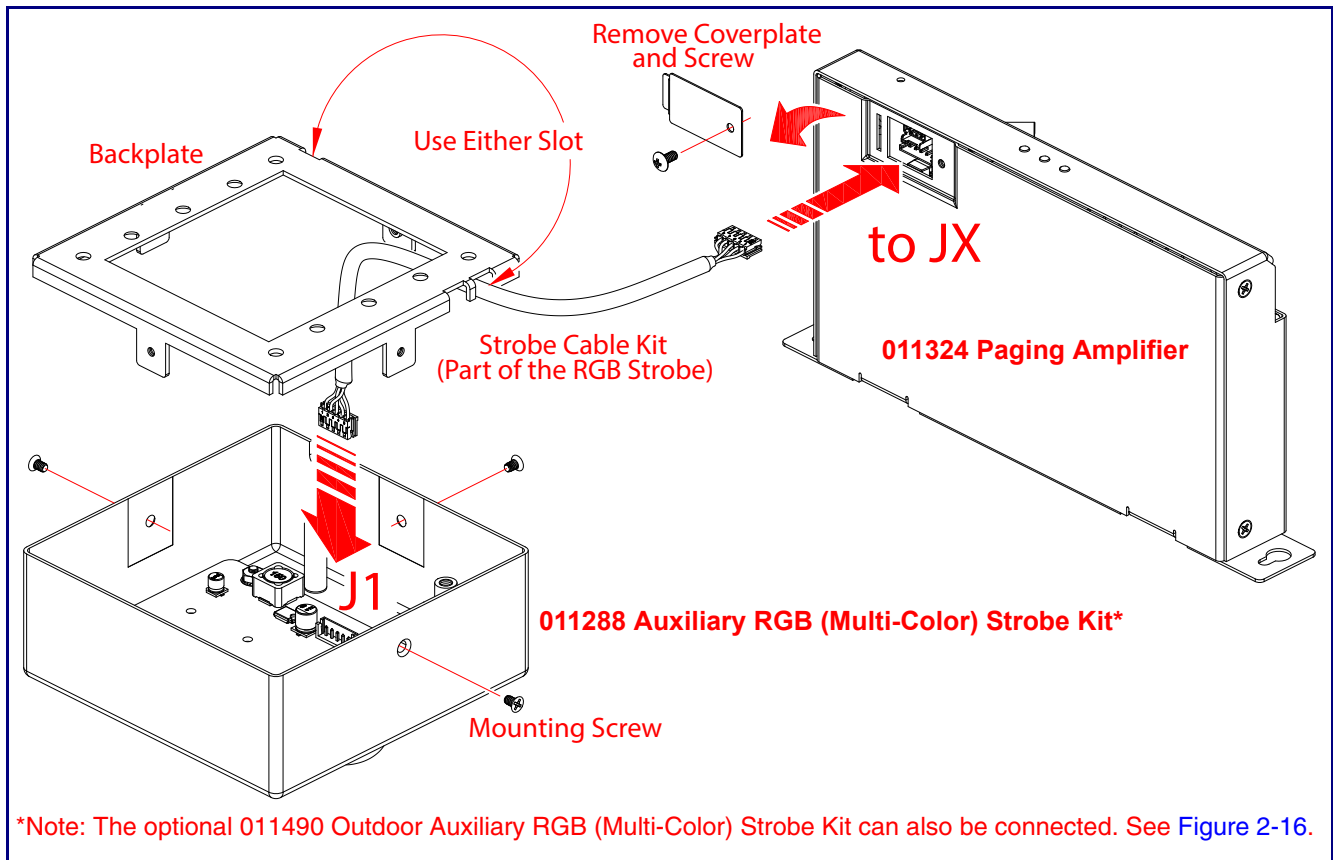
Table 2-4. Connections Behind the Port Cover

Connection	Description
J6-1	+24VDC
J6-2	Ground
J6-3	Chassis Ground
Strobe Connections	
Connection	Description
JX-1	Ground
JX-2	Strobe positive power (+24V)
JX-3	Ground
JX-4	I2C data
JX-5	I2C clock

2.2.5 Connecting the 011288 Auxiliary RGB (Multi-Color) Strobe Kit¹

1. Remove the mounting screw to remove the cover plate. See [Figure 2-14](#).
2. Remove the hole plug and grommet. See [Figure 2-14](#).
3. Slide the cover plate through the slot on the cable grommet. See [Figure 2-14](#).
4. Install the mounting screw to secure the cover plate. See [Figure 2-14](#).

Figure 2-14. Connecting the 011288 Auxiliary RGB (Multi-Color) Strobe Kit



1. The optional 011490 Outdoor Auxiliary RGB (Multi-Color) Strobe Kit can also be connected. See [Figure 2-16](#).

Figure 2-15. Connecting the 011288 Auxiliary RGB (Multi-Color) Strobe Kit

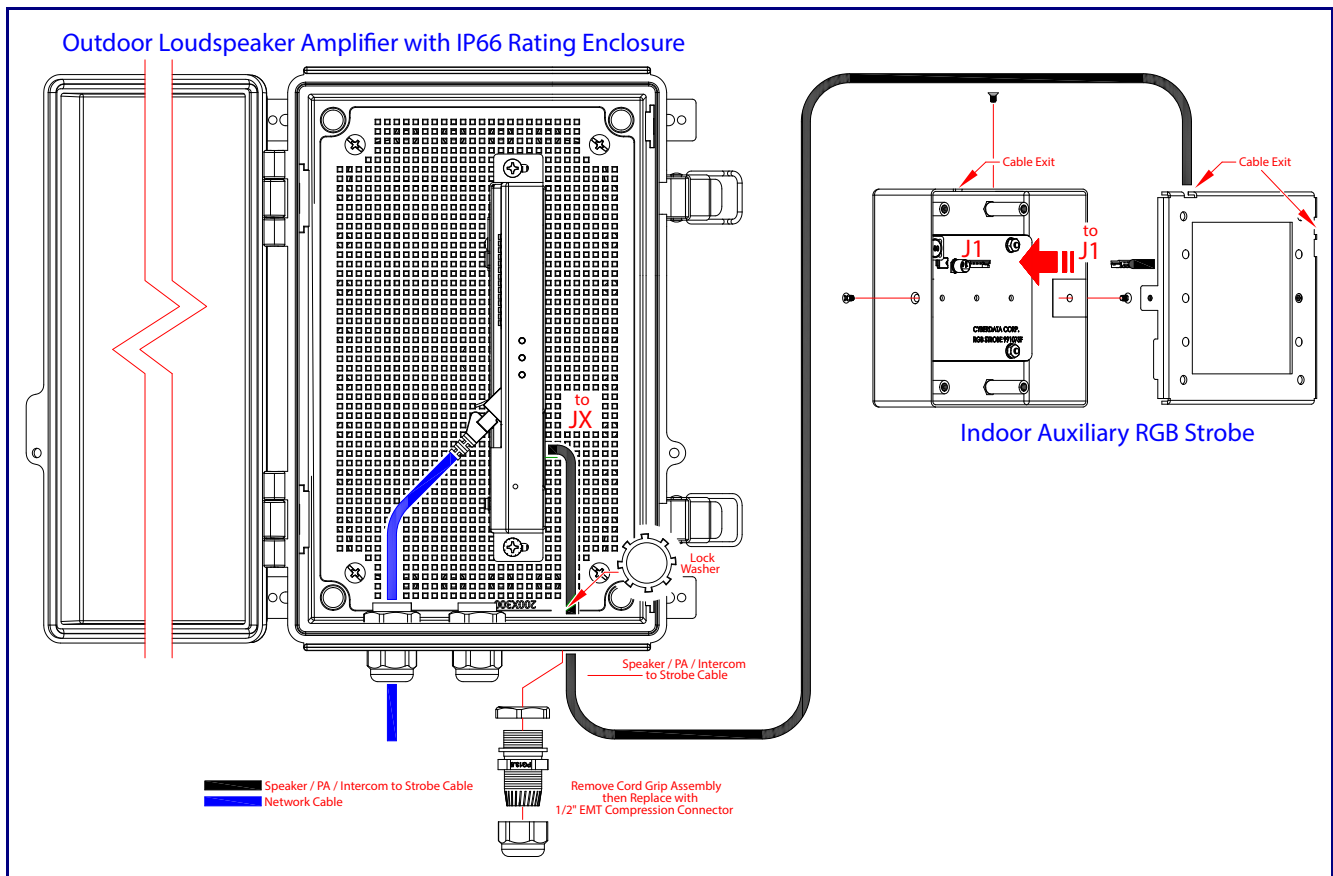
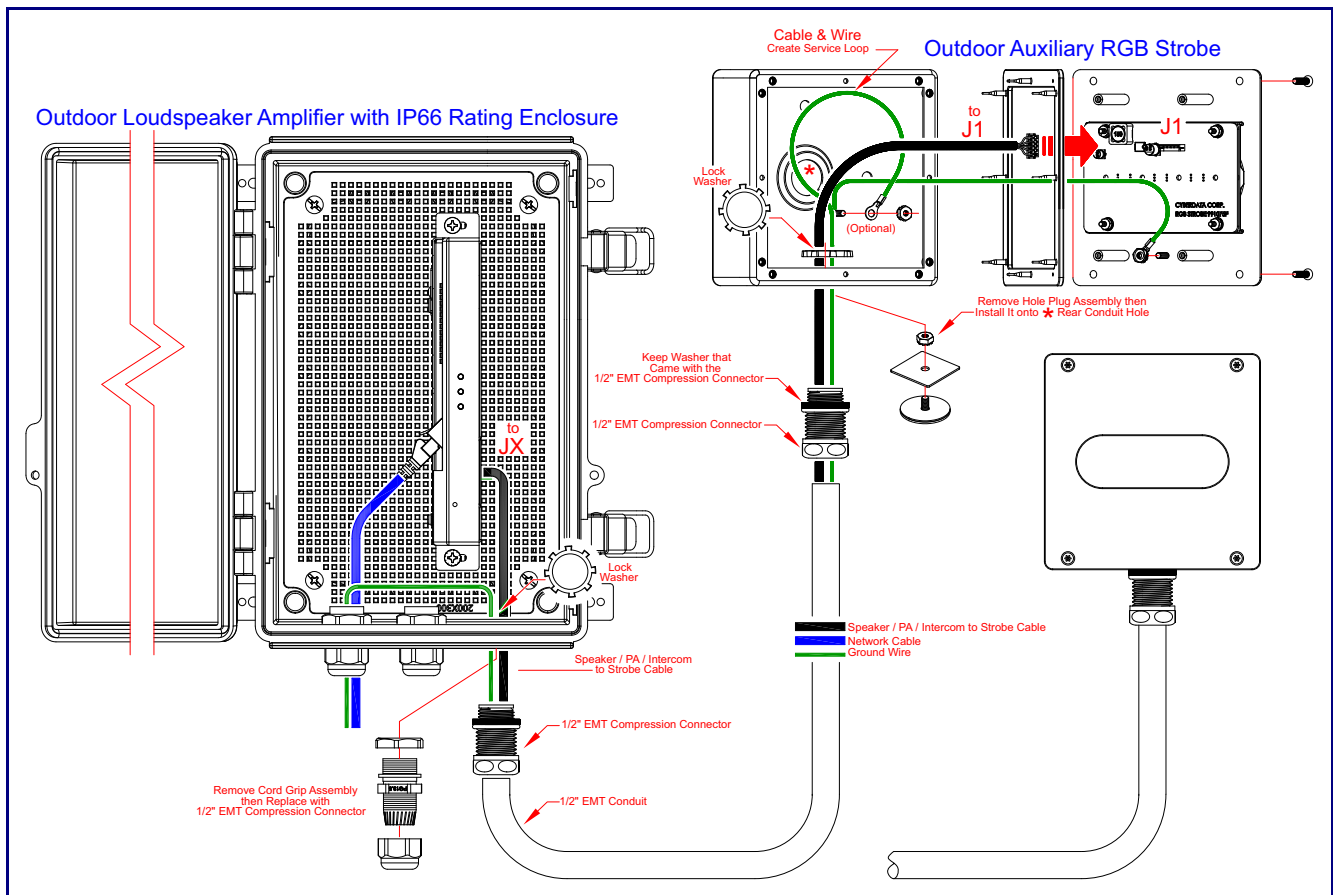


Figure 2-16. Connecting the 011490 Outdoor Auxiliary RGB (Multi-Color) Strobe Kit



2.2.6 Ethernet Connection

See [Table 2-5](#) for details about the SIP Paging Amplifier connection.

Table 2-5. SIP Paging Amplifier Connection

Connection	Connection Details	Location
Ethernet	Use a RJ 45 cable.	SIP Paging Amplifier

2.2.7 Loudspeaker Type

Using the amplified output, the CyberData SIP Paging Amplifier supports the 011471 IP66 Analog Horn or equivalent unamplified loudspeaker.

Figure 2-17. 011471 IP66 Analog Horn



2.2.8 Cabling/Wiring

Using the amplified output, you may connect a 011471 Horn or equivalent unamplified speaker to a SIP Paging Amplifier with good quality speaker wire that is 16 gauge and limited to 25 feet in length with two loudspeakers or 50 feet in length with one loudspeaker.

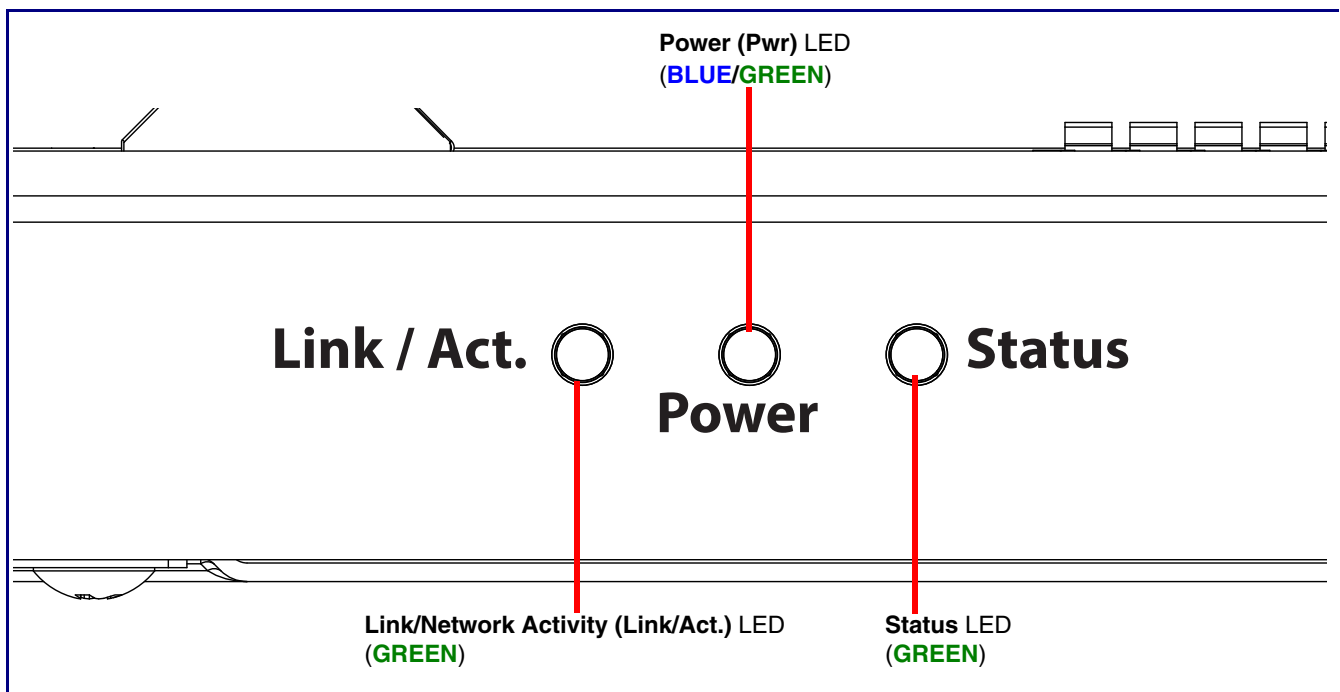
2.2.9 Confirm Operation

After connecting the SIP Paging Amplifier to the 802.3af compliant ethernet hub, use the LEDs on the SIP Paging Amplifier face to confirm that the SIP Paging Amplifier is operational and linked to the network.

Table 2-6. SIP Paging Amplifier LEDs

LED	Color	Function
Power (PWR)	BLUE/GREEN	The power LED is GREEN in low power mode (802.3af) and a BLUE during high power mode (802.3at). The power LED will blink during a boot up or a phone call.
Status	GREEN	After supplying power to the device, a steady GREEN Status LED illuminates. After about 20 seconds the GREEN Status LED will blink twice to indicate that the board is fully booted. The status LED will blink during a page when it is online.
Link/Network Activity (Link/Act.)	GREEN	The Link/Network Activity (Link/Act.) GREEN LED blinks to indicate network traffic.

Figure 2-18. SIP Paging Amplifier LEDs

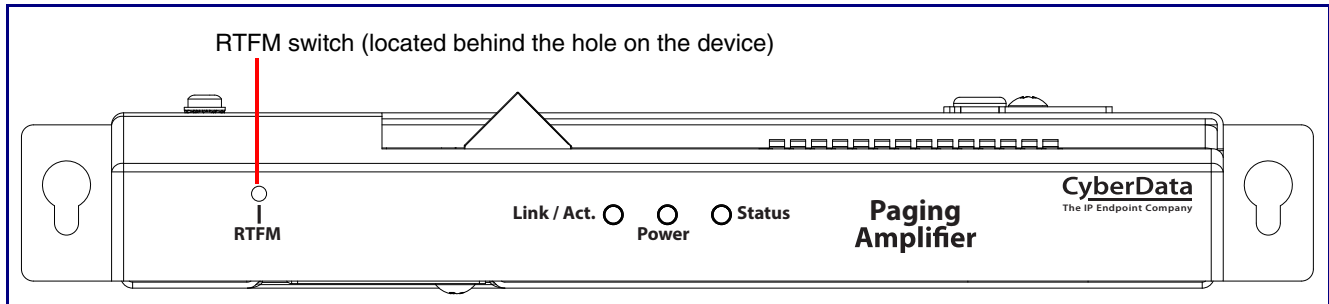


2.2.10 Confirm the IP Address and Test the Audio

2.2.10.1 RTFM Switch


When the SIP Paging Amplifier is operational and linked to the network, use the Reset Test Function Management (**RTFM**) switch ([Figure 2-19](#)) (located behind the hole on the device) to announce and confirm the device's IP Address and test the audio to verify that it is working.

Figure 2-19. RTFM Switch



Announcing the IP Address To announce a device's current IP address:

- Use a bent paperclip or a similar object to briefly press the RTFM switch and release it.

 <p>GENERAL ALERT</p>	<p>Caution</p> <p><i>Equipment Caution:</i> Pressing and holding the RTFM switch for more than five seconds will restore the device to the factory default settings. See the “Restoring the Factory Default Settings” section.</p>
--	---

Restoring the Factory Default Settings

To restore the factory default settings, complete the following steps:

1. Use a bent paperclip or a similar object to press and hold the RTFM switch for several seconds.
2. Release the RTFM switch. The device will be restored to the factory default settings, and will announce "restoring defaults" and "rebooting."

2.3 Configure the SIP Paging Amplifier Parameters

To configure the SIP Paging Amplifier online, use a standard web browser.

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

2.3.1 Factory Default Settings

All SIP Paging Amplifiers are initially configured with the following default IP settings:

When configuring more than one SIP Paging Amplifier, attach the SIP Paging Amplifiers to the network and configure one at a time to avoid IP address conflicts.

Table 2-7. Factory Default Settings

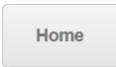
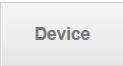
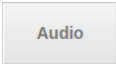
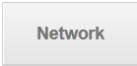

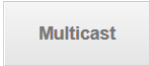

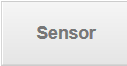
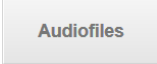
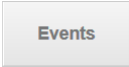


Parameter	Factory Default Setting
IP Addressing	DHCP
IP Address ^a	192.168.1.23
Web Access Username	admin
Web Access Password	admin
Subnet Mask ^a	255.255.255.0
Default Gateway ^a	192.168.1.1

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

2.3.2 SIP Paging Amplifier Web Page Navigation

Table 2-8 shows the navigation buttons that you will see on every SIP Paging Amplifier web page.

Table 2-8. Web Page Navigation

Web Page Item	Description
	Link to the Home page.
	Link to the Device page.
	Link to the Audio page.
	Link to the Network page.
	Link to go to the SIP page.
	Link to the Multicast page.
	Link to the SSL 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:

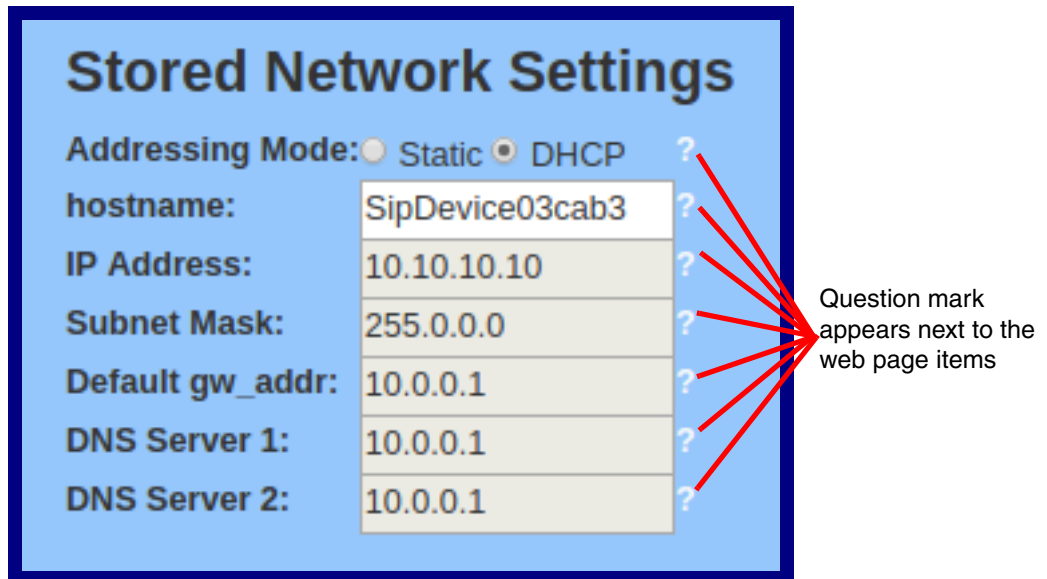
1. Click on the **Toggle Help** button that is on the UI webpage. See [Figure 2-20](#) and [Figure 2-21](#).

Figure 2-20. Toggle/Help Button



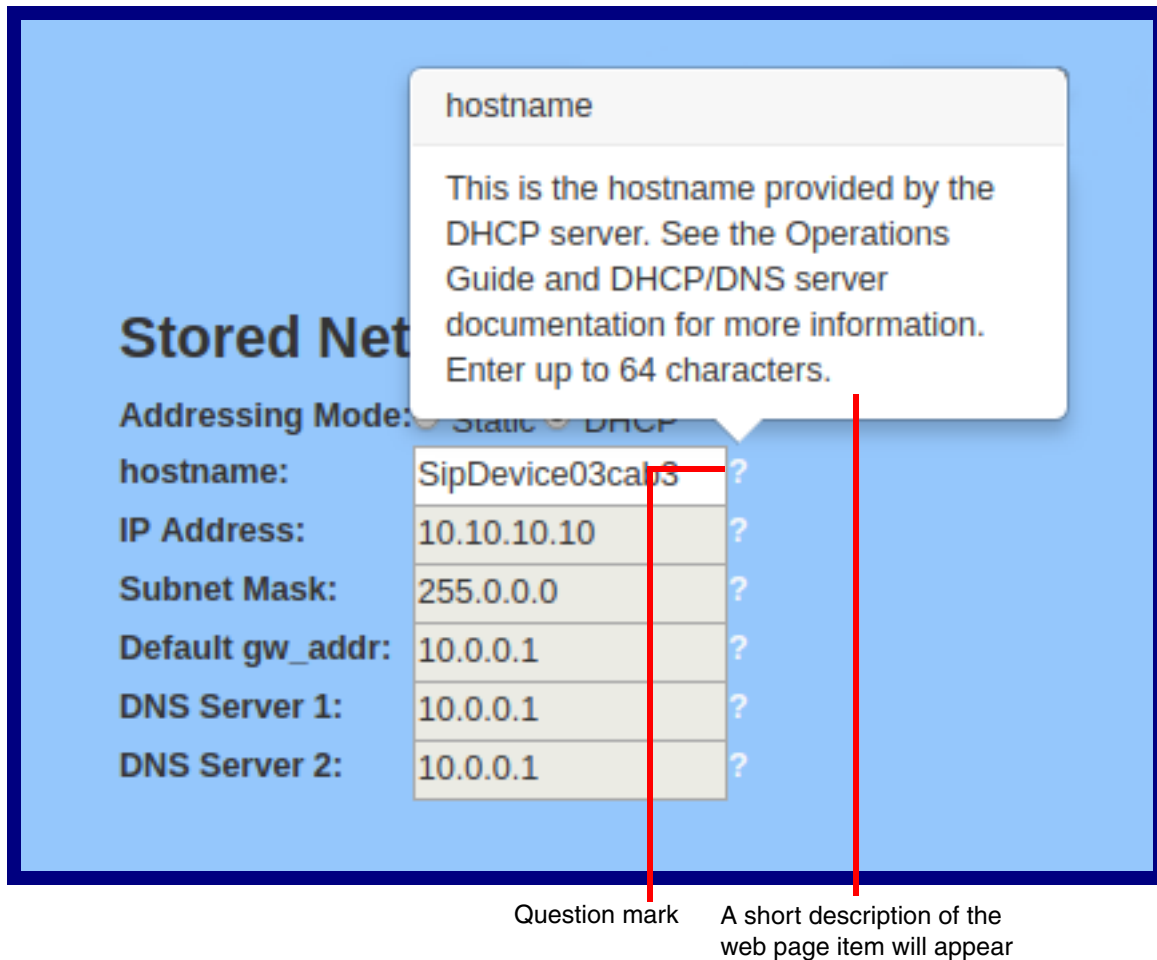
2. You will see a question mark (?) appear next to each web page item that has been provided with a short description by the Help feature. See [Figure 2-21](#).

Figure 2-21. Toggle Help Button and Question Marks



3. Move the mouse pointer to hover over the question mark (?), and a short description of the web page item will appear. See [Figure 2-22](#).

Figure 2-22. Short Description Provided by the Help Feature



2.3.4 Log in to the Home Page

1. Open your browser to the device IP address.

Note If the network does not have access to a DHCP server, the device will default to an IP address of 192.168.123.

Note Make sure that the PC is on the same IP network as the SIP Paging Amplifier.

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 device 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 2-23):

Web Access Username: **admin**

Web Access Password: **admin**

Figure 2-23. Home Page

HomeDeviceAudioNetworkSIPSSLMulticastSensorAudiofilesEventsAutoprovFirmware

CyberData SIP Paging Amp

Current Status

Serial Number:324200001
Mac Address:00:20:f7:04:fb:37
Firmware Version:v20.5.0
Partition 2:v20.5.0
Partition 3:v20.5.0
Bootling From:partition 2

Boot From Other Partition

IP Addressing:DHCP
IP Address:10.10.1.15
Subnet Mask:255.0.0.0
Default Gateway:10.0.0.1
DNS Server 1:10.0.1.56
DNS Server 2:

SIP Volume:4
Multicast Volume:4
Ring Volume:4
Sensor Volume:4
Volume Boost:0

SIP Mode:Enabled
Multicast Mode:Disabled
Event Reporting:Disabled

Primary SIP Server:**Not registered**
Backup Server 1:Not registered
Backup Server 2:Not registered
Nightringer Server:Not registered

Admin Settings

Username:

admin

Password:

Confirm Password:

SaveRebootToggle Help

Import Settings

Browse...

No file chosen

Import Config

Export Settings

Export Config

3. On the **Home** page, review the setup details and navigation buttons described in [Table 2-9](#).

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. Home Page Overview


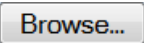





Web Page Item	Description
Admin Settings	
Username ?	The username to access the web interface. Enter up to 25 characters.
Password ?	The password to access the web interface. Enter up to 25 characters.
Confirm Password ?	Confirm the web interface password.
Current Status	
Serial Number	Shows the device 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.
Bootting From	Indicates the partition currently used for boot.
	Allows the user to boot from the alternate partition.
IP Addressing	Shows the current IP addressing setting (DHCP or static).
IP Address	Shows the current IP address.
Subnet Mask	Shows the current subnet mask address.
Default Gateway	Shows the current default gateway address.
DNS Server 1	Shows the current DNS Server 1 address.
DNS Server 2	Shows the current DNS Server 2 address.
SIP Volume	Shows the current SIP volume level.
Multicast Volume	Shows the current Multicast volume level.
Ring Volume	Shows the current Ring volume level.
Sensor Volume	Shows the current Sensor volume level.
Volume Boost	Shows the current Volume Boost level.
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.
Import Settings	

Table 2-9. Home Page Overview (continued)

Web Page Item	Description
	Use this button to select a configuration file to import.
	After selecting a configuration file, click Import to import the configuration from the selected file. Then, click Save to store changes.
Export Settings	
	Click Export to export the current configuration to a file.
	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.

2.3.5 Configure the Device

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

Figure 2-24. Device Page

Home Device Audio Network SIP SSL Multicast Sensor Audiofiles Events Autoprov Firmware

CyberData SIP Paging Amp

Relay Settings

Activate Relay with DTMF code: ☐

Relay Pulse Code:

Relay Pulse Duration (seconds):

Relay Activation Code:

Relay Deactivation Code:

Activate Relay During Ring: ☐

Activate Relay During Night Ring: ☐

Activate Relay While Call Active: ☐

DTMF Settings

Require Security Code: ☐

Security Code:

Play Stored Message: ☐

Save Reboot Toggle Help Test Relay

Time Settings

Enable NTP: ☒

NTP Server:

Timezone:

Current Time: Fri, 30 Sep 2022 12:42:37

Power Settings

802.3AT Mode: Detected and enabled.

Force 802.3AT Mode (NOT recommended): ☐

Misc Settings

Device Name:

Auto-Answer Incoming Calls: ☐

Beep on Init: ☐

Beep Before Page: ☐

Two Speakers Connected: ☐

RGB Strobe Status: Installed



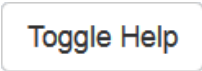

2. On the **Device** page, you may enter values for the parameters indicated in [Table 2-10](#).

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. Device Page Parameters

Web Page Item	Description
Relay Settings	
Activate Relay with DTMF Code ?	Activates the relay when the DTMF Activation Code is entered on the phone during a SIP call with the device. RFC2833 DTMF payload types are supported.
Relay Pulse Code ?	DTMF code used to pulse the relay when entered on a phone during a SIP call with the device. Relay will activate for Relay Pulse Duration seconds then deactivate. Activate Relay with DTMF Code must be enabled. Enter up to 25 digits (* and # are supported).
Relay Pulse Duration (in seconds) ?	The length of time (in seconds) during which the relay will be activated when the DTMF Relay Activation Code is detected. Enter up to 5 digits.
Relay Activation Code ?	Activation code used to activate the relay when entered on a phone during a SIP call with the device. Relay will be active indefinitely, or until the DTMF Relay Deactivation code is entered. Activate Relay with DTMF Code must be enabled. Enter up to 25 digits (* and # are supported).
Relay Deactivation Code ?	Code used to deactivate the relay when entered on a phone during a SIP call with the device. Activate Relay with DTMF Code must be enabled. Enter up to 25 digits (* and # are supported).
Activate Relay During Ring ?	When selected, the relay will be activated for as long as the device is ringing. When Auto-Answer Incoming Calls is enabled, the device will not ring and this option does nothing.
Activate Relay During Night Ring ?	When selected, the relay will be activated as long as the Nightringer extension is ringing.
Activate Relay While Call Active ?	When selected, the relay will be activated as long as the SIP call is active.
Time 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.
Power Settings	

Table 2-10. Device Page Parameters (continued)

Web Page Item	Description
802.3AT Mode ?	This device automatically detects if it is plugged into an 802.3AT (also known as PoE Plus) power source. 802.3AT provides more power than older 802.3AT power sources and allows this speaker to play audio at higher volumes. If you are sure this speaker is connected to an 802.3AT power source, but it is not being detected correctly, you can override the automatic settings below.
Force 802.3AT Mode (NOT recommended) ?	Enable this option if you are sure this speaker is connected to an 802.3AT power source, but it is not being detected correctly (not recommended).
Misc Settings	
Device Name ?	Type the device name. Enter up to 25 characters.
Auto-Answer Incoming Calls ?	When selected, the device will automatically answer incoming calls. When Auto-Answer Incoming Calls is disabled, the device will play a ring tone (corresponds to Ring Tone on the Audiofiles page) out of the speaker.
Beep on Init ?	Device will play the user-defined "pagetone" audio file when it boots.
Beep on Page ?	Device will play the user defined "pagetone" audio file before playing a SIP page.
Two Speakers Connected ?	Specify if one or two speakers are connected to the paging amplifier. If only one is connected, ensure that it is wired to the first set of terminal blocks.
RGB Strobe ?	Status of optional RGB Strobe.
DTMF Settings	
Require Security Code ?	When selected, the user will be prompted to enter a Security Code (entered on this page) before being able to execute a page when calling the device.
Security Code ?	Type the Security Code in this field. The Security Code must only use characters '0-9', '*' and '#'. Enter up to 25 characters.
Play Stored Message ?	When selected, the caller will be prompted to select one of nine stored messages to play through the speaker. Stored messages may be customized on the Audiofiles page.
	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.
	Click on the Test Relay button to do a relay test.

2.3.6 Configure the Audio

1. Click the **Audio** menu button to open the **Audio** page. See [Figure 2-25](#).

Figure 2-25. Audio Page

The screenshot shows the 'Audio' configuration page of the CyberData SIP Paging Amp. At the top is a navigation bar with buttons for Home, Device, Audio (selected), Network, SIP, SSL, Multicast, Sensor, Audiofiles, Events, Autopro, and Firmware. The main heading is 'CyberData SIP Paging Amp'. Below it is the 'Volume Settings (0-9)' section. This section includes a checkbox for 'Enable Line-in to Line-out Loopback' which is currently unchecked. There are five volume controls, each with a label and a dropdown menu: 'SIP Volume:' (4), 'Multicast Volume:' (4), 'Ring Volume:' (4), 'Sensor Volume:' (4), and 'Volume Boost:' (No Volume Boost). At the bottom of the settings are four buttons: 'Save', 'Reboot', 'Toggle Help', and 'Test Audio'.

Setting	Value
Enable Line-in to Line-out Loopback	<input type="checkbox"/>
SIP Volume	4
Multicast Volume	4
Ring Volume	4
Sensor Volume	4
Volume Boost	No Volume Boost

Buttons: Save, Reboot, Toggle Help, Test Audio

2. On the **Audio** page, you may 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. Audio Page Parameters

Web Page Item	Description
Volume Settings (0-9)	
Enable Line-in to Line-out Loopback ?	Line-in audio will play back out the device's audio output ports. This is the lowest priority audio and will be preempted by any other audio stream.
SIP Volume ?	Set the speaker volume for a SIP call. A value of 0 will mute the speaker during SIP calls.
Multicast Volume ?	Set the speaker volume for multicast audio streams. A value of 0 will mute the speaker during multicasts.
Ring Volume ?	Set the ring volume for the Nightringer. A value of 0 will mute the speaker for the Nightringer.
Sensor Volume ?	Set the speaker volume for playing sensor activated audio. A value of 0 will mute the speaker during sensor activated audio.
Volume Boost: ? No Volume Boost Volume Boost 1 Volume Boost 2 Volume Boost 3	NOT RECOMMENDED! Set the Boost level to increase the volume output of the speaker. Using Volume Boost may introduce audio clipping, reduce intelligibility of the speaker audio, or cause instability. Boost will raise the volume above level '9', regardless of the digital volumesettings. If Boost is going to be used, it should be used with low gain audio sources and at a low volume output level.
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 Audio	Click on the Test Audio button to do an audio test. When the Test Audio button is pressed, you will hear a voice message for testing the device audio quality and volume.

2.3.7 Configure the Network Parameters

1. Click the **Network** menu button to open the **Network** page (Figure 2-26).

Figure 2-26. Network Page

HomeDeviceAudio**Network**SIPSSLMulticastSensorAudiofilesEventsAutoprovFirmware

CyberData SIP Paging Amp

Stored Network Settings

Addressing Mode:

Static

DHCP

Hostname:

SipDevice04f7ec

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

DHCP Timeout in seconds:

60

Current Network Settings

IP Address:

10.10.0.151

Subnet Mask:

255.0.0.0

Default Gateway:

10.0.0.1

DNS Server 1:

10.0.1.56

DNS Server 2:

VLAN Settings

VLAN ID (0-4095):

0

VLAN Priority (0-7):

0

Save

Reboot

Toggle Help

Operations Guide

931971A

CyberData Corporation

2. On the **Network** 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. Network Page 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.
DHCP Timeout in seconds ?	Specify the desired time-out duration (in seconds) that the device will wait for a response from the DHCP server before reverting back to the stored static IP address. The stored static IP address may be the last known IP address or the factory default address if no prior DHCP lease was established. Enter up to 8 characters. A value of -1 will retry forever.
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. 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.

Table 2-12. Network Page Parameters (continued)

Web Page Item	Description
<div>Save</div>	<p>Click the Save button to save your configuration settings.</p> <p>Note: You need to reboot for changes to take effect.</p>
<div>Reboot</div>	<p>Click on the Reboot button to reboot the system.</p>
<div>Toggle Help</div>	<p>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.</p>

2.3.8 Configure the SIP (Session Initiation Protocol) Parameters

1. Click on the **SIP** menu button to open the **SIP** page (Figure 2-27).

Figure 2-27. SIP Page—Top

SIP Settings

Enable SIP operation: ☒

Register with a SIP Server: ☒

Buffer SIP Calls: ☐

Primary SIP Server:

Primary SIP User ID:

Primary SIP Auth ID:

Primary SIP Auth Password:

Re-registration Interval (in seconds):

Backup SIP Server 1:

Backup SIP User ID:

Backup SIP Auth ID:

Backup SIP Auth Password:

Re-registration Interval (in seconds):

Backup SIP Server 2:

Backup SIP User ID:

Backup SIP Auth ID:

Backup SIP Auth Password:

Re-registration Interval (in seconds):

Remote SIP Port:

Local SIP Port:

SIP Transport Protocol:

TLS Version:

Verify Server Certificate: ☐

Outbound Proxy:

Outbound Proxy Port:

Use Cisco SRST: ☐

Disable rport Discovery: ☐

Keep Alive Period:

Nightringer Settings

SIP Server:

Remote SIP Port:

Local SIP Port:

Outbound Proxy:

Outbound Proxy Port:

SIP User ID:

SIP Auth ID:

SIP Auth Password:

Re-registration Interval (in seconds):

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:

Audio Codec Selection

Codec:

RTP Settings

RTP Port (even):

Asymmetric RTP: ☐

Jitter Buffer:

RTP Encryption (SRTP):

The strobe settings will only appear if you are using the Strobe Kit. If you are not using the Strobe Kit, you will not see the strobe settings.

Figure 2-28. SIP Page—Bottom

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:

Keep Alive Period: 10000

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

Save Reboot Toggle Help

SIP Ring Strobe Settings

Blink Strobe on Ring:

Scene Brightness Color Red Green Blue

ADA 255 Color 255 255 255 Preview

SIP Call Strobe Settings

Blink Strobe during Call:

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

The strobe settings will only appear if you are using the Strobe Kit. If you are not using the Strobe Kit, you will not see the strobe settings.

2. On the **SIP** 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. SIP Page 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.
Buffer SIP Calls ?	Device will buffer audio and play it back after hang up. Length of the buffer varies with codec.
Primary SIP Server ?	Enter the SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the primary SIP server. This field can accept entries of up to 255 characters in length.
Primary SIP User ID ?	Specify the SIP User ID for the Primary SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the primary SIP server. Enter up to 64 alphanumeric characters.
Primary SIP Auth ID ?	Specify the Authenticate ID for the Primary SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Primary SIP Auth Password ?	Specify the Authenticate Password for the Primary SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Re-registration Interval (in seconds) ?	The SIP Re-registration interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
Backup SIP Server 1 ?	Enter the backup SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the backup SIP server. This field can accept entries of up to 255 characters in length.
Backup SIP User ID 1 ?	Specify the SIP User ID for the first backup SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the first backup SIP server. Enter up to 64 alphanumeric characters.
Backup SIP Auth ID 1 ?	Specify the Authenticate ID for the first backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Auth Password 1 ?	Specify the Authenticate Password for the first backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
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 2 ?	Specify the SIP User ID for the second backup SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the second backup SIP server. Enter up to 64 alphanumeric characters.

Table 2-13. SIP Page Parameters (continued)

Web Page Item	Description
Backup SIP Auth ID 2 ?	Specify the Authenticate ID for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Auth Password 2 ?	Specify the Authenticate Password for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
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.
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.

Table 2-13. SIP Page Parameters (continued)


Web Page Item	Description
SIP Ring Strobe Settings	The following strobe settings will only appear if a CyberData Strobe product is connected to your device. If a CyberData Strobe product is not connected to your device, you will not see the strobe settings.
Blink Strobe on Ring ?	When selected, the Strobe will blink a scene when ringing.
Scene ?	Select desired scene (only one may be chosen).
ADA Compliant ?	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.
Slow Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink ?	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.
Fast Blink ?	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.
Color ?	Select desired color (only one may be chosen).
Brightness ?	How bright the strobe will blink when there is a SIP Ring. This is the maximum brightness for “fade” type scenes.
Red ?	The red LED value for SIP Ring.
Green ?	The green LED value for SIP Ring.
Blue ?	The blue LED value for SIP Ring.
	Use this button to preview the strobe flashing behavior for the SIP Ring Strobe Settings .
SIP Call Strobe Settings	The following strobe settings will only appear if a CyberData Strobe product is connected to your device. If a CyberData Strobe product is not connected to your device, you will not see the strobe settings.
Blink Strobe during Call ?	When selected, the Strobe will blink a scene during a call.
Scene ?	Select desired scene (only one may be chosen).
ADA Compliant ?	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.
Slow Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink ?	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.
Fast Blink ?	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.
Color ?	Select desired color (only one may be chosen).
Brightness ?	How bright the strobe will blink when there is a SIP Call. This is the maximum brightness for “fade” type scenes.
Red ?	The red LED value for SIP Call.

Table 2-13. SIP Page Parameters (continued)



Web Page Item	Description
Green ?	The green LED value for SIP Call.
Blue ?	The blue LED value for SIP Call.
	Use this button to preview the strobe flashing behavior for the SIP Call Strobe Settings .
MWI Strobe Settings	
The following strobe settings will only appear if you are using the Strobe Kit. If you are not using the Strobe Kit, you will not see the strobe settings.	
Blink Strobe on MWI ?	When selected, the strobe will blink a scene when a voicemail is waiting for its extension.
Scene ?	Select desired scene (only one may be chosen).
ADA Compliant ?	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.
Slow Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink ?	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.
Fast Blink ?	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.
MWI Call Color ?	Select desired color (only one may be chosen).
Brightness ?	How bright the strobe will blink when there is a message waiting. This is the maximum brightness for “fade” type scenes.
Red ?	The red LED value for MWI.
Green ?	The green LED value for MWI.
Blue ?	The blue LED value for MWI.
	Use this button to preview the strobe flashing behavior for the MWI Strobe Settings .
Nightringer Settings	
Enable Nightringer ?	When Nightringer is enabled, the device will attempt to register a second extension with the SIP server. Any calls made to this extension will play a ringtone (corresponds to Night Ring on the Audiofiles page). By design, it is not possible to answer a call to the Nightringer extension.
SIP Server ?	Enter the SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's Nightringer extension on the SIP server. This field can accept entries of up to 255 characters in length.
Remote SIP Port ?	The Remote SIP Port is the port number the device will use as the destination port when sending SIP messages for the Nightringer extension. The default Remote SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.

Table 2-13. SIP Page Parameters (continued)





Web Page Item	Description
Local SIP Port ?	The Local SIP Port is the port number the device will use to receive SIP messages for the Nightringer extension. This value cannot be the same as the Local SIP Port for the primary extension. The default Local SIP Port is 5061. The supported range is 0-65536. Enter up to 5 digits.
Outbound Proxy ?	Enter the Outbound Proxy address as an IPv4 address in dotted decimal notation or a fully qualified domain name (FQDN). When an IP address is configured, the device will send all SIP messages to this IP address for the Nightringer extension. When an FQDN is configured, the device will run DNS NAPTR, SRV, and A queries on the FQDN to resolve an IP address to which it will send all SIP messages for the Nightringer extension. This field can accept entries of up to 255 characters in length.
Outbound Proxy Port ?	The Outbound Proxy Port is port number used as the destination port when sending SIP messages to the outbound proxy for the Nightringer extension. A value of 0 will default to 5060. The supported range is 0-65536. Enter up to 5 digits.
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.
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.
Nightringer Strobe Settings	The following strobe settings will only appear if you are using the Strobe Kit. If you are not using the Strobe Kit, you will not see the strobe settings.
Blink Strobe on Nightring ?	When selected, the Strobe will blink a scene when the Nightringer is ringing.
Scene ?	Select desired scene (only one may be chosen).
ADA Compliant ?	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.
Slow Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink ?	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.
Fast Blink ?	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.
Color ?	Select desired color (only one may be chosen).
Brightness ?	How bright the strobe will blink when the Nightringer is ringing. This is the maximum brightness for "fade" type scenes.
Red ?	The red LED value for Nightringer.
Green ?	The green LED value for Nightringer.
Blue ?	The blue LED value for Nightringer.
	Use this button to preview the strobe flashing behavior for the Nightringer Strobe Settings .

Table 2-13. SIP Page Parameters (continued)

Web Page Item	Description
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 ?	<p>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.</p> <p>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.</p> <p>Most installations should not enable asymmetric RTP.</p>
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.
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.
Codec Selection	
Force Selected Codec ?	When configured, this option will allow you to force the device to negotiate for the selected codec. Otherwise, the device will perform codec negotiation using the default list of supported codecs.
Codec ?	Select the desired codec (only one may be chosen).
	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.

Note For specific server configurations, go to the following website address:
<https://www.cyberdata.net/pages/connecting-to-ip-pbx-servers>

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

2.3.8.1 Point-to-Point Configuration

When the device is set to not register with a SIP server (see [Figure 2-29](#)), it is possible for the speaker to receive Point-to-Point calls by setting the dial out extension to the IP address of the remote device. The delayed DTMF functionality is available in Point-to-Point Mode.

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

Figure 2-29. SIP Page Set to Point-to-Point Mode

The screenshot shows the 'SIP' tab in the configuration menu. The 'SIP Settings' section has 'Enable SIP operation' checked and 'Register with a SIP Server' unchecked. A red line points to the 'Register with a SIP Server' checkbox. The 'Nightringer Settings' section includes fields for SIP Server, Remote SIP Port (5060), Local SIP Port (5061), Outbound Proxy, Outbound Proxy Port (0), SIP User ID, SIP Auth ID, SIP Auth Password, and Re-registration Interval (360 seconds). The 'Nightringer Strobe Settings' section has 'Blink Strobe on Nightring' unchecked and a 'Color' dropdown set to 'Blue'.

Home	Device	Audio	Network	SIP	SSL	Multicast	Sensor	Audiofiles	Events	Autoprov	Firmware
<h1>CyberData SIP Paging Amp</h1> <h2>SIP Settings</h2> <p>Enable SIP operation: <input checked="" type="checkbox"/></p> <p>Register with a SIP Server: <input type="checkbox"/></p> <p>Buffer SIP Calls: <input type="checkbox"/></p> <p>Primary SIP Server: 10.0.0.253</p> <p>Primary SIP User ID: 199</p> <p>Primary SIP Auth ID: 199</p> <p>Primary SIP Auth Password: *****</p> <p>Re-registration Interval (in seconds): 360</p> <p>Backup SIP Server 1: Host or IP address</p> <p>Backup SIP User ID: User ID</p> <p>Backup SIP Auth ID: Auth ID</p> <p>Backup SIP Auth Password: Password</p> <p>Re-registration Interval (in seconds): 360</p> <h2>Nightringer Settings</h2> <p>SIP Server: Host or IP address</p> <p>Remote SIP Port: 5060</p> <p>Local SIP Port: 5061</p> <p>Outbound Proxy: Host or IP address</p> <p>Outbound Proxy Port: 0</p> <p>SIP User ID: User ID</p> <p>SIP Auth ID: Auth ID</p> <p>SIP Auth Password: Password</p> <p>Re-registration Interval (in seconds): 360</p> <h2>Nightringer Strobe Settings</h2> <p>Blink Strobe on Nightring: <input type="checkbox"/></p> <p>Scene Brightness Color Red Green Blue</p>											

Device is set to NOT register with a SiP server

2.3.8.2 Delayed DTMF

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

Table 2-14. Examples of Dial-Out Extension Strings

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

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

2.3.9 Configure the SSL Parameters

1. Click **SSL** menu button to open the **SSL** page (Figure 2-30 and Figure 2-31).

Figure 2-30. SSL Configuration Page

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

CyberData SIP Paging Amp

Web Server Certificate

```

subject=
countryName           = US
stateOrProvinceName   = California
localityName          = Monterey
organizationName      = Cyberdata
commonName             = 0020f704f7ec
notBefore=Sep 20 16:03:51 2022 GMT
notAfter=Sep 17 16:03:51 2032 GMT
                    
```

Browse... No file chosen

Import Web Certificate

Restore Web Certificate

SIP Client Certificate

```

subject=
countryName           = US
stateOrProvinceName   = California
localityName          = Monterey
organizationName      = Cyberdata
commonName             = 0020f704f7ec
notBefore=Sep 20 16:03:51 2022 GMT
notAfter=Sep 17 16:03:51 2032 GMT
                    
```

Browse... No file chosen

Import SIP Certificate

Restore SIP Certificate

Password (optional):

Autoprovisioning Client Certificate

```

subject=
countryName           = US
stateOrProvinceName   = California
localityName          = Monterey
organizationName      = Cyberdata
commonName             = 0020f704f7ec
notBefore=Sep 20 16:03:51 2022 GMT
notAfter=Sep 17 16:03:51 2032 GMT
                    
```

Browse... No file chosen

Import Autoprovisioning Certificate

Restore Autoprovisioning Certificate

Password (optional):

Download Cyberdata CA Save Reboot Toggle Help

Test TLS Connection

Server: 10.0.0.253 Port: 5060

Test SIP Connection Test Autoprovisioning Connection

List of Trusted CAs

Upload CA Certificate: Browse... No file chosen

Import CA Certificate Remove All Restore Defaults

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
6	DigiCert_Global_Root_G2.crt	Info	Remove
7	DigiCert_Global_Root_G3.crt	Info	Remove
8	DigiCert_Hiob_Assurance_EV_Root_CA.crt	Info	Remove

Figure 2-31. SSL Configuration Page

4	DigiCert_Assured_ID_Root_G3.crt	Info	Remove
5	DigiCert_Global_Root_CA.crt	Info	Remove
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

2. On the **SSL** 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. SSL Configuration Parameters

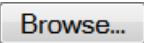


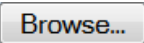


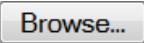
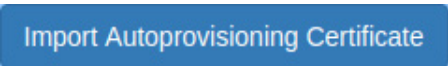



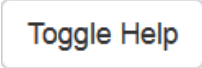

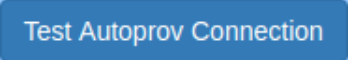
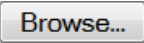




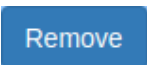
Web Page Item	Description
Web Server Certificate	Certificate used by the web server.
	Click Browse to select a certificate to import.
	After selecting a certificate, click Import Web Certificate to import it as the certificate used by this device's web server.
	Restore the device's default web server 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.
	Click Browse to select a certificate to import.
	After selecting a certificate, click Import SIP Certificate to import it as the certificate used by the device during SIP transactions.
	Restore the device's default sip client certificate. This will remove any user-uploaded sip client certificates (Server CAs and Trusted CAs are unaffected).
Password (optional) ?	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.
	Click Browse to select a certificate to import.
	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 the device's default autoprovisioning certificate. This will remove any user-uploaded autoprovisioning certificates. (Server CAs and Trusted CAs are unaffected).
Password (optional) ?	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.
Download Cyberdata CA ?	Right click and Save Link As... to get the Cyberdata CA used to sign this client certificate.
	Click the Save button to save your configuration settings.

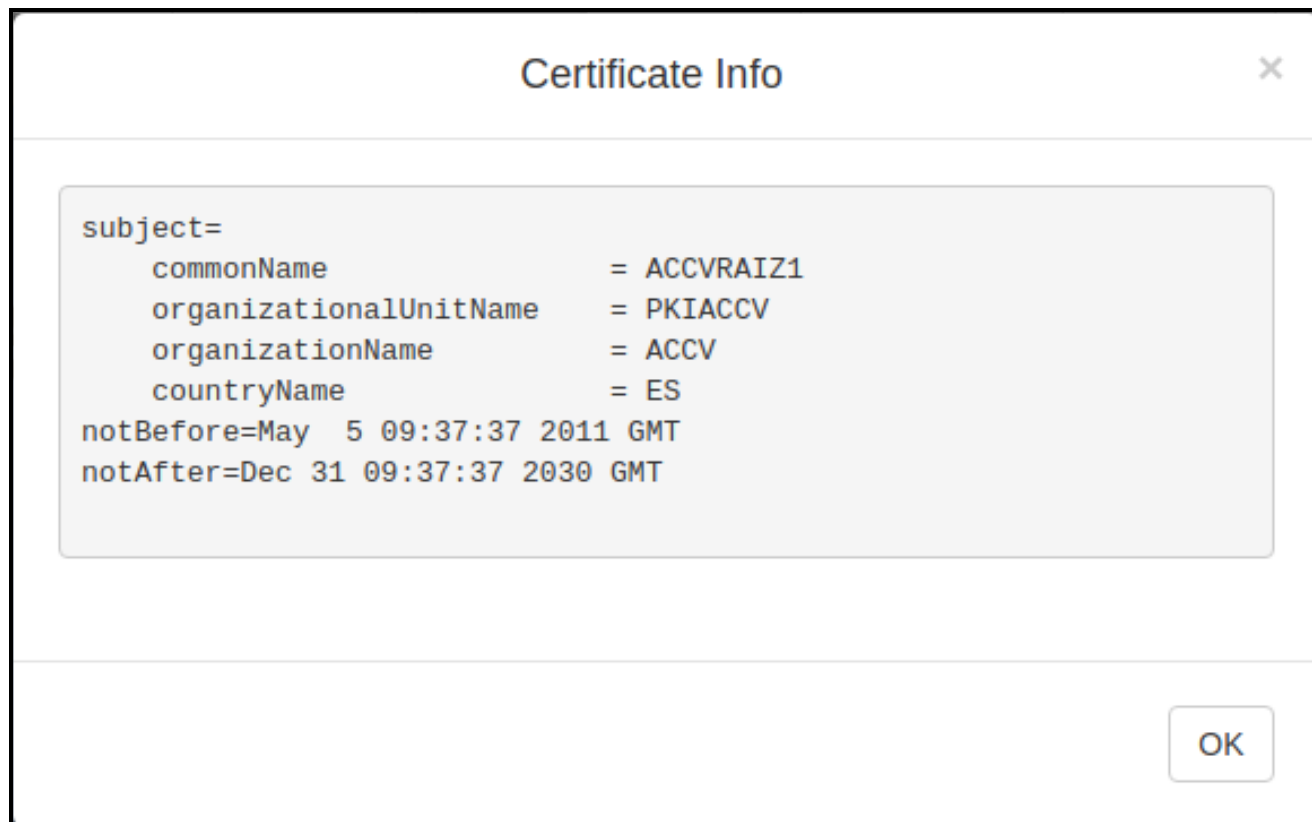
Table 2-15. SSL Configuration Parameters (continued)

Web Page Item	Description
	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.
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.
	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.
	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	
	Use this button to select a configuration file to import.
Upload 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 will restore the default list of registered CAs and Remove All will remove all registered CAs.
	Restore Defaults will restore the default list of registered CAs and Remove All will remove all registered CAs.
	Provides details of the certificate. After clicking on this button, the Certificate Info Window appears. See Section 2.3.9.1, "Certificate Info Window" .
	Removes this certificate from the list of trusted certificates. After clicking on this button, the Remove Server Certificate Window appears. See Section 2.3.9.2, "Remove Server Certificate Window" .

2.3.9.1 Certificate Info Window

The **Certificate Info Window** provides details of the certificate. This window appears after clicking on the **Info** button. See [Figure 2-32](#).

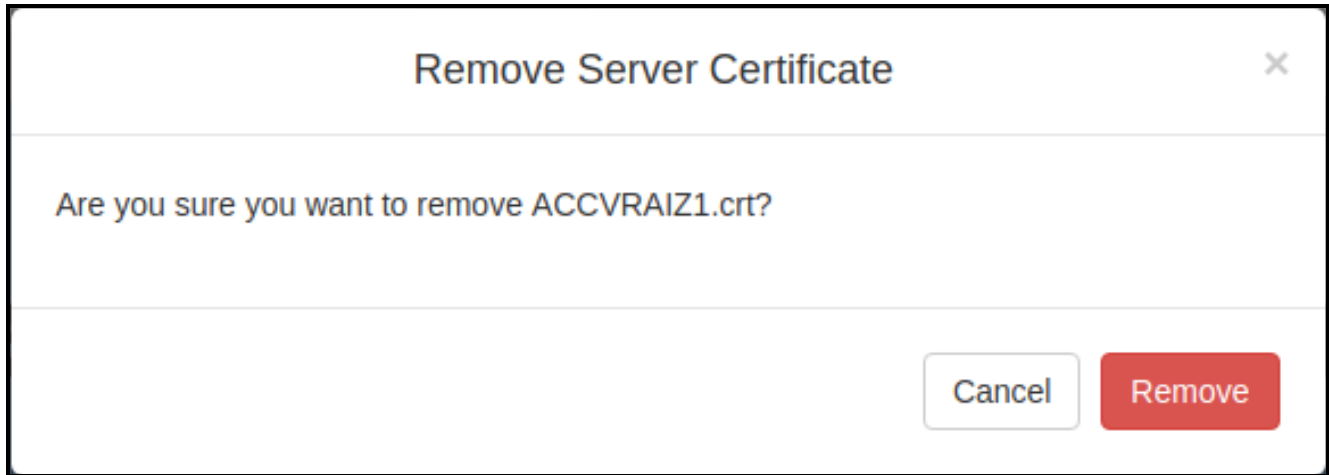
Figure 2-32. Certificate Info Window



2.3.9.2 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 2-33](#).

Figure 2-33. Remove Server Certificate Window



2.3.10 Configure the Multicast Parameters

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

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

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

1. Click on the **Multicast** menu button to open the **Multicast** page. See [Figure 2-34](#).

Figure 2-34. Multicast Page

Home
Device
Audio
Network
SIP
SSL
Multicast
Sensor
Audiofiles
Events
Autoprov
Firmware

CyberData SIP Paging Amp

Multicast Settings

Enable Multicast Operation: ☒

Priority	Address	Port	Name	Buffer	Beep	Relay	Scene	Brightness	Color	Red	Green	Blue	
0	239.168.3.1	2000	Background Music	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Off	255	Color	255	255	255	Preview
1	239.168.3.2	3000	MG1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Slow Fade	180	Color	0	255	0	Preview
2	239.168.3.3	4000	MG2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Slow Blink	35	Color	0	0	255	Preview
3	239.168.3.4	5000	MG3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Slow Fade	255	Color	0	250	60	Preview
4	239.168.3.5	6000	MG4	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Fast Fade	120	Color	255	5	100	Preview
5	239.168.3.6	7000	MG5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ADA	255	Color	255	255	255	Preview
6	239.168.3.7	8000	MG6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Fast Fade	80	Color	255	35	0	Preview
7	239.168.3.8	9000	MG7	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Slow Fade	120	Color	0	250	60	Preview
8	239.168.3.9	10000	MG8	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Fast Blink	255	Color	255	0	0	Preview
9	239.168.3.10	11000	Emergency	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	ADA	255	Color	255	255	255	Preview

Polycom Default Channel
Polycom Priority Channel
Polycom Emergency Channel

1
24
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
Priority 9 streams will play at maximum volume

Save
Reboot

The strobe settings will only appear if you are using the Strobe Kit. If you are not using the Strobe Kit, you will not see the strobe settings.

2. On the **Multicast** 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. 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 2.3.10.1, "Assigning Priority" for more details.
Address	Enter the multicast IP Address for this multicast group (15 character limit).
Port	Enter the port number for this multicast group (5 character limit [range can be from 2000 to 65535]). Note: The multicast ports have to be even values. The webpage will enforce this restriction.
Name	Assign a descriptive name for this multicast group (25 character limit).
Buffer	Device will buffer up to four minutes of audio and then play back the recording after the multicast stream finishes or after the buffer is full.
Beep	When selected, the device will play a beep before multicast audio is sent.
Relay	When selected, the device will activate a relay before multicast audio is sent.
Scene ?	Select desired scene (only one may be chosen). Note: The strobe settings will only appear if you are using the Strobe Kit. If you are not using the Strobe Kit, you will not see the strobe settings.
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.
Brightness ?	How bright the strobe will blink on a multicast page. This is the maximum brightness for "fade" type scenes.
	Select desired color (only one may be chosen).
Red ?	The red LED value for Multicast.
Green ?	The green LED value for Multicast.
Blue ?	The blue LED value for Multicast.
	Use this button to preview the strobe flashing behavior for the Multicast Strobe Settings .

Table 2-16. Multicast Page Parameters (continued)

Web Page Item	Description
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.
	Click the Save button to save your configuration settings.
	Click on the Reboot button to reboot the system.

2.3.10.1 Assigning Priority

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

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

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

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

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

2.3.11 Configure the Sensor Page Parameters

The door sensor (pins 3 and 4) on the terminal block 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 [Sensor Timeout \(seconds\)](#) parameter has been met.

Each sensor can trigger up to three different actions:

- Activate the relay until the sensor is deactivated
- Loop an audio file out of the speaker until the sensor is deactivated
- Call an extension and play a pre-recorded audio file

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 2-35).

Figure 2-35. Sensor Page

HomeDeviceAudioNetworkSIPSSLMulticastSensorAudiofilesEventsAutoprovFirmware

CyberData SIP Paging Amp

Sensor Settings

Sensor Normally Closed:

Yes

No

Sensor Timeout (seconds):

5

Activate Relay:

Make call to extension:

Dial Out Extension:

204

Dial Out ID:

id204

Play Audio Locally:

Repeat Sensor Message:

5

Sensor Strobe Settings

Blink Strobe on Sensor:

Scene

Brightness

Color

Red

Green

Blue

ADA

255

Color

255

255

255

Preview

Save

Reboot

Toggle Help

Test Sensor

The strobe settings will only appear if you are using the Strobe Kit. If you are not using the Strobe Kit, you will not see the strobe settings.





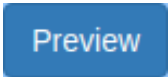


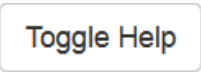


2. On the **Sensor** page, enter values for the parameters indicated in [Table 2-17](#).

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. Sensor Page Parameters

Web Page Item	Description
Sensor Settings	
Sensor Normally Closed ?	Select the inactive state of the sensor. The sensor is also known as the Sense Input on the device's terminal block.
Sensor Timeout (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 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 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 sensor is activated. Enter up to 64 alphanumeric characters.
Dial Out ID ?	An additional Caller identification string added to outbound calls. Enter up to 64 alphanumeric characters.
Play Audio Locally ?	When selected, the device will loop an audio file out of the speaker until the sensor is deactivated.
Repeat Sensor Message ?	The number of times to repeat the audio message through the local speaker or to the remote endpoint. A value of 0 will repeat the message while the sensor is active. 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.
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.
Brightness ?	How bright the strobe will blink when the sensor is triggered. This is the maximum brightness for "fade" type scenes.

Table 2-17. Sensor Page Parameters (continued)

Web Page Item	Description
	Select desired color (only one may be chosen).
Red 	The red LED value for Sensor.
Green 	The green LED value for Sensor.
Blue 	The blue LED value for Sensor.
	Use this button to preview the strobe flashing behavior for the Sensor Strobe Settings .
	Click the Save button to save your configuration settings. Note: You need to reboot for changes to take effect.
	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.
	Click the Test Sensor button to test the sensor.

2.3.12 Configure the Audiofiles Page Parameters

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

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

Figure 2-36. Audiofiles Page

Home	Device	Audio	Network	SIP	SSL	Multicast	Sensor	Audiofiles	Events	Autopro	Firmware
<h2>CyberData SIP Paging Amp</h2>											
Available Space: 1380MB											
<h3>Audio Files</h3>											
0:	Currently set to:	default	Browse...	No file chosen	Play	Delete	Save				
1:	Currently set to:	default	Browse...	No file chosen	Play	Delete	Save				
2:	Currently set to:	default	Browse...	No file chosen	Play	Delete	Save				
3:	Currently set to:	default	Browse...	No file chosen	Play	Delete	Save				
4:	Currently set to:	default	Browse...	No file chosen	Play	Delete	Save				
5:	Currently set to:	default	Browse...	No file chosen	Play	Delete	Save				
6:	Currently set to:	default	Browse...	No file chosen	Play	Delete	Save				
7:	Currently set to:	default	Browse...	No file chosen	Play	Delete	Save				
8:	Currently set to:	default	Browse...	No file chosen	Play	Delete	Save				
9:	Currently set to:	default	Browse...	No file chosen	Play	Delete	Save				
Audio Test:	Currently set to:	default	Browse...	No file chosen	Play	Delete	Save				
Dot:	Currently set to:	default	Browse...	No file chosen	Play	Delete	Save				
Night Ring:	Currently set to:	default	Browse...	No file chosen	Play	Delete	Save				
Page Tone:	Currently set to:	default	Browse...	No file chosen	Play	Delete	Save				
Rebooting:	Currently set to:	default	Browse...	No file chosen	Play	Delete	Save				
Restoring Default:	Currently set to:	default	Browse...	No file chosen	Play	Delete	Save				
Ring Tone:	Currently set to:	default	Browse...	No file chosen	Play	Delete	Save				
Sensor Triggered:	Currently set to:	default	Browse...	No file chosen	Play	Delete	Save				
Stored Message File Not Found:	Currently set to:	default	Browse...	No file chosen	Play	Delete	Save				
Your IP Address Is:	Currently set to:	default	Browse...	No file chosen	Play	Delete	Save				
<h3>Menu Audio Files</h3>											

Figure 2-37. Audiofiles Page

Ring Tone:	Currently set to:	default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Sensor Triggered:	Currently set to:	default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Stored Message File Not Found:	Currently set to:	default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Your IP Address Is:	Currently set to:	default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>

Menu Audio Files

Cancel:	Currently set to:	default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Currently Playing:	Currently set to:	default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Invalid Entry:	Currently set to:	default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Page:	Currently set to:	default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Play Stored Message:	Currently set to:	default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Pound (#):	Currently set to:	default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Press:	Currently set to:	default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Through:	Currently set to:	default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
To:	Currently set to:	default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Enter Security Code Followed by Pound (#) key:	Currently set to:	default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>

Stored Messages

Stored Message 1:	Currently set to:	default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>	Repeat: <input type="text" value="0"/>	Infinite: <input type="checkbox"/>
Stored Message 2:	Currently set to:	default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>	Repeat: <input type="text" value="0"/>	Infinite: <input type="checkbox"/>
Stored Message 3:	Currently set to:	default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>	Repeat: <input type="text" value="0"/>	Infinite: <input type="checkbox"/>
Stored Message 4:	Currently set to:	default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>	Repeat: <input type="text" value="0"/>	Infinite: <input type="checkbox"/>
Stored Message 5:	Currently set to:	default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>	Repeat: <input type="text" value="0"/>	Infinite: <input type="checkbox"/>
Stored Message 6:	Currently set to:	default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>	Repeat: <input type="text" value="0"/>	Infinite: <input type="checkbox"/>
Stored Message 7:	Currently set to:	default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>	Repeat: <input type="text" value="0"/>	Infinite: <input type="checkbox"/>
Stored Message 8:	Currently set to:	default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>	Repeat: <input type="text" value="0"/>	Infinite: <input type="checkbox"/>
Stored Message 9:	Currently set to:	default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>	Repeat: <input type="text" value="0"/>	Infinite: <input type="checkbox"/>

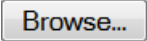

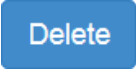

2. On the **Audiofiles** page, enter values for the parameters indicated in [Table 2-18](#).

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

Table 2-18. Audiofiles Page Parameters

Web Page Item	Description
Available Space	Shows the space available for the user to save custom audio files.
Audio Files	
0-9	The name of the audio configuration option is the same as the spoken audio that plays on the board (24 character limit). '0' corresponds to the spoken word "zero." '1' corresponds to the spoken word "one." '2' corresponds to the spoken word "two." '3' corresponds to the spoken word "three." '4' corresponds to the spoken word "four." '5' corresponds to the spoken word "five." '6' corresponds to the spoken word "six." '7' corresponds to the spoken word "seven." '8' corresponds to the spoken word "eight." '9' corresponds to the spoken word "nine."
Audio Test	Corresponds to the message "This is the CyberData IP speaker test message..." (24 character limit).
Dot	Corresponds to the spoken word "dot." (24 character limit).
Night Ring	Specifies the ringtone for nightring. By default this parameter uses the same audio file that is selected for the Ring Tone parameter.
Page Tone	Corresponds to a simple tone that is unused by default (24 character limit).
Rebooting	Corresponds to the spoken word "Rebooting" (24 character limit).
Restoring Default	Corresponds to the message "Restoring default" (24 character limit).
Ring Tone	Specifies the Ring Tone.
Sensor Triggered	Corresponds to the message "Sensor Triggered." (24 character limit).
Stored Message File Not Found	Corresponds to the message "Stored Message File Not Found."
Your IP Address is	Corresponds to the message "Your IP address is..." (24 character limit).
Menu Audio Files	
Menu Audio Files are user-uploadable messages that create the audio menu played to the caller.	
Cancel	Corresponds to the word "Cancel" used in the audio menu played to the caller. (24 character limit).
Currently Playing	Corresponds to the words "Currently Playing" used in the audio menu played to the caller. (24 character limit).
Invalid Entry	Corresponds to the words "Invalid Entry" used in the audio menu played to the caller. (24 character limit).
Page	Corresponds to the word "Page" used in the audio menu played to the caller. (24 character limit).

Table 2-18. Audiofiles Page Parameters (continued)

Web Page Item	Description
Play Stored Message	Corresponds to the words "Play Stored Message" used in the audio menu played to the caller. (24 character limit).
Pound (#)	Corresponds to whatever word or phrase the user wishes to call the pound key in the audio menu played to the caller (24 character limit).
Press	Corresponds to the word "Press" used in the audio menu played to the caller. (24 character limit).
Stored Message	Corresponds to the words "Stored Message" used in the audio menu played to the caller. (24 character limit).
Through	Corresponds to the word "Through" used in the audio menu played to the caller. (24 character limit).
To	Corresponds to the word "To" used in the audio menu played to the caller. (24 character limit).
Enter Security Code Followed by Pound (#) key	Corresponds to the words "Enter Security Code Followed by Pound (#) key" used in the audio menu played to the caller. (24 character limit).
Stored Messages	
Stored Message 1 through 9	<p>Stored Message 1 corresponds to the message played after pressing 1 on a phone keypad.</p> <p>Stored Message 2 corresponds to the message played after pressing 2 on a phone keypad.</p> <p>Stored Message 3 corresponds to the message played after pressing 3 on a phone keypad.</p> <p>Stored Message 4 corresponds to the message played after pressing 4 on a phone keypad.</p> <p>Stored Message 5 corresponds to the message played after pressing 5 on a phone keypad.</p> <p>Stored Message 6 corresponds to the message played after pressing 6 on a phone keypad.</p> <p>Stored Message 7 corresponds to the message played after pressing 7 on a phone keypad.</p> <p>Stored Message 8 corresponds to the message played after pressing 8 on a phone keypad.</p> <p>Stored Message 9 corresponds to the message played after pressing 9 on a phone keypad.</p>
	Click on the Browse button to navigate to and select an audio file.
	The Play button will play that audio file.
	The Delete button will delete any user uploaded audio and restore the stock audio file.
	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.

2.3.12.1 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 2-38](#) through [Figure 2-40](#).

Figure 2-38. Audacity 1

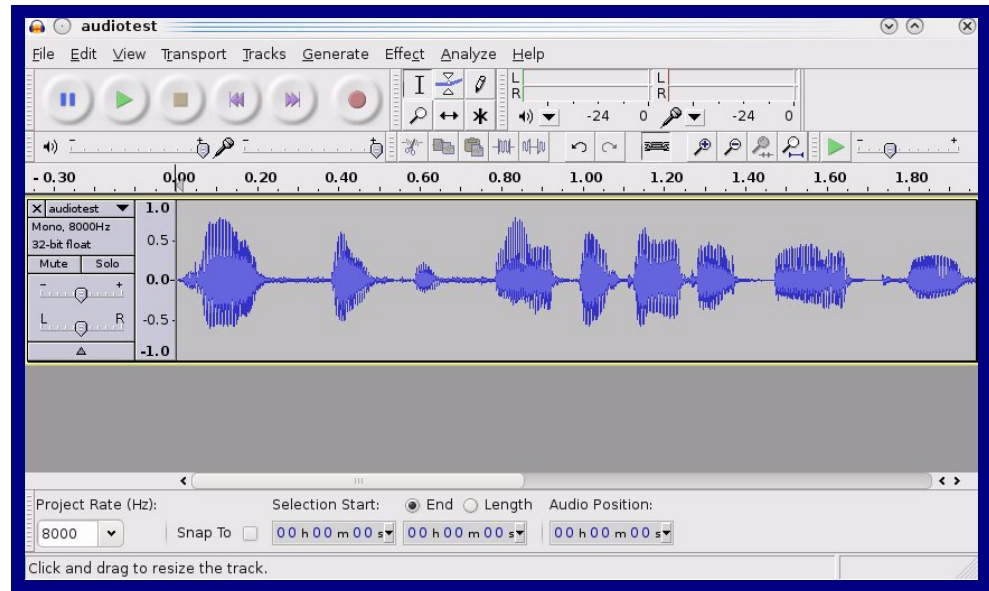
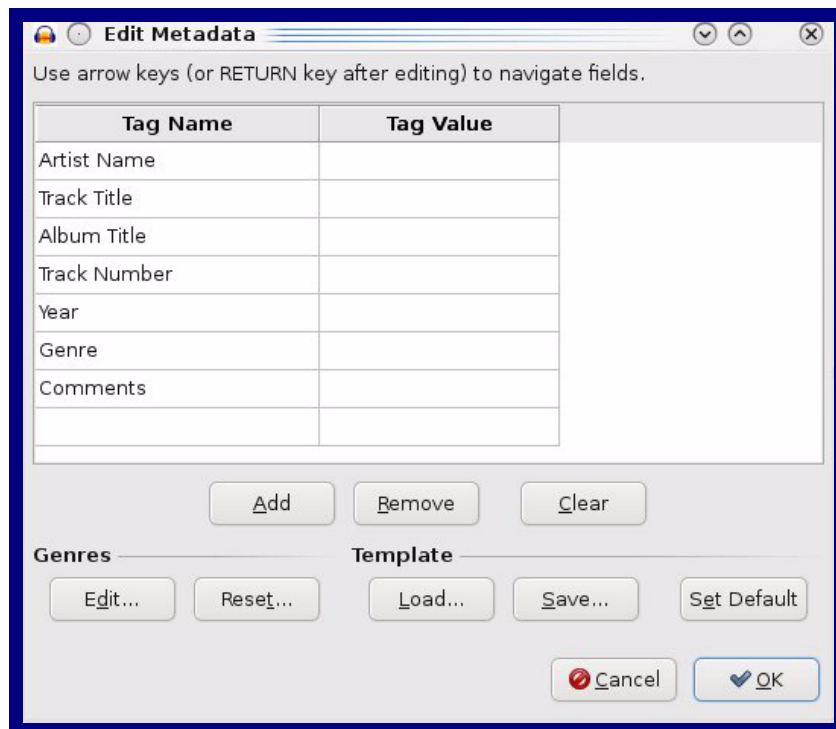


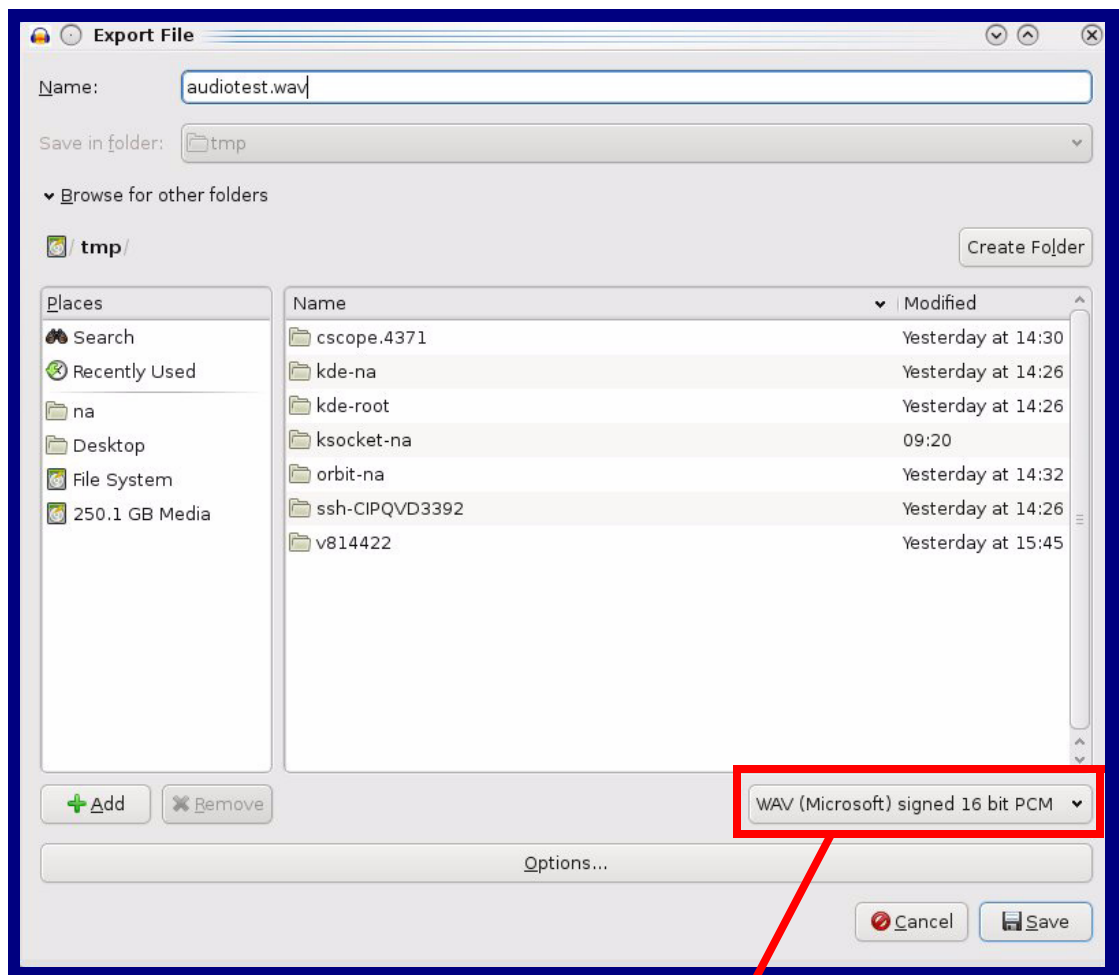
Figure 2-39. Audacity 2



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

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

Figure 2-40. WAV (Microsoft) signed 16 bit PCM



WAV (Microsoft) signed 16 bit PCM

2.3.13 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 2-41).

Figure 2-41. Event Page



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

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

Table 2-19. Events Page 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 Call Start Events ?	When selected, the device will report the start of a SIP call.
Enable Call Terminated Events ?	When selected, the device will report the end of a SIP call.
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 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 Power On Events ?	When selected, the device will report when it boots.
Enable Multicast Start Events ?	When selected, the device will report when the device starts playing a multicast audio stream.
Enable Multicast Stop Events ?	When selected, the device will report when the device stops playing a multicast audio stream.
Enable 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.
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.

2.3.13.1 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 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 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 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 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 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 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 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 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 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 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 Device' MAC='0020f70015b6'>
<event>NIGHTRINGING</event>
</cyberdata>
```

2.3.14 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 2-42](#).

Figure 2-42. Autoprovisioning Page

Home Device Audio Network SIP SSL Multicast Sensor Audiofiles Events Autoprov Firmware

CyberData SIP Paging Amp

Enable Autoprovisioning: ☒

Autoprovisioning Server:

Autoprovisioning Filename:

Use tftp: ☐

Verify Server Certificate: ☐

Username:

Password:

Autoprovisioning autoupdate (in minutes):

Autoprovision at time (HHMM):

Autoprovision when idle (in minutes > 10):

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

Autoprovisioning happens on boot.

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

If these haven't been configured, it will look for an autoprovisioning server in your list of DHCP options and try to download '0020f704f7ec.xml' and if this fails, '000000cd.xml'.

Save Reboot Toggle Help

Download Template

Autoprovisioning log

```
2022-09-30 12:55:37 Autoprov: no autoprov triggers. Exiting...
2022-09-30 12:55:38 Autoprovisioning on boot
2022-09-30 12:55:39 Autoprov found server='http://10.0.0.242' in dhcp option 43
2022-09-30 12:55:39 Autoprov looking for 0020f704f7ec.xml at http://10.0.0.242
2022-09-30 12:55:39 Autoprov downloading http://10.0.0.242/0020f704f7ec.xml
2022-09-30 12:55:39 Got autoprov file. Parsing "0020f704f7ec.xml"
2022-09-30 12:55:39 Autoprov: Processing ssl certificates
2022-09-30 12:55:39 No certificate elements in SSLCertificates
2022-09-30 12:55:39 Autoprov: Processing audio files
2022-09-30 12:55:39 Autoprov found server='10.0.1.118' in dhcp option 72
```





2. On the **Autoprovisioning** page, you may enter values for the parameters indicated in [Table 2-20](#).

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

Table 2-20. Autoprovisioning Page Parameters

Web Page Item	Description
Enable Autoprovisioning ?	The device will automatically fetch a configuration file, also known as the 'autoprovisioning file', based on the configured settings below.
Autoprovisioning Server ?	Enter the IPv4 address of the provisioning server in dotted decimal notation.
Autoprovisioning Filename ?	<p>The autoprovisioning filename is the configuration filename. The default autoprovisioning filename is in the format of <mac address>.xml.</p> <p>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.</p> <p>A file may have any name with an xml extension. If a file name is entered, the device will look for the specified file name, and only that file.</p>
Use tftp ?	The device will use TFTP (instead of http) to download autoprovisioning files.
Verify Server Certificate ?	When using ssl to download autoprovisioning files, reject connections where the server address doesn't match the server certificate's common name.
Username ?	The username used to authenticate with an autoprovisioning server. Leave this field blank to disable authentication.
Password ?	The password used to authenticate with an autoprovisioning server. Leave this field blank to disable authentication.
Autoprovisioning Autoupdate (in minutes) ?	<p>The reoccurring time (in minutes) the device will wait before checking for new autoprovisioning files. Enter up to 6 digits. A value of 0 will disable this option.</p> <p>Note: To use the auto update options, make sure that the Enable NTP setting on the Device Page page is selected (see Table 2-10).</p>
Autoprovision at time (HHMMSS) ?	<p>The time of day the device will check for a new autoprovisioning file. The time must be 6 characters in length and in HHMMSS format. An empty value will disable this option.</p> <p>Note: To use the auto update options, make sure that the Enable NTP setting on the Device Page page is selected (see Table 2-10).</p>
Autoprovision when idle (in minutes > 10) ?	<p>The idle time (in minutes greater than 10) after which the device will check for a new autoprovisioning file. Enter up to 6 digits. A value of 0 will disable this option.</p> <p>Note: To use the auto update options, make sure that the Enable NTP setting on the Device Page page is selected (see Table 2-10).</p>

Table 2-20. Autoprovisioning Page Parameters (continued)

Web Page Item	Description
	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.
	Press the Download Template button to create an autoprovisioning file for the device. See Section 2.3.14.3, "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).

2.3.14.1 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 2.3.14.2, "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 2-20](#)). 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
Device</DeviceName>
<!--      <AutprovFile>common.xml</AutprovFile>-->
<!--      <AutprovFile>sip_reg[macaddress].xml</AutprovFile>-->
<!--      <AutprovFile>audio[macaddress]</AutprovFile>-->
<!--      <AutprovFile>device[macaddress].xml</AutprovFile>-->
</MiscSettings>
```

After downloading the first autoprovisioning file, the device will step through up to twenty additional <AutprovFile> 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 2-21. Autoprovisioning File Name

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

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

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

For example:

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

The autoprovisioning filename is set to “cyberdata/”

On boot, the device will try to download:

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

...and if this fails:

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

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

```

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

```

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

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

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

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

The list of valid product strings:

```

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

```

Autoprovisioning
Example 1

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

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

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

000000cd.xml

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

sip_common.xml

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

sip_0020f7020001.xml

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

sip_0020f7020002.xml

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

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

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

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

Autoprovisioning Example 2

Here is another example of setting up your autoprovisioning files:

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

0020f7020001.xml

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

0020f7020002.xml

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

common_settings.xml

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

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

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

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

XML Files

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

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

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

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

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

From the common file, a pointer to sip_common.xml

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

Autoprovisioned Audio Files

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

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

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

2.3.14.2 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; }
```

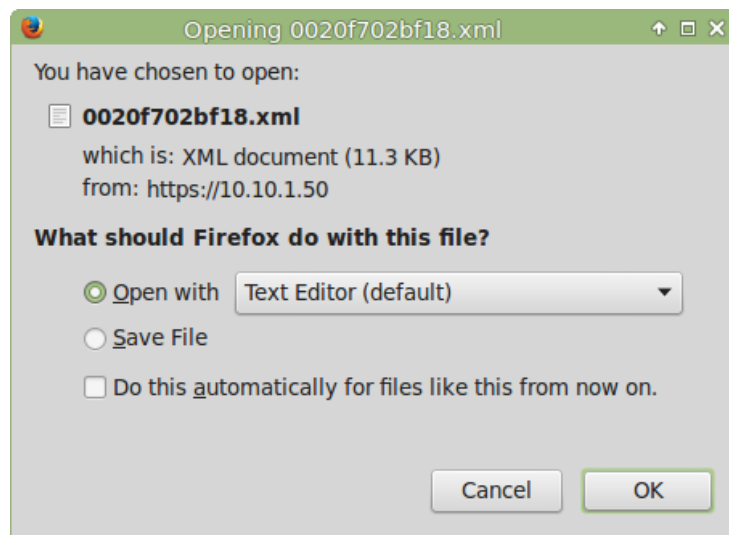

2.3.14.3 Download Template Button

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 2-43](#)). 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 2-43](#).

Figure 2-43. Configuration File



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

2.4 Upgrade the Firmware and Reboot the SIP Paging Amplifier

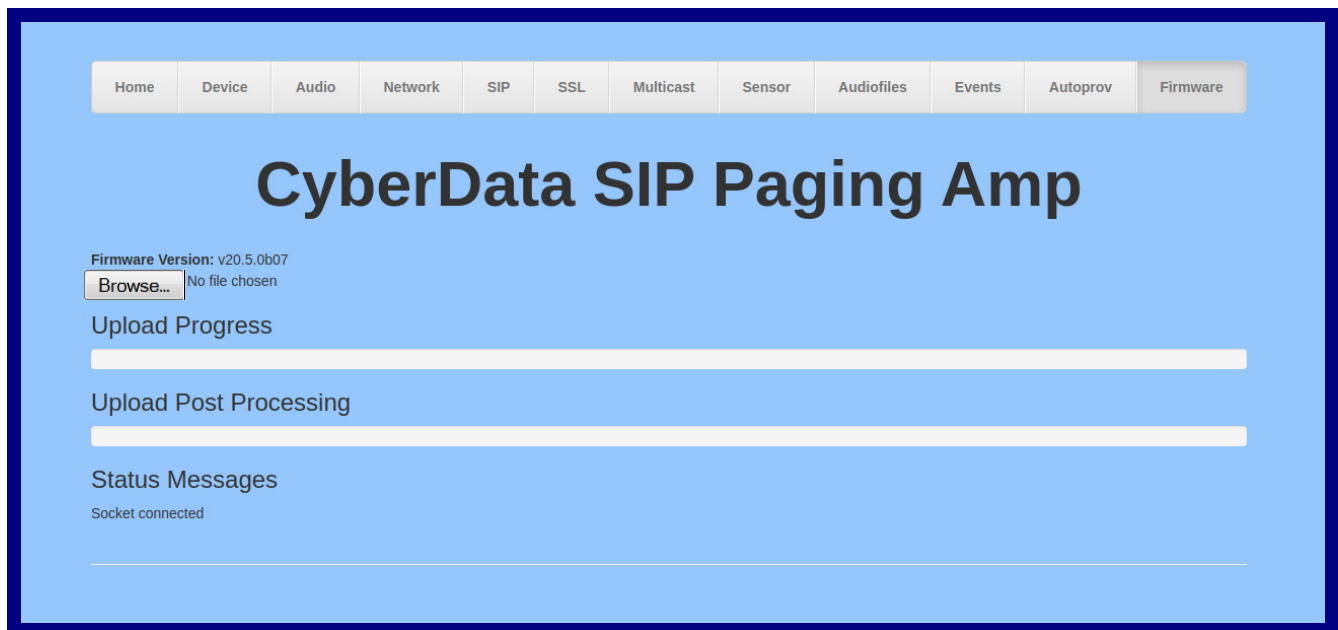
2.4.1 Downloading the Firmware

To download the firmware to your computer:

1. Download the latest firmware file from the **Downloads** tab at the following webpage:
<https://www.cyberdata.net/products/011324>
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 Home Page"](#).
4. Click on the **Firmware** menu button to open the **Firmware** page ([Figure 2-44](#)).

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

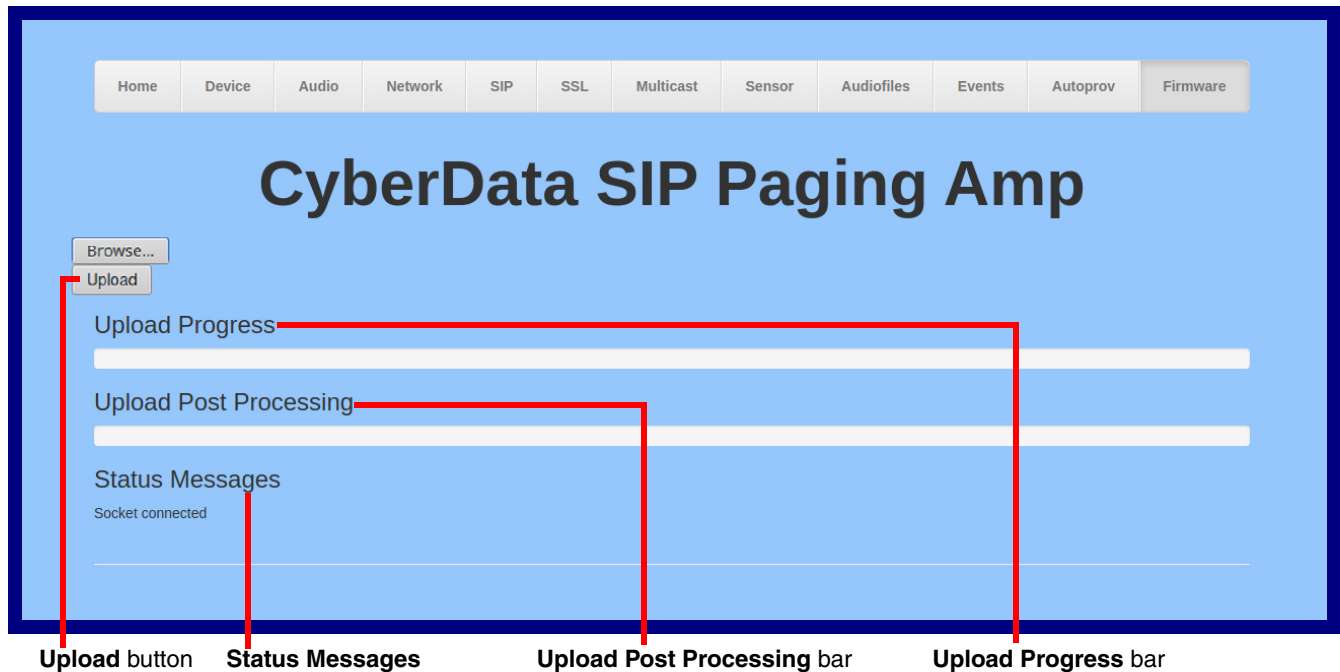
Figure 2-44. Firmware Page



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

6. Select the firmware file. This reveals the **Upload** button (Figure 2-45).

Figure 2-45. Upload Button



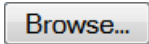
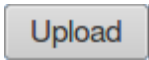
7. Click on the **Upload** button. After selecting the **Upload** button, you will see the progress of the upload in the **Upload Progress** bar.
8. When the upload is complete, you will see the words **Upload finished** under **Status Messages**.
9. At this point, you will see the progress of the upload's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

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

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

Table 2-22 shows the web page items on the **Firmware** page.

Table 2-22. Firmware Page Parameters

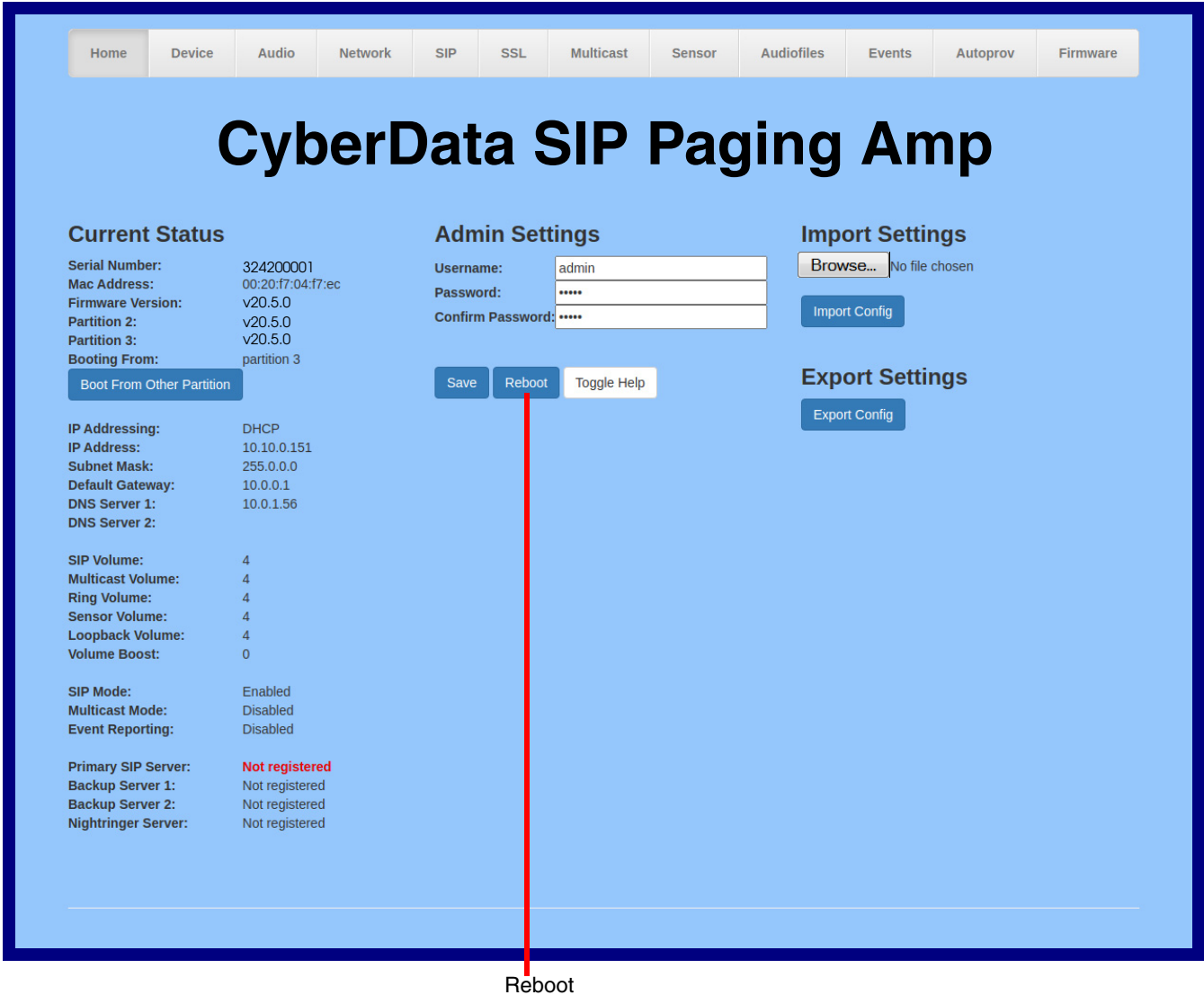
Web Page Item	Description
	Use the Browse button to navigate to the location of the firmware file that you want to upload.
	Click on the Upload button to automatically upload the selected firmware and reboot the system. Note: This button only appears after the user has selected a firmware file.
Upload 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.

2.4.2 Reboot the Device

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

1. Click on the **Reboot** button on the **Home** page ([Figure 2-46](#)). A normal restart will occur.

Figure 2-46. Home Page



2.5 Command Interface

Some functions on the device can be activated using simple POST commands to the web interface. The examples in [Table 2-23](#) use the free unix utility, **wget**, but any program that can send http POST commands to the device should work.

2.5.1 Command Interface Post Commands

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

Table 2-23. Command Interface Post Commands

Device Action	HTTP Post Command ^a
Reboot	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.247/command" --post-data "request=reboot"
Place call to extension (example: extension 600)	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.247/command" --post-data "request=call&extension=600"
Terminate a call	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.247/command" --post-data "request=terminate"
Speak IP Address	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.247/command" --post-data "request=speak_ip_address"
Test Audio	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.247/command" --post-data "request=test_audio"
Swap Boot partitions	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.10.1.81/command" --post-data "request=swap_boot_partition"

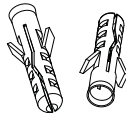
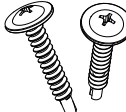
a.Type and enter all of each http POST command on one line.

Appendix A: Mounting the Amplifier

A.1 Mount the Amplifier

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

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

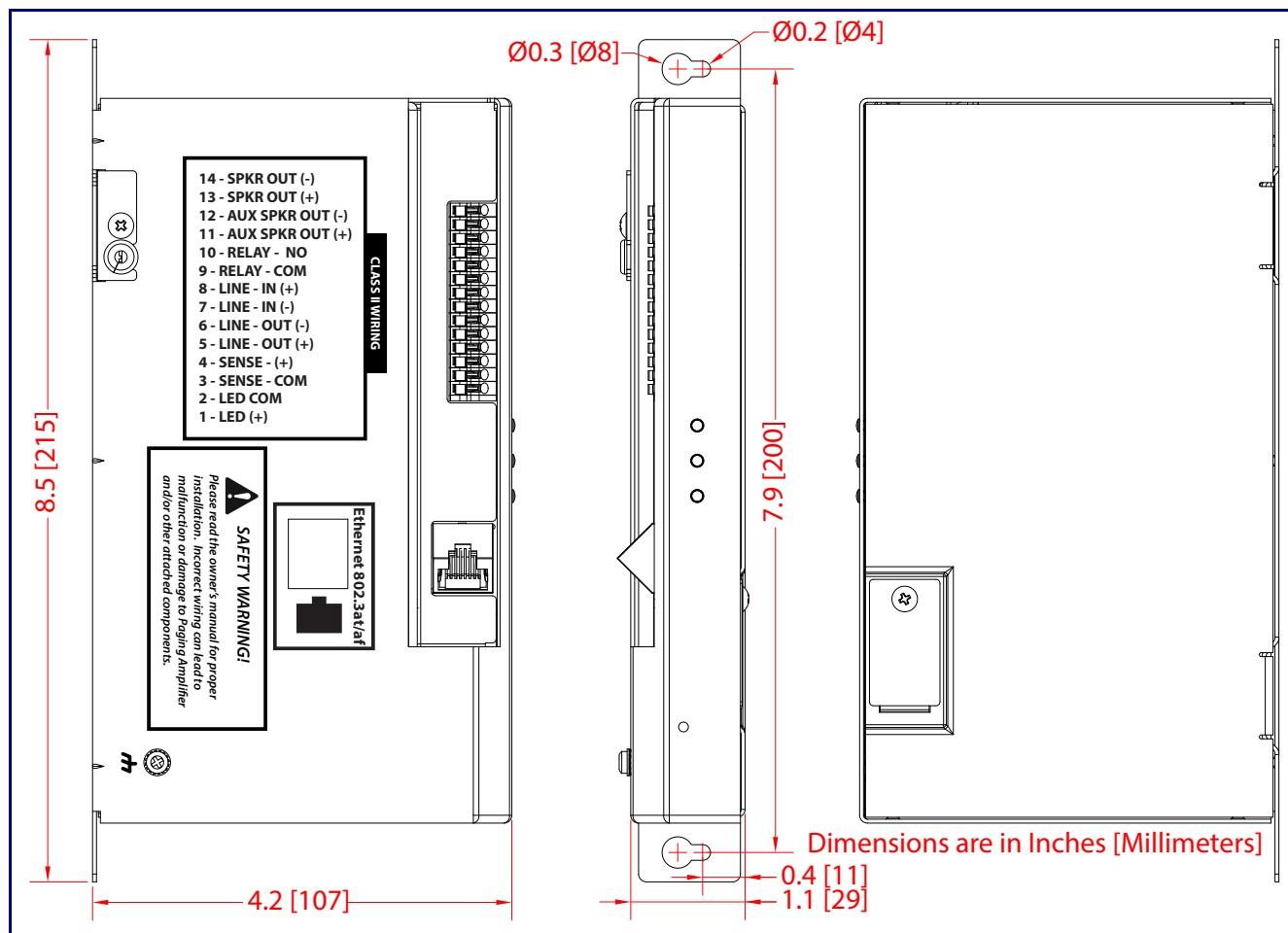
Quantity	Part Name	Illustration
2	Plastic Ribbed Anchors	
2	Size 8 x 1-inch Extra-Wide Rounded Head Drilling Screws	

Note The SIP Paging Amplifier was designed for indoor use. Mounting it on the external part of a building will require additional hardware for weatherproofing, cabling access, and lightning suppression. Consult a certified electrician for details.

Note For mounting, use the two Size 8 Extra-Wide Round Head Self-Tapping Screws to secure the enclosure.

A.2 Dimensions

Figure A-1. Dimensions



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/011324>

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/011324>

B.3 Contact Information

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

B.4 Warranty and RMA Information

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

<https://support.cyberdata.net/>

Index

Numerics

1 speaker configuration 12, 13, 14
 2 speaker configuration 14
 802.3af mode 12, 13, 14
 802.3at compliance switch 12, 13, 14
 802.3at mode 14
 802.3at power injector (high power mode) 12, 13, 14

A

activate relay (door sensor) 62
 activity LED 22
 address, configuration login 28
 amplified outputs 12, 13, 14
 high power mode 14
 how to use and connect 12
 low power mode 12, 13
 announcing an IP address 23
 audio configuration 64
 night ring tone parameter 66
 audio encodings 4
 audio files, user-created 68
 audio page 64
 audio test 23
 autoprovision at time (HHMMSS) 76
 autoprovision when idle (in minutes > 10) 76
 autoprovisioning 77
 download template button 77
 autoprovisioning autoupdate (in minutes) 76
 autoprovisioning configuration 75, 76
 autoprovisioning filename 76
 autoprovisioning server (IP Address) 76

B

backup SIP server 1 42
 backup SIP server 2 42
 backup SIP servers, SIP server
 backups 42

C

cabling 21
 changing
 the web access password 32

Cisco SRST 43
 command interface 91
 commands 91
 configurable parameters 42
 configuration
 audio 64
 default IP settings 24
 door sensor 50, 60
 intrusion sensor 50, 60
 network 37
 SIP 40
 configuration home page 28
 connecting the amplified outputs 12
 connection options 15
 connections 15
 contact information 95
 contact information for CyberData 95
 current network settings 38
 CyberData contact information 95

D

default
 web login username and password 28
 default gateway 38
 default IP settings 24
 default login address 28
 device configuration 32
 device configuration page 32, 35
 device configuration parameters 33
 device configuration password
 changing for web configuration access 32
 DHCP Client 4
 dial out extension (door sensor) 62
 dial out extension strings 47
 dial-out extension strings 49
 dimensions 5, 93
 discovery utility program 28
 distortion, total harmonic 5
 DNS server 38
 door sensor 60, 66
 activate relay 62
 dial out extension 62
 door sensor normally closed 62
 play audio locally 62
 download autoprovisioning template button 77
 DTMF tones 49
 DTMF tones (using rfc2833) 47

E

- enable night ring events 71
- enclosure, mounting 92
- ethernet I/F 5
- event configuration
 - enable night ring events 71
- expiration time for SIP server lease 42, 43, 46
- export settings 30, 31

F

- factory defaults 11, 23
- firmware
 - where to get the latest firmware 87

G

- get autoprovisioning template 77

H

- harmonic distortion 5
- hazard levels 5
- high power mode (amplified outputs) 14
- home page 28
- http POST command 91
- http web-based configuration 4

I

- identifying your product 1
- illustration of amplifier mounting process 92
- import settings 30, 31
- import/export settings 30, 31
- input specifications 5
- installation 2
- IP address 38
- IP address announcement 23
- IP address confirmation 23

L

- lease, SIP server expiration time 42, 43, 46
- LEDs 22
- lengthy pages 59

- line input specifications 5
- line output specifications 5
- local SIP port 43
- log in address 28
- loudspeaker type 21
- loudspeaker, cabling/wiring 21
- low power mode (amplified outputs) 12, 13

M

- MGROUP
 - MGROUP Name 58
- mounting an amplifier 92
- multicast configuration 50, 64
- Multicast IP Address 58

N

- navigation (web page) 25
- navigation table 25
- network configuration 37
- network link activity, verifying 22
- nightring tones 59
- Nightringer 86
- nightringer settings 45
- NTP server 33

O

- on-board relay 5
- one speaker configuration 12, 13, 14
- optional two speaker configuration 14
- output impedance 5
- output level 5
- output signal amplitudes 5
- output specifications 5

P

- packet time 4
- pages (lengthy) 59
- parts list 9
- password
 - for SIP server login 42
 - login 28
- payload types 5
- play audio locally (door sensor) 62
- point-to-point configuration 48
- polycom default channel 59

- polycom emergency channel 59
- polycom priority channel 59
- port
 - local SIP 43
 - remote SIP 43
- POST command 91
- power input 5
- power LED 11, 22
- power, connecting to paging amplifier 12
- priority
 - assigning 59
- product
 - mounting 92
 - parts list 9
- product features 3
- product overview
 - product features 3
 - product specifications 5
 - supported protocols 4
 - supported SIP servers 4
 - typical system installation 2
- product specifications 5
- protocols supported 4

R

- reboot 89, 90
- remote SIP port 43
- reset test function management switch 23
- resetting the IP address to the default 92
- restoring the factory defaults 11, 23
- ringtones 59
 - lengthy pages 59
- rport discovery setting, disabling 43
- RTFM switch 11, 23
- RTP/AVP 4

S

- safety instructions 4
- sales 95
- sensor
 - sensor normally closed 62
 - sensor timeout 62
- sensor connection 16
- sensor setup page 50, 61
- sensor setup parameters 50, 60
- sensors 62
- server address, SIP 42
- service 95
- SIP
 - enable SIP operation 42, 43

- local SIP port 43
 - user ID 42
- SIP (session initiation protocol) 4
- SIP configuration 40
- SIP configuration parameters
 - outbound proxy 43, 46
 - registration and expiration, SIP server lease 42, 43, 46
 - user ID, SIP 42
- SIP registration 42
- SIP remote SIP port 43
- SIP server 42
 - password for login 42
 - SIP servers supported 4
 - user ID for login 42
- SIP server configuration 42
- SIP volume 36
- Size 8 Extra-Wide Round Head Self-Tapping Screws 92
- speaker cable 21
- speaker configuration 12, 13, 14
- speaker configuration for two speakers 14
- speaker wire 21
- SRST 43
- standard 1 speaker configuration 12, 13, 14
- status LED 11, 22
- subnet mask 38
- supported protocols 4

T

- tech support 95
- technical support, contact information 95
- test audio 23
- TFTP server 4
- two speaker configuration 14

U

- user ID
 - for SIP server login 42
- username
 - changing for web configuration access 32
 - default for web configuration access 28
- using the amplified outputs 12

V

- verifying
 - network link and activity 22
 - power on 22
- VLAN ID 38

- VLAN Priority 38
- VLAN tagging support 38
- VLAN tags 38
- volume
 - multicast volume 36
 - sensor volume 36
 - SIP volume 36

W

- warranty policy at CyberData 95
- web configuration log in address 28
- web page
 - navigation 25
- web page navigation 25
- wget, free unix utility 91
- wiring 21