CyberData

The IP Endpoint Company

InformaCast Enabled Loudspeaker Amplifier (PoE) Operations Guide

Part #*011407*

Document Part #*931277J*
for Firmware Version *12.1.0*

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

Operations Guide 931277J
Part # 011407

CyberData
The IP Endpoint Company

Technical Support

The fastest way to get technical support for your VoIP product is to submit a VoIP Technical Support form at the following website:
http://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 931277J, which corresponds to firmware version 12.1.0, was released on August 22, 2019 and has the following changes:

- Updates Figure 1-2, "Typical Installation"
- Updates Section 1.3, "Features" to add TLS 1.2 and SRTP enhanced security for IP endpoints in a local or cloud-based environment
- Updates Section 1.4, "Supported Protocols" to add SRTP
- Updates Table 1-1, "Specifications"
- Updates Figure 2-29, "SIP Page—Top"
- Updates Figure 2-30, "SIP Page—Bottom"
- Updates Table 2-16, "SIP Page Parameters" to add the SRTP setting

Browsers Supported

The following browsers have been tested against firmware version 12.1.0:

- Chrome (version 78.0.3904.70)
- Firefox (version 72.0.2)
- Microsoft Edge (80.0.361.50)
- Internet Explorer (version: 11)

Pictorial Alert Icons

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

Hazard Levels

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

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

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

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

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

Important Safety Instructions

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

Warning

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

Warning

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

Warning

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

Abbreviations and Terms

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

Contents

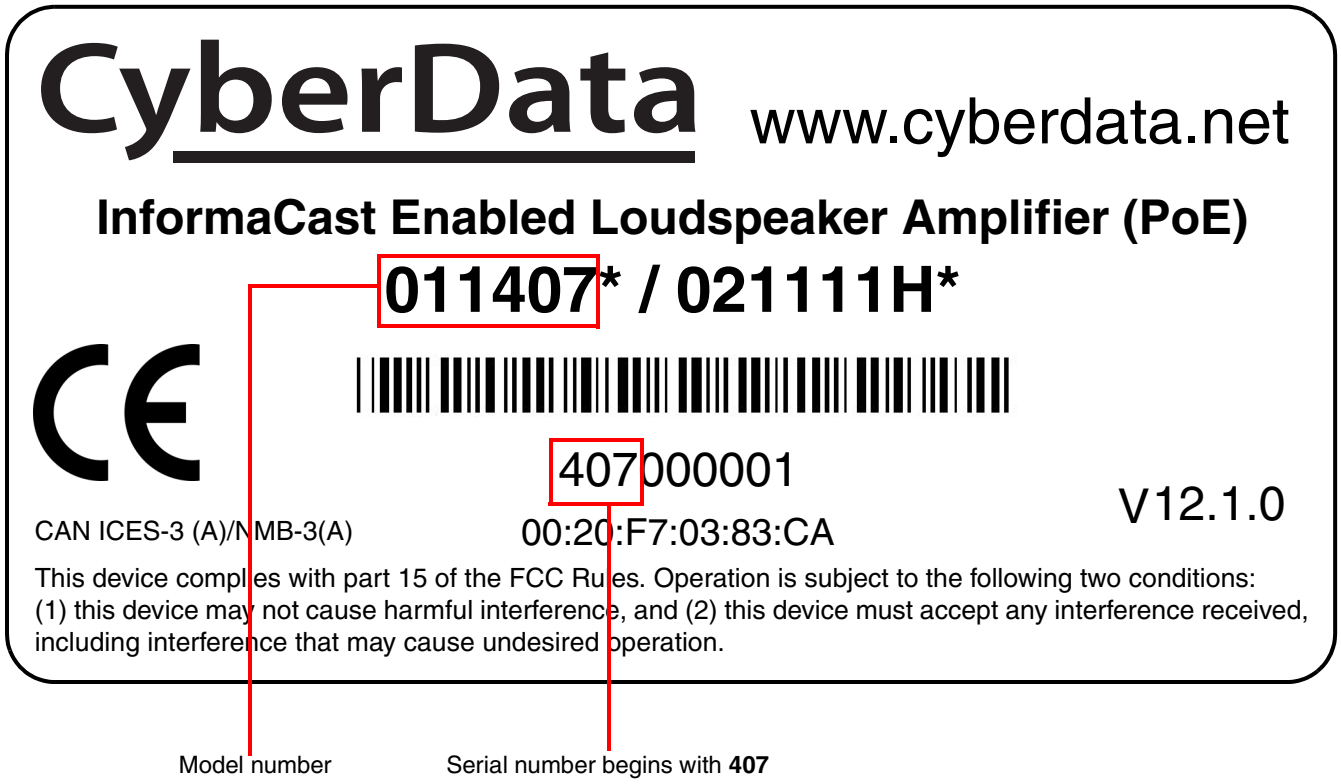
1 Product Overview

1.1 How to Identify This Product

To identify the InformaCast Enabled Loudspeaker 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 **011407**.

Figure 1-1. Model Number Label[1]

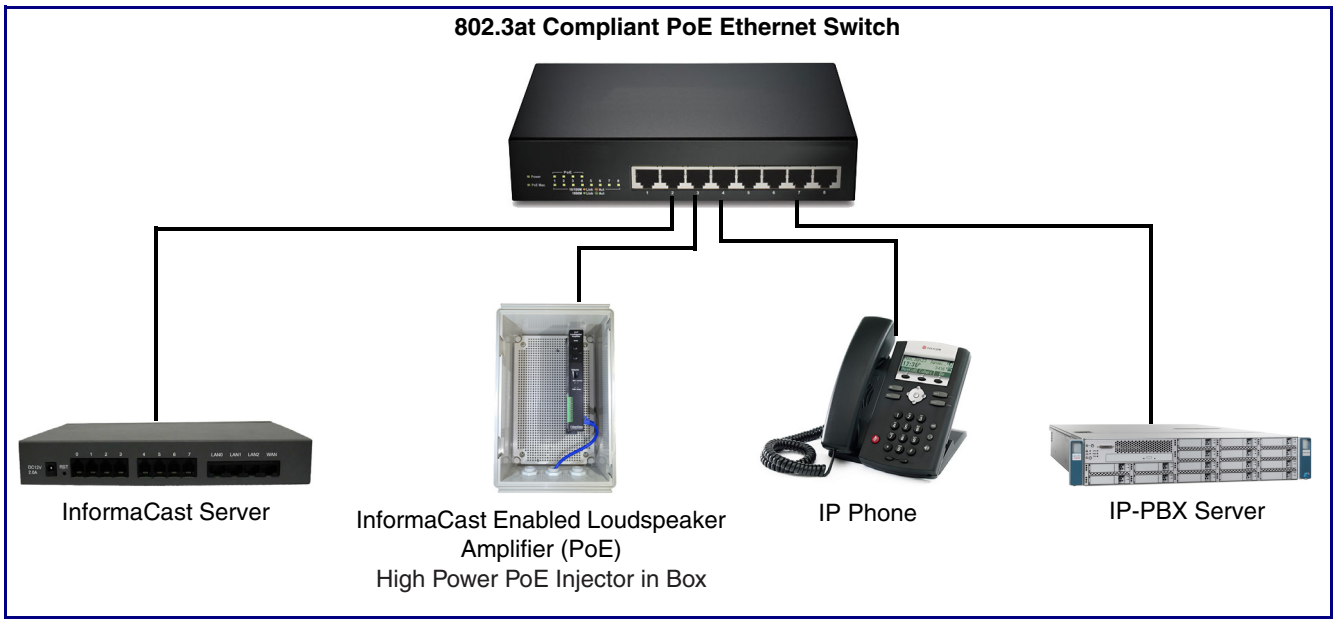


1. This figure is just an example. The revision and version information in this figure may be different than the label on your product.

1.2 Typical System Installation

Figure 1-2 illustrates how the InformaCast Enabled Loudspeaker Amplifier (PoE) is normally installed as part of a public address system.

Figure 1-2. Typical Installation



1.3 Features

- Compatible with Singlewire InformaCast v12.1, including support for downloading SIP credentials from InformaCast
- Supports Singlewire InformaCast High Quality Audio
- Capable of receiving Singlewire InformaCast, SIP, and Multicast messages
- Support for InformaCast resiliency
- Support for Cisco SRST resiliency

- Concurrent InformaCast, 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 with 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 and manual volume control

- Autoprovisioning via HTTPS, HTTP or TFTP
- HTTPS or HTTP web based configuration. HTTPS is enabled by default.
- Configurable event generation for device health and status monitoring
- TLS 1.2 and SRTP enhanced security for IP endpoints in a local or cloud-based environment
- 802.11q VLAN tagging
- HTTP command interface

1.4 Supported Protocols

The InformaCast Enabled Loudspeaker Amplifier (PoE) supports:

- SIP
- InformaCast Version 4.0 and greater
- Multicast
- HTTP and HTTPS web-based configuration

  Provides an intuitive user interface for easy system configuration and verification of InformaCast Enabled Loudspeaker Amplifier (PoE) operations.
- TLS 1.2
- DHCP Client

  Dynamically assigns IP addresses in addition to the option to use static addressing.
- InformaCast Version 4.0 and greater
- 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 InformaCast Enabled Loudspeaker Amplifier (PoE) for the supported SIP servers:

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

1.6 Specifications

Table 1-1. Specifications

Specifications	
Ethernet I/F	10/100 Mbps
Protocol	SIP RFC 3261 Compatible
Notification Software	Singlewire InformaCast v4.0 and above
Power Input	PoE 802.3at 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/SSL 1.2 and SRTP
Enclosure	UL 94-HB flame resistant, IK 08 Impact-rated, IP66 enclosure
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]	10 in. [254 mm] Length 4 in. [101.6 mm] Width 14 in. [355.6 mm] Height
Weight	3.6 lbs. [1.63 kg] 4.6 lbs. [2.1 kg]
Compliance	CE; EMC Directive – Class A EN 55032 & EN 55024, LV Safety Directive – EN 60950-1, RoHS Compliant, FCC; Part 15 Class A, Industry Canada; ICES-3 Class A, IEEE 802.3 Compliant
Warranty	2 Years Limited
Part Number	011407

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.

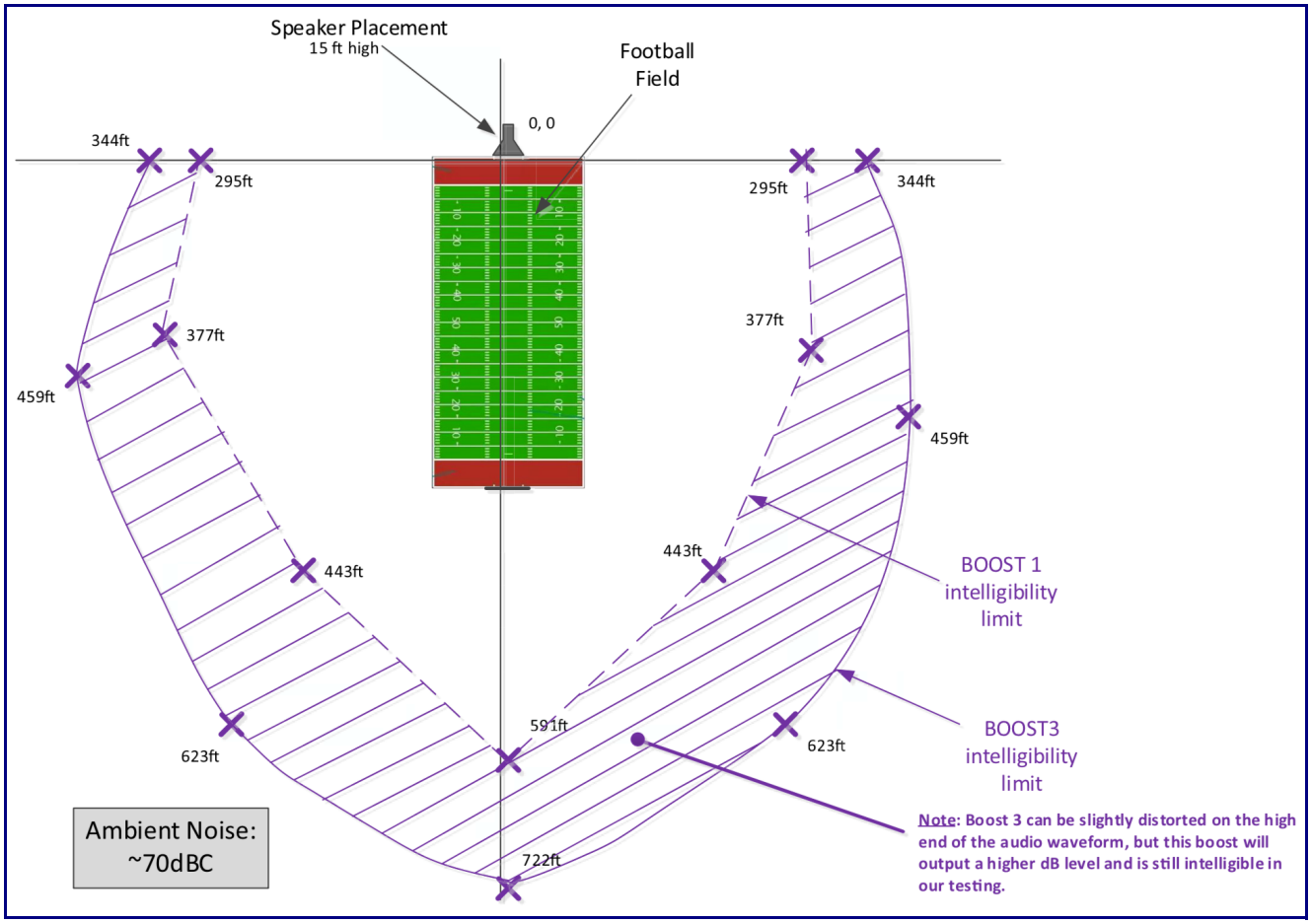
1.7 Typical Coverage

With one horn attached to 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

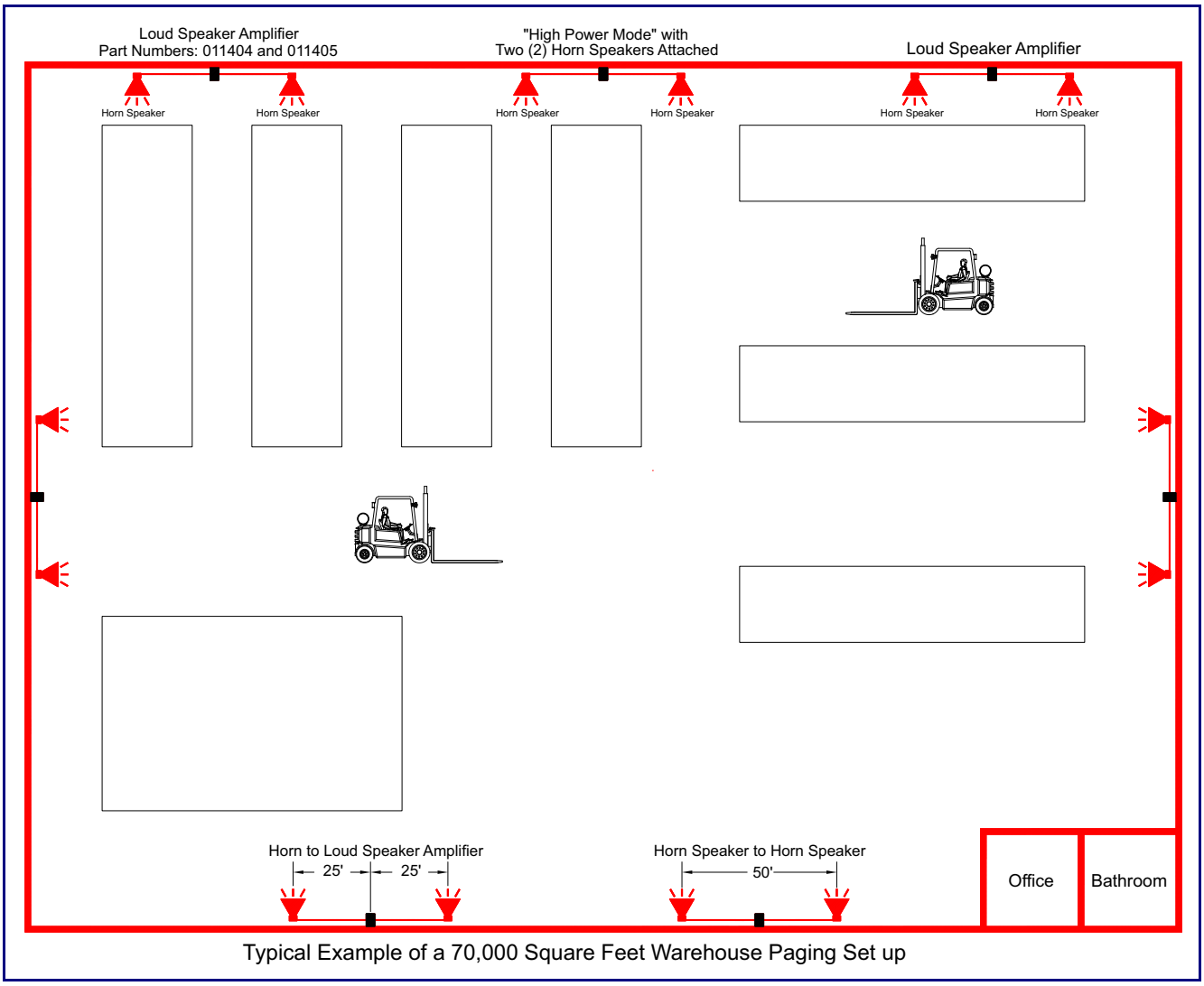
The figure below shows the intelligibility outdoor field test of the device when it is used with the 011471 IP66 Outdoor Analog Horn.

Figure 1-3. Intelligibility Outdoor Field Test



1.7.2 Typical Warehouse Paging Setup

Figure 1-4. Typical Warehouse Paging Setup



Typical Example of a 70,000 Square Feet Warehouse Paging Set up

1.8 Compliance

1.8.1 CE Testing

CE testing has been performed according to EN ISO/IEC 17050 for Emissions, Immunity, and Safety.

Note You can download the Declaration of Conformity document from the **Downloads** tab of the product's webpage.

1.8.2 FCC Statement

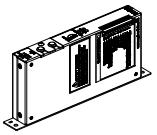
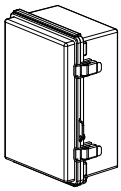
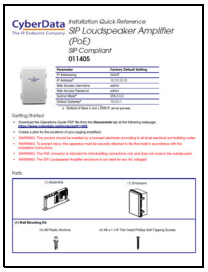
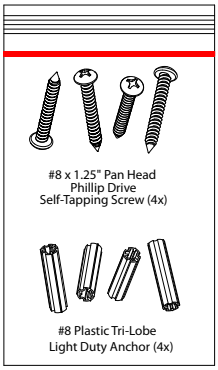
This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, 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.

2 Installing the InformaCast Enabled Loudspeaker Amplifier (PoE)

2.1 Parts List

Table 2-1 illustrates the parts for each InformaCast Enabled Loudspeaker Amplifier (PoE) and includes a kit for mounting.

Table 2-1. Parts List

Quantity	Part Name	Illustration
1	Singlewire InformaCast Paging Amplifier Assembly	
1	Enclosure	
1	Installation Quick Reference Guide	
1	Mounting Accessory Kit which includes: (4) #8 Plastic Anchors (4) #8 x 1-1/4" Pan Head Phillips Self-Tapping Screws	

2.2 InformaCast Enabled Loudspeaker Amplifier (PoE) Setup

Set up and configure each InformaCast Enabled Loudspeaker Amplifier (PoE) *before* you mount it.

CyberData delivers each InformaCast Enabled Loudspeaker Amplifier (PoE) with the factory default values indicated in
Table 2-2:

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

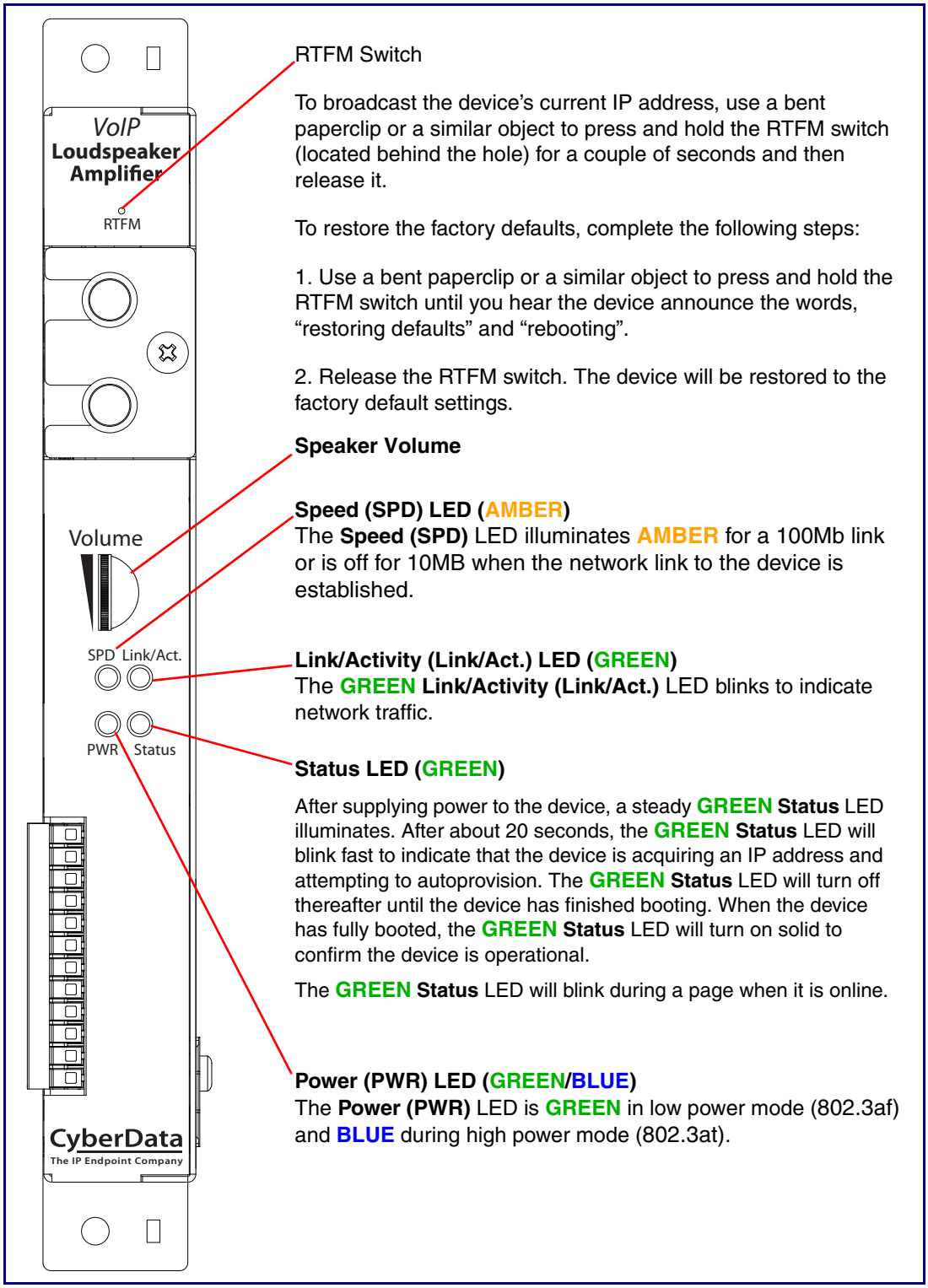
Parameter	Factory Default Setting
IP Addressing	DHCP
IP Address[a]	10.10.10.10
Web Access Username	admin
Web Access Password	admin
Subnet Mask[a]	255.0.0.0
Default Gateway[a]	10.0.0.1

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

2.2.1 InformaCast Enabled Loudspeaker Amplifier (PoE) Components

Figure 2-1 shows the components of the InformaCast Enabled Loudspeaker Amplifier (PoE).

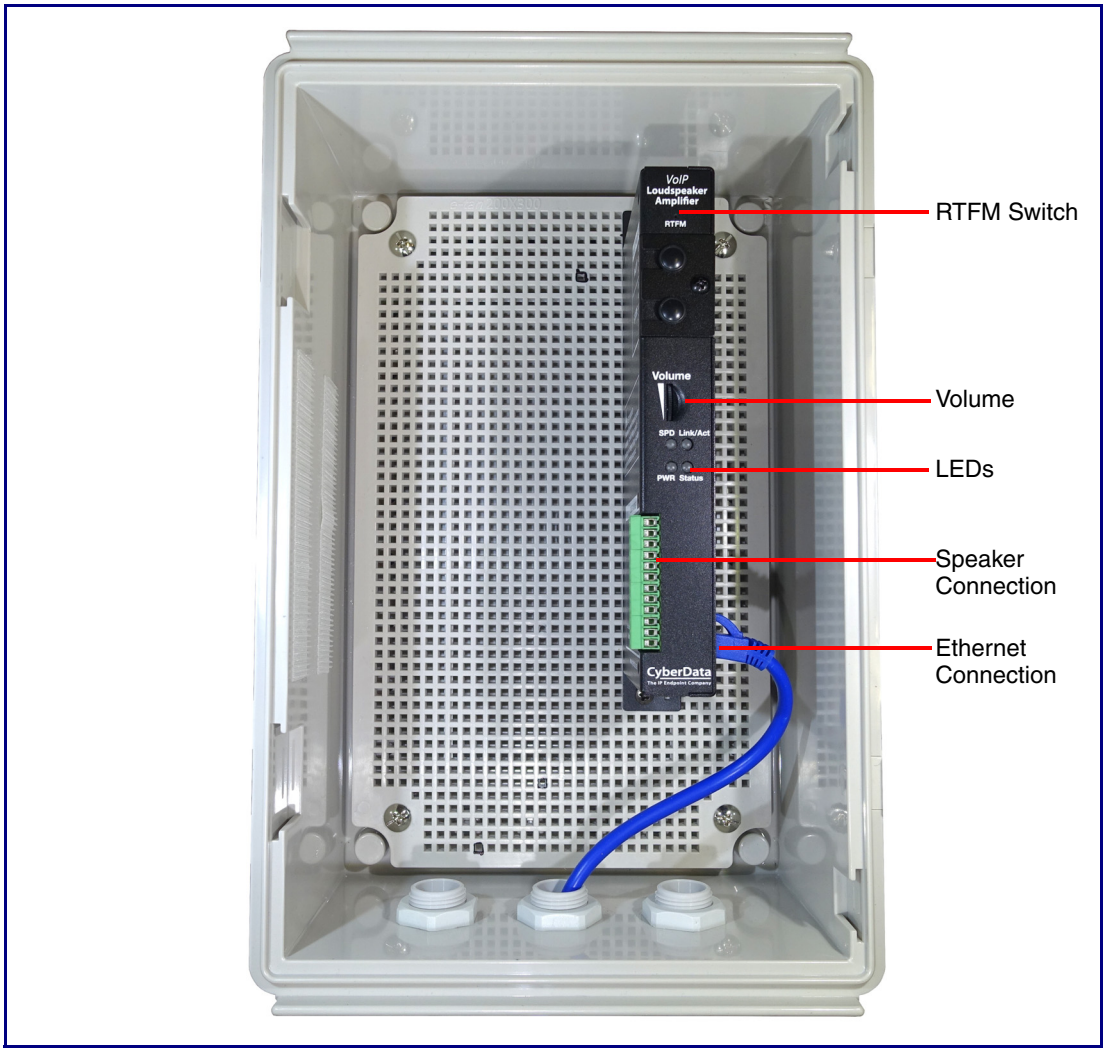
Figure 2-1. InformaCast Enabled Loudspeaker Amplifier (PoE) Components



2.2.2 NEMA Box Components of the InformaCast Enabled Loudspeaker Amplifier (PoE)

Figure 2-2 shows all of the NEMA box components of the InformaCast Enabled Loudspeaker Amplifier (PoE).

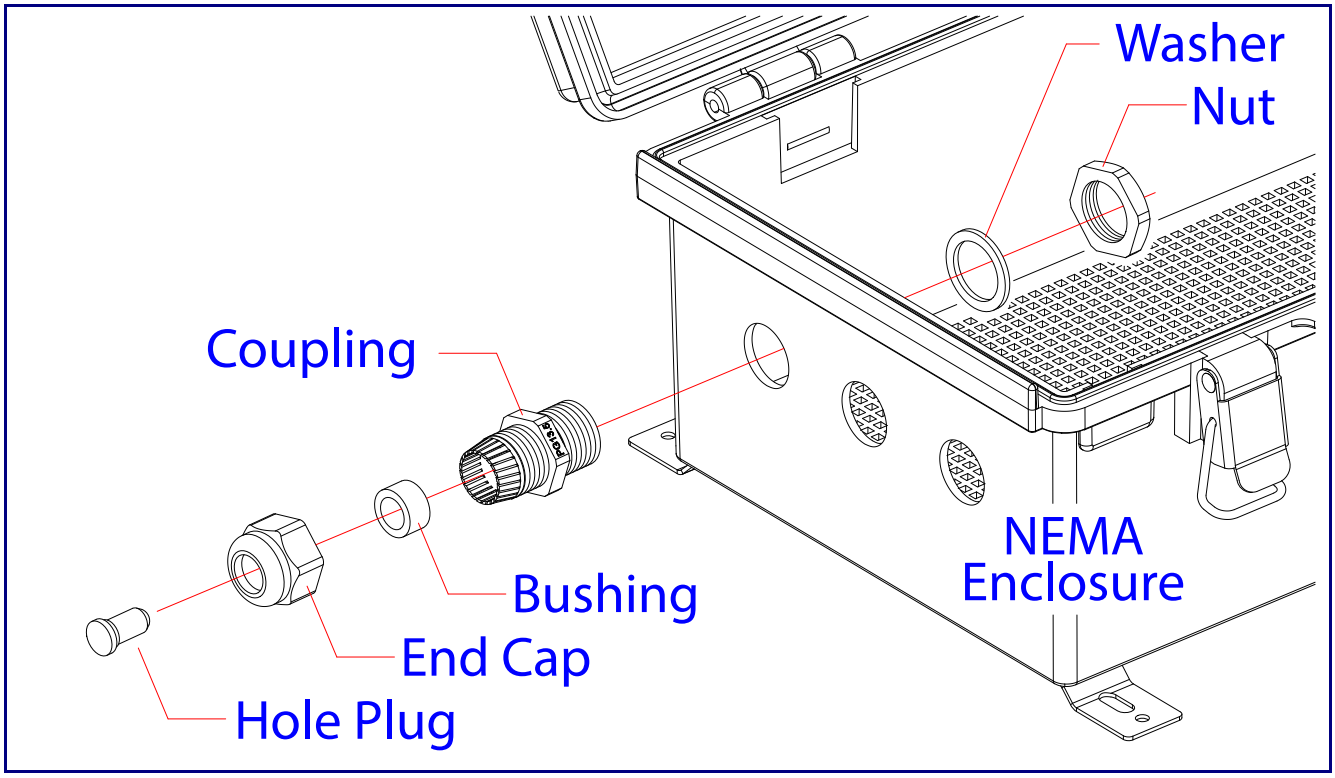
Figure 2-2. Loudspeaker Amplifier Components—PoE



2.2.3 Assembling the Cable Gland

Assemble the cable gland as shown in Figure 2-3.

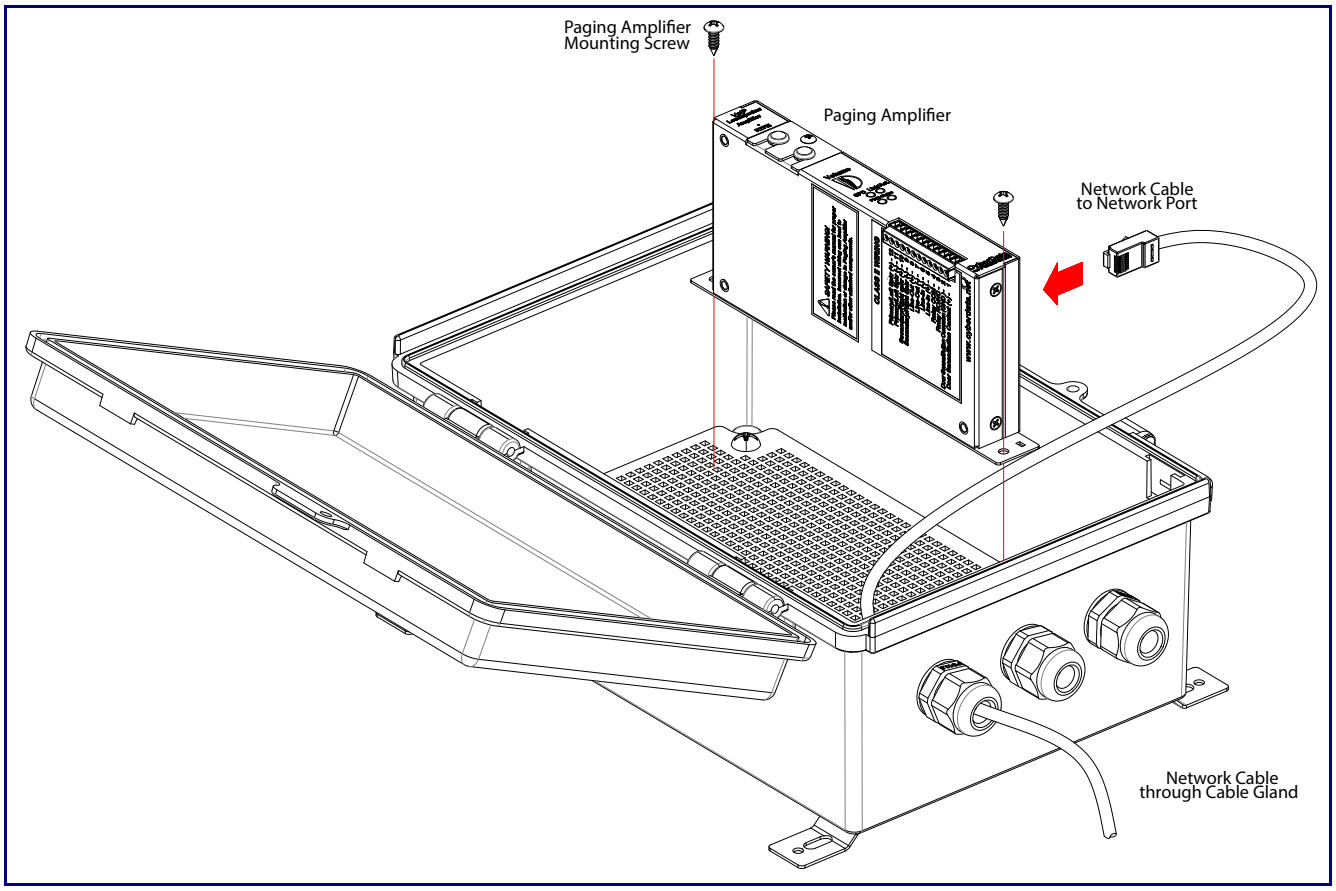
Figure 2-3. Assembling the Cable Gland



2.2.4 Installing the InformaCast Enabled Loudspeaker Amplifier (PoE)

Install the InformaCast Enabled Loudspeaker Amplifier (PoE) as shown in Figure 2-4.

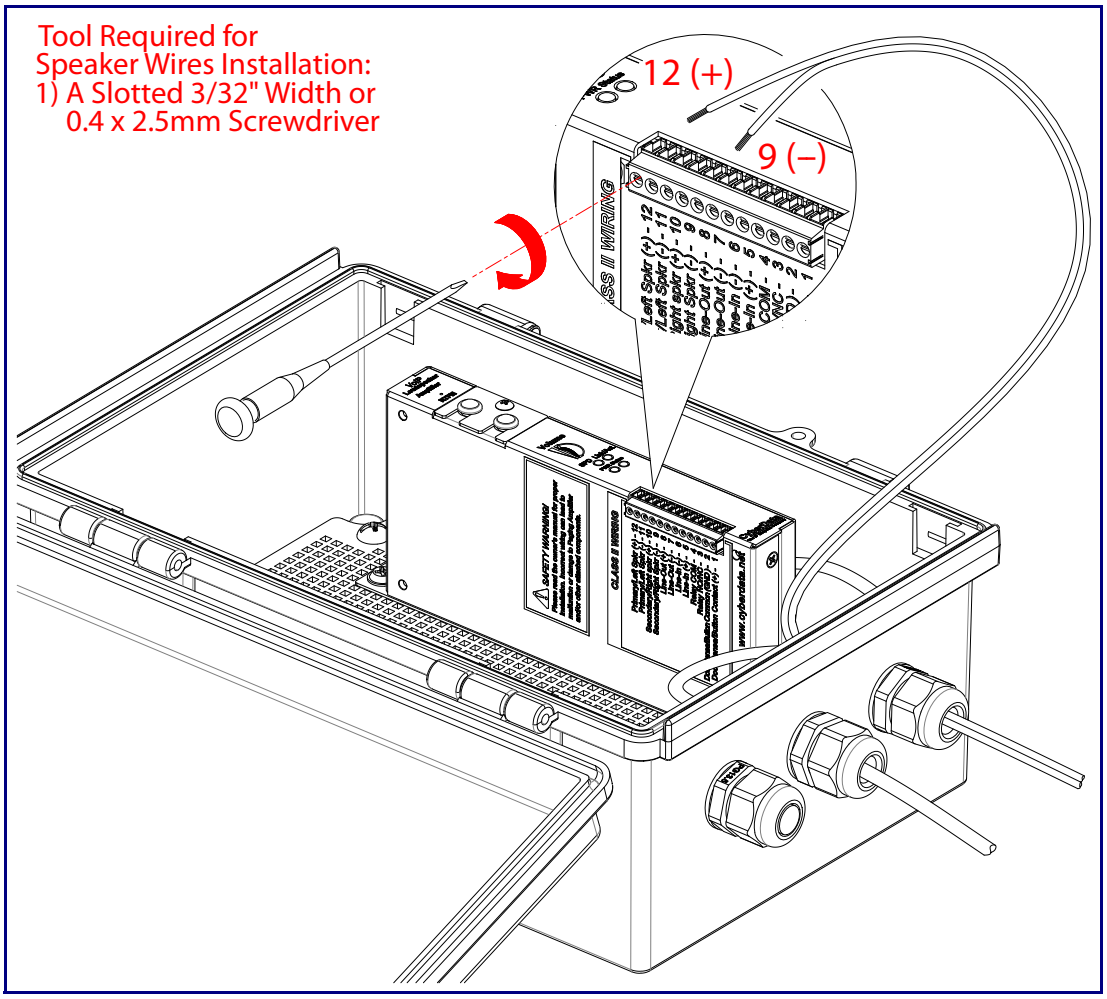
Figure 2-4. Installing the InformaCast Enabled Loudspeaker Amplifier (PoE)



2.2.5 Connecting the Speaker Wires

Connect the speaker wires to the terminal block as shown in Figure 2-5.

Figure 2-5. Connecting the Speaker Wires



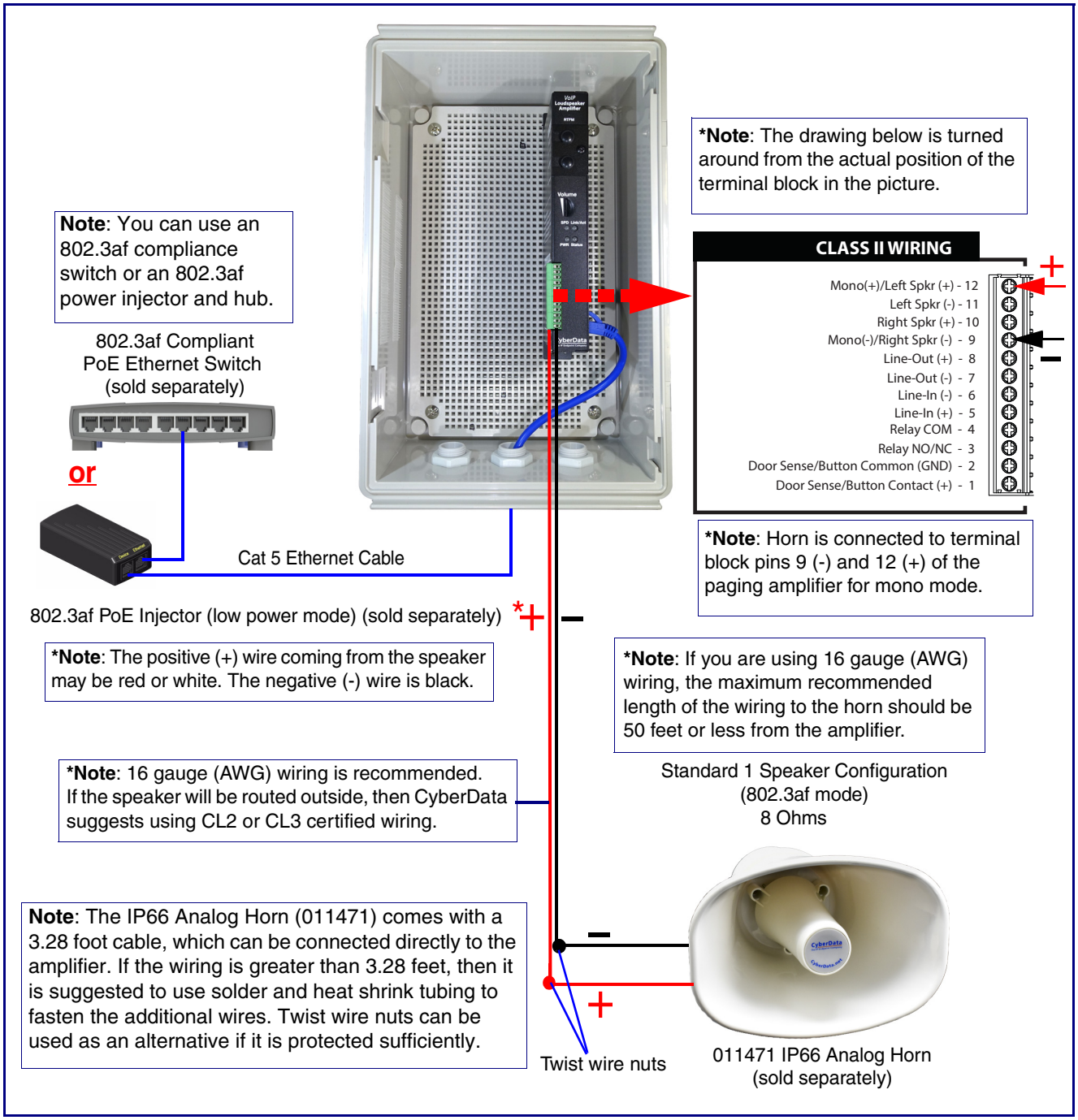
2.2.6 Connecting the InformaCast Enabled Loudspeaker Amplifier (PoE)

2.2.6.1 Using the Amplified Outputs

Low Power Mode (One Speaker)

The following figure illustrate how to connect the InformaCast Enabled Loudspeaker Amplifier (PoE) and use the amplified outputs in low power mode to one speaker or horn.

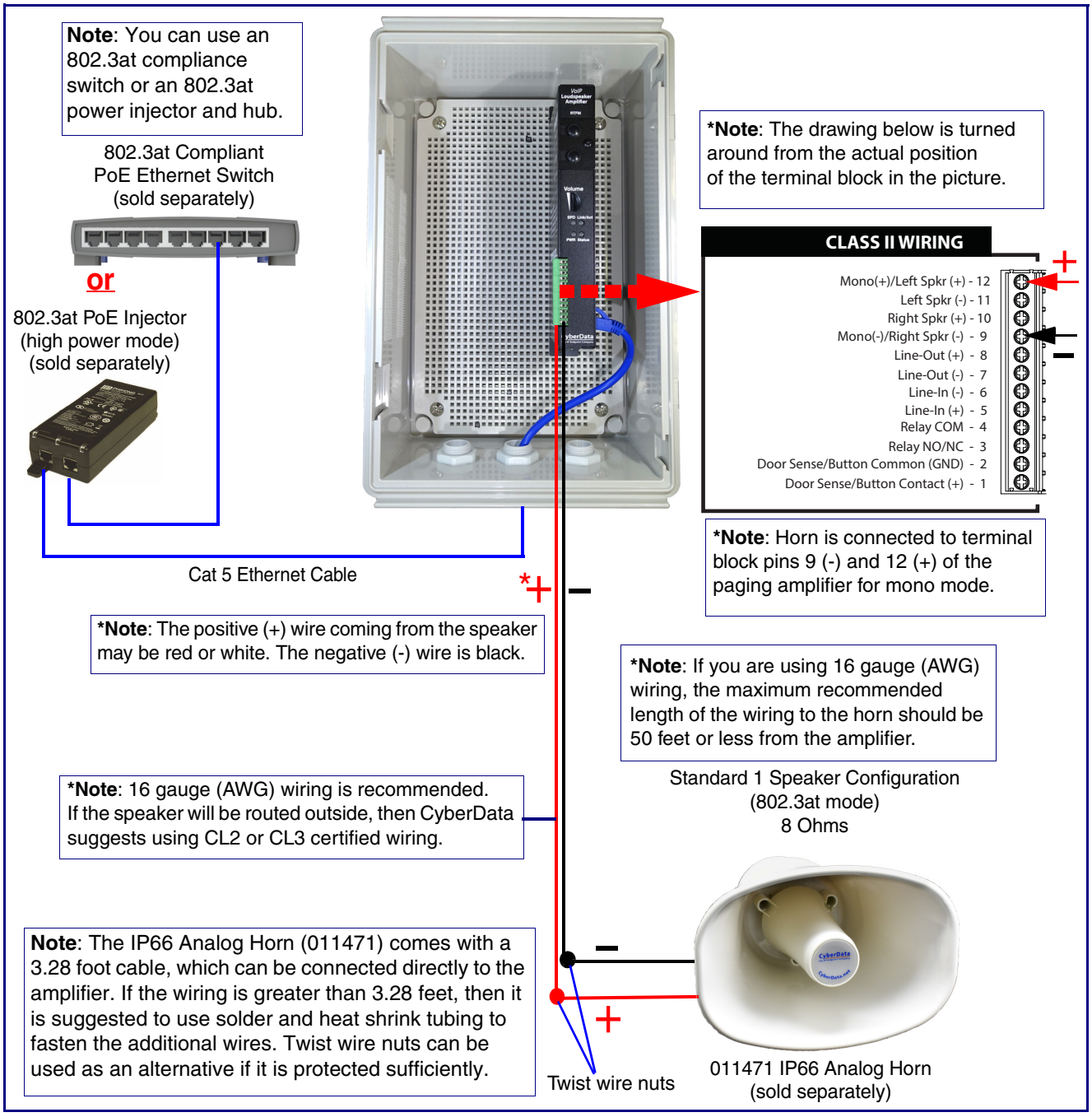
Figure 2-6. Using the Amplified Outputs—Low Power Mode with One Speaker



High Power Mode (One Speaker)

The following figure illustrate how to connect the InformaCast Enabled Loudspeaker Amplifier (PoE) and use the amplified outputs in high power mode to one speaker or horn.

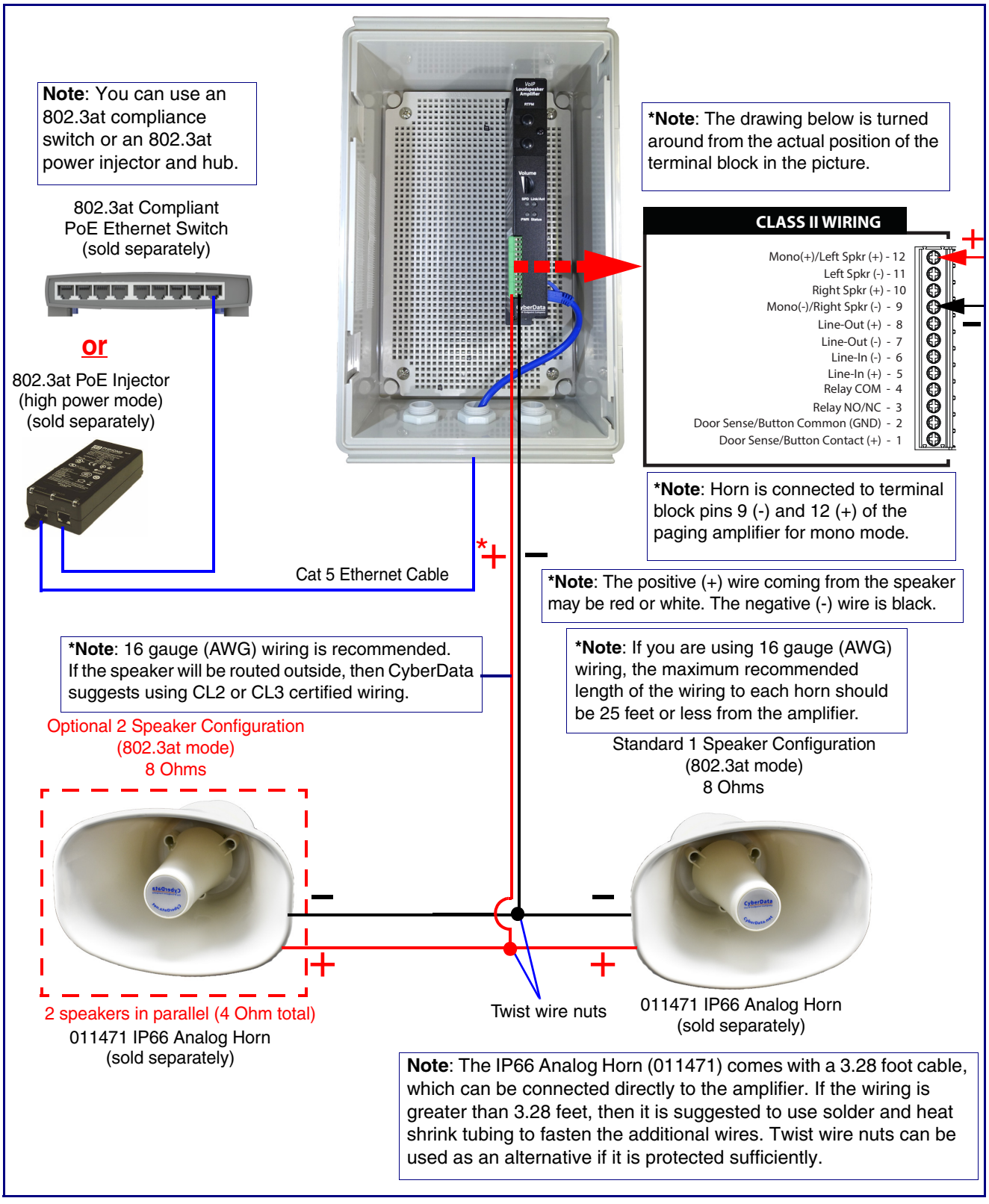
Figure 2-7. Using the Amplified Outputs—High Power Mode with One Speaker



High Power Mode (Two Speakers)

The following figure illustrate how to connect the InformaCast Enabled Loudspeaker Amplifier (PoE) 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



2.2.7 InformaCast Enabled Loudspeaker Amplifier (PoE) System Installation and Connection Options

The following figures show the connection options for the InformaCast Enabled Loudspeaker Amplifier (PoE).

Figure 2-9. InformaCast Enabled Loudspeaker Amplifier (PoE) Connections

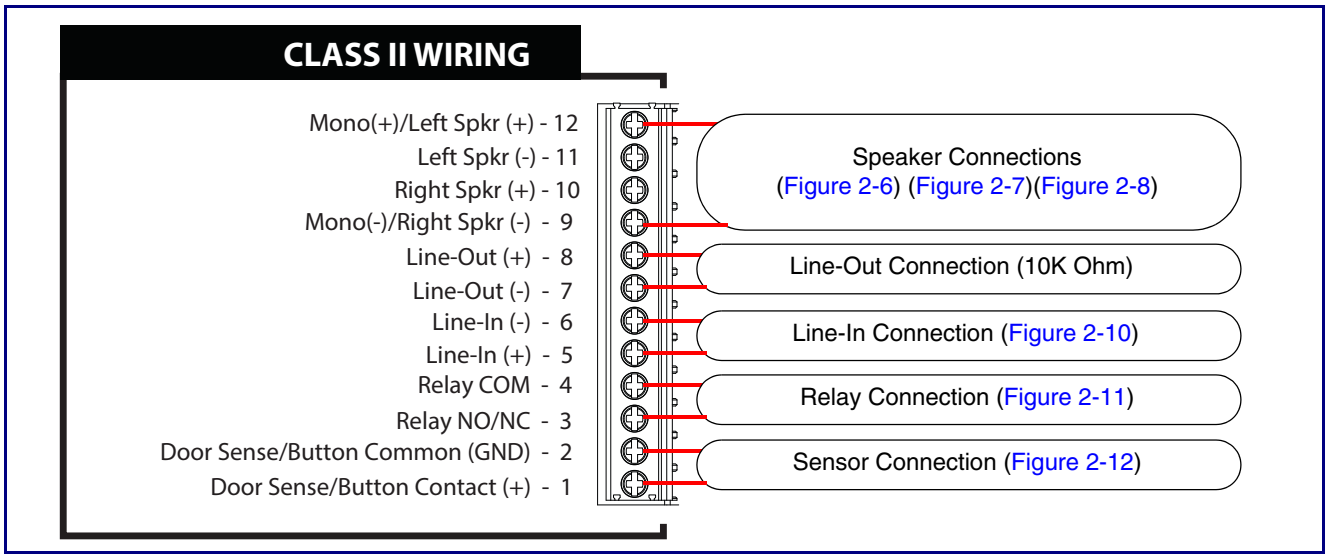


Figure 2-10. Line-In Connection

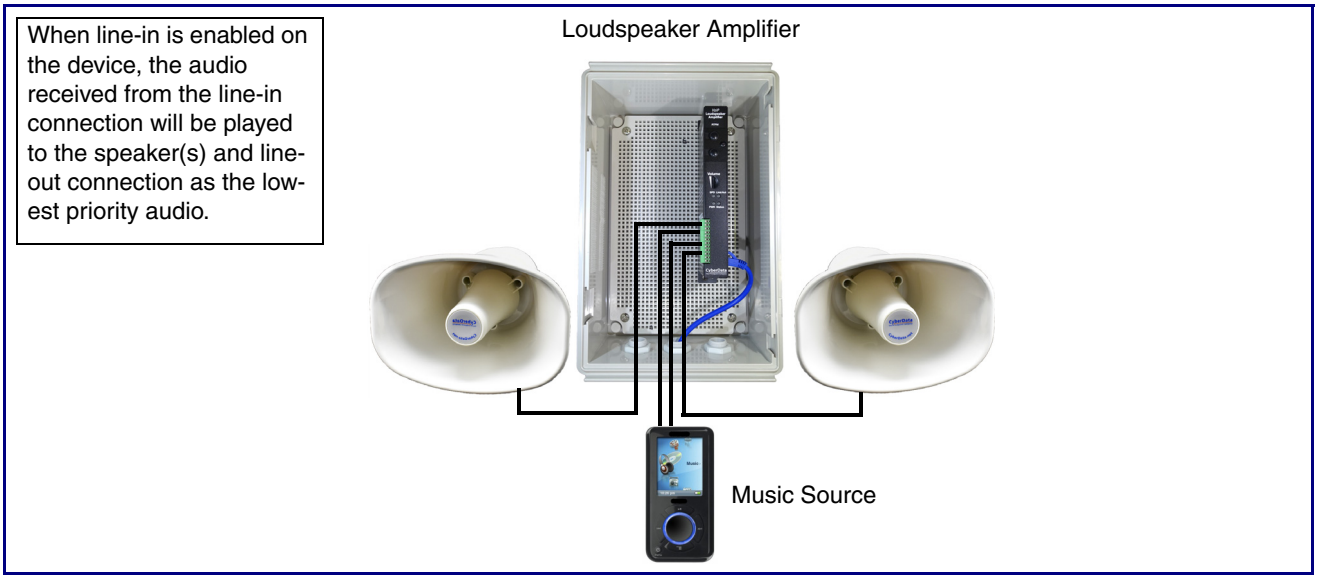


Figure 2-11. Relay or LED Strobe Connection

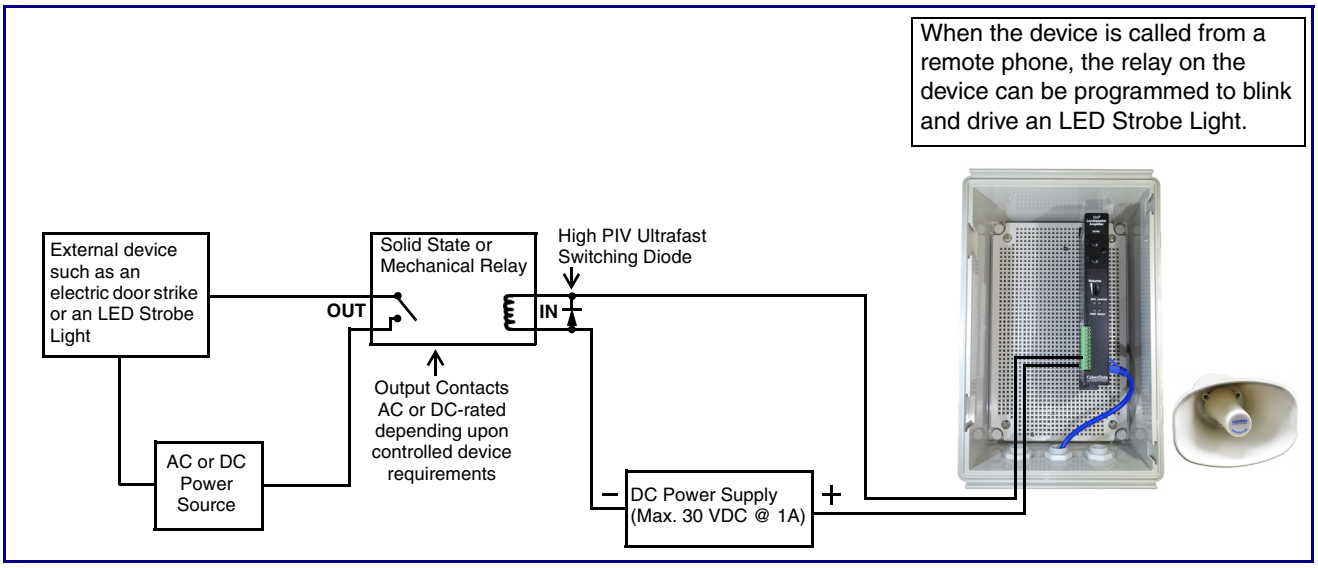
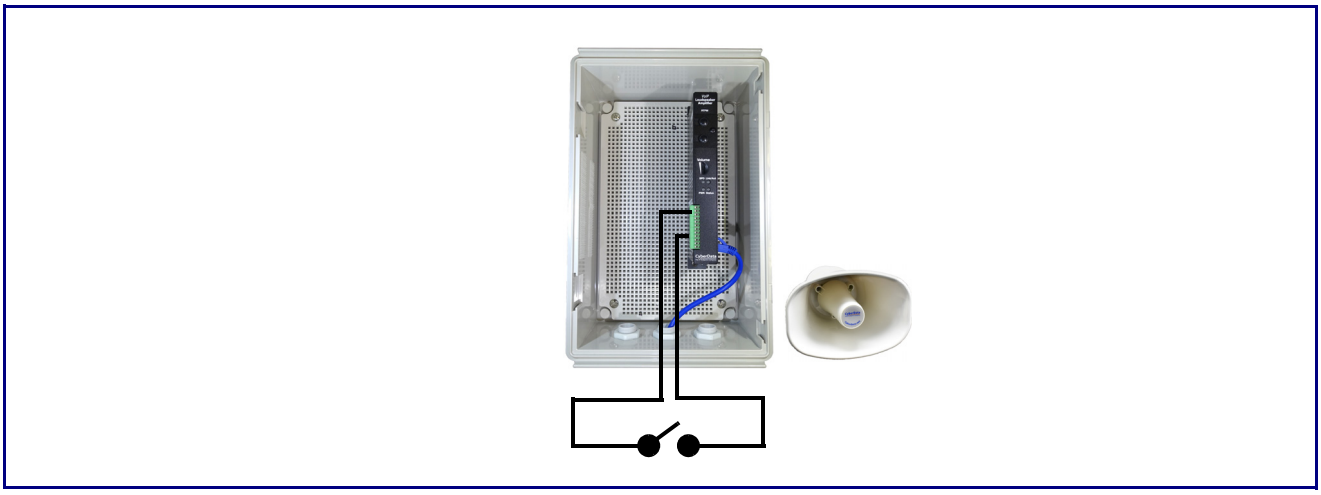


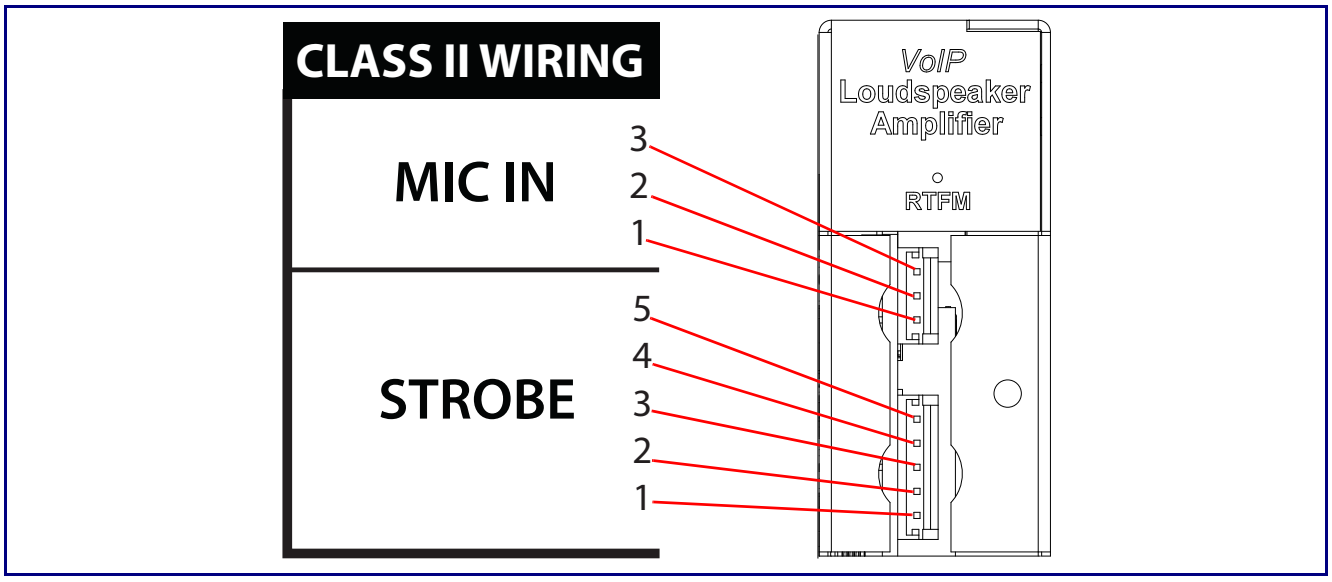
Figure 2-12. Sensor Connection



2.2.8 Strobe Connections Behind the Port Cover

See Figure 2-13 for the additional connection options for the InformaCast Enabled Loudspeaker Amplifier (PoE).

Figure 2-13. Connections Behind the Port Cover



See Table 2-3 for the descriptions of the connections behind the port cover.

Table 2-3. Connections Behind the Port Cover

Microphone Connections		
Name	**Connection**	**Description**
MIC IN	J6-1	Microphone chassis ground connections
	J6-2	Microphone positive input
	J6-3	Microphone negative input
Strobe Connections		
Name	**Connection**	**Description**
STROBE	J9-1	Ground
	J9-2	Strobe positive power (+24V)
	J9-3	Ground
	J9-4	I2C data
	J9-5	I2C clock

2.2.9 Connecting the Optional 011288 Auxiliary RGB Strobe

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. Feed the strobe cable through an available gland near the bottom of the enclosure.
5. Connect the strobe cable to the **STROBE IN** connection (J9) (see Figure 2-14 and Figure 2-15) and to **J1** of the board of the optional 011288 Auxiliary RGB Strobe (sold separately).
6. Install the mounting screw to secure the cover plate. See Figure 2-14.

Figure 2-14. Connecting the Optional 011288 Auxiliary RGB Strobe

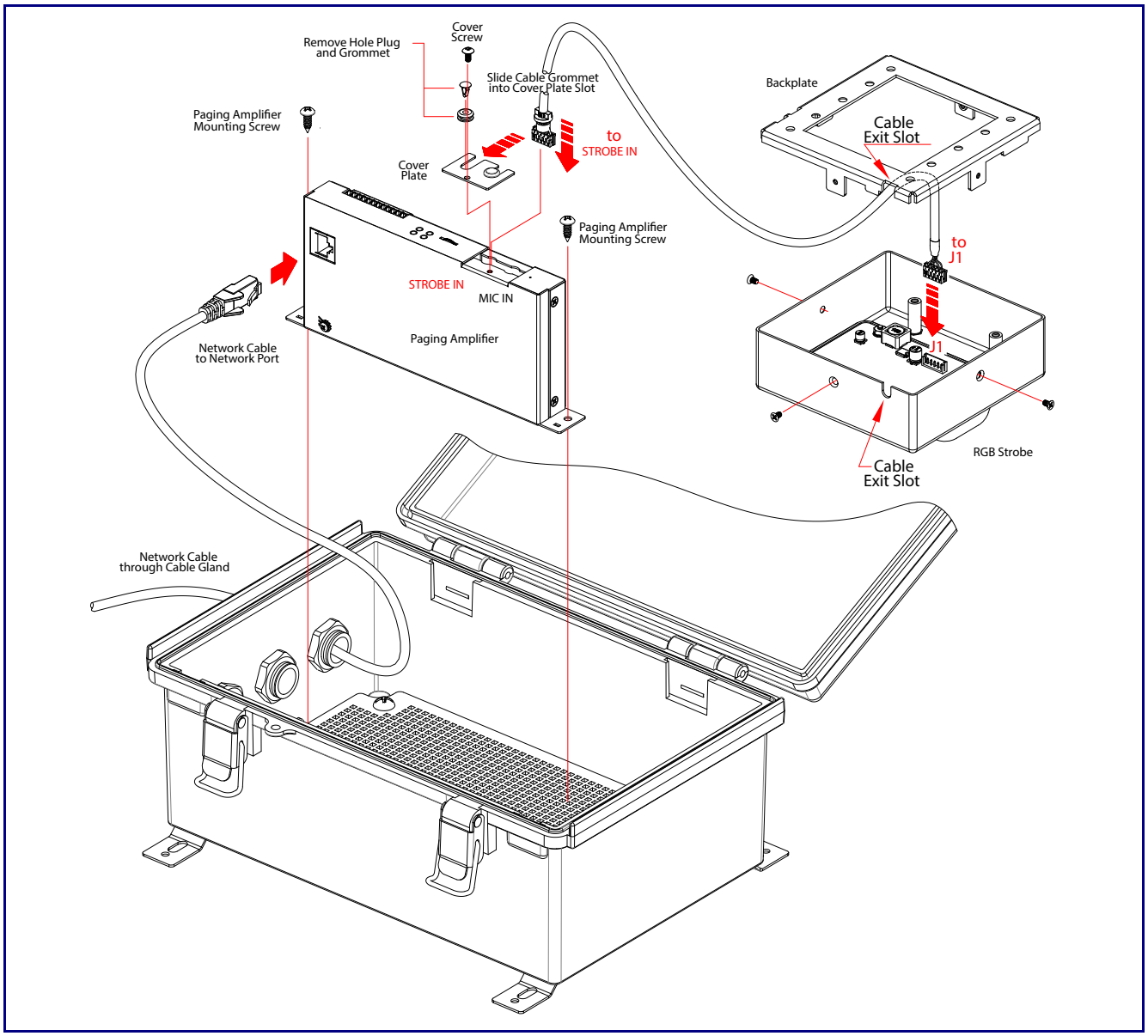
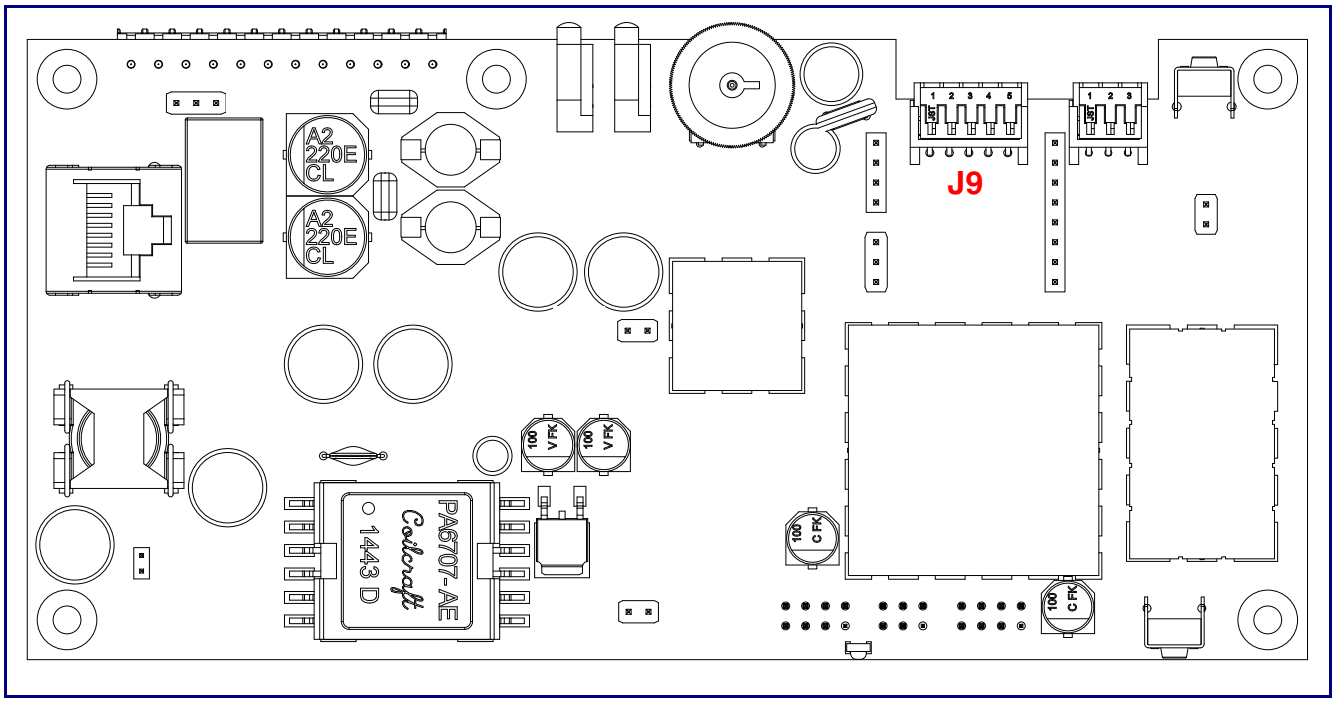


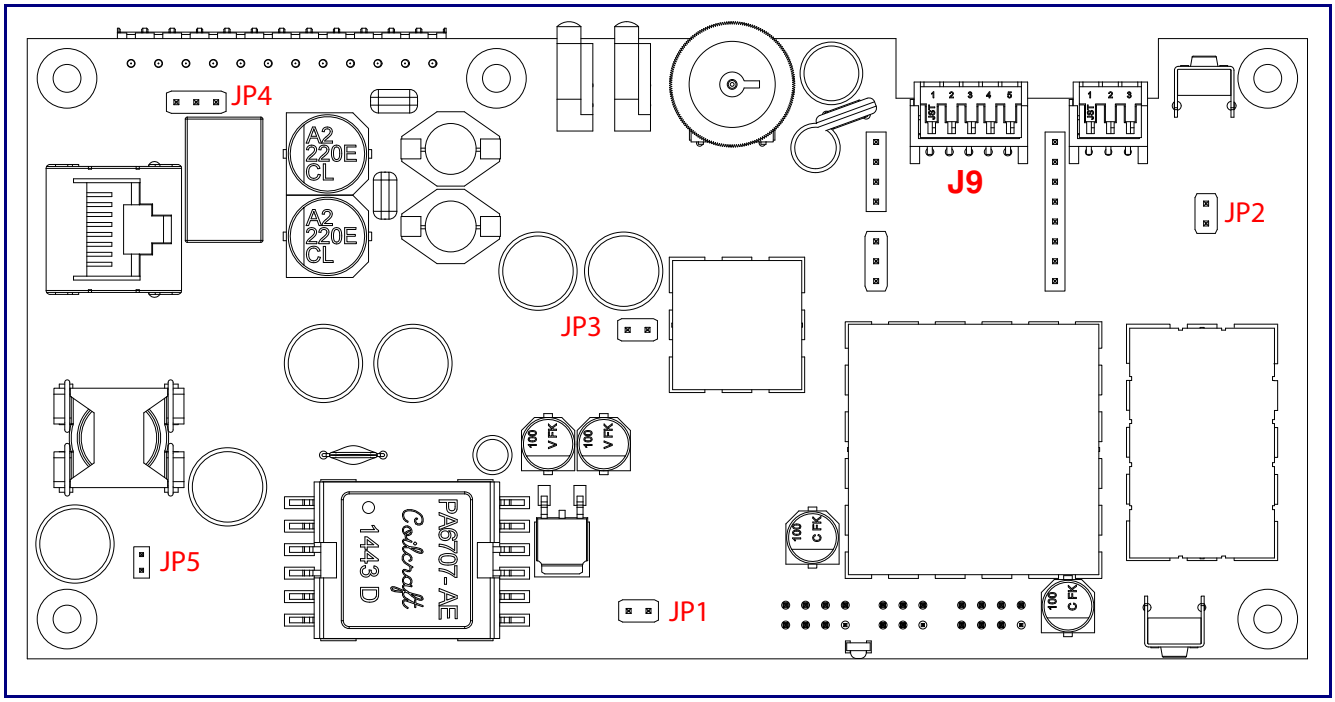
Figure 2-15. J9 STROBE IN



2.2.10 InformaCast Enabled Loudspeaker Amplifier (PoE) Jumpers

See Figure 2-16 for the jumper locations.

Figure 2-16. Jumper Locations



See Table 2-4 for the jumper descriptions.

Table 2-4. Jumper Descriptions

Jumper	Description
JP1	Reset—Factory Only
JP2	RTFM (not installed)
JP3	Audio Enable Jumper—Factory Only
JP4	Relay NO/NC (default to NO)—Factory Only
JP5	PoE IEEE 802.3at—Factory Only

2.2.11 Ethernet Connection

See Table 2-5 for details about the InformaCast Enabled Loudspeaker Amplifier (PoE) connection.

Table 2-5. InformaCast Enabled Loudspeaker Amplifier (PoE) Connection

Connection	Connection Details	Location
Ethernet	Use a RJ 45 cable.	InformaCast Enabled Loudspeaker Amplifier (PoE)

2.2.12 Loudspeaker Type

Using the amplified output, the CyberData InformaCast Enabled Loudspeaker Amplifier (PoE) supports the 011471 Horn or equivalent unamplified loudspeaker.

Figure 2-17. 011471 Horn

2.2.13 Cabling/Wiring

Using the amplified output, you may connect a 011471 loudspeaker or equivalent unamplified speaker to a SIP Loudspeaker Amplifier (PoE-powered) 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.

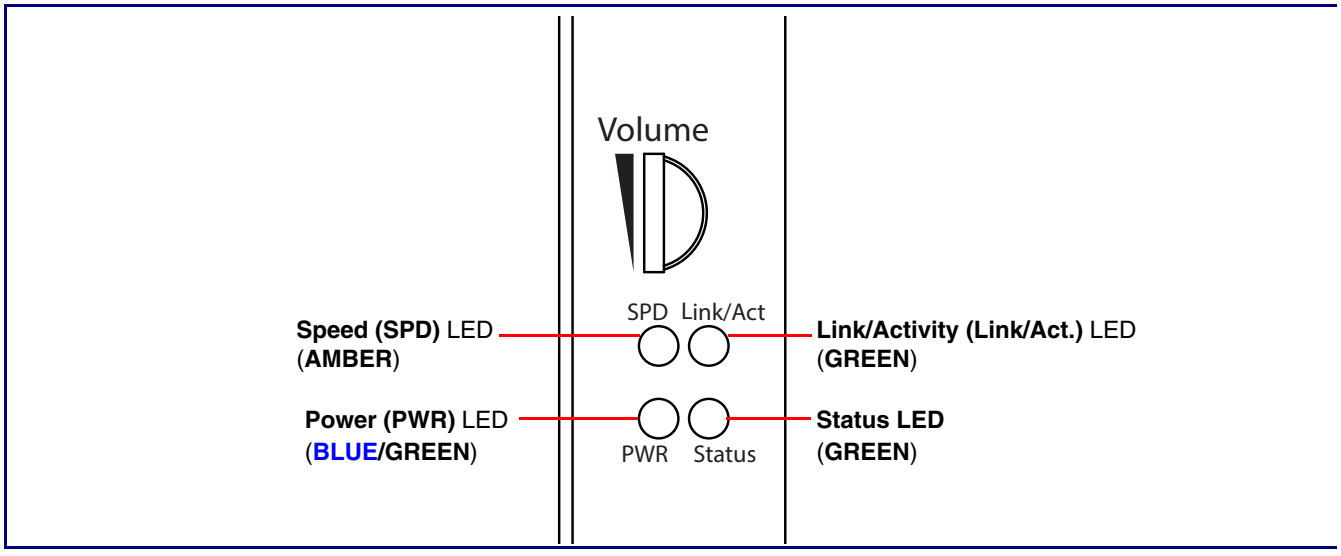
2.2.14 Confirm Operation

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

Table 2-6. InformaCast Enabled Loudspeaker Amplifier (PoE) LEDs

LED	Color	Function
Power (PWR)	**BLUE/GREEN**	The 802.3at power injector that is provided with the device should cause the **Power (PWR)** LED to illuminate **BLUE** to indicate that high power is available. The **Power (PWR)** LED may illuminate **GREEN** if a low power mode (802.3af) power source is used (not included and sold separately).
Status	**GREEN**	After supplying power to the device, a steady **GREEN Status** LED illuminates. After about 20 seconds, the **GREEN Status** LED will blink fast to indicate that the device is acquiring an IP address and attempting to autoprovision. The **GREEN Status** LED will turn off thereafter until the device has finished booting. When the device has fully booted, the **GREEN Status** LED will turn on solid to confirm the device is operational. The **GREEN Status** LED will blink during a page when it is online.
Speed (SPD)	**AMBER**	The **Speed (SPD)** LED illuminates **AMBER** for a 100Mb link or is off for 10MB when the network link to the device is established.
Link/Activity (Link/Act.)	**GREEN**	The **Link/Activity (Link/Act.) GREEN** LED blinks to indicate network traffic.

Figure 2-18. InformaCast Enabled Loudspeaker Amplifier (PoE) LEDs

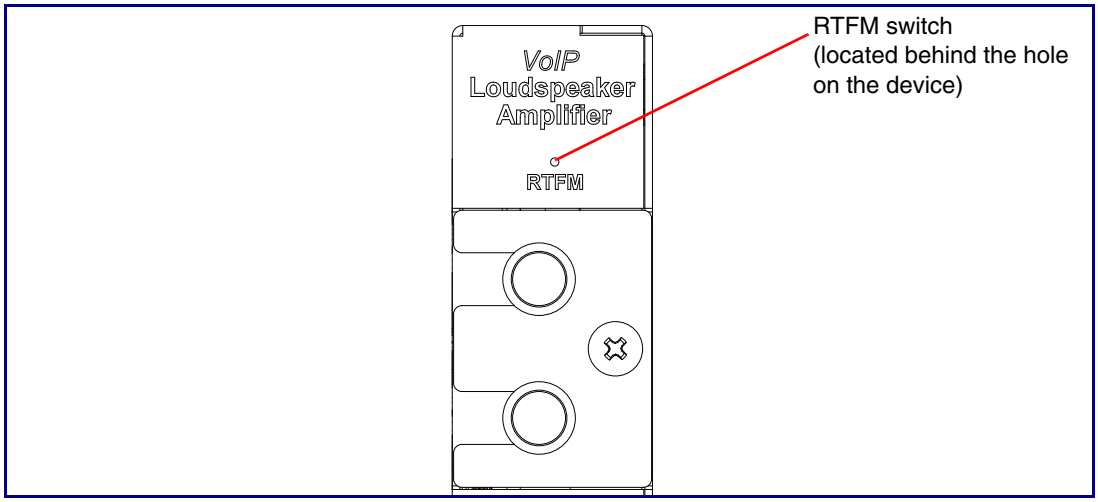


2.2.15 Confirm the IP Address and Test the Audio

2.2.15.1 RTFM Switch

When the InformaCast Enabled Loudspeaker Amplifier (PoE) 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 press and hold the RTFM switch for a couple of seconds and then release it.

Caution

Equipment Caution: 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.

Restoring the Factory Default Settings

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

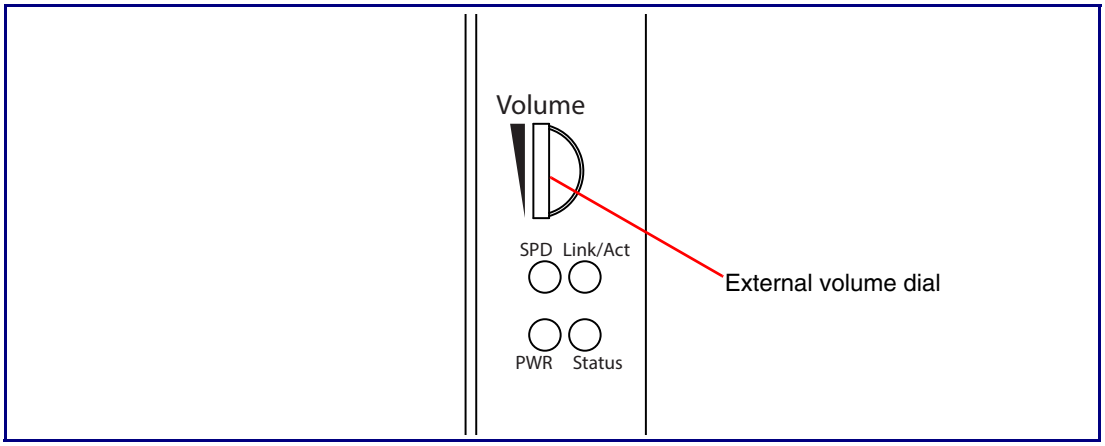
1. Use a bent paperclip or a similar object to press and hold the RTFM switch until you hear the device announce the words, "restoring defaults" and "rebooting".
2. Release the RTFM switch. The device will be restored to the factory default settings.

2.2.16 Adjust the Volume

There are two ways to adjust the volume for the InformaCast Enabled Loudspeaker Amplifier (PoE):

- The **SIP Volume** setting on the **Device Page**
- The external **Volume** dial (Figure 2-21) on the InformaCast Enabled Loudspeaker Amplifier (PoE) face

Figure 2-20. External Volume Dial



2.2.16.1 The SIP Volume Setting

To adjust the volume of the device with the **SIP Volume** setting on the **Device Page**, complete the following steps:

1. Go to the **Home Page**.
2. Select the **Device Page** page.
3. In the **SIP Volume** box, type a number between **0** (lowest) and **9** (highest).
4. Select **Save**.

2.2.16.2 The Multicast Volume Setting

To adjust the **Multicast Volume** volume with the **Multicast Volume** setting on the **Device Page**, complete the following steps:

1. Go to the **Home Page**.
2. Select the **Device Page**.
3. In the **Multicast Volume** box, type a number between **0** (lowest) and **9** (highest).
4. Select **Save**.

2.2.16.3 The Ring Volume Setting

To adjust the ring volume with the **Ring Volume** setting on the **Device Page**, complete the following steps:

1. Go to the **Home Page**.
2. Select the **Device Page**.
3. In the **Multicast Volume** box, type a number between **0** (lowest) and **9** (highest).
4. Select **Save**.

2.2.16.4 The Sensor Volume Setting

To adjust the sensor volume with the **Sensor Volume** setting on the **Device Page**, complete the following steps:

1. Go to the **Home Page**.
2. Select the **Device Page**.
3. In the **Sensor Volume** box, type a number between **0** (lowest) and **9** (highest).
4. Select **Save**.

2.2.16.5 The Loopback Volume Setting

To adjust the loopback volume with the **Loopback Volume** setting on the **Device Page**, complete the following steps:

1. Go to the **Home Page**.
2. Select the **Device Page**.
3. In the **Loopback Volume** box, type a number between **0** (lowest) and **9** (highest).
4. Select **Save**.

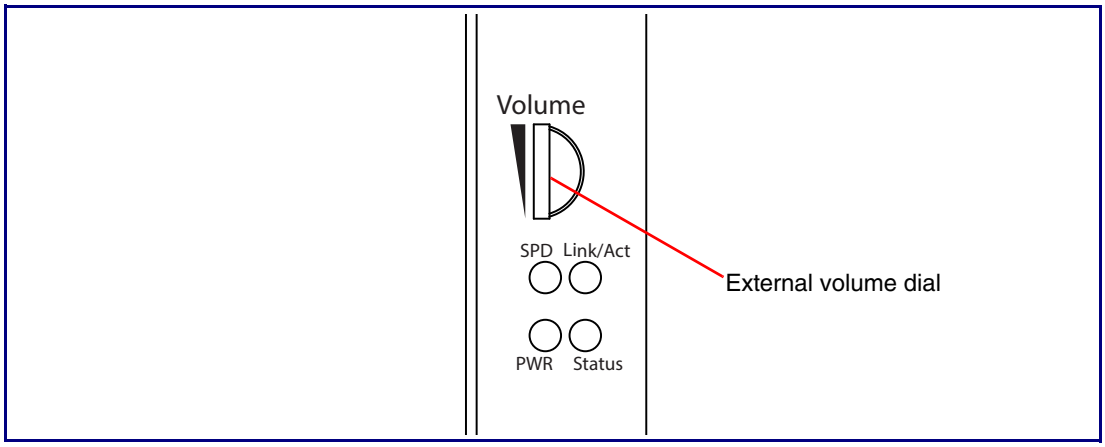
2.2.16.6 External Volume Dial

To adjust the InformaCast Enabled Loudspeaker Amplifier (PoE) volume with the external volume dial, complete the following steps:

1. Turn the external **Volume** dial (Figure 2-20) on the InformaCast Enabled Loudspeaker Amplifier (PoE) face.

Note For the lineout volume, the volume is fixed and the volume control is adjusted through an external amplifier.

Figure 2-21. External Volume Dial



2.3 Configure the InformaCast Enabled Loudspeaker Amplifier (PoE) Parameters

To configure the InformaCast Enabled Loudspeaker Amplifier (PoE) online, use a standard web browser.

Configure each InformaCast Enabled Loudspeaker Amplifier (PoE) and verify its operation *before* you mount it. When you are ready to mount an InformaCast Enabled Loudspeaker Amplifier (PoE), refer to Appendix A, "Mounting the Amplifier" for instructions.

2.3.1 Factory Default Settings

All InformaCast Enabled Loudspeaker Amplifier (PoE)s are initially configured with the following default IP settings:

When configuring more than one InformaCast Enabled Loudspeaker Amplifier (PoE), attach the InformaCast Enabled Loudspeaker Amplifier (PoE)s to the network and configure one at a time to avoid IP address conflicts.

Table 2-7. Factory Default Settings

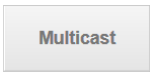
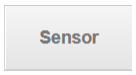
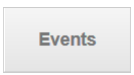
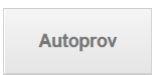
Parameter	Factory Default Setting
IP Addressing	DHCP
IP Address[a]	10.10.10.10
Web Access Username	admin
Web Access Password	admin
Subnet Mask[a]	255.0.0.0
Default Gateway[a]	10.0.0.1

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

2.3.2 InformaCast Enabled Loudspeaker Amplifier (PoE) Web Page Navigation

Table 2-8 shows the navigation buttons that you will see on every InformaCast Enabled Loudspeaker Amplifier (PoE) web page.

Table 2-8. Web Page Navigation

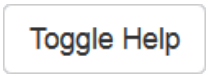
Web Page Item	Description
	Link to the **Home** page.
	Link to the **Device** page.
	Link to the **Network** page.
	Link to go to the **SIP** page.
	Link to the **Multicast** page.
	Link to the **SSL** page.
	Link to the **Sensor** page.
	Link to the **Audiofiles** page.
	Link to the **Events** page.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

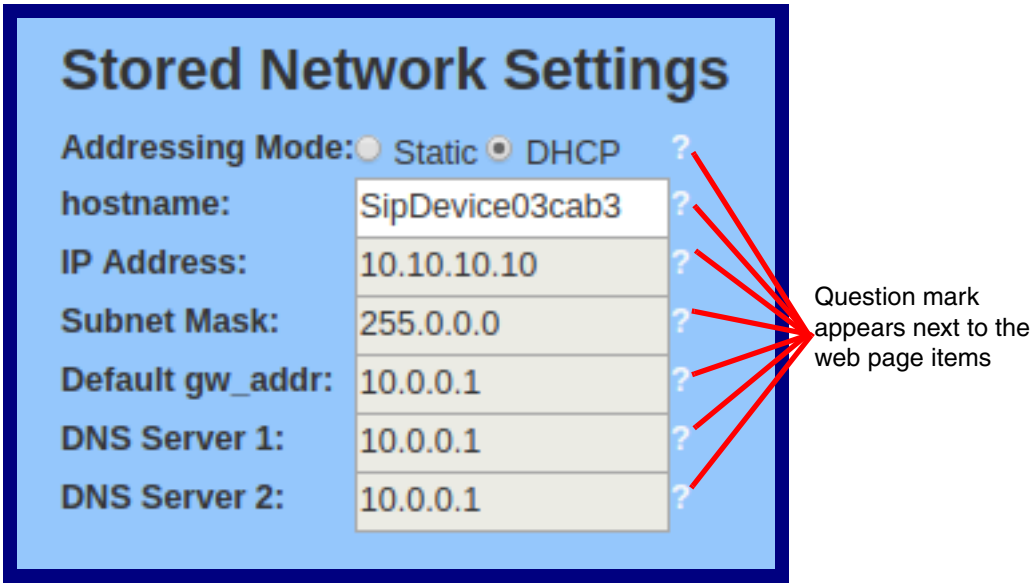
1. Click on the **Toggle Help** button that is on the UI webpage. See Figure 2-22 and Figure 2-23.

Figure 2-22. Toggle/Help Button



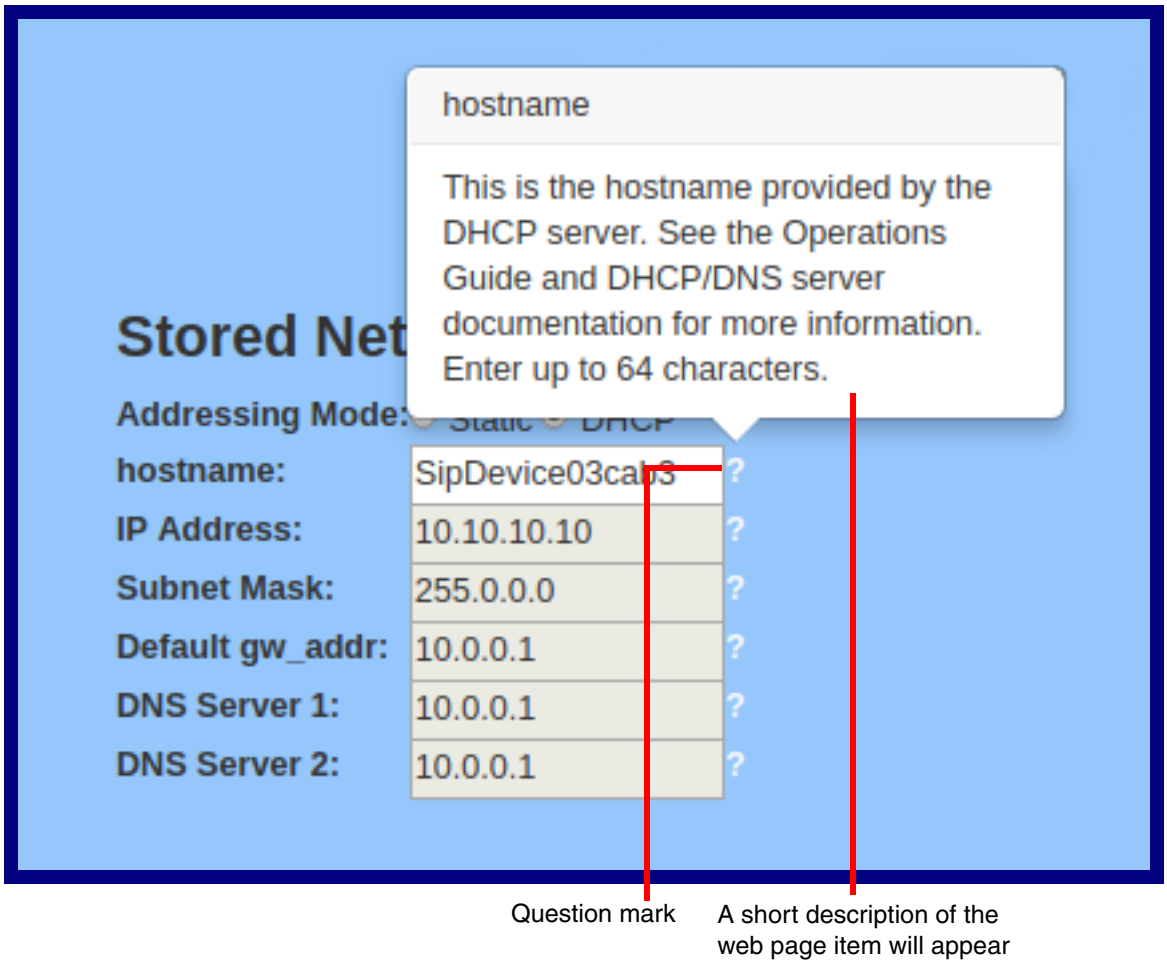
2. You will see a question mark (?) appear next to each web page item that has been provided with a short description by the Help feature. See Figure 2-23.

Figure 2-23. 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 2-24.

Figure 2-24. 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 10.10.10.10.

Note Make sure that the PC is on the same IP network as the InformaCast Enabled Loudspeaker Amplifier (PoE).

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

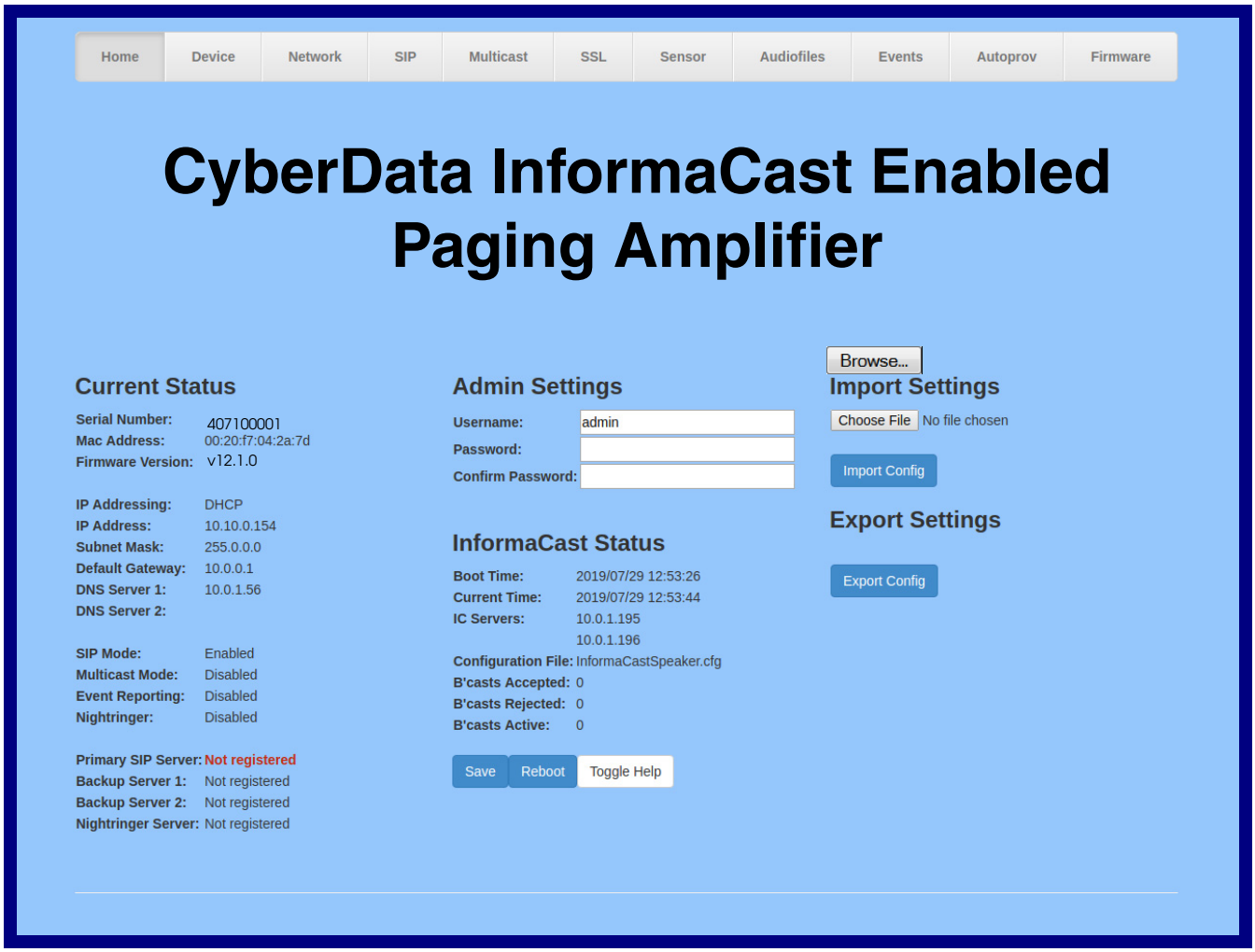
Note The device ships in DHCP mode. To get to the **Home** page, use the discovery utility to scan for the device on the network and open your browser from there.

2. When prompted, use the following default **Web Access Username** and **Web Access Password** to access the **Home Page** (Figure 2-25):

   Web Access Username: **admin**

   Web Access Password: **admin**

Figure 2-25. Home Page



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.
IP Addressing	Shows the current IP addressing setting (**DHCP** or **static**).
IP Address	Shows the current IP address.
Subnet Mask	Shows the current subnet mask address.
Default Gateway	Shows the current default gateway address.
DNS Server 1	Shows the current DNS Server 1 address.
DNS Server 2	Shows the current DNS Server 2 address.
SIP Mode	Shows the current status of the SIP mode.
Multicast Mode	Shows the current status of the Multicast mode.
Event Reporting	Shows the current status of the Event Reporting mode.
Nightringer	Shows the current status of the Nightringer mode.
Primary SIP Server	Shows the current status of the Primary SIP Server.
Backup Server 1	Shows the current status of Backup Server 1.
Backup Server 2	Shows the current status of Backup Server 2.
Nightringer Server	Shows the current status of Nightringer Server.
InformaCast Status	
Boot Time	Shows the boot time.
Current Time	Shows the current time.
IC Servers	Shows the InformaCast server IP addresses.
Configuration File	Shows the configuration file.
B'casts Accepted	Shows the number of B'casts accepted.
B'casts Rejected	Shows the number of B'casts rejected.
B'casts Active	Shows the number of active B'casts.
Import Settings	
Browse...	Use this button to select a configuration file to import.

Table 2-9. Home Page Overview (continued)

Web Page Item	Description
Import Config	After selecting a configuration file, click Import to import the configuration from the selected file. Then, click Save and Reboot to store changes.
Export Settings	
Export Config	Click Export to export the current configuration to a file.
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.
Toggle Help	Click on the **Toggle Help** button to see a short description of some of the web page items. First click on the **Toggle Help** button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

2.3.5 Configure the Device

1. Click the **Device** menu button to open the **Device** page. See Figure 2-26.

Figure 2-26. Device Page

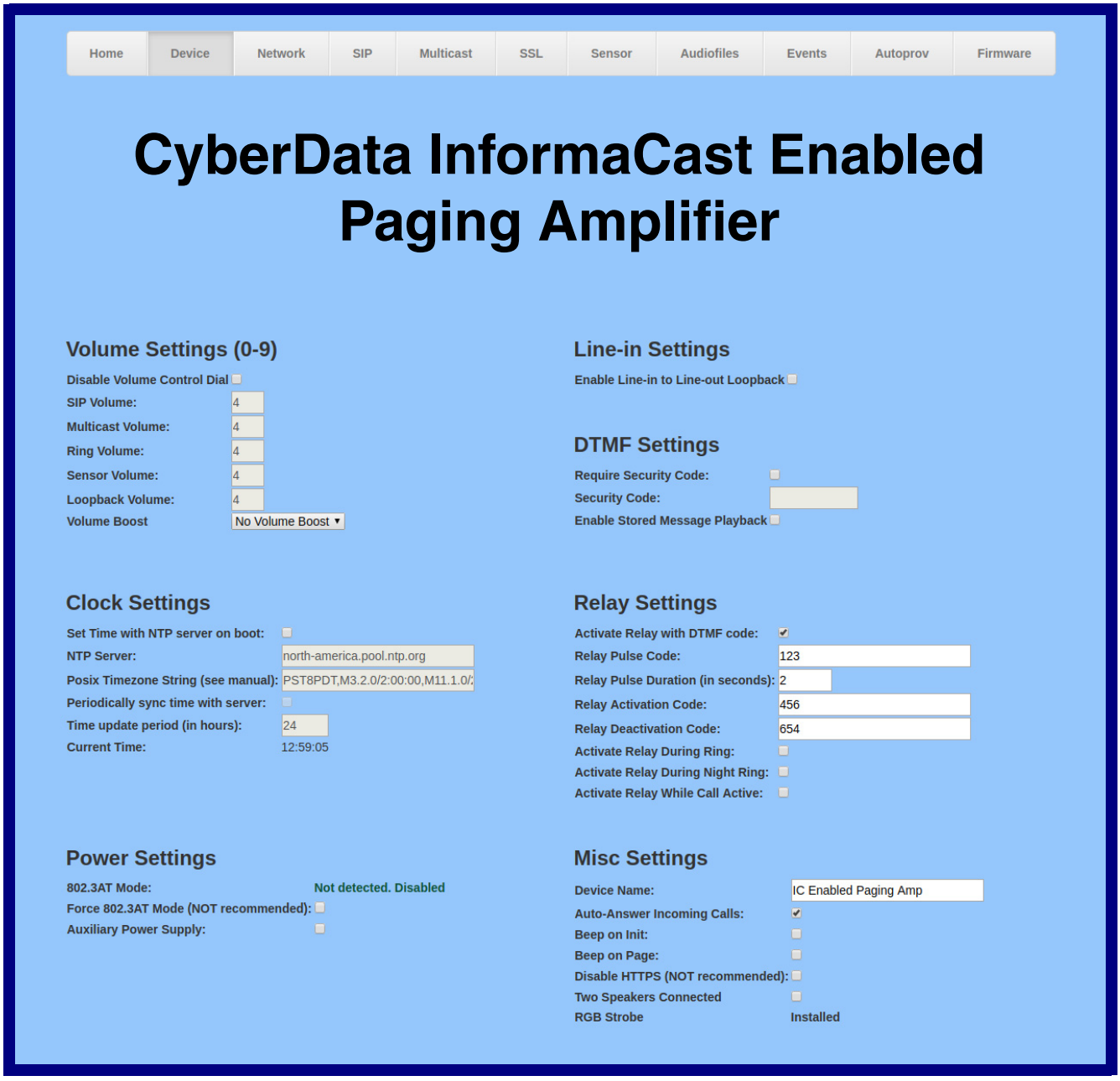
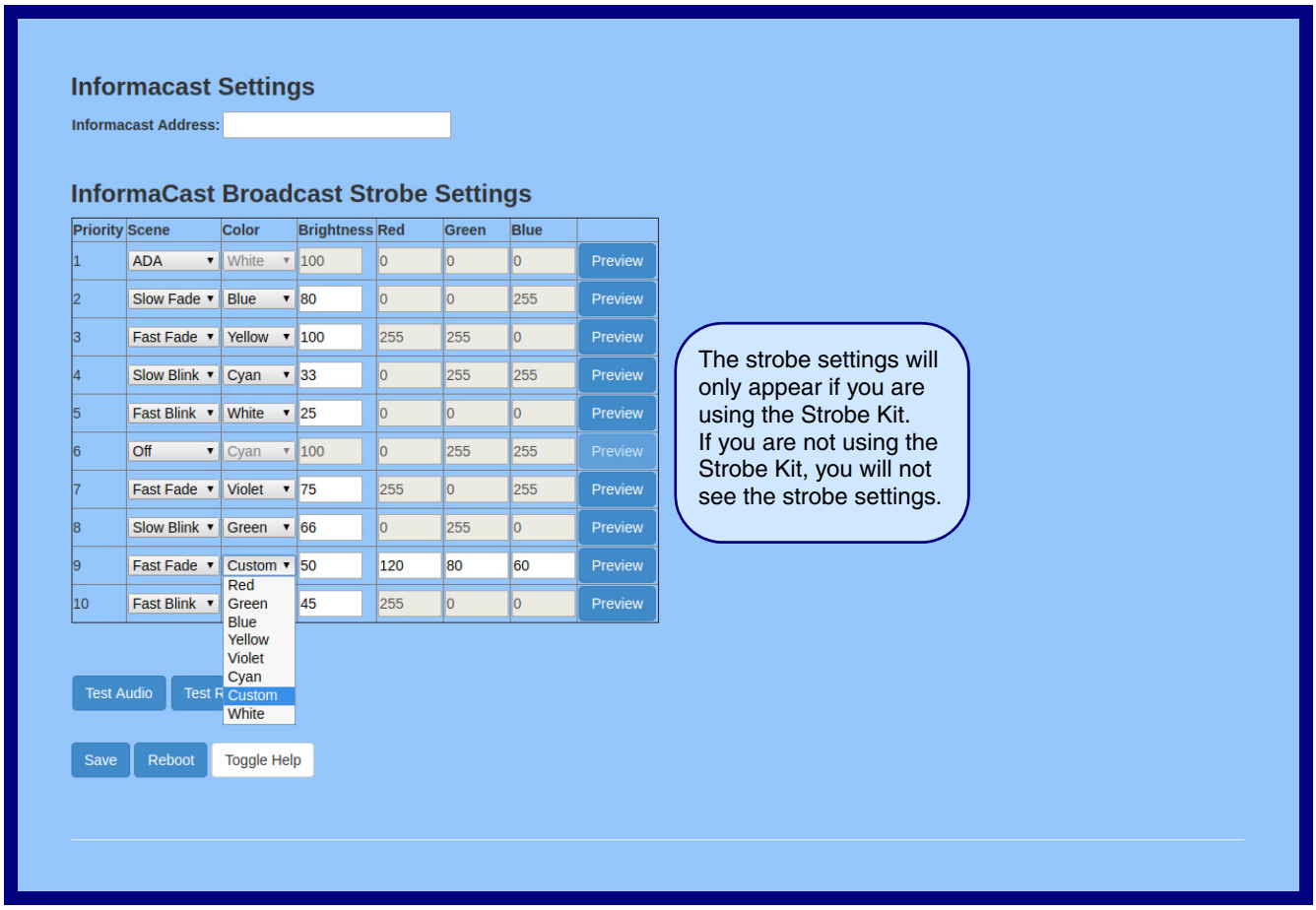


Figure 2-27. Device Page



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
Volume Settings (0-9)	
Disable Volume Control Dial ?	Select this option to disable the volume control dial and enable digital volume control settings.
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 incoming calls. A value of 0 will mute the speaker instead of playing the ring tone when **Auto-Answer Incoming Calls** is disabled.
Sensor Volume ?	Set the speaker volume for playing sensor activated audio. A value of 0 will mute the speaker during sensor activated audio.
Loopback Volume ?	Speaker volume for Line-in Loopback. This value only affects the volume of the speaker(s). Line-out volume must be controlled by the amplifier connected to the line-out port.
Volume Boost: ? No Volume Boost +4dB	Set the Boost level to increase the volume output of the speaker. Using Volume Boost may introduce audio clipping and/or distortion. Boost is only recommended for use with volumes set to level 9.
Clock Settings	
Set Time with NTP Server on boot ?	When selected, the time is set with an external NTP server when the device restarts.
NTP Server ?	Use this field to set the address (in IPv4 dotted decimal notation or as a canonical name) for the NTP Server. This field can accept canonical names of up to 64 characters in length.
Posix Timezone String ?	See Section 2.3.5.1, "Time Zone Strings" for information about how to use the Posix Timezone String to specify time zone and daylight savings time where applicable. Enter up to 63 characters.
Periodically sync time with server ?	When selected, the time is periodically updated with the NTP server at the configured interval below.
Time update period (in hours) ?	The time interval after which the device will contact the NTP server to update the time. Enter up to 4 digits.
Current Time ?	Allows you to input the current time. (6 character limit)
Power Settings	
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.

Table 2-10. Device Page Parameters (continued)

Web Page Item	Description
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).
Auxiliary Power Supply	This device can be connected to a +24VDC auxiliary power supply. Check this box if this is how this speaker is being powered.
Line-In Settings	
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.
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.
Enable Stored Message Playback	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.
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.
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.

Table 2-10. Device Page Parameters (continued)

Web Page Item	Description
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.
Disable HTTPS (NOT recommended)	Disables the encrypted connection to the webpage. We do not recommend disabling HTTPS for security reasons.
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.
InformaCast Settings	
InformaCast Address	Use this field to set the address of your Informacast server. This will override any Informacast server addresses received via SLP or DHCP. If using TFTP for configuration, simply enter an IP address (eg. 10.0.1.195)If using HTTP for configuration, enter the full URL to the path that contains the configuration file. Do not input the file name(eg.http://10.0.1.195:8081/InformaCast/resources/).
Singlewire Broadcast Strobe Settings	For up to 10 Singlewire pages, when a priority is specified for the page, a corresponding strobe scene will be activated. The color may be selected from the drop down menu, or customized by the user with the 0-255 scale. Brightness is specified with a value between 0 and 100. **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.**
Priority	Indicates the priority of the Singlewire broadcast, with 1 the highest priority and 10 the lowest.
Scene	Use this section to select the strobe flashing behavior for the Singlewire Broadcast.
ADA Compliant	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.
Slow Fade	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.
Fast Blink	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.
Color	Select the desired color (only one may be chosen).
Brightness	How bright the strobe will blink when there is a Singlewire Broadcast. This is the maximum brightness for “fade” type scenes.
Red	The red LED value for the Singlewire Broadcast.
Green	The green LED value for the Singlewire Broadcast.
Blue	The blue LED value for the Singlewire Broadcast.

Table 2-10. Device Page Parameters (continued)

Web Page Item	Description
Preview	Use this button to preview the strobe flashing behavior for the **Singlewire Broadcast Strobe Settings**.
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.
Test Relay	Click on the **Test Relay** button to do a relay test.
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.
Toggle Help	Click on the **Toggle Help** button to see a short description of some of the web page items. First click on the **Toggle Help** button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

2.3.5.1 Time Zone Strings

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

Table 2-11. Common Time Zone Strings

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

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

The following table shows a breakdown of the parts that constitute the following time zone string:

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

Table 2-12. Time Zone String Parts

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

Time Zone String Examples

The following table has some more examples of time zone strings.

Table 2-13. Time Zone String Examples

Time Zone	Time Zone String
Tokyo[a]	IST-9
Berlin[b]	CET-1MET,M3.5.0/1:00,M10.5.0/1:00
Adelaide, Australia[c]	ACST-9:30ACDT,M10.1.0/2:00:00,M4.1.0/2:00:00

a.Tokyo does not use daylight savings time.
b.For Berlin, daylight savings time starts on the last Sunday in March at 01:00 UTC, and ends on the last Sunday in October at 01:00 UTC, and is one hour ahead of UTC.
c.Times for those in the Eastern Hemisphere need to have a negative time value.

Time Zone Identifier

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

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

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

World GMT Table

The following table has information about the GMT time in various time zones.

Table 2-14. World GMT Table

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

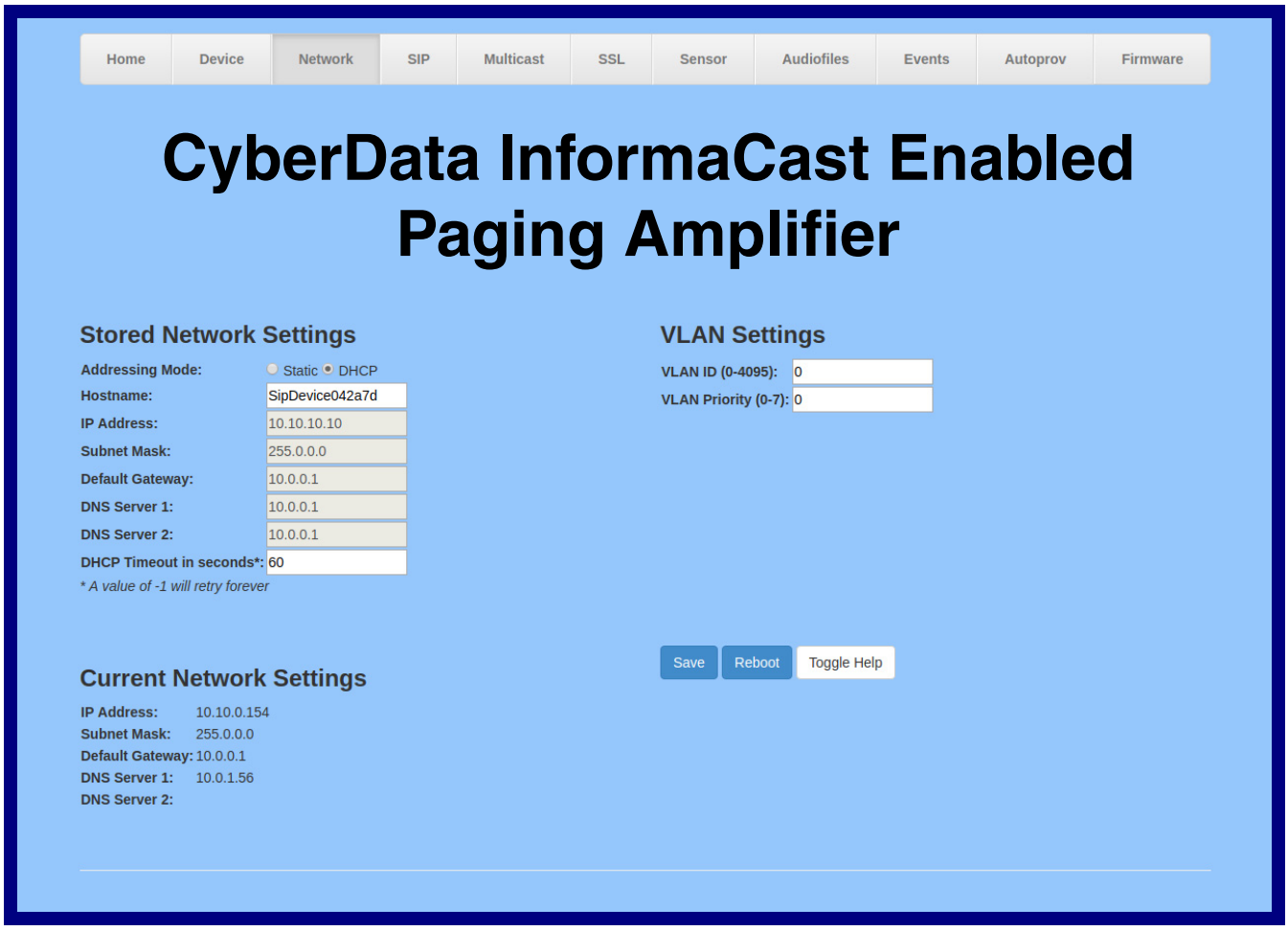
Table 2-14. World GMT Table (continued)

Time Zone	City or Area Zone Crosses
GMT+5	Islamabad, Karachi
GMT+6	Almaty, Dhaka
GMT+7	Bangkok, Jakarta
GMT+8	Hong Kong, Beijing
GMT+9	Tokyo, Osaka
GMT+10	Sydney, Melbourne, Guam
GMT+11	Magadan, Soloman Is.
GMT+12	Fiji, Wellington, Auckland

2.3.6 Configure the Network Parameters

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

Figure 2-28. Network Page



2. On the **Network** 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. 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	Shows the current network settings.
IP Address	Shows the current Static IP address.
Subnet Mask	Shows the current Subnet Mask address.
Default Gateway	Shows the current Default Gateway address.
DNS Server 1	Shows the current DNS Server 1 address.
DNS Server 2	Shows the current DNS Server 2 address.
VLAN Settings	
VLAN ID (0-4095) ?	Specify the IEEE 802.1Q VLAN ID number. Enter up to 4 digits. **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 2-15. Network Page Parameters (continued)

Web Page Item	Description
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.
Toggle Help	Click on the **Toggle Help** button to see a short description of some of the web page items. First click on the **Toggle Help** button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

2.3.7 Configure the SIP (Session Initiation Protocol) Parameters

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

Figure 2-29. SIP Page—Top

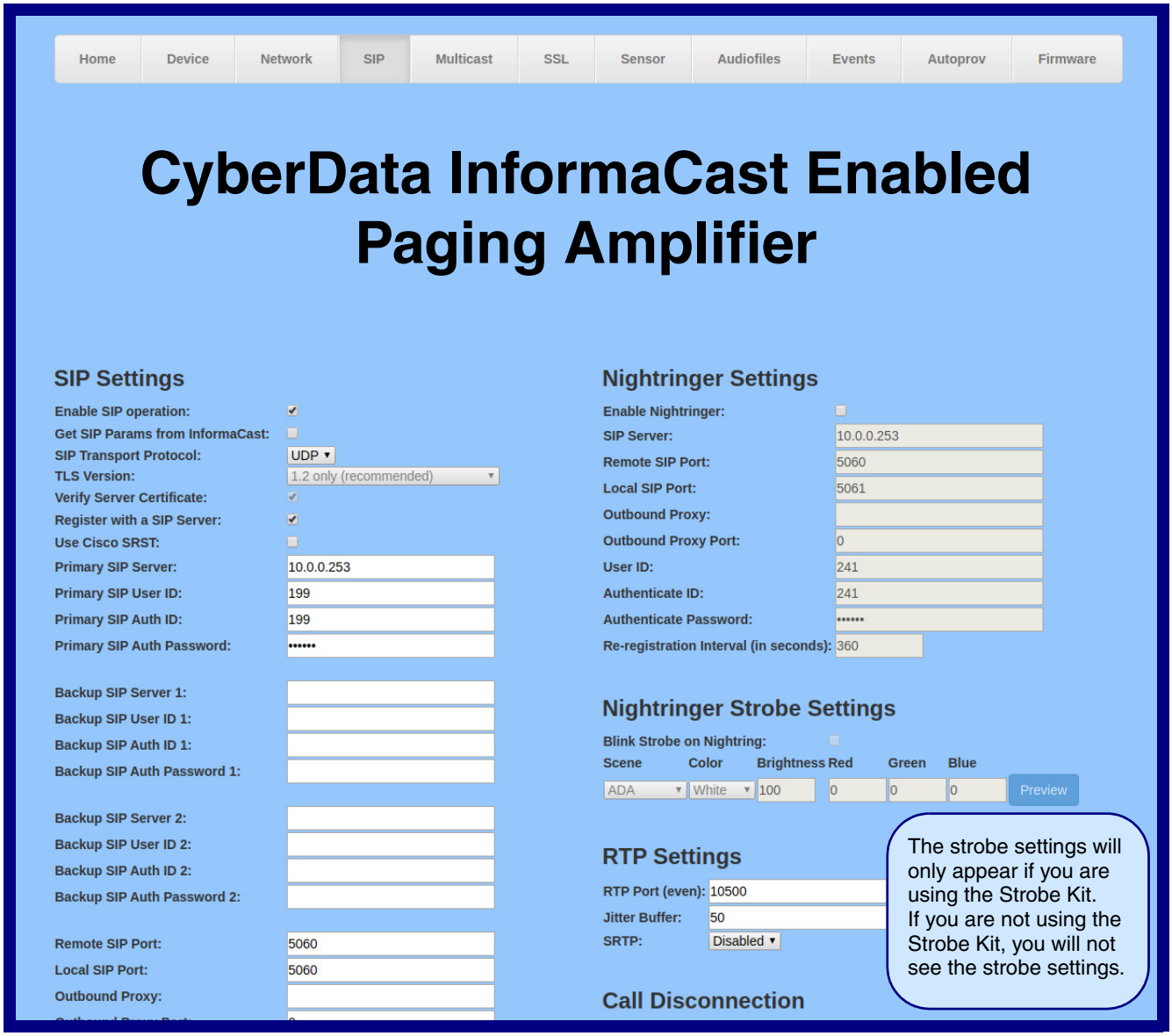
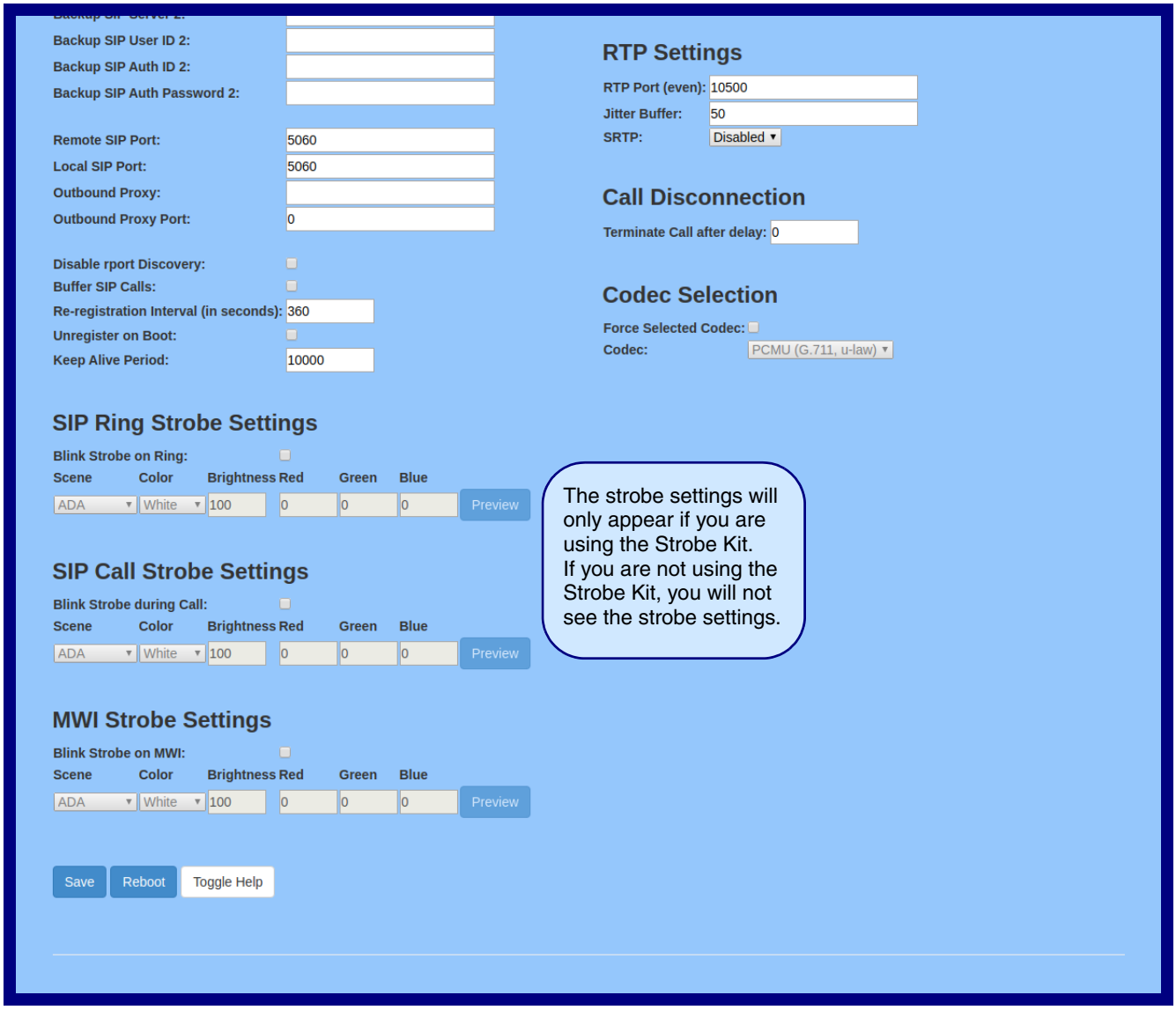


Figure 2-30. SIP Page—Bottom



2. On the **SIP** 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. 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.
Get SIP Params from InformaCast ?	When enabled, the device will get its SIP configuration parameters from the InformaCast server. This will override the manually entered/auto provisioned SIP configuration.
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.
Register with a SIP Server ?	When enabled, the device will attempt to register to the configured SIP Server(s) on this page. To configure the device to send and receive point-to-point SIP calls, enable **SIP Operation** and disable **Register with a SIP Server** (see Section 2.3.7.1, "Point-to-Point Configuration").
Use Cisco SRST ?	When enabled, the backup servers are handled according to Cisco SRST (Survivable Remote Site Telephony). It is required for use in clustered Cisco Unified Communications Manager topologies.
Primary SIP Server ?	Enter the SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the primary SIP server. This field can accept entries of up to 255 characters in length.
Primary SIP User ID ?	Specify the SIP User ID for the Primary SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the primary SIP server. Enter up to 64 alphanumeric characters.
Primary SIP Auth ID ?	Specify the Authenticate ID for the Primary SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Primary SIP Auth Password ?	Specify the Authenticate Password for the Primary SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Server 1 ?	Enter the backup SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the backup SIP server. This field can accept entries of up to 255 characters in length.
Backup SIP User ID 1 ?	Specify the SIP User ID for the first backup SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the first backup SIP server. Enter up to 64 alphanumeric characters.
Backup SIP Auth ID 1 ?	Specify the Authenticate ID for the first backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Auth Password 1 ?	Specify the Authenticate Password for the first backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.

Table 2-16. SIP Page Parameters (continued)

Web Page Item	Description
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.
Backup SIP Auth ID 2	Specify the Authenticate ID for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Auth Password 2	Specify the Authenticate Password for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Remote SIP Port	The Remote SIP Port is the port number the device will use as the destination port when sending SIP messages. The default Remote SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
Local SIP Port	The Local SIP Port is the port number the device will use to receive SIP messages. The default Local SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
Outbound Proxy	Enter the Outbound Proxy address as an IPv4 address in dotted decimal notation or a fully qualified domain name (FQDN). When an IP address is configured, the device will send all SIP messages to this IP address. When an FQDN is configured, the device will run DNS NAPTR, SRV, and A queries on the FQDN to resolve an IP address to which it will send all SIP messages. This field can accept entries of up to 255 characters in length.
Outbound Proxy Port	The Outbound Proxy Port is port number used as the destination port when sending SIP messages to the outbound proxy. A value of 0 will default to 5060. The supported range is 0-65536. Enter up to 5 digits.
Disable rport Discovery	Disabling rport Discovery will prevent the device from including the public WAN IP address and port number in the contact information that is sent to the remote SIP servers. This will generally only need to be enabled when using an SBC or SIP ALG in conjunction with a remote SIP server.
Buffer SIP Calls	Device will buffer audio and play it back after hang up. Length of the buffer varies with codec.
Re-registration Interval (in seconds)	The SIP Re-registration interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
Unregister on Boot	When enabled, the device will send one registration with an expiry of 0 on boot.
Keep Alive Period	The minimum time in milliseconds between keep-alive packets sent for nat traversal. A value of 0 will disable keep alive packets.

Table 2-16. 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.
Preview	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 2-16. SIP Page Parameters (continued)

Web Page Item	Description
Green	The green LED value for SIP Call.
Blue	The blue LED value for SIP Call.
Preview	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.
Preview	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 2-16. 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.
User ID	Specify the SIP User ID for the SIP server. This parameter becomes the user portion of the SIP-URI for the device's Nightringer extension. Enter up to 64 alphanumeric characters.
Authenticate ID	Specify the Authenticate ID for the SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Authenticate Password	Specify the Authenticate Password for the SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Re-registration Interval (in seconds)	The SIP Re-registration Interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
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.
Preview	Use this button to preview the strobe flashing behavior for the **Nightringer Strobe Settings**.

Table 2-16. SIP Page Parameters (continued)

Web Page Item	Description
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.
Jitter Buffer	Specify the size of the jitter buffer (in milliseconds) used for SIP calls. Valid values are 50-1000.
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).
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.
Toggle Help	Click on the **Toggle Help** button to see a short description of some of the web page items. First click on the **Toggle Help** button, and you will see a question mark ( ) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

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

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

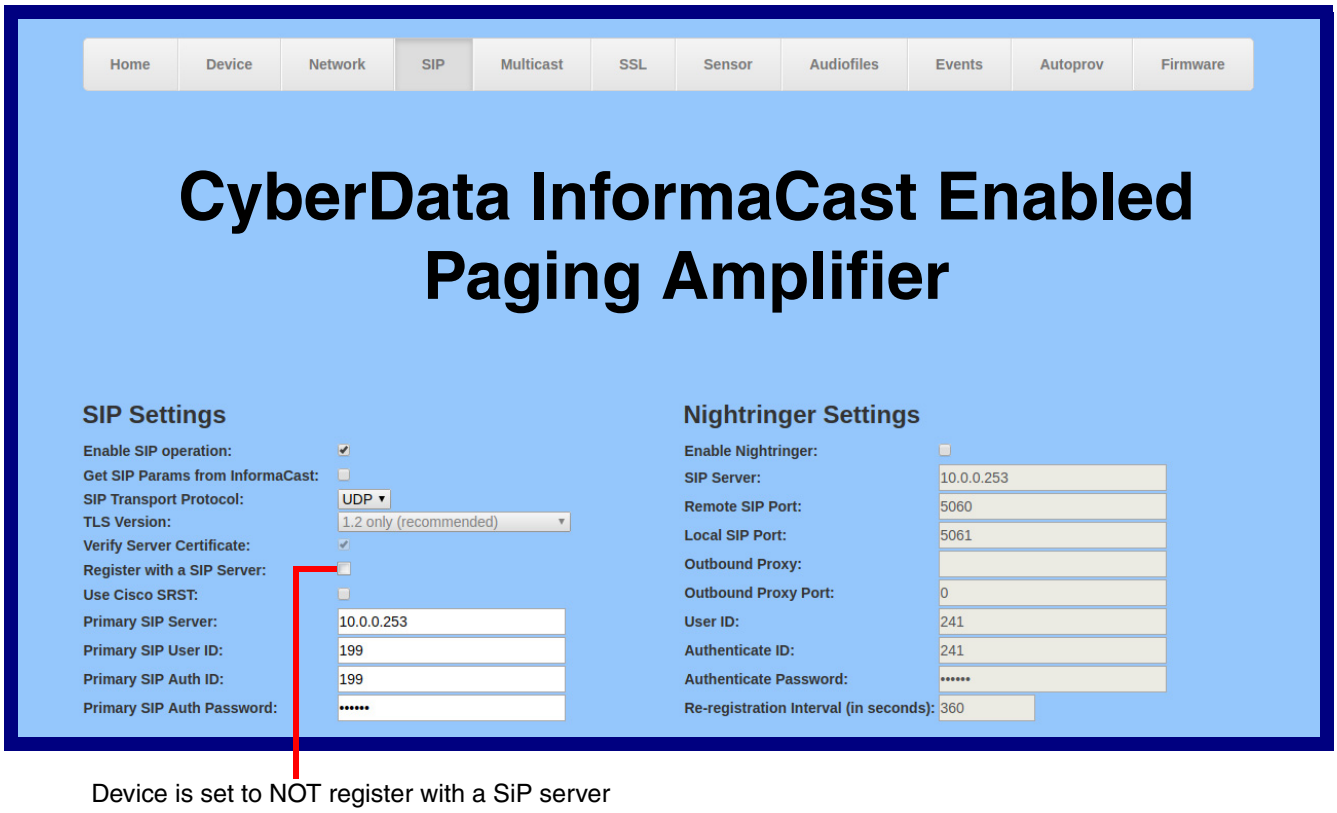
Note The maximum number of total characters in the dial-out field is 64.

2.3.7.1 Point-to-Point Configuration

When the device is set to not register with a SIP server (see Figure 2-31), 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 2-31. SIP Page Set to Point-to-Point Mode



2.3.7.2 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 2-17. Examples of Dial-Out Extension Strings

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

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

2.3.8 Configure the Multicast Parameters

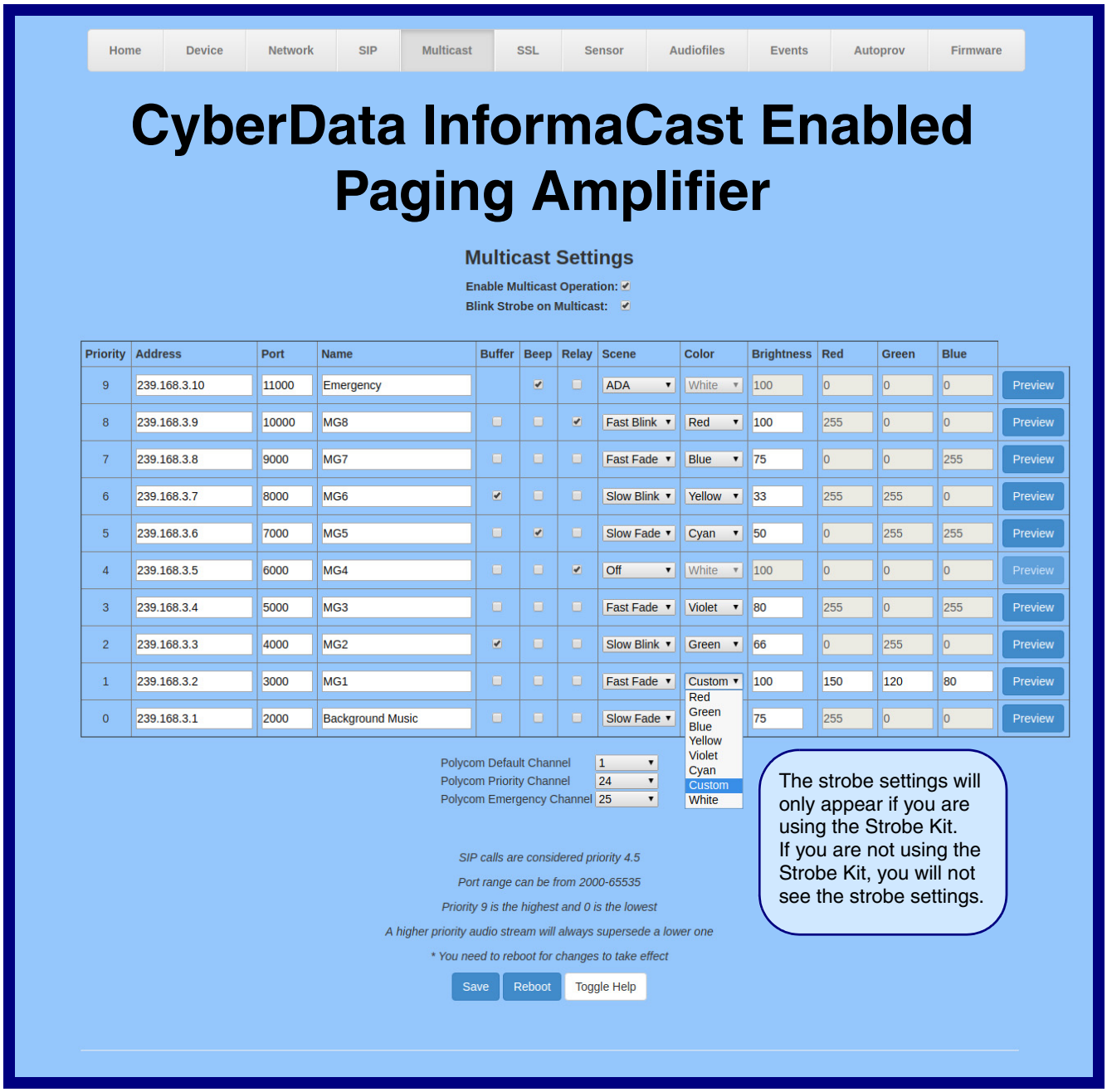
The **Multicast** page allows the device to join up to ten paging zones for receiving ulaw/alaw encoded RTP audio streams.

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 2-32.

Figure 2-32. Multicast Page



2. On the **Multicast** page, enter values for the parameters indicated in Table 2-18.

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

Table 2-18. Multicast Page Parameters

Web Page Item	Description
Enable Multicast Operation	Enables or disables multicast operation.
Blink Strobe on Multicast ?	When selected, the Strobe will blink a scene when a multicast is received. **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.**
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 2.3.8.1, "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.
Color ?	Select desired color (only one may be chosen).
Brightness ?	How bright the strobe will blink on a multicast page. This is the maximum brightness for “fade” type scenes.
Red ?	The red LED value for Multicast.
Green ?	The green LED value for Multicast.
Blue ?	The blue LED value for Multicast.

Table 2-18. 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.
Preview	Use this button to preview the strobe flashing behavior for the **Multicast Strobe Settings**.
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.
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.

2.3.8.1 Assigning Priority

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

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

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

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

Ringtones and Nightringtones

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

2.3.9 Configure the SSL Parameters

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

Figure 2-33. SSL Configuration Page

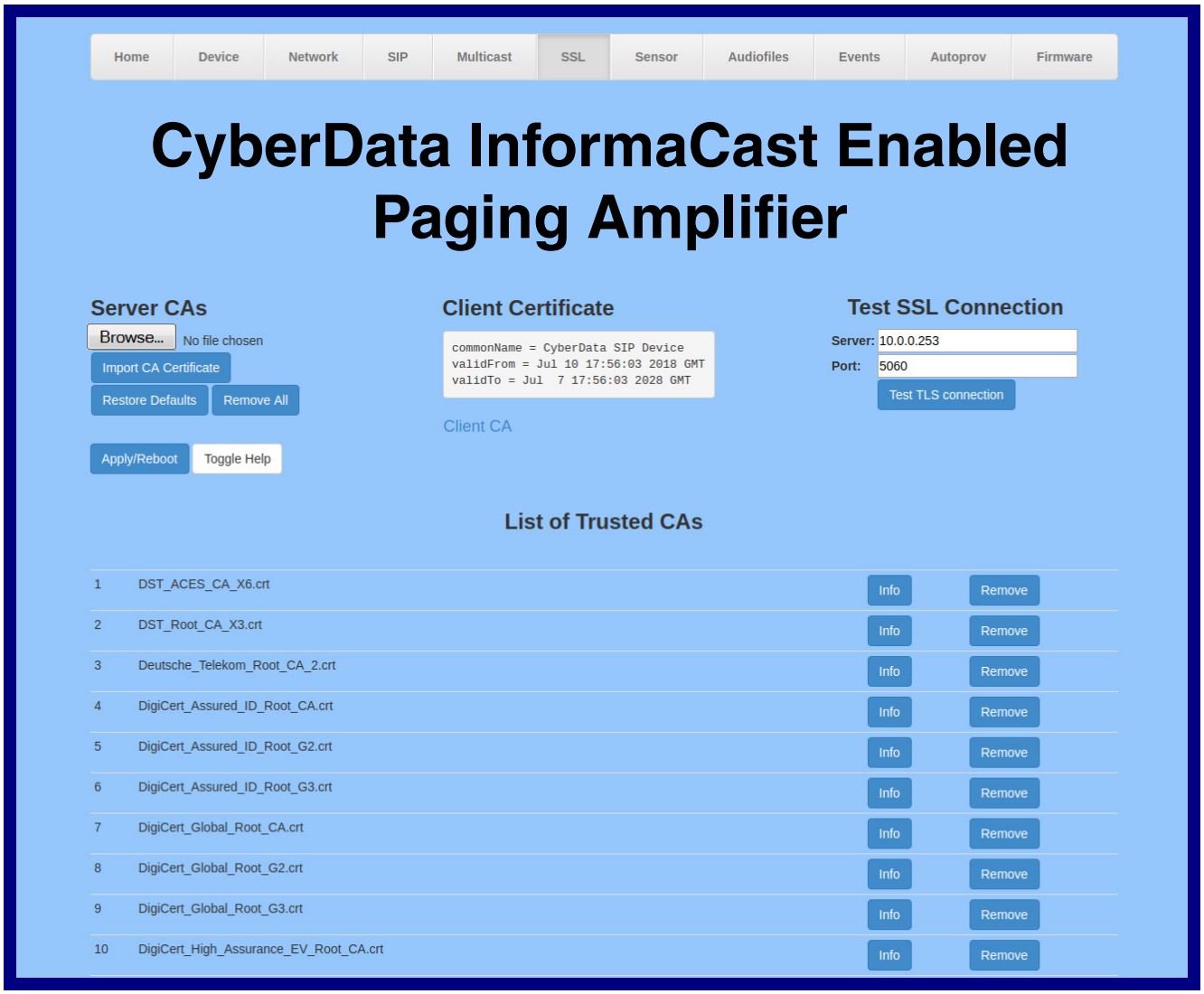
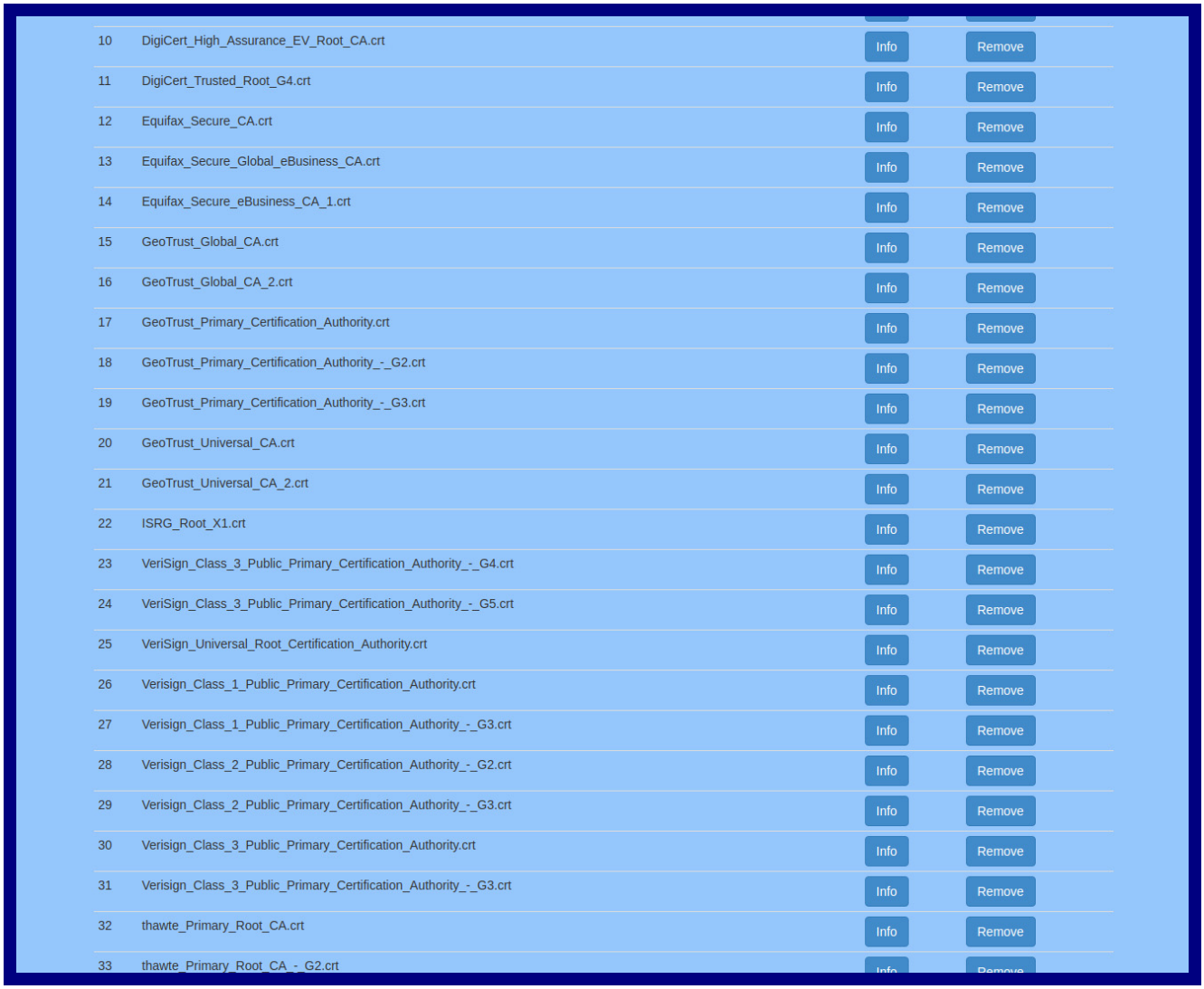
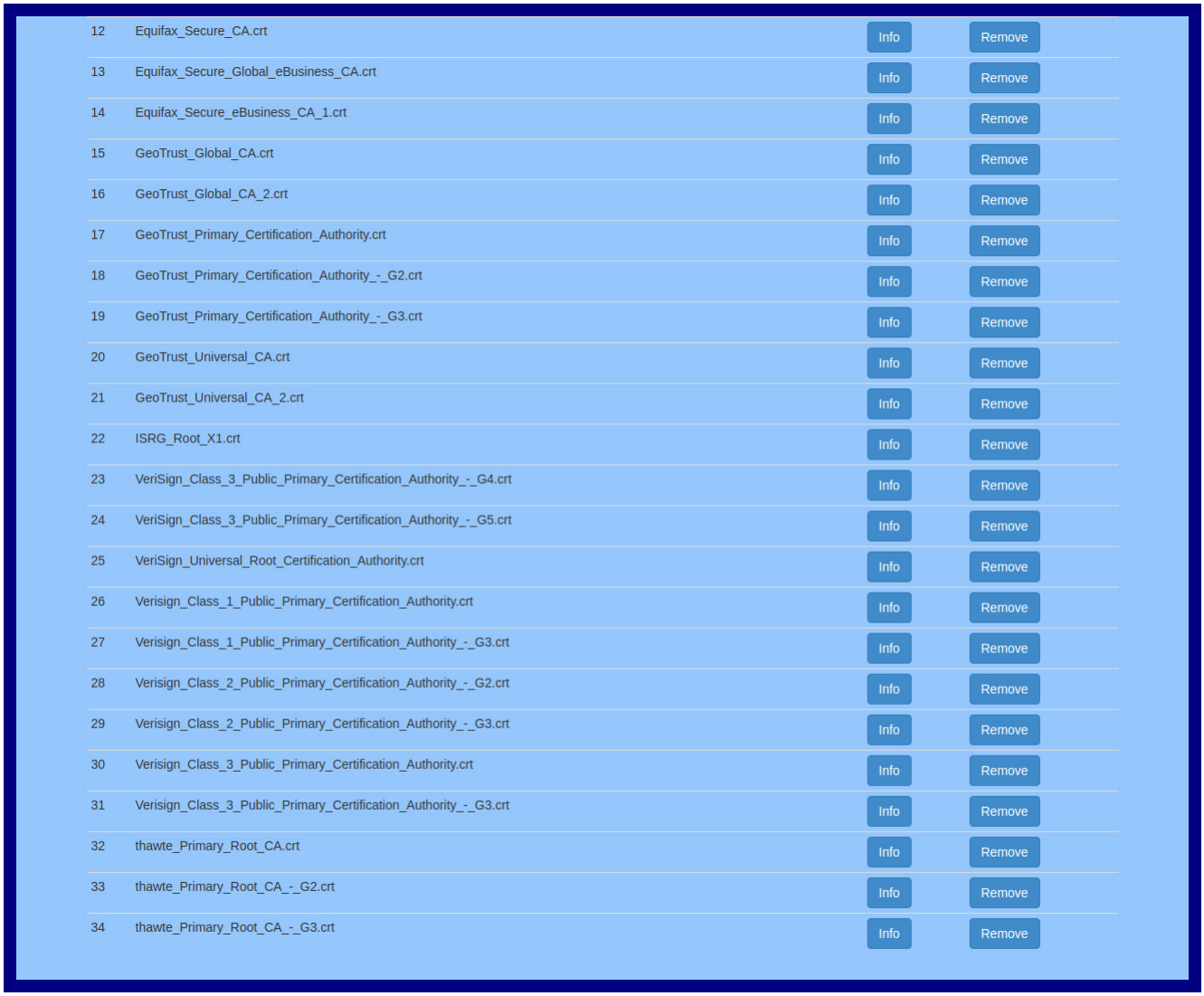


Figure 2-34. SSL Configuration Page



10	DigiCert_High_Assurance_EV_Root_CA.crt	Info	Remove
11	DigiCert_Trusted_Root_G4.crt	Info	Remove
12	Equifax_Secure_CA.crt	Info	Remove
13	Equifax_Secure_Global_eBusiness_CA.crt	Info	Remove
14	Equifax_Secure_eBusiness_CA_1.crt	Info	Remove
15	GeoTrust_Global_CA.crt	Info	Remove
16	GeoTrust_Global_CA_2.crt	Info	Remove
17	GeoTrust_Primary_Certification_Authority.crt	Info	Remove
18	GeoTrust_Primary_Certification_Authority_-_G2.crt	Info	Remove
19	GeoTrust_Primary_Certification_Authority_-_G3.crt	Info	Remove
20	GeoTrust_Universal_CA.crt	Info	Remove
21	GeoTrust_Universal_CA_2.crt	Info	Remove
22	ISRG_Root_X1.crt	Info	Remove
23	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G4.crt	Info	Remove
24	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5.crt	Info	Remove
25	VeriSign_Universal_Root_Certification_Authority.crt	Info	Remove
26	Verisign_Class_1_Public_Primary_Certification_Authority.crt	Info	Remove
27	Verisign_Class_1_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
28	Verisign_Class_2_Public_Primary_Certification_Authority_-_G2.crt	Info	Remove
29	Verisign_Class_2_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
30	Verisign_Class_3_Public_Primary_Certification_Authority.crt	Info	Remove
31	Verisign_Class_3_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
32	thawte_Primary_Root_CA.crt	Info	Remove
33	thawte_Primary_Root_CA_-_G2.crt	Info	Remove

Figure 2-35. SSL Configuration Page



2. On the **SSL** 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.

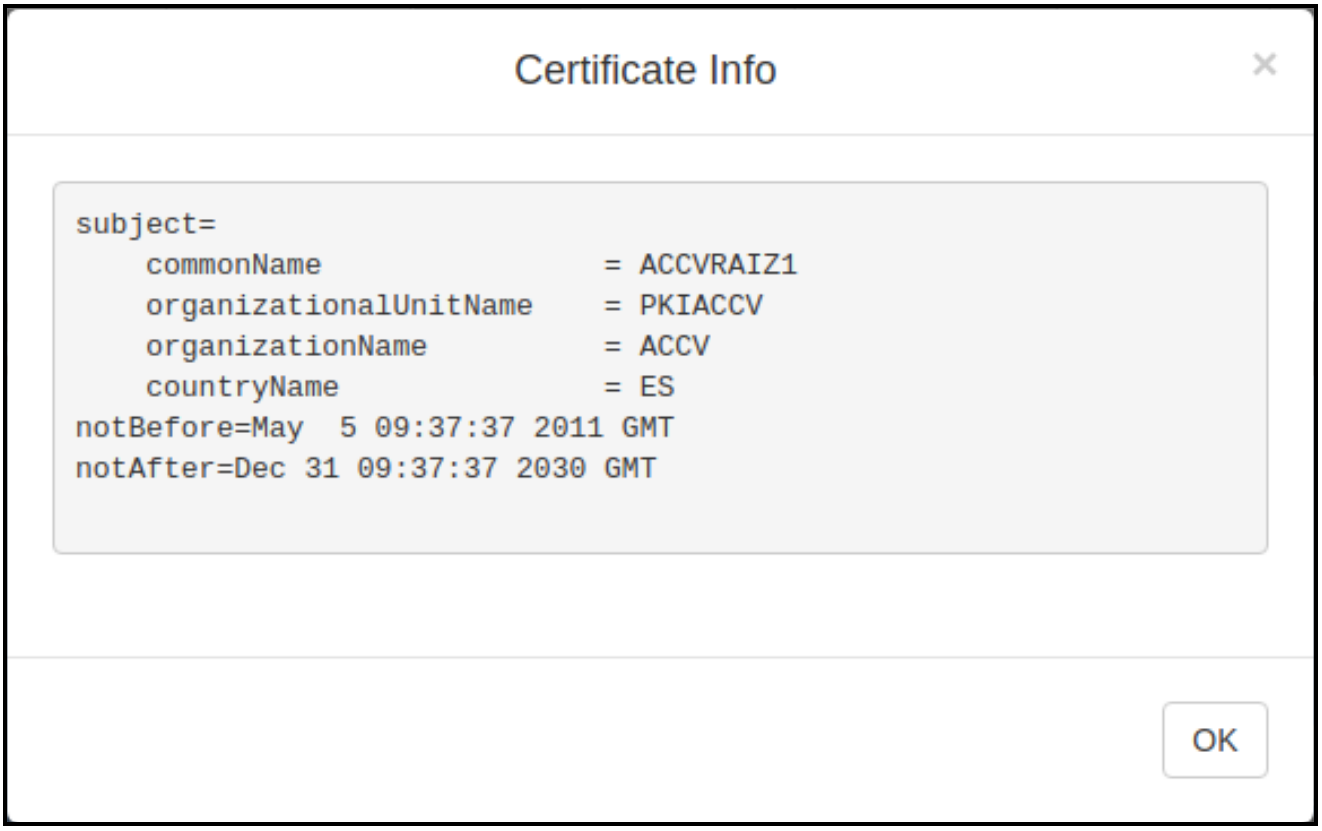
Table 2-19. SSL Configuration Parameters

Web Page Item	Description
Server CAs	
Browse...	Use this button to select a configuration file to import.
Import CA Certificate	Click **Browse** to select a CA certificate to import. After selecting a server certificate authority (CA), click **Import CA Certificate** to import it to the list of trusted CAs. CAs are used to validate the certificate presented by the server when establishing a TLS connection.
Restore Defaults	**Restore Defaults** will restore the default list of registered CAs and **Remove All** will remove all registered CAs.
Remove All	**Restore Defaults** will restore the default list of registered CAs and **Remove All** will remove all registered CAs.
Apply/Reboot	Reboots the device and applies settings and activates imported certificates.
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.
Client Certificate	When doing mutual authentication this device will present a client certificate with these parameters.
Client CA ?	Right click and **Save Link As...** to get the Cyberdata CA used to sign this client certificate.
Test SSL Connection	
Server ?	The ssl test server address as a fully qualified domain name or in IPv4 dotted decimal notation.
Port ?	The ssl test server port. The supported range is 0-65536. SIP connections over TLS to port 5060 will do the same.
Test TLS connection	Use this button to test a TLS connection to a remote server. This will attempt to make a socket connection to the configured test server and port and report the success or failure. This can be used to debug TLS connection issues separate from SIP registration issues.
List of Trusted CAs	
Info	Provides details of the certificate. After clicking on this button, the **Certificate Info Window** appears. See Section 2.3.9.1, "Certificate Info Window".
Remove	Removes this certificate from the list of trusted certificates. After clicking on this button, the **Remove Server Certificate Window** appears. See Section 2.3.9.2, "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 2-36.

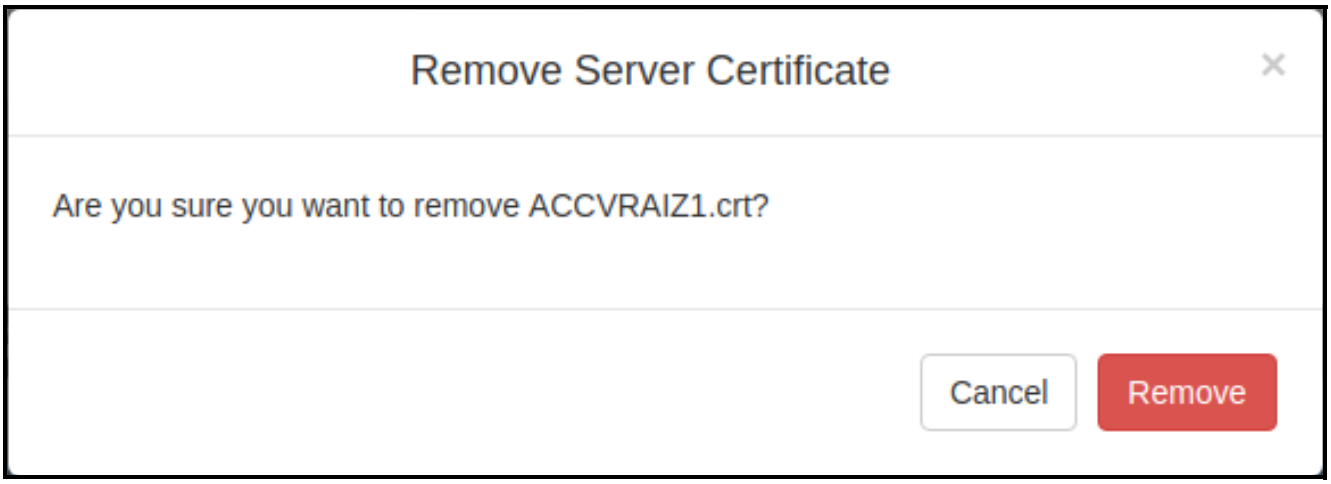
Figure 2-36. Certificate Info Window



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 2-37.

Figure 2-37. Remove Server Certificate Window



2.3.10 Configure the Sensor Page Parameters

The door sensor (pins 1 and 2) 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 (in seconds)** parameter has been met.

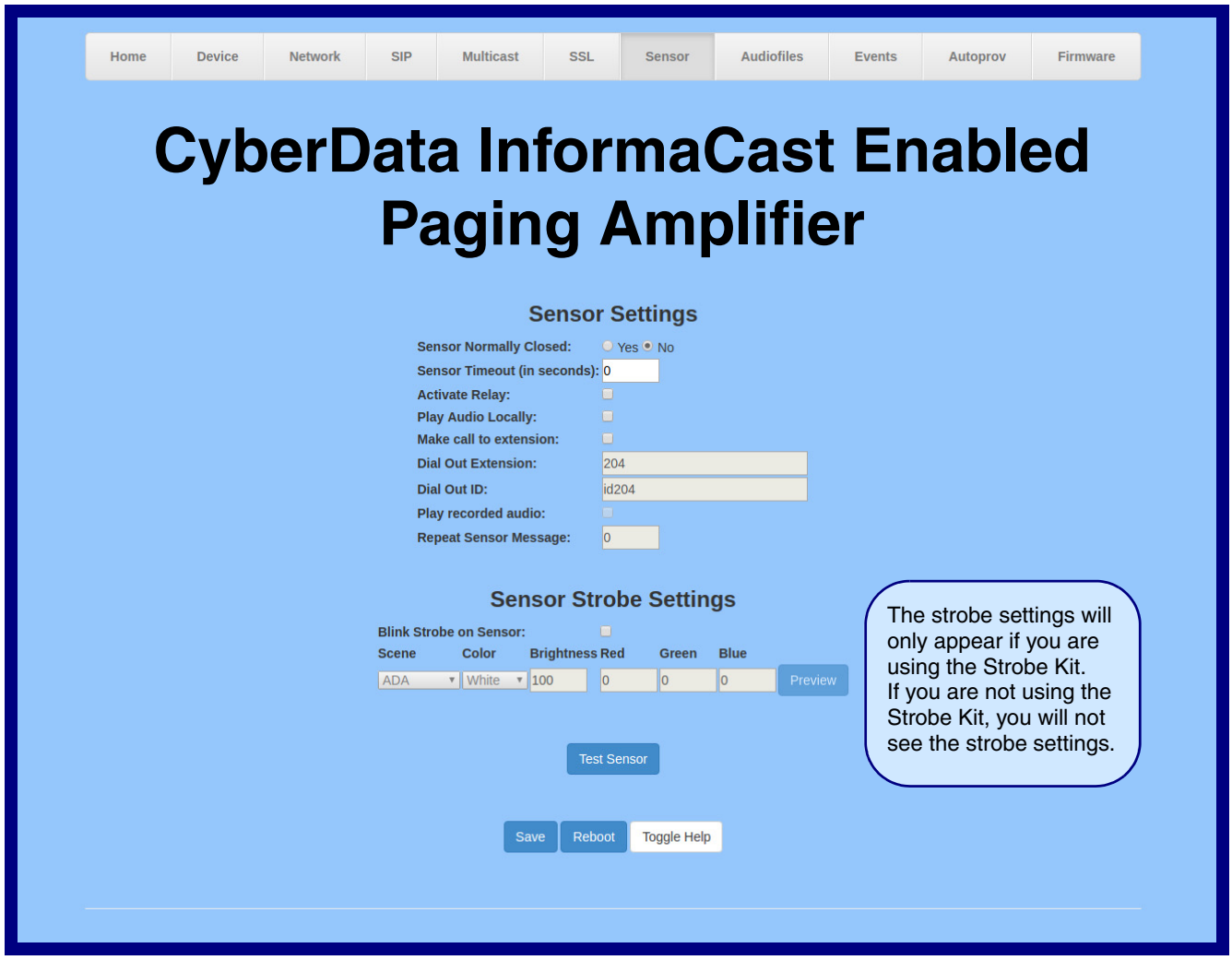
Each sensor can trigger up to five different actions:

- Flash the LED until the sensor is deactivated (roughly 10 times/second)
- 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 establish two way audio
- 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 2-38).

Figure 2-38. Sensor Page



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

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

Table 2-20. 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 (in seconds) ?	The time (in seconds) the device will wait before it performs an action when the on-board door sensor is activated. The action(s) performed are based on the configured 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.
Play Audio Locally ?	When selected, the device will loop an audio file out of the speaker until the 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 recorded audio ?	When selected, the device will call the **Dial Out Extension** and play an audio file to the phone answering the SIP call (corresponds to **Sensor Triggered** on the **Audiofiles Page** page).
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.

Table 2-20. Sensor Page Parameters (continued)

Web Page Item	Description
Fast Blink	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.
Color	Select desired color (only one may be chosen).
Brightness	How bright the strobe will blink when the sensor is triggered. This is the maximum brightness for “fade” type scenes.
Red	The red LED value for Sensor.
Green	The green LED value for Sensor.
Blue	The blue LED value for Sensor.
Test Sensor	Click the **Test Sensor** button to test the sensor.
Preview	Use this button to preview the strobe flashing behavior for the **Sensor Strobe Settings**.
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.
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.

2.3.11 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 2-39).

Figure 2-39. Audiofiles Page

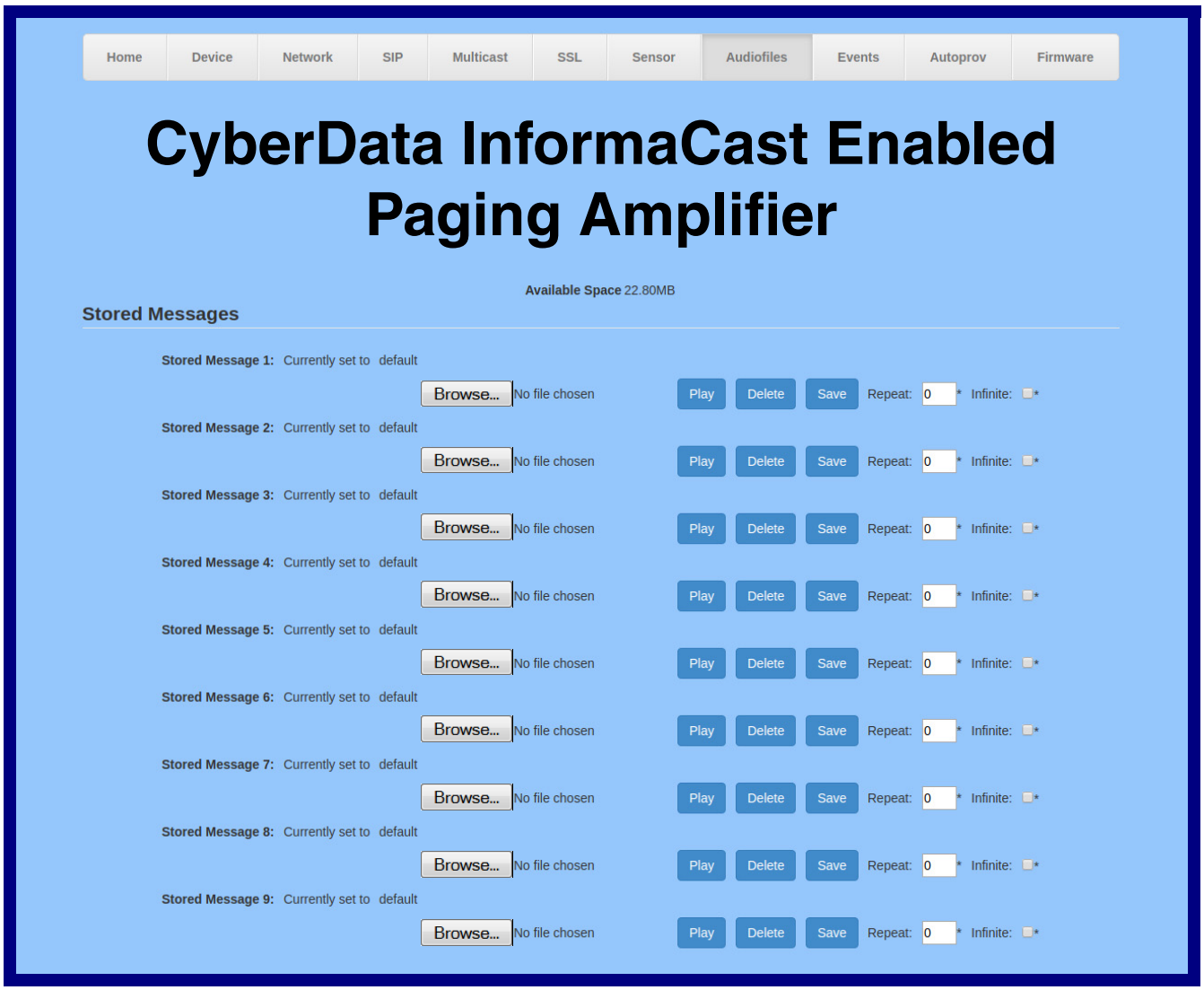


Figure 2-40. Audiofiles Page

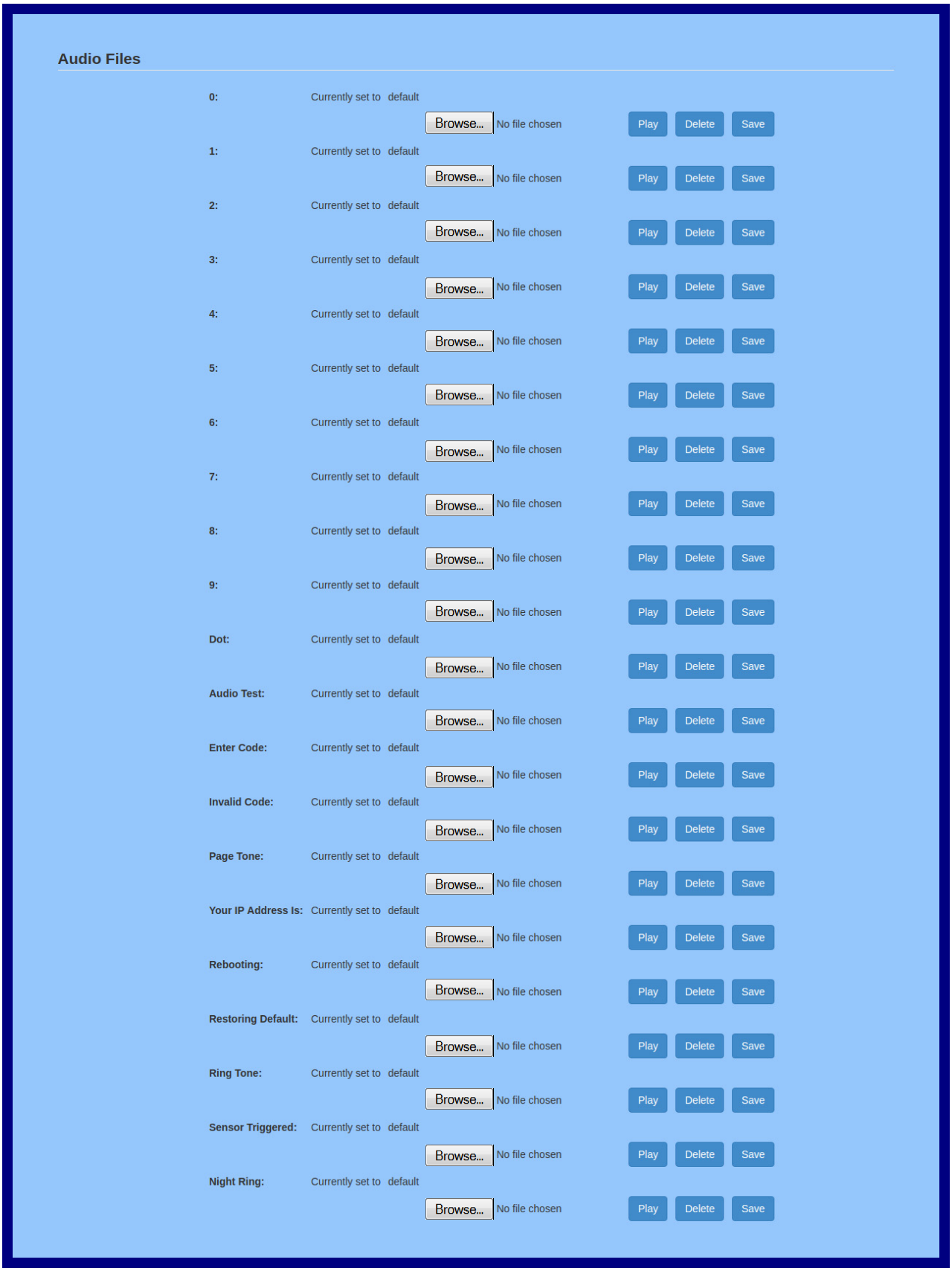


Figure 2-41. Audiofiles Page

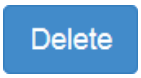
2. On the **Audiofiles** page, enter values for the parameters indicated in Table 2-21.

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

Table 2-21. Audiofiles Page Parameters

Web Page Item	Description
Available Space	Shows the space available for the user to save custom audio files if they want to change the message when the door or sensor is triggered.
Stored Messages	
Stored Message 1 through 9	**Stored Message 1** corresponds to the message played after pressing **1** on a phone keypad. **Stored Message 2** corresponds to the message played after pressing **2** on a phone keypad. **Stored Message 3** corresponds to the message played after pressing **3** on a phone keypad. **Stored Message 4** corresponds to the message played after pressing **4** on a phone keypad. **Stored Message 5** corresponds to the message played after pressing **5** on a phone keypad. **Stored Message 6** corresponds to the message played after pressing **6** on a phone keypad. **Stored Message 7** corresponds to the message played after pressing **7** on a phone keypad. **Stored Message 8** corresponds to the message played after pressing **8** on a phone keypad. **Stored Message 9** corresponds to the message played after pressing **9** on a phone keypad.
Audio Files	
0-4	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.”
5-9	The name of the audio configuration option is the same as the spoken audio that plays on the board (24 character limit). '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.”
Dot	Corresponds to the spoken word “dot.” (24 character limit)
Audio Test	Corresponds to the message ***“This is the CyberData IP speaker test message...”*** (24 character limit)
Enter Code	Corresponds to the message “Enter Code” (24 character limit).
Invalid Code	Corresponds to the message “Invalid Code” (24 character limit).
Page Tone	Corresponds to a simple tone used for beep on initialization and beep on page (24 character limit).
Your IP Address is	Corresponds to the message “Your IP address is...” (24 character limit).
Rebooting	Corresponds to the spoken word “Rebooting” (24 character limit).

Table 2-21. Audiofiles Page Parameters (continued)

Web Page Item	Description
Restoring Default	Corresponds to the message “Restoring default” (24 character limit).
Ring Tone	This is the tone that plays when set to ring when receiving a call (24 character limit).
Sensor Triggered	Corresponds to the message “Sensor Triggered” (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.
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).
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).
	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.

2.3.11.1 User-created Audio Files

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

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

You can use the free utility *Audacity* to convert audio files into this format. See Figure 2-42 through Figure 2-44.

Figure 2-42. Audacity 1

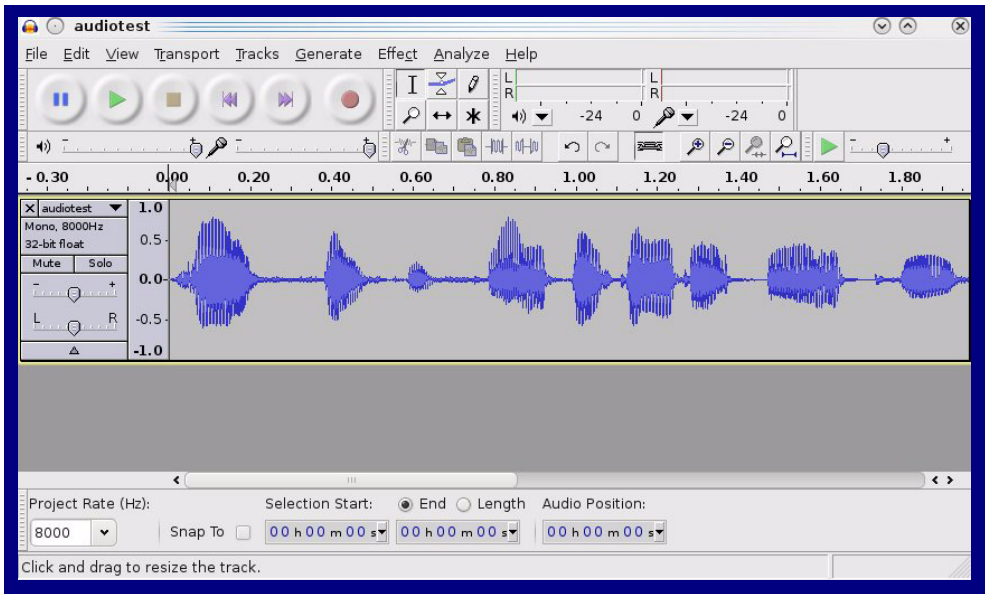
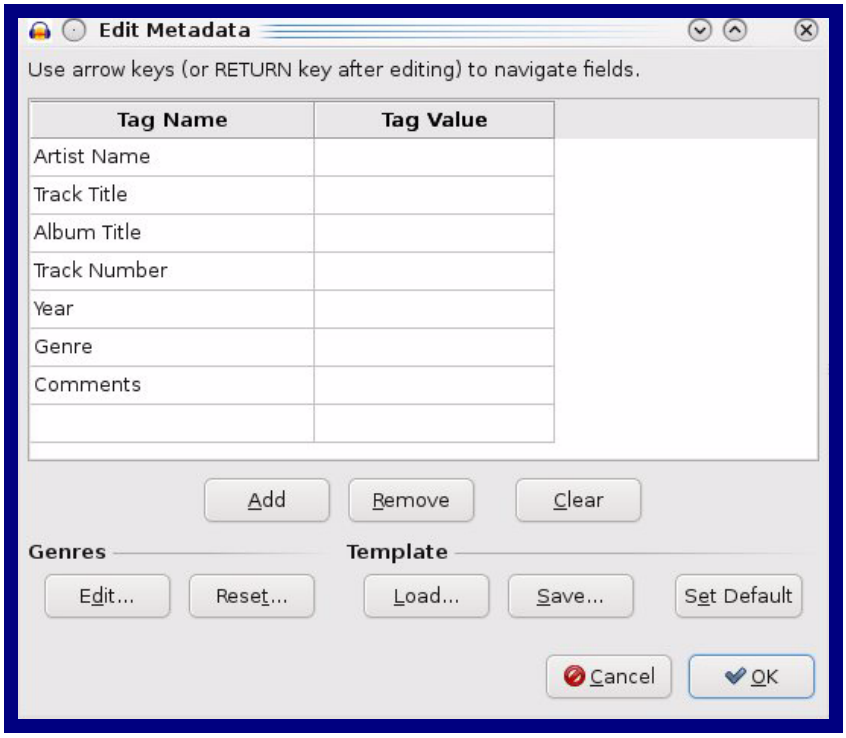


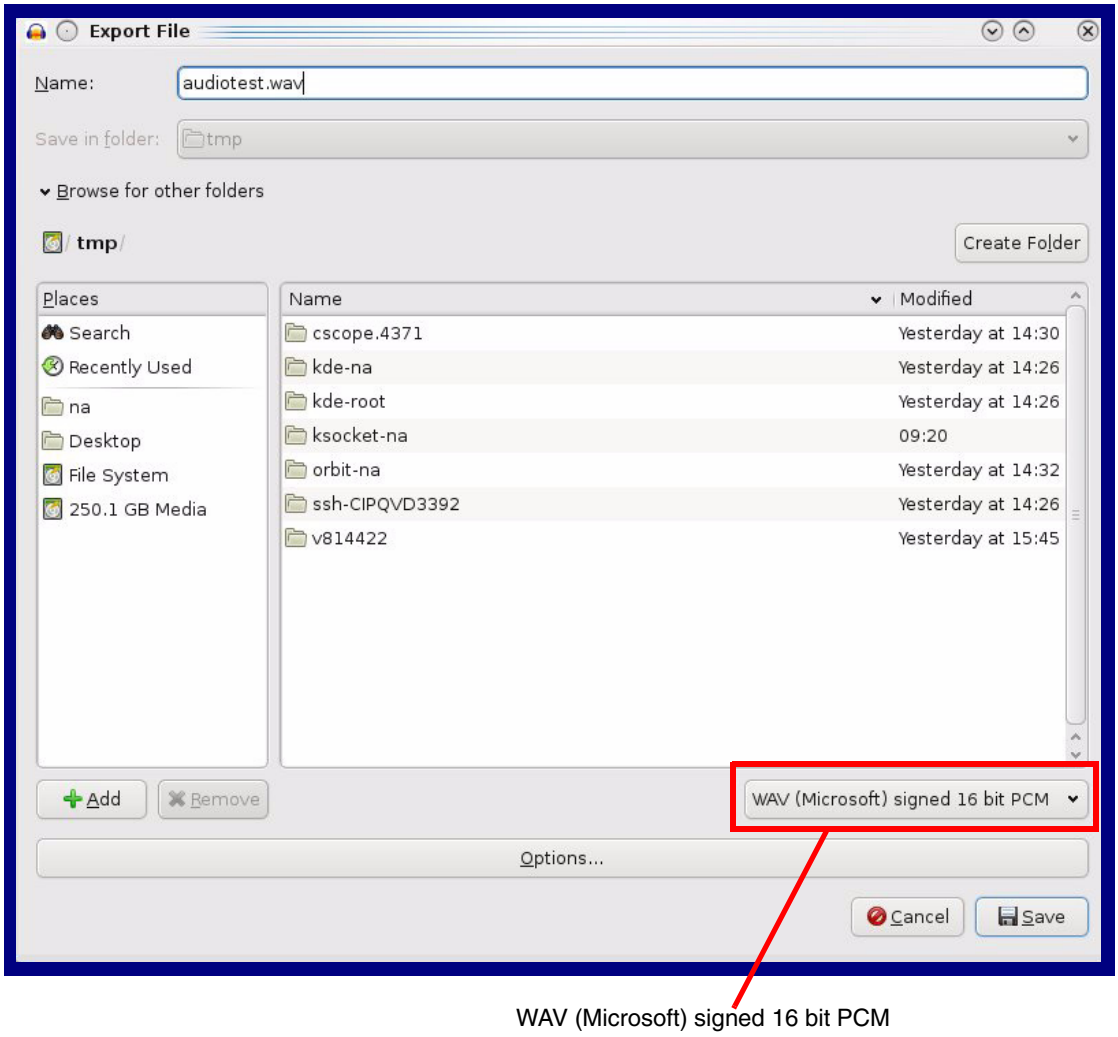
Figure 2-43. Audacity 2



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

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

Figure 2-44. WAV (Microsoft) signed 16 bit PCM



2.3.12 Configure the Events Parameters

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

1. Click on the **Events** menu button to open the **Events** page (Figure 2-45).

Figure 2-45. Events Page

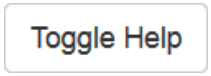
2. On the **Events** page, enter values for the parameters indicated in Table 2-22.

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

Table 2-22. 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.
Enable Singlewire Start Events ?	When selected, the device will report when a Start event has been received from the Singlewire server.
Enable Singlewire Stop Events ?	When selected, the device will report when a Stop event has been received from the Singlewire server.
Check All	Click on **Check All** to select all of the events on the page.
Uncheck All	Click on **Uncheck All** to de-select all of the events on the page.
Event Server	
Server IP Address ?	The IPv4 address of the event server in dotted decimal notation.
Server Port ?	Specify the event server port number. The supported range is 0-65536. Enter up to 5 digits.
Server URL ?	Generally, the destination URL is the name of the application that receives the events and the string in the HTTP POST command. It can be a script used to parse and process the HTTP POST events. Enter up to 127 characters.
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.

Table 2-22. Events Page 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.

2.3.12.1 Example Packets for Events

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

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

Here are example packets for every event:

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

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData 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>
```

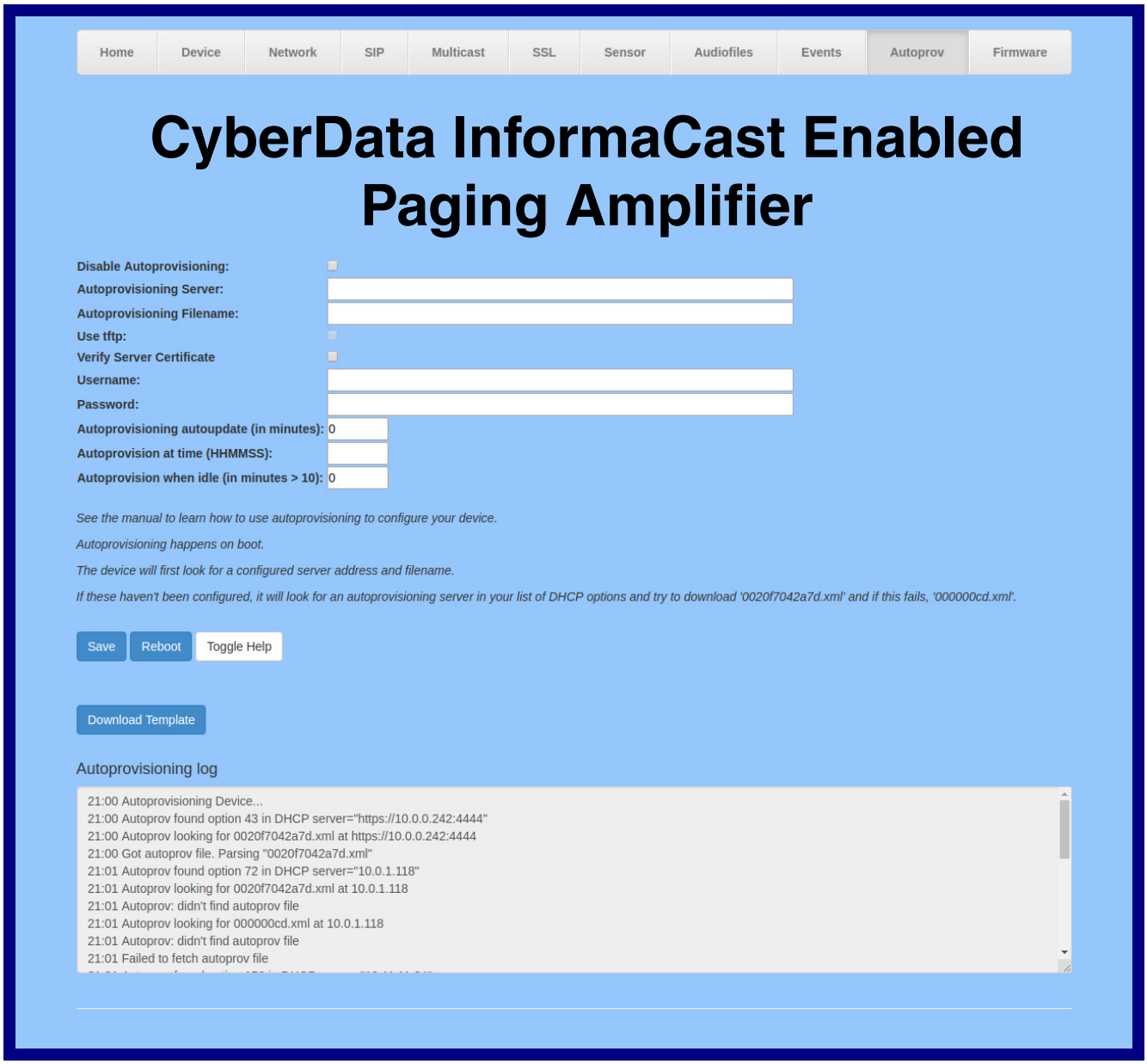
2.3.13 Configure the Autoprovisioning Parameters

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

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

1. Click the **Autoprov** menu button to open the **Autoprovisioning** page. See Figure 2-46.

Figure 2-46. Autoprovisioning Page



2. On the **Autoprovisioning** page, you may enter values for the parameters indicated in Table 2-23.

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 2-23. Autoprovisioning Page Parameters

Web Page Item	Description
Disable Autoprovisioning ?	Prevent the device from automatically trying to download a configuration file. See Section 2.3.13.1, "Autoprovisioning" for more information.
Autoprovisioning Server ?	Enter the IPv4 address of the provisioning server in dotted decimal notation.
Autoprovisioning Filename ?	The autoprovisioning filename is the configuration filename. The default autoprovisioning filename is in the format of **<mac address>.xml**. Supported filename extensions are .txt, and .xml. The current filename is denoted by an asterisk at the bottom of the **Autoprovisioning Page**. Enter up to 256 characters. A file may have any name with an xml extension. If a file name is entered, the device will look for the specified file name, and only that file.
Use tftp ?	The device will use TFTP (instead of http) to download autoprovisioning files.
Verify Server Certificate ?	When using ssl to download autoprovisioning files, reject connections where the server address doesn't match the server certificate's common name.
Username ?	The username used to authenticate with an autoprovisioning server. Leave this field blank to disable authentication.
Password ?	The password used to authenticate with an autoprovisioning server. Leave this field blank to disable authentication.
Autoprovisioning Autoupdate (in minutes) ?	The reoccurring time (in minutes) the device will wait before checking for new autoprovisioning files. Enter up to 6 digits. A value of 0 will disable this option. **Note**: To use the auto update options, enable the **Set Time with NTP Server on boot** setting on the **Device Page** page (see Table 2-10).
Autoprovision at time (HHMMSS) ?	The time of day the device will check for a new autoprovisioning file. The time must be 6 characters in length and in HHMMSS format. An empty value will disable this option. **Note**: To use the auto update options, enable the **Set Time with NTP Server on boot** setting on the **Device Page** page (see Table 2-10).
Autoprovision when idle (in minutes > 10) ?	The idle time (in minutes greater than 10) after which the device will check for a new autoprovisioning file. Enter up to 6 digits. A value of 0 will disable this option. **Note**: To use the auto update options, enable the **Set Time with NTP Server on boot** setting on the **Device Page** page (see Table 2-10).

Table 2-23. Autoprovisioning Page Parameters (continued)

Web Page Item	Description
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** button to reboot the system.
Toggle Help	Click on the **Toggle Help** button to see a short description of some of the web page items. First click on the **Toggle Help** button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.
Download Template	Press the **Download Template** button to create an autoprovisioning file for the device. See Section 2.3.13.3, "Download Template Button"
Autoprovisioning log	The autoprovisioning log provides information about the latest autoprovisioning attempt (i.e. dhcp options and server accessed and files parsed or not found).

2.3.13.1 Autoprovisioning

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

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

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

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

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

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

You can download an autoprovisioning template file from the Autoprovisioning Page using the **Download Template** button (see Table 2-23). 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>
<!--    <AutoprovFile>common.xml</AutoprovFile>-->
<!--    <AutoprovFile>sip_reg[macaddress].xml</AutoprovFile>-->
<!--    <AutoprovFile>audio[macaddress]</AutoprovFile>-->
<!--    <AutoprovFile>device[macaddress].xml</AutoprovFile>-->
    </MiscSettings>
```

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

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

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

The file 0020f7123456.xml contains:

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

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

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

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

Checking for New Autoprovisioning Files after Boot

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

The Autoprovisioning Filename

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

Table 2-24. Autoprovisioning File Name

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

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

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

For example:

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

The autoprovisioning filename is set to "cyberdata/"

On boot, the device will try to download:

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

...and if this fails:

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

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

Autoprovisioning Firmware Updates

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

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

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

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

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

The list of valid product strings:

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

Autoprovisioning Example 1

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

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

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

000000cd.xml

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

sip_common.xml

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

sip_0020f7020001.xml

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

sip_0020f7020002.xml

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

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

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

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

Autoprovisioning Example 2

Here is another example of setting up your autoprovisioning files:

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

0020f7020001.xml

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

0020f7020002.xml

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

common_settings.xml

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

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

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

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

XML Files

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

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

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

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

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

From the common file, a pointer to sip_common.xml

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

Autoprovisioned Audio Files

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

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

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

2.3.13.2 Sample dhcpd.conf

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

ddns-update-style none;

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

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

    option routers                  10.0.0.1;
    option subnet-mask              255.0.0.0;

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

    option time-offset              -8;             # Pacific Standard Time

#     option www-server               99.99.99.99;                    # OPTION 72

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

#     option option-150                10.0.0.252;                    # OPTION 150

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

    range 10.10.0.1 10.10.2.1; }
```

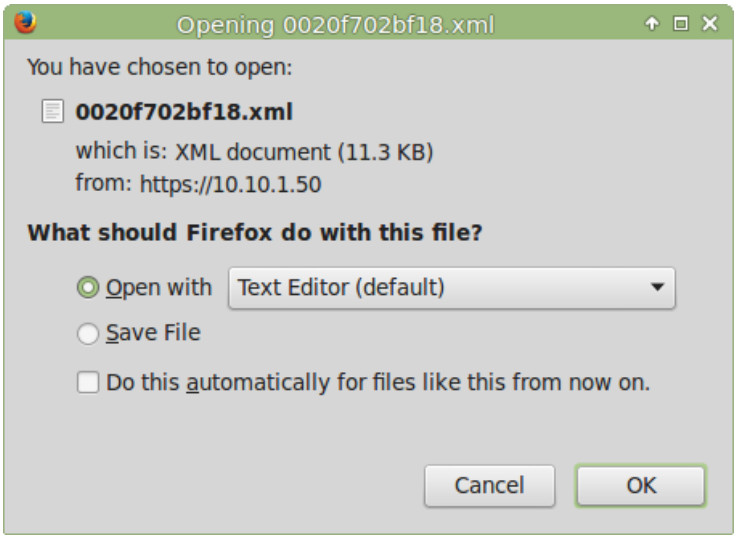
2.3.13.3 Download Template Button

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

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

1. On the **Autoprovisioning** page, click on the **Download Template** button.
2. You will see a window prompting you to save a configuration file (**.xml**) to a location on your computer (Figure 2-47). 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 2-47.

Figure 2-47. 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 InformaCast Enabled Loudspeaker Amplifier (PoE)

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/011407
2. Unzip the firmware version file. This file may contain the following:

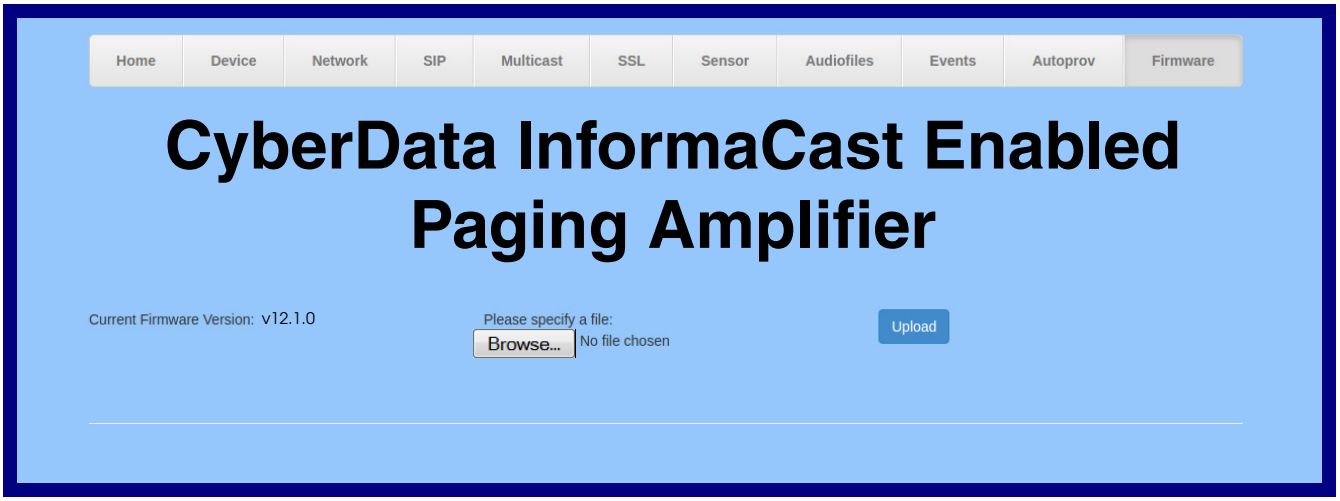
- Firmware file
- Release notes

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. See Figure 2-48.

Caution

Equipment Hazard: CyberData strongly recommends that you first reboot the device before attempting to upgrade the firmware of the device. See Section 2.4.2, "Reboot the Device".

Figure 2-48. Firmware Page



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

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

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

8. Table 2-25 shows the web page items on the **Firmware** page.

Table 2-25. Firmware Parameters

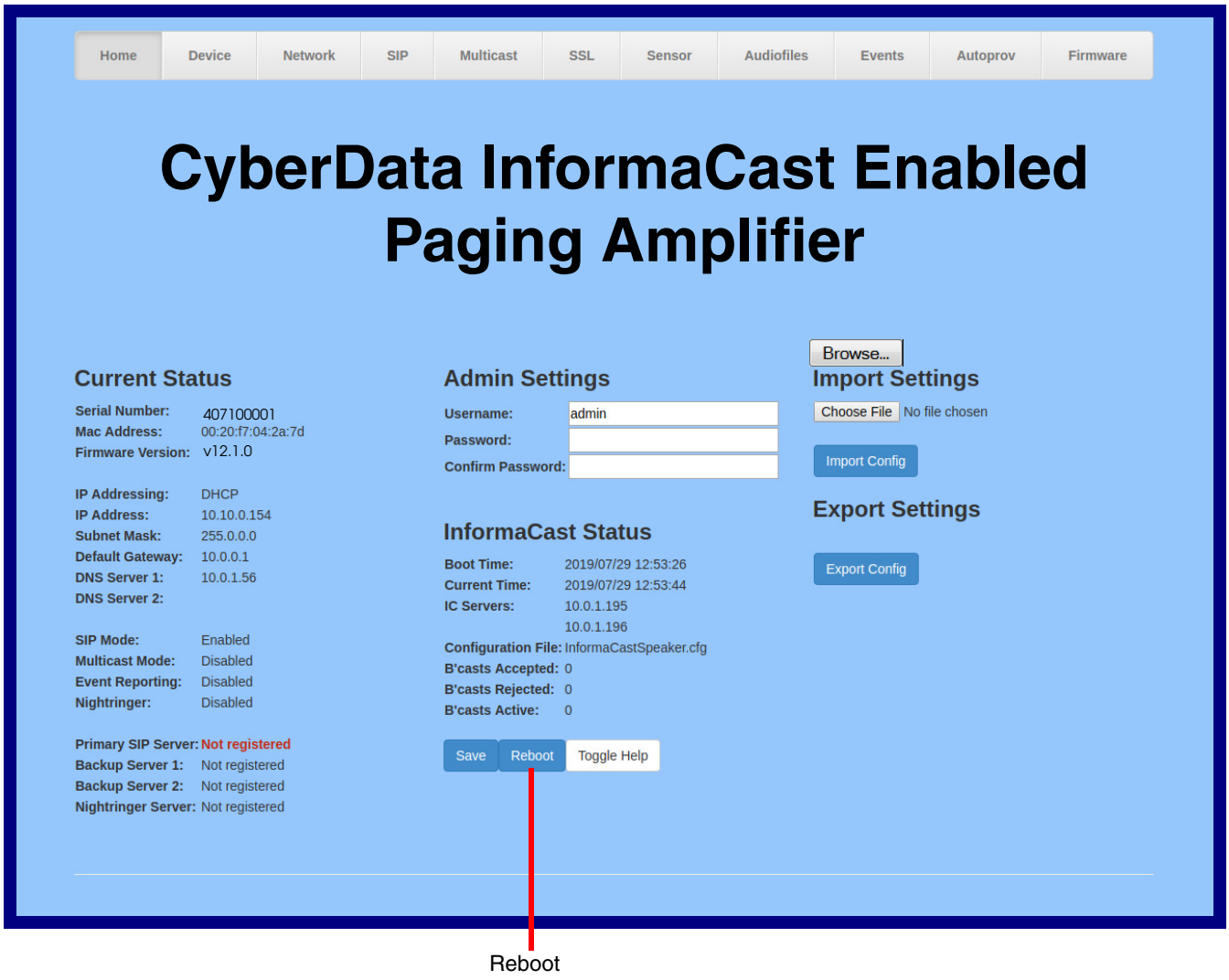
Web Page Item	Description
Current Firmware Version	Shows the current firmware version.
	Use the **Browse** button to navigate to the location of the firmware file that you want to upload.
	Click on the **Upload** button to automatically upload the selected firmware and reboot the system.

2.4.2 Reboot the Device

To reboot a InformaCast Enabled Loudspeaker Amplifier (PoE), 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 2-49). A normal restart will occur.

Figure 2-49. 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 2-26 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

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

Table 2-26. Command Interface Post Commands

Device Action	HTTP Post Command[a]
Trigger relay (for configured delay)	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/command.cgi" --post-data "test_relay=yes"
Place call to extension (example: extension 130)	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/command.cgi" --post-data "call=130"
Terminate active call	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/command.cgi" --post-data "terminate=yes"
Force reboot	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/command.cgi" --post-data "reboot=yes"
Test Audio button	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/command.cgi" --post-data "test_audio=yes"
Announce IP address	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/command.cgi" --post-data "speak_ip_address=yes"
Play the "0" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_0=yes"
Play the "1" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_1=yes"
Play the "2" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_2=yes"
Play the "3" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_3=yes"
Play the "4" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_4=yes"

Table 2-26. Command Interface Post Commands (continued)

Device Action	HTTP Post Command[a]
Play the "5" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_5=yes"
Play the "6" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_6=yes"
Play the "7" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_7=yes"
Play the "8" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_8=yes"
Play the "9" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_9=yes"
Play the "Dot" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_d=yes"
Play the "Audio Test" audio file (from Audio Config)	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_audiotest=yes"
Play the "Page Tone" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_pagetone=yes"
Play the "Your IP Address Is" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_youripaddressis=yes"
Play the "Rebooting" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_rebooting=yes"
Play the "Restoring Default" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_restoringdefault=yes"
Play the "Ringback tone" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_ringback=yes"
Play the "Ring tone" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_ringtone=yes"
Play the "Night Ring" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_nightring=yes"
Delete the "0" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_0=yes"
Delete the "1" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_1=yes"

Table 2-26. Command Interface Post Commands (continued)

Device Action	HTTP Post Command[a]
Delete the "2" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_2=yes"
Delete the "3" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_3=yes"
Delete the "4" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_4=yes"
Delete the "5" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_5=yes"
Delete the "6" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_6=yes"
Delete the "7" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_7=yes"
Delete the "8" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_8=yes"
Delete the "9" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_9=yes"
Delete the "Audio Test" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_audiotest=yes"
Delete the "Page Tone" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_pagetone=yes"
Delete the "Your IP Address Is" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_youripaddressis=yes"
Delete the "Rebooting" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_rebooting=yes"
Delete the "Restoring Default" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_restoringdefault=yes"
Delete the "Ringback tone" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_ringback=yes"
Delete the "Ring tone" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_ringtone=yes"
Delete the "Night Ring" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_nightring=yes"

Table 2-26. Command Interface Post Commands (continued)

Device Action	HTTP Post Command[a]
Trigger the Door Sensor Test (Sensor Config page)	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/sensor.cgi" --post-data "doortest=yes"

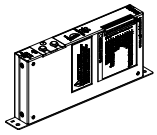
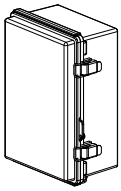
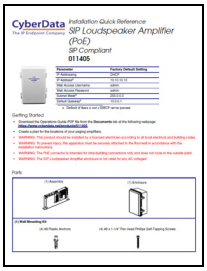
a.Type and enter all of each http POST command on one line.

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. Parts List

Quantity	Part Name	Illustration
1	Singlewire InformaCast Paging Amplifier Assembly	
1	Enclosure	
1	Installation Quick Reference Guide	
1	Mounting Accessory Kit which includes: (4) #8 Plastic Anchors (4) #8 x 1-1/4" Pan Head Phillips Self-Tapping Screws	

Note The InformaCast Enabled Loudspeaker Amplifier (PoE) 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.

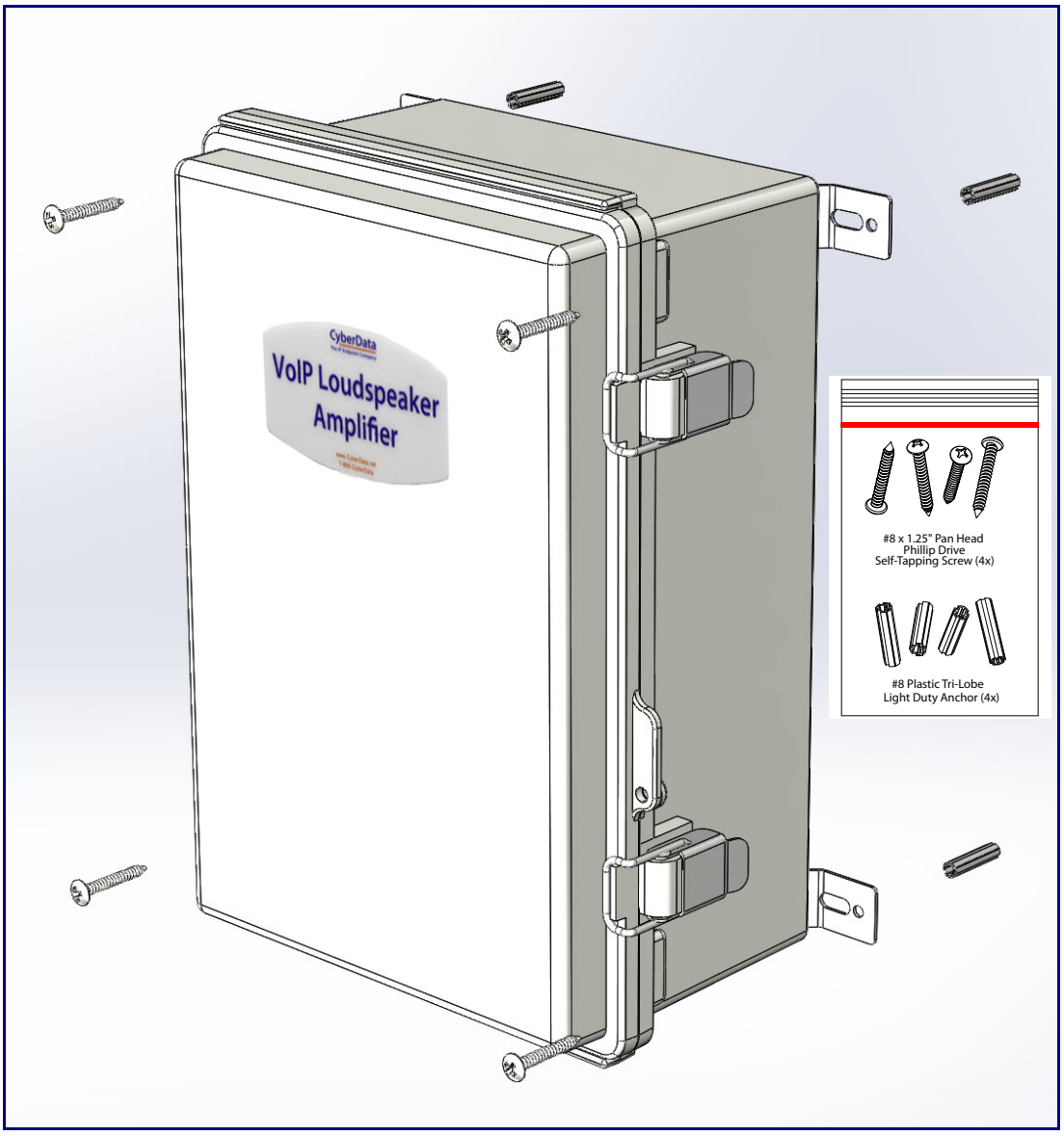
Note For mounting, use the three **#8 SHEET METAL SCREWS** to secure the enclosure.

A.1.1 Mounting the Enclosure

To mount the enclosure:

1. Prepare holes for the screws.
2. Plug in the power adapter and use the **Power (PWR)** LED to verify that the power is on.
3. Plug the ethernet cable into the device. The **Link/Activity (Link/Act.)** LED verifies the network connection.
4. For wall mounting, use the three #8 x 1-1/4-inch Truss Head Phillip screws to secure the speaker. See Figure A-1.

Figure A-1. Mounting the Enclosure



Appendix B: Setting up a TFTP Server

B.1 Set up a TFTP Server

Autoprovisioning requires a TFTP server for hosting the configuration file.

B.1.1 In a LINUX Environment

To set up a TFTP server on LINUX:

1. Create a directory dedicated to the TFTP server, and move the files to be uploaded to that directory.
2. Run the following command where `/tftpboot/` is the path to the directory you created in Step 1: the directory that contains the files to be uploaded. For example:

   ```
   in.tftpd -l -s /tftpboot/your_directory_name
   ```

B.1.2 In a Windows Environment

You can find several options online for setting up a Windows TFTP server. This example explains how to use the Solarwinds freeware TFTP server, which you can download at:

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

To set up a TFTP server on Windows:

1. Install and start the software.
2. Select **File**/**Configure**/**Security** tab/**Transmit Only**.
3. Make a note of the default directory name, and then move the firmware files to be uploaded to that directory.

Appendix C: Troubleshooting/Technical Support

C.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/011407

C.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/011407

C.3 Contact Information

Contact

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

Sales

Sales 831-373-2601, Extension 334

Technical Support

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

http://support.cyberdata.net/

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

Phone: (831) 373-2601, Extension 333

C.4 Warranty and RMA Information

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

http://support.cyberdata.net/

Index

Symbols

Numerics

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

W