



SIP IP66 Outdoor Horn Operations Guide

Part #011457
Document Part #931508A
for Firmware Version 11.8.0

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

SIP IP66 Outdoor Horn Operations Guide 931508A
Part # 011457

COPYRIGHT NOTICE:

© 2018, CyberData Corporation, ALL RIGHTS RESERVED.

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

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

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

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

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



Technical Support

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

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

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

Email: support@cyberdata.net

Fax: (831) 373-4193

Company and product information is at www.cyberdata.net.

Revision Information

Revision 931508A, which corresponds to firmware version 11.8.0, was released on April 16, 2018.




Browsers Supported

The following browsers have been tested against firmware version 11.8.0:



- Internet Explorer (version: 10)
- Firefox (also called Mozilla Firefox) (version: 52.02)
- Chrome (version 570.2987.98)
- Safari (version: 5.1.7)

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.

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

Pictorial Alert Icons

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

Hazard Levels

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

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

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

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

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

Abbreviations and Terms

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

Chapter 1 Product Overview	1
1.1 How to Identify This Product	1
1.2 Typical System Installation	2
1.3 Product Features	3
1.4 Supported Protocols	4
1.5 Supported SIP Servers	4
1.6 Specifications	5
1.7 Typical Coverage	6
1.8 Typical Warehouse Paging Setup	6
1.9 Compliance	7
1.9.1 CE Testing	7
1.9.2 FCC Statement	7
Chapter 2 Installing the SIP IP66 Outdoor Horn	8
2.1 Parts List	8
2.2 SIP IP66 Outdoor Horn Setup	9
2.2.1 SIP IP66 Outdoor Horn System Installation and Connection Options	10
2.2.2 Install the Network Cable Through Weatherproof Cable Gland	10
2.2.3 Power Test and Status LED	11
2.2.4 RTFM Switch	12
2.3.1 Factory Default Settings	15
2.3.2 SIP IP66 Outdoor Horn Web Page Navigation	16
2.3.3 Using the Toggle Help Button	17
2.3.4 Log in to the Home Page	19
2.3.5 Configure the Device	23
2.3.6 Configure the Network Parameters	29
2.3.7 Configure the SIP (Session Initiation Protocol) Parameters	32
2.3.8 Configure the Multicast Parameters	40
2.3.9 Configure the Audiofiles Page Parameters	44
2.3.10 Configure the Events Parameters	51
2.3.11 Configure the Autoprovisioning Parameters	56
2.4.1 Downloading the Firmware	68
2.4.2 Reboot the Device	70
2.5.1 Command Interface Post Commands	71
Appendix A Mounting the Amplifier	75
A.1 Dimensions	75
Appendix B Setting up a TFTP Server	76
B.1 Set up a TFTP Server	76
2.1.1 In a LINUX Environment	76
2.1.2 In a Windows Environment	76
Appendix C Troubleshooting/Technical Support	77
C.1 Frequently Asked Questions (FAQ)	77
C.2 Documentation	77
C.3 Contact Information	78
C.4 Warranty and RMA Information	78
Index	79

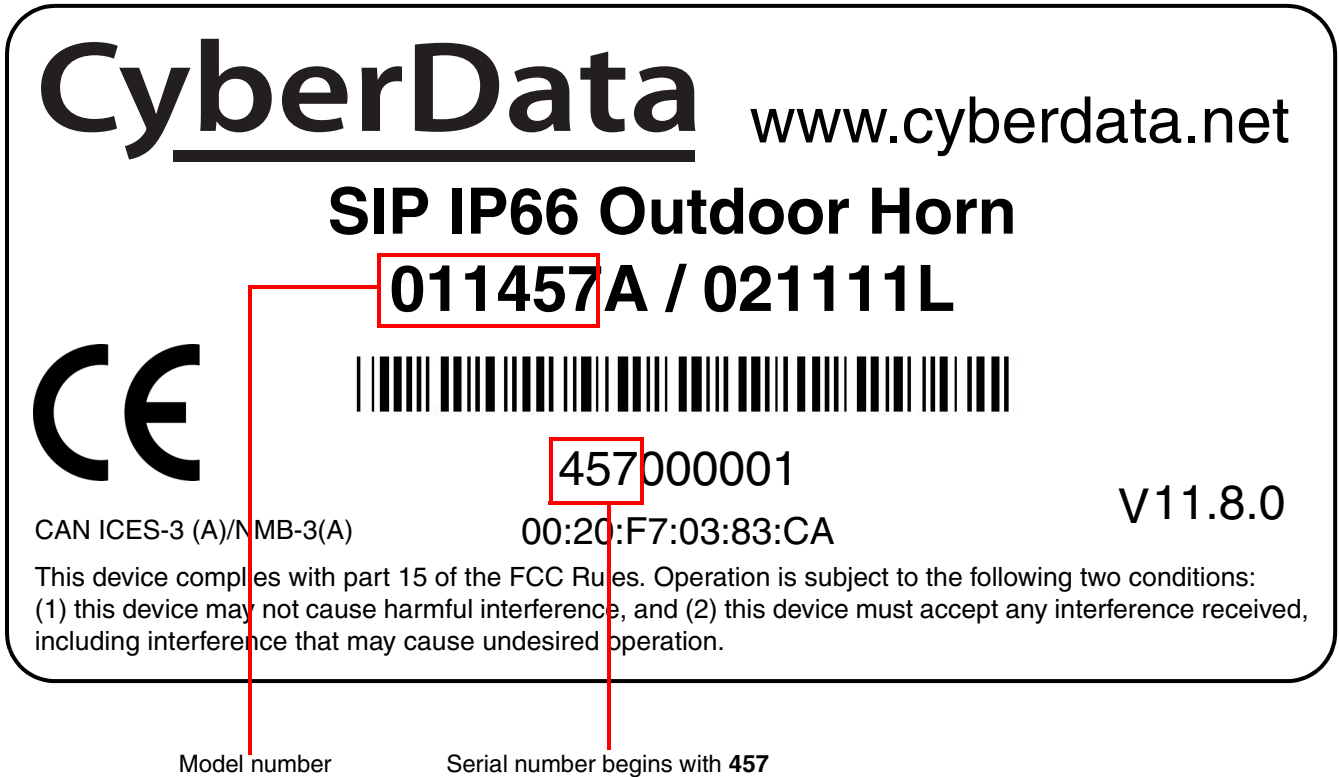
1 Product Overview

1.1 How to Identify This Product

To identify the SIP IP66 Outdoor Horn (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 **011457**.

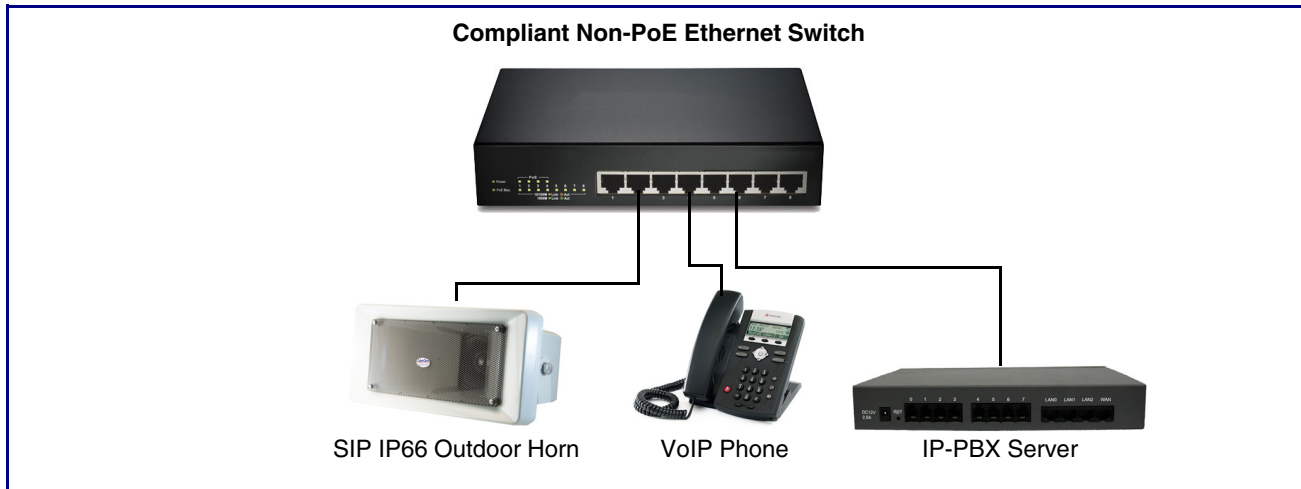
Figure 1-1. Model Number Label



1.2 Typical System Installation

Figure 1-2 illustrates how the SIP IP66 Outdoor Horn is normally installed as part of a public address system.

Figure 1-2. Typical Installation



1.3 Product Features

- Support for security code access for SIP paging
- Autoprovisioning via HTTPS
- HTTPS web based configuration
- SIP Enhanced interoperability for hosted environments
- CyberData has maintained one of the most comprehensive list of IP PBX servers certified to work with CyberData
- Support for G.711, G.722, G.729 codecs
- 802.11q VLAN tagging
- Configurable event generation for device health and status monitoring
- 9 user-uploadable page messages
- IP66-rated
- Sealed network cable gland
- SIP and Simultaneous Multicast
- Page from Polycom phones
- Dual-speed ethernet 10/100 Mbps
- Web-based configuration
- PoE 802.3at and 802.3af-enabled
- User-uploadable tones and messages
- Digital volume control
- Second SIP endpoint "Night Ringer"
- Autoprovisioning
- HTTP Command Interface
- 10 channel prioritized Multicast ports
- Built-in diagnostics
- Delayed page support
- Cisco SRST

1.4 Supported Protocols

The SIP IP66 Outdoor Horn supports:

- SIP
- Multicast
- HTTP and HTTPS web-based configuration
Provides an intuitive user interface for easy system configuration and verification of SIP IP66 Outdoor Horn operations.
- DHCP Client
Dynamically assigns IP addresses in addition to the option to use static addressing.
- TFTP Client
Facilitates hosting for the configuration file for Autoprovisioning.
- RTP
- SPEEX
- Audio Encodings
PCMU (G.711 mu-law)
PCMA (G.711 A-law)
G.722
729
Packet Time 20 ms

1.5 Supported SIP Servers

The following link contains information on how to configure the SIP IP66 Outdoor Horn for the supported SIP servers:

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

1.6 Specifications

Table 1-1. Specifications

Specifications	
Ethernet I/F	10/100 Mbps
Protocol	SIP RFC 3261 Compatible
Power Input	PoE 802.3at or 802.3af
Audio Output	802.3at: 107.7 (+/- 0.2) dBC @1M and 1kHz 802.3af: 104.8 (+/- 0.2) dBC @1M and 1kHz
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)
Payload Types	G.711 a-law, G.711 u-law, and G.722, G.729
Dimensions ^a	14.41 inches [366 mm] Length 10.71 inches [272 mm] Width 9.06 inches [230 mm] Height
Weight	6.6 lbs. [3 kg]
Boxed Weight	2.0 lbs. [0.90 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
Part Number	011457

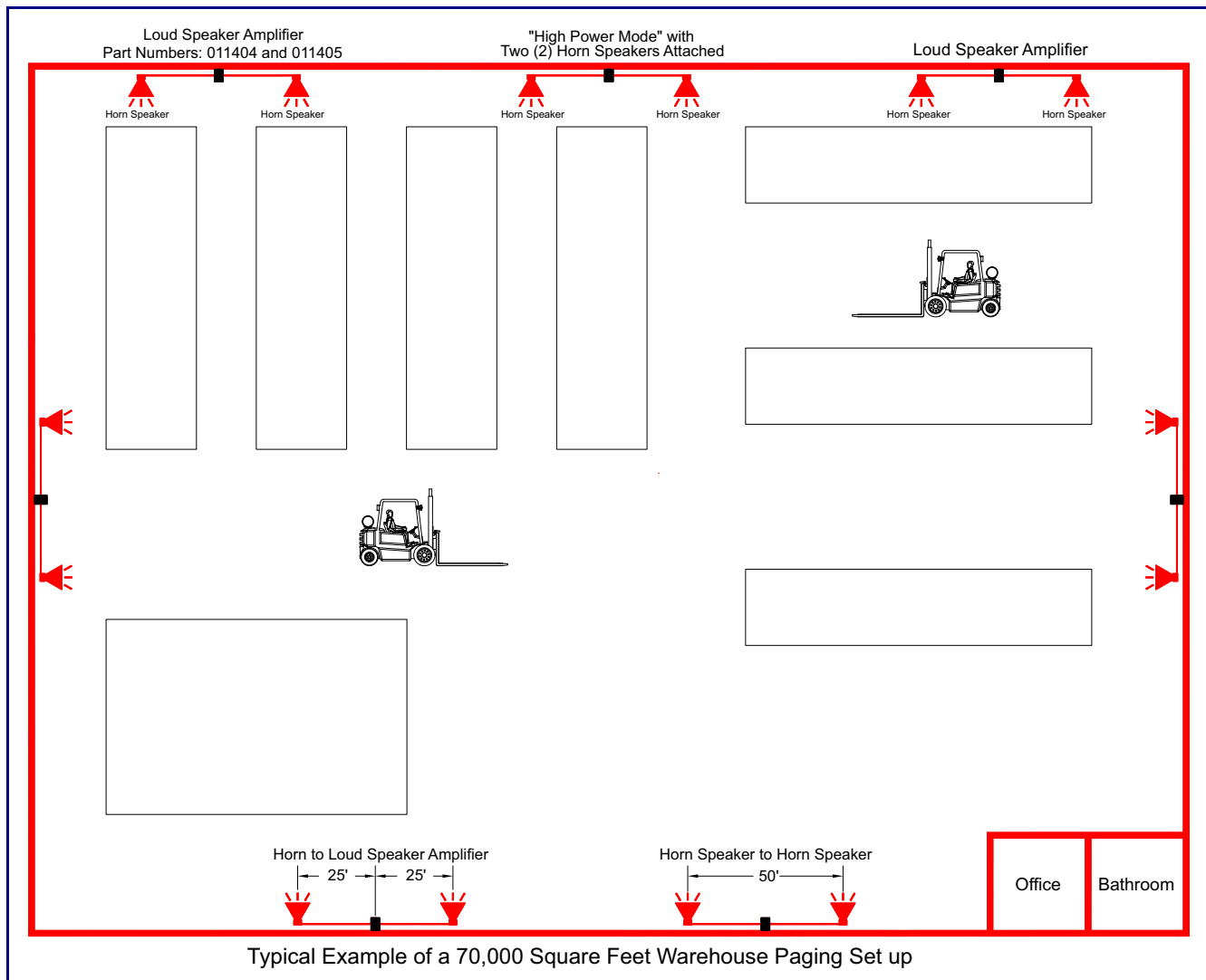
a. Dimensions are measured from the perspective of the product being upright with the front of the product facing you.

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.

1.8 Typical Warehouse Paging Setup

Figure 1-3. Typical Warehouse Paging Setup



1.9 Compliance

1.9.1 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.

1.9.2 FCC Statement


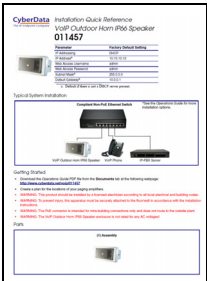
This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, 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 SIP IP66 Outdoor Horn

2.1 Parts List

Table 2-2 illustrates the parts for each SIP IP66 Outdoor Horn and includes a kit for mounting.

Table 2-2. Parts List

Quantity	Part Name	Illustration
1	SIP IP66 Outdoor Horn Assembly	
1	Installation Quick Reference Guide	

2.2 SIP IP66 Outdoor Horn Setup

Set up and configure each SIP IP66 Outdoor Horn *before* you mount it.

CyberData delivers each SIP IP66 Outdoor Horn with the factory default values indicated in [Table 2-3](#):

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

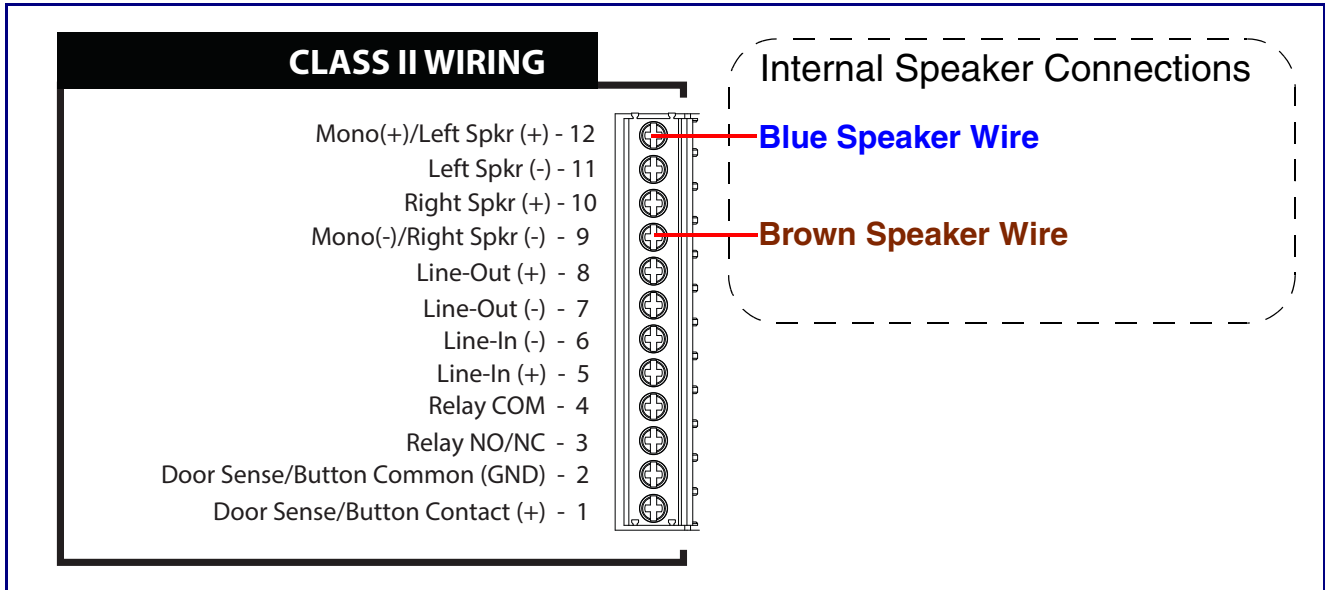
Parameter	Factory Default Setting
IP Addressing	DHCP
IP Address ^a	10.10.10.10
Web Access Username	admin
Web Access Password	admin
Subnet Mask ^a	255.0.0.0
Default Gateway ^a	10.0.0.1

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

2.2.1 SIP IP66 Outdoor Horn System Installation and Connection Options

The following figures show the connection options for the SIP IP66 Outdoor Horn.

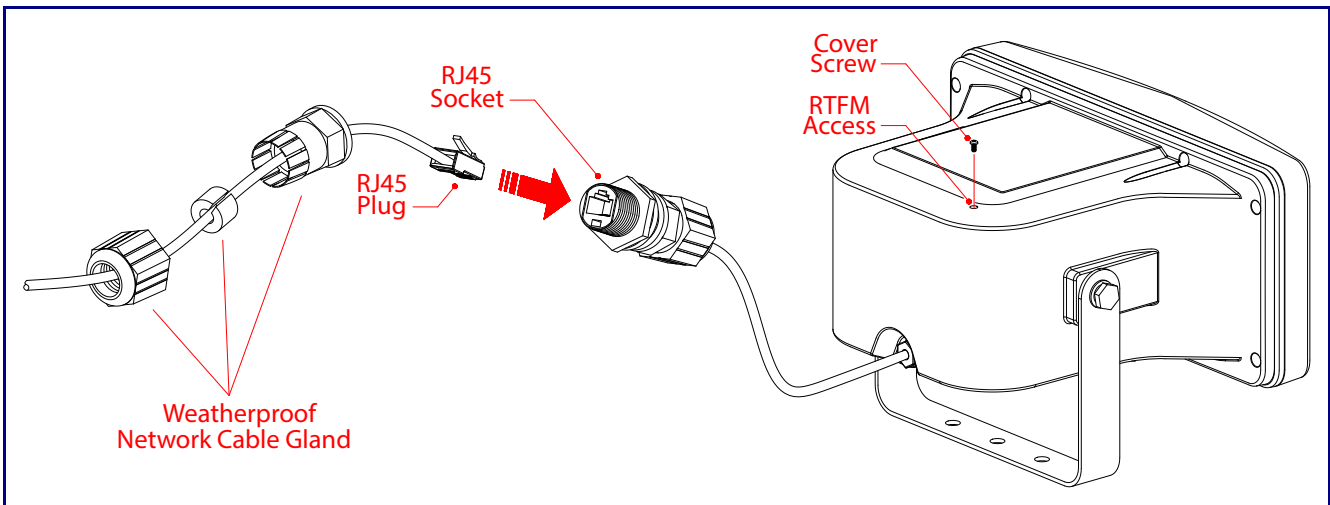
Figure 2-4. SIP IP66 Outdoor Horn Connections



2.2.2 Install the Network Cable Through Weatherproof Cable Gland

Install the network cable through weatherproof cable gland as shown in [Figure 2-5](#).

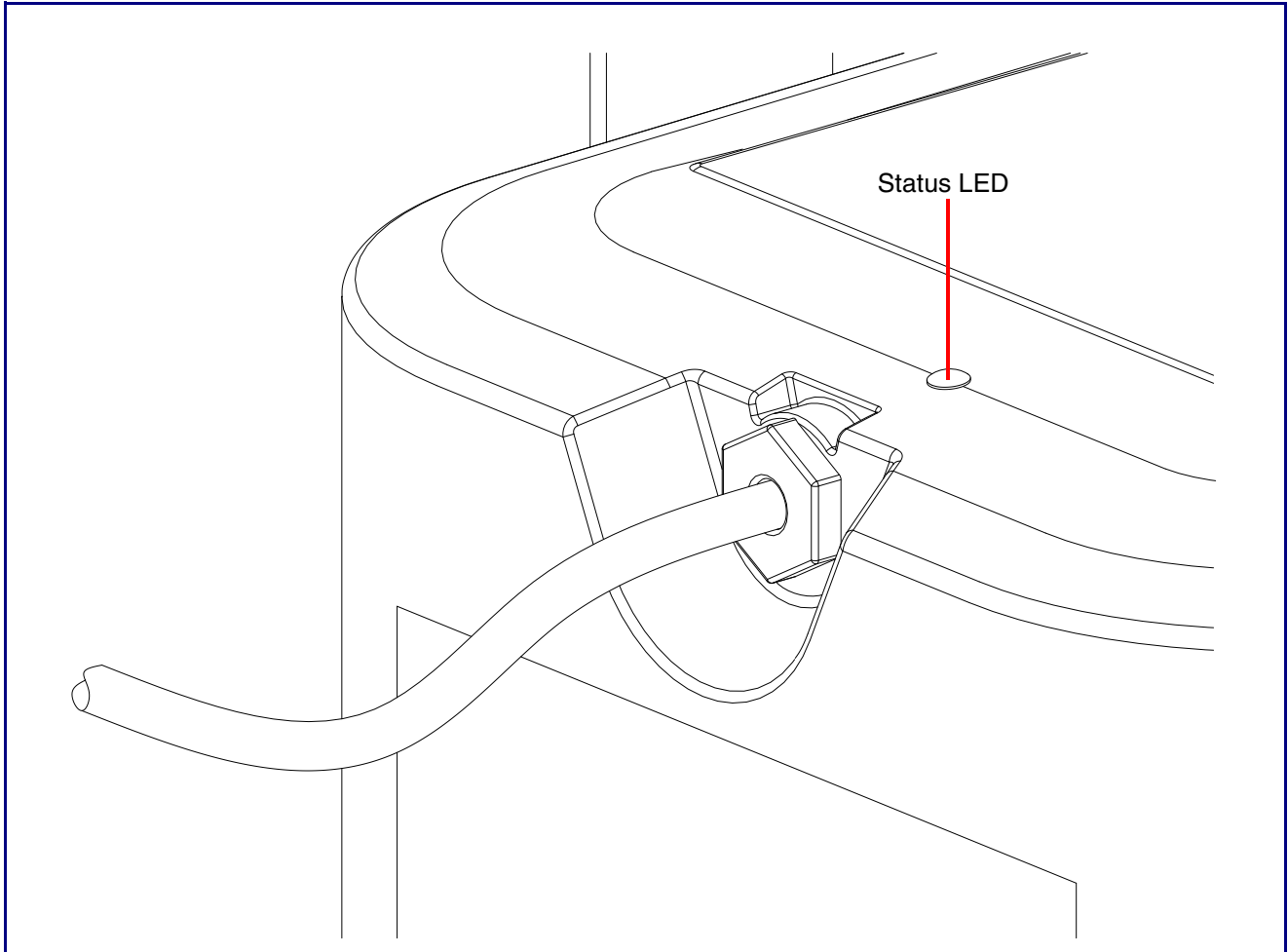
Figure 2-5. Install the Network Cable Through Weatherproof Cable Gland



2.2.3 Power Test and Status LED

1. Plug in the CyberData device and monitor the Status LED activity on the bottom side of the horn during the initialization process. See [Figure 2-6](#).

Figure 2-6. Status LED



2. 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. It will turn off thereafter until the device has finished booting. When the device has fully booted, the **GREEN Status** LED will turn on solid.

If there is no DHCP server available on the network, it will try 12 times for 60 seconds and eventually fall back to the programmed static IP address (by default 10.10.10.10) or the previously used DHCP address if a prior lease was established. This process will take approximately 80 seconds.
3. When the device has completed the initialization process, pressing and holding the RTFM switch for a couple of seconds will announce the IP address. See [Section 2.2.4, "RTFM Switch"](#)

This concludes the power test.

2.2.4 RTFM Switch

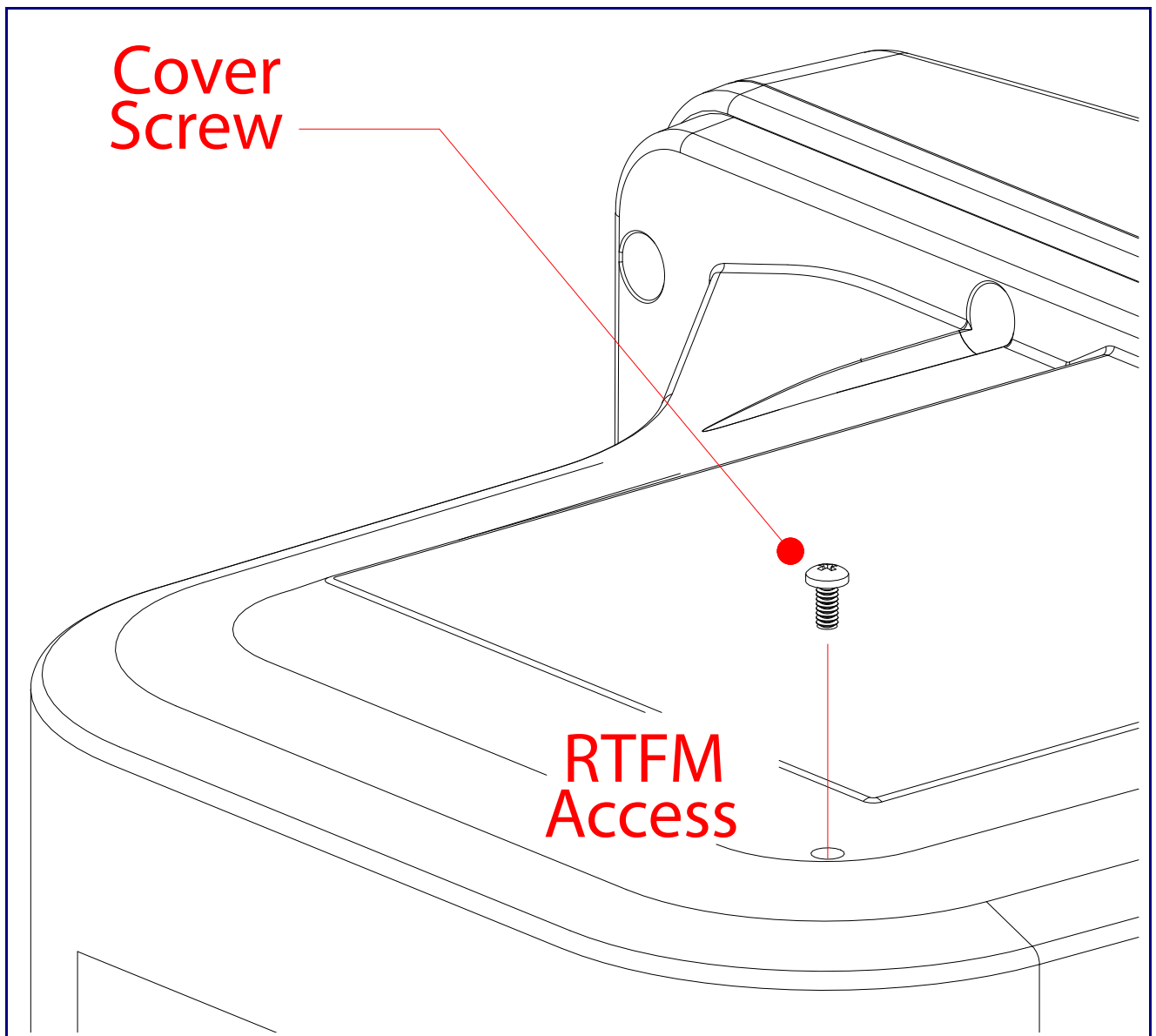
When the SIP IP66 Outdoor Horn is operational and linked to the network, use the Reset Test Function Management (**RTFM**) switch (Figure 2-8) (located behind the hole on the device) to announce and confirm the device's IP Address and test the audio to verify that it is working.

2.2.4.1 RTFM Access

The RTFM button access will be on the top side of the horn hidden under a screw that will be used to keep the unit secured. To access the RTFM, complete the following steps:

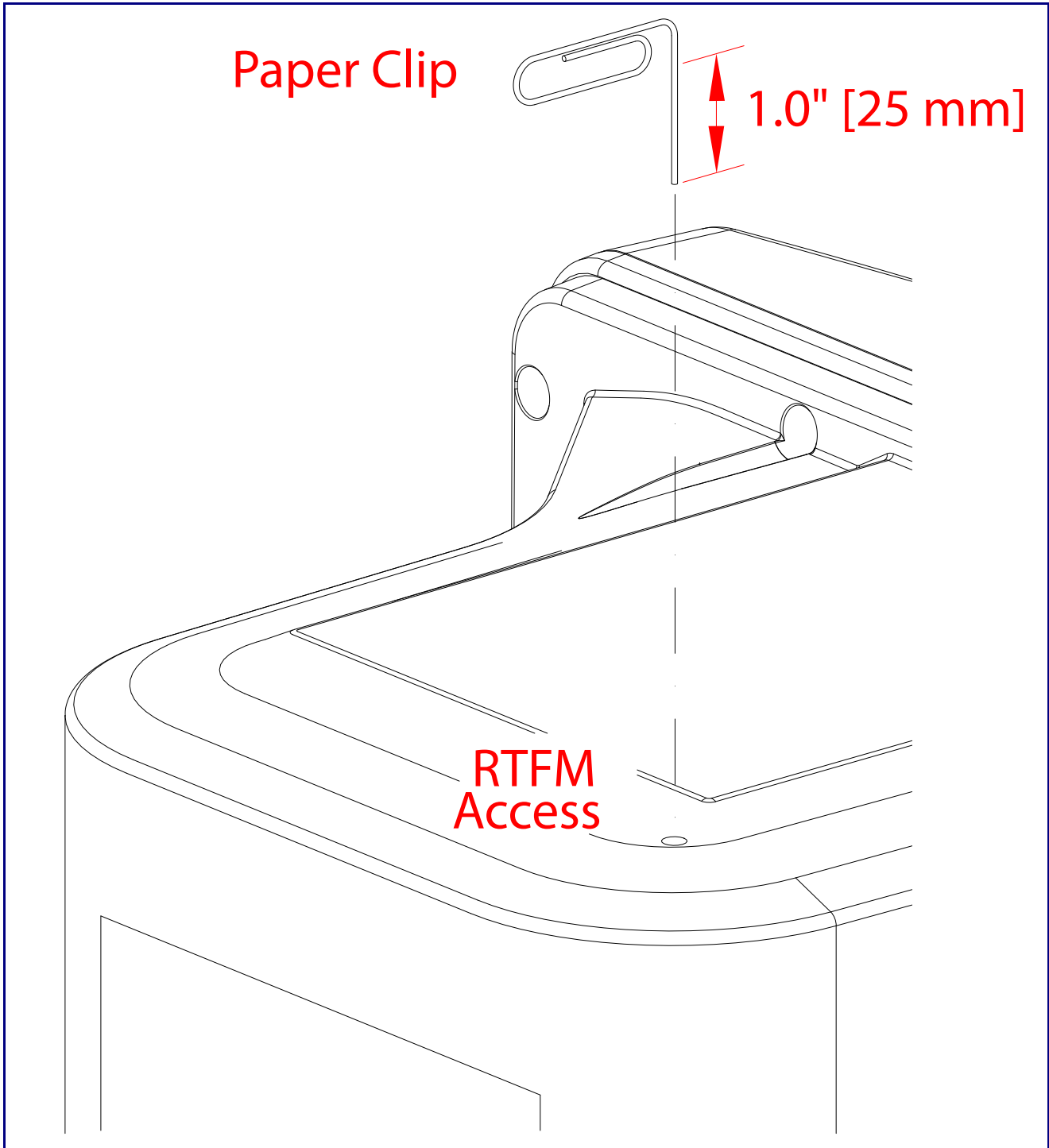
1. Remove the screw to gain access to the RTFM button (Figure 2-8).

Figure 2-7. RTFM Switch



2. Use a paper clip to feed through the hole to press the RTFM button. See [Figure 2-8](#).


Figure 2-8. RTFM Switch



2.2.4.2 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.

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

2.2.4.3 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.

2.3 Configure the SIP IP66 Outdoor Horn Parameters

To configure the SIP IP66 Outdoor Horn online, use a standard web browser.

Configure each SIP IP66 Outdoor Horn and verify its operation *before* you mount it. When you are ready to mount an SIP IP66 Outdoor Horn, refer to [Appendix A, "Mounting the Amplifier"](#) for instructions.

2.3.1 Factory Default Settings

All SIP IP66 Outdoor Horns are initially configured with the following default IP settings:

When configuring more than one SIP IP66 Outdoor Horn, attach the SIP IP66 Outdoor Horns to the network and configure one at a time to avoid IP address conflicts.

Table 2-4. Factory Default Settings

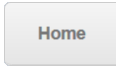
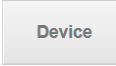
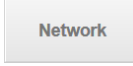


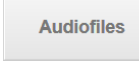
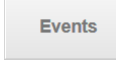

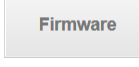
Parameter	Factory Default Setting
IP Addressing	DHCP
IP Address ^a	10.10.10.10
Web Access Username	admin
Web Access Password	admin
Subnet Mask ^a	255.0.0.0
Default Gateway ^a	10.0.0.1

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

2.3.2 SIP IP66 Outdoor Horn Web Page Navigation

Table 2-5 shows the navigation buttons that you will see on every SIP IP66 Outdoor Horn web page.

Table 2-5. Web Page Navigation

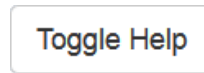
Web Page Item	Description
	Link to the Home page.
	Link to the Device page.
	Link to the Network page.
	Link to go to the SIP page.
	Link to the Multicast page.
	Link to the Audiofiles page.
	Link to the Events page.
	Link to the Autoprovisioning page.
	Link to the Firmware page.

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:

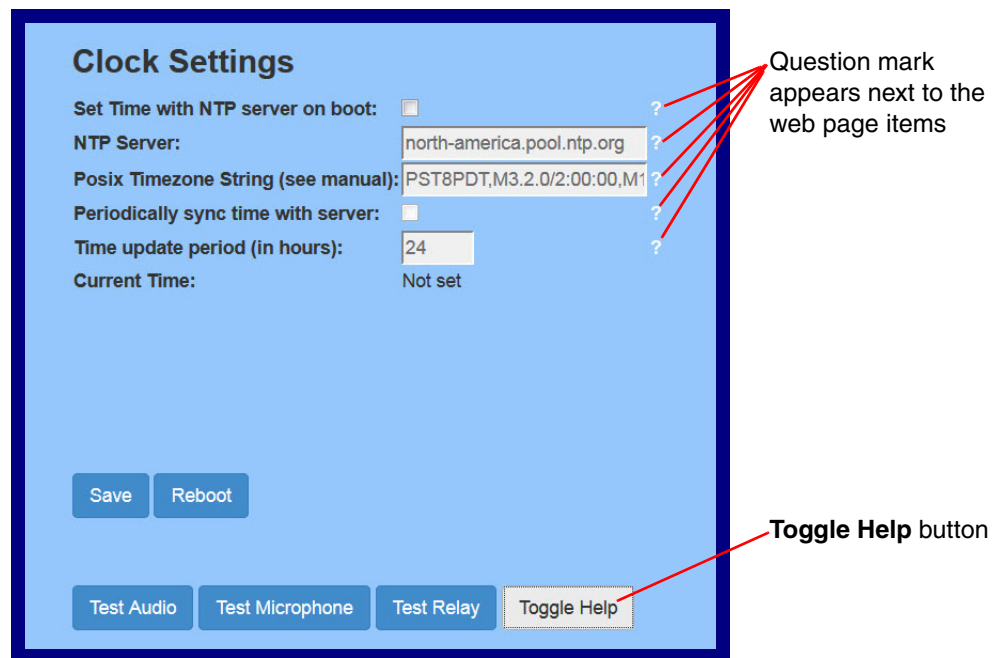
1. Click on the **Toggle Help** button that is on the UI webpage. See [Figure 2-9](#) and [Figure 2-10](#).

Figure 2-9. Toggle/Help Button



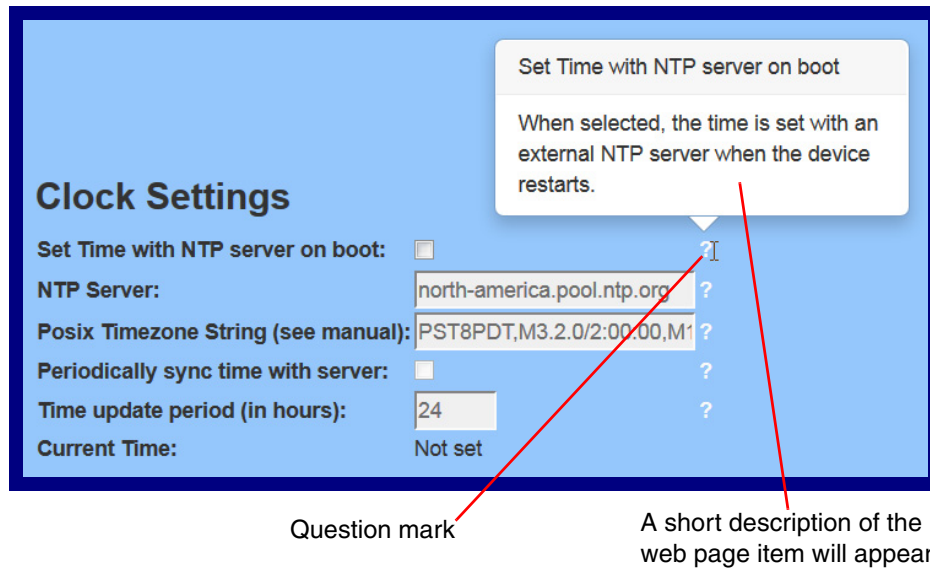
2. You will see a question mark (?) appear next to each web page item that has been provided with a short description by the Help feature. See [Figure 2-10](#).

Figure 2-10. 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 2-11.

Figure 2-11. 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 SIP IP66 Outdoor Horn.

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:

<http://www.cyberdata.net/assets/common/discovery.zip>

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 2-12):

Web Access Username: **admin**

Web Access Password: **admin**

Figure 2-12. Home Page

Home Device Network SIP Multicast Audiofiles Events Autopro Firmware

CyberData Outdoor Horn

Current Status

Serial Number: 457000001
Mac Address: 00:20:f7:03:4a:d9
Firmware Version: v11.8.5

IP Addressing: DHCP
IP Address: 10.10.0.189
Subnet Mask: 255.0.0.0
Default Gateway: 10.0.0.1
DNS Server 1: 10.0.1.56
DNS Server 2:

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

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

Admin Settings

Username:
Password:
Confirm Password:

Import Settings

No file chosen

Export Settings

3. On the **Home** page, review the setup details and navigation buttons described in [Table 2-6](#).

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 2-6. Home Page Overview

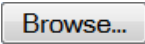




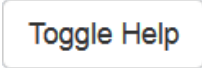
Web Page Item	Description
Admin Settings	
Username ?	The username to access the web interface. Enter up to 25 characters.
Password ?	The password to access the web interface. Enter up to 25 characters.
Confirm Password ?	Confirm the web interface password.
Current Status	
Serial Number	Shows the device 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.
Import Settings	
	Use this button to select a configuration file to import.
	After selecting a configuration file, click Import to import the configuration from the selected file. Then, click Save and Reboot to store changes.
Export Settings	
	Click Export to export the current configuration to a file.
	Click the Save button to save your configuration settings. Note: You need to reboot for changes to take effect.

Table 2-6. Home Page Overview (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.

2.3.5 Configure the Device

1. Click the **Device** menu button to open the **Device** page. See [Figure 2-13](#).

Figure 2-13. Device Page

The screenshot shows the 'Device' configuration page for a CyberData Outdoor Horn. At the top, there is a navigation menu with buttons for Home, Device (selected), Network, SIP, Multicast, Audiofiles, Events, Autopro, and Firmware. The main heading is 'CyberData Outdoor Horn'. Below this, the page is divided into several settings sections:

- Volume Settings (0-9)**: SIP Volume (4), Multicast Volume (4), and Volume Boost (No Volume Boost).
- DTMF Settings**: Require Security Code (checkbox), Security Code (text field), and Enable Stored Message Playback (checkbox).
- Clock Settings**: Set Time with NTP server on boot (checkbox), NTP Server (north-america.pool.ntp.org), Posix Timezone String (PST8PDT,M3.2.0/2:00:00,M11.1), Periodically sync time with server (checkbox), Time update period (24 hours), and Current Time (18:22:54).
- Power Settings**: 802.3AT Mode (Not detected. Disabled), Force 802.3AT Mode (checkbox), and Auxiliary Power Supply (checkbox).
- Misc Settings**: Device Name (Outdoor Horn), Beep on Init (checkbox), Beep on Page (checkbox), and Disable HTTPS (checkbox).

At the bottom left, there are buttons for 'Test Audio', 'Save', 'Reboot', and 'Toggle Help'.













2. On the **Device** page, you may enter values for the parameters indicated in [Table 2-7](#).

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 2-7. Device Page Parameters

Web Page Item	Description
Volume Settings (0-9)	
SIP Volume ?	Set the speaker volume for a SIP call. A value of 0 will mute the speaker during SIP calls. Note: You can change this setting without rebooting the device.
Multicast Volume ?	Set the speaker volume for multicast audio streams. A value of 0 will mute the speaker during multicasts. Note: You can change this setting without rebooting the device.
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 or reduce intelligibility of the speaker audio. Boost will raise the volume above level 9, regardless of the digital volume settings, and also applies when using the analog volume control dial.
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)
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.
Power Settings	

Table 2-7. Device Page Parameters (continued)

Web Page Item	Description
802.3AT Mode 	This device automatically detects if it is plugged into an 802.3AT (also known as PoE Plus) power source. 802.3AT provides more power than older 802.3AT power sources and allows this speaker to play audio at higher volumes. If you are sure this speaker is connected to an 802.3AT power source, but it is not being detected correctly, you can override the automatic settings below.
Force 802.3AT Mode (NOT recommended) 	Enable this option if you are sure this speaker is connected to an 802.3AT power source, but it is not being detected correctly (not recommended).
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.
Misc Settings	
Device Name 	Type the device name. Enter up to 25 characters.
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.
	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.
	Click the Save button to save your configuration settings. Note: You need to reboot for changes to take effect.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark () appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

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

2.3.5.1 Time Zone Strings

The posix time zone string tells the internal date and time utilities how to handle daylight savings time for different time zones. [Table 2-19](#) shows some common strings.

Table 2-8. 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.

[Table 2-20](#) 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 2-9. Time Zone String Parts

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

Time Zone String Examples

[Table 2-21](#) has some more examples of time zone strings.

Table 2-10. 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

a. Tokyo does not use daylight savings time.

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

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

Figure 2-14. Three or Four Character Time Zone Identifier

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

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

World GMT Table

[Table 2-22](#) has information about the GMT time in various time zones.

Table 2-11. 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
GMT+5	Islamabad, Karachi

Table 2-11. World GMT Table (continued)

Time Zone	City or Area Zone Crosses
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 2-15).

Figure 2-15. Network Page

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

CyberData Outdoor Horn

Stored Network Settings

Addressing Mode: Static DHCP

Hostname: SipDevice034ad9

IP Address: 10.10.10.10

Subnet Mask: 255.0.0.0

Default Gateway: 10.0.0.1

DNS Server 1: 10.0.0.1

DNS Server 2: 10.0.0.1

DHCP Timeout in seconds*: 60

* A value of -1 will retry forever

VLAN Settings

VLAN ID (0-4095): 0

VLAN Priority (0-7): 0

Save Reboot Toggle Help

Current Network Settings

IP Address: 10.10.0.189

Subnet Mask: 255.0.0.0

Default Gateway: 10.0.0.1

DNS Server 1: 10.0.1.56

DNS Server 2:




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

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

Table 2-12. Network Page Parameters

Web Page Item	Description
Stored Network Settings	
Addressing Mode ?	Select either DHCP IP Addressing or Static Addressing by marking the appropriate radio button. DHCP Addressing mode is enabled on default and the device will attempt to resolve network addressing with the local DHCP server upon boot. If DHCP Addressing fails, the device will revert to the last known IP address or the factory default address if no prior DHCP lease was established. See Section 2.3.1, "Factory Default Settings" for factory default settings. Be sure to click Save and Reboot to store changes when configuring a Static address.
Hostname ?	This is the hostname provided by the DHCP server. See the DHCP/DNS server documentation for more information. Enter up to 64 characters.
IP Address ?	Enter the Static IPv4 network address in dotted decimal notation.
Subnet Mask ?	Enter the Subnet Mask in dotted decimal notation.
Default Gateway ?	Enter the Default Gateway IPv4 address in dotted decimal notation.
DNS Server 1 ?	Enter the primary DNS Server IPv4 address in dotted decimal notation.
DNS Server 2 ?	Enter the secondary DNS Server IPv4 address in dotted decimal notation.
DHCP Timeout in seconds ?	Specify the desired time-out duration (in seconds) that the device will wait for a response from the DHCP server before reverting back to the stored static IP address. The stored static IP address may be the last known IP address or the factory default address if no prior DHCP lease was established. Enter up to 8 characters. A value of -1 will retry forever.
Current Network Settings	
IP Address	Shows the current Static IP address.
Subnet Mask	Shows the current Subnet Mask address.
Default Gateway	Shows the current Default Gateway address.
DNS Server 1	Shows the current DNS Server 1 address.
DNS Server 2	Shows the current DNS Server 2 address.
VLAN Settings	
VLAN ID (0-4095) ?	Specify the IEEE 802.1Q VLAN ID number. Enter up to 4 digits. Note: The device supports 802.1Q VLAN tagging support. The switch port connected to the device will need to be in "trunking mode" for the VLAN tags to propagate.
VLAN Priority (0-7) ?	Specify the IEEE 802.1p VLAN priority level. Enter 1 digit. A value of 0 may cause the VLAN ID tag to be ignored.

Table 2-12. Network Page Parameters (continued)

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

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

2.3.7 Configure the SIP (Session Initiation Protocol) Parameters

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

Figure 2-16. SIP Page

The screenshot shows the 'SIP' configuration page for the CyberData Outdoor Horn. The page has a navigation bar at the top with tabs for Home, Device, Network, SIP (selected), Multicast, Audiofiles, Events, Autopro, and Firmware. The main heading is 'CyberData Outdoor Horn'. The configuration is organized into several sections:

- SIP Settings:** Includes checkboxes for 'Enable SIP operation' (checked), 'Register with a SIP Server' (checked), and 'Use Cisco SRST' (unchecked). It features input fields for 'Primary SIP Server' (10.0.0.253), 'Primary SIP User ID' (199), 'Primary SIP Auth ID' (199), and 'Primary SIP Auth Password' (masked with asterisks). There are also fields for 'Backup SIP Server 1', 'Backup SIP User ID 1', 'Backup SIP Auth ID 1', 'Backup SIP Auth Password 1', 'Backup SIP Server 2', 'Backup SIP User ID 2', 'Backup SIP Auth ID 2', and 'Backup SIP Auth Password 2'. Other fields include 'Remote SIP Port' (5060), 'Local SIP Port' (5060), 'Outbound Proxy', 'Outbound Proxy Port' (0), 'Disable rport Discovery' (unchecked), 'Buffer SIP Calls' (unchecked), 'Re-registration Interval (in seconds)' (360), 'Unregister on Boot' (unchecked), and 'Keep Alive Period' (10000).
- Nightringer Settings:** Includes 'Enable Nightringer' (unchecked), 'SIP Server' (10.0.0.253), 'Remote SIP Port' (5060), 'Local SIP Port' (5061), 'Outbound Proxy', 'Outbound Proxy Port' (0), 'User ID' (241), 'Authenticate ID' (241), 'Authenticate Password' (masked with asterisks), and 'Re-registration Interval (in seconds)' (360).
- RTP Settings:** Includes 'RTP Port (even)' (10500) and 'Jitter Buffer' (50).
- Call Disconnection:** Includes 'Terminate Call after delay' (0).
- Codec Selection:** Includes 'Force Selected Codec' (unchecked) and 'Codec' (PCM U (G.711, u-law)).

At the bottom of the page, there are three buttons: 'Save', 'Reboot', and 'Toggle Help'.

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

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

Table 2-13. SIP Page Parameters

Web Page Item	Description
SIP Settings	
Enable SIP Operation ?	When enabled, the device will transmit, receive, and process SIP messages according to the configured SIP settings below.
SIP Transport Protocol ?	Choose the transport protocol for SIP signaling. This will affect all extensions, including the Nightringer. Default is UDP.
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 2.3.7.2, "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 2-13. 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 ?	Also referred to as delayed paging. Device will buffer up to 4 minutes of audio then play back the recording after hang up.
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.
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.

Table 2-13. SIP Page Parameters (continued)

Web Page Item	Description
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.
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.
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.
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	

Table 2-13. SIP Page Parameters (continued)

Web Page Item	Description
Force Selected Codec 	When configured, this option will allow you to force the device to negotiate for the selected codec. Otherwise, the device will perform codec negotiation using the default list of supported codecs.
Codec 	Select the desired codec (only one may be chosen).
	Click the Save button to save your configuration settings. Note: You need to reboot for changes to take effect.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark () appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

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

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

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

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

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

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

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

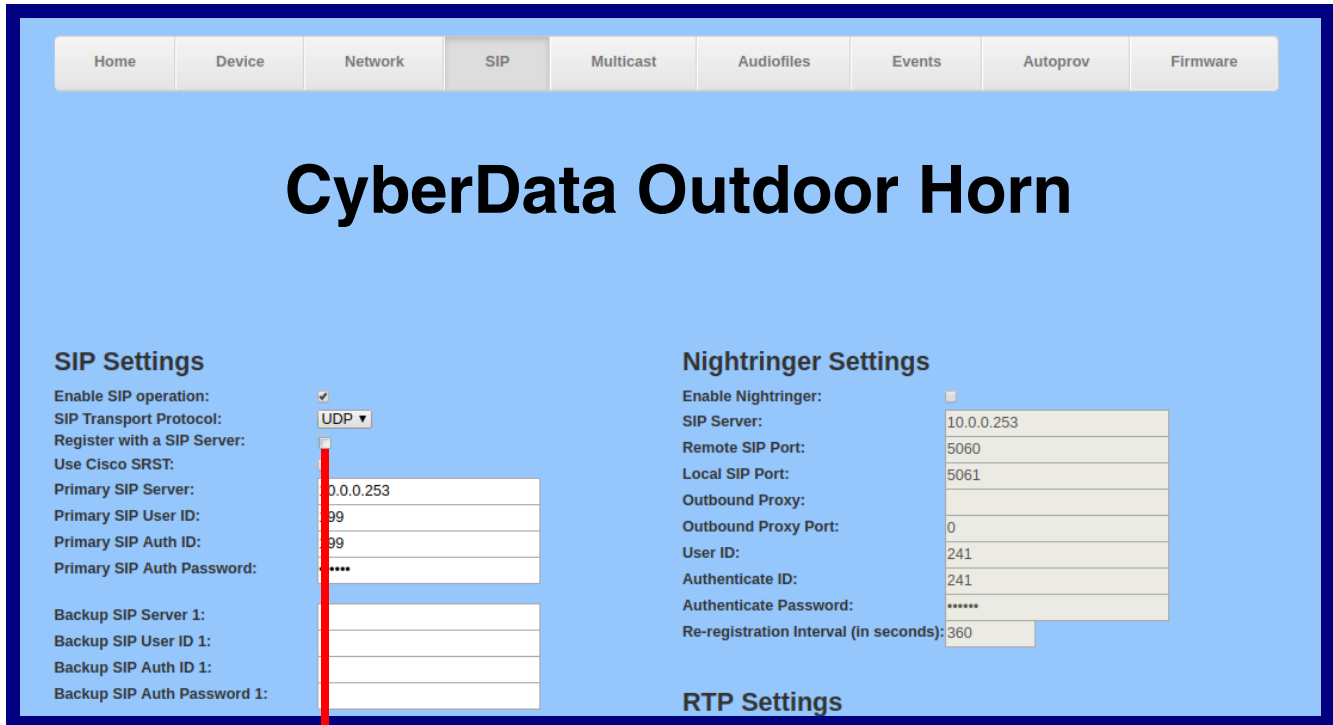
2.3.7.2 Point-to-Point Configuration

When the device is set to not register with a SIP server (see [Figure 2-17](#)), it is possible to set the device to dial out to a single endpoint.

In this case, the dial-out extension should be the IP address of the remote device. The device can also receive Point-to-Point calls. The delayed DTMF functionality is available in the Point-to-Point Mode.

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

Figure 2-17. SIP Page Set to Point-to-Point Mode



Device is set to NOT register with a SIP server

2.3.7.3 Delayed DTMF

On the **SIP** 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 2-15. 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 2-18](#).

Figure 2-18. Multicast Page

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

CyberData Outdoor Horn

Multicast Settings

Enable Multicast Operation:

Priority	Address	Port	Name	Buffer	Beep
9	239.168.3.10	11000	Emergency	<input type="checkbox"/>	<input type="checkbox"/>
8	239.168.3.9	10000	MG8	<input type="checkbox"/>	<input type="checkbox"/>
7	239.168.3.8	9000	MG7	<input type="checkbox"/>	<input type="checkbox"/>
6	239.168.3.7	8000	MG6	<input type="checkbox"/>	<input type="checkbox"/>
5	239.168.3.6	7000	MG5	<input type="checkbox"/>	<input type="checkbox"/>
4	239.168.3.5	6000	MG4	<input type="checkbox"/>	<input type="checkbox"/>
3	239.168.3.4	5000	MG3	<input type="checkbox"/>	<input type="checkbox"/>
2	239.168.3.3	4000	MG2	<input type="checkbox"/>	<input type="checkbox"/>
1	239.168.3.2	3000	MG1	<input type="checkbox"/>	<input type="checkbox"/>
0	239.168.3.1	2000	Background Music	<input type="checkbox"/>	<input type="checkbox"/>

Polycom Default Channel

Polycom Priority Channel

Polycom Emergency Channel

SIP calls are considered priority 4.5

Port range can be from 2000-65535

Priority 9 is the highest and 0 is the lowest




A higher priority audio stream will always supersede a lower one

** You need to reboot for changes to take effect*

2. On the **Multicast** page, enter values for the parameters indicated in [Table 2-16](#).

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

Table 2-16. Multicast Page Parameters

Web Page Item	Description
Enable Multicast Operation	Enables or disables multicast operation.
Priority	Indicates the priority for the multicast group. Priority 9 is the highest (emergency streams). 0 is the lowest (background music). SIP calls are considered priority 4.5 . See Section 2.3.8.1, "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.
Polycom Default Channel	When a default Polycom channel/group number is selected, the device will subscribe to the default channel for one-way group pages. Group Numbers 1-25 are supported. Or, select Disabled to disable this channel.
Polycom Priority Channel	When a priority Polycom channel/group number is selected, the device will subscribe to the priority channel for one-way group pages. Group Numbers 1-25 are supported. Or, select Disabled to disable this channel.
Polycom Emergency Channel	When an emergency Polycom channel/group number is selected, the device will subscribe to the default channel for one-way group pages. Group Numbers 1-25 are supported. Or, select Disabled to disable this channel.
	Click the Save button to save your configuration settings. Note: You need to reboot for changes to take effect.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

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

2.3.8.1 Assigning Priority

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

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

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

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

Ringtones and
Nightringtones

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

2.3.9 Configure the 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 2-19).

Figure 2-19. Audiofiles Page

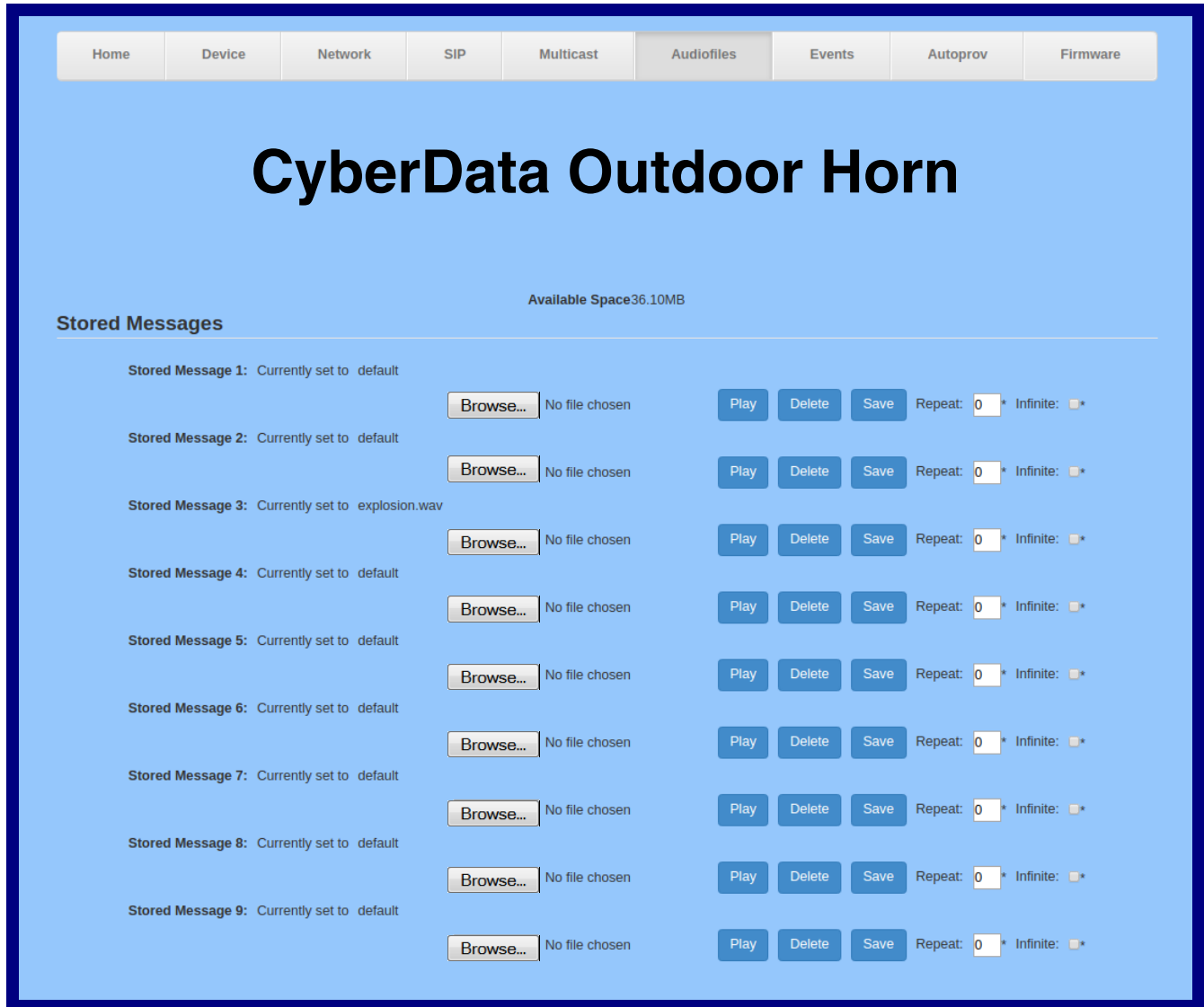


Figure 2-20. Audiofiles Page

Dot:	Currently set to default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Audio Test:	Currently set to default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Enter Code:	Currently set to default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Invalid Code:	Currently set to default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Page Tone:	Currently set to default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Your IP Address Is:	Currently set to default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Rebooting:	Currently set to default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Restoring Default:	Currently set to default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Ring Tone:	Currently set to default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Sensor Triggered:	Currently set to default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Night Ring:	Currently set to default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>

Figure 2-21. Audiofiles Page

Menu Audio Files

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





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

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

Table 2-17. 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.
Dot	Corresponds to the spoken word "dot." (24 character limit)
Audio Test	Corresponds to the message " <i>This is the CyberData IP speaker test message...</i> " (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).
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	
Cancel	Corresponds to the word "Cancel" used in the audio menu played to the caller. (24 character limit).
Currently Playing	Corresponds to the words "Currently Playing" used in the audio menu played to the caller. (24 character limit).
Invalid Entry	Corresponds to the words "Invalid Entry" used in the audio menu played to the caller. (24 character limit).
Page	Corresponds to the word "Page" used in the audio menu played to the caller. (24 character limit).

Table 2-17. Audiofiles Page Parameters (continued)

Web Page Item	Description
Play Stored Message	Corresponds to the words "Play Stored Message" used in the audio menu played to the caller. (24 character limit).
Pound (#)	Corresponds to whatever word or phrase the user wishes to call the pound key in the audio menu played to the caller (24 character limit).
Press	Corresponds to the word "Press" used in the audio menu played to the caller. (24 character limit).
Stored Message	Corresponds to the words "Stored Message" used in the audio menu played to the caller. (24 character limit).
Through	Corresponds to the word "Through" used in the audio menu played to the caller. (24 character limit).
To	Corresponds to the word "To" used in the audio menu played to the caller. (24 character limit).
	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.

2.3.9.1 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 2-22](#) through [Figure 2-24](#).

Figure 2-22. Audacity 1

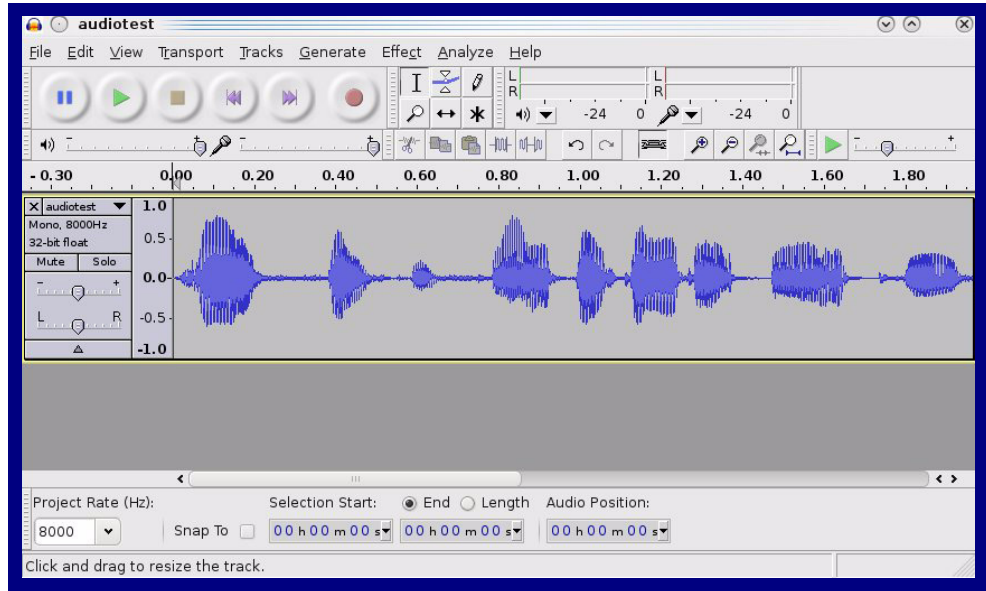
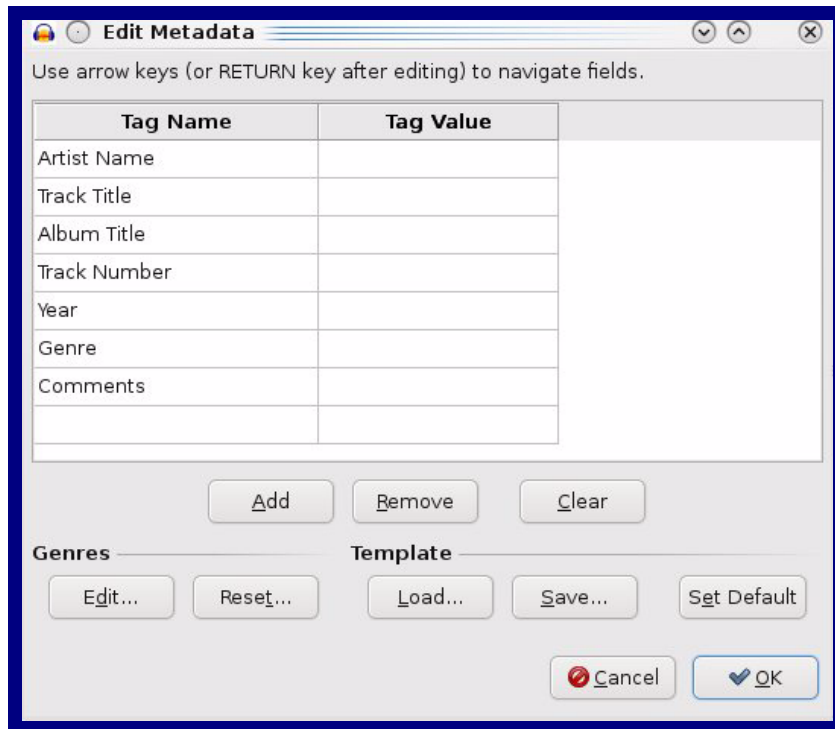


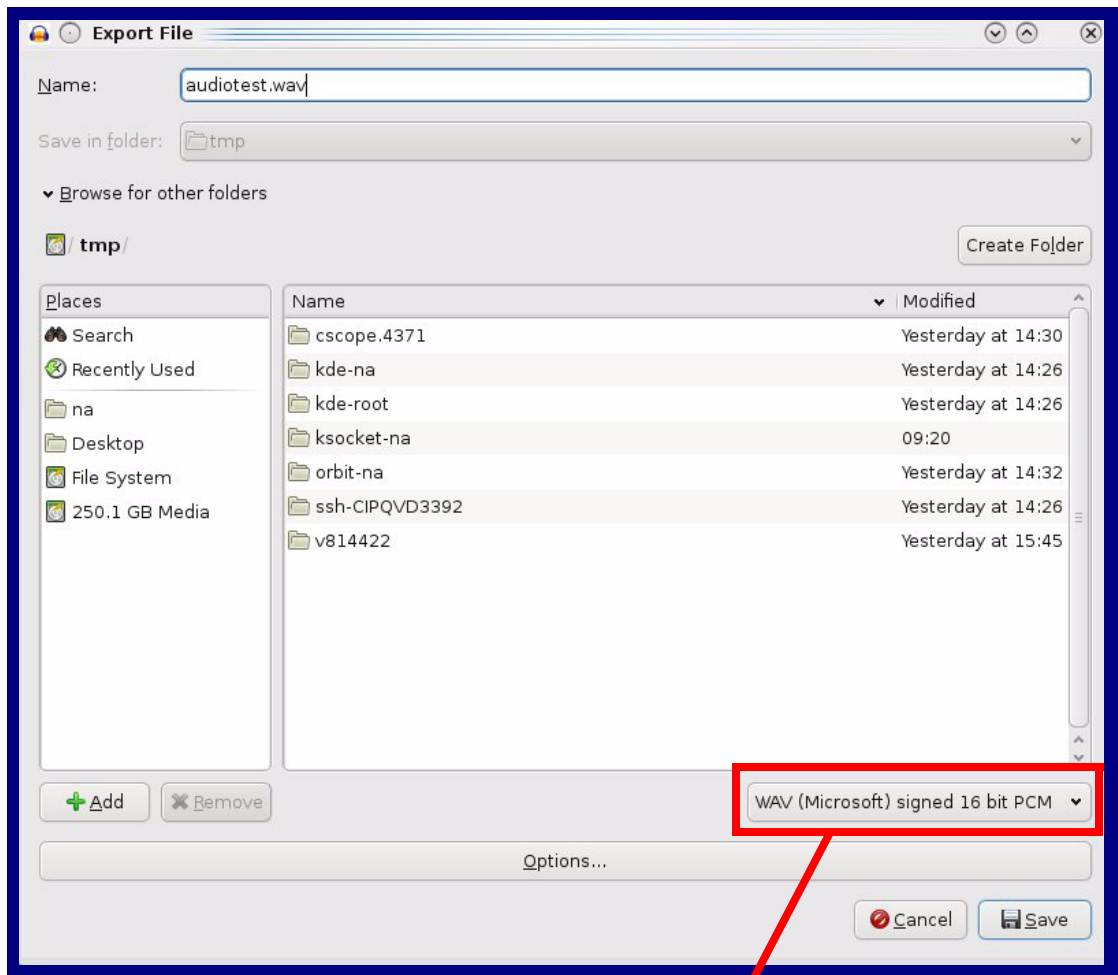
Figure 2-23. Audacity 2



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

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

Figure 2-24. WAV (Microsoft) signed 16 bit PCM



WAV (Microsoft) signed 16 bit PCM

2.3.10 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 2-25).

Figure 2-25. Event Page

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

CyberData Outdoor Horn

Enable Event Generation:

Events

Enable Call Start Events:

Enable Call Terminated Events:

Enable Night Ring Events:

Enable Power On Events:

Enable Multicast Start Events:

Enable Multicast Stop Events:

Enable 60 Second Heartbeat:

[Check All](#) [Uncheck All](#)

Event Server

Server IP Address: 10.0.0.250

Server Port: 8080

Server URL: xmlparse_engine

[Save](#) [Reboot](#) [Toggle Help](#)

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

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. 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 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 60 Second Heartbeat Events ?	When enabled, the device will report a Heartbeat event every 60 seconds. SIP registration is not required to generate Heartbeat events.
Check All	Click on Check All to select all of the events on the page.
Uncheck All	Click on Uncheck All to de-select all of the events on the page.
Event Server	
Server IP Address ?	The IPv4 address of the event server in dotted decimal notation.
Server Port ?	Specify the event server port number. The supported range is 0-65536. Enter up to 5 digits.
Server URL ?	Generally, the destination URL is the name of the application that receives the events and the string in the HTTP POST command. It can be a script used to parse and process the HTTP POST events. Enter up to 127 characters.
Save	Click the Save button to save your configuration settings. 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 You must click on the **Save** button and then the **Reboot** button for the changes to take effect.

2.3.10.1 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>
```

2.3.11 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 2-26](#).

Figure 2-26. Autoprovisioning Page

Home Device Network SIP Multicast Audiofiles Events Autoprov Firmware

CyberData Outdoor Horn

Disable Autoprovisioning:

Autoprovisioning Server:

Autoprovisioning Filename:

Use tftp:

Username:

Password:

Autoprovisioning autoupdate (in minutes): 0

Autoprovision at time (HHMMSS):

Autoprovision when idle (in minutes > 10): 0

See the manual to learn how to use autoprovisioning to configure your device.
Autoprovisioning happens on boot.
The device will first look for a configured server address and filename.
If these haven't been configured, it will look for an autoprovisioning server in your list of DHCP options and try to download '0020f7034ad9.xml' and if this fails, '000000cd.xml'.

Save Reboot Toggle Help

Download Template

Autoprovisioning log

```
54:45 Autoprovisioning Device...
54:45 Autoprov found option 43 in DHCP server="10.0.0.242"
54:45 Autoprov looking for 0020f7034ad9.xml at 10.0.0.242
54:45 Autoprov: didn't find autoprov file
54:45 Autoprov looking for 000000cd.xml at 10.0.0.242
54:45 Autoprov: didn't find autoprov file
54:45 Failed to fetch autoprov file
54:45 Autoprov found option 72 in DHCP server="10.0.0.242"
54:45 Autoprov looking for 0020f7034ad9.xml at 10.0.0.242
54:45 Autoprov: didn't find autoprov file
```

- On the **Autoprovisioning** page, you may 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. Autoprovisioning Page Parameters





Web Page Item	Description
Disable Autoprovisioning ?	Prevent the device from automatically trying to download a configuration file. See Section 2.3.11.1, "Autoprovisioning" for more information.
Autoprovisioning Server ?	Enter the IPv4 address of the provisioning server in dotted decimal notation.
Autoprovisioning Filename ?	<p>The autoprovisioning filename is the configuration filename. The default autoprovisioning filename is in the format of <mac address>.xml.</p> <p>Supported filename extensions are .txt, and .xml. The current filename is denoted by an asterisk at the bottom of the Autoprovisioning Page. Enter up to 256 characters.</p> <p>A file may have any name with an xml extension. If a file name is entered, the device will look for the specified file name, and only that file.</p>
Use tftp ?	The device will use TFTP (instead of http) to download autoprovisioning files.
Username ?	The username used to authenticate with an autoprovisioning server. Leave this field blank to disable authentication.
Password ?	The password used to authenticate with an autoprovisioning server. Leave this field blank to disable authentication.
Autoprovisioning Autoupdate (in minutes) ?	<p>The reoccurring time (in minutes) the device will wait before checking for new autoprovisioning files. Enter up to 6 digits. A value of 0 will disable this option.</p> <p>Note: To use the auto update options, enable the Set Time with NTP Server on boot setting on the Device Page (see Table 2-7).</p>
Autoprovision at time (HHMMSS) ?	<p>The time of day the device will check for a new autoprovisioning file. The time must be 6 characters in length and in HHMMSS format. An empty value will disable this option.</p> <p>Note: To use the auto update options, enable the Set Time with NTP Server on boot setting on the Device Page (see Table 2-7).</p>
Autoprovision when idle (in minutes > 10) ?	<p>The idle time (in minutes greater than 10) after which the device will check for a new autoprovisioning file. Enter up to 6 digits. A value of 0 will disable this option.</p> <p>Note: To use the auto update options, enable the Set Time with NTP Server on boot setting on the Device Page (see Table 2-7).</p>
	<p>Click the Save button to save your configuration settings.</p> <p>Note: You need to reboot for changes to take effect.</p>

Table 2-19. Autoprovisioning 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.
	Press the Download Template button to create an autoprovisioning file for the device. See Section 2.3.11.3, "Download Template Button"
Autoprovisioning log	The autoprovisioning log provides information about the latest autoprovisioning attempt (i.e. dhcp options and server accessed and files parsed or not found).

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

2.3.11.1 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 2.3.11.2, "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 2-19](#)). This file contains every configuration option that can be set on the board.

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

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

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

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

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

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

The file 0020f7123456.xml contains:

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

1. The device will first set its 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 2-20. Autoprovisioning File Name

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

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

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

For example:

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

The autoprovisioning filename is set to “cyberdata/”

On boot, the device will try to download:

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

...and if this fails:

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

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

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

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

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

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

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

The list of valid product strings:

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

Autoprovisioning
 Example 1

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

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

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

000000cd.xml

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

sip_common.xml

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

sip_0020f7020001.xml

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

sip_0020f7020002.xml

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

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

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

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

Autoprovisioning
 Example 2

Here is another example of setting up your autoprovisioning files:

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

0020f7020001.xml

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

0020f7020002.xml

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

common_settings.xml

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

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

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

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

XML Files

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

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

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

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

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

From the common file, a pointer to sip_common.xml

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

Autoprovisioned Audio Files

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

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

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

2.3.11.2 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; }

```

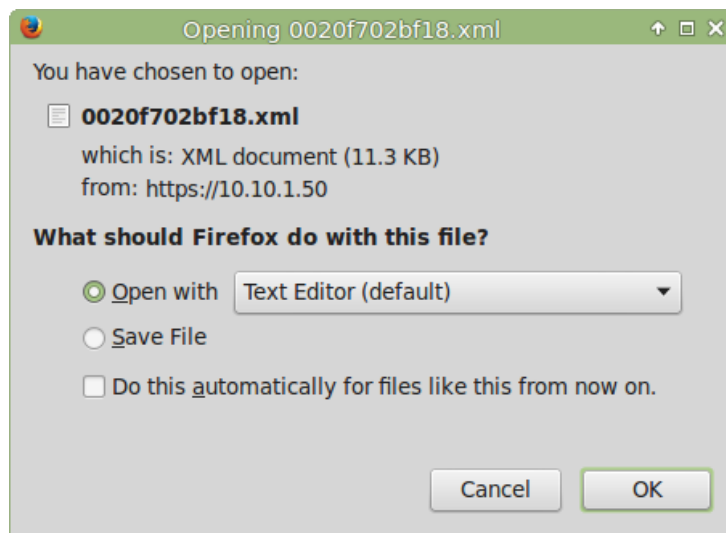
2.3.11.3 Download Template Button

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 2-27](#)). 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 2-27](#).

Figure 2-27. Configuration File



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

2.4 Upgrade the Firmware and Reboot the SIP IP66 Outdoor Horn

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:
<http://www.cyberdata.net/voip/011457/>
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 2-28](#).

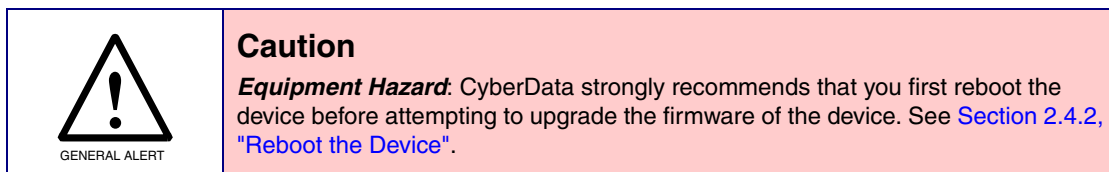


Figure 2-28. Firmware Page





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 SIP IP66 Outdoor Horn has uploaded the file, the **Uploading Firmware** countdown page appears, indicating that the firmware is being written to flash. The SIP IP66 Outdoor Horn 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 2-21](#) shows the web page items on the **Firmware** page.

Table 2-21. Firmware Parameters

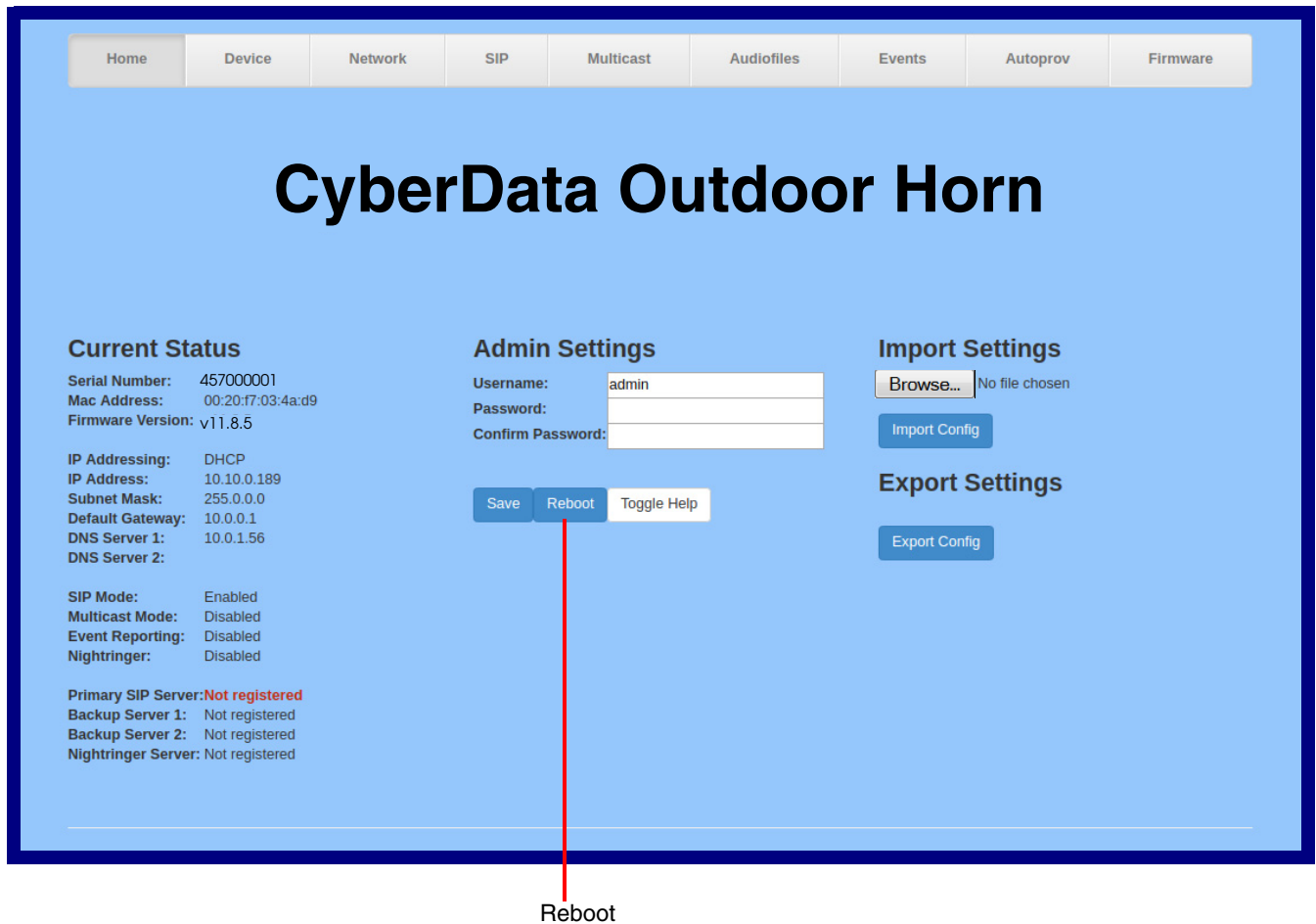
Web Page Item	Description
Current Firmware Version	Shows the current firmware version.
	Use the Browse button to navigate to the location of the firmware file that you want to upload.
	Click on the Upload button to automatically upload the selected firmware and reboot the system.

2.4.2 Reboot the Device

To reboot a SIP IP66 Outdoor Horn, 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 2-29](#)). A normal restart will occur.

Figure 2-29. 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 2-22](#) 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 2-22. 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 2-22. 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_ringtones=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 2-22. Command Interface Post Commands (continued)

Device Action	HTTP Post Command^a
Delete the "2" audio file	<code>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"</code>
Delete the "3" audio file	<code>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"</code>
Delete the "4" audio file	<code>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"</code>
Delete the "5" audio file	<code>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"</code>
Delete the "6" audio file	<code>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"</code>
Delete the "7" audio file	<code>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"</code>
Delete the "8" audio file	<code>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"</code>
Delete the "9" audio file	<code>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"</code>
Delete the "Audio Test" audio file	<code>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"</code>
Delete the "Page Tone" audio file	<code>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"</code>
Delete the "Your IP Address Is" audio file	<code>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"</code>
Delete the "Rebooting" audio file	<code>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"</code>
Delete the "Restoring Default" audio file	<code>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"</code>
Delete the "Ringback tone" audio file	<code>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"</code>
Delete the "Ring tone" audio file	<code>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_ringtones=yes"</code>
Delete the "Night Ring" audio file	<code>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"</code>

Table 2-22. Command Interface Post Commands (continued)

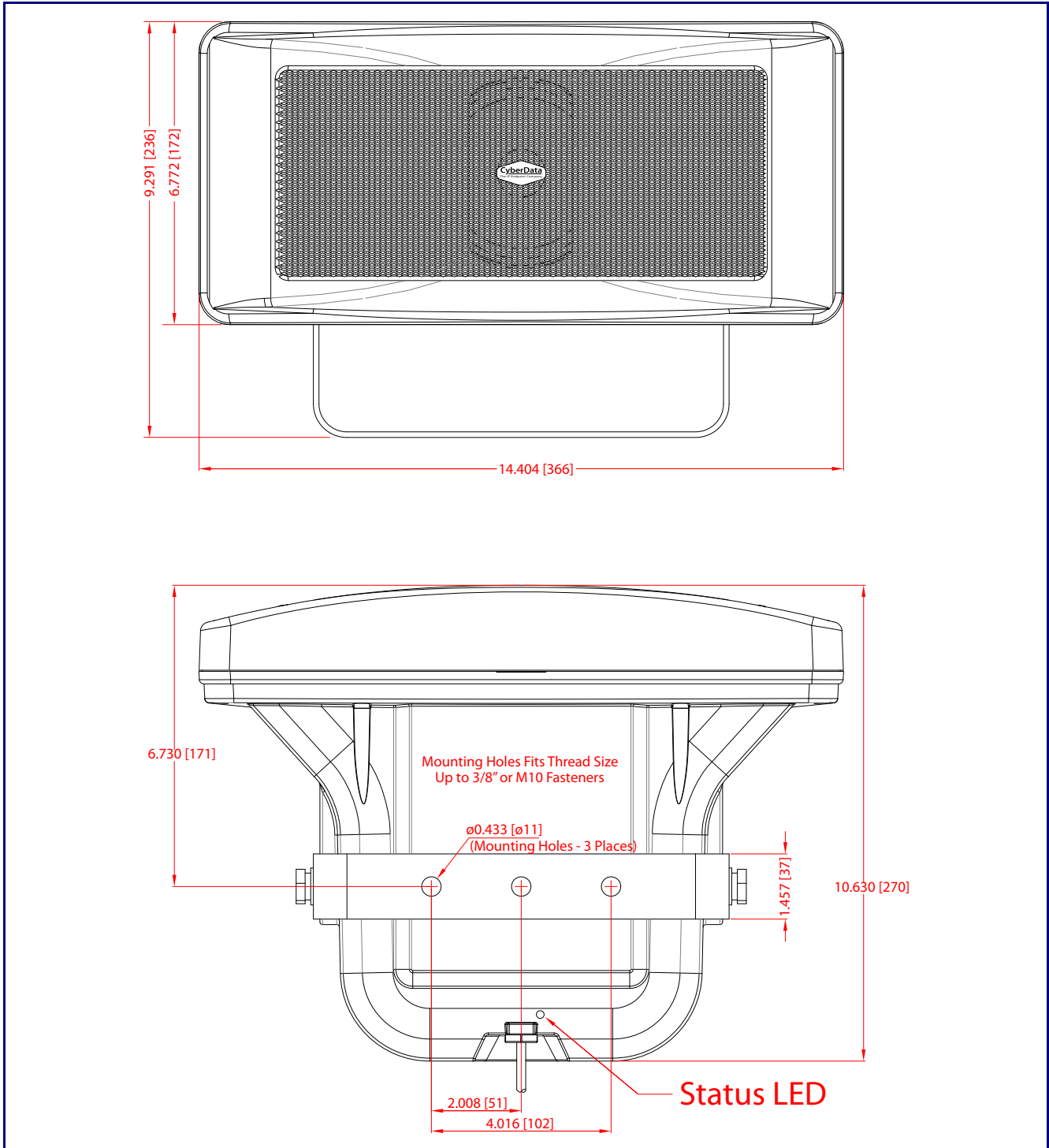
Device Action	HTTP Post Command^a
Trigger the Door Sensor Test (Sensor Config page)	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/sensor.cgi" --post-data "doortest=yes"

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

Appendix A: Mounting the Amplifier

A.1 Dimensions

Figure A-1. Dimensions



Appendix B: Setting up a TFTP Server

B.1 Set up a TFTP Server

Autoprovisioning requires a TFTP server for hosting the configuration file.

2.1.1 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
```

2.1.2 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:

<http://www.cyberdata.net/support/voip/solarwinds.html>

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:

<http://www.cyberdata.net/voip/011457/>

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:

<http://www.cyberdata.net/voip/011457/>

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 The fastest way to get technical support for your VoIP product is to submit a VoIP Technical
Support 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

A

address, configuration login 19
 announcing an IP address 14
 audio configuration 44
 night ring tone parameter 47
 audio encodings 4
 audio files, user-created 49
 audio page 44
 audio test 12
 autoprovision at time (HHMMSS) 57
 autoprovision when idle (in minutes > 10) 57
 autoprovisioning 58
 download template button 58
 autoprovisioning autoupdate (in minutes) 57
 autoprovisioning configuration 56, 57
 autoprovisioning filename 57
 autoprovisioning server (IP Address) 57

B

backup SIP server 1 33
 backup SIP server 2 33
 backup SIP servers, SIP server
 backups 33
 boost (volume) 24

C

changing
 the web access password 23
 Cisco SRST 33
 command interface 71
 commands 71
 configurable parameters 33
 configuration
 audio 44
 default IP settings 15
 network 29
 SIP 32
 configuration home page 19
 connection options 10
 connections 10
 contact information 78
 contact information for CyberData 78
 current network settings 30
 CyberData contact information 78

D

default
 gateway 9, 15
 IP address 9, 15
 subnet mask 9, 15
 username and password 9, 15
 web login username and password 19
 default gateway 9, 15, 30
 default IP settings 15
 default login address 19
 device configuration 23
 device configuration page 23
 device configuration parameters 24
 device configuration password
 changing for web configuration access 23
 DHCP Client 4
 dial out extension strings 37
 dial-out extension strings 39
 dimensions 5, 75
 discovery utility program 19
 DNS server 30
 door sensor 47
 download autoprovisioning template button 58
 DTMF tones 37, 39
 DTMF tones (using rfc2833) 37

E

enable night ring events 52
 enclosure, mounting 75
 ethernet I/F 5
 event configuration
 enable night ring events 52
 expiration time for SIP server lease 34, 35
 export settings 21

F

factory defaults 14
 firmware
 where to get the latest firmware 68

G

get autoprovisioning template 58

GMT table 27
GMT time 27

H

hazard levels 5
home page 19
http POST command 71
http web-based configuration 4

I

identifier names (PST, EDT, IST, MUT) 27
identifying your product 1
import settings 21
import/export settings 21
installation 2
IP address 9, 15, 30
IP address announcement 14
IP address confirmation 12
IP addressing
 default
 IP addressing setting 9, 15

L

lease, SIP server expiration time 34, 35
lengthy pages 43
Linux, setting up a TFTP server on 76
local SIP port 34
log in address 19

M

MGROUP
 MGROUP Name 42
multicast configuration 40, 44
Multicast IP Address 42

N

navigation (web page) 16
navigation table 16
network configuration 29
nightring tones 43
Nightringer 67
nightringer settings 34

NTP server 24

P

packet time 4
pages (lengthy) 43
parts list 8
password
 for SIP server login 33
 login 19
 restoring the default 9, 15
payload types 5
point-to-point configuration 38
polycom default channel 42
polycom emergency channel 42
polycom priority channel 42
port
 local SIP 34
 remote SIP 34
posix timezone string
 timezone string 24
POST command 71
power input 5
priority
 assigning 43
product
 parts list 8
product features 3
product overview
 product features 3
 product specifications 5
 supported protocols 4
 supported SIP servers 4
 typical system installation 2
product specifications 5
protocols supported 4

R

reboot 69, 70
remote SIP port 34
reset test function management switch 12
resetting the IP address to the default 75
restoring the factory defaults 14
ringtones 43
 lengthy pages 43
rport discovery setting, disabling 34
RTFM switch 12
RTP/AVP 4

S

- safety instructions 4
- sales 78
- server address, SIP 33
- service 78
- set time with external NTP server on boot 24
- SIP
 - enable SIP operation 33
 - local SIP port 34
 - user ID 33
- SIP (session initiation protocol) 4
- SIP configuration 32
- SIP configuration parameters
 - outbound proxy 34, 35
 - registration and expiration, SIP server lease 34, 35
 - unregister on reboot 34
 - user ID, SIP 33
- SIP registration 33
- SIP remote SIP port 34
- SIP server 33
 - password for login 33
 - SIP servers supported 4
 - unregister from 34
 - user ID for login 33
- SIP server configuration 33
- SIP volume 24
- SRST 33
- subnet mask 9, 15, 30
- supported protocols 4

T

- tech support 78
- technical support, contact information 78
- test audio 12
- TFTP server 4, 76
- time zone string examples 27

U

- user ID
 - for SIP server login 33
- username
 - changing for web configuration access 23
 - default for web configuration access 19
 - restoring the default 9, 15

V

- VLAN ID 30
- VLAN Priority 30
- VLAN tagging support 30
- VLAN tags 30
- volume
 - multicast volume 24
 - SIP volume 24
- volume boost 24

W

- warranty policy at CyberData 78
- web access password 9, 15
- web access username 9, 15
- web configuration log in address 19
- web page
 - navigation 16
- web page navigation 16
- wget, free unix utility 71
- Windows, setting up a TFTP server on 76