



SIP IP66 Indoor/Outdoor Horn Operations Guide

Part #011457
Document Part #931960B
for Firmware Version 20.6.1

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

SIP IP66 Indoor/Outdoor Horn Operations Guide 931960B
Part # 011457

COPYRIGHT NOTICE:

© 2023, CyberData Corporation, ALL RIGHTS RESERVED.

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

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

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

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

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



Technical Support

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

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

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

Email: support@cyberdata.net

Fax: (831) 373-4193

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

Revision Information

Revision 931960B, which corresponds to firmware version 20.6.1, was released on September 14, 2023, and has the following changes:

- Updates [Section 1.3, "Product Features"](#)
- Adds [Figure 2-12, "User Login Page"](#)
- Updates [Figure 2-13, "Home Page"](#)
- Adds [Figure 2-14, "Users List"](#)
- Adds [Figure 2-15, "Add New User"](#)
- Updates [Table 2-6, "Home Page Overview"](#)
- Adds [Table 2-7, "Users List"](#)
- Adds [Table 2-8, "Add New User"](#)
- Updates [Figure 2-37, "Home Page"](#)
- Updates [Appendix B, "Contact Information"](#)

Important Safety Instructions

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



Warning

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



Warning



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



Warning

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

Pictorial Alert Icons

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

Hazard Levels

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

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

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

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

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

Abbreviations and Terms

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

Chapter 1 Product Overview	1
1.1 How to Identify This Product	1
1.2 Typical System Installation	2
1.3 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 Intelligibility Outdoor Field Test	6
1.9 Compliance	7
1.9.1 CE Statement	7
1.9.2 FCC Statement	7
1.9.3 Industry Canada (IC) Compliance Statement	7
 Chapter 2 Installing the SIP IP66 Indoor/Outdoor Horn	 8
2.1 Parts List	8
2.2 SIP IP66 Indoor/Outdoor Horn Setup	9
2.2.1 SIP IP66 Indoor/Outdoor Horn System Installation and Connection Options	10
2.2.2 Install the Network Cable Through Weatherproof Cable Gland	11
2.2.3 Power Test and Status LED	12
2.2.4 RTFM Switch	13
2.3.1 Factory Default Settings	16
2.3.2 SIP IP66 Indoor/Outdoor Horn Web Page Navigation	17
2.3.3 Using the Toggle Help Button	18
2.3.4 Log in to the Home Page	20
2.3.5 Configure the Device	29
2.3.6 Configure the Audio	32
2.3.7 Configure the Network Parameters	35
2.3.8 Configure the SIP (Session Initiation Protocol) Parameters	38
2.3.9 Configure the SSL Parameters	44
2.3.10 Configure the Multicast Parameters	50
2.3.11 Configure the Audiofiles Page Parameters	54
2.3.12 Configure the Events Parameters	60
2.3.13 Configure the Autoprovisioning Parameters	65
2.4 Upgrade the Firmware	77
2.4.1 Reboot the Device	80
2.5.1 Command Interface Post Commands	81
 Appendix A Mounting the SIP IP66 Indoor/Outdoor Horn	 82
A.1 Dimensions	82
 Appendix B Troubleshooting/Technical Support	 83
B.1 Frequently Asked Questions (FAQ)	83
B.2 Documentation	83
B.3 Contact Information	84
B.4 Warranty and RMA Information	84
 Index	 85

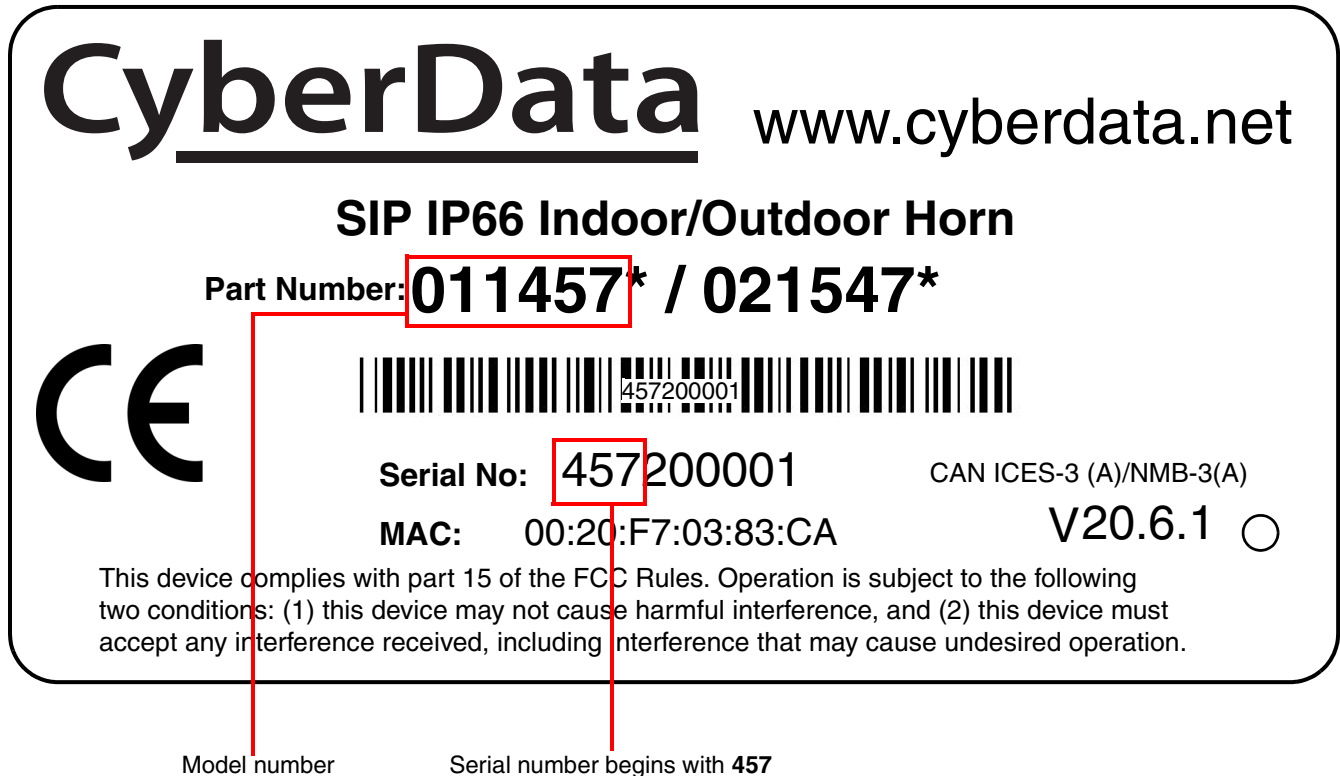
1 Product Overview

1.1 How to Identify This Product

To identify the SIP IP66 Indoor/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**.

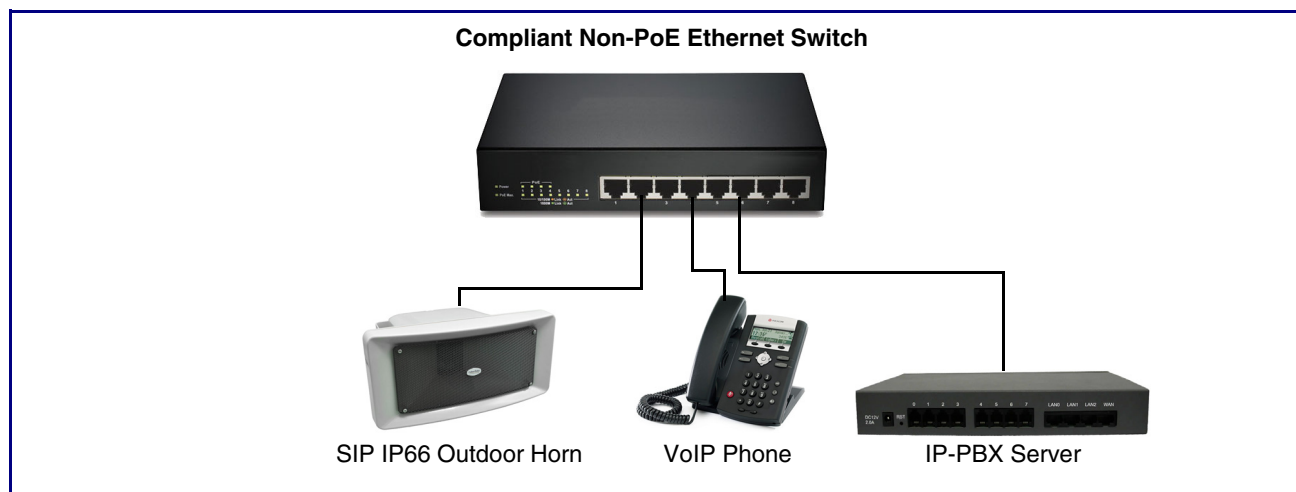
Figure 1-1. Model Number Label



1.2 Typical System Installation

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

Figure 1-2. Typical Installation



1.3 Product Features

- Concurrent SIP and multicast
 - Paging prioritization
 - Support for 10 multicast paging groups
 - Supports user-uploadable ring tones and up to ten stored messages
 - Ambient Noise Compensation adjusts the volume, at the start of a stream, to adjust to noise in the environment
 - Support for security code to prevent unwanted SIP calls
 - Supports multiple user accounts, with distinct log in credentials
 - Can receive pages directly from Poly phones as well as other devices that can send standard multicast
 - Loud/Night Ringer function - second SIP extension
 - Supports delayed pages with call buffering
 - Audio health check, to verify operation of hardware, that can be scheduled or launched manually
-
- Digital volume control
 - Sealed network cable gland
 - Protective screen keeps out flying pests and reduces maintenance
-
- TLS 1.2 and SRTP enhanced security for IP Endpoints in a local or cloud-based environment
 - Autoprovisioning via HTTP, HTTPS, or TFTP
 - HTTPS web-based configuration.
 - 802.11q VLAN tagging
 - Configurable event generation for device health and status monitoring
 - Support for Cisco SRST resiliency

1.4 Supported Protocols

The SIP IP66 Indoor/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 Indoor/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
- SRTP
- TLS 1.2
- SPEEX

- Audio Encodings

PCMU (G.711 mu-law)

PCMA (G.711 A-law)

G.722

G.729

Packet Time 20 ms

1.5 Supported SIP Servers

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

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

1.6 Specifications

Table 1-1. Specifications

Specifications	
Ethernet I/F	10/100 Mbps
Protocol	SIP RFC 3261 Compatible
Power Input	PoE 802.3at or 802.3af
Audio Output	802.3at: 107.7 (+/- 0.2) dBC @1M and 1kHz 802.3af: 104.8 (+/- 0.2) dBC @1M and 1kHz
Payload Types	G.711 a-law, G.711 u-law, G.722, and G.729
Network Security	TLS 1.2, SRTP, HTTPS
IP Rating	IP66
Operating Range	Temperature: -40° C to 55° C (-40° F to 131° F) Humidity: 5-95%, non-condensing
Storage Temperature	-40° C to 70° C (-40° F to 158° F)
Storage Altitude	Up to 15,000 ft. (4573 m)
Dimensions ^a	Length: 14.404 in. [366 mm] Width: 10.630 in. [270 mm] Height: 6.772 in. [172 mm] (without stand) Height: 9.291 in. [236 mm] (with stand)
Weight	6.6 lbs. [3.00 kg]
Boxed Weight	8.8 lbs. [3.99 kg]
Compliance	CE: EMC Directive – Class A EN 55032 & EN 55024, LV Safety Directive – EN 62368-1; RoHS Compliant; FCC Part 15 Class A; Industry Canada ICES-3 Class A; IEEE 802.3 Compliant; TAA Compliant
Warranty	2 Years Limited
Part Number	011457

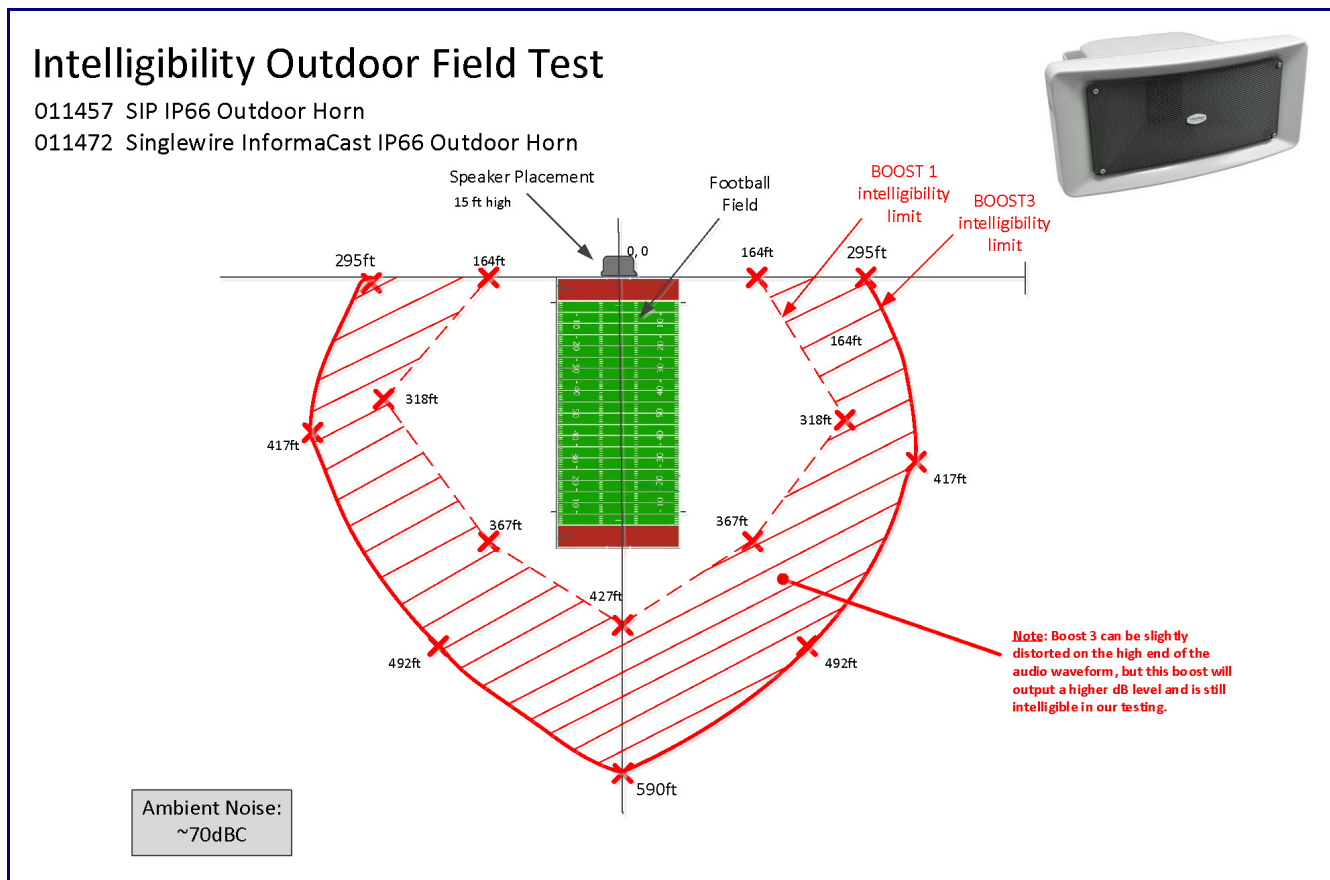
a. Dimensions are measured from the perspective of the product being upright with the front of the product facing you.

1.7 Typical Coverage

The horn is designed for use with PoE 802.3at power. When the device is allocated this power, it can cover up to 7,500 square feet depending on ambient noise levels.

1.8 Intelligibility Outdoor Field Test

Figure 1-3. Intelligibility Outdoor Field Test



1.9 Compliance

1.9.1 CE Statement



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

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

1.9.2 FCC Statement



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

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

1.9.3 Industry Canada (IC) Compliance Statement

Operation is subject to the following two conditions:

- 1.This device may not cause interference, and
- 2.This device must accept any interference, including interference that may cause undesired operations of the device.



ICES-3 Class A

2 Installing the SIP IP66 Indoor/Outdoor Horn

2.1 Parts List

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

Table 2-2. Parts List

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

2.2 SIP IP66 Indoor/Outdoor Horn Setup

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

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

Table 2-3. Factory Default Settings

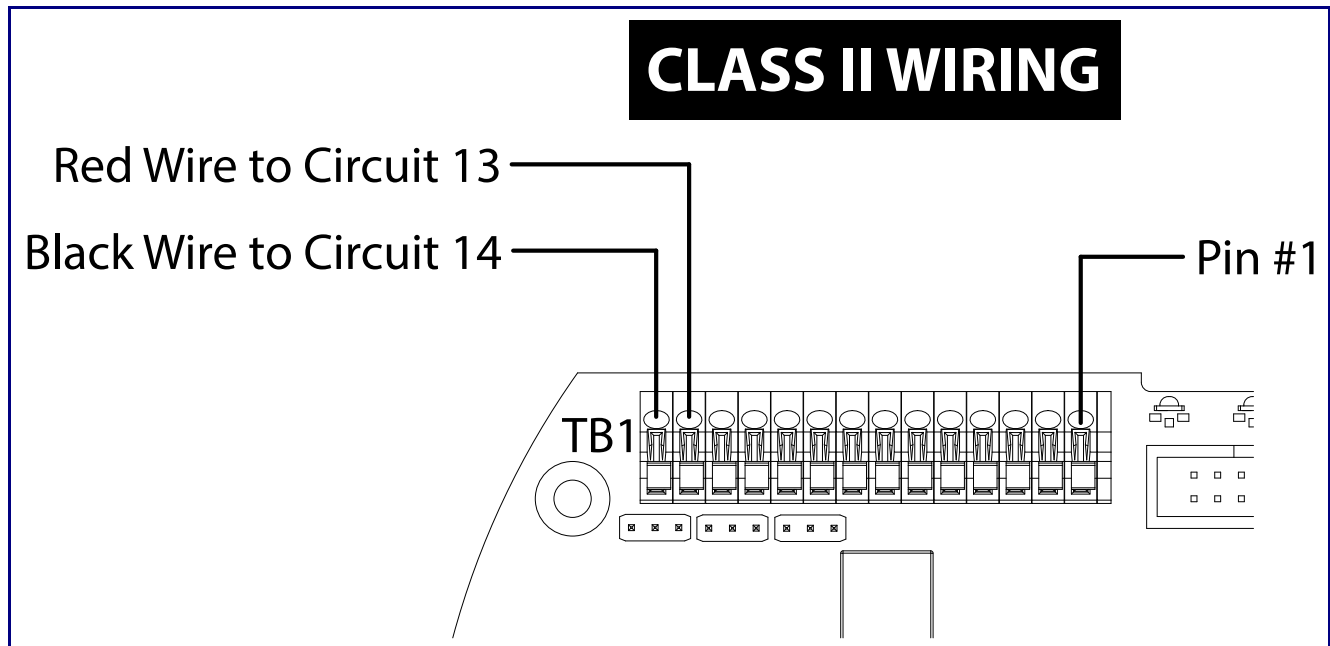
Parameter	Factory Default Setting
IP Addressing	DHCP
IP Address ^a	192.168.1.23
Web Access Username	admin
Web Access Password	admin
Subnet Mask ^a	255.255.255.0
Default Gateway ^a	192.168.1.1

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

2.2.1 SIP IP66 Indoor/Outdoor Horn System Installation and Connection Options

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

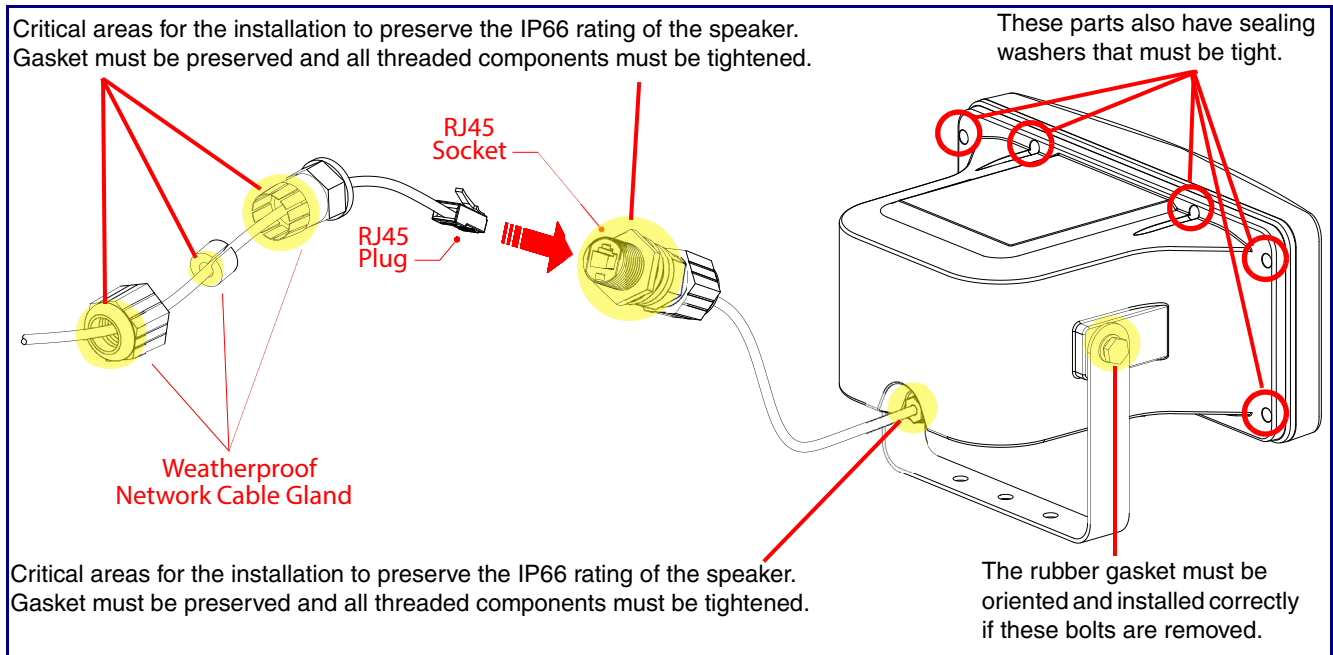
Figure 2-4. SIP IP66 Indoor/Outdoor Horn Connections



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](#).

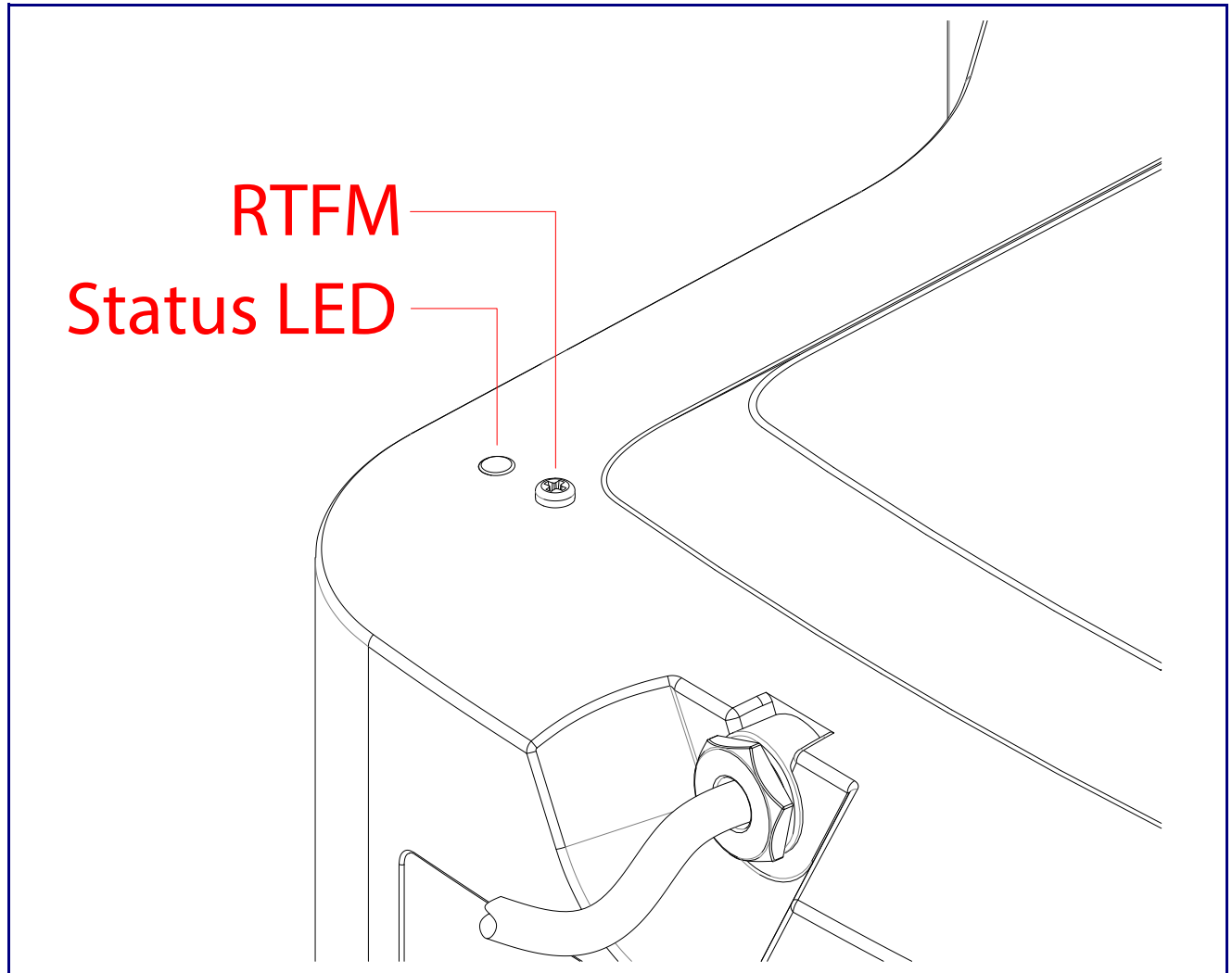
Figure 2-5. Install the Network Cable Through Weatherproof Cable Gland



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 192.168.1.23) 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.

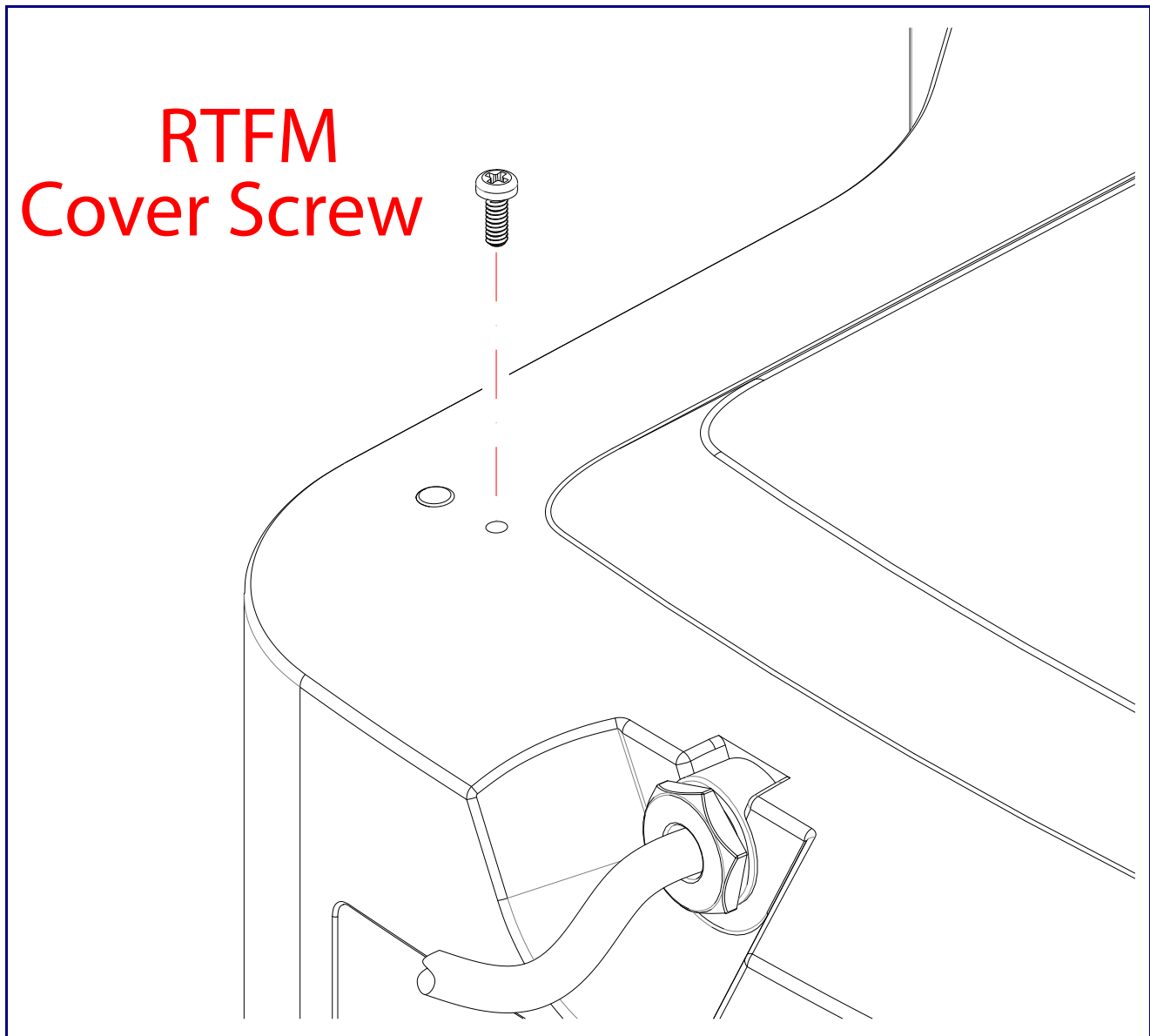
2.2.4 RTFM Switch

When the SIP IP66 Indoor/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

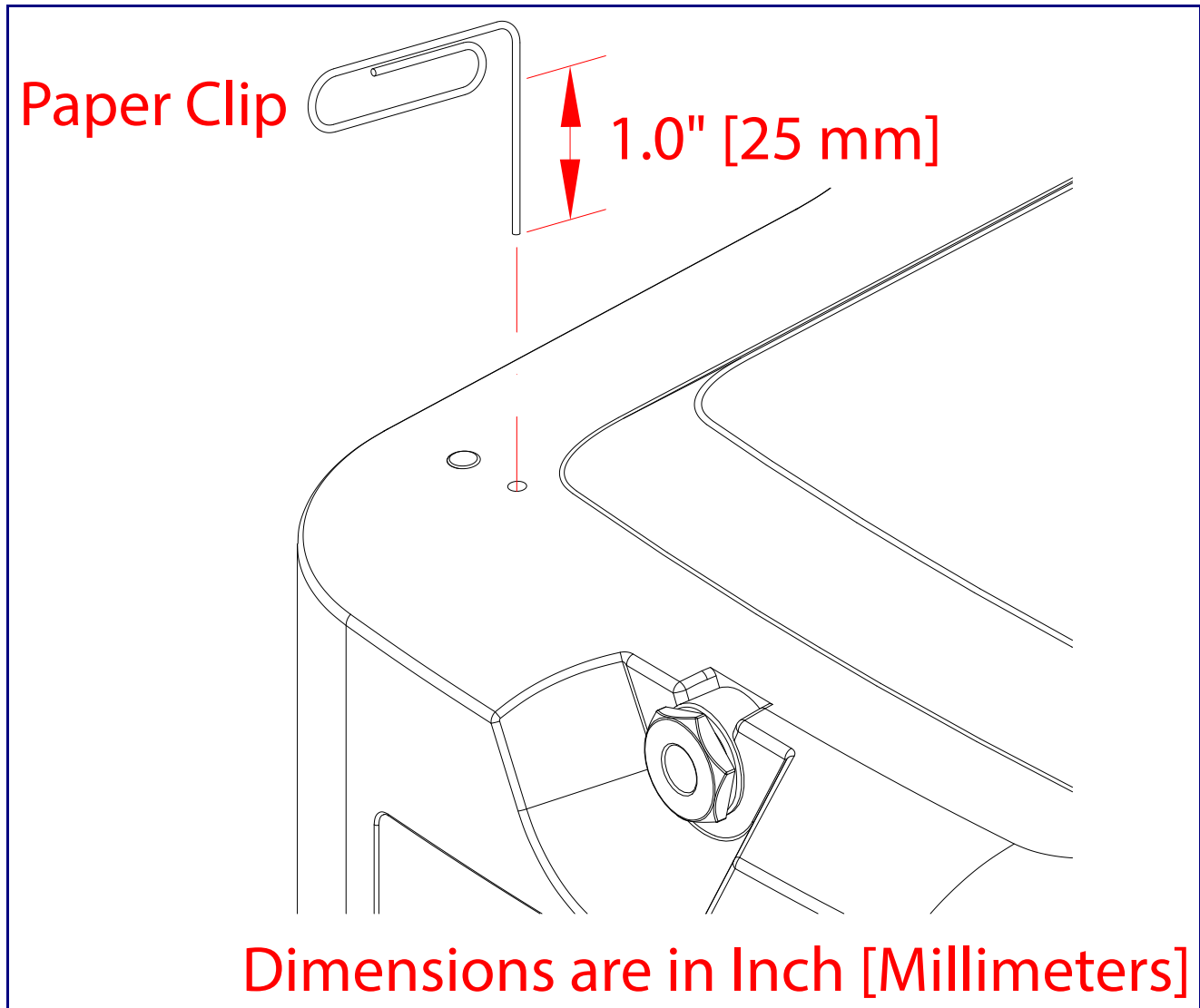
The RTFM switch access will be on the bottom side of the horn hidden under a screw (Figure 2-7) that will be used to keep the unit IP66 sealed with the gasket washer. Remove the screw to gain access to the RTFM switch (Figure 2-8).

Figure 2-7. Remove the screw to gain access to the RTFM switch



4. Use a paper clip to feed through the hole to press the RTFM switch. 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.



Caution

Equipment Caution: Pressing and holding the RTFM switch for more than five seconds will restore the device to the factory default settings. See the “[Restoring the Factory Default Settings](#)” section.

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 Indoor/Outdoor Horn Parameters

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

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

2.3.1 Factory Default Settings

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

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

Table 2-4. Factory Default Settings

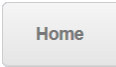
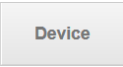
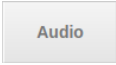




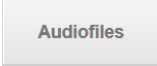
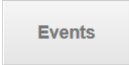
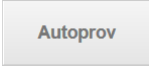

Parameter	Factory Default Setting
IP Addressing	DHCP
IP Address ^a	192.168.1.23
Web Access Username	admin
Web Access Password	admin
Subnet Mask ^a	255.255.255.0
Default Gateway ^a	192.168.1.1

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

2.3.2 SIP IP66 Indoor/Outdoor Horn Web Page Navigation

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

Table 2-5. Web Page Navigation

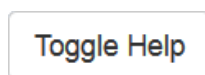
Web Page Item	Description
	Link to the Home page.
	Link to the Device page.
	Link to the Audio page.
	Link to the Network page.
	Link to go to the SIP page.
	Link to the Multicast page.
	Link to the SSL page.
	Link to the Audiofiles page.
	Link to the Events page.
	Link to the Autoprovisioning page.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

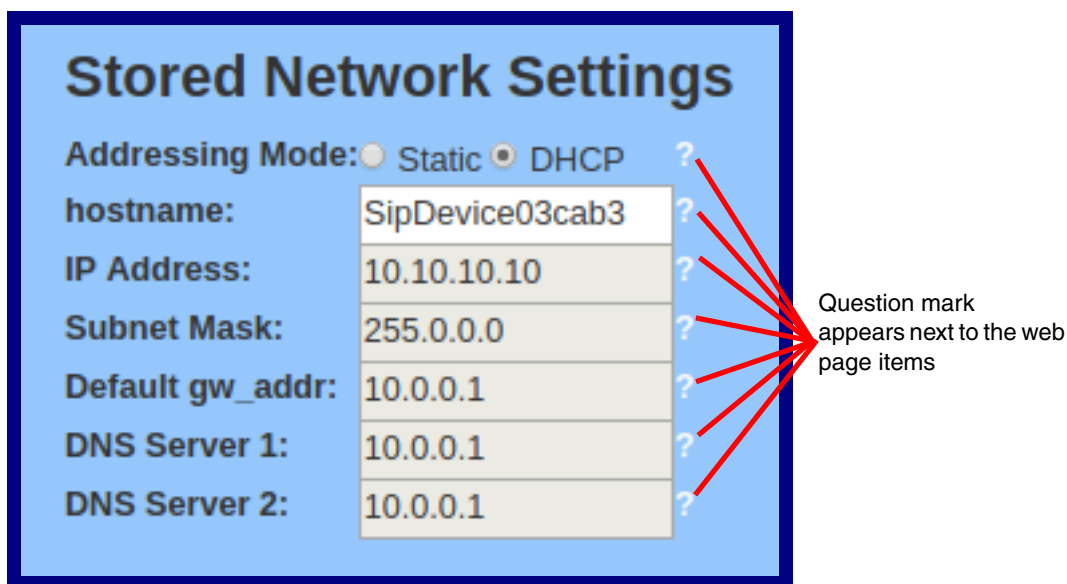
1. Click on the **Toggle Help** button that is on the UI webpage. See [Figure 2-9](#) and [Figure 2-10](#).

Figure 2-9. Toggle/Help Button



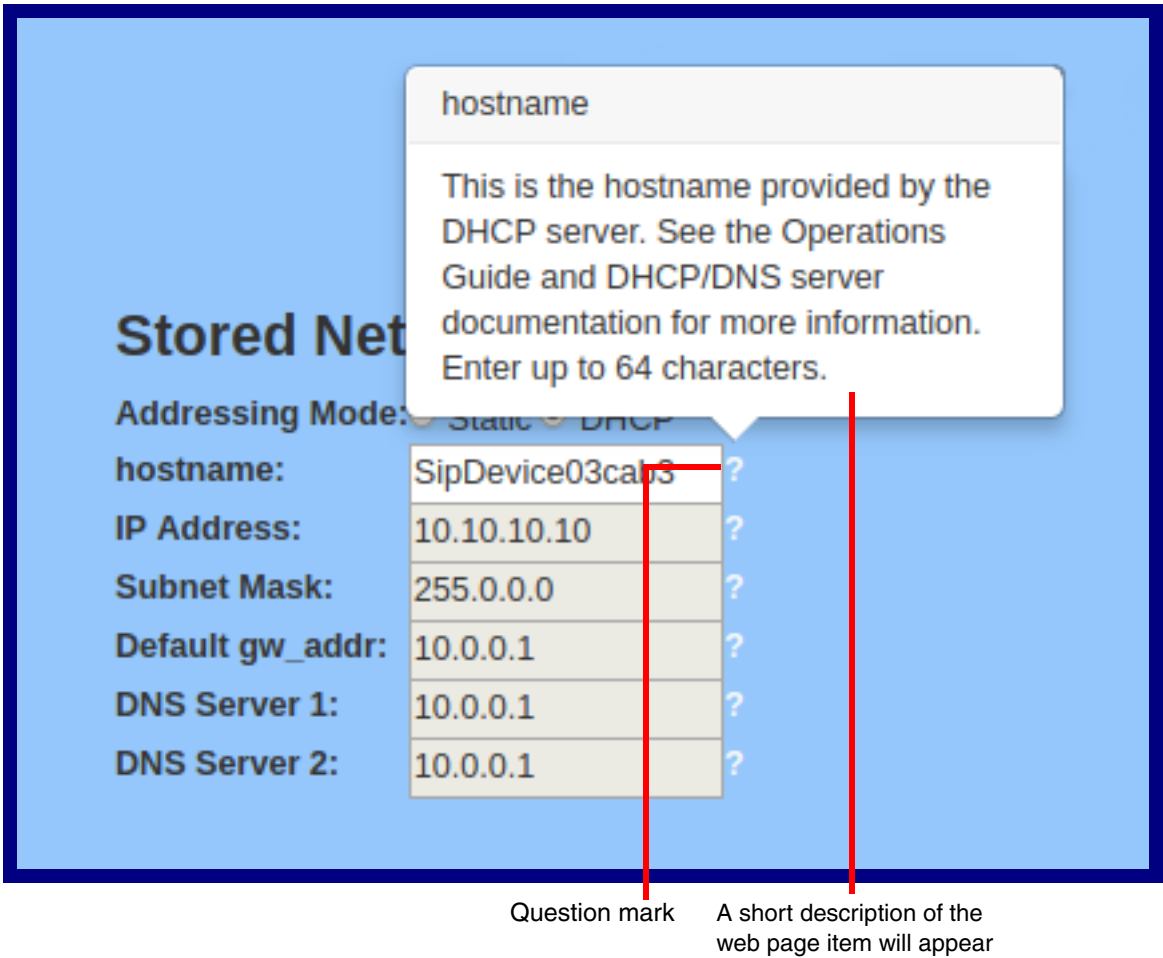
2. You will see a question mark (?) appear next to each web page item that has been provided with a short description by the Help feature. See [Figure 2-10](#).

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 192.168.1.23.

Note Make sure that the PC is on the same IP network as the SIP IP66 Indoor/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:

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

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

Note To work with the SIP IP66 Indoor/Outdoor Horn configuration *after* the initial configuration, log in using the IP address you assign to the device. [Section 2.3.7, "Configure the Network Parameters"](#) provides instructions for entering the IP address.

2. Use the following default username and password on the **User Login** page. ([Figure 2-12](#)):

username: **admin**

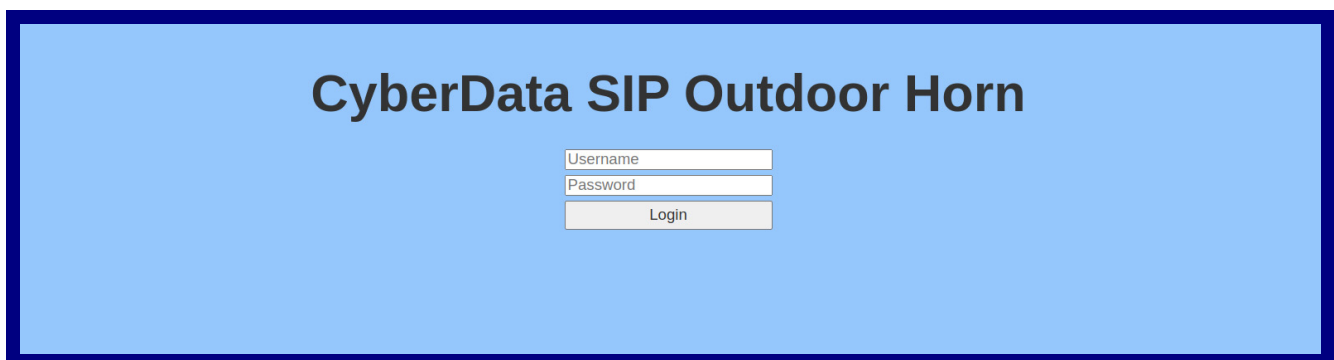
password: **admin**

Change the
Default Username
and Password

To change the default web access username and password from the **Home** page ([Figure 2-13](#)):

1. Enter the new username from four to 25 alphanumeric characters in the **Change Username** field. The username is case-sensitive.
2. Enter the new Password from four to 20 alphanumeric characters in the **Change Password** field. The Password is case-sensitive.
3. Enter the new password again in the **Re-enter New Password** field.
4. Click **Save Settings**.

Figure 2-12. User Login Page



CyberData SIP Outdoor Horn

Username

Password

Login

Figure 2-13. Home Page

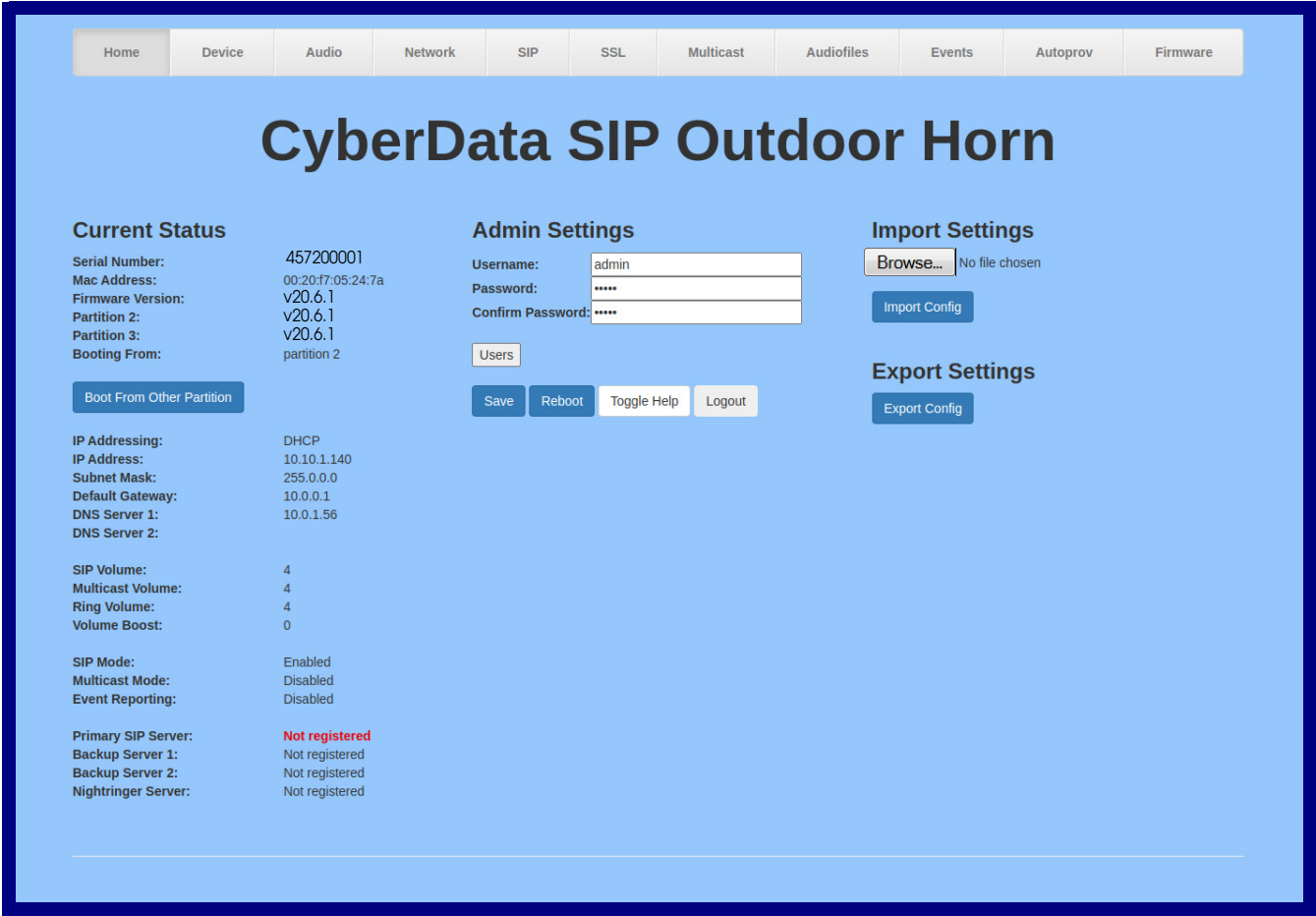


Figure 2-14. Users List

HomeDeviceAudioNetworkSIPSSLMulticastAudiofilesEventsAutoprovFirmware

CyberData SIP Outdoor Horn

Users List

Add New UserDelete AllImport UsersExport UsersLogout

Username	Home	Device	Audio	Network	SIP	SSL	Multicast	Audiofiles	Events	Autoprov	Firmware		
Olivia	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Edit	Delete
Liam	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Edit	Delete
Emima	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Edit	Delete
Noah	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Edit	Delete
Amelia	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Edit	Delete
Oliver	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Edit	Delete
Ava	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Edit	Delete
Elijah	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Edit	Delete
Sophia	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Edit	Delete
Mateo	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Edit	Delete
Isabella	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Edit	Delete
Lucas	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Edit	Delete
Luna	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Edit	Delete

Figure 2-15. Add New User

Add New User

Username: A-Z, a-z, -, _

Password: Confirm Password:

Authorized Pages

HomeDeviceAudioNetworkSIPSSLMulticastAudiofilesEventsAutoprovFirmware

☐☐☐☐☐☐☐☐☐☐☐☐

SaveCancel

5. 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

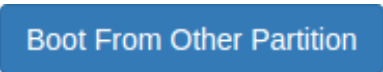
Web Page Item	Description
Current Status	
Serial Number	Shows the device serial number.
Mac Address	Shows the device Mac address.
Firmware Version	Shows the current firmware version.
Partition 2	Contains a complete copy of bootable software.
Partition 3	Contains an alternate, complete copy of bootable software.
Bootting From	Indicates the partition currently used for boot.
	Allows the user to boot from the alternate partition.
IP Addressing	Shows the current IP addressing setting (DHCP or static).
IP Address	Shows the current IP address.
Subnet Mask	Shows the current subnet mask address.
Default Gateway	Shows the current default gateway address.
DNS Server 1	Shows the current DNS Server 1 address.
DNS Server 2	Shows the current DNS Server 2 address.
SIP Volume	Shows the current SIP volume level.
Multicast Volume	Shows the current Multicast volume level.
Ring Volume	Shows the current Ring volume level.
Volume Boost	Shows the current Volume Boost level.
SIP Mode	Shows the current status of the SIP mode.
Multicast Mode	Shows the current status of the Multicast mode.
Event Reporting	Shows the current status of the Event Reporting mode.
Nightringer	Shows the current status of the Nightringer mode.
Primary SIP Server	Shows the current status of the Primary SIP Server.
Backup Server 1	Shows the current status of Backup Server 1.
Backup Server 2	Shows the current status of Backup Server 2.
Nightringer Server	Shows the current status of Nightringer Server.
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.
Import Settings	

Table 2-6. Home Page Overview (continued)







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

Figure 2-16. Users List

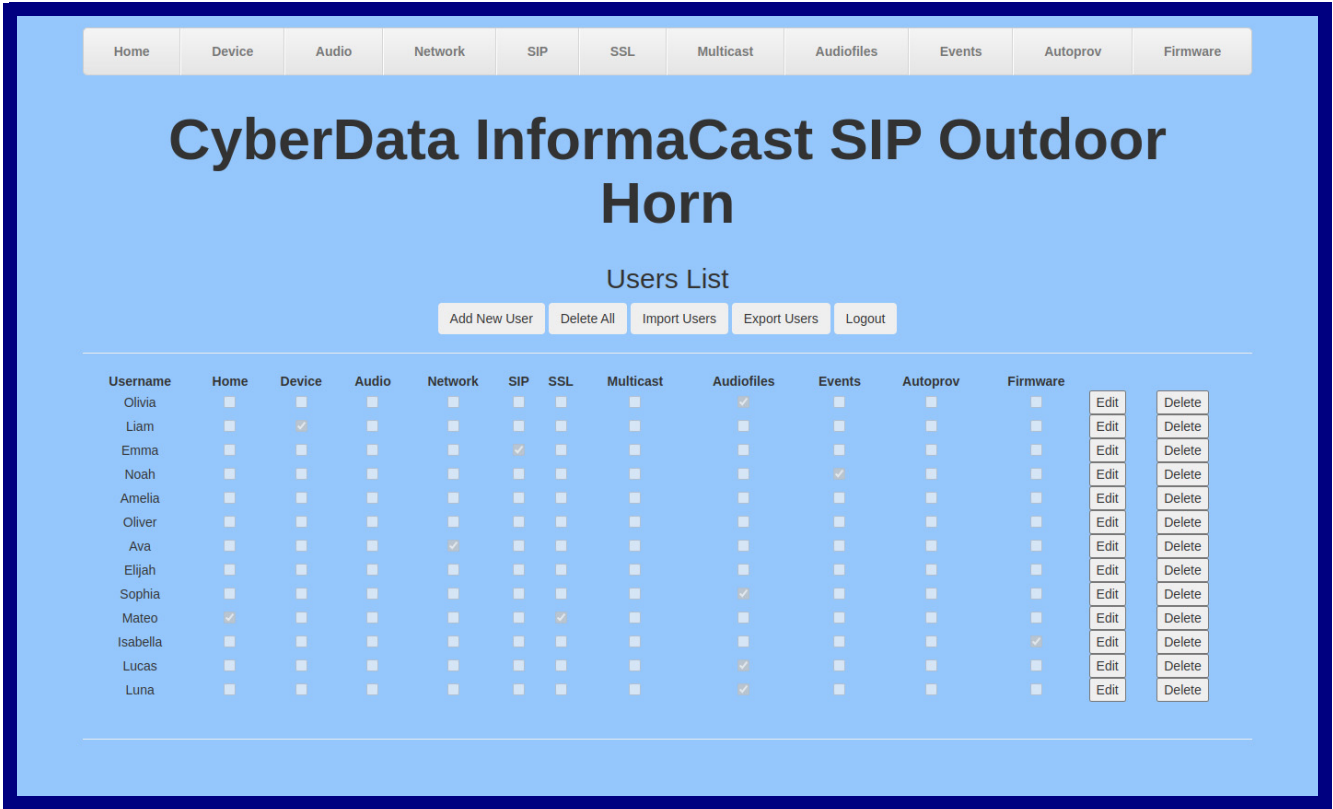


Table 2-7. Users List

Web Page Item	Description
Users List	
Add New User	Adds an authorized user to the user list
Delete All	Deletes all users from the current list
Import Users	Imports a previously exported user list
Export Users	Saves the current user list as a .json file. Please note that the data is encrypted and cannot be edited outside of the Paging Server Users dialog box.
Logout	Logs out the current user and returns to the user log in page
Edit	Allows administrator to modify the user's profile
Delete	Deletes the profile
Username	Name of the user

Table 2-7. Users List

Web Page Item	Description
Home	Authorizes a user to view the Home page, allowing the user to see status, but does not grant administrative privileges.
Device	Authorizes a user to view and edit the Device web page.
Audio	Authorizes a user to view and edit the Audio web page.
Network	Authorizes a user to view and edit the Network web page.
SIP	Authorizes a user to view and edit the SIP web page.
SSL	Authorizes a user to view and edit the SSL web page.
Multicast	Authorizes a user to view and edit the Multicast web page.
Audiofiles	Authorizes a user to view and edit the Audiofiles web page.
Events	Authorizes a user to view and edit the Events web page.
Autoprov	Authorizes a user to view and edit the Autoprov web page.
Firmware	Authorizes a user to view and edit the Firmware web page.

Figure 2-17. Add New User

Add New User

Username:

Password:

Confirm Password:

Authorized Pages

Home

Device

Audio

Network

SIP

SSL

Multicast

Audiofiles

Events

Autoprov

Firmware

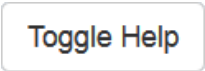
Save

Cancel

Table 2-8. Add New User

Web Page Item	Description
Add New User	
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.
Authorized Pages	
Home	Authorizes a user to view the Home page, allowing the user to see status, but does not grant administrative privileges.
Device	Authorizes a user to view and edit the Device web page.
Audio	Authorizes a user to view and edit the Audio web page.
Network	Authorizes a user to view and edit the Network web page.
SIP	Authorizes a user to view and edit the SIP web page.
SSL	Authorizes a user to view and edit the SSL web page.
Multicast	Authorizes a user to view and edit the Multicast web page.
Audiofiles	Authorizes a user to view and edit the Audiofiles web page.
Events	Authorizes a user to view and edit the Events web page.
Autoprov	Authorizes a user to view and edit the Autoprov web page.
Firmware	Authorizes a user to view and edit the Firmware web page.
Save	Click the Save button to save your configuration settings.
Cancel	Closes the dialog box without saving changes

Table 2-8. Add New User(continued)

Web Page Item	Description
	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 2-18](#).

Figure 2-18. Device Page

Home Device Audio Network SIP SSL Multicast Audiofiles Events Autopro Firmware

CyberData SIP Outdoor Horn

Clock Settings

Enable NTP: ☒
NTP Server:
Timezone:
Current Time: Tue, 19 Jul 2022 13:52:50

DTMF Settings

Require Security Code: ☐
Security Code:
Play Stored Message: ☐

Misc Settings

Device Name:
Beep on Init: ☐
Beep Before Page: ☐

Power Settings

802.3AT Mode: Not detected. Disabled
Force 802.3AT Mode (NOT recommended): ☐





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

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

Table 2-9. Device Page Parameters

Web Page Item	Description
Clock Settings	
Enable NTP ?	Sync device's local time with the specified NTP Server.
NTP Server ?	Use this field to set the address (in IPv4 dotted decimal notation or as a canonical name) for the NTP Server. This field can accept canonical names of up to 64 characters in length.
Timezone	Enter the tz database string of your timezone. Examples: America/Los_Angeles America/New_York Europe/London America/Toronto See https://en.wikipedia.org/wiki/List_of_tz_database_time_zones for a full list of valid strings.
Current Time	Displays the current time.
Misc Settings	
Device Name ?	Type the device name. Enter up to 25 characters.
Beep on Init ?	Device will play the user-defined "pagetone" audio file when it boots.
Beep Before Page ?	Device will play the user defined "pagetone" audio file before playing a SIP page.
DTMF Settings	
Require Security Code ?	When selected, the user will be prompted to enter a Security Code (entered on this page) before being able to execute a page when calling the device.
Security Code ?	Type the Security Code in this field. The Security Code must only use characters '0-9', '*' and '#'. Enter up to 25 characters.
Play Stored Message ?	When selected, the caller will be prompted to select one of nine stored messages to play through the speaker. Stored messages may be customized on the Audiofiles page.
Power Settings	
802.3AT Mode ?	This device automatically detects if it is plugged into an 802.3AT (also known as PoE Plus) power source. 802.3AT provides more power than older 802.3AT power sources and allows this speaker to play audio at higher volumes. If you are sure this speaker is connected to an 802.3AT power source, but it is not being detected correctly, you can override the automatic settings below.
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).

Table 2-9. Device Page Parameters (continued)

Web Page Item	Description
	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.
	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.

2.3.6 Configure the Audio

1. Click the **Audio** menu button to open the **Audio** page. See [Figure 2-19](#).

Figure 2-19. Audio Page

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

CyberData SIP Outdoor Horn

Volume Settings (0-9)

Enable Ambient Noise Compensation (ANC) ☐

SIP Volume: 4

Multicast Volume: 4

Ring Volume: 4

Volume Boost: No Volume Boost

Test Audio

Audio Health Check

Schedule Audio Health Check: ☐

Run once per: ☐ Day ☐ Week ☐ Month

Time of Day (HH:MM): 00 : 00

Day of Week: Sunday

Day of Month (1-31): 1

Run Audio Health Check

Save Reboot Toggle Help

Audio Health Check Log

Health check log removed

Download Health Check Log Remove Health Check Log


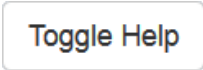
2. On the **Audio** page, you may enter values for the parameters indicated in [Table 2-10](#).

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

Table 2-10. Audio Page Parameters

Web Page Item	Description
Volume Settings (0-9)	
Enable Ambient Noise Compensation (ANC) ?	When selected, the device will measure the ambient sound level in the area and adjust the volume of the speaker accordingly.
SIP Volume ?	Set the speaker volume for a SIP call. A value of 0 will mute the speaker during SIP calls.
Multicast Volume ?	Set the speaker volume for multicast audio streams. A value of 0 will mute the speaker during multicasts.
Ring Volume ?	Set the ring volume for the Nightringer. A value of 0 will mute the speaker for the Nightringer.
Volume Boost: ? No Volume Boost Volume Boost 1 Volume Boost 2 Volume Boost 3	NOT RECOMMENDED! Set the Boost level to increase the volume output of the speaker. Using Volume Boost may introduce audio clipping, reduce intelligibility of the speaker audio, or cause instability. Boost will raise the volume above level '9', regardless of the digital volumesettings. If Boost is going to be used, it should be used with low gain audio sources and at a low volume output level.
Test Audio	Click on the Test Audio button to do an audio test. When the Test Audio button is pressed, you will hear a voice message for testing the device audio quality and volume.
Audio Health Check	
Schedule Audio Health Check ?	Select this option to schedule an audio health check.
Run once per ?	Select how often to run the audio health check.
Time of Day ?	Enter the time of day to run the audio health check.
Day of Week ?	Select the day of the week to run the audio health check.
Day of Month ?	Enter the day of the month to run the audio health check.
Run Audio Health Check	The audio health check will run once this button is clicked. Once the test has completed, the results can be viewed in the audio health check log displayed on the web page.
Audio Health Check Log	
Download Health Check Log	Downloads the health check log.
Remove Health Check Log	Removes the health check log.
Save	Click the Save button to save your configuration settings.

Table 2-10. Audio Page Parameters (continued)

Web Page Item	Description
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

2.3.7 Configure the Network Parameters

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

Figure 2-20. Network Page

HomeDeviceAudioNetworkSIPSSLMulticastAudiofilesEventsAutoprovFirmware

CyberData SIP Outdoor Horn

Stored Network Settings

Addressing Mode:

Static

DHCP

Hostname:

SipDevice04ec3a

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

VLAN Settings

VLAN ID (0-4095):

0

VLAN Priority (0-7):

0

Save

Reboot

Toggle Help

Current Network Settings

IP Address:

10.10.1.162

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 2-11](#).

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

Table 2-11. 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 2-11. Network Page Parameters (continued)

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

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

2.3.8 Configure the SIP (Session Initiation Protocol) Parameters

1. Click on the **SIP** menu button to open the **SIP** page (Figure 2-21).

Figure 2-21. SIP Page

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

CyberData SIP Outdoor Horn

SIP Settings

Enable SIP operation: ☒
Register with a SIP Server: ☒
Buffer SIP Calls: ☐
Primary SIP Server: 10.0.0.253
Primary SIP User ID: 199
Primary SIP Auth ID: 199
Primary SIP Auth Password: *****
Re-registration Interval (in seconds): 360

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

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

Remote SIP Port: 5060
Local SIP Port: 5060

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

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

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

Nightringer Settings

SIP Server: Host or IP address
Remote SIP Port: 5060
Local SIP Port: 5061
Outbound Proxy: Host or IP address
Outbound Proxy Port: 0
SIP User ID: User ID
SIP Auth ID: Auth ID
SIP Auth Password: Password
Re-registration Interval (in seconds): 360

Call Disconnection

Terminate Call after delay: 0

Audio Codec Selection

Codec: Auto Select

RTP Settings

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

Save **Reboot** **Toggle Help**

2. On the **SIP** 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. SIP Page Parameters

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

Table 2-12. SIP Page Parameters (continued)

Web Page Item	Description
Backup SIP Auth ID 2 ?	Specify the Authenticate ID for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Auth Password 2 ?	Specify the Authenticate Password for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Re-registration Interval (in seconds) ?	The SIP Re-registration interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
Remote SIP Port ?	The Remote SIP Port is the port number the device will use as the destination port when sending SIP messages. The default Remote SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
Local SIP Port ?	The Local SIP Port is the port number the device will use to receive SIP messages. The default Local SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
SIP Transport Protocol ?	Choose the transport protocol for SIP signaling. This will affect all extensions, including the Nightringer. Default is UDP.
TLS Version ?	Choose the TLS version for SIP over TLS. Modern security standards strongly recommend using TLS 1.2.
Verify Server Certificate ?	When enabled, the device will verify the authenticity of the server during the TLS handshake by its certificate and common name. The TLS handshake will be aborted if the server is deemed to be inauthentic and SIP registration will not proceed.
Outbound Proxy ?	Enter the Outbound Proxy address as an IPv4 address in dotted decimal notation or a fully qualified domain name (FQDN). When an IP address is configured, the device will send all SIP messages to this IP address. When an FQDN is configured, the device will run DNS NAPTR, SRV, and A queries on the FQDN to resolve an IP address to which it will send all SIP messages. This field can accept entries of up to 255 characters in length.
Outbound Proxy Port ?	The Outbound Proxy Port is port number used as the destination port when sending SIP messages to the outbound proxy. A value of 0 will default to 5060. The supported range is 0-65536. Enter up to 5 digits.
Use Cisco SRST ?	When enabled, the backup servers are handled according to Cisco SRST (Survivable Remote Site Telephony). It is required for use in clustered Cisco Unified Communications Manager topologies.
Disable rport Discovery ?	Disabling rport Discovery will prevent the device from including the public WAN IP address and port number in the contact information that is sent to the remote SIP servers. This will generally only need to be enabled when using an SBC or SIP ALG in conjunction with a remote SIP server.
Keep Alive Period ?	The minimum time in milliseconds between keep-alive packets sent for nat traversal. A value of 0 will disable keep alive packets.
Nightringer Settings	
Enable Nightringer ?	When Nightringer is enabled, the device will attempt to register a second extension with the SIP server. Any calls made to this extension will play a ringtone (corresponds to Night Ring on the Audiofiles page). By design, it is not possible to answer a call to the Nightringer extension.
SIP Server ?	Enter the SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's Nightringer extension on the SIP server. This field can accept entries of up to 255 characters in length.








Table 2-12. SIP Page Parameters (continued)

Web Page Item	Description
Remote SIP Port ?	The Remote SIP Port is the port number the device will use as the destination port when sending SIP messages for the Nightringer extension. The default Remote SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
Local SIP Port ?	The Local SIP Port is the port number the device will use to receive SIP messages for the Nightringer extension. This value cannot be the same as the Local SIP Port for the primary extension. The default Local SIP Port is 5061. The supported range is 0-65536. Enter up to 5 digits.
Outbound Proxy ?	Enter the Outbound Proxy address as an IPv4 address in dotted decimal notation or a fully qualified domain name (FQDN). When an IP address is configured, the device will send all SIP messages to this IP address for the Nightringer extension. When an FQDN is configured, the device will run DNS NAPTR, SRV, and A queries on the FQDN to resolve an IP address to which it will send all SIP messages for the Nightringer extension. This field can accept entries of up to 255 characters in length.
Outbound Proxy Port ?	The Outbound Proxy Port is port number used as the destination port when sending SIP messages to the outbound proxy for the Nightringer extension. A value of 0 will default to 5060. The supported range is 0-65536. Enter up to 5 digits.
SIP User ID ?	Specify the SIP User ID for the SIP server. This parameter becomes the user portion of the SIP-URI for the device's Nightringer extension. Enter up to 64 alphanumeric characters.
SIP Auth ID ?	Specify the Authenticate ID for the SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
SIP Auth Password ?	Specify the Authenticate Password for the SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Re-registration Interval (in seconds) ?	The SIP Re-registration Interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
Call Disconnection	
Terminate Call After Delay ?	Automatically terminate an active call after a given delay in seconds. A value of 0 will disable this function. Enter up to 8 digits.
Audio Codec Selection	
Codec ?	Select desired codec (only one may be chosen).

Table 2-12. SIP Page Parameters (continued)

Web Page Item	Description
RTP Settings	
RTP Port (even) ?	Specify the port number used for the RTP stream after establishing a SIP call. This port number must be an even number and defaults to 10500. The supported range is 0-65536. Enter up to 5 digits.
Asymmetric RTP ?	<p>Specify if the remote endpoint will send and receive RTP packets on different ports. If set to false, the device will track the address/port that is sending RTP packets during a SIP call. If the address/port changes mid-stream, the device will disregard the SDP and send all further RTP packets to this new address.</p> <p>If set to true, this device will ignore the sending address/port and send RTP as specified in the SDP. Warning! Enabling asymmetric RTP can cause the RTP stream to be lost.</p> <p>Most installations should not enable asymmetric RTP.</p>
Jitter Buffer ?	Specify the size of the jitter buffer (in milliseconds) used for SIP calls. Valid values are 50-1000.
RTP Encryption (SRTP) ?	When enabled, a SIP call's audio streams are encrypted using SRTP.

Table 2-12. SIP Page Parameters (continued)

Web Page Item	Description
Call Disconnection	
Terminate Call After Delay 	Automatically terminate an active call after a given delay in seconds. A value of 0 will disable this function. Enter up to 8 digits.
Codec Selection	
Force Selected Codec 	When configured, this option will allow you to force the device to negotiate for the selected codec. Otherwise, the device will perform codec negotiation using the default list of supported codecs.
Codec 	Select the desired codec (only one may be chosen).
	Click the Save button to save your configuration settings.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark () appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

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

2.3.9 Configure the SSL Parameters

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

Figure 2-22. SSL Configuration Page

Home Device Audio Network SIP **SSL** Multicast Audiofiles Events Autoprovision Firmware

CyberData SIP Outdoor Horn

Web Server Certificate

```
subject=
countryName      = US
stateOrProvinceName = California
localityName     = Monterey
organizationName  = Cyberdata
commonName       = 0020f704ec3a
notBefore=Jul  1 16:57:22 2022 GMT
notAfter=Jun 28 16:57:22 2032 GMT
```

No file chosen

SIP Client Certificate

```
subject=
countryName      = US
stateOrProvinceName = California
localityName     = Monterey
organizationName  = Cyberdata
commonName       = 0020f704ec3a
notBefore=Jul  1 16:57:22 2022 GMT
notAfter=Jun 28 16:57:22 2032 GMT
```

No file chosen

Password (optional):

Autoprovisioning Client Certificate

```
subject=
countryName      = US
stateOrProvinceName = California
localityName     = Monterey
organizationName  = Cyberdata
commonName       = 0020f704ec3a
notBefore=Jul  1 16:57:22 2022 GMT
notAfter=Jun 28 16:57:22 2032 GMT
```

No file chosen

Password (optional):

[Download Cyberdata CA](#)

Test TLS Connection

Server: Port:

List of Trusted CAs

Upload CA Certificate: No file chosen

1	CyberData_CA.pem	<input type="button" value="Info"/>	<input type="button" value="Remove"/>
2	DigiCert_Assured_ID_Root_CA.crt	<input type="button" value="Info"/>	<input type="button" value="Remove"/>
3	DigiCert_Assured_ID_Root_G2.crt	<input type="button" value="Info"/>	<input type="button" value="Remove"/>
4	DigiCert_Assured_ID_Root_G3.crt	<input type="button" value="Info"/>	<input type="button" value="Remove"/>
5	DigiCert_Global_Root_CA.crt	<input type="button" value="Info"/>	<input type="button" value="Remove"/>
6	DigiCert_Global_Root_G2.crt	<input type="button" value="Info"/>	<input type="button" value="Remove"/>
7	DigiCert_Global_Root_G3.crt	<input type="button" value="Info"/>	<input type="button" value="Remove"/>
8	DigiCert_High_Assurance_EV_Root_CA.crt	<input type="button" value="Info"/>	<input type="button" value="Remove"/>

Figure 2-23. SSL Configuration Page

4	DigiCert_Assured_ID_Root_G3.crt	Info	Remove
5	DigiCert_Global_Root_CA.crt	Info	Remove
6	DigiCert_Global_Root_G2.crt	Info	Remove
7	DigiCert_Global_Root_G3.crt	Info	Remove
8	DigiCert_High_Assurance_EV_Root_CA.crt	Info	Remove
9	DigiCert_Trusted_Root_G4.crt	Info	Remove
10	GeoTrust_Global_CA.crt	Info	Remove
11	GeoTrust_Primary_Certification_Authority.crt	Info	Remove
12	GeoTrust_Primary_Certification_Authority_-_G2.crt	Info	Remove
13	GeoTrust_Primary_Certification_Authority_-_G3.crt	Info	Remove
14	GeoTrust_Universal_CA.crt	Info	Remove
15	GeoTrust_Universal_CA_2.crt	Info	Remove
16	Go_Daddy_Class_2_CA.pem	Info	Remove
17	Go_Daddy_Root_Certificate_Authority_-_G2.pem	Info	Remove
18	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G4.crt	Info	Remove
19	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5.crt	Info	Remove
20	VeriSign_Universal_Root_Certification_Authority.crt	Info	Remove
21	Verisign_Class_1_Public_Primary_Certification_Authority.crt	Info	Remove
22	Verisign_Class_1_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
23	Verisign_Class_2_Public_Primary_Certification_Authority_-_G2.crt	Info	Remove
24	Verisign_Class_2_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
25	Verisign_Class_3_Public_Primary_Certification_Authority.crt	Info	Remove
26	Verisign_Class_3_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
27	thawte_Primary_Root_CA.crt	Info	Remove
28	thawte_Primary_Root_CA_-_G2.crt	Info	Remove
29	thawte_Primary_Root_CA_-_G3.crt	Info	Remove

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

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. SSL Configuration Parameters

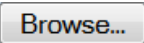


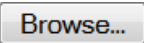


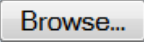
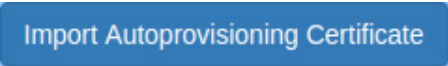
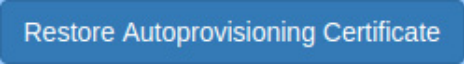


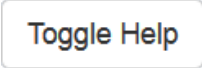








Web Page Item	Description
Web Server Certificate	Certificate used by the web server.
	Click Browse to select a certificate to import.
	After selecting a certificate, click Import Web Certificate to import it as the certificate used by this device's web server.
	Restore the device's default web server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

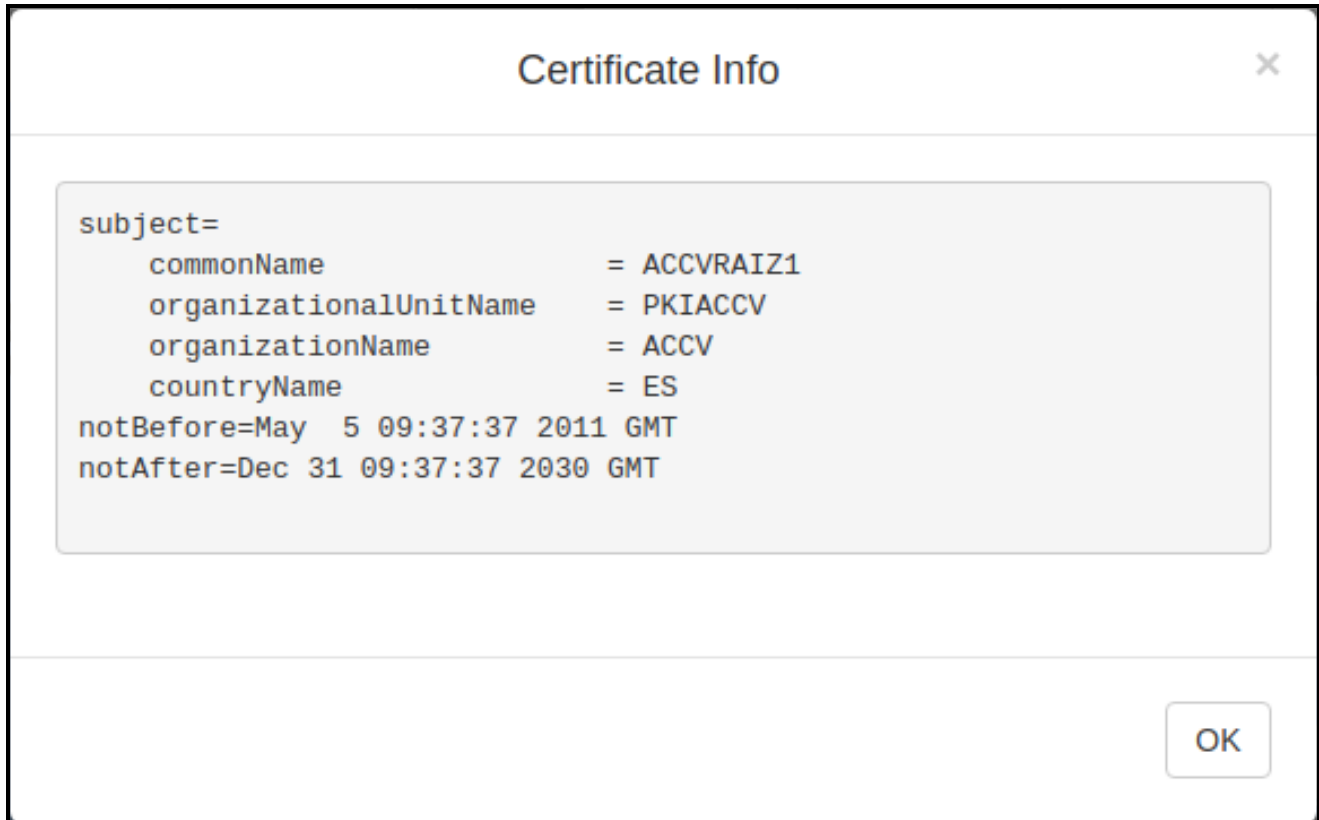
Table 2-13. SSL Configuration Parameters (continued)

Web Page Item	Description
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.
Test TLS Connection	
Server ?	The ssl test server address as a fully qualified domain name or in IPv4 dotted decimal notation.
Port ?	The supported range is 0-65536. SIP connections over TLS to port 5060 are modified to connect to port 5061. This test button will do the same.
	Use this button to test a TLS connection to a remote server using the sip client key and password. This will attempt to make a socket connection to the configured test server and port and report the success or failure. This can be used to debug TLS connection issues separate from SIP registration issues.
	Use this button to test a TLS connection to a remote server using the autoprovisioning client key and password. This will attempt to make a socket connection to the configured test server and port and report the success or failure. This can be used to debug TLS connection issues with secure autoprovisioning.
List of Trusted CAs	
	Use this button to select a configuration file to import.
Upload CA Certificate ?	
	Click Browse to select a CA certificate to import. After selecting a server certificate authority (CA), click Import CA Certificate to import it to the list of trusted CAs. CAs are used to validate the certificate presented by the server when establishing a TLS connection.
	Restore Defaults will restore the default list of registered CAs and Remove All will remove all registered CAs.
	Restore Defaults will restore the default list of registered CAs and Remove All will remove all registered CAs.
	Provides details of the certificate. After clicking on this button, the Certificate Info Window appears. See Section 2.3.9.1, "Certificate Info Window" .
	Removes this certificate from the list of trusted certificates. After clicking on this button, the Remove Server Certificate Window appears. See Section 2.3.9.2, "Remove Server Certificate Window" .

2.3.9.1 Certificate Info Window

The **Certificate Info Window** provides details of the certificate. This window appears after clicking on the **Info** button. See [Figure 2-24](#).

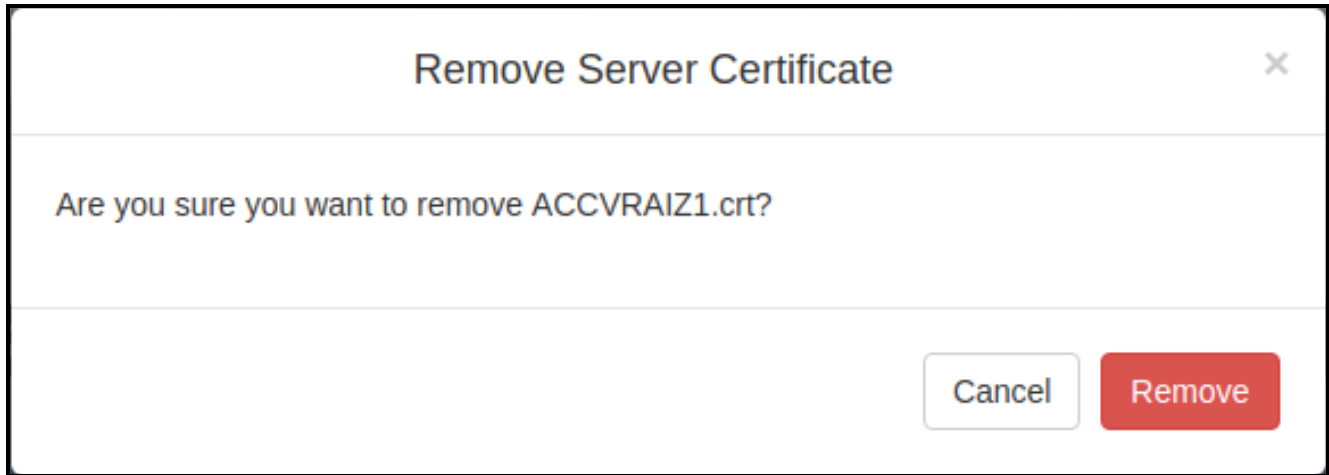
Figure 2-24. Certificate Info Window



2.3.9.2 Remove Server Certificate Window

The **Remove Server Certificate Window** will ask if the user wants to remove a certificate from the list of trusted certificates. This window appears after clicking on the **Remove** button. See [Figure 2-25](#).

Figure 2-25. Remove Server Certificate Window



2.3.10 Configure the Multicast Parameters

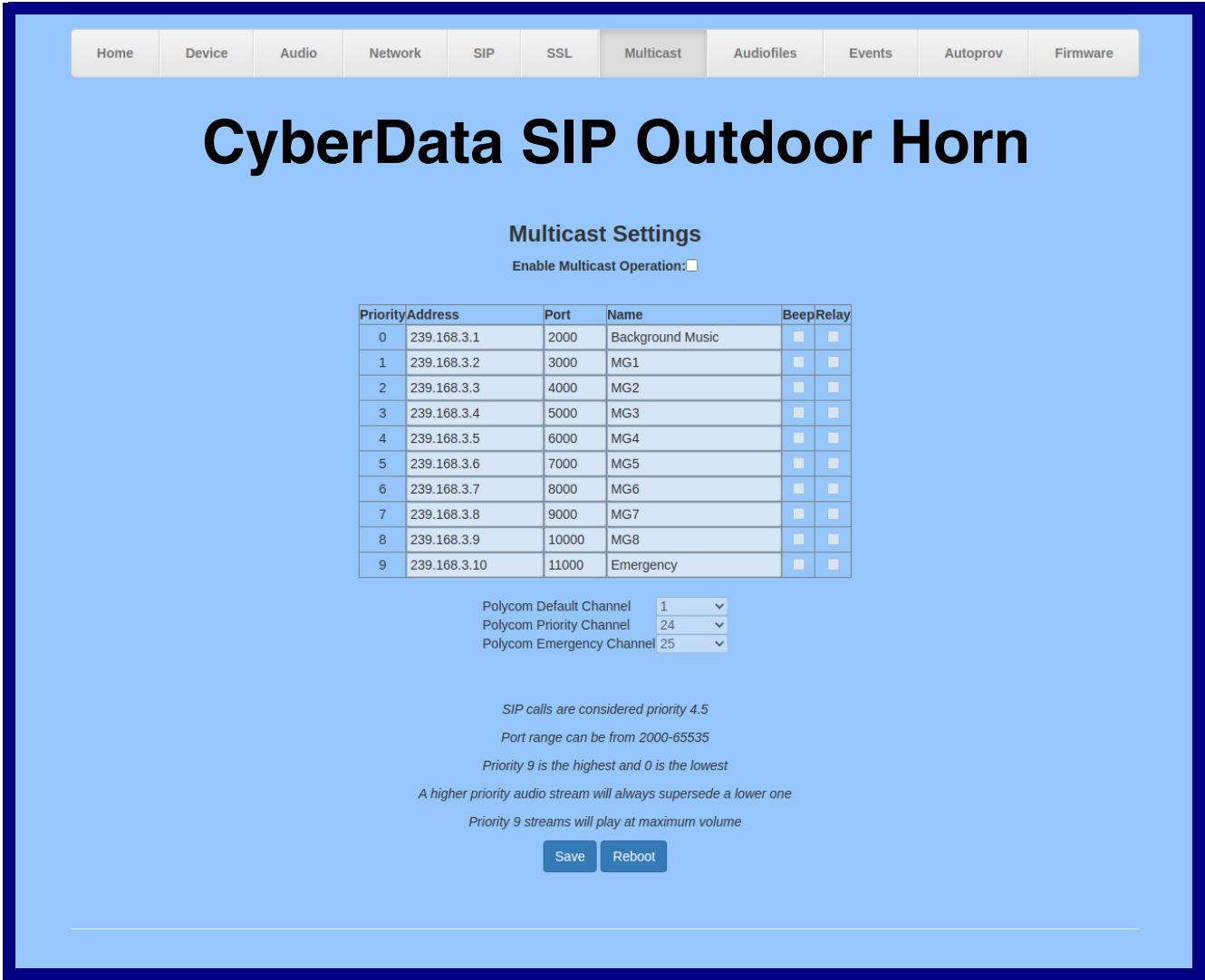
The **Multicast** page allows the device to join up to ten paging zones for receiving ulaw/alaw encoded RTP audio streams.

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

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

1. Click on the **Multicast** menu button to open the **Multicast** page. See [Figure 2-26](#).



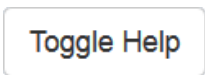
Figure 2-26. Multicast Page



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

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

Table 2-14. Multicast Page Parameters

Web Page Item	Description
Enable Multicast Operation	Enables or disables multicast operation.
Priority	Indicates the priority for the multicast group. Priority 9 is the highest (emergency streams). 0 is the lowest (background music). SIP calls are considered priority 4.5 . See Section 2.3.10.1, "Assigning Priority" for more details.
Address	Enter the multicast IP Address for this multicast group (15 character limit).
Port	Enter the port number for this multicast group (5 character limit [range can be from 2000 to 65535]).
Name	Assign a descriptive name for this multicast group (25 character limit).
Beep	When selected, the device will play a beep before multicast audio is sent.
Relay	When selected, the device will activate a relay before multicast audio is sent.
Polycom Default Channel	When a default Polycom channel/group number is selected, the device will subscribe to the default channel for one-way group pages. Group Numbers 1-25 are supported. Or, select Disabled to disable this channel.
Polycom Priority Channel	When a priority Polycom channel/group number is selected, the device will subscribe to the priority channel for one-way group pages. Group Numbers 1-25 are supported. Or, select Disabled to disable this channel.
Polycom Emergency Channel	When an emergency Polycom channel/group number is selected, the device will subscribe to the default channel for one-way group pages. Group Numbers 1-25 are supported. Or, select Disabled to disable this channel.
	Click the Save button to save your configuration settings.
	Click on the Reboot button to reboot the system.
	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.

2.3.10.1 Assigning Priority

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

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

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

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

Ringtones and
Nightringtones

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

2.3.11 Configure the 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 2-27).

Figure 2-27. Audiofiles Page

HomeDeviceAudioNetworkSIPSSLMulticastAudiofilesEventsAutoprovFirmware

CyberData SIP Outdoor Horn

Available Space: 1464MB

Audio Files

0:	Currently set to:	default	<div>Browse...</div>	No file chosen	<div>Play</div>	<div>Delete</div>	<div>Save</div>
1:	Currently set to:	default	<div>Browse...</div>	No file chosen	<div>Play</div>	<div>Delete</div>	<div>Save</div>
2:	Currently set to:	default	<div>Browse...</div>	No file chosen	<div>Play</div>	<div>Delete</div>	<div>Save</div>
3:	Currently set to:	default	<div>Browse...</div>	No file chosen	<div>Play</div>	<div>Delete</div>	<div>Save</div>
4:	Currently set to:	default	<div>Browse...</div>	No file chosen	<div>Play</div>	<div>Delete</div>	<div>Save</div>
5:	Currently set to:	default	<div>Browse...</div>	No file chosen	<div>Play</div>	<div>Delete</div>	<div>Save</div>
6:	Currently set to:	default	<div>Browse...</div>	No file chosen	<div>Play</div>	<div>Delete</div>	<div>Save</div>
7:	Currently set to:	default	<div>Browse...</div>	No file chosen	<div>Play</div>	<div>Delete</div>	<div>Save</div>
8:	Currently set to:	default	<div>Browse...</div>	No file chosen	<div>Play</div>	<div>Delete</div>	<div>Save</div>
9:	Currently set to:	default	<div>Browse...</div>	No file chosen	<div>Play</div>	<div>Delete</div>	<div>Save</div>
Audio Test:	Currently set to:	default	<div>Browse...</div>	No file chosen	<div>Play</div>	<div>Delete</div>	<div>Save</div>
Dot:	Currently set to:	default	<div>Browse...</div>	No file chosen	<div>Play</div>	<div>Delete</div>	<div>Save</div>
Night Ring:	Currently set to:	default	<div>Browse...</div>	No file chosen	<div>Play</div>	<div>Delete</div>	<div>Save</div>
Page Tone:	Currently set to:	default	<div>Browse...</div>	No file chosen	<div>Play</div>	<div>Delete</div>	<div>Save</div>
Rebooting:	Currently set to:	default	<div>Browse...</div>	No file chosen	<div>Play</div>	<div>Delete</div>	<div>Save</div>
Restoring Default:	Currently set to:	default	<div>Browse...</div>	No file chosen	<div>Play</div>	<div>Delete</div>	<div>Save</div>
Stored Message File Not Found:	Currently set to:	default	<div>Browse...</div>	No file chosen	<div>Play</div>	<div>Delete</div>	<div>Save</div>
Your IP Address Is:	Currently set to:	default	<div>Browse...</div>	No file chosen	<div>Play</div>	<div>Delete</div>	<div>Save</div>

Menu Audio Files

Cancel:	Currently set to:	default	<div>Browse...</div>	No file chosen	<div>Play</div>	<div>Delete</div>	<div>Save</div>
Currently Playing:	Currently set to:	default	<div>Browse...</div>	No file chosen	<div>Play</div>	<div>Delete</div>	<div>Save</div>

Figure 2-28. Audiofiles Page

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

Menu Audio Files

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

Stored Messages

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

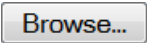



2. On the **Audiofiles** page, enter values for the parameters indicated in [Table 2-15](#).

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

Table 2-15. Audiofiles Page Parameters

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

Table 2-15. Audiofiles Page Parameters (continued)

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

2.3.11.1 User-created Audio Files

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

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

You can use the free utility *Audacity* to convert audio files into this format. See [Figure 2-29](#) through [Figure 2-31](#).

Figure 2-29. Audacity 1

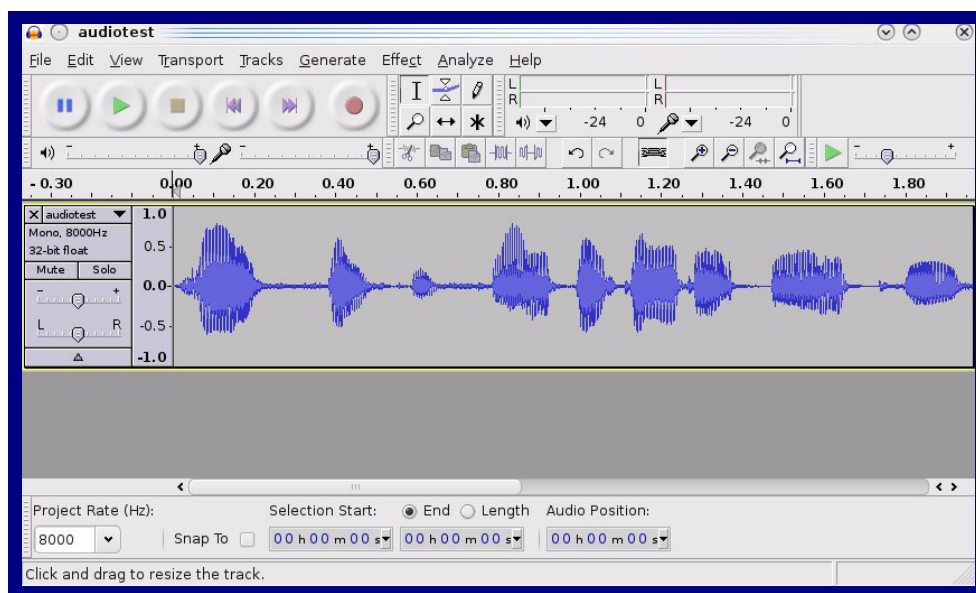
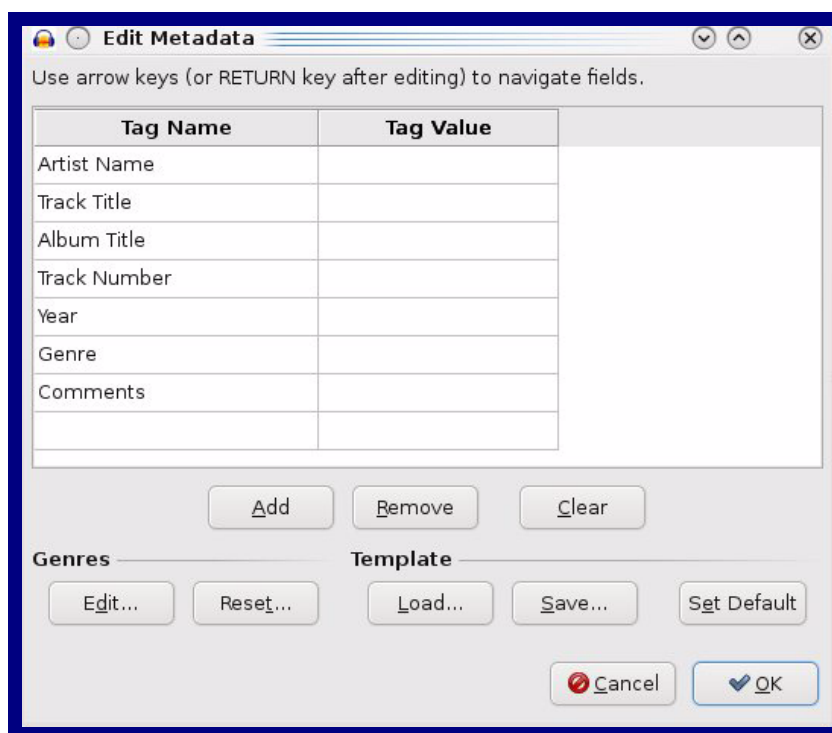


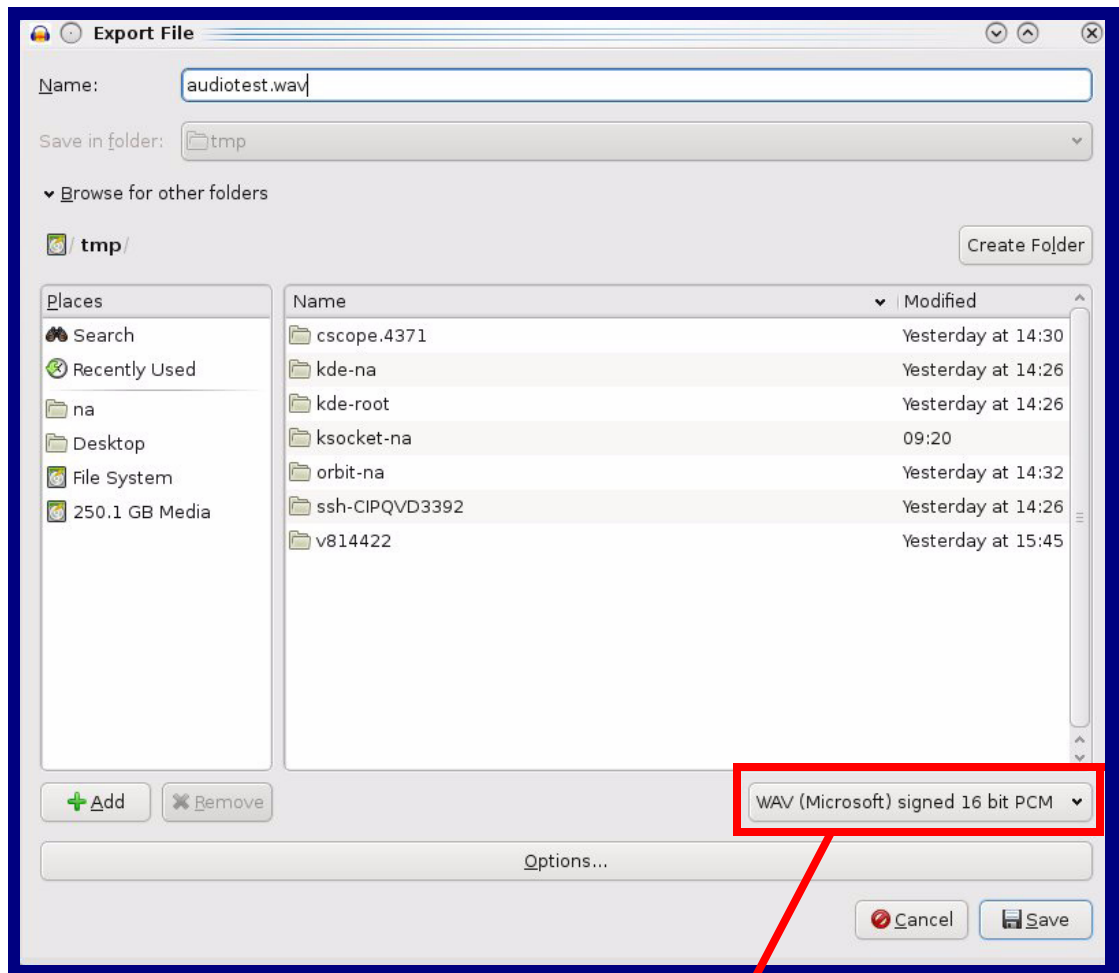
Figure 2-30. Audacity 2



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

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

Figure 2-31. WAV (Microsoft) signed 16 bit PCM



WAV (Microsoft) signed 16 bit PCM

2.3.12 Configure the Events Parameters

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

1. Click on the **Events** menu button to open the **Events** page (Figure 2-32).

Figure 2-32. Events Page

HomeDeviceAudioNetworkSIPSSLMulticastAudiofilesEventsAutoprovFirmware

CyberData SIP Outdoor Horn

Enable Event Generation:☐

Events

Enable Multicast Start Events:☐

Enable Multicast Stop Events:☐

Enable Call Start Events:☐

Enable Call Terminated Events:☐

Enable Night Ring Events:☐

Enable Power On Events:☐

Enable 60 Second Heartbeat:☐

Enable Audio Health Check Events:☐

Event Server

Server IP Address:10.0.0.250

Server Port:8080

Server URL:xmlparse_engine

Save




Reboot

Toggle Help

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

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

Table 2-16. Events 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 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 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 60 Second Heartbeat Events ?	When enabled, the device will report a Heartbeat event every 60 seconds. SIP registration is not required to generate Heartbeat events.
Enable Audio Health Check Events ?	When selected, the device will report the results of an audio health check.
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.
	Click the Save button to save your configuration settings.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

2.3.12.1 Example Packets for Events

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

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

Here are example packets for every event:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.3.13 Configure the Autoprovisioning Parameters

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

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

1. Click the **Autoprov** menu button to open the **Autoprovisioning** page. See [Figure 2-33](#).

Figure 2-33. Autoprovisioning Page

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

CyberData SIP Outdoor Horn

Enable Autoprovisioning: ☒

Autoprovisioning Server:

Autoprovisioning Filename:

Use tftp: ☐

Verify Server Certificate: ☐

Username:

Password:

Autoprovisioning autoupdate (in minutes):

Autoprovision at time (HHMM):

Autoprovision when idle (in minutes > 10):

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

Autoprovisioning happens on boot.

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

If these haven't been configured, it will look for an autoprovisioning server in your list of DHCP options and try to download '0020f704ec3a.xml' and if this fails, '000000cd.xml'.

Autoprovisioning log

```
2022-07-19 14:58:16 Autoprov: no autoprov triggers. Exiting...
2022-07-19 14:58:19 Autoprovisioning on boot
2022-07-19 14:58:19 Autoprov found server='http://10.0.0.242' in dhcp option 43
2022-07-19 14:58:19 Autoprov looking for 0020f704ec3a.xml at http://10.0.0.242
2022-07-19 14:58:19 Autoprov downloading http://10.0.0.242/0020f704ec3a.xml
2022-07-19 14:58:19 Got autoprov file. Parsing "0020f704ec3a.xml"
2022-07-19 14:58:19 Autoprov: Processing ssl certificates
2022-07-19 14:58:19 No certificate elements in SSLCertificates
2022-07-19 14:58:19 Autoprov: Processing audio files
2022-07-19 14:58:20 Autoprov found server='10.0.1.118' in dhcp option 72
```






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

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

Table 2-17. Autoprovisioning Page Parameters

Web Page Item	Description
Enable Autoprovisioning ?	The device will automatically fetch a configuration file, also known as the 'autoprovisioning file', based on the configured settings below.
Autoprovisioning Server ?	Enter the IPv4 address of the provisioning server in dotted decimal notation.
Autoprovisioning Filename ?	<p>The autoprovisioning filename is the configuration filename. The default autoprovisioning filename is in the format of <mac address>.xml.</p> <p>Supported filename extensions are .txt, and .xml. The current filename is denoted by an asterisk at the bottom of the Autoprovisioning Page. Enter up to 256 characters.</p> <p>A file may have any name with an xml extension. If a file name is entered, the device will look for the specified file name, and only that file.</p>
Use tftp ?	The device will use TFTP (instead of http) to download autoprovisioning files.
Verify Server Certificate ?	When using ssl to download autoprovisioning files, reject connections where the server address doesn't match the server certificate's common name.
Username ?	The username used to authenticate with an autoprovisioning server. Leave this field blank to disable authentication.
Password ?	The password used to authenticate with an autoprovisioning server. Leave this field blank to disable authentication.
Autoprovisioning Autoupdate (in minutes) ?	<p>The reoccurring time (in minutes) the device will wait before checking for new autoprovisioning files. Enter up to 6 digits. A value of 0 will disable this option.</p> <p>Note: To use the auto update options, make sure that the Enable NTP setting on the Device Page page is selected (see Table 2-9).</p>
Autoprovision at time (HHMMSS) ?	<p>The time of day the device will check for a new autoprovisioning file. The time must be 6 characters in length and in HHMMSS format. An empty value will disable this option.</p> <p>Note: To use the auto update options, make sure that the Enable NTP setting on the Device Page page is selected (see Table 2-9).</p>
Autoprovision when idle (in minutes > 10) ?	<p>The idle time (in minutes greater than 10) after which the device will check for a new autoprovisioning file. Enter up to 6 digits. A value of 0 will disable this option.</p> <p>Note: To use the auto update options, make sure that the Enable NTP setting on the Device Page page is selected (see Table 2-9).</p>

Table 2-17. Autoprovisioning Page Parameters (continued)

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

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

2.3.13.1 Autoprovisioning

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

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

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

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

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

1. Option 43 - a FQDN or an IP address to an http server
2. Option 72 - an IP address to an http server
3. Option 150 - an IP address to a tftp server

4. Option 66 - an IP address to a tftp server or if the entry starts with 'http', a FQDN to a http server.

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

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

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

```
<MiscSettings>
  <DeviceName>CyberData 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 “https://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 <https://example.com/common.xml>.
3. It will try to download https://example.com/sip_reg0020f7123456.xml.
4. It will try to download <https://example.com/audio0020f7123456>.
5. It will try to download <https://example.com/device.xml>.

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

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

Checking for New Autoprovisioning Files after Boot

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

The
Autoprovisioning
Filename

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

Table 2-18. Autoprovisioning File Name

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

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

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

For example:

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

The autoprovisioning filename is set to “cyberdata/”

On boot, the device will try to download:

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

...and if this fails:

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

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

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

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

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

The <FirmwareFile> name can contain path elements (i.e. /path/to/firmware/10.3.0-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.

2.3.13.2 Sample dhcpd.conf

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

ddns-update-style none;

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

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

    option routers                10.0.0.1;
    option subnet-mask            255.0.0.0;

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

    option time-offset            -8;          # Pacific Standard Time

#    option www-server            99.99.99.99;          # OPTION 72

#    option tftp-server-name      "10.0.1.52";          # OPTION 66
#    option tftp-server-name      "https://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 "https://test.cyberdata.net";  # OPTION 43

    range 10.10.0.1 10.10.2.1; }
```

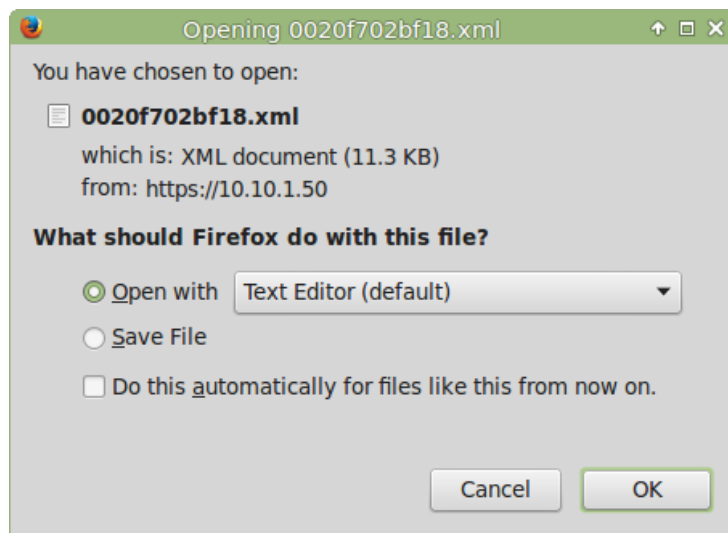
2.3.13.3 Download Template Button

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

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

1. On the **Autoprovisioning** page, click on the **Download Template** button.
2. You will see a window prompting you to save a configuration file (**.xml**) to a location on your computer ([Figure 2-34](#)). 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 2-34](#).

Figure 2-34. 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

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

To upgrade the firmware of your device:

1. Download the latest firmware file from the **Downloads** tab at the following webpage:
<https://www.cyberdata.net/products/011457>
2. Unzip the firmware version file. This file may contain the following:
 - Firmware file
 - Release notes
 - Autoprovisioning template
3. Log in to the **Home** page as instructed in [Section 2.3.4, "Log in to the Home Page"](#).
4. Click on the **Firmware** menu button to open the **Firmware** page ([Figure 2-35](#)).

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

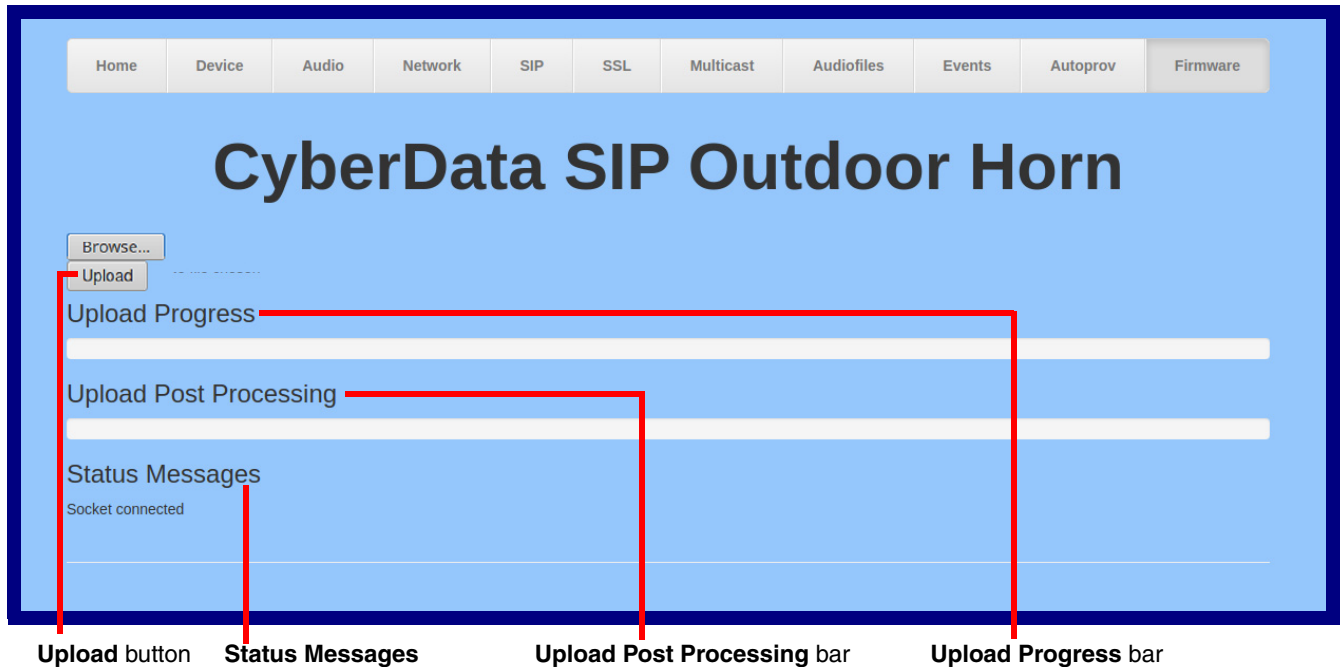
Figure 2-35. Firmware Page



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

6. Select the firmware file. This reveals the **Upload** button (Figure 2-36).

Figure 2-36. Upload Button



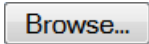
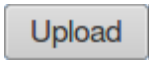
7. Click on the **Upload** button. After selecting the **Upload** button, you will see the progress of the upload in the **Upload Progress** bar.
8. When the upload is complete, you will see the words **Upload finished** under **Status Messages**.
9. At this point, you will see the progress of the upload's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

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

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

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

Table 2-19. Firmware Page Parameters

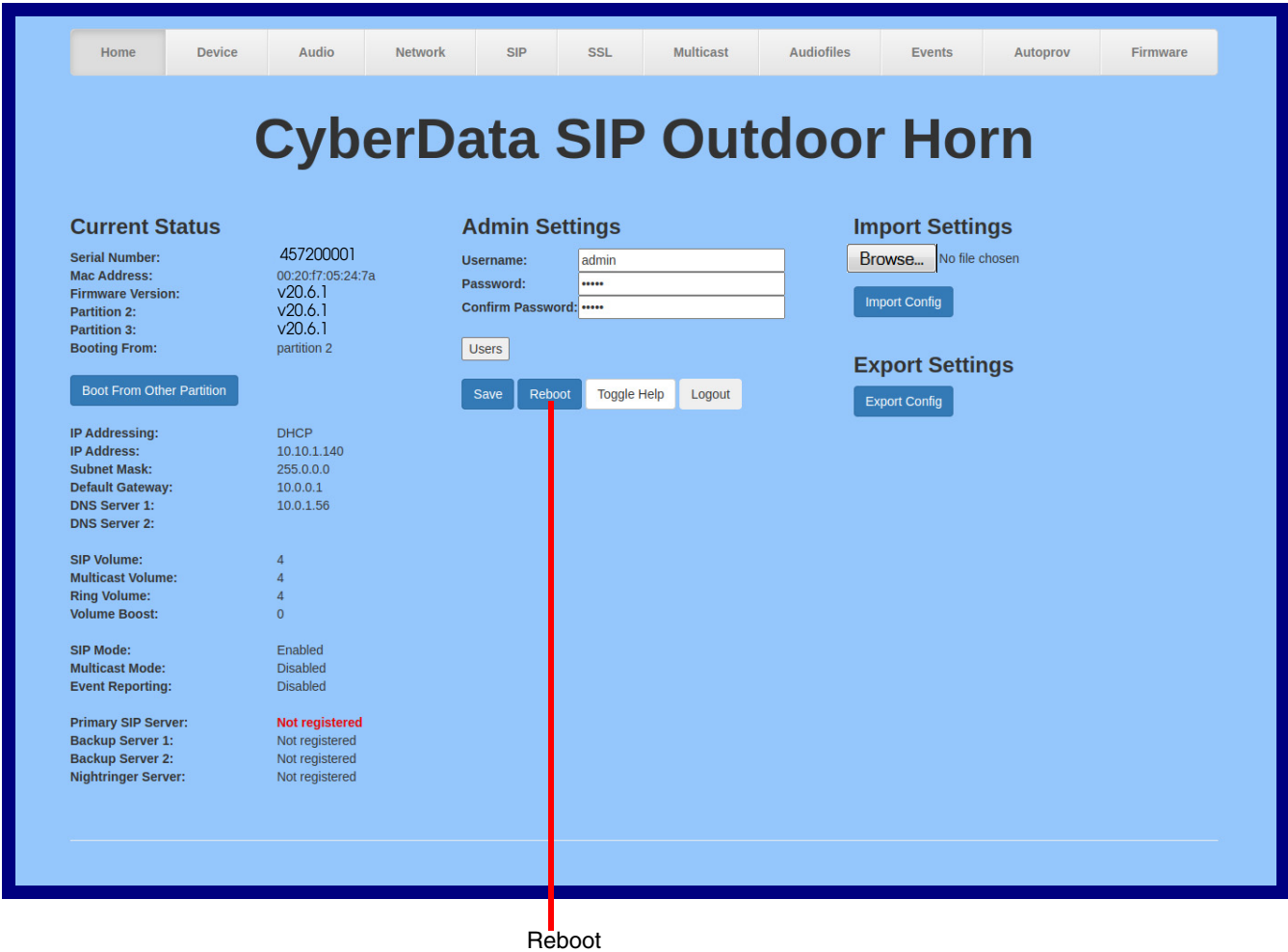
Web Page Item	Description
	Use the Browse button to navigate to the location of the firmware file that you want to upload.
	Click on the Upload button to automatically upload the selected firmware and reboot the system. Note: This button only appears after the user has selected a firmware file.
Upload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

2.4.1 Reboot the Device

To reboot a SIP IP66 Indoor/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 2-37](#)). A normal restart will occur.

Figure 2-37. 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 2-20](#) use the free unix utility, **wget**, but any program that can send http POST commands to the device should work.

2.5.1 Command Interface Post Commands

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

Table 2-20. Command Interface Post Commands

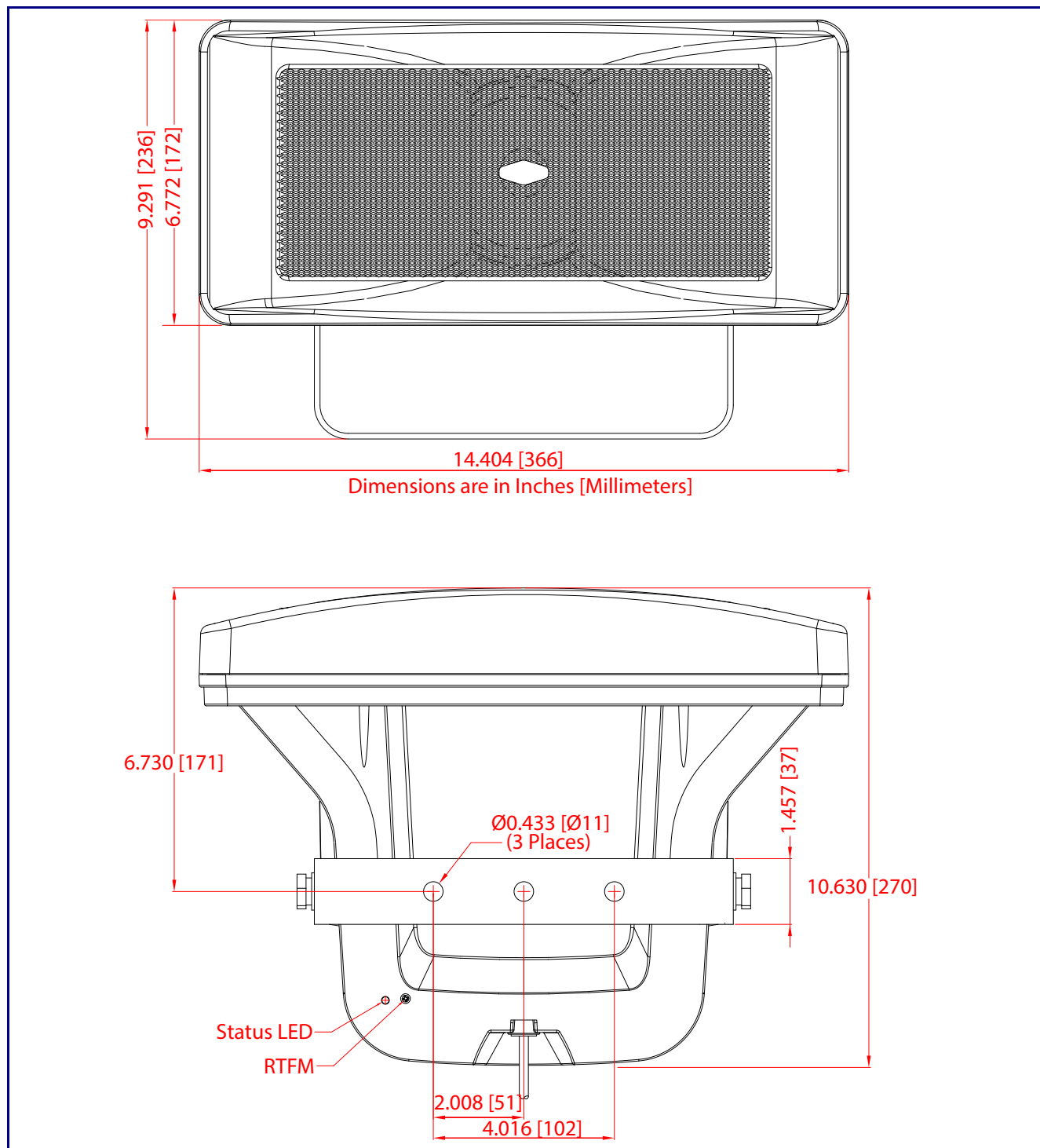
Device Action	HTTP Post Command ^a
Reboot	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.247/command" --post-data "request=reboot"
Place call to extension (example: extension 600)	wget --user admin --password admin --auth-no-challenge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

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

Appendix A: Mounting the SIP IP66 Indoor/Outdoor Horn

A.1 Dimensions

Figure A-1. Dimensions



Appendix B: Troubleshooting/Technical Support

B.1 Frequently Asked Questions (FAQ)

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

<https://www.cyberdata.net/products/011457>

B.2 Documentation

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

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

<https://www.cyberdata.net/products/011457>

B.3 Contact Information

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

B.4 Warranty and RMA Information

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

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

Index

A

- address, configuration login 20
- admin username and password 20
- announcing an IP address 15
- audio configuration 54
 - night ring tone parameter 56
- audio encodings 4
- audio files, user-created 58
- audio page 54
- audio test 13
- autoprovision at time (HHMMSS) 66
- autoprovision when idle (in minutes > 10) 66
- autoprovisioning 67
 - download template button 67
- autoprovisioning autoupdate (in minutes) 66
- autoprovisioning configuration 65, 66
- autoprovisioning filename 66
- autoprovisioning server (IP Address) 66

B

- backup SIP server 1 39
- backup SIP server 2 39
- backup SIP servers, SIP server
 - backups 39

C

- changing
 - the web access password 29
- changing default username and password for
 - configuration GUI 20
- Cisco SRST 40
- command interface 81
- commands 81
- configurable parameters 39
- configuration
 - audio 54
 - default IP settings 16
 - door sensor 44
 - intrusion sensor 44
 - network 35
 - SIP 38
- connection options 10
- connections 10
- contact information 84
- contact information for CyberData 84

- current network settings 36
- CyberData contact information 84

D

- default gateway 36
- default IP settings 16
- default login address 20
- device configuration 29
- device configuration page 29, 32
- device configuration parameters 30
- device configuration password
 - changing for web configuration access 29
- DHCP Client 4
- dial out extension strings 50
- dimensions 5, 82
- discovery utility program 20
- DNS server 36
- door sensor 56
- download autoprovisioning template button 67
- DTMF tones (using rfc2833) 50

E

- enable night ring events 61
- ethernet I/F 5
- event configuration
 - enable night ring events 61
- expiration time for SIP server lease 39, 40, 41
- export settings 23, 24

F

- factory defaults 15
- firmware
 - where to get the latest firmware 77

G

- get autoprovisioning template 67
- GUI username and password 20

H

hazard levels 5
 http POST command 81
 http web-based configuration 4

I

identifying your product 1
 import settings 23, 24
 import/export settings 23, 24
 installation 2
 IP address 36
 IP address announcement 15
 IP address confirmation 13

L

lease, SIP server expiration time 39, 40, 41
 lengthy pages 53
 local SIP port 40
 log in address 20

M

MGROUP
 MGROUP Name 52
 multicast configuration 50, 54
 Multicast IP Address 52

N

navigation (web page) 17
 navigation table 17
 network configuration 35
 nightring tones 53
 Nightringer 76
 nightringer settings 40
 NTP server 30, 33

P

packet time 4
 pages (lengthy) 53
 parts list 8
 password

configuration GUI 20
 for SIP server login 39
 payload types 5
 polycom default channel 52
 polycom emergency channel 52
 polycom priority channel 52
 port
 local SIP 40
 remote SIP 40
 POST command 81
 power input 5
 priority
 assigning 52
 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 79, 80
 remote SIP port 40
 required configuration for web access username and password 20
 reset test function management switch 13
 resetting the IP address to the default 82
 restoring the factory defaults 15
 ringtones 53
 lengthy pages 53
 rport discovery setting, disabling 40
 RTFM switch 13
 RTP/AVP 4

S

safety instructions 4
 sales 84
 sensor setup page 44
 sensor setup parameters 44
 server address, SIP 39
 service 84
 SIP
 enable SIP operation 39, 40
 local SIP port 40
 user ID 39

- SIP (session initiation protocol) 4
- SIP configuration 38
- SIP configuration parameters
 - outbound proxy 40, 41
 - registration and expiration, SIP server lease 39, 40, 41
 - user ID, SIP 39
- SIP registration 39
- SIP remote SIP port 40
- SIP server 39
 - password for login 39
 - SIP servers supported 4
 - user ID for login 39
- SIP server configuration 39
- SIP volume 33
- SRST 40
- subnet mask 36
- supported protocols 4
 - navigation 17
 - web page navigation 17
 - wget, free unix utility 81

T

- tech support 84
- technical support, contact information 84
- test audio 13
- TFTP server 4

U

- user ID
 - for SIP server login 39
- username
 - changing for web configuration access 29
- username for configuration GUI 20

V

- VLAN ID 36
- VLAN Priority 36
- VLAN tagging support 36
- VLAN tags 36
- volume
 - multicast volume 33
 - SIP volume 33

W

- warranty policy at CyberData 84
- web configuration log in address 20
- web page