



SIP Talk-Back Speaker Operations Guide

Part #011397*, RAL 9002, Gray White
Part #011398*, RAL 9003, Signal White

*Replaces #011180 and 011181

Document Part #931191M
for Firmware Version 12.1.0

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

SIP Talk-Back Speaker Operations Guide 931191M
Part # 011397
Part # 011398

COPYRIGHT NOTICE:

© 2020, CyberData Corporation, ALL RIGHTS RESERVED.

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

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

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

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

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



Technical Support

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

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

Email: support@cyberdata.net

Fax: (831) 373-4193

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

Revision Information

Revision 931191M, which corresponds to firmware version 12.1.0, was released on April 3, 2020, and has the following changes:



- Updates [Figure 2-5, "Running the Speaker with a Remote Call Button"](#)
- Updates [Section 1.3, "Product Features"](#)
- Updates [Section 1.4, "Supported Protocols"](#) to add [SRTP](#)
- Updates [Table 1-1, "Product Specifications"](#)
- Updates [Figure 2-22, "SIP Page—Top"](#)
- Updates [Figure 2-23, "SIP Page—Bottom"](#)
- Updates [Table 2-13, "SIP Page Parameters"](#) to add the [RTP Encryption \(SRTP\)](#) setting

Browsers Supported

The following browsers have been tested against firmware version 12.1.0:

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

Pictorial Alert Icons

 <p>GENERAL ALERT</p>	<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.

Important Safety Instructions

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

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

Abbreviations and Terms

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

Contents

Chapter 1 Product Overview	1
1.1 How to Identify This Product	1
1.2 Installation	2
1.3 Product Features	3
1.4 Supported Protocols	4
1.5 Supported SIP Servers	4
1.6 Product Specifications	5
1.7 Optional Connections (J9 and J10)	6
1.8 Compliance	6
1.8.1 CE Testing	6
1.8.2 FCC Statement	6
1.9 Audio Modes for the Talk Back Speaker	7
1.9.1 Acoustic Echo Canceler	7
1.9.2 Voice-operated Switch (VOX)	8
1.9.3 Push to Talk	9
1.9.4 DTMF Push to Talk	11
1.9.5 Monitor Mode	11
Chapter 2 Installing the SIP Talk-Back Speaker	13
2.1 Parts List	13
2.2 Device Configuration	14
2.2.1 Connect Power to the Speaker	15
2.2.2 Installation Options	18
2.2.3 Confirm that the Speaker is Operational and Linked to the Network	23
2.2.4 Confirm the IP Address and Test the Audio	24
2.2.5 Adjust the Volume	25
2.2.6 How to Set the Factory Default Settings	26
2.3.1 Factory Default Settings	27
2.3.2 SIP Talk-Back Speaker Web Page Navigation	28
2.3.3 Using the Toggle Help Button	29
2.3.4 Log in to the Configuration Home Page	31
2.3.5 Configure the Device	35
2.3.6 Configure the Audio	43
2.3.7 Configure the Network Parameters	47
2.3.8 Configure the SIP (Session Initiation Protocol) Parameters	50
2.3.9 Configure the Multicast Parameters	61
2.3.10 Configure the SSL Parameters	64
2.3.11 Configure the Sensor Configuration Parameters	70
2.3.12 Configure the Audiofiles Parameters	74
2.3.13 Configure the Events Parameters	81
2.3.14 Configure the Autoprovisioning Parameters	87
2.4.1 Downloading the Firmware	98
2.4.2 Reboot the Device	100
2.5.1 Command Interface Post Commands	101
Appendix A Mounting the Speaker	105
A.1 Mount the Speaker	105
A.2 Dimensions	107
Appendix B Setting up a TFTP Server	108
B.1 Set up a TFTP Server	108
B.1.1 In a LINUX Environment	108
B.1.2 In a Windows Environment	108

Appendix C Troubleshooting/Technical Support	109
C.1 Frequently Asked Questions (FAQ)	109
C.2 Documentation	109
C.3 Contact Information	110
C.4 Warranty and RMA Information	110
Index	111

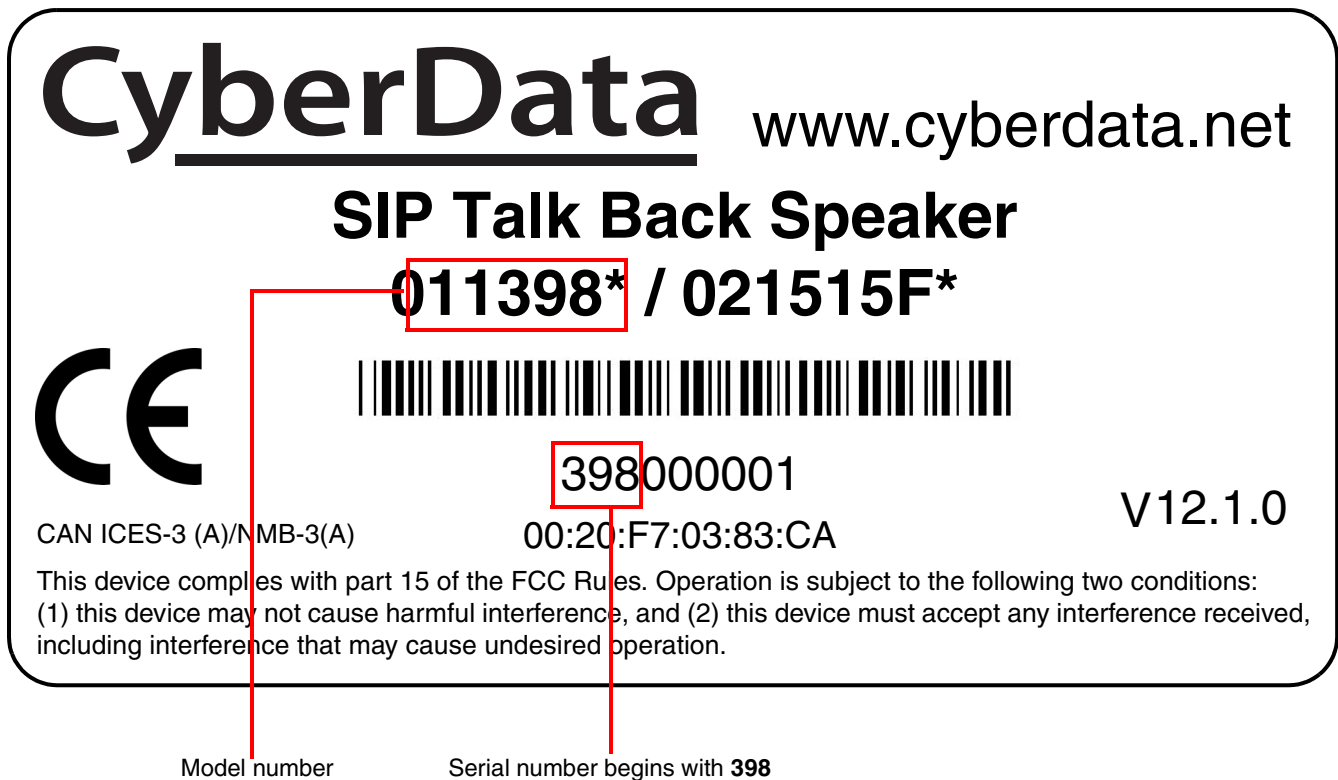
1 Product Overview

1.1 How to Identify This Product

To identify the SIP Talk-Back Speaker, look for a model number label similar to the one shown in [Figure 1-1](#). The model number on the label should be one of the following:

- **011397**, RAL 9002, Gray White
- **011398**, RAL 9003, Signal White

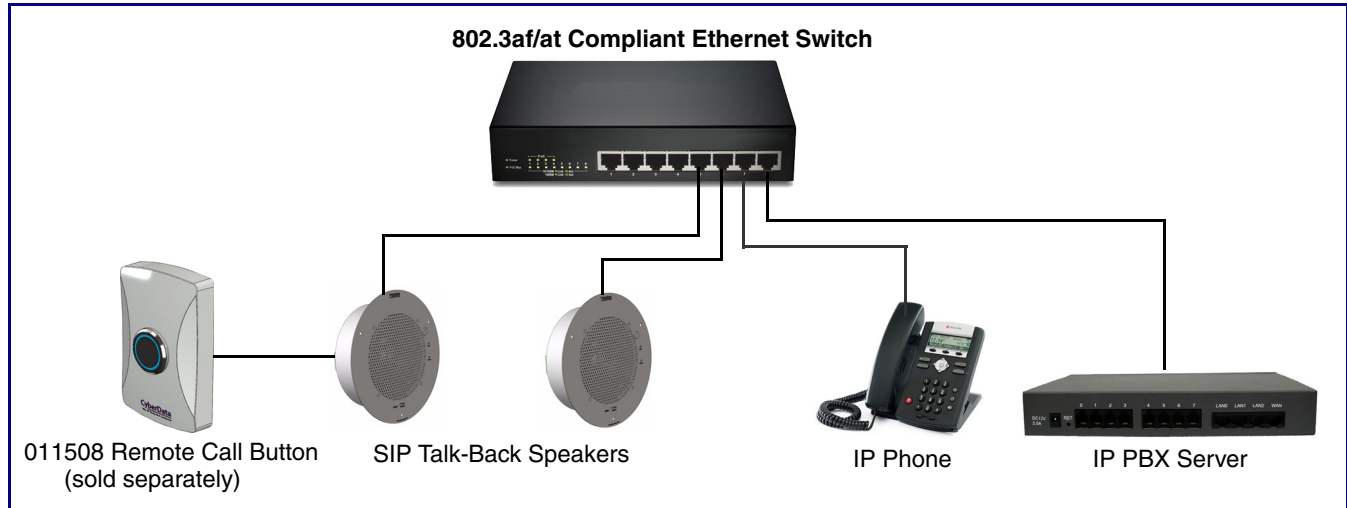
Figure 1-1. Model Number Label



1.2 Installation

Figure 1-2 illustrates a typical configurations for the SIP Talk-Back Speaker.

Figure 1-2. Typical Installation



See the following sections for other installation options:

- [Section 2.2.1.3, "Running the SIP Talk-Back Speaker with Auxiliary Power"](#)
- [Section 2.2.2.3, "SIP Talk-Back Speaker with an External Device"](#)
- [Section 2.2.2.4, "SIP Talk-Back Speaker with Auxiliary Speaker Connection"](#)
- [Section 2.2.2.5, "SIP Talk-Back Speaker with Line Out"](#)

1.3 Product Features

- Full-duplex audio with configurable echo cancelling
 - Adaptive half duplex audio with configurable VOX (Voice Operated Switch) settings
 - Half duplex audio from speaker side using Push to Talk
 - Half duplex audio from phone side using DTMF commands
 - Audio health check, to verify operation of hardware, that can be scheduled or launched manually
 - Supports a Monitor Mode
-
- Simultaneous SIP and multicast
 - Paging prioritization
 - User-uploadable ring and alert tones
 - Support for security code to prevent unwanted SIP calls
 - Can receive pages directly from Poly phones as well as other devices that can send standard multicast
 - Loud/Night Ringer function - second SIP extension
 - Support for 10 multicast paging groups
-
- Can drive one external analog speaker for greater coverage
 - DTMF-controlled relay
 - Line-out connection
 - Network and manual speaker volume control
-
- TLS 1.2 and SRTP enhanced security for IP endpoints in a local or cloud-based environment
 - Autoprovisioning via HTTP, HTTPS, or TFTP
 - HTTPS or HTTP web-based configuration. HTTPS is enabled by default.
 - 802.11q VLAN tagging
 - Configurable event generation for device health and status monitoring
 - Web-based upgradeable firmware
 - Support for multiple SIP servers for redundancy

1.4 Supported Protocols

The SIP Talk-Back Speaker supports:

- SIP
- Multicast
- HTTP Web-based configuration
 - Provides an intuitive user interface for easy system configuration and verification of speaker operations.
- DHCP Client
 - Dynamically assigns IP addresses in addition to the option to use static addressing.
- HTTP TCP Post auto-updating event notification in XML format
- SRTP
- TLS 1.2
- TFTP Client
 - Facilitates hosting for the configuration file for Autoprovisioning.
- Audio Encodings
 - PCMU (G.711 mu-law)
 - PCMA (G.711 A-law)
 - Packet Time 20 ms
 - G.722
 - G.729

1.5 Supported SIP Servers

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

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

1.6 Product Specifications

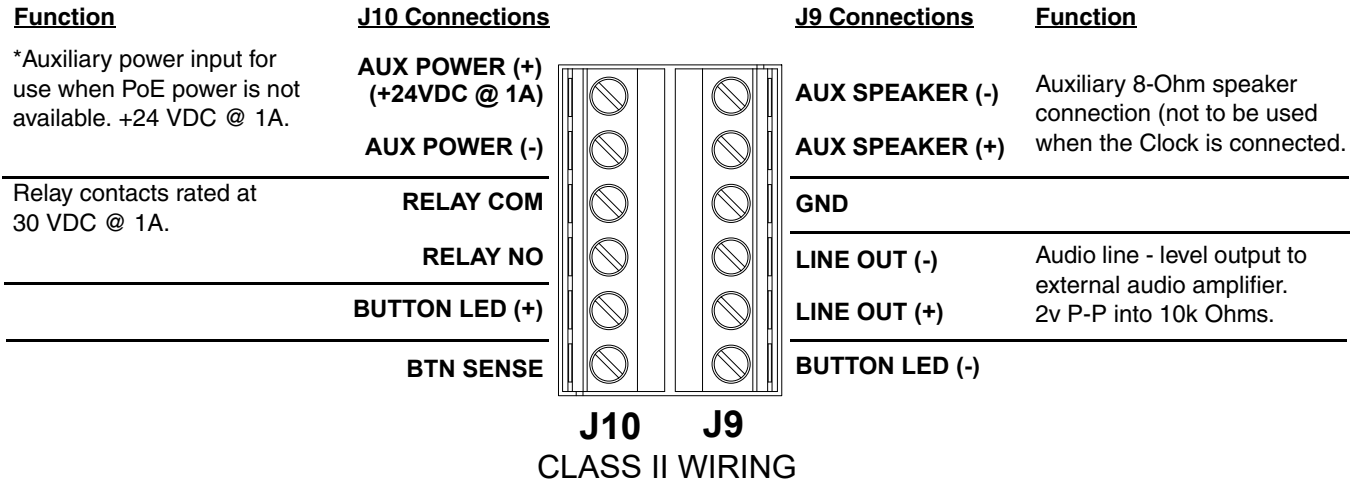
Table 1-1. Product Specifications

Category	Specification
Ethernet I/F	10/100 Mbps
Protocol	SIP RFC 3261 Compatible
Power Input	PoE 802.3af/802.3at compliant or 24VDC @ 1A Auxiliary Power Supply (not included)
Audio Output	802.3af - SPL 109.2 dB @ 1 meter 802.3at - SPL 111.9 dB @ 1 meter
On-Board Relay	1A @ 30 VDC
Payload Types	G.711 a-law, G.711 μ -law, G.722, and G.729
Network Security	TLS/SSL 1.2 and SRTP
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	9 in. [228.6 mm] Grill Diameter 7.25 in. [184.2 mm] Can Diameter 2.4 in. [60.96 mm] Can Depth
Weight	3.0 lbs [1.36 kg]
Boxed Weight	4.0 lbs. [1.81 kg]
Compliance	CE; EMC Directive – Class A EN 55032 & EN 55024, LV Safety Directive – EN 60950-1, RoHS Compliant, FCC; Part 15 Class A, Industry Canada; ICES-3 Class A, IEEE 802.3 Compliant
Warranty	2 Years Limited
Part number	011398

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

1.7 Optional Connections (J9 and J10)

Figure 1-3. Optional Connections (J9 and J10)



*Do not use auxiliary power input when speaker J1 is connected to a PoE power source.

1.8 Compliance

1.8.1 CE Testing

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

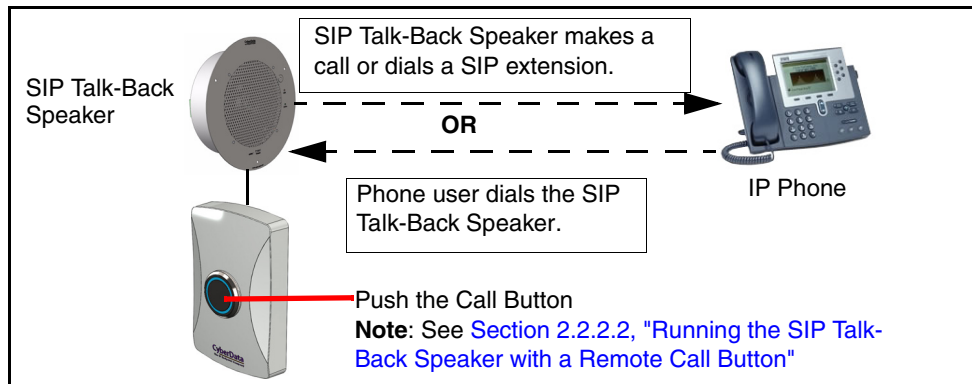
Note You can download the Declaration of Conformity document from the **Downloads** tab of the product's webpage.

1.8.2 FCC Statement

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

1.9 Audio Modes for the Talk Back Speaker

Figure 1-4. Push to Talk Mode



Note Note: Call button is optional for all modes except Push to Talk.

1.9.1 Acoustic Echo Canceler

By default, the speaker will be in echo cancelling mode, which allows the speaker to function in a full duplex conversation.

Figure 1-5. Acoustic Echo Canceler

Acoustic Echo Canceler (AEC)

Enable Echo Canceler:

Echo Frame Size (bytes): 160

Echo Tail Length (ms): 160

Echo Delay (ms): 48

Distance to furthest surface (ft): 30

Calculate Echo Tail Length

The user enters the Echo Frame Size and the Distance to furthest surface.

The **Echo Frame Size** setting should be 160 for G.711 and G.722, and 20 for G.729.

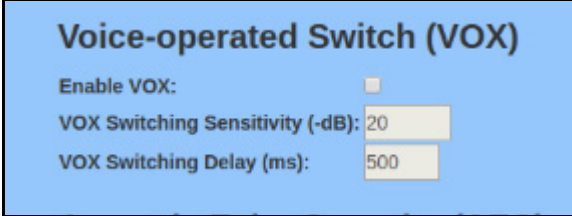
The **Distance to the furthest surface** setting is the distance from the speaker to the furthest reflective surface. This value can be used to calculate an approximate echo tail length for the echo canceler. Additional adjustments to the echo tail length may be needed, depending on the reflective characteristics of the room. Surfaces like carpet or vaulted ceilings create different acoustic characteristics for a room.

The **Calculate Echo Tail Length** button will adjust the tail length and echo delay to accommodate the room dimensions.

1.9.2 Voice-operated Switch (VOX)

If echo cancellation does not adequately cancel the echo, VOX offers adaptive half-duplex audio.

Figure 1-6. Voice-operated Switch (VOX)



The screenshot shows a configuration window titled "Voice-operated Switch (VOX)". It contains three settings: "Enable VOX:" with a checked checkbox, "VOX Switching Sensitivity (-dB):" with a text input field containing "20", and "VOX Switching Delay (ms):" with a text input field containing "500".

1.9.2.1 VOX Switching Sensitivity

Sensitivity for whether the far-end (remote) signal is considered strong enough to mute the microphone. This setting may need to be adjusted to account for the strength of a given remote signal. The higher the value, the more sensitive the switching will be. A value of '0' is considered the least sensitive; the microphone will likely never be muted at this level.

1.9.2.2 VOX Switching Delay (ms)

Delay (in milliseconds) after the threshold has been exceeded before the remote signal level will be measured again.

1.9.3 Push to Talk

Another option for half-duplex audio is Push to Talk, which requires the installation of a call button (Figure 1-8), and is enabled on the **Device Page** by enabling the **Button Installed** and **Enable Push to Talk** settings. See Figure 1-7.

Figure 1-7. Enable the Button Installed and Enable Push to Talk Settings

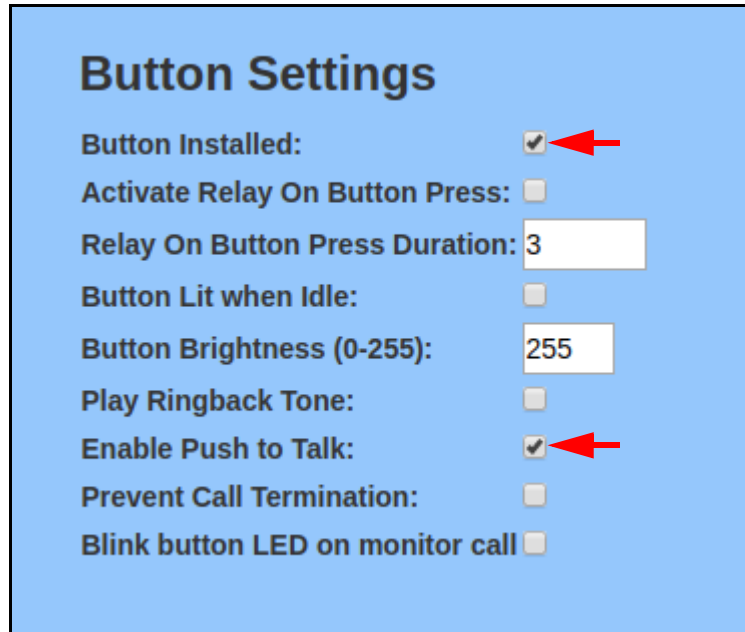
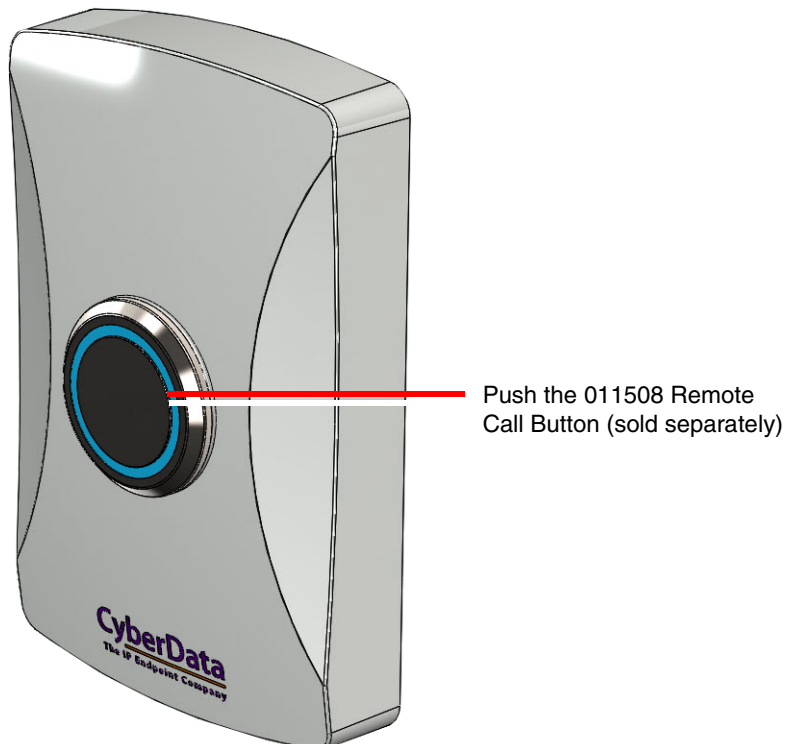
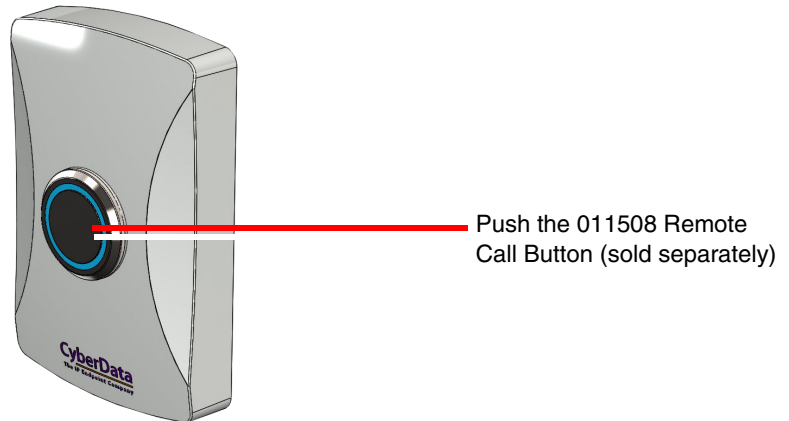


Figure 1-8. Remote Call Button (sold separately)



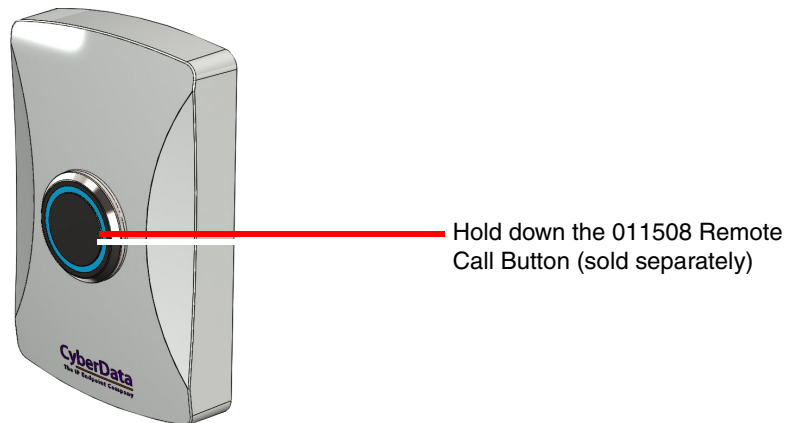
1. Push the Call Button to make a call or dial the SIP extension. See [Figure 1-9](#).

Figure 1-9. Push the Call Button to Make a Call



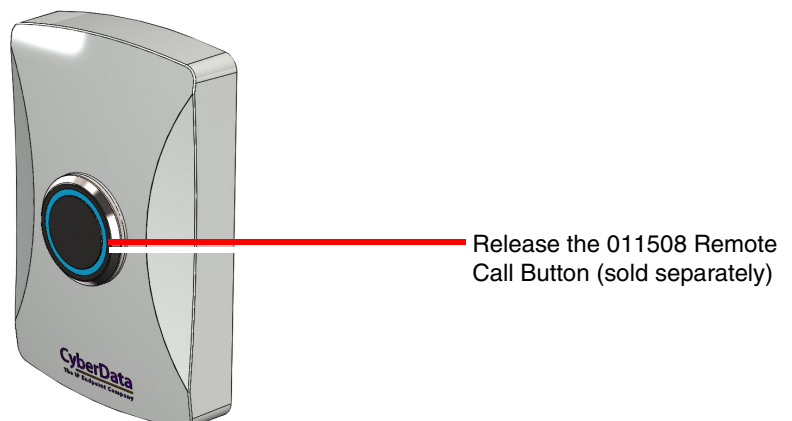
2. To talk to someone on the other end, the person at the SIP Talk-Back Speaker, must hold down the Call Button while they are talking to the person on the other end. See [Figure 1-10](#).

Figure 1-10. Hold Down the Call Button While Talking



3. To listen to someone talking on the other end, the person at the SIP Talk-Back Speaker must release the Call Button. See [Figure 1-11](#).

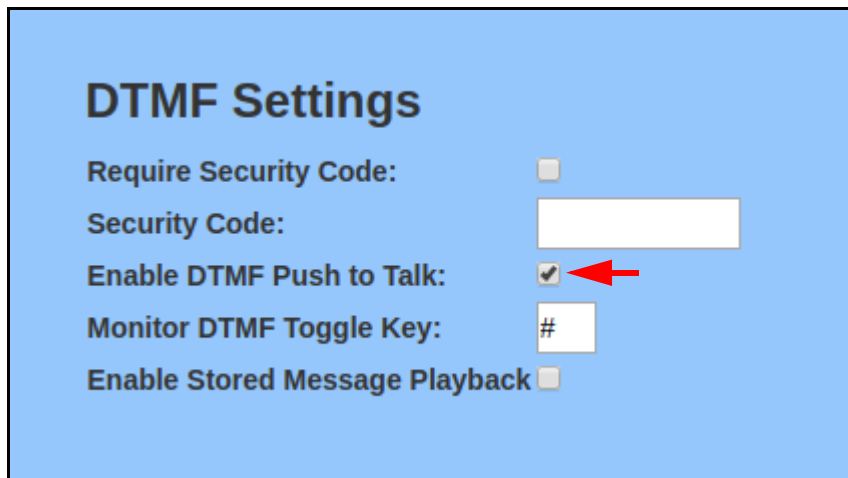
Figure 1-11. Release the Call Button While Listening



1.9.4 DTMF Push to Talk

Some installations in extremely noisy environments (e.g., tollbooths) opt to use DTMF Push to Talk, where the audio flow is controlled by the phone. This is enabled on the Device Page by enabling the **Enable DTMF Push to Talk** setting. The **Monitor DTMF Toggle Key** setting is configurable. See [Figure 1-12](#).

Figure 1-12. DTMF Settings



DTMF Settings

Require Security Code:

Security Code:

Enable DTMF Push to Talk: ←

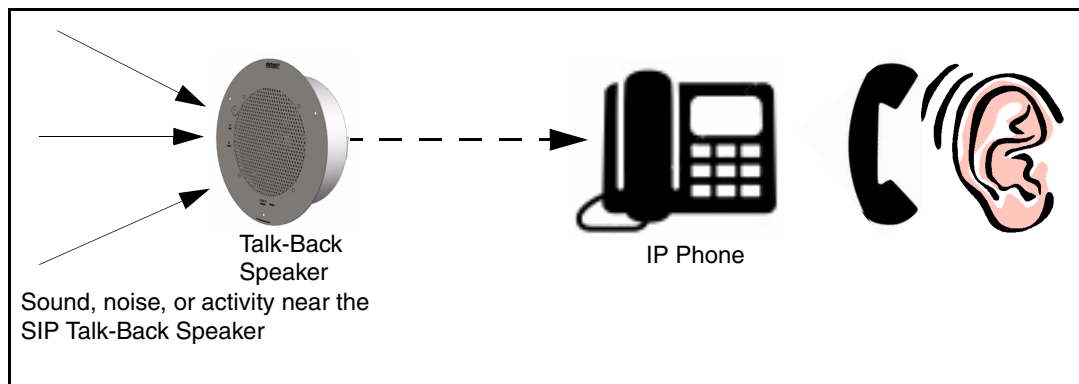
Monitor DTMF Toggle Key:

Enable Stored Message Playback

1.9.5 Monitor Mode

In **Monitor Mode**, the person on the phone can listen to any activity that is occurring near the Push-to-Talk Speaker. See [Figure 1-13](#).

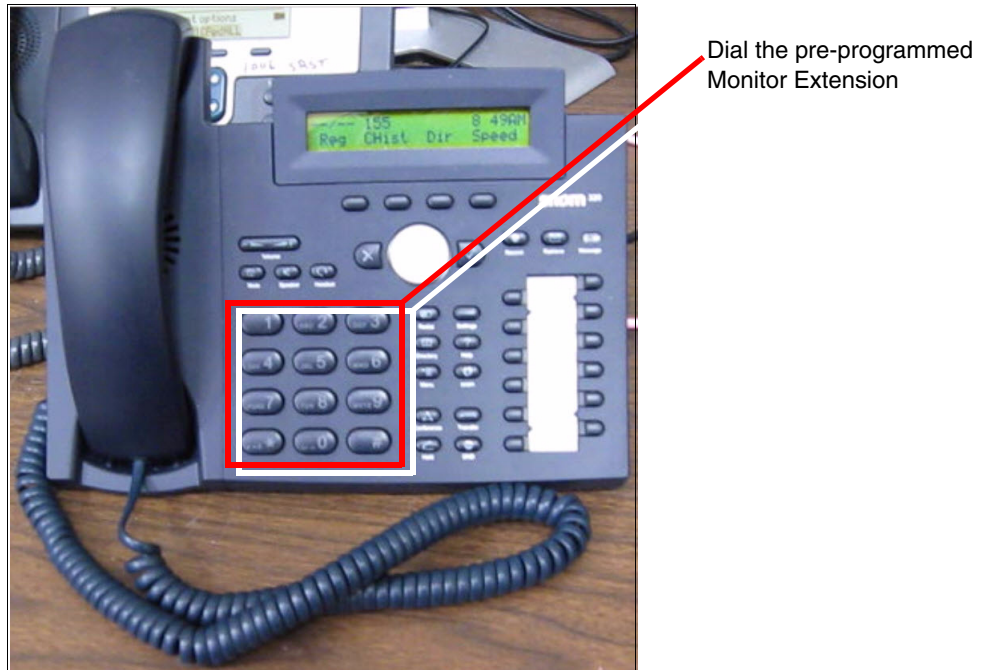
Figure 1-13. Monitor Mode



- The Call Button is not used during **Monitor Mode**.
- **Monitor Mode** is controlled by the phone instead of the Push-to-Talk Speaker.

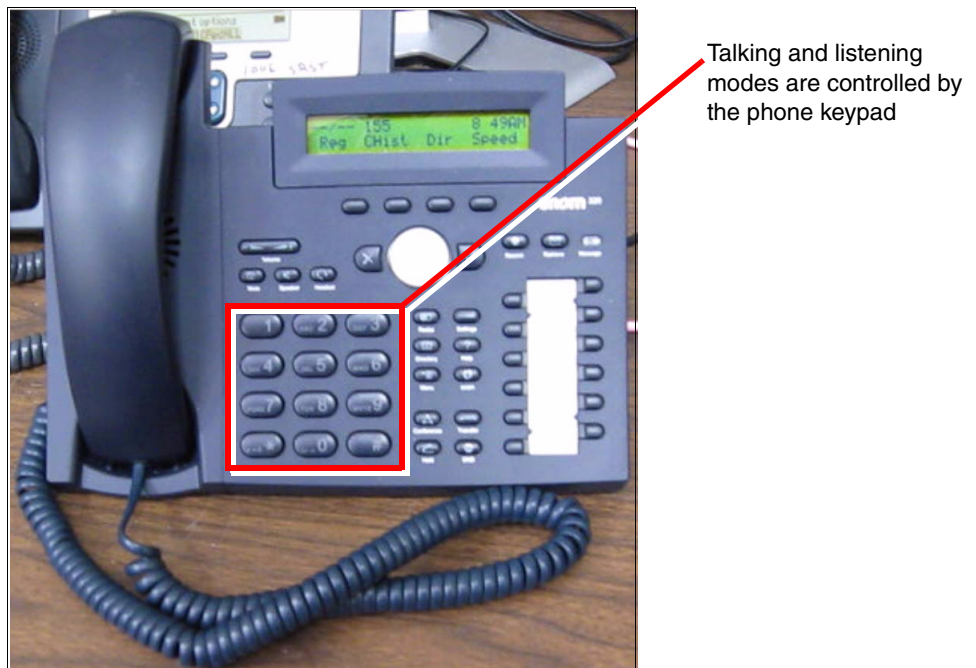
- To initiate the **Monitor Mode**, someone on a phone must dial the pre-programmed **Monitor Extension**. See [Figure 1-14](#).

Figure 1-14. Dial the Monitor Extension



- In **Monitor Mode**, the "talking mode" and the "listening mode" are controlled by one of the pre-programmed buttons on the phone keypad. Therefore, if someone is in the "listening mode," they must press a pre-programmed keypad button to enter the "talking mode." Conversely, if someone is in the "talking mode," they must press a pre-programmed keypad button to enter the "listening mode."

Figure 1-15. Talking and Listening Modes are Controlled by the Phone Keypad



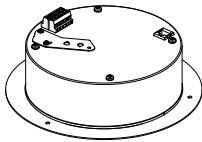


2 Installing the SIP Talk-Back Speaker

2.1 Parts List

Table 2-1 illustrates the parts for each speaker and includes kits for the drop ceiling and drywall mounting.

Note The installation template for the SIP Talk-Back Speaker is located on the *Installation Quick Reference Guide* that is included in the packaging with each speaker.

Table 2-1. Parts

Quantity	Part Name	Illustration
1	SIP Talk-Back Speaker Assembly	
1	Installation Quick Reference Guide	
1	Speaker Mounting Accessory Kit	

2.2 Device Configuration

Set up and configure each speaker *before* you mount it.

CyberData delivers each speaker with the following factory default values:

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

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

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

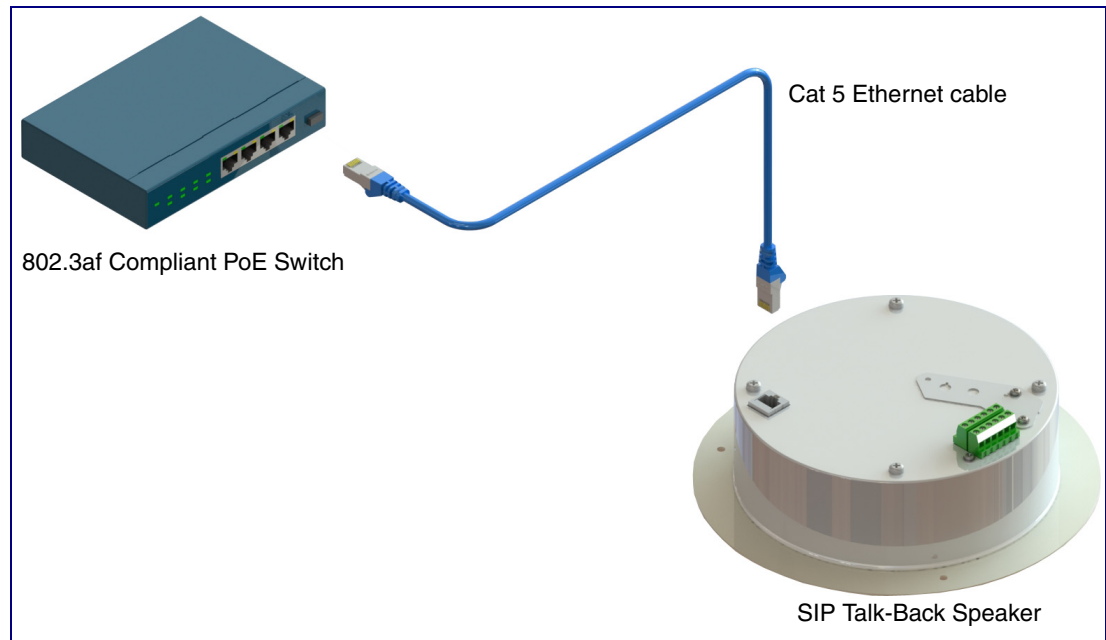
2.2.1 Connect Power to the Speaker

Figure 2-1 through Figure 2-3 illustrates how to connect power to the SIP Talk-Back Speaker.

2.2.1.1 SIP Talk-Back Speaker to a 802.3af Compliant PoE Switch

Figure 2-1 illustrates how to connect the SIP Talk-Back Speaker to a 802.3af compliant PoE switch via a Cat 5 Ethernet cable.

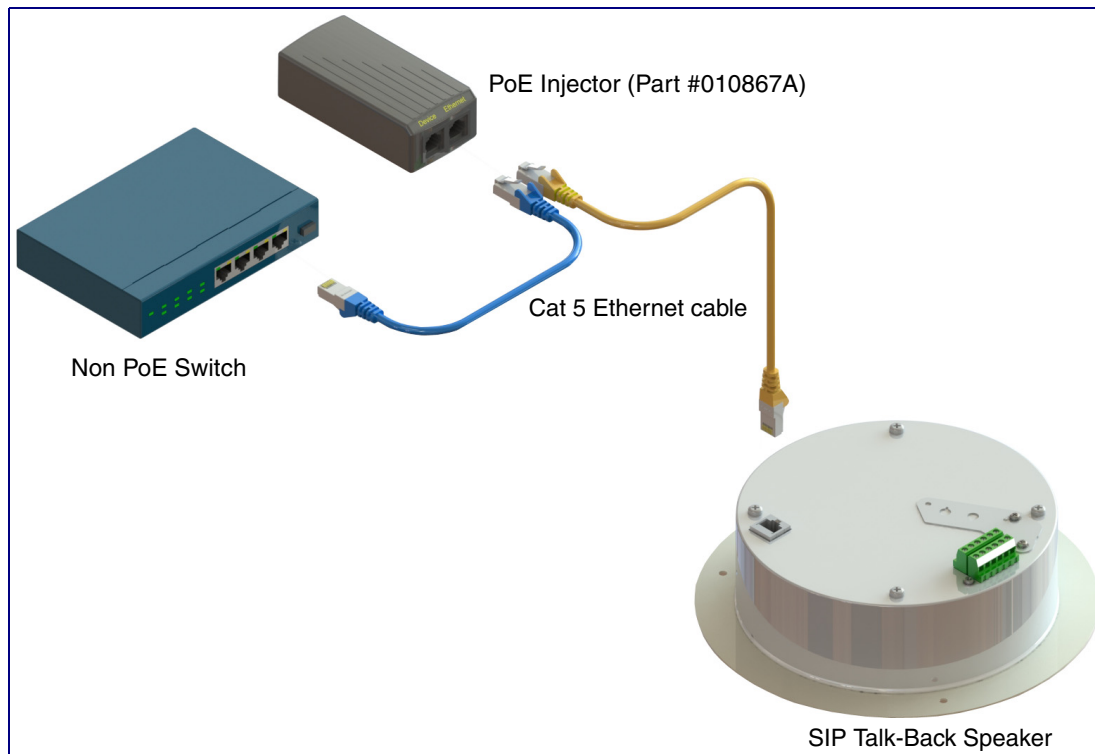
Figure 2-1. SIP Talk-Back Speaker to a 802.3af Compliant PoE Switch



2.2.1.2 SIP Talk-Back Speaker (with PoE Injector) to a 802.3af Compliant PoE Switch

In [Figure 2-2](#), if a PoE switch is not available, you will need a PoE Injector, part #010867A (ordered separately). A PoE Injector is a power supply solution for those who have a standard Non PoE Switch.

Figure 2-2. SIP Talk-Back Speaker (with PoE Injector) to a Non PoE Switch



2.2.1.3 Running the SIP Talk-Back Speaker with Auxiliary Power

In [Figure 2-3](#), the power for the SIP Talk-Back Speaker can either come from an 802.3af Network connection or from an external source.


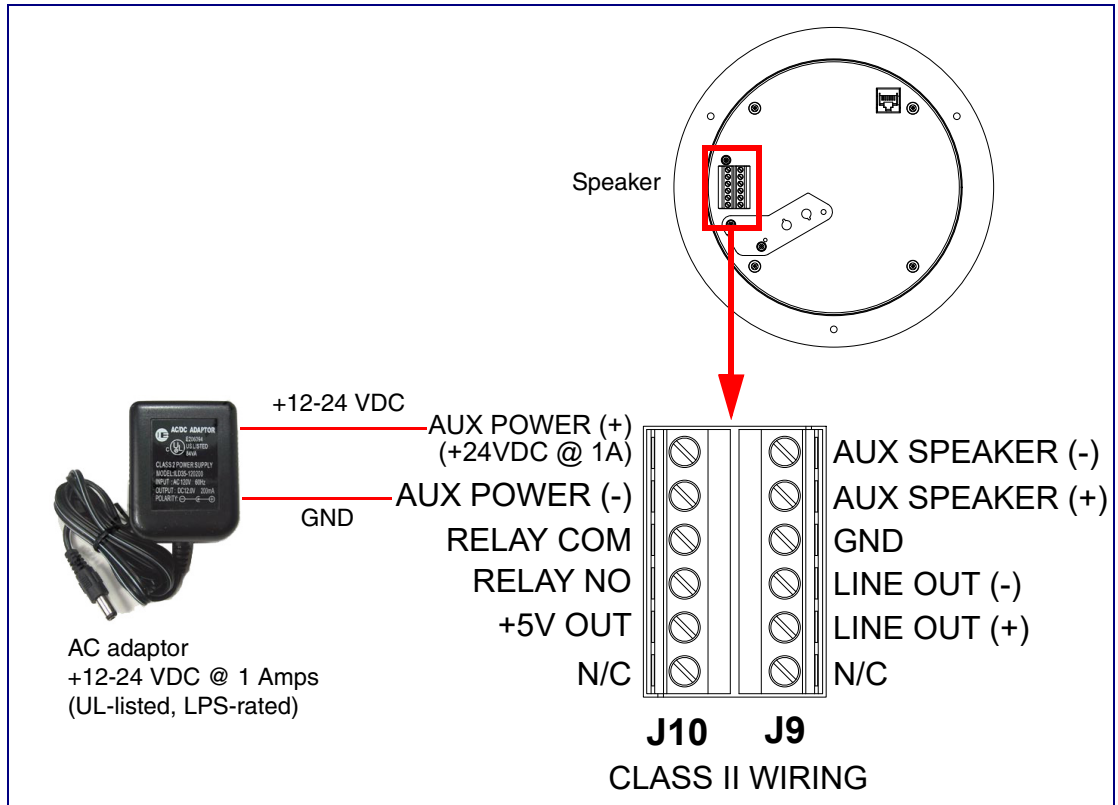
 GENERAL ALERT	<p>Caution</p> <p><i>Operational Note:</i> Do not connect an auxiliary power supply when the SIP Talk-Back Speaker is connected to a PoE power source through J1. Improper operation or equipment damage may occur.</p>
--	--

Figure 2-3. Running the Speaker with Auxiliary Power



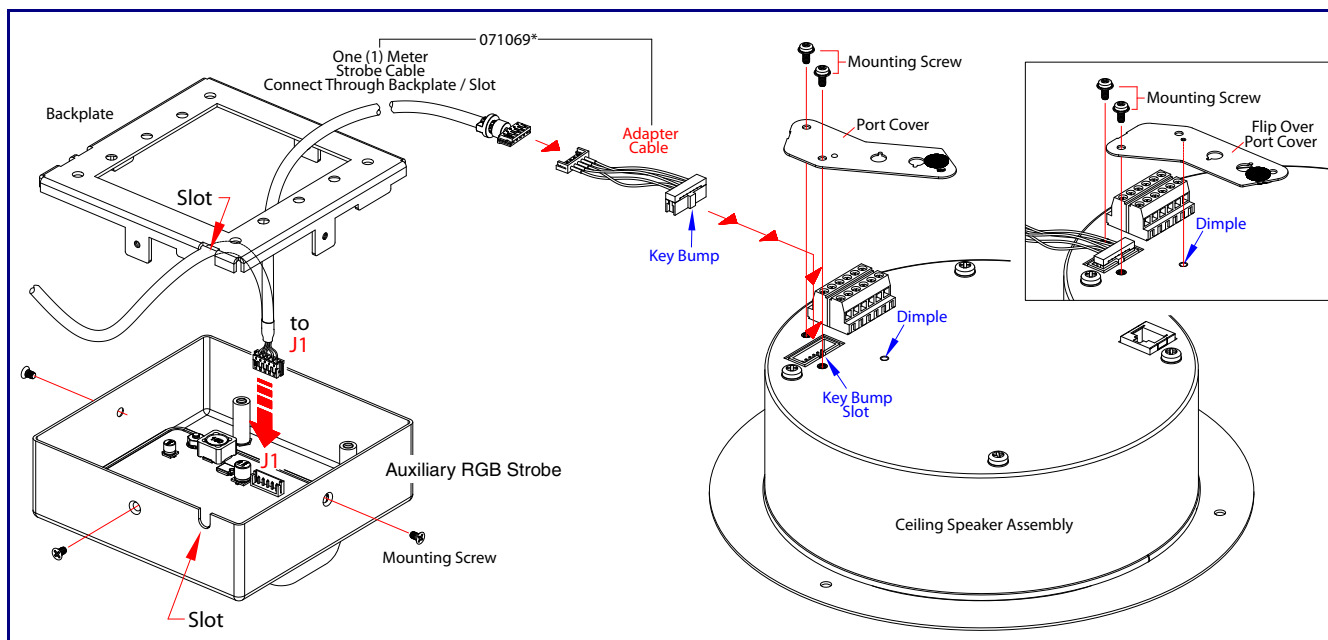
2.2.2 Installation Options

This section shows various installation options for the SIP Talk-Back Speaker.

2.2.2.1 Connecting the Auxiliary RGB Strobe to the SIP Speaker

1. Connect the one meter strobe cable to the adapter cable. See [Figure 2-4](#).
2. Remove the mounting screws and port cover from the SIP Speaker. See [Figure 2-4](#).
3. Align the key bump on the adapter cable to the key bump slot on the SIP Speaker. See [Figure 2-4](#).
4. Replace the port cover and mounting screw. See [Figure 2-4](#).

Figure 2-4. Connecting the Auxiliary RGB Strobe Kit to the SIP Speaker



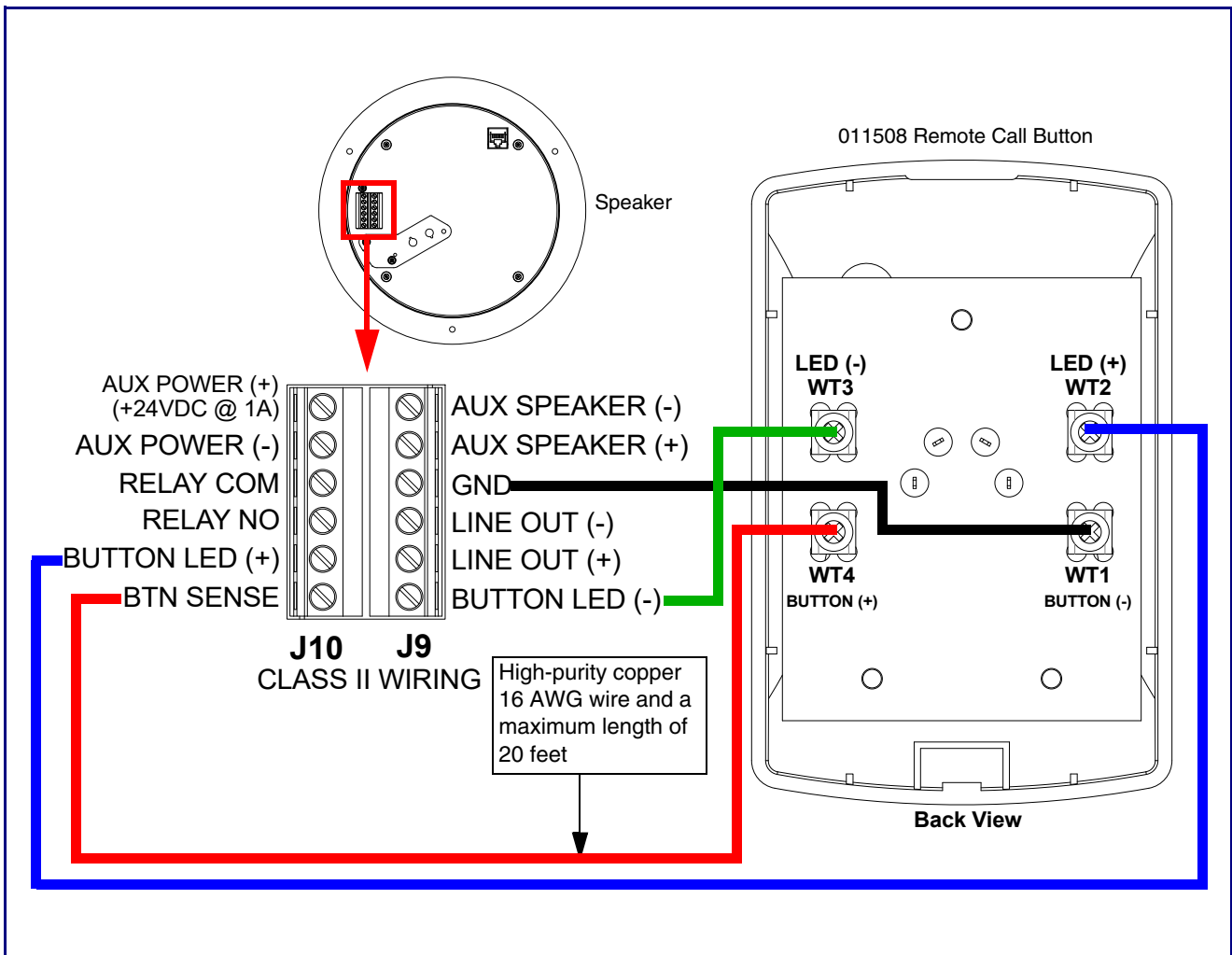
2.2.2.2 Running the SIP Talk-Back Speaker with a Remote Call Button

Note Figure 2-3 shows the optional 011185 Remote Call Button (sold separately). See Section Figure 1-15., "Talking and Listening Modes are Controlled by the Phone Keypad"

In Figure 2-3, the optional Remote Call Button (sold separately) enables calls to the SIP Talk-Back Speaker that can be initiated or answered from a remotely-mounted switch. When enabled through the web interface, if the Remote Call Button is pressed, the speaker would initiate a SIP call to a predetermined extension.

When the SIP Talk-Back Speaker is called from a remote phone and Auto-Answer is not enabled within the unit's Web interface, the LED on the Remote Button will blink. The call will be answered when the button is pressed.

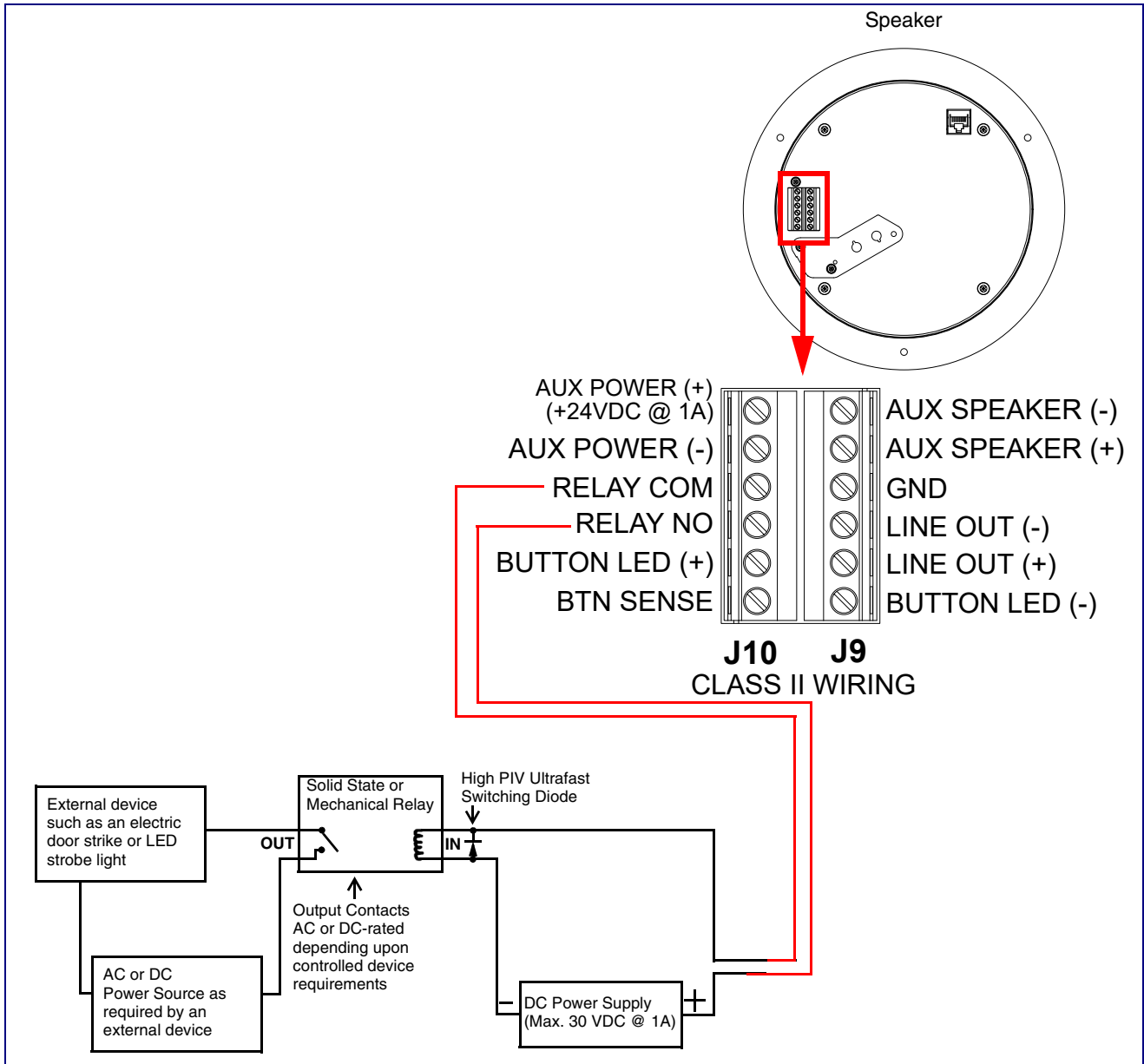
Figure 2-5. Running the Speaker with a Remote Call Button



2.2.2.3 SIP Talk-Back Speaker with an External Device

In [Figure 2-6](#), when the SIP Talk-Back Speaker is called from a remote phone, the relay on the speaker can be programmed to drive an external device such as an alert strobe. This external device may also be addressed from a separate Unified Communication (UC) server.

Figure 2-6. Speaker with an External Device



2.2.2.4 SIP Talk-Back Speaker with Auxiliary Speaker Connection

In [Figure 2-7](#), the SIP Talk-Back Speaker supports an amplified audio output for a second analog speaker. While the total speaker wattage is the same, by connecting a low cost analog speaker, additional coverage can be realized


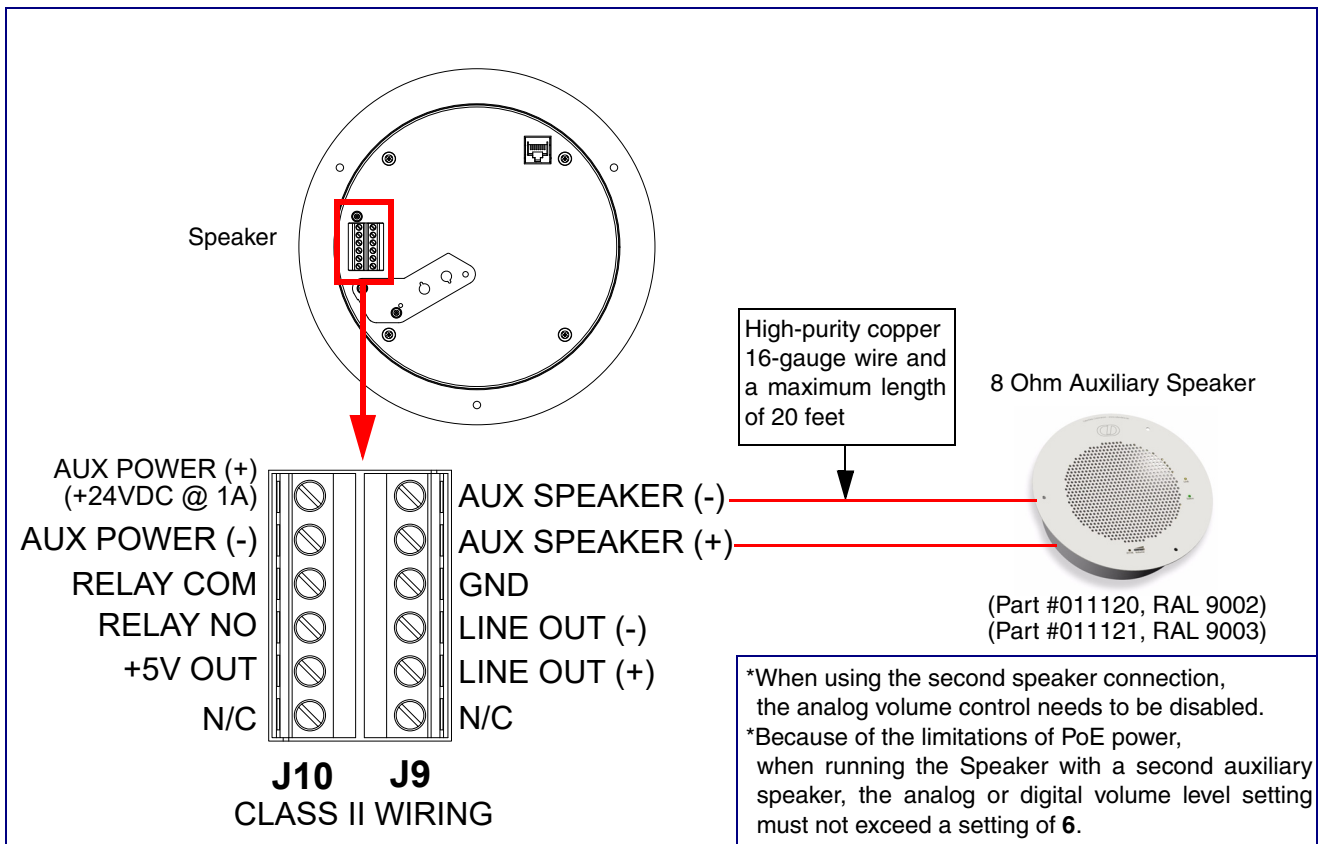
 <small>GENERAL ALERT</small>	<p>Caution</p> <p><i>Operational Note:</i> The SIP speaker dynamically adjusts volume to properly budget power when accessories are connected. For best performance, it is recommended that either an 802.3AT or 24V auxiliary power source is used when connecting an auxiliary speaker and a clock kit.</p>
---	--

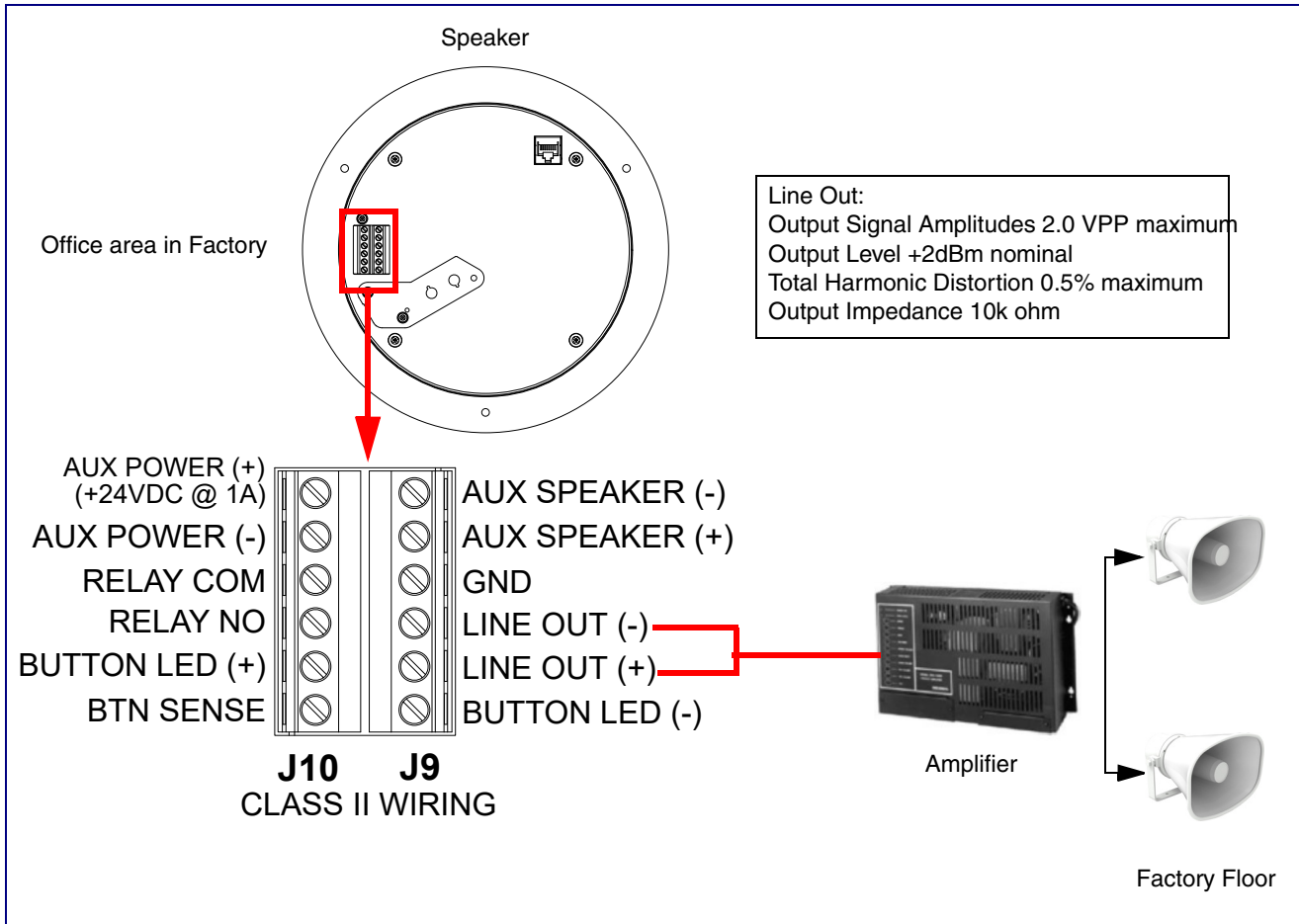
Figure 2-7. SIP Talk-Back Speaker with Auxiliary Speaker Connection



2.2.2.5 SIP Talk-Back Speaker with Line Out

In [Figure 2-8](#), for areas that require more speaker volume, the SIP Talk-Back Speaker can be connected directly to an auxiliary amplifier to drive additional horns or speakers. This is done through the line-out connection.

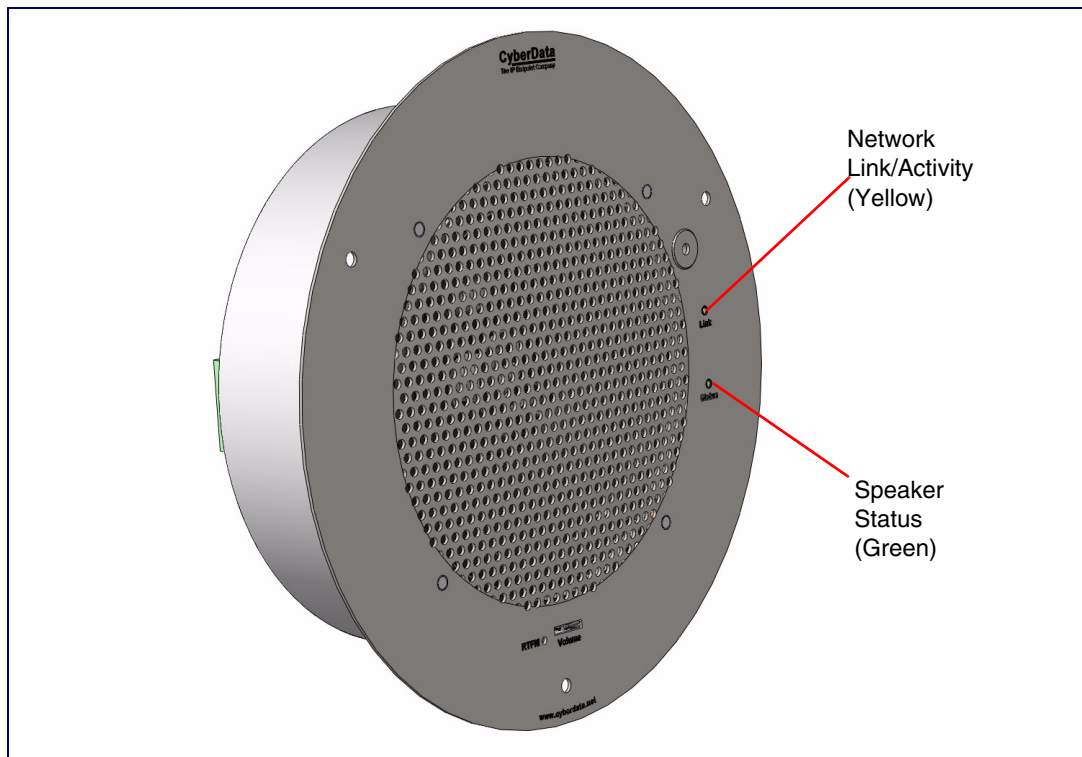
Figure 2-8. SIP Talk-Back Speaker with Line Out



2.2.3 Confirm that the Speaker is Operational and Linked to the Network

After connecting the speaker to the 802.3af compliant Ethernet hub, the LEDs on the speaker face confirm that the speaker is operational and linked to the network.

Figure 2-9. Status and Activity LEDs



2.2.3.1 Status LED

After supplying power to the speaker:

1. The green power/status LED and the yellow network LED comes on immediately.
2. After about 23 seconds with a static IP address (or 27 seconds if the board is set to use DHCP), the green LED will blink twice to indicate that the board is fully booted. The speaker will beep at this time if the **Beep on Init** option is enabled on the **Device Page** (see [Section 2.3.5](#)).

Note If the board is set to use DHCP and there is not a DHCP server available on the network, it will try 12 times with a three second delay between tries and eventually fall back to the programmed static IP address (by default 10.10.10.10). This process will take approximately 80 seconds.

Note The front power/status LED will remain solid on during operation.

2.2.3.2 Link LED

- The **Link** LED is illuminated when the network link to the speaker is established.
- The **Link** LED blinks to indicate network traffic.

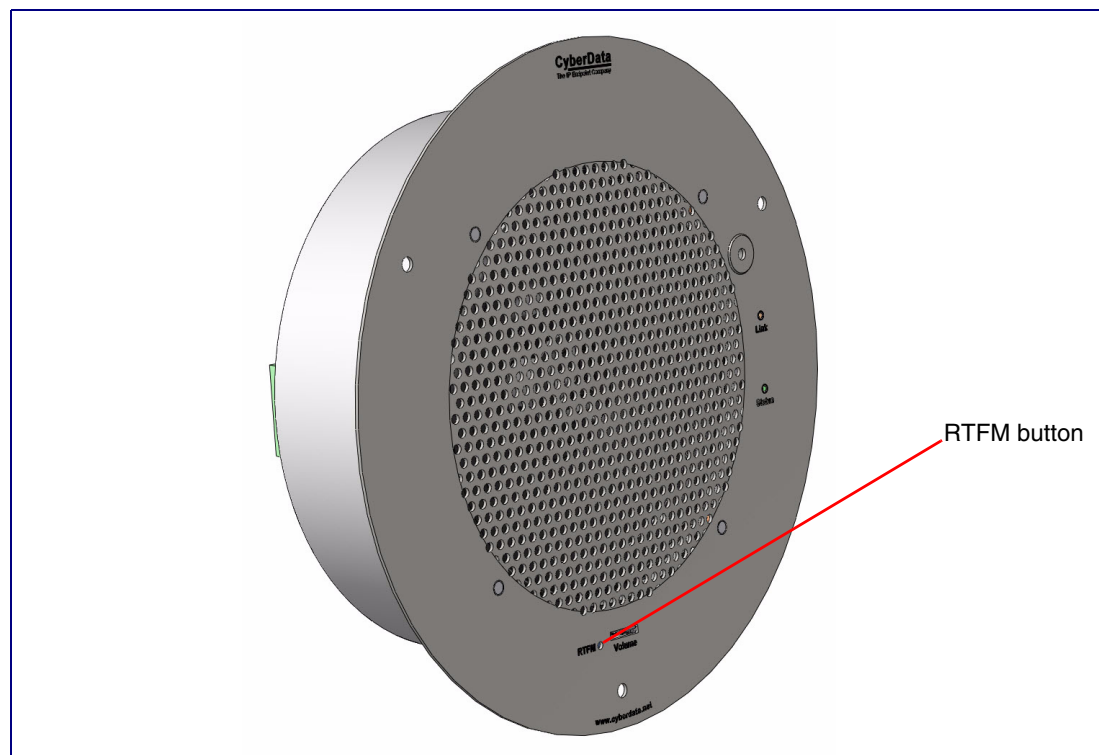
2.2.4 Confirm the IP Address and Test the Audio

2.2.4.1 Reset Test Function Management (RTFM) Button

When the speaker is operational and linked to the network, use the Reset Test Function Management (RTFM) button (Figure 2-10) on the speaker face to announce and confirm the speaker's IP Address and test that the audio is working.

Note Using the RTFM button will lock the digital volume level to 4 and disable the analog volume control dial.

Figure 2-10. RTFM Button



To announce a speaker's current IP address, press and release the RTFM button within a five second window.

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

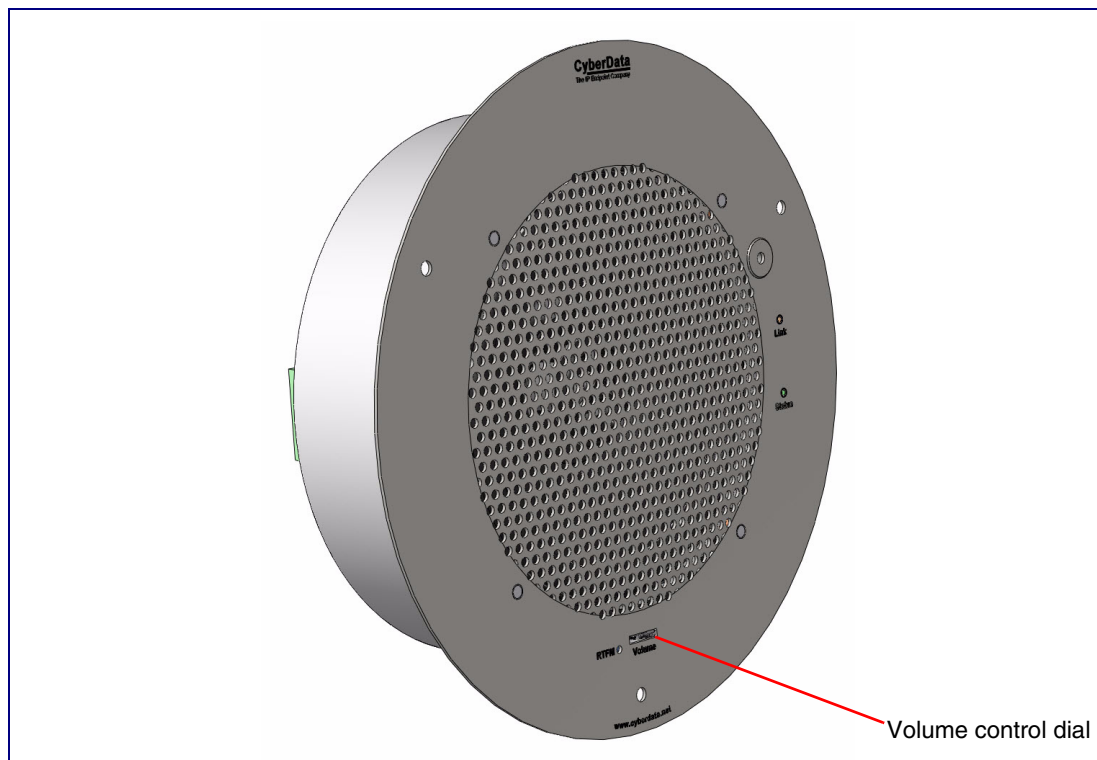
Note Pressing and holding the RTFM button for longer than five seconds will restore the speaker to the factory default settings.

2.2.5 Adjust the Volume

To adjust the speaker volume, turn the **Volume** control dial (Figure 2-11) on the speaker face.

Note The SIP Talk-Back Speaker has two volume controls: **Internal** (web-based) and **External** (volume knob). The external volume control can be disabled from the web interface by selecting **Disable Volume Control Dial** on the **Audio Page** (see Section 2.3.5).

Figure 2-11. Volume Control

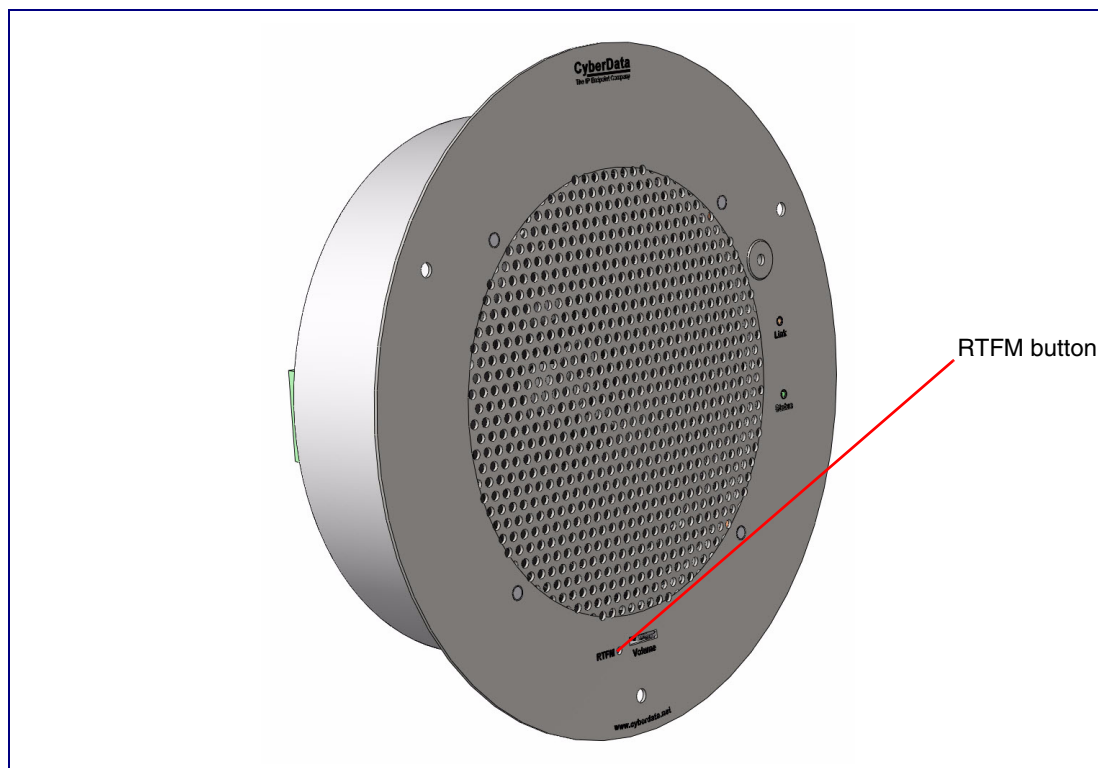


2.2.6 How to Set the Factory Default Settings

2.2.6.1 RTFM Button

When the speaker is operational and linked to the network, use the Reset Test Function Management (RTFM) button (Figure 2-12) on the speaker face to set the factory default settings.

Figure 2-12. RTFM Button



To set the factory default settings:

1. Press and hold the **RTFM** button for more than five seconds.
2. The speaker announces that it is restoring the factory default settings.

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

2.3 Configure the SIP Talk-Back Speaker Parameters

To configure the SIP Talk-Back Speaker online, use a standard web browser.

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

2.3.1 Factory Default Settings

All SIP Talk-Back Speakers are initially configured with the following default IP settings:

When configuring more than one SIP Talk-Back Speaker, attach the SIP Talk-Back Speakers to the network and configure one at a time to avoid IP address conflicts.

Table 2-3. Factory Default Settings

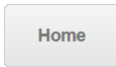
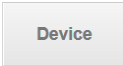
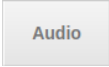
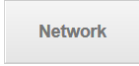



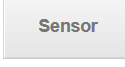
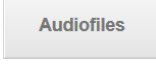
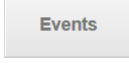
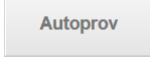
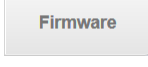
Parameter	Factory Default Setting
IP Addressing	DHCP
IP Address ^a	10.10.10.10
Web Access Username	admin
Web Access Password	admin
Subnet Mask ^a	255.0.0.0
Default Gateway ^a	10.0.0.1

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

2.3.2 SIP Talk-Back Speaker Web Page Navigation

Table 2-4 shows the navigation buttons that you will see on every SIP Talk-Back Speaker web page.

Table 2-4. Web Page Navigation

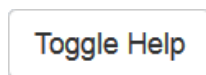
Web Page Item	Description
	Link to the Home page.
	Link to the Device page.
	Link to the Audio page.
	Link to the Network page.
	Link to go to the SIP page.
	Link to the Multicast page.
	Link to the SSL page.
	Link to the Sensor page.
	Link to the Audiofiles page.
	Link to the Events page.
	Link to the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

2.3.3 Using the Toggle Help Button

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

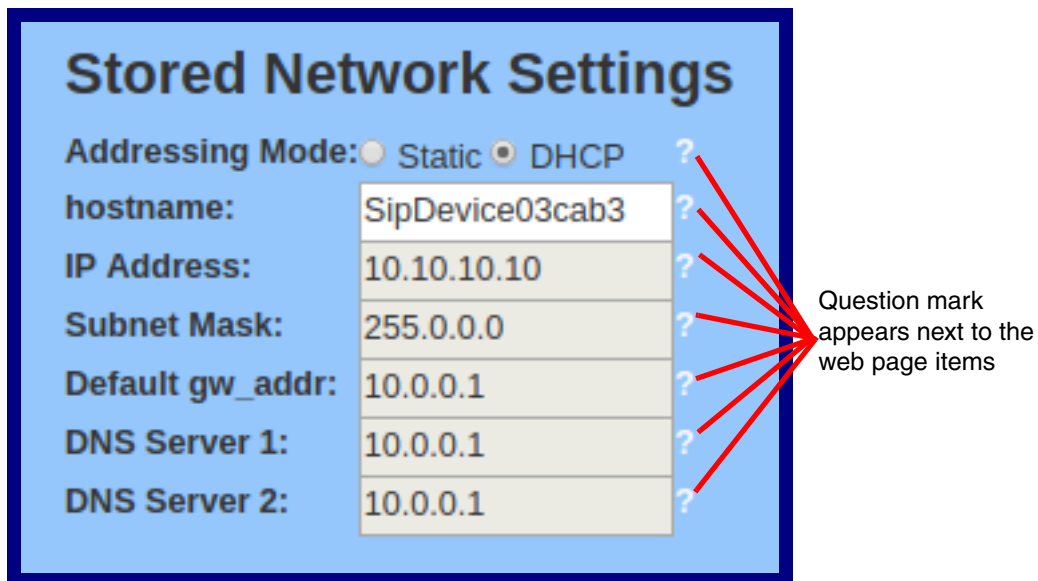
1. Click on the **Toggle Help** button that is on the UI webpage. See [Figure 2-13](#) and [Figure 2-14](#).

Figure 2-13. Toggle/Help Button



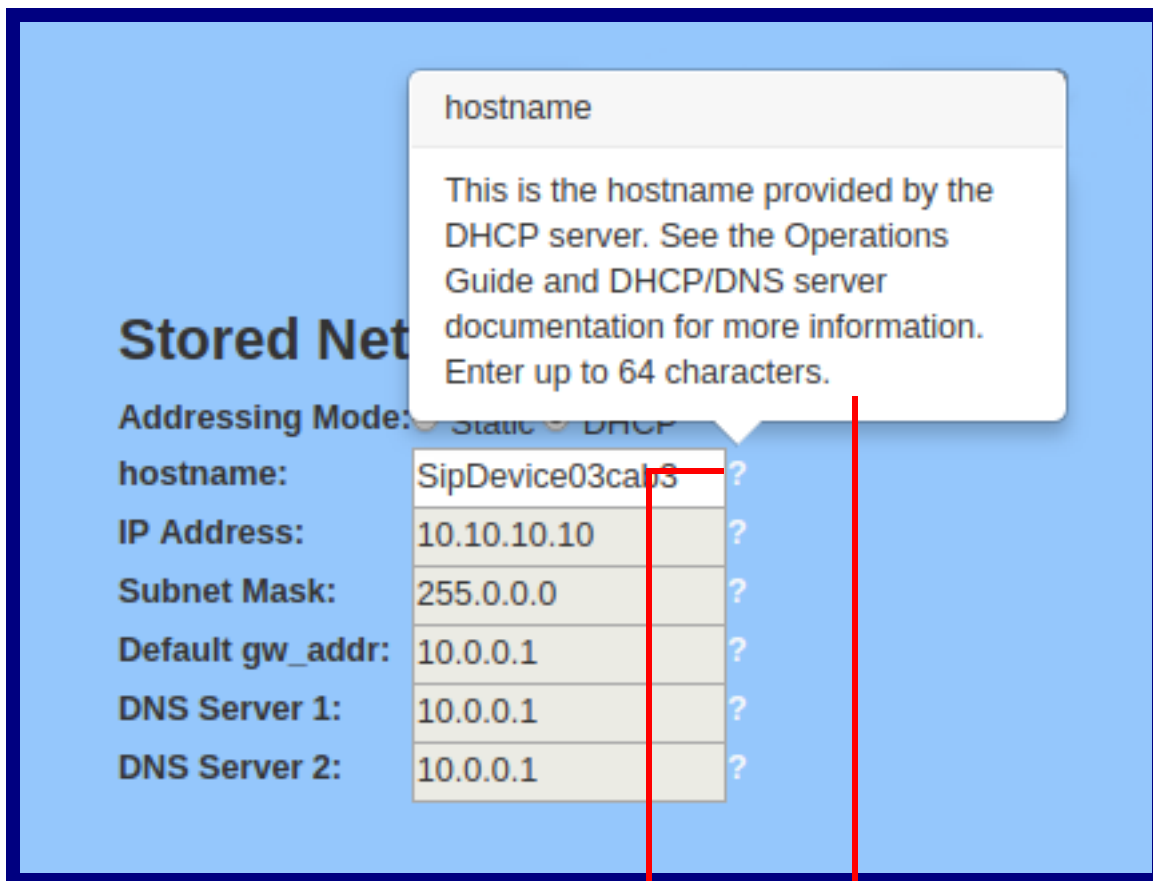
2. You will see a question mark (?) appear next to each web page item that has been provided with a short description by the Help feature. See [Figure 2-14](#).

Figure 2-14. 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 2-15.

Figure 2-15. Short Description Provided by the Help Feature



Question mark

A short description of the web page item will appear

2.3.4 Log in to the Configuration Home Page

Note The version of InformaCast needs to be 4.0 or higher.

4. Open your browser to the SIP Talk-Back Speaker IP address.

Note If the network does not have access to a DHCP server, the device will default to an IP address of 10.10.10.10.

Note Make sure that the PC is on the same IP network as the SIP Talk-Back Speaker.

Note You may also download CyberData's VoIP Discovery Utility program which allows you to easily find and configure the default web address of the CyberData VoIP products.

CyberData's VoIP Discovery Utility program is available at the following website address:

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

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

5. When prompted, use the following default **Web Access Username** and **Web Access Password** to access the **Home Page** (Figure 2-16):

Web Access Username: **admin**

Web Access Password: **admin**

Figure 2-16. Home Page

The screenshot displays the home page of the CyberData V3.1 Speaker configuration interface. At the top, there is a navigation bar with tabs for Home, Device, Audio, Network, SIP, Multicast, SSL, Sensor, Audiofiles, Events, Autopro, and Firmware. The main heading is "CyberData V3.1 Speaker".

The page is divided into three main sections:

- Current Status:** Displays device information such as Serial Number (398100001), Mac Address (00:20:f7:04:10:46), and Firmware Version (v12.1.0). It also shows IP Addressing (DHCP), IP Address (10.10.1.204), Subnet Mask (255.0.0.0), Default Gateway (10.0.0.1), and DNS Server 1 (10.0.1.56). SIP Mode is Enabled, while Multicast Mode, Event Reporting, and Nightringer are Disabled. SIP server status is shown as "Not registered" for Primary, Backup 1, Backup 2, Nightringer, and Monitor servers.
- Admin Settings:** Includes fields for Username (admin), Password, and Confirm Password. Action buttons for Save, Reboot, and Toggle Help are present.
- Import Settings:** Features a file selection button (Browse... No file chosen) and an Import Config button.
- Export Settings:** Includes an Export Config button.

6. On the **Home** page, review the setup details and navigation buttons described in [Table 2-5](#).

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 2-5. Home Page Parameters

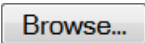




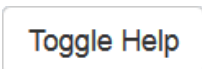
Web Page Item	Description
Admin Settings	
Username ?	The username to access the web interface. Enter up to 25 characters.
Password ?	The password to access the web interface. Enter up to 25 characters.
Confirm Password ?	Confirm the web interface password.
Current Status	
Serial Number	Shows the device serial number.
Mac Address	Shows the device Mac address.
Firmware Version	Shows the current firmware version.
IP Addressing	Shows the current IP addressing setting (DHCP or static).
IP Address	Shows the current IP address.
Subnet Mask	Shows the current subnet mask address.
Default Gateway	Shows the current default gateway address.
DNS Server 1	Shows the current DNS Server 1 address.
DNS Server 2	Shows the current DNS Server 2 address.
SIP Mode	Shows the current status of the SIP mode.
Multicast Mode	Shows the current status of the Multicast mode.
Event Reporting	Shows the current status of the Event Reporting mode.
Nightringer	Shows the current status of the Nightringer mode.
Primary SIP Server	Shows the current status of the Primary SIP Server.
Backup Server 1	Shows the current status of Backup Server 1.
Backup Server 2	Shows the current status of Backup Server 2.
Nightringer Server	Shows the current status of Nightringer Server.
Monitor SIP Server	Shows the current status of the Monitor SIP Server.
Import Settings	
	Use this button to select a configuration file to import.
	After selecting a configuration file, click Import to import the configuration from the selected file. Then, click Save and Reboot to store changes.
Export Settings	
	Click Export to export the current configuration to a file.

Table 2-5. Home Page Parameters (continued)

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

2.3.5 Configure the Device

1. Click the **Device** menu button to open the **Device** page. See [Figure 2-17](#) and [Figure 2-18](#).

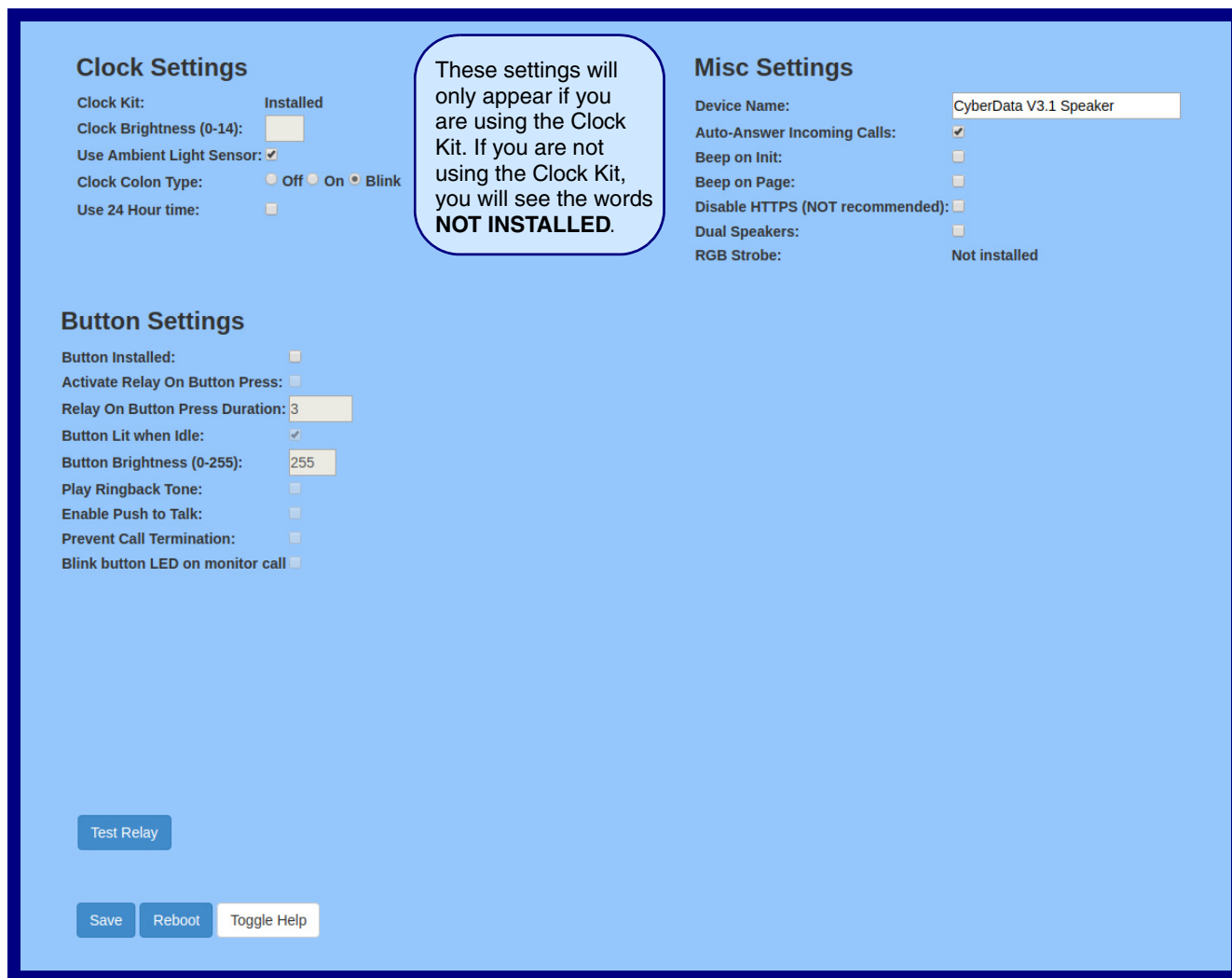
Figure 2-17. Device Page

The screenshot shows the configuration page for a CyberData V3.1 Speaker. At the top, there is a navigation menu with buttons for Home, Device, Audio, Network, SIP, Multicast, SSL, Sensor, Audiofiles, Events, Autopro, and Firmware. The main heading is "CyberData V3.1 Speaker".

The page is divided into four main sections:

- DTMF Settings:**
 - Require Security Code:
 - Security Code:
 - Enable DTMF Push to Talk:
 - Monitor DTMF Toggle Key:
 - Enable Stored Message Playback:
- Power Settings:**
 - 802.3AT Mode: Not detected. Disabled
 - Force 802.3AT Mode (NOT recommended):
 - Auxiliary Power Supply:
- Time Settings:**
 - Set Time with NTP server on boot:
 - NTP Server:
 - Posix Timezone String (see manual):
 - Periodically sync time with server:
 - Time update period (in hours):
 - Current Time:
 - Set Time Manually:
 -
- Relay Settings:**
 - Activate Relay with DTMF code:
 - Relay Pulse Code:
 - Relay Pulse Duration (in seconds):
 - Relay Activation Code:
 - Relay Deactivation Code:
 - Activate Relay During Ring:
 - Activate Relay During Night Ring:
 - Activate Relay While Call Active:

Figure 2-18. Device Page



2. On the **Device** page, you may enter values for the parameters indicated 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. Device Page Parameters

Web Page Item	Description
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.

















Table 2-6. Device Page Parameters (continued)

Web Page Item	Description
Enable DTMF Push to Talk ?	This option is for noisy environments. When enabled, in an active call the remote phone can force receive only audio (setting the mic gain to max and muting the speaker) by pressing the '*' key. Pressing the '#' key will force send only audio (setting the max speaker volume and muting the mic). Pressing the '0' key will restore full duplex operation with the normal microphone and speaker volume.
Monitor DTMF Toggle Key ?	Specify the key that toggles between monitor mode's 'talk' and 'listen' state. Defaults to '#'. Note: Some PBX's use # for other call functions
Enable Stored Message Playback ?	When selected, the caller will be prompted to select one of nine stored messages to play through the speaker. Stored messages may be customized on the Audiofiles page.
Time Settings	
Set Time with NTP Server on boot ?	When selected, the time is set with an external NTP server when the device restarts.
NTP Server ?	Use this field to set the address (in IPv4 dotted decimal notation or as a canonical name) for the NTP Server. This field can accept canonical names of up to 64 characters in length.
Posix Timezone String ?	See Section 2.3.5.1, "Time Zone Strings" for information about how to use the Posix Timezone String to specify time zone and daylight savings time where applicable. Enter up to 63 characters.
Periodically sync time with server ?	When selected, the time is periodically updated with the NTP server at the configured interval below.
Time update period (in hours) ?	The time interval after which the device will contact the NTP server to update the time. Enter up to 4 digits.
Current Time ?	Allows you to input the current time. (6 character limit)
Set Time Manually ?	Set the system time when NTP is not enabled. Format is HH:MM:SS
Clock Settings	
These settings will only appear if you are using the Clock Kit. If you are not using the Clock Kit, you will see the words NOT INSTALLED.	
Clock Kit ?	Displays the status of optional Clock Kit.
Clock Brightness (0 - 14) ?	This setting allows you to select the clock brightness level (0-14).
Use Ambient Light Sensor ?	This setting enables or disables the ambient light sensor.
Clock Colon Type ?	This setting allows you to select the clock colon type.
Use 24 Hour Time ?	When selected, the time will be show in 24 hour format on the optional clock display.
Button Settings	
Button Installed ?	When selected, the speaker is assumed to be wired to a push-to-talk button. Button settings will be enabled and sensor settings will be disabled. When not selected, the speaker is assumed to be wired to a sensor. Sensor settings will be enabled and button settings will be disabled.
Activate Relay On Button Press ?	When selected, the relay will be activated when the Call button is pressed.

Table 2-6. Device Page Parameters (continued)

Web Page Item	Description
Relay On Button Press Duration ?	The length of time (in seconds) during which the relay will be activated when the Call button is pressed. Enter up to 5 digits. A Relay on Button Press Duration value of 0 will pulse the relay once when the Call button is pressed.
Button Lit when Idle ?	When selected, the Call button LED is illuminated while the device is idle (a call is not in progress).
Button Brightness (0-255) ?	The desired Call button LED brightness level. Acceptable values are 0-255, where 0 is the dimmest and 255 is the brightest. Enter up to 3 digits.
Play Ringback Tone ?	When selected, the device will play a ringback tone (corresponds to Ringback Tone on the Audiofiles page) out of the speaker while placing an outbound call. The Ringback Tone will play until the call is answered.
Enable Push to Talk ?	This option is for noisy environments. When enabled, the microphone will be muted normally. When the Call button is pressed and held, it will unmute the microphone and allow the operator to send audio back. Using Push to Talk prevents the operator from terminating a call by pressing the Call button. The call must be terminated by the phone user.
Prevent Call Termination ?	When this option is enabled, a call cannot be terminated using the call button.
Blink Button LED on monitor call ?	Selecting this will cause the button LED blink during a monitor call. Unselecting this will cause the speaker to give no indication that it is in a monitor call.
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).
Auxiliary Power Supply ?	This device can be connected to a +24VDC auxiliary power supply. Check this box if this is how this speaker is being powered.
Relay Settings	
Activate Relay with DTMF Code ?	Activates the relay when the DTMF Activation Code is entered on the phone during a SIP call with the device. RFC2833 DTMF payload types are supported.
Relay Pulse Code ?	DTMF code used to pulse the relay when entered on a phone during a SIP call with the device. Relay will activate for Relay Pulse Duration seconds then deactivate. Activate Relay with DTMF Code must be enabled. Enter up to 25 digits (* and # are supported).
Relay Pulse Duration (in seconds) ?	The length of time (in seconds) during which the relay will be activated when the DTMF Relay Activation Code is detected. Enter up to 5 digits.
Relay Activation Code ?	Activation code used to activate the relay when entered on a phone during a SIP call with the device. Relay will be active indefinitely, or until the DTMF Relay Deactivation code is entered. Activate Relay with DTMF Code must be enabled. Enter up to 25 digits (* and # are supported).

Table 2-6. Device Page Parameters (continued)

Web Page Item	Description
Relay Deactivation Code 	Code used to deactivate the relay when entered on a phone during a SIP call with the device. Activate Relay with DTMF Code must be enabled. Enter up to 25 digits (* and # are supported).
Activate Relay During Ring 	When selected, the relay will be activated for as long as the device is ringing. When Auto-Answer Incoming Calls is enabled, the device will not ring and this option does nothing.
Activate Relay During Night Ring 	When selected, the relay will be activated as long as the Nightringer extension is ringing.
Activate Relay While Call Active 	When selected, the relay will be activated as long as the SIP call is active.
Misc Settings	
Device Name 	Type the device name. Enter up to 25 characters.
Auto-Answer Incoming Calls 	When selected, the device will automatically answer incoming calls. When Auto-Answer Incoming Calls is disabled, the device will play a ring tone (corresponds to Ring Tone on the Audiofiles page) out of the speaker until someone presses the Call button to answer the call or the caller disconnects before the call can be answered.
Beep on Init 	Device will play the user-defined “pagetone” audio file when it boots.
Beep on Page 	Device will play the user defined “pagetone” audio file before playing a SIP page.
Disable HTTPS (NOT recommended) 	Disables the encrypted connection to the webpage. We do not recommend disabling HTTPS for security reasons.
Dual Speakers 	Select this option if two speakers (main and auxiliary) are connected to the board.
RGB Strobe 	Status of optional RGB Strobe.
	Click on the Test Relay button to do a relay test.
	Click the Save button to save your configuration settings. Note: You need to reboot for changes to take effect.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark () appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

2.3.5.1 Time Zone Strings

The posix time zone string tells the internal date and time utilities how to handle daylight savings time for different time zones. [Table 2-21](#) shows some common strings.

Table 2-7. Common Time Zone Strings

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

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

[Table 2-22](#) shows a breakdown of the parts that constitute the following time zone string:

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

Table 2-8. Time Zone String Parts

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

Time Zone String Examples [Table 2-23](#) has some more examples of time zone strings.

Table 2-9. Time Zone String Examples

Time Zone	Time Zone String
Tokyo ^a	IST-9
Berlin ^b	CET-1MET,M3.5.0/1:00,M10.5.0/1:00

a. Tokyo does not use daylight savings time.

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

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

Figure 2-19. Three or Four Character Time Zone Identifier

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

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

World GMT Table [Table 2-24](#) has information about the GMT time in various time zones.

Table 2-10. World GMT Table

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

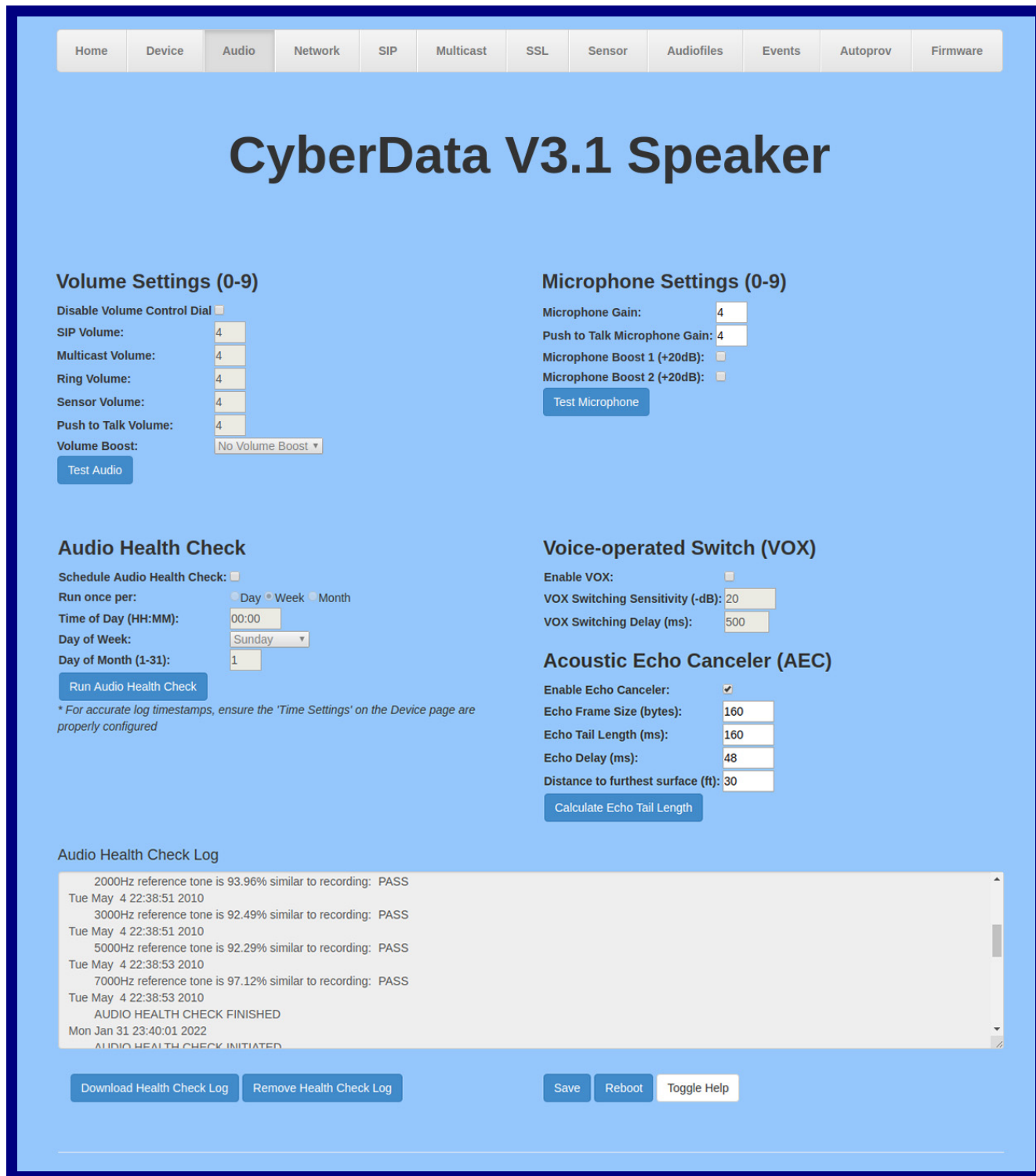
Table 2-10. World GMT Table (continued)

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

2.3.6 Configure the Audio

1. Click the **Audio** menu button to open the **Audio** page. See [Figure 2-17](#).

Figure 2-20. Audio Page



2. On the **Device** page, you may enter values for the parameters indicated 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 2-11. Audio Page Parameters



Web Page Item	Description
Volume Settings (0-9)	
Disable Volume Control Dial ?	Select this option to disable the volume control dial and enable digital volume control settings.
SIP Volume ?	Set the speaker volume for a SIP call. A value of 0 will mute the speaker during SIP calls.
Multicast Volume ?	Set the speaker volume for multicast audio streams. A value of 0 will mute the speaker during multicasts.
Ring Volume ?	Set the ring volume for incoming calls. A value of 0 will mute the speaker instead of playing the ring tone when Auto-Answer Incoming Calls is disabled.
Sensor Volume ?	Set the speaker volume for playing sensor activated audio. A value of 0 will mute the speaker during sensor activated audio.
Push To Talk Volume ?	Set the speaker volume for Push to Talk operation. A value of 0 will mute the speaker in Push to Talk mode.
Volume Boost: ? No Volume Boost +4dB	Set the Boost level to increase the volume output of the speaker. Using Volume Boost may introduce audio clipping and/or distortion. Boost is only recommended for use with volumes set to level 9.
	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 ?	Configure the audio health check to run automatically at a specified periodic interval. See options below. Note: make sure the 'Time Settings' on the Device page are configured properly.
Run once per Day/Week/Month ?	Specify frequency at which scheduled audio health check will run. Only one may be selected.
Time of Day ?	Input the time of day the scheduled audio health check will run. Time must be input in 24 hour format (e.g. 11:45pm will be input as 23:45). This setting applies to all three options above.
Day of Week ?	Select the day of the week the scheduled audio health check will run. This setting only applies when configured to run once per week.
Day of Month (1-31) ?	Input the day of the month the scheduled audio health check will run. This setting only applies when configured to run once per month. If the day input exceeds the last day of a given month, then the last day of that month will be used (e.g. inputting 31 will schedule the health check to run on the last day of every month, even if the month does not have 31 days).
	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 webpage. Note: For accurate log timestamps, ensure the Time Settings on the Device page are properly configured.

Table 2-11. Audio Page Parameters (continued)

















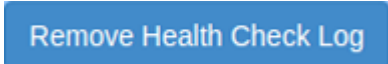


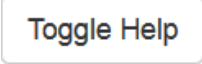
Web Page Item	Description
Microphone Settings	These settings will only appear if you are using the Talk-Back Speaker. If you are not using the Talk-Back Speaker, you will see the words NOT INSTALLED.
Microphone 	Displays the status of optional microphone.
Microphone Gain 	Set the microphone gain level.
Push to Talk Microphone Gain 	Set the microphone gain level for Push to Talk operation.
Microphone Boost 1 (+20dB) 	Enables one of two +20dB gain boosts on the microphone when checked.
Microphone Boost 2 (+20dB) 	Enables one of two +20dB gain boosts on the microphone when checked.
	Click on the Test Microphone button to do a microphone test. When the Test Microphone button is pressed, the following occurs: <ol style="list-style-type: none"> 1. The device will immediately start recording 3 seconds of audio. 2. The device will beep (indicating the end of recording). 3. The device will play back the recorded audio.
Voice-operated Switch (VOX)	
Enable VOX 	Enable voice activation switching (VOX) mode. This will allow the device to operate with adaptive half-duplex audio. If the signal playing out of the speaker is above a specified level, the microphone will be muted. This mode can be desirable if the echo experienced in full-duplex operation cannot be adequately canceled.
VOX Switching Sensitivity 	Sensitivity for whether the far-end (remote) signal is considered strong enough to mute the microphone. This setting may need to be adjusted to account for the strength of a given remote signal. The higher the value, the more sensitive the switching will be. A value of '0' is considered the least sensitive; the microphone will likely never be muted at this level.
VOX Switching Delay (ms) 	Delay (in milliseconds) after the threshold has been exceeded before the remote signal level will be measured again.
Acoustic Echo Canceler (AEC)	
Enable Echo Canceler 	Enable echo cancellation mode. This will allow the device to operate with full-duplex audio. If the echo heard on the far (remote) cannot be canceled adequately, VOX mode is recommended.
Echo Frame Size 	The size of an individual RTP packet for the codec being used. This value should be 160 for G.711 and G.722, and 20 for G.729.
Echo Tail Length (ms) 	Length of time over which the echo canceler will remove the echo from the near end audio signal. This value is directly related to the room dimensions and the materials making up the reflective surfaces in the room. The larger and more reflective the room is, the longer the tail length will need to be; however, the tail length should be kept as short as possible to ensure the fastest adaptation time of the echo canceler.
Echo Delay 	Time interval between the played and recorded audio signal input to the echo canceler. This value should be kept minimal, approximately 0.3 times the echo tail length, or less.
Distance to furthest surface (ft) 	Enter the distance from the speaker to the furthest reflective surface. This value can be used to calculate an approximate echo tail length for the echo canceler. Additional adjustments to the echo tail length may be needed, depending on the reflective characteristics of the room surfaces.

Table 2-11. Audio Page Parameters (continued)

Web Page Item	Description
	Calculate the approximate echo tail length from distance to the furthest reflective surface. The echo tail length may need to be adjusted further after the calculation, depending on the reflective characteristics of the room. The more reflective the surfaces of the room, the longer the tail length will need to be.
Audio Health Check Log	Logs the time and results of the audio health check.
	Downloads the health check log.
	Removes the health check log.
	Click the Save button to save your configuration settings. Note: You need to reboot for changes to take effect.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

2.3.7 Configure the Network Parameters

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

Figure 2-21. Network Page

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

CyberData V3.1 Speaker

Stored Network Settings

Addressing Mode: Static DHCP

Hostname:

IP Address:

Subnet Mask:

Default Gateway:

DNS Server 1:

DNS Server 2:

DHCP Timeout in seconds*:

* A value of -1 will retry forever

VLAN Settings

VLAN ID (0-4095):

VLAN Priority (0-7):

Save Reboot Toggle Help

Current Network Settings

IP Address: 10.10.1.204
Subnet Mask: 255.0.0.0
Default Gateway: 10.0.0.1
DNS Server 1: 10.0.1.56
DNS Server 2:

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

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

Table 2-12. Network Page Parameters



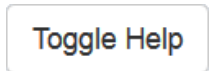
Web Page Item	Description
Stored Network Settings	
Addressing Mode ?	Select either DHCP IP Addressing or Static Addressing by marking the appropriate radio button. DHCP Addressing mode is enabled on default and the device will attempt to resolve network addressing with the local DHCP server upon boot. If DHCP Addressing fails, the device will revert to the last known IP address or the factory default address if no prior DHCP lease was established. See Section 2.3.1, "Factory Default Settings" for factory default settings. Be sure to click Save and Reboot to store changes when configuring a Static address.
Hostname ?	This is the hostname provided by the DHCP server. See the DHCP/DNS server documentation for more information. Enter up to 64 characters.
IP Address ?	Enter the Static IPv4 network address in dotted decimal notation.
Subnet Mask ?	Enter the Subnet Mask in dotted decimal notation.
Default Gateway ?	Enter the Default Gateway IPv4 address in dotted decimal notation.
DNS Server 1 ?	Enter the primary DNS Server IPv4 address in dotted decimal notation.
DNS Server 2 ?	Enter the secondary DNS Server IPv4 address in dotted decimal notation.
DHCP Timeout in seconds ?	Specify the desired time-out duration (in seconds) that the device will wait for a response from the DHCP server before reverting back to the stored static IP address. The stored static IP address may be the last known IP address or the factory default address if no prior DHCP lease was established. Enter up to 8 characters. A value of -1 will retry forever.
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.
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.
	Click the Save button to save your configuration settings. Note: You need to reboot for changes to take effect.
	Click on the Reboot button to reboot the system.

Table 2-12. Network Page Parameters (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.

2.3.8 Configure the SIP (Session Initiation Protocol) Parameters

1. Click on the **SIP** menu button to open the **SIP** page (Figure 2-22).

Figure 2-22. SIP Page—Top

The screenshot shows the 'SIP Page—Top' configuration interface for the CyberData SIP Speaker. The page has a navigation bar at the top with tabs for Home, Device, Audio, Network, SIP (selected), Multicast, SSL, Sensor, Audiofiles, Events, Autoprov, and Firmware. The main heading is 'CyberData SIP Speaker'.

SIP Settings

- Enable SIP operation:
- SIP Transport Protocol: UDP
- TLS Version: 1.2 only (recommended)
- Verify Server Certificate:
- Register with a SIP Server:
- Use Cisco SRST:
- Primary SIP Server: 10.0.0.253
- Primary SIP User ID: 199
- Primary SIP Auth ID: 199
- Primary SIP Auth Password: *****
- Backup SIP Server 1: [Empty]
- Backup SIP User ID 1: [Empty]
- Backup SIP Auth ID 1: [Empty]
- Backup SIP Auth Password 1: [Empty]
- Backup SIP Server 2: [Empty]
- Backup SIP User ID 2: [Empty]
- Backup SIP Auth ID 2: [Empty]
- Backup SIP Auth Password 2: [Empty]
- Remote SIP Port: 5060
- Local SIP Port: 5060
- Outbound Proxy: [Empty]
- Outbound Proxy Port: 0
- Monitor User ID: [Empty]
- Monitor Authenticate ID: [Empty]

Nightringer Settings

- Enable Nightringer:
- SIP Server: 10.0.0.253
- Remote SIP Port: 5060
- Local SIP Port: 5061
- Outbound Proxy: [Empty]
- Outbound Proxy Port: 0
- User ID: 241
- Authenticate ID: 241
- Authenticate Password: *****
- Re-registration Interval (in seconds): 360

Nightringer Strobe Settings

- Blink Strobe on Nightring:
- Scene: ADA
- Color: White
- Brightness: 100
- Red: 0
- Green: 0
- Blue: 0
- Preview button

RTP Settings

- RTP Port (even): 10500
- Jitter Buffer: 50
- SRTP: Disabled

Call Disconnection

- Terminate Call after delay: 0

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

Figure 2-23. SIP Page—Bottom

Monitor User ID:

Monitor Authenticate ID:

Monitor Authenticate Password:

Disable rport Discovery:

Buffer SIP Calls:

Re-registration Interval (in seconds):

Unregister on Boot:

Keep Alive Period:

Terminate Call after delay:

Codec Selection

Force Selected Codec:

Codec:

Button Settings

Dial Out Extension:

Extension ID:

SIP Ring Strobe Settings

Blink Strobe on Ring:

Scene	Color	Brightness	Red	Green	Blue	
ADA	White	100	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="button" value="Preview"/>

SIP Call Strobe Settings

Blink Strobe during Call:

Scene	Color	Brightness	Red	Green	Blue	
ADA	White	100	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="button" value="Preview"/>

MWI Strobe Settings

Blink Strobe on MWI:

Scene	Color	Brightness	Red	Green	Blue	
ADA	White	100	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="button" value="Preview"/>

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

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

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

Table 2-13. SIP Page Parameters

Web Page Item	Description
SIP Settings	
Enable SIP Operation ?	When enabled, the device will transmit, receive, and process SIP messages according to the configured SIP settings below.
SIP Transport Protocol ?	Choose the transport protocol for SIP signaling. This will affect all extensions, including the Nightringer. Default is UDP.
TLS Version ?	Choose the TLS version for SIP over TLS. Modern security standards strongly recommend using TLS 1.2.
Verify Server Certificate ?	When enabled, the device will verify the authenticity of the server during the TLS handshake by its certificate and common name. The TLS handshake will be aborted if the server is deemed to be inauthentic and SIP registration will not proceed.
Register with a SIP Server ?	When enabled, the device will attempt to register to the configured SIP Server(s) on this page. To configure the device to send and receive point-to-point SIP calls, enable SIP Operation and disable Register with a SIP Server (see Section 2.3.8.2, "Point-to-Point Configuration").
Use Cisco SRST ?	When enabled, the backup servers are handled according to Cisco SRST (Survivable Remote Site Telephony). It is required for use in clustered Cisco Unified Communications Manager topologies.
Primary SIP Server ?	Enter the SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the primary SIP server. This field can accept entries of up to 255 characters in length.
Primary SIP User ID ?	Specify the SIP User ID for the Primary SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the primary SIP server. Enter up to 64 alphanumeric characters.
Primary SIP Auth ID ?	Specify the Authenticate ID for the Primary SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Primary SIP Auth Password ?	Specify the Authenticate Password for the Primary SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Server 1 ?	Enter the backup SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the backup SIP server. This field can accept entries of up to 255 characters in length.
Backup SIP User ID 1 ?	Specify the SIP User ID for the first backup SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the first backup SIP server. Enter up to 64 alphanumeric characters.
Backup SIP Auth ID 1 ?	Specify the Authenticate ID for the first backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Auth Password 1 ?	Specify the Authenticate Password for the first backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.

Table 2-13. SIP Page Parameters (continued)

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

Table 2-13. SIP Page Parameters (continued)


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

Table 2-13. SIP Page Parameters (continued)



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

Table 2-13. SIP Page Parameters (continued)

































Web Page Item	Description
Local SIP Port 	The Local SIP Port is the port number the device will use to receive SIP messages for the Nightringer extension. This value cannot be the same as the Local SIP Port for the primary extension. The default Local SIP Port is 5061. The supported range is 0-65536. Enter up to 5 digits.
Outbound Proxy 	Enter the Outbound Proxy address as an IPv4 address in dotted decimal notation or a fully qualified domain name (FQDN). When an IP address is configured, the device will send all SIP messages to this IP address for the Nightringer extension. When an FQDN is configured, the device will run DNS NAPTR, SRV, and A queries on the FQDN to resolve an IP address to which it will send all SIP messages for the Nightringer extension. This field can accept entries of up to 255 characters in length.
Outbound Proxy Port 	The Outbound Proxy Port is port number used as the destination port when sending SIP messages to the outbound proxy for the Nightringer extension. A value of 0 will default to 5060. The supported range is 0-65536. Enter up to 5 digits.
User ID 	Specify the SIP User ID for the SIP server. This parameter becomes the user portion of the SIP-URI for the device's Nightringer extension. Enter up to 64 alphanumeric characters.
Authenticate ID 	Specify the Authenticate ID for the SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Authenticate Password 	Specify the Authenticate Password for the SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Re-registration Interval (in seconds) 	The SIP Re-registration Interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
Nightringer Strobe Settings	The following strobe settings will only appear if you are using the Strobe Kit. If you are not using the Strobe Kit, you will not see the strobe settings.
Blink Strobe on Nightring 	When selected, the Strobe will blink a scene when the Nightringer is ringing.
Scene 	Select desired scene (only one may be chosen).
ADA Compliant 	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.
Slow Fade 	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade 	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink 	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.
Fast Blink 	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.
Color 	Select desired color (only one may be chosen).
Brightness 	How bright the strobe will blink when the Nightringer is ringing. This is the maximum brightness for "fade" type scenes.
Red 	The red LED value for Nightringer.
Green 	The green LED value for Nightringer.
Blue 	The blue LED value for Nightringer.
	Use this button to preview the strobe flashing behavior for the Nightringer Strobe Settings .

Table 2-13. SIP Page Parameters (continued)

Web Page Item	Description
RTP Settings	
RTP Port (even) 	Specify the port number used for the RTP stream after establishing a SIP call. This port number must be an even number and defaults to 10500. The supported range is 0-65536. Enter up to 5 digits.
Jitter Buffer 	Specify the size of the jitter buffer (in milliseconds) used for SIP calls. Valid values are 50-1000.
RTP Encryption (SRTP) 	When enabled, a SIP call's audio streams are encrypted using SRTP.
Call Disconnection	
Terminate Call After Delay 	Automatically terminate an active call after a given delay in seconds. A value of 0 will disable this function. Enter up to 8 digits.
Codec Selection	
Force Selected Codec 	When configured, this option will allow you to force the device to negotiate for the selected codec. Otherwise, the device will perform codec negotiation using the default list of supported codecs.
Codec 	Select the desired codec (only one may be chosen).
Button Settings	
Dial Out Extension 	Specify the extension the device will call when someone presses the Call button. Enter up to 64 alphanumeric characters. Note: For information about dial-out extension strings and DTMF tones, see Section 2.3.8.1, "Dial Out Extension Strings and DTMF Tones (using rfc2833)" .
Extension ID 	A Caller identification string added to outbound calls. Enter up to 64 alphanumeric characters.
	Click the Save button to save your configuration settings. Note: You need to reboot for changes to take effect.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark () appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

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

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

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

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

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

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

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

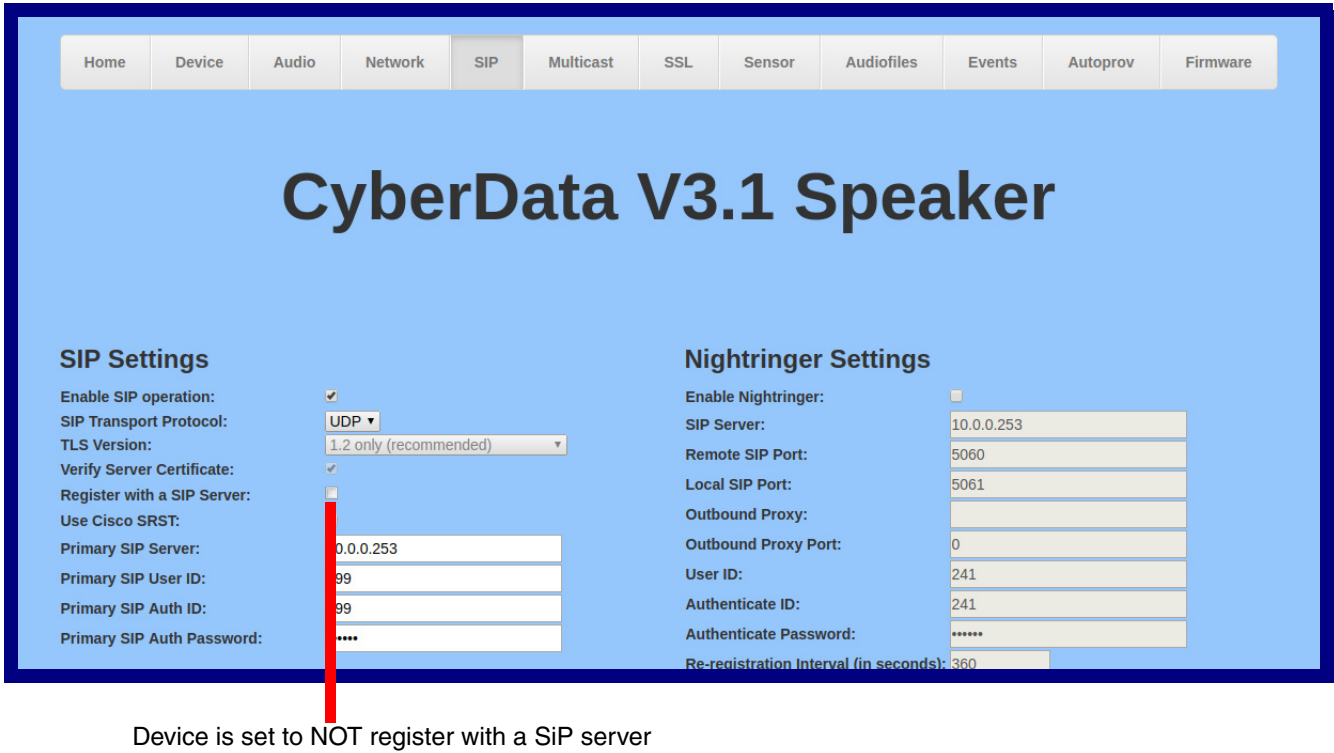
2.3.8.2 Point-to-Point Configuration

When the device is set to not register with a SIP server (see [Figure 2-24](#)), it is possible to set the device to dial out to a single endpoint.

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

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

Figure 2-24. SIP Page Set to Point-to-Point Mode



2.3.8.3 Delayed DTMF

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

Table 2-15. Examples of Dial-Out Extension Strings

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

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

2.3.9 Configure the Multicast Parameters

The Multicast Configuration 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 2-25](#).

Figure 2-25. Multicast Page

Multicast Settings
 Enable Multicast Operation:
 Blink Strobe on Multicast:

Priority	Address	Port	Name	Buffer	Beep	Relay	Scene	Color	Brightness	Red	Green	Blue	
9	239.168.3.10	11000	Emergency	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	ADA	White	100	0	0	0	Preview
8	239.168.3.9	10000	MG8	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Fast Blink	Red	100	255	0	0	Preview
7	239.168.3.8	9000	MG7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Slow Fade	Blue	100	0	0	255	Preview
6	239.168.3.7	8000	MG6	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Slow Blink	Cyan	100	0	255	255	Preview
5	239.168.3.6	7000	MG5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Fast Blink	Violet	80	255	0	255	Preview
4	239.168.3.5	6000	MG4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Fast Fade	Green	75	0	255	0	Preview
3	239.168.3.4	5000	MG3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Off	White	100	0	255	255	Preview
2	239.168.3.3	4000	MG2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Slow Fade	Violet	100	255	0	255	Preview
1	239.168.3.2	3000	MG1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Slow Blink	Yellow	66	255	255	0	Preview
0	239.168.3.1	2000	Background Music	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Fast Blink	Custom	40	120	40	80	Preview

Polycorn Default Channel: 1
 Polycorn Priority Channel: 24
 Polycorn Emergency Channel: 25

SIP calls are considered priority 4.5
 Port range can be from 2000-65535
 Priority 9 is the highest and 0 is the lowest
 A higher priority audio stream will always supersede a lower one
 * You need to reboot for changes to take effect

Save Reboot

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




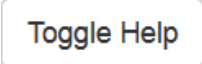
- On the **Multicast** page, enter values for the parameters indicated in [Table 2-16](#).

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

Table 2-16. Multicast Page Parameters

Web Page Item	Description
Enable Multicast Operation	Enables or disables multicast operation.
Blink Strobe on Multicast ?	When selected, the Strobe will blink a scene when a multicast is received. Note: The strobe settings will only appear if you are using the Strobe Kit. If you are not using the Strobe Kit, you will not see the strobe settings.
Priority	Indicates the priority for the multicast group. Priority 9 is the highest (emergency streams). 0 is the lowest (background music). SIP calls are considered priority 4.5 . See Section 2.3.9.1, "Assigning Priority" for more details.
Address	Enter the multicast IP Address for this multicast group (15 character limit).
Port	Enter the port number for this multicast group (5 character limit [range can be from 2000 to 65535]). Note: The multicast ports have to be even values. The webpage will enforce this restriction.
Name	Assign a descriptive name for this multicast group (25 character limit).
Buffer	Device will buffer up to four minutes of audio and then play back the recording after the multicast stream finishes or after the buffer is full.
Beep	When selected, the device will play a beep before multicast audio is sent.
Relay	When selected, the device will activate a relay before multicast audio is sent.
Scene ?	Select desired scene (only one may be chosen). Note: The strobe settings will only appear if you are using the Strobe Kit. If you are not using the Strobe Kit, you will not see the strobe settings.
ADA Compliant ?	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.
Slow Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.
Fast Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink ?	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.
Fast Blink ?	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.
Color ?	Select desired color (only one may be chosen).
Brightness ?	How bright the strobe will blink on a multicast page. This is the maximum brightness for "fade" type scenes.
Red ?	The red LED value for Multicast.
Green ?	The green LED value for Multicast.
Blue ?	The blue LED value for Multicast.

Table 2-16. Multicast Page Parameters (continued)

Web Page Item	Description
Polycom Default Channel	When a default Polycom channel/group number is selected, the device will subscribe to the default channel for one-way group pages. Group Numbers 1-25 are supported. Or, select Disabled to disable this channel.
Polycom Priority Channel	When a priority Polycom channel/group number is selected, the device will subscribe to the priority channel for one-way group pages. Group Numbers 1-25 are supported. Or, select Disabled to disable this channel.
Polycom Emergency Channel	When an emergency Polycom channel/group number is selected, the device will subscribe to the default channel for one-way group pages. Group Numbers 1-25 are supported. Or, select Disabled to disable this channel.
	Use this button to preview the strobe flashing behavior for the Multicast Strobe Settings .
	Click the Save button to save your configuration settings. Note: You need to reboot for changes to take effect.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

2.3.9.1 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.

2.3.10 Configure the SSL Parameters

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

Figure 2-26. SSL Configuration Page

The screenshot shows the 'SSL Configuration Page' for a 'CyberData V3.1 Speaker'. The page has a light blue background and a navigation bar at the top with buttons for Home, Device, Audio, Network, SIP, Multicast, SSL (selected), Sensor, Audiofiles, Events, Autoprov, and Firmware.

Server CAs

- Browse... No file chosen
- Import CA Certificate
- Restore Defaults
- Remove All
- Apply/Reboot
- Toggle Help

Client Certificate

```
commonName = CyberData SIP Device
validFrom = Jul 10 17:56:03 2018 GMT
validTo = Jul 7 17:56:03 2028 GMT
```

Client CA

Test SSL Connection

Server: 10.0.0.253
Port: 5060
Test TLS connection

List of Trusted CAs

1	DST_ACES_CA_X6.crt	Info	Remove
2	DST_Root_CA_X3.crt	Info	Remove
3	Deutsche_Telekom_Root_CA_2.crt	Info	Remove
4	DigiCert_Assured_ID_Root_CA.crt	Info	Remove
5	DigiCert_Assured_ID_Root_G2.crt	Info	Remove
6	DigiCert_Assured_ID_Root_G3.crt	Info	Remove
7	DigiCert_Global_Root_CA.crt	Info	Remove
8	DigiCert_Global_Root_G2.crt	Info	Remove
9	DigiCert_Global_Root_G3.crt	Info	Remove
10	DigiCert_High_Assurance_EV_Root_CA.crt	Info	Remove
11	DigiCert_Trusted_Root_G4.crt	Info	Remove
12	Equifax_Secure_CA.crt	Info	Remove
13	Equifax_Secure_Global_eBusiness_CA.crt	Info	Remove
14	Equifax_Secure_eBusiness_CA_1.crt	Info	Remove

Figure 2-27. SSL Configuration Page

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

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

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

Table 2-17. SSL Configuration Parameters

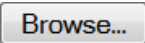

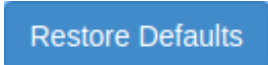






Web Page Item	Description
Server CAs	
	Use this button to select a configuration file to import.
	Click Browse to select a CA certificate to import. After selecting a server certificate authority (CA), click Import CA Certificate to import it to the list of trusted CAs. CAs are used to validate the certificate 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.
	Reboots the device and applies settings and activates imported certificates.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.
Client Certificate	
Client CA ?	Right click and Save Link As... to get the Cyberdata CA used to sign this client certificate.
Test SSL Connection	
Server ?	The ssl test server address as a fully qualified domain name or in IPv4 dotted decimal notation.
Port ?	The ssl test server port. The supported range is 0-65536. SIP connections over TLS to port 5060 will do the same.
	Use this button to test a TLS connection to a remote server. This will attempt to make a socket connection to the configured test server and port and report the success or failure. This can be used to debug TLS connection issues separate from SIP registration issues.
List of Trusted CAs	
	Provides details of the certificate. After clicking on this button, the Certificate Info Window appears. See Section 2.3.10.1, "Certificate Info Window" .

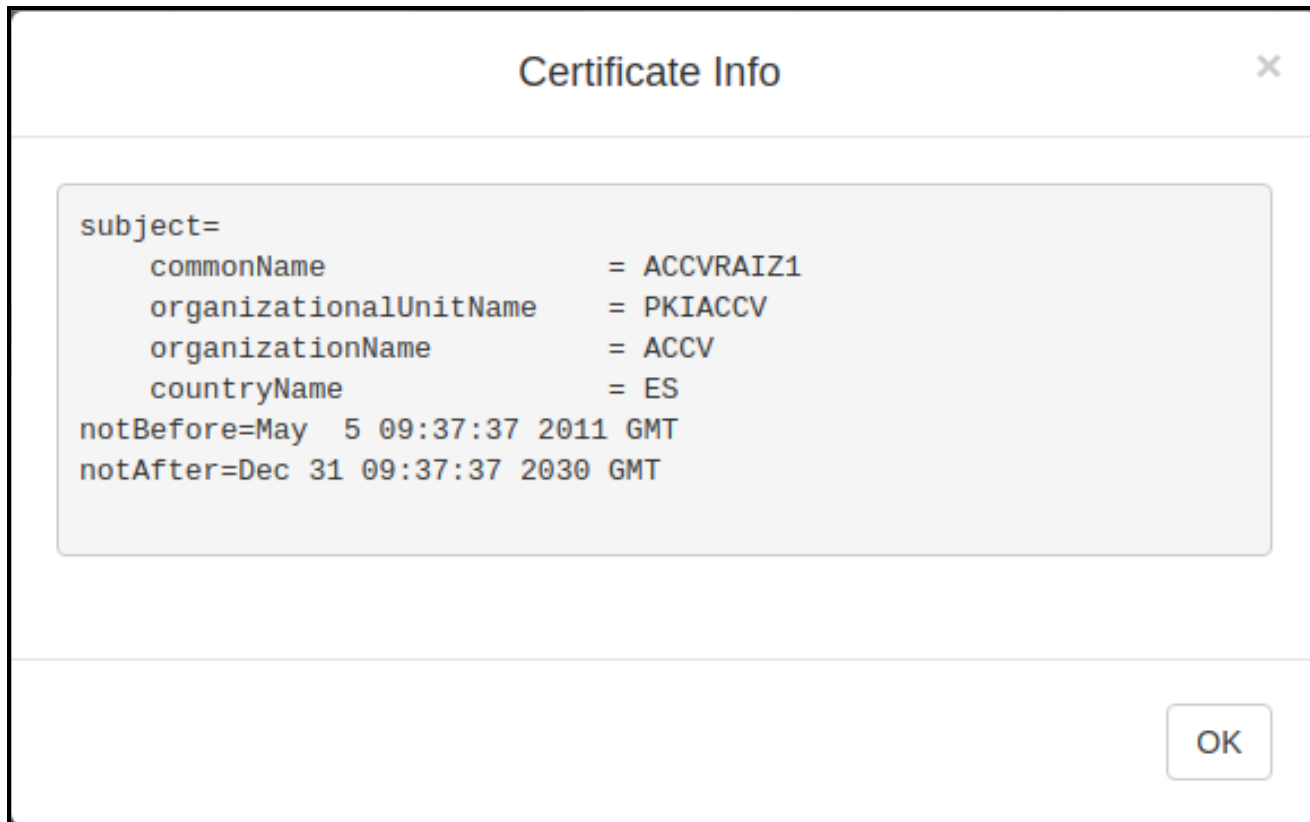
Table 2-17. SSL Configuration Parameters (continued)

Web Page Item	Description
	Removes this certificate from the list of trusted certificates. After clicking on this button, the Remove Server Certificate Window appears. See Section 2.3.10.2, "Remove Server Certificate Window" .

2.3.10.1 Certificate Info Window

The **Certificate Info Window** provides details of the certificate. This window appears after clicking on the **Info** button. See [Figure 2-28](#).

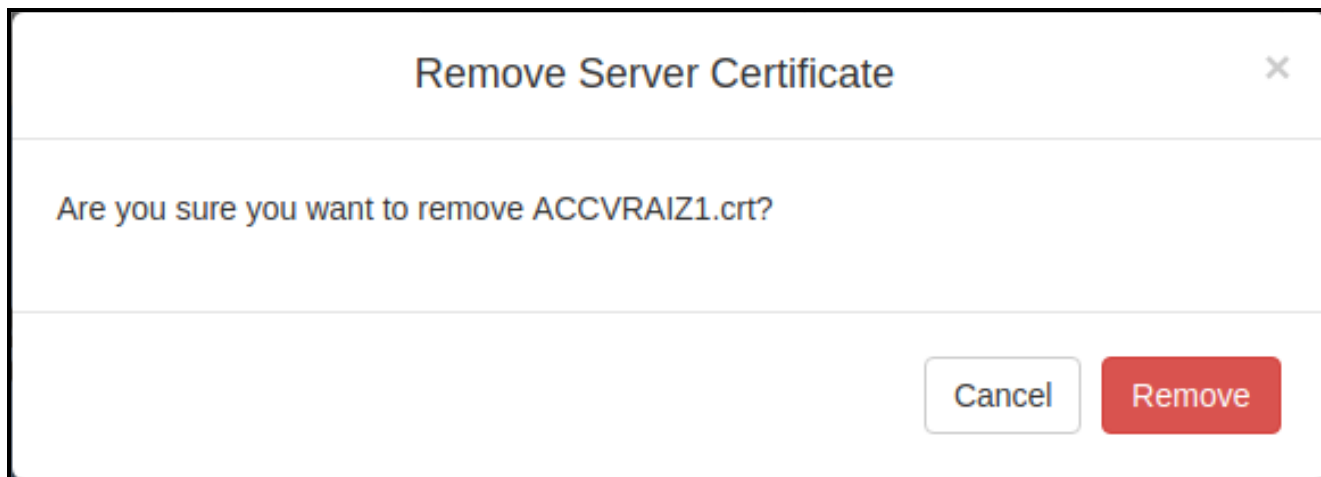
Figure 2-28. Certificate Info Window



2.3.10.2 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 2-29](#).

Figure 2-29. Remove Server Certificate Window



2.3.11 Configure the Sensor Configuration Parameters

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

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

Each sensor can trigger up to five different actions:

- Flash the LED until the sensor is deactivated (roughly 10 times/second)
- Activate the relay until the sensor is deactivated
- Loop an audio file out of the speaker until the sensor is deactivated
- Call an extension and establish two way audio
- Call an extension and play a pre-recorded audio file

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

1. Click **Sensor** menu button to open the **Sensor** page ([Figure 2-30](#)).

Figure 2-30. Sensor Page

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

CyberData V3.1 Speaker

Sensor Settings

Sensor Normally Closed: Yes No

Sensor Timeout (in seconds):

Activate Relay:

Play Audio Locally:

Make call to extension:

Dial Out Extension:

Dial Out ID:

Play recorded audio:

Repeat Sensor Message:

Sensor Strobe Settings

Blink Strobe on Sensor:

Scene	Color	Brightness	Red	Green	Blue
ADA	White	100	0	0	0

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

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

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

Table 2-18. Sensor Page Parameters















Web Page Item	Description
Sensor Settings	
Sensor Normally Closed ?	Select the inactive state of the sensor. The sensor is also known as the Sense Input on the device's terminal block. See the Operations Guide for more information.
Sensor Timeout (in seconds) ?	The time (in seconds) the device will wait before it performs an action when the on-board door sensor is activated. The action(s) performed are based on the configured Sensor Settings below. Enter up to 5 digits.
Activate Relay ?	When selected, the device's on-board relay will be activated until the on-board door sensor is deactivated.
Play Audio Locally ?	When selected, the device will loop an audio file out of the speaker until the door sensor is deactivated.
Make call to extension ?	When selected, the device will call an extension when the on-board door sensor is activated. Use the Dial Out Extension field below to specify the extension the device will call.
Dial Out Extension ?	Specify the extension the device will call when the on-board door sensor is activated. Enter up to 64 alphanumeric characters.
Dial Out ID ?	An additional Caller identification string added to outbound calls. Enter up to 64 alphanumeric characters.
Play recorded audio ?	When selected, the device will call the Dial Out Extension and play an audio file to the phone answering the SIP call (corresponds to Door Ajar on the Audiofiles page).
Repeat Sensor Message ?	The number of times to repeat the audio message through the local speaker or to the remote endpoint. A value of 0 will repeat forever. Enter a value from 0-65536.
	Click the Test Sensor button to test the sensor.
Sensor Strobe Settings	
The following strobe settings will only appear if you are using the Strobe Kit. If you are not using the Strobe Kit, you will not see the strobe settings.	
Blink Strobe on Sensor ?	When selected, the Strobe will blink a scene when the sensor is triggered.
Scene ?	Select desired scene (only one may be chosen).
ADA Compliant ?	Strobe will blink ON at the specified brightness for 150ms then OFF for 350ms during the duration of the event.
Slow Fade ?	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 3.5 seconds during the duration of the event.

Table 2-18. Sensor Page Parameters (continued)

Web Page Item	Description
Fast Fade 	Strobe will increase in brightness from 0 to the specified brightness and back to 0 over the course of about 1.5 seconds during the duration of the event.
Slow Blink 	Strobe will blink ON at the specified brightness for one second then OFF for one second during the duration of the event.
Fast Blink 	Strobe will blink ON at the specified brightness then OFF five times per second during the duration of the event.
Color 	Select desired color (only one may be chosen).
Brightness 	How bright the strobe will blink when the sensor is triggered. This is the maximum brightness for “fade” type scenes.
Red 	The red LED value for Sensor.
Green 	The green LED value for Sensor.
Blue 	The blue LED value for Sensor.
	Use this button to preview the strobe flashing behavior for the Sensor Strobe Settings .
	Click the Save button to save your configuration settings. Note: You need to reboot for changes to take effect.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark () appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

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

2.3.12 Configure the Audiofiles 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 2-31).

Figure 2-31. Audiofiles Page



Figure 2-32. Audiofiles Page

The screenshot displays the 'Audio Files' configuration page. It features a list of audio files, each with a label, a status, a file selection button, and action buttons. The labels include '0:', '1:', '2:', '3:', '4:', '5:', '6:', '7:', '8:', '9:', 'Dot:', 'Audio Test:', 'Enter Code:', 'Invalid Code:', and 'Page Tone:'. Each entry shows 'Currently set to default' and a 'Browse...' button with the text 'No file chosen'. To the right of each entry are three buttons: 'Play', 'Delete', and 'Save'.

Label	Status	File Selection	Actions
0:	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"/>
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"/>
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"/>
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"/>
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"/>
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"/>
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"/>
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"/>
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"/>
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"/>
Dot:	Currently set to default	<input type="button" value="Browse..."/> No file chosen	<input type="button" value="Play"/> <input type="button" value="Delete"/> <input type="button" value="Save"/>
Audio Test:	Currently set to default	<input type="button" value="Browse..."/> No file chosen	<input type="button" value="Play"/> <input type="button" value="Delete"/> <input type="button" value="Save"/>
Enter Code:	Currently set to default	<input type="button" value="Browse..."/> No file chosen	<input type="button" value="Play"/> <input type="button" value="Delete"/> <input type="button" value="Save"/>
Invalid Code:	Currently set to default	<input type="button" value="Browse..."/> No file chosen	<input type="button" value="Play"/> <input type="button" value="Delete"/> <input type="button" value="Save"/>
Page Tone:	Currently set to default	<input type="button" value="Browse..."/> No file chosen	<input type="button" value="Play"/> <input type="button" value="Delete"/> <input type="button" value="Save"/>

Figure 2-33. 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"/>
Ring Tone:	Currently set to default	<input type="button" value="Browse..."/> No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Sensor Triggered:	Currently set to default	<input type="button" value="Browse..."/> No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Night Ring:	Currently set to default	<input type="button" value="Browse..."/> No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Talk:	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"/>
Listen:	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"/>
Stored Message:	Currently set to default	<input type="button" value="Browse..."/> No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Through:	Currently set to default	<input type="button" value="Browse..."/> No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
To:	Currently set to default	<input type="button" value="Browse..."/> No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>

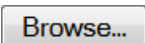



2. On the **Audiofiles** page, enter values for the parameters indicated in [Table 2-19](#).

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

Table 2-19. Audiofiles Page Parameters

Web Page Item	Description
Available Space	Shows the space available for the user to save custom audio files if they want to change the message when the door or sensor is triggered.
Stored Messages	
Stored Message 1 through 9	<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>
Audio Files	
0-4	<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>
5-9	<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>'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>
Dot	Corresponds to the spoken word "dot." (24 character limit)
Audio Test	Corresponds to the message " <i>This is the CyberData IP speaker test message...</i> " (24 character limit)
Enter Code	Corresponds to the message "Enter Code" (24 character limit).
Invalid Code	Corresponds to the message "Invalid Code" (24 character limit).
Page Tone	Corresponds to a simple tone used for beep on initialization and beep on page (24 character limit).
Your IP Address is	Corresponds to the message "Your IP address is.." (24 character limit).
Rebooting	Corresponds to the spoken word "Rebooting" (24 character limit).

Table 2-19. Audiofiles Page Parameters (continued)

Web Page Item	Description
Restoring Default	Corresponds to the message "Restoring default" (24 character limit).
Ring Tone	This is the tone that plays when set to ring when receiving a call (24 character limit).
Sensor Triggered	Corresponds to the message "Sensor Triggered" (24 character limit).
Night Ring	Specifies the ringtone for nightring. By default this parameter uses the same audio file that is selected for the Ring Tone parameter.
Talk	Corresponds to the message "Talk" (24 character limit).
Listen	Corresponds to the message "Listen" (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).
Pound (#)	Corresponds to whatever word or phrase the user wishes to call the pound key in the audio menu played to the caller (24 character limit).
Press	Corresponds to the word "Press" used in the audio menu played to the caller. (24 character limit).
Stored Message	Corresponds to the words "Stored Message" used in the audio menu played to the caller. (24 character limit).
Through	Corresponds to the word "Through" used in the audio menu played to the caller. (24 character limit).
To	Corresponds to the word "To" used in the audio menu played to the caller. (24 character limit).
	Click on the Browse button to navigate to and select an audio file.
	The Play button will play that audio file.
	The Delete button will delete any user uploaded audio and restore the stock audio file.
	The Save button will download a new user audio file to the board once you've selected the file by using the Browse button. The Save button will delete any pre-existing user-uploaded audio files.

2.3.12.1 User-created Audio Files

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

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

You can use the free utility *Audacity* to convert audio files into this format. See [Figure 2-34](#) through [Figure 2-36](#).

Figure 2-34. Audacity 1

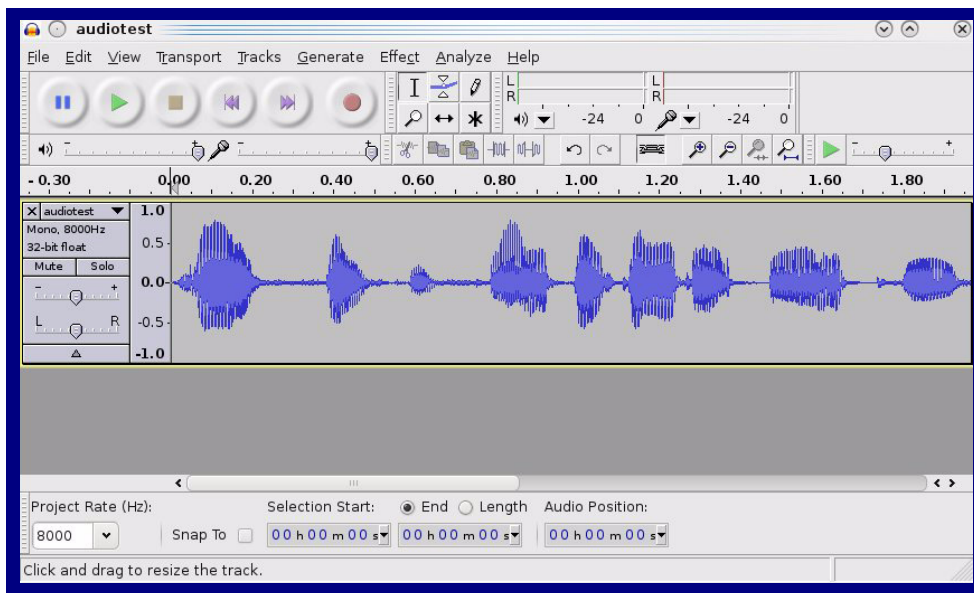
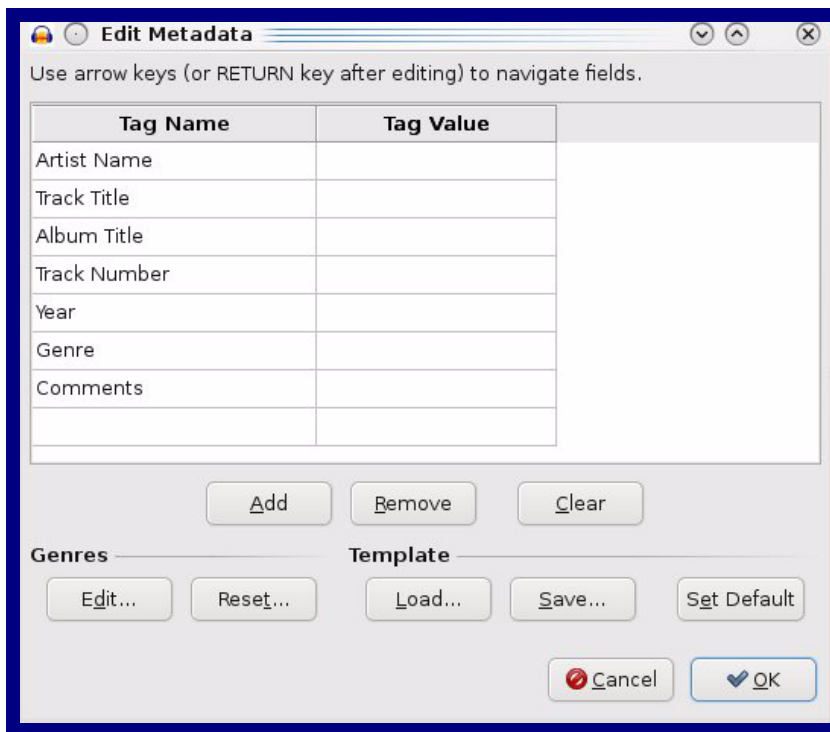


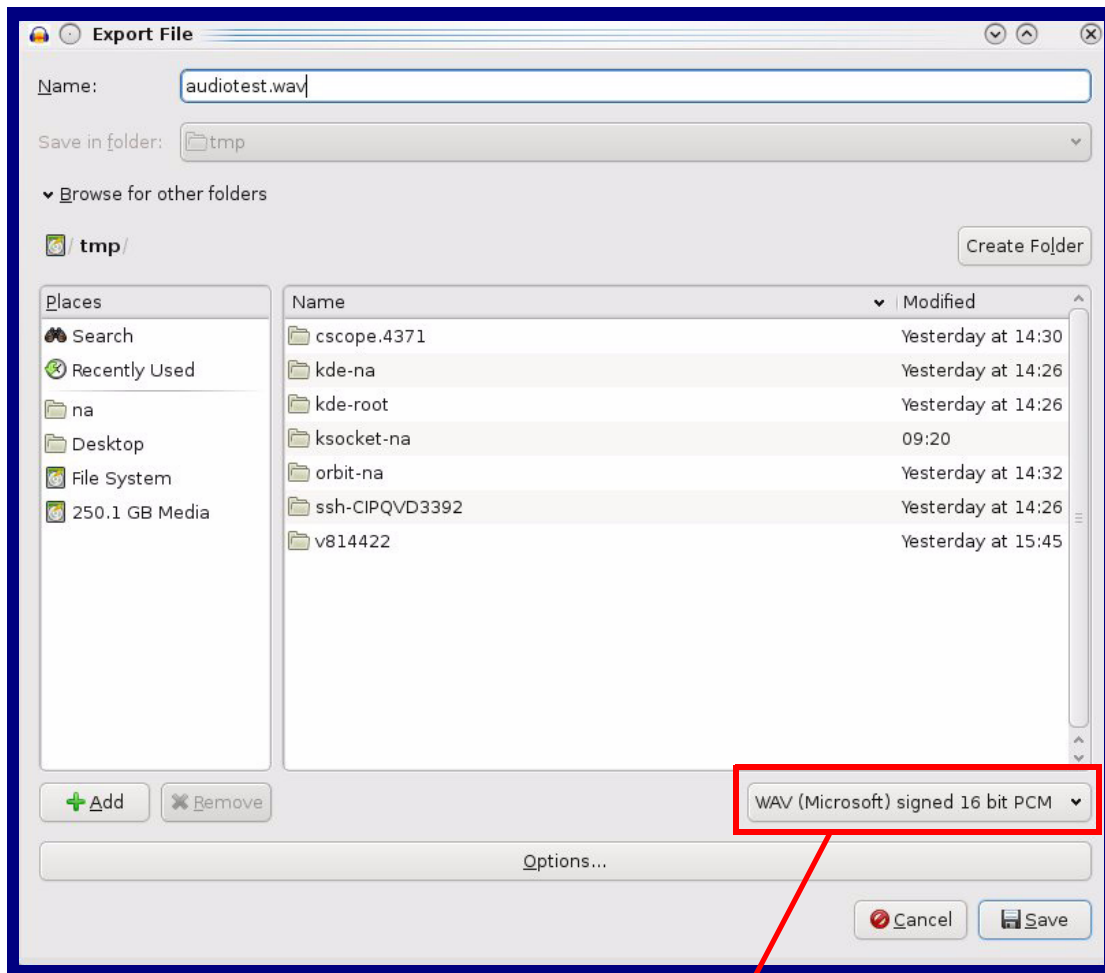
Figure 2-35. Audacity 2



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

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

Figure 2-36. WAV (Microsoft) signed 16 bit PCM



WAV (Microsoft) signed 16 bit PCM

2.3.13 Configure the Events Parameters

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

1. Click on the **Events** menu button to open the **Events** page (Figure 2-37).

Figure 2-37. Event Configuration Page

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

CyberData V3.1 Speaker

Enable Event Generation:

Events

Enable Call Start Events:

Enable Call Terminated Events:

Enable Relay Activated Events:

Enable Relay Deactivated Events:

Enable Night Ring Events:

Enable Power On Events:

Enable Multicast Start Events:

Enable Multicast Stop Events:

Enable Sensor Events:

Enable 60 Second Heartbeat:

Enable Audio Health Check Events:

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

Event Server

Server IP Address:

Server Port:

Server URL:

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

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

Table 2-20. Events Configuration Parameters



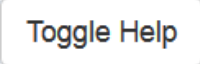
Web Page Item	Description
Enable Event Generation ?	The device will send HTTP POST events to the specified remote server and port number whenever a certain action takes place. Select an event type below to generate an HTTP POST event.
Events	
Enable Button Events ?	When selected, the device will report Call button presses.
Enable Call Start Events ?	When selected, the device will report the start of a SIP call.
Enable Call Terminated Events ?	When selected, the device will report the end of a SIP call.
Enable Relay Activated Events ?	When selected, the device will report relay activation.
Enable Relay Deactivated Events ?	When selected, the device will report relay deactivation.
Enable Night Ring Events ?	When selected, the device will report when it starts ringing upon an incoming SIP call to the Nightringer extension. As a reminder, the Nightringer extension always rings upon an incoming SIP call and it is not possible to alter this behavior.
Enable Power On Events ?	When selected, the device will report when it boots.
Enable Multicast Start Events ?	When selected, the device will report when the device starts playing a multicast audio stream.
Enable Multicast Stop Events ?	When selected, the device will report when the device stops playing a multicast audio stream.
Enable Sensor Events ?	When selected, the device will report when the on-board sensor is activated.
Enable 60 Second Heartbeat Events ?	When enabled, the device will report a Heartbeat event every 60 seconds. SIP registration is not required to generate Heartbeat events.
Enable Audio Health Check Events ?	When selected, the device will report the results of an audio health check.
Check All	Click on Check All to select all of the events on the page.
Uncheck All	Click on Uncheck All to de-select all of the events on the page.
Event Server	
Server IP Address ?	The IPv4 address of the event server in dotted decimal notation.
Server Port ?	Specify the event server port number. The supported range is 0-65536. Enter up to 5 digits.
Server URL ?	Generally, the destination URL is the name of the application that receives the events and the string in the HTTP POST command. It can be a script used to parse and process the HTTP POST events. Enter up to 127 characters.
	Click the Save button to save your configuration settings. Note: You need to reboot for changes to take effect.
	Click on the Reboot button to reboot the system.

Table 2-20. Events Configuration Parameters(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.

2.3.13.1 Example Packets for Events

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

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

Here are example packets for every event:

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

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

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

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

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

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

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

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



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

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

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

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

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

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

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

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

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

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

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

2.3.14 Configure the Autoprovisioning Parameters

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

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

1. Click the **Autoprov** menu button to open the **Autoprovisioning** page. See [Figure 2-38](#).

Figure 2-38. Autoprovisioning Page

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

CyberData V3.1 Speaker

Disable Autoprovisioning:

Autoprovisioning Server:

Autoprovisioning Filename:

Use tftp:

Verify Server Certificate

Username:

Password:

Autoprovisioning autoupdate (in minutes):

Autoprovision at time (HHMMSS):

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 '0020f7041046.xml' and if this fails, '00000cd.xml'.

Save Reboot Toggle Help

Download Template

Autoprovisioning log

```
21:00 Autoprovisioning Device...
21:00 Autoprov found option 43 in DHCP server="https://10.0.0.242:4444"
21:00 Autoprov looking for 0020f7041046.xml at https://10.0.0.242:4444
21:00 Got autoprov file. Parsing "0020f7041046.xml"
21:01 Autoprov found option 72 in DHCP server="10.0.1.118"
21:01 Autoprov looking for 0020f7041046.xml at 10.0.1.118
21:02 Autoprov: didn't find autoprov file
21:02 Autoprov looking for 00000cd.xml at 10.0.1.118
```

2. On the **Autoprovisioning** page, you may enter values for the parameters indicated in [Table 2-21](#).

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

Table 2-21. Autoprovisioning Configuration Parameters





Web Page Item	Description
Disable Autoprovisioning ?	Prevent the device from automatically trying to download a configuration file. See Section 2.3.14.1, "Autoprovisioning" for more information.
Autoprovisioning Server ?	Enter the IPv4 address of the provisioning server in dotted decimal notation.
Autoprovisioning Filename ?	The autoprovisioning filename is the configuration filename. The default autoprovisioning filename is in the format of <mac address>.xml . Supported filename extensions are .txt, and .xml. The current filename is denoted by an asterisk at the bottom of the Autoprovisioning Page . Enter up to 256 characters. A file may have any name with an xml extension. If a file name is entered, the device will look for the specified file name, and only that file.
Use tftp ?	The device will use TFTP (instead of http) to download autoprovisioning files.
Verify Server Certificate ?	When using ssl to download autoprovisioning files, reject connections where the server address doesn't match the server certificate's common name.
Username ?	The username used to authenticate with an autoprovisioning server. Leave this field blank to disable authentication.
Password ?	The password used to authenticate with an autoprovisioning server. Leave this field blank to disable authentication.
Autoprovisioning Autoupdate (in minutes) ?	The reoccurring time (in minutes) the device will wait before checking for new autoprovisioning files. Enter up to 6 digits. A value of 0 will disable this option. Note: To use the auto update options, enable the Set Time with NTP Server on boot setting on the Device Page page (see Table 2-6).
Autoprovision at time (HHMMSS) ?	The time of day the device will check for a new autoprovisioning file. The time must be 6 characters in length and in HHMMSS format. An empty value will disable this option. Note: To use the auto update options, enable the Set Time with NTP Server on boot setting on the Device Page page (see Table 2-6).
Autoprovision when idle (in minutes > 10) ?	The idle time (in minutes greater than 10) after which the device will check for a new autoprovisioning file. Enter up to 6 digits. A value of 0 will disable this option. Note: To use the auto update options, enable the Set Time with NTP Server on boot setting on the Device Page page (see Table 2-6).
	Click the Save button to save your configuration settings. Note: You need to reboot for changes to take effect.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

Table 2-21. Autoprovisioning Configuration Parameters (continued)

Web Page Item	Description
	Press the Download Template button to create an autoprovisioning file for the device. See Section 2.3.14.3, "Download Template Button"
Autoprovisioning log	The autoprovisioning log provides information about the latest autoprovisioning attempt (i.e. dhcp options and server accessed and files parsed or not found).

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

2.3.14.1 Autoprovisioning

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

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

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

By default, the device will get its autoprovisioning server from the DHCP options. See [Section 2.3.14.2, "Sample dhcpd.conf"](#) for an example of how to configure dhcpd to offer autoprovisioning server addresses. If multiple options are set, the device will attempt to download autoprovisioning files from every server.

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

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

You can download an autoprovisioning template file from the [Autoprovisioning Page](#) using the **Download Template** button (see [Table 2-21](#)). This file contains every configuration option that can be set on the board.

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

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

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

```
<!-- <AutprovFile>audio [macaddress] </AutprovFile>-->
<!-- <AutprovFile>device [macaddress] .xml</AutprovFile>-->
</MiscSettings>
```

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

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

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

The file 0020f7123456.xml contains:

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

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

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

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

Checking for New Autoprovisioning Files after Boot

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

The
Autoprovisioning
Filename

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

Table 2-22. Autoprovisioning File Name

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

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

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

For example:

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

The autoprovisioning filename is set to “cyberdata/”

On boot, the device will try to download:

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

...and if this fails:

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

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

```

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

```

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

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

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

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

The list of valid product strings:

```

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

```


Autoprovisioning
Example 1

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

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

The devices are set to use DHCP and that server provides an autoprovisioning server address with option 43. The address is "https://autoprovttest.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://autoprovttest.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://autoprovttest.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://autoprovttest.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 auto provisioning 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 auto provisioning 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 auto provisioned 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 auto provisioning 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 auto provisioning 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 Configuration** page or by changing the auto provisioning file with “**default**” set as the file name.

2.3.14.2 Sample dhcpd.conf

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

ddns-update-style none;

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

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

    option routers                10.0.0.1;
    option subnet-mask            255.0.0.0;

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

    option time-offset            -8;          # Pacific Standard Time

#   option www-server             99.99.99.99;      # OPTION 72

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

#   option option-150             10.0.0.252;     # OPTION 150

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

    range 10.10.0.1 10.10.2.1; }
}
```

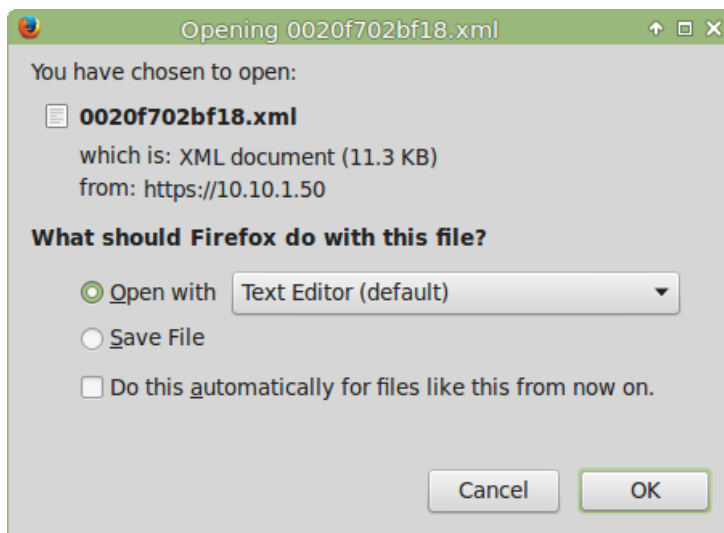
2.3.14.3 Download Template Button

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

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

1. On the **Auto provisioning** 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 2-39](#)). 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 2-39](#).

Figure 2-39. Configuration File



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

2.4 Upgrade the Firmware and Reboot the SIP Talk-Back Speaker



GENERAL ALERT

Caution

Equipment Hazard: Devices with a serial number that begins with 0981xxxxx can only run firmware versions 10.0.0 or later.

2.4.1 Downloading the Firmware

To download the firmware to your computer:

1. Download the latest firmware file from the **Downloads** tab at the following webpage:
<https://www.cyberdata.net/products/011397-011398>
2. Unzip the firmware version file. This file may contain the following:
 - Firmware file
 - Release notes
3. Log in to the home page as instructed in [Section 2.3.4, "Log in to the Configuration Home Page"](#).

- Click on the **Firmware** menu button to open the **Firmware** page. See [Figure 2-40](#).


 <small>GENERAL ALERT</small>	<p>Caution</p> <p>Equipment Hazard: CyberData strongly recommends that you first reboot the device before attempting to upgrade the firmware of the device. See Section 2.4.2, "Reboot the Device".</p>
---	---

Figure 2-40. Firmware Page



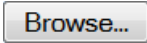

- Click on the **Browse** button, and then navigate to the location of the firmware file.
- Select the firmware file.
- Click on the **Upload** button.

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

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

- [Table 2-23](#) shows the web page items on the **Firmware** page.

Table 2-23. Firmware Parameters

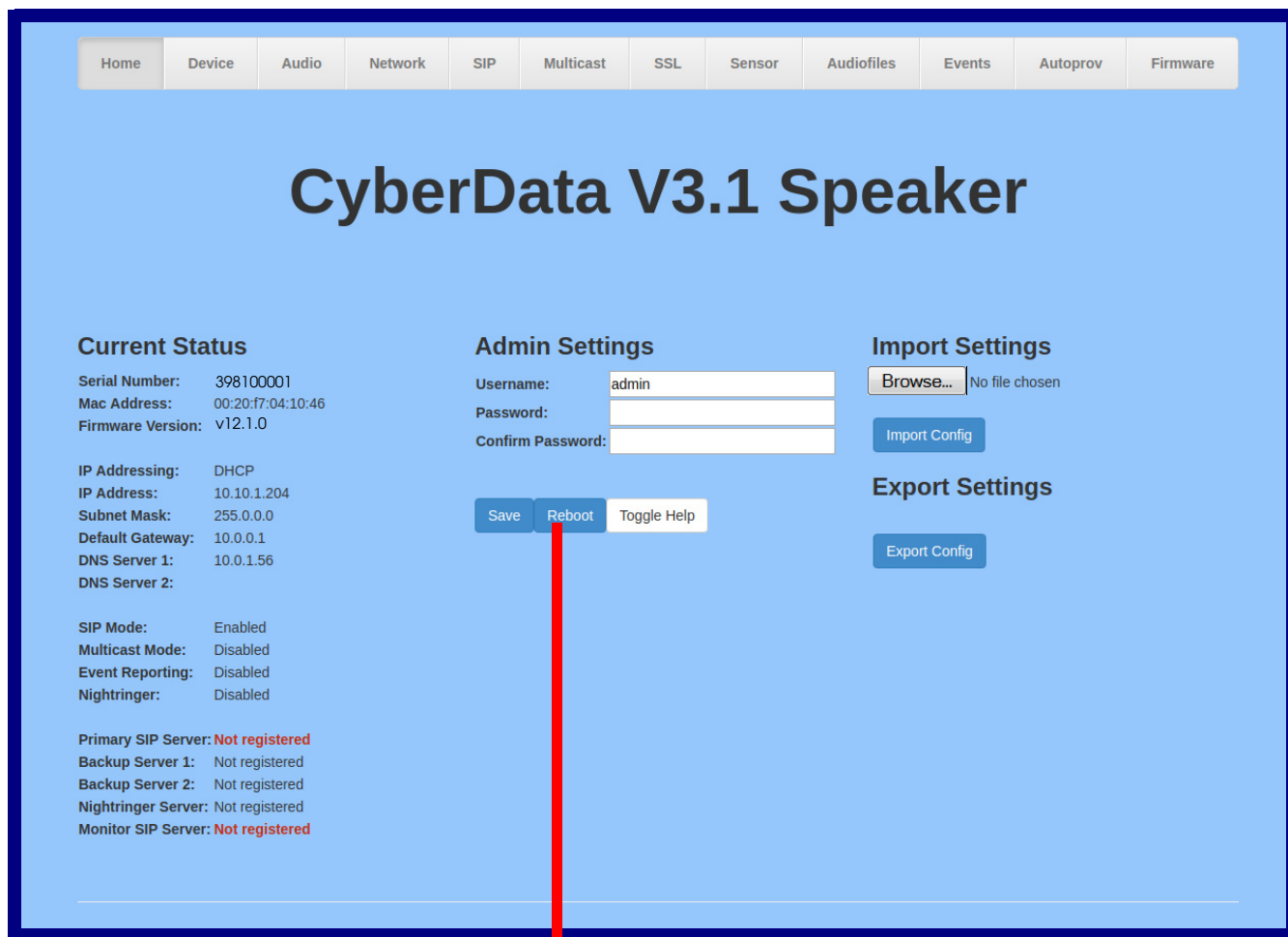
Web Page Item	Description
Current Firmware Version	Shows the current firmware version.
	Use the Browse button to navigate to the location of the firmware file that you want to upload.
	Click on the Upload button to automatically upload the selected firmware and reboot the system.

2.4.2 Reboot the Device

To reboot a SIP Talk-Back Speaker, log in to the web page as instructed in [Section 2.3.4, "Log in to the Configuration Home Page"](#).

1. Click on the **Reboot** button on the **Home** page ([Figure 2-41](#)). A normal restart will occur.

Figure 2-41. Home Page



Reboot

2.5 Command Interface

Some functions on the device can be activated using simple POST commands to the web interface. The examples in [Table 2-24](#) use the free unix utility, **wget**, but any program that can send http POST commands to the device should work.

2.5.1 Command Interface Post Commands

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

Table 2-24. Command Interface Post Commands

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

Table 2-24. Command Interface Post Commands (continued)

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

Table 2-24. Command Interface Post Commands (continued)

Device Action	HTTP Post Command^a
Delete the "0" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_0=yes"</code>
Delete the "1" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_1=yes"</code>
Delete the "2" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_2=yes"</code>
Delete the "3" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_3=yes"</code>
Delete the "4" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_4=yes"</code>
Delete the "5" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_5=yes"</code>
Delete the "6" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_6=yes"</code>
Delete the "7" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_7=yes"</code>
Delete the "8" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_8=yes"</code>
Delete the "9" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_9=yes"</code>
Delete the "Audio Test" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_audiotest=yes"</code>
Delete the "Page Tone" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_pagetone=yes"</code>
Delete the "Your IP Address Is" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_youripaddressis=yes"</code>
Delete the "Rebooting" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_rebooting=yes"</code>
Delete the "Restoring Default" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_restoringdefault=yes"</code>
Delete the "Ringback tone" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_ringback=yes"</code>

Table 2-24. Command Interface Post Commands (continued)

Device Action	HTTP Post Command^a
Delete the "Ring tone" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_ringtone=yes"
Delete the "Intrusion Sensor Triggered" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_intrusionsensortriggered=yes"
Delete the "Door Ajar" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_doorajar=yes"
Delete the "Night Ring" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_nightring=yes"
Trigger the Door Sensor Test (Sensor Config page)	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/sensor.cgi" --post-data "doortest=yes"
Trigger the Intrusion Sensor Test (Sensor Config page)	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/sensor.cgi" --post-data "intrusiontest=yes"

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

Appendix A: Mounting the Speaker

A.1 Mount the Speaker

Before you mount the speaker, make sure that you have received all the parts for each speaker. Refer to [Table A-1](#) and [Table A-2](#).

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



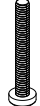
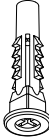
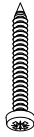
Quantity	Part Name	Illustration
3	#8 Nylon Thumb Nuts	
3	#8 Fender Washers	
3	8-32 x 1 1/4" Mounting Screws	

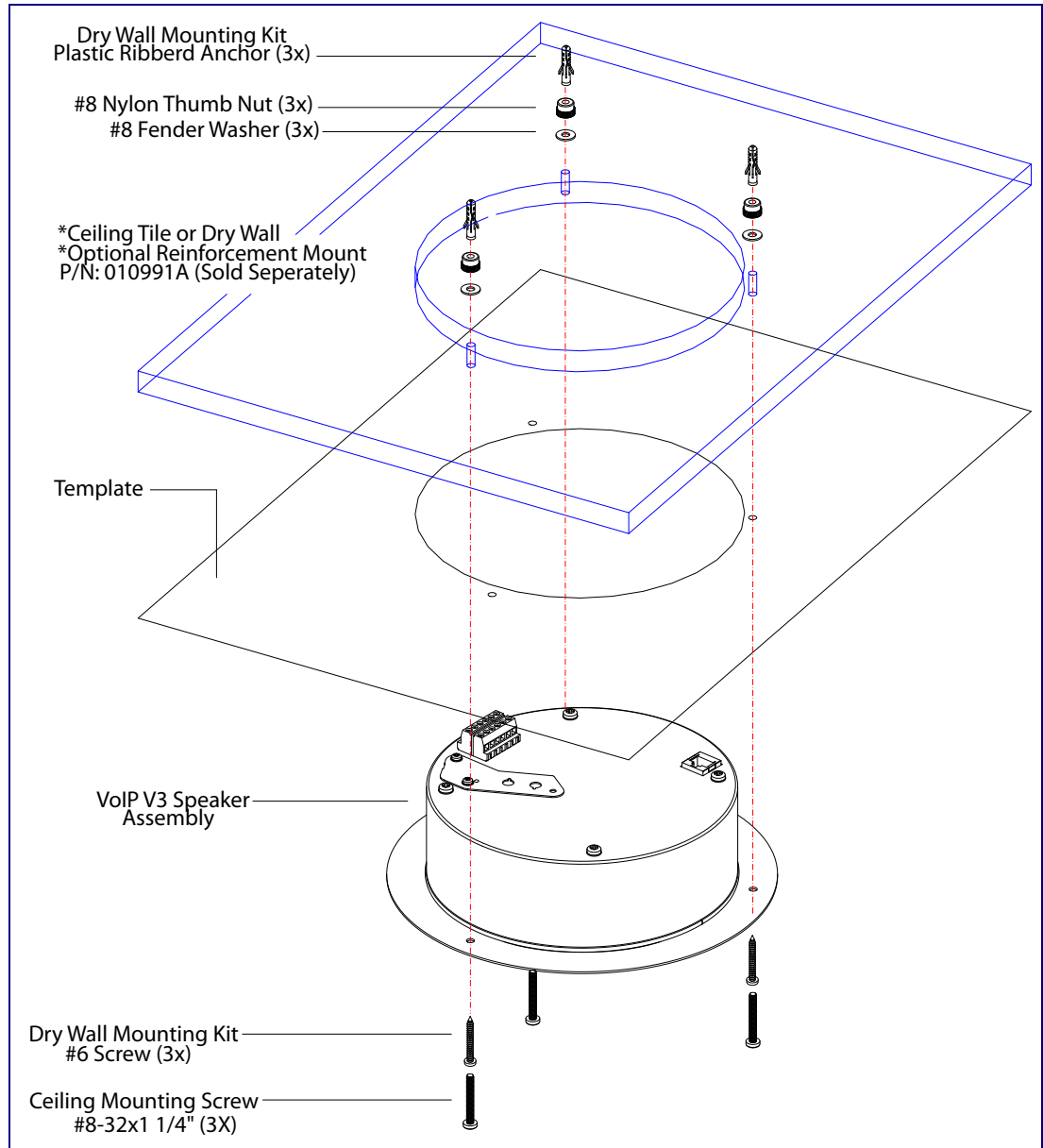
Table A-2. Drywall Mounting Components (Part of the Accessory Kit)

Quantity	Part Name	Illustration
3	Plastic Ribbed Anchors	
3	#8 Sheet Metal Screws	

To mount the speaker:

1. Use the **TEMPLATE** to cut the speaker hole and prepare holes for the screws (**Figure A-1**). This template is located on the back page of the *Installation Quick Reference Guide* that is delivered with each speaker.

Figure A-1. VoIP Speaker Assembly



2. Plug the Ethernet cable into the Speaker Assembly. [Section 2.2.3, "Confirm that the Speaker is Operational and Linked to the Network"](#) explains how the **Link** and **Status** LEDs work.
3. At this point:
 - For *drop ceiling mounting*, position the **VoIP SPEAKER ASSEMBLY** in the ceiling so that its screw holes align with those you prepared.
 - For *drywall mounting*, place the three **PLASTIC RIBBED ANCHORS** in the holes you prepared, and position the **VoIP SPEAKER ASSEMBLY** over them, aligning the screw holes in the assembly with the anchors.
4. To fasten the speaker:
 - For *drop ceiling mounting*, use the three **8-32 x 1 1/4" MOUNTING SCREWS, #8 NYLON THUMB NUTS**, and **#8 FENDER WASHERS** to secure the speaker.

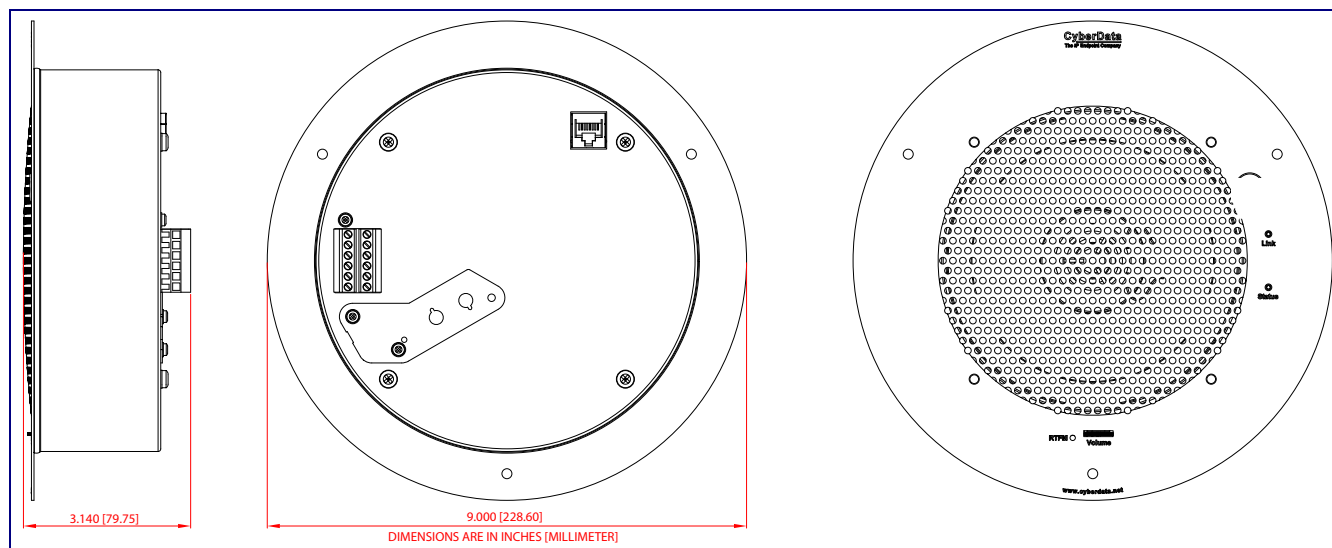
Note For weak ceiling tile, CyberData offers a reinforcing mount (CyberData part number 010991A).

- For *drywall mounting*, use the three **#8 SHEET METAL SCREWS** to secure the speaker.

A.2 Dimensions

Figure A-2 shows the dimensions for the SIP Talk-Back Speaker.

Figure A-2. Dimensions



Appendix B: Setting up a TFTP Server

B.1 Set up a TFTP Server

Autoprovisioning requires a TFTP server for hosting the configuration file.

B.1.1 In a LINUX Environment

To set up a TFTP server on LINUX:

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

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

B.1.2 In a Windows Environment

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

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

To set up a TFTP server on Windows:

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

Appendix C: Troubleshooting/Technical Support

C.1 Frequently Asked Questions (FAQ)

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

<https://www.cyberdata.net/products/011397-011398>

C.2 Documentation

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

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

<https://www.cyberdata.net/products/011397-011398>

C.3 Contact Information

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

Sales Sales 831-373-2601, Extension 334

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

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

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

Phone: (831) 373-2601, Extension 333

C.4 Warranty and RMA Information

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

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

Index

Symbols

#8 fender washers 105, 107
 #8 nylon thumb nuts 105, 107
 #8 sheet metal screws 105, 107

Numerics

8-32 x 1 1/4" mounting screws 105, 107

A

activate relay (door sensor) 72
 address, configuration login 31
 adjusting volume 26
 analog speaker
 analog volume control needs to be disabled 21
 announcing a speaker's IP address 24, 26
 audio configuration 74
 night ring tone parameter 78
 audio configuration page 74
 audio files, user-created 79
 audio output 5
 audio test 24, 26
 autoprovision at time (HHMMSS) 88
 autoprovision when idle (in minutes > 10) 88
 autoprovisioning 89
 download template button 89
 autoprovisioning autoupdate (in minutes) 88
 autoprovisioning configuration 87, 88
 autoprovisioning filename 88
 autoprovisioning server (IP Address) 88

B

backup SIP server 1 52
 backup SIP server 2 52
 backup SIP servers, SIP server
 backups 52
 boost (volume) 44

C

changing

 the web access password 35
 Cisco SRST 52
 command interface 101
 commands 101
 configurable parameters 36, 44, 48, 52
 configuration
 audio 74
 default IP settings 27
 device 14
 door sensor 64, 70
 intrusion sensor 64, 70
 network 47
 SIP 50
 configuration home page 31
 configuration page
 configurable parameters 36, 44, 48
 confirming IP address 24, 26
 contact information 110
 contact information for CyberData 110
 current network settings 48
 CyberData contact information 110

D

default
 gateway 14, 27
 IP address 14, 27
 subnet mask 14, 27
 username and password 14, 27
 web login username and password 31
 default gateway 14, 27, 48
 default IP settings 27
 default login address 31
 device configuration 14, 35
 device configuration parameters 88
 the device configuration page 87
 device configuration page 35, 43
 device configuration parameters 36, 44
 device configuration password
 changing for web configuration access 35
 dial out extension (door sensor) 72
 dial out extension strings 58
 dial-out extension strings 60
 dimensions 5
 disable volume control dial 44
 discovery utility program 31
 DNS server 48
 door sensor 70, 78
 activate relay 72
 dial out extension 72

- door sensor normally closed 72
- play audio locally 72
- download autoprovisioning template button 89
- drop ceiling mounting of speaker 107
- drywall mounting of speaker 107
- DTMF
 - monitor DTMF toggle key 37, 44
- DTMF tones 58, 60
- DTMF tones (using rfc2833) 58

E

- enable night ring events 82
- Ethernet cable 107
- event configuration
 - enable night ring events 82
- expiration time for SIP server lease 53, 56
- export settings 33

F

- factory default settings
 - how to set 26
- features 3
- firmware
 - where to get the latest firmware 98

G

- get autoprovisioning template 89
- GMT table 41
- GMT time 41

H

- home page 31
- http POST command 101

I

- identifier names (PST, EDT, IST, MUT) 41
- identifying your product 1
- illustration of speaker mounting process 105
- import settings 33
- import/export settings 33
- InformaCast needs to be 4.0 or higher 31
- installation, typical speaker system 2

- intrusion sensor 70
- IP address 14, 27, 48
- IP addressing
 - default
 - IP addressing setting 14, 27

L

- lease, SIP server expiration time 53, 56
- lengthy pages 63
- link LED 107
- Linux, setting up a TFTP server on 108
- local SIP port 53
- log in address 31

M

- MGROUP
 - MGROUP Name 62
- monitor authenticate ID 53
- monitor authenticate password 53
- monitor DTMF toggle key 37, 44
- monitor mode 11
- monitor user ID 53
- mounting a speaker 105
- multicast configuration 61, 74
- Multicast IP Address 62

N

- navigation (web page) 28
- navigation table 28
- network configuration 47
- network link activity, verifying 23
- nightring tones 63
- Nightringer 97
- nightringer settings 55
- NTP server 37

O

- overview 1

P

- pages (lengthy) 63
- parts

- #8 fender washers 105
- #8 nylon thumb nuts 105
- #8 sheet metal screws 105
- 8-32 x 1 1/4" mounting screws 105
- plastic ribbed anchors 105
- password
 - for SIP server login 52
 - login 31
 - restoring the default 14, 27
- payload types 5
- plastic ribbed anchors 105, 107
- play audio locally (door sensor) 72
- point-to-point configuration 59
- polycom default channel 63
- polycom emergency channel 63
- polycom priority channel 63
- port
 - local SIP 53
 - remote SIP 53
- posix timezone string
 - timezone string 37
- POST command 101
- power input (J1) 5
- power requirement 5
- power, connecting to speaker 15
- priority
 - assigning 63
- product
 - mounting 105
 - parts list 13
- product features 3
- product overview 1
 - product features 3
 - product specifications 5
- product specifications 5

R

- reboot 99, 100
- remote SIP port 53
- Reset Test Function Management (RTFM) button 24, 26
- restoring the factory default settings 26
- ringtones 63
 - lengthy pages 63
- rport discovery setting, disabling 53
- RTFM button 24, 26

S

- sales 110
- sensor
 - sensor normally closed 72

- sensor timeout 72
- sensor setup page 64, 71
- sensor setup parameters 64, 70
- sensors 72
- server address, SIP 52
- service 110
- set time with external NTP server on boot 37
- SIP
 - enable SIP operation 52
 - local SIP port 53
 - user ID 52
- SIP configuration 50
- SIP configuration parameters
 - outbound proxy 53, 56
 - registration and expiration, SIP server lease 53, 56
 - unregister on reboot 53
 - user ID, SIP 52
- SIP registration 52
- SIP remote SIP port 53
- SIP server 52
 - password for login 52
 - unregister from 53
 - user ID for login 52
- SIP server configuration 52
- SIP volume 44
- SRST 52
- status LED 107
- subnet mask 14, 27, 48

T

- tech support 110
- technical support, contact information 110
- template for speaker and screw holes 106
- testing audio 24, 26
- TFTP server 108
- time zone string examples 41
- typical system installation 2

U

- user ID
 - for SIP server login 52
- username
 - changing for web configuration access 35
 - default for web configuration access 31
 - restoring the default 14, 27

V

- verifying

- network link and activity 23
- power on to speaker 23
- VLAN ID 48
- VLAN Priority 48
- VLAN tagging support 48
- VLAN tags 48
- VoIP speaker assembly 107
- volume
 - multicast volume 44
 - ring volume 44
 - sensor volume 44
 - SIP volume 44
- volume boost 44
- volume control dial
 - disable 44
- volume, adjusting 26

W

- warranty policy at CyberData 110
- web access password 14, 27
- web access username 14, 27
- web configuration log in address 31
- web page
 - navigation 28
- web page navigation 28
- weight 5
- wget, free unix utility 101
- Windows, setting up a TFTP server on 108