



VoIP SIP/Multicast Ceiling Mount Speaker Operations Guide

Part #011511

Document Part #931903A
for Firmware Version 20.0.1

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

VoIP SIP/Multicast Ceiling Mount Speaker Operations Guide 931903A
Part # 011511

COPYRIGHT NOTICE:

© 2022, CyberData Corporation, ALL RIGHTS RESERVED.

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

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

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

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

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



Technical Support

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

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

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

Email: support@cyberdata.net

Fax: (831) 373-4193

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

Revision Information

Revision 931903A, which corresponds to firmware version 20.0.1, was released on February 23, 2022.

Alert Icons

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

Hazard Levels

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

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

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

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

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

Important Safety Instructions

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

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

Abbreviations and Terms

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

Contents

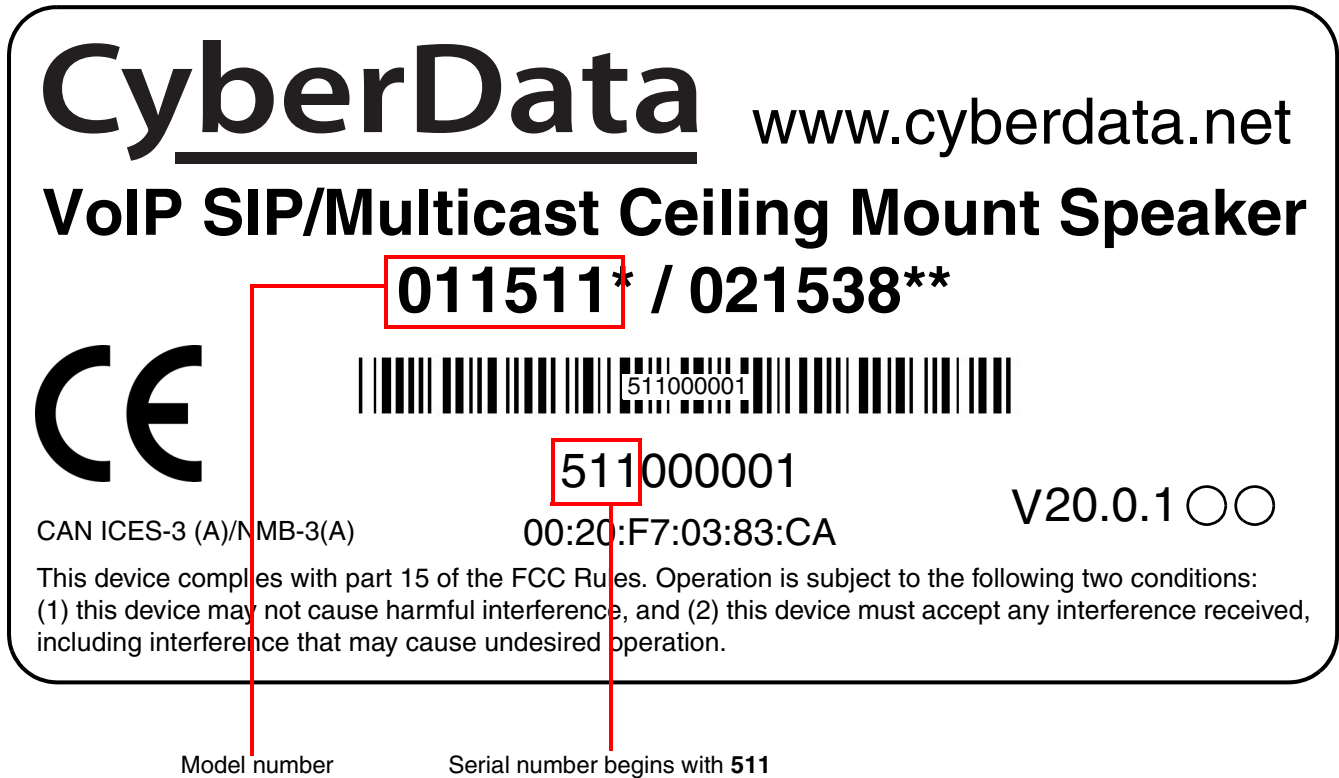
Chapter 1 Product Overview	1
1.1 How to Identify This Product	1
1.2 Typical Configuration	2
1.3 Product Features	3
1.4 Supported Protocols	4
1.5 Product Specifications	5
1.6 Compliance	6
1.6.1 CE Statement	6
1.6.2 FCC Statement	6
1.6.3 Industry Canada (IC) Compliance Statement	6
Chapter 2 Installing the VoIP SIP/Multicast Ceiling Mount Speaker	7
2.1 Parts List	7
2.2 Device Configuration	8
2.2.1 Connect Power to the Speaker	9
2.2.2 Confirm that the Speaker is Operational and Linked to the Network	10
2.2.3 Confirm the IP Address and Test the Audio	11
2.2.4 How to Set the Factory Default Settings	12
2.3.1 Factory Default Settings	13
2.3.2 VoIP SIP/Multicast Ceiling Mount Speaker Web Page Navigation	14
2.3.3 Using the Toggle Help Button	15
2.3.4 Log in to the Configuration Home Page	17
2.3.5 Configure the Device	21
2.3.6 Configure the Network Parameters	23
2.3.7 Configure the SIP Parameters	26
2.3.8 Configure the SSL Parameters	32
2.3.9 Configure the Multicast Parameters	38
2.3.10 Configure the Audio Configuration Parameters	40
2.3.11 Configure the Events Parameters	45
2.3.12 Configure the Autoprovisioning Parameters	50
2.4.1 Downloading the Firmware	61
2.4.2 Reboot the Device	64
2.5.1 Command Interface Post Commands	65
Appendix A Mounting the Speaker	67
A.1 Mounting	67
A.2 Dimensions	68
A.3 Disassembling the Speaker	69
Appendix C Setting up a TFTP Server	70
C.1 Set up a TFTP Server	70
C.1.1 Autoprovisioning requires a TFTP server for hosting the configuration file.	70
C.1.2 In a LINUX Environment	70
C.1.3 In a Windows Environment	70
Appendix C Troubleshooting/Technical Support	71
C.1 Frequently Asked Questions (FAQ)	71
C.2 Documentation	71
C.3 Contact Information	72
C.4 Warranty and RMA Information	72
Index	73

1 Product Overview

1.1 How to Identify This Product

To identify the VoIP SIP/Multicast Ceiling Mount Speaker, look for a model number label similar to the one shown in [Figure 1-1](#). The model number on the label should be **011511**.

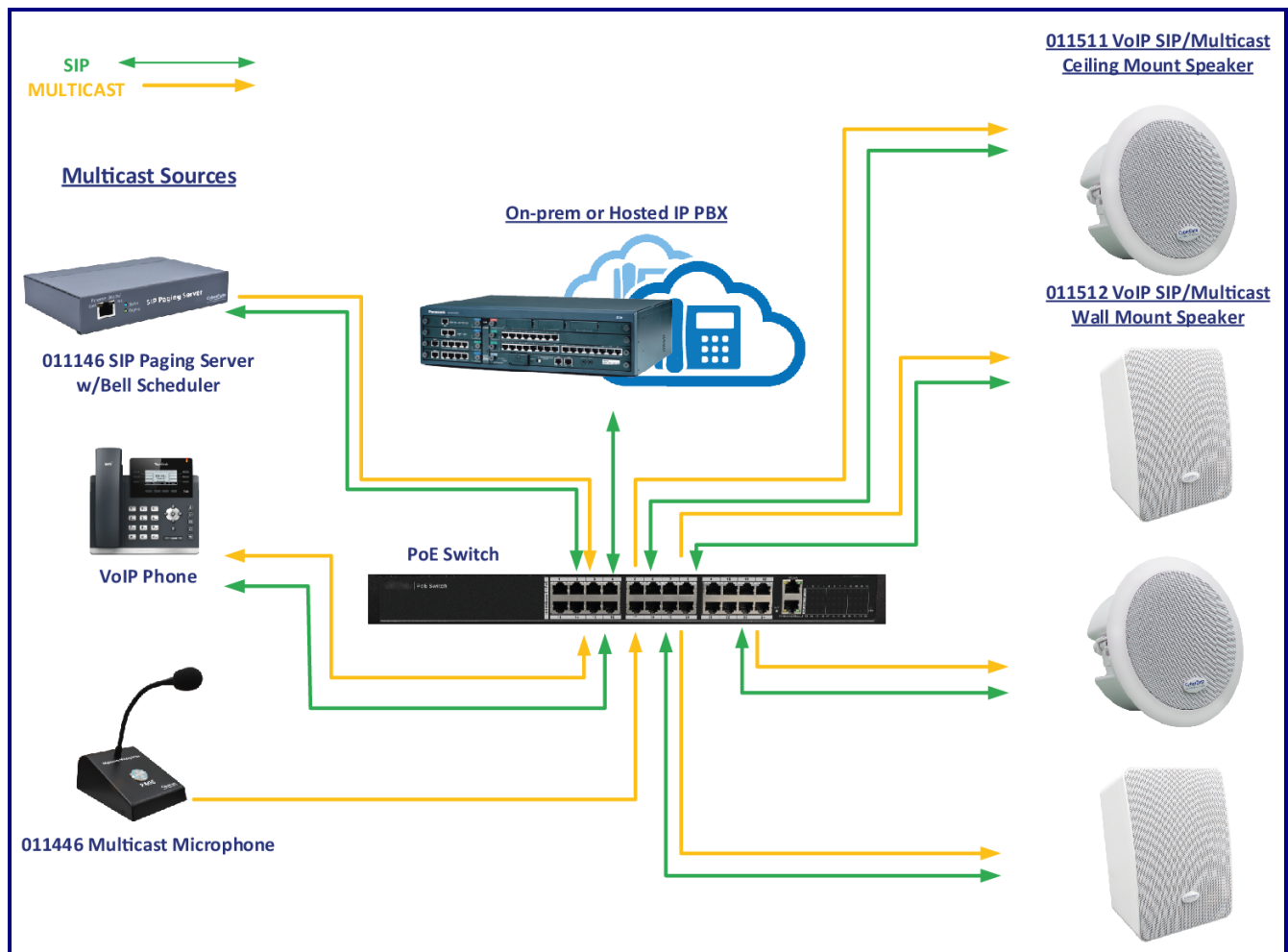
Figure 1-1. Model Number Label



1.2 Typical Configuration

Figure 1-2 shows a typical configuration for the VoIP SIP/Multicast Ceiling Mount Speaker.

Figure 1-2. Typical Configuration



1.3 Product Features

- Simultaneous SIP and multicast
- Paging prioritization
- 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

- Network-adjustable speaker volume
- High efficiency speaker driver
- Small footprint

- TLS 1.2 (includes mutual authentication) 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 VoIP SIP/Multicast Ceiling Mount Speaker supports:

- SIP (session initiation protocol)
- 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
- TFTP Client
 - Facilitates hosting for the configuration file for Autoprovisioning.
- Audio Encodings
 - PCMU (G.711 μ -law)
 - PCMA (G.711 a-law)
 - G.722
 - G.729

1.5 Product Specifications

Table 1-1. Product Specifications

Category	Specification
Ethernet I/F	10/100 Mbps
Protocol	RTP, SIP (RFC 3261)
Power Input	PoE 802.3af
Audio Output	802.3af - SPL 99 dB @ 1 meter
Payload types	G.711 a-law, G.711μ-law, G.722 and G.729
Network Security	TLS 1.2, SRTP, HTTPS
Operating Range	Temperature: -40° C to 55° C (-40° F to 131° F) Humidity: 5-95%, non-condensing
Storage Temperature	-40° C to 70° C (-40° F to 158° F)
Storage Altitude	Up to 15,000 ft. (4573 m)
Dimensions ^a	7.93 in. [201.5 mm] Grill Diameter 6.70 in. [170 mm] Can Diameter 3.52 in. [89.4 mm] Can Depth
Weight	2.4 lbs [1.09 kg]
Boxed Weight	2.9 lbs [1.32 kg]
Compliance	CE: EMC Directive – Class A EN 55032 & EN 55024, LV Safety Directive – EN 62368-1; RoHS Compliant; FCC Part 15 Class A; Industry Canada ICES-3 Class A; IEEE 802.3 Compliant; TAA Compliant
Warranty	2 Years Limited
Part number	011511

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

1.6 Compliance

1.6.1 CE Statement



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

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

1.6.2 FCC Statement



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

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

1.6.3 Industry Canada (IC) Compliance Statement

Operation is subject to the following two conditions:

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

ICES-3 Class A

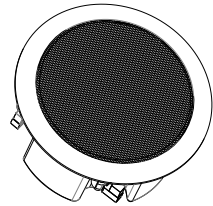
2 Installing the VoIP SIP/Multicast Ceiling Mount Speaker

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 VoIP SIP/Multicast Ceiling Mount 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	VoIP SIP/Multicast Ceiling Mount Speaker Assembly	
1	Installation Quick Reference Guide	

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	IPv4 Link Local
Web Access Username	admin
Web Access Password	admin
Subnet Mask ^a	IPv4 Link Local
Default Gateway ^a	IPv4 Link Local

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

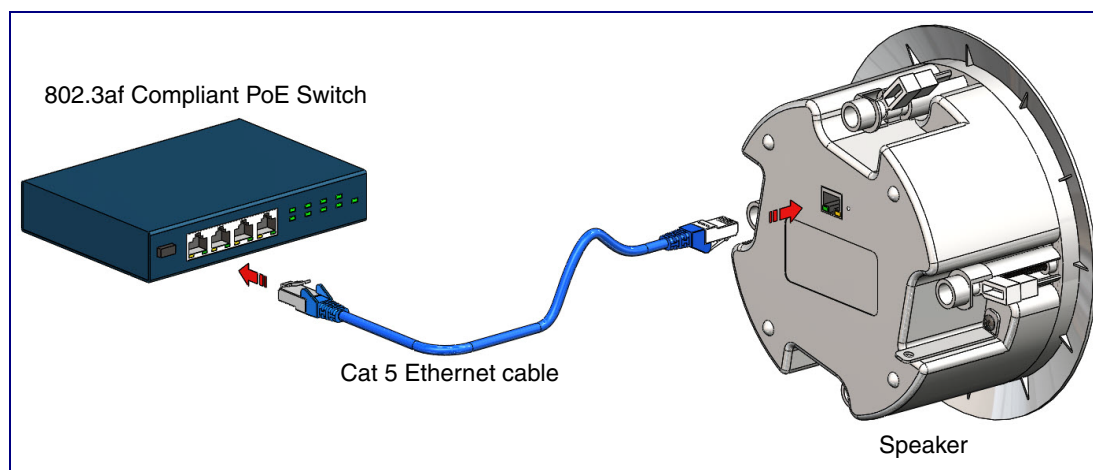
2.2.1 Connect Power to the Speaker

Figure 2-1 through Figure 2-2 illustrates how to connect power to the VoIP SIP/Multicast Ceiling Mount Speaker.

2.2.1.1 VoIP SIP/Multicast Ceiling Mount Speaker to a 802.3af Compliant PoE Switch

Figure 2-1 illustrates how to connect the VoIP SIP/Multicast Ceiling Mount Speaker to a 802.3af compliant PoE switch via a Cat 5 Ethernet cable.

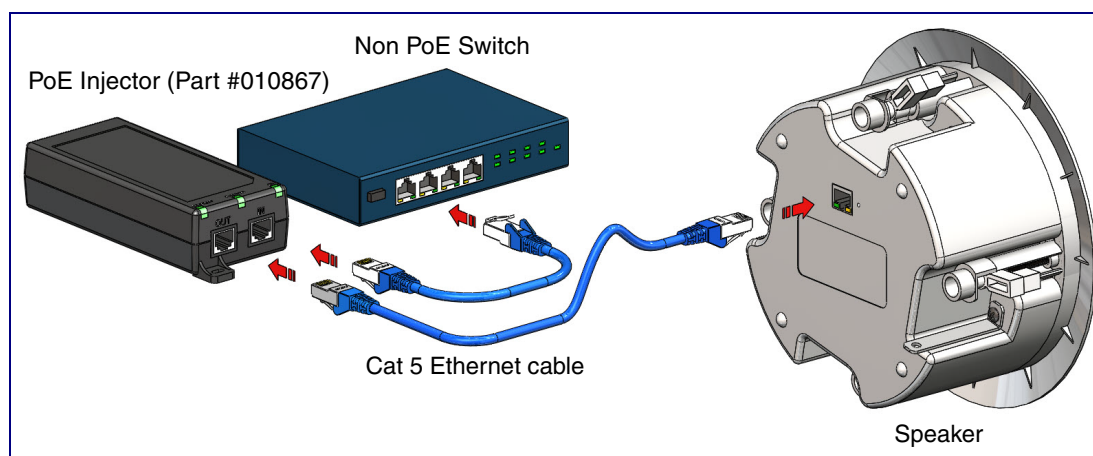
Figure 2-1. VoIP SIP/Multicast Ceiling Mount Speaker to a 802.3af Compliant PoE Switch



2.2.1.2 VoIP SIP/Multicast Ceiling Mount 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.

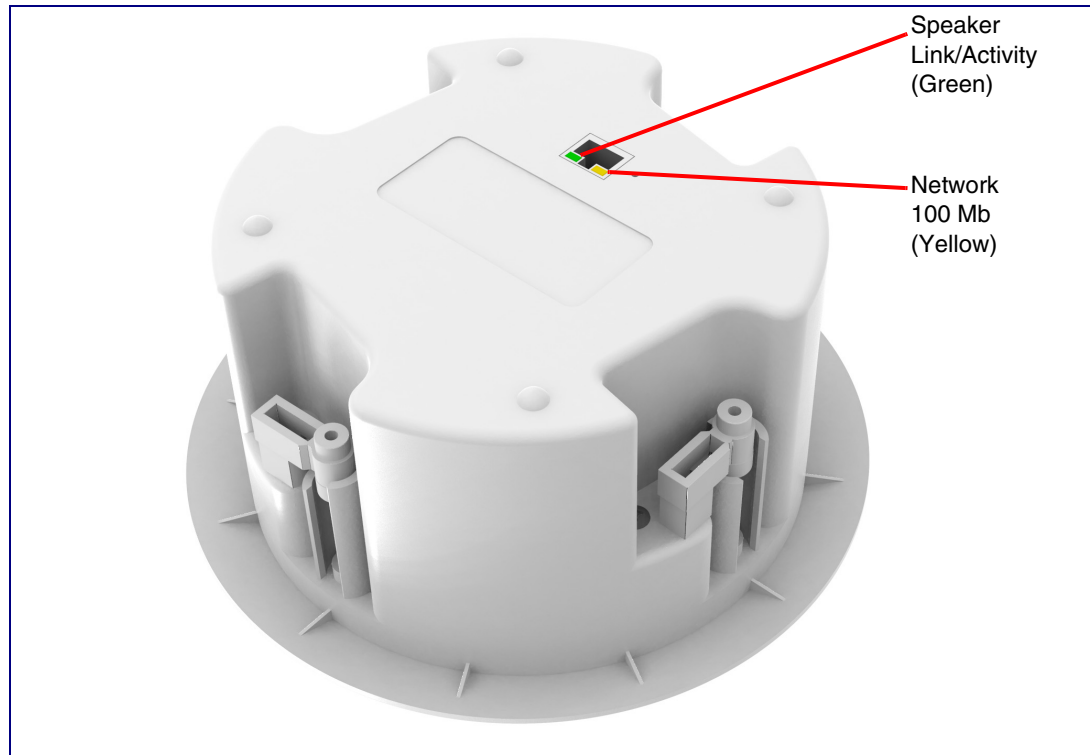
Figure 2-2. VoIP SIP/Multicast Ceiling Mount Speaker (with PoE Injector) to a Non PoE Switch



2.2.2 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 2-3. Status and Activity LEDs



2.2.2.1 Link/Activity LED

After supplying power to the speaker:

1. The green Link/Activity LED comes on immediately to show that there is a good network connection, and then blinks to show network activity.
2. After about 23 seconds with a static IP address (or 27 seconds if the board is set to use DHCP), the speaker should be ready.

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 IPv4 Link Local). This process will take approximately 80 seconds.

2.2.2.2 100 Mb LED

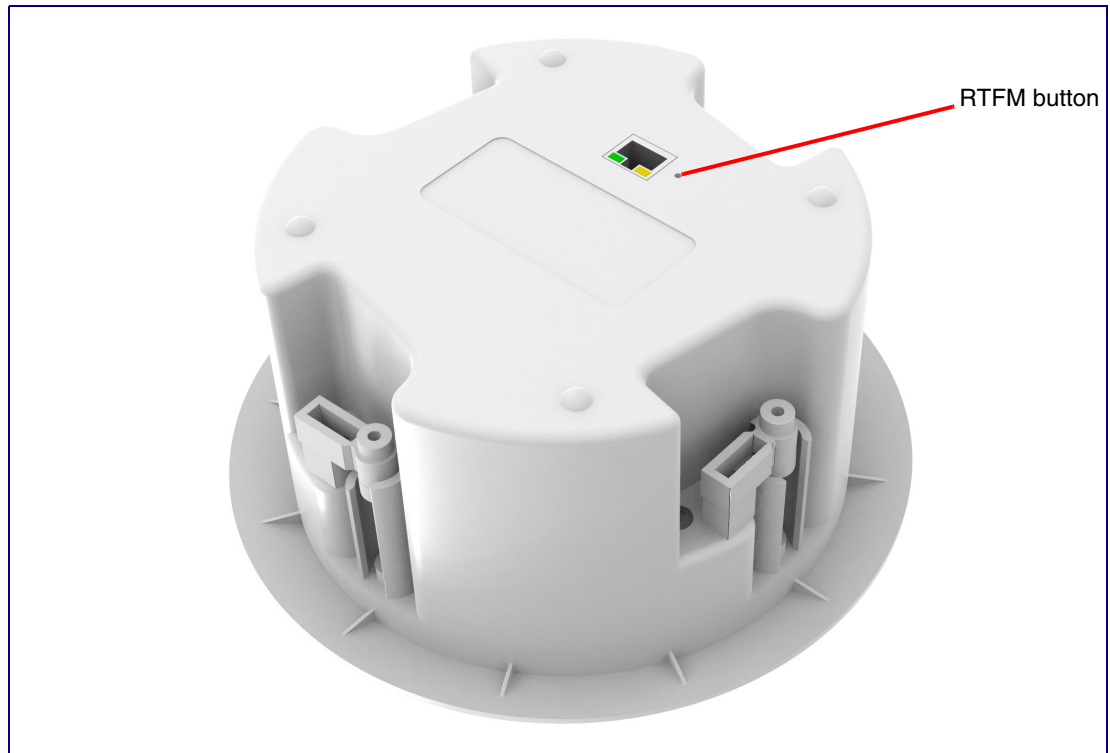
- The yellow **100 Mb** LED is illuminated when the network 100 Mb link to the speaker is established.

2.2.3 Confirm the IP Address and Test the Audio

2.2.3.1 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 2-4) on the speaker face to announce and confirm the speaker's IP Address and test that the audio is working.

Figure 2-4. RTFM Button



To announce a speaker's current IP address, use an instrument through the hole to 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 IPv4 Link Local if a DHCP server is not present).

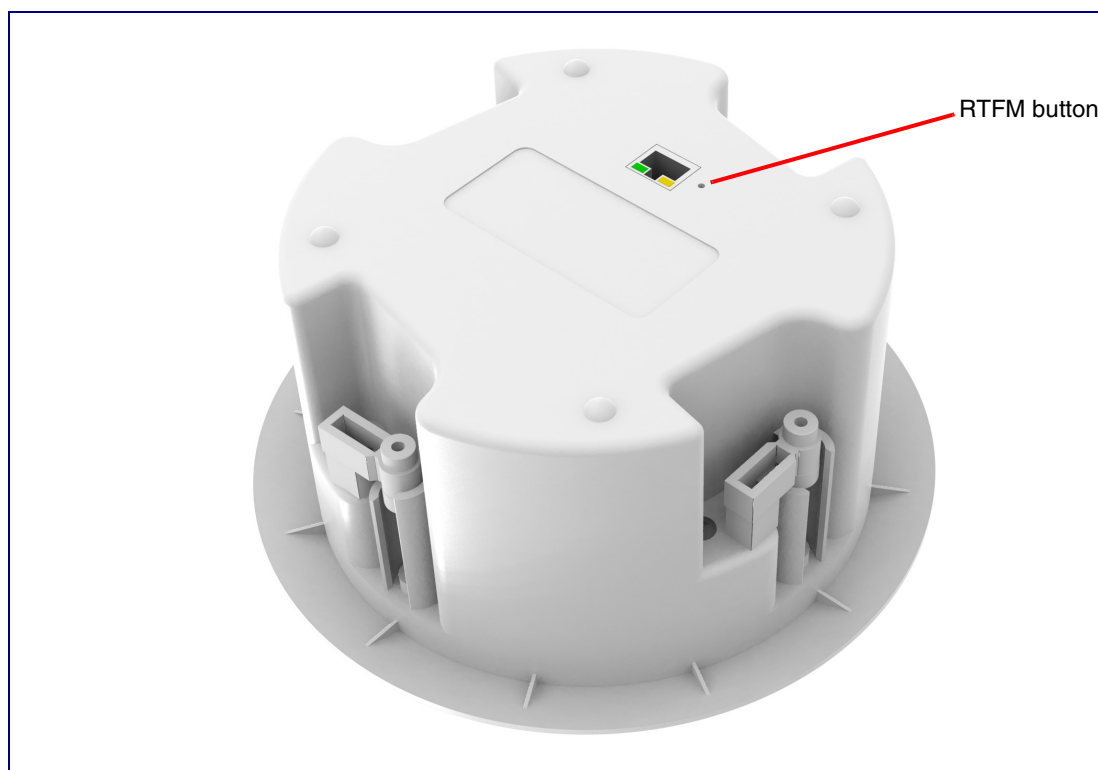
Note Pressing and holding the RTFM button for longer than five seconds will restore the speaker to the factory default settings.

2.2.4 How to Set the Factory Default Settings

2.2.4.1 RTFM Button

When the speaker is operational and linked to the network, use the Reset Test Function Management (RTFM) button (Figure 2-5) on the speaker face to set the factory default settings.

Figure 2-5. 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 IPv4 Link Local if a DHCP server is not present).

2.3 Configure the VoIP SIP/Multicast Ceiling Mount Speaker Parameters

To configure the VoIP SIP/Multicast Ceiling Mount Speaker online, use a standard web browser.

Configure each VoIP SIP/Multicast Ceiling Mount Speaker and verify its operation *before* you mount it. When you are ready to mount a VoIP SIP/Multicast Ceiling Mount Speaker, refer to [Appendix A, "Mounting the Speaker"](#) for instructions.

2.3.1 Factory Default Settings

All VoIP SIP/Multicast Ceiling Mount Speakers are initially configured with the following default IP settings:

Table 2-3. Factory Default Settings

Parameter	Factory Default Setting
IP Addressing	DHCP
IP Address ^a	IPv4 Link Local
Web Access Username	admin
Web Access Password	admin
Subnet Mask ^a	IPv4 Link Local
Default Gateway ^a	IPv4 Link Local

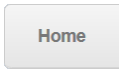
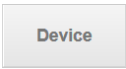
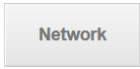
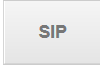
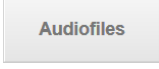
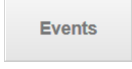
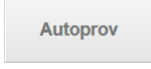
a. Default if there is not a DHCP server present.

When configuring more than one VoIP SIP/Multicast Ceiling Mount Speaker, attach the VoIP SIP/Multicast Ceiling Mount Speakers to the network and configure one at a time to avoid IP address conflicts.

2.3.2 VoIP SIP/Multicast Ceiling Mount Speaker Web Page Navigation

Table 2-4 shows the navigation buttons that you will see on every VoIP SIP/Multicast Ceiling Mount 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 Network page.
	Link to go to the SIP page.
	Link to the SSL page.
	Link to the Multicast page.
	Link to the Audiofiles page.
	Link to the Events page.
	Link to the Autoprovisioning page.
	Link to the Firmware page.

2.3.3 Using the Toggle Help Button

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

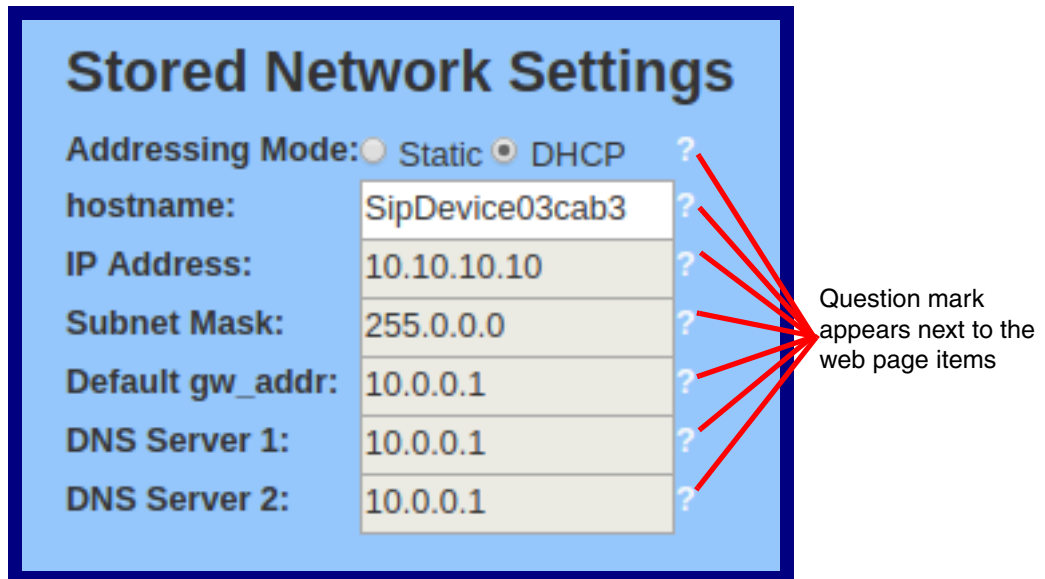
1. Click on the **Toggle Help** button that is on the UI webpage. See [Figure 2-6](#) and [Figure 2-7](#).

Figure 2-6. Toggle/Help Button



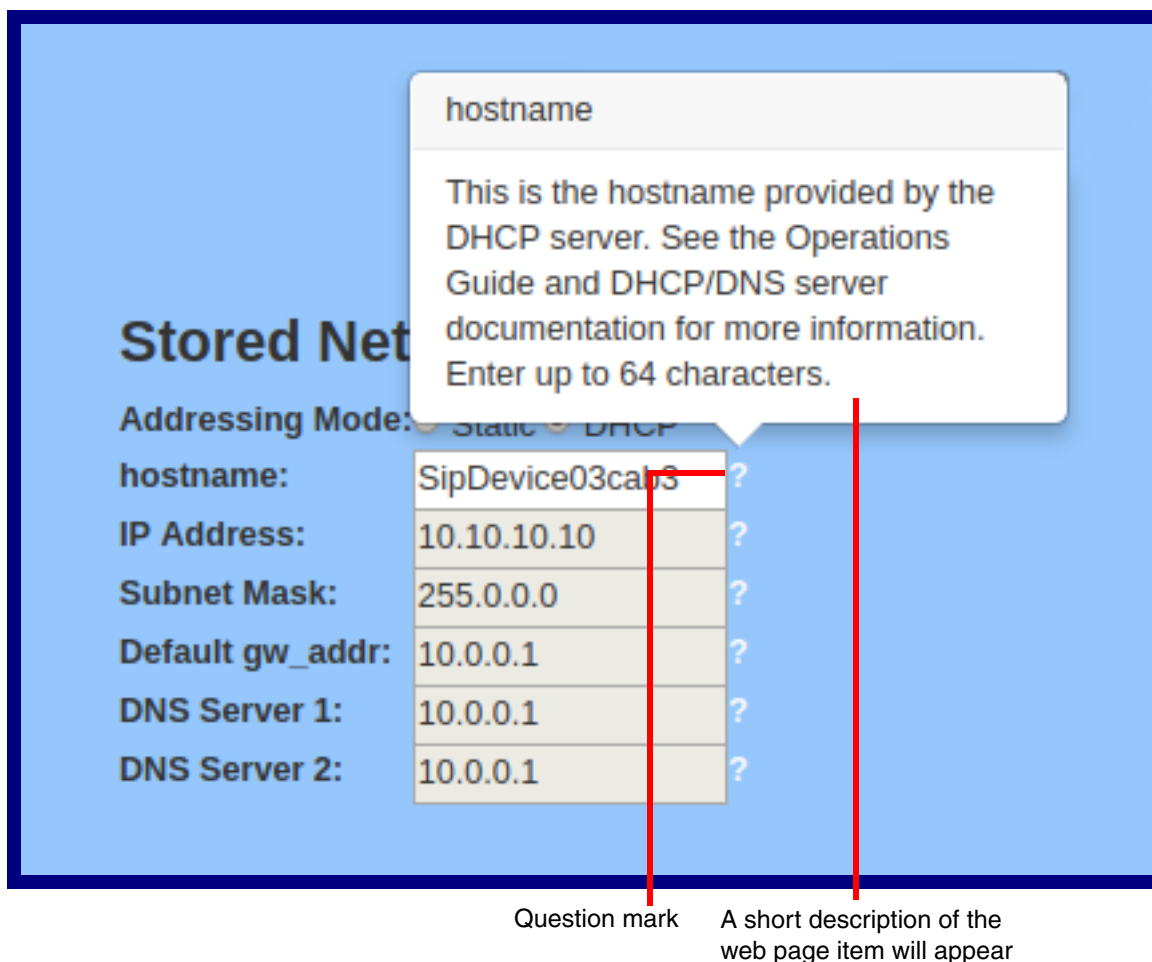
2. You will see a question mark (?) appear next to each web page item that has been provided with a short description by the Help feature. See [Figure 2-7](#).

Figure 2-7. 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 2-8](#).

Figure 2-8. Short Description Provided by the Help Feature



2.3.4 Log in to the Configuration Home Page

1. Open your browser to the VoIP SIP/Multicast Ceiling Mount Speaker IP address.

Note If the network does not have access to a DHCP server, the device will default to an IP address of IPv4 Link Local.

Note Make sure that the PC is on the same IP network as the VoIP SIP/Multicast Ceiling Mount 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.

2. When prompted, use the following default **Web Access Username** and **Web Access Password** to access the **Home Page** (Figure 2-9):

Web Access Username: **admin**

Web Access Password: **admin**

Figure 2-9. Home Page

HomeDeviceNetworkSIPSSLMulticastAudiofilesEventsAutoprovFirmware

CyberData VoIP Speaker

Current Status

Serial Number:511000001
Mac Address:00:20:f7:04:cf:33
Firmware Version:v20.0.1
Partition 2:v20.0.1
Partition 3:v20.0.1
Booting From:partition 3

Boot From Other Partition

IP Addressing:DHCP
IP Address:10.10.0.233
Subnet Mask:255.0.0.0
Default Gateway:10.0.0.1
DNS Server 1:10.0.1.56
DNS Server 2:

SIP Volume:4
Multicast Volume:4

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

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

Admin Settings

Username:admin
Password:*****
Confirm Password:*****

SaveRebootToggle Help

Import Settings

Browse...

No file chosen

Import Config

Export Settings

Export Config

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

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 Overview

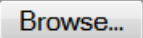
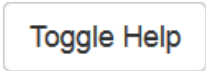
Web Page Item	Description
Admin Settings	
Username ?	The username to access the web interface. Enter up to 25 characters.
Password ?	The password to access the web interface. Enter up to 25 characters.
Confirm Password ?	Confirm the web interface password.
Current Status	
Serial Number	Shows the device serial number.
Mac Address	Shows the device Mac address.
Firmware Version	Shows the current firmware version.
Partition 2	Contains a complete copy of bootable software.
Partition 3	Contains an alternate, complete copy of bootable software.
Bootting From	Indicates the partition currently used for boot.
	Allows the user to boot from the alternate partition.
IP Addressing	Shows the current IP addressing setting (DHCP or static).
IP Address	Shows the current IP address.
Subnet Mask	Shows the current subnet mask address.
Default Gateway	Shows the current default gateway address.
DNS Server 1	Shows the current DNS Server 1 address.
DNS Server 2	Shows the current DNS Server 2 address.
SIP Volume	Shows the current SIP volume level.
Multicast Volume	Shows the current Multicast volume level.
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.
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 the Nightringer Server.
Import Settings	
	Use this button to select a configuration file to import.
	After selecting a configuration file, click Import to import the configuration from the selected file. Then, click Save and Reboot to store changes.

Table 2-5. Home Page Overview (continued)

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

2.3.5 Configure the Device

1. Click the **Device** menu button to open the **Device** page. See [Figure 2-10](#).

Figure 2-10. Device Page

Home Device Network SIP SSL Multicast Audiofiles Events Autoprovisioning Firmware

CyberData VoIP Speaker

Volume Settings (0-9)

SIP Volume:

Multicast Volume:

Clock Settings

Enable NTP: ☒

NTP Server:

Timezone:

Current Time: Tue, 21 Dec 2021 14:23:28

Misc Settings

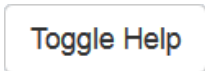
Device Name:

Disable HTTPS (NOT recommended): ☐

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
Volume Settings (0-9)	
SIP Volume ?	Set the speaker volume for a SIP call. A value of 0 will mute the speaker during SIP calls.
Multicast Volume ?	Set the speaker volume for multicast audio streams. A value of 0 will mute the speaker during multicasts. Note: You can change this setting without rebooting the device.
Clock Settings	
Enable NTP ?	Sync device's local time with the specified NTP Server.
NTP Server ?	Use this field to set the address (in IPv4 dotted decimal notation or as a canonical name) for the NTP Server. This field can accept canonical names of up to 64 characters in length.
Timezone	Enter the tz database string of your timezone. Examples: America/Los_Angeles America/New_York Europe/London America/Toronto See https://en.wikipedia.org/wiki/List_of_tz_database_time_zones for a full list of valid strings.
Current Time	Displays the current time.
Misc Settings	
Device Name ?	Type the device name. Enter up to 25 characters.
Disable HTTPS (NOT recommended) ?	Disables the encrypted connection to the webpage. We do not recommend disabling HTTPS for security reasons.
	Click on the Test Audio button to do an audio test. When the Test Audio button is pressed, you will hear a voice message for testing the device audio quality and volume.
	Click the Save button to save your configuration settings.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

2.3.6 Configure the Network Parameters

1. Click the **Network** menu button to open the **Network** page (Figure 2-11).

Figure 2-11. Network Page

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

CyberData VoIP Speaker

Stored Network Settings

Addressing Mode: ☐ Static ☒ DHCP

Hostname:

IP Address:

Subnet Mask:

Default Gateway:

DNS Server 1:

DNS Server 2:

VLAN Settings

VLAN ID (0-4095):

VLAN Priority (0-7):

Current Network Settings

IP Address: 10.10.1.220

Subnet Mask: 255.0.0.0

Default Gateway: 10.0.0.1

DNS Server 1: 10.0.1.56

DNS Server 2:

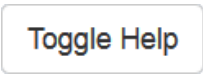
2. On the **Network** page, enter values for the parameters indicated in [Table 2-7](#).

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

Table 2-7. Network Configuration 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.
Current Network Settings	
IP Address	Shows the current Static IP address.
Subnet Mask	Shows the current Subnet Mask address.
Default Gateway	Shows the current Default Gateway address.
DNS Server 1	Shows the current DNS Server 1 address.
DNS Server 2	Shows the current DNS Server 2 address.
VLAN Settings	
VLAN ID (0-4095) ?	Specify the IEEE 802.1Q VLAN ID number. Enter up to 4 digits. Note: The device supports 802.1Q VLAN tagging support. The switch port connected to the device will need to be in "trunking mode" for the VLAN tags to propagate.
VLAN Priority (0-7) ?	Specify the IEEE 802.1p VLAN priority level. Enter 1 digit. A value of 0 may cause the VLAN ID tag to be ignored.
	Click the Save button to save your configuration settings.
	Click on the Reboot button to reboot the system.

Table 2-7. Network 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.

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

2.3.7 Configure the SIP Parameters

The SIP parameters enable the VoIP SIP/Multicast Ceiling Mount Speaker to contact and register with the SIP server. Click on the **SIP** button to open the **SIP** page.

Figure 2-12. SIP Page

The screenshot displays the 'SIP' configuration page for the CyberData VoIP Speaker. The page has a blue header with the title 'CyberData VoIP Speaker' and a navigation bar with tabs: Home, Device, Network, SIP (selected), SSL, Multicast, Audiofiles, Events, Autopro, and Firmware.

SIP Settings

- Enable SIP operation: ☒
- Register with a SIP Server: ☒
- Buffer SIP Calls: ☐
- Primary SIP Server: 10.0.0.253
- Primary SIP User ID: 199
- Primary SIP Auth ID: 199
- Primary SIP Auth Password: *****
- Re-registration Interval (in seconds): 360
- Backup SIP Server 1: Host or IP address
- Backup SIP User ID: User ID
- Backup SIP Auth ID: Auth ID
- Backup SIP Auth Password: Password
- Re-registration Interval (in seconds): 360
- Backup SIP Server 2: Host or IP address
- Backup SIP User ID: User ID
- Backup SIP Auth ID: Auth ID
- Backup SIP Auth Password: Password
- Re-registration Interval (in seconds): 360
- Remote SIP Port: 5060
- Local SIP Port: 5060
- SIP Transport Protocol: UDP
- TLS Version: 1.2 only (recommended)
- Verify Server Certificate: ☐
- Outbound Proxy: Host or IP address
- Outbound Proxy Port: 0
- Use Cisco SRST: ☐
- Disable rport Discovery: ☐
- Keep Alive Period: 10000

Nightringer Settings

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

Call Disconnection

- Terminate Call after delay: 0

Audio Codec Selection

- Codec: Auto Select

RTP Settings

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

Buttons: Save, Reboot, Toggle Help

On the **SIP** page, enter values for the parameters indicated in [Table 2-8](#).

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 2-8. SIP Configuration 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 2.3.7.1, "Point-to-Point Configuration").
Use Cisco SRST ?	When enabled, the backup servers are handled according to Cisco SRST (Survivable Remote Site Telephony). It is required for use in clustered Cisco Unified Communications Manager topologies.
Primary SIP Server ?	Enter the SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the primary SIP server. This field can accept entries of up to 255 characters in length.
Primary SIP User ID ?	Specify the SIP User ID for the Primary SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the primary SIP server. Enter up to 64 alphanumeric characters.
Primary SIP Auth ID ?	Specify the Authenticate ID for the Primary SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Primary SIP Auth Password ?	Specify the Authenticate Password for the Primary SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Server 1 ?	Enter the backup SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the backup SIP server. This field can accept entries of up to 255 characters in length.
Backup SIP User ID 1 ?	Specify the SIP User ID for the first backup SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the first backup SIP server. Enter up to 64 alphanumeric characters.
Backup SIP Auth ID 1 ?	Specify the Authenticate ID for the first backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Auth Password 1 ?	Specify the Authenticate Password for the first backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.

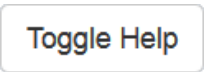
Table 2-8. SIP Configuration Parameters (continued)

Web Page Item	Description
Backup SIP Server 2 ?	Enter a second backup SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the second backup SIP server. This field can accept entries of up to 255 characters in length.
Backup SIP User ID 2 ?	Specify the SIP User ID for the second backup SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the second backup SIP server. Enter up to 64 alphanumeric characters.
Backup SIP Auth ID 2 ?	Specify the Authenticate ID for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Auth Password 2 ?	Specify the Authenticate Password for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Remote SIP Port ?	The Remote SIP Port is the port number the device will use as the destination port when sending SIP messages. The default Remote SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
Local SIP Port ?	The Local SIP Port is the port number the device will use to receive SIP messages. The default Local SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
Outbound Proxy ?	Enter the Outbound Proxy address as an IPv4 address in dotted decimal notation or a fully qualified domain name (FQDN). When an IP address is configured, the device will send all SIP messages to this IP address. When an FQDN is configured, the device will run DNS NAPTR, SRV, and A queries on the FQDN to resolve an IP address to which it will send all SIP messages. This field can accept entries of up to 255 characters in length.
Outbound Proxy Port ?	The Outbound Proxy Port is port number used as the destination port when sending SIP messages to the outbound proxy. A value of 0 will default to 5060. The supported range is 0-65536. Enter up to 5 digits.
Disable rport Discovery ?	Disabling rport Discovery will prevent the device from including the public WAN IP address and port number in the contact information that is sent to the remote SIP servers. This will generally only need to be enabled when using an SBC or SIP ALG in conjunction with a remote SIP server.
Buffer SIP Calls ?	Also referred to as "delayed paging." Device will buffer up to four minutes of audio then play back the recording after hang up or after the buffer is full. Note: Pressing the '#' key while recording a buffered SIP call will end the call and cancel the page before it is sent.
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.
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.

Table 2-8. SIP Configuration Parameters (continued)

Web Page Item	Description
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.
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.
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 [PCMU(G.711, u-law), PCMA(G.711, a-law), G.722, or G.729. Otherwise, the device will perform codec negotiation using the default list of supported codecs.
Codec ?	Select desired codec (only one may be chosen).

Table 2-8. SIP Configuration Parameters (continued)

Web Page Item	Description
RTP Settings	
RTP Port (even) ?	Specify the port number used for the RTP stream after establishing a SIP call. This port number must be an even number and defaults to 10500. The supported range is 0-65536. Enter up to 5 digits.
Asymmetric RTP ?	Specify if the remote endpoint will send and receive RTP packets on different ports. If set to false, the device will track the address/port that is sending RTP packets during a SIP call. If the address/port changes mid-stream, the device will disregard the SDP and send all further RTP packets to this new address. If set to true, this device will ignore the sending address/port and send RTP as specified in the SDP. Warning! Enabling asymmetric RTP can cause the RTP stream to be lost. Most installations should not enable asymmetric RTP.
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.
	Click the Save button to save your configuration settings.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

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

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

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

1. Enter the IP address of the **SIP Server**.
2. Enter the port numbers used for SIP signaling:
 - a. **Remote SIP Port**
 - b. **Local SIP Port**
3. Enter the SIP registration parameters:
 - a. **SIP User ID**
 - b. **Authenticate ID**
 - c. **Authenticate Password**
4. For **SIP Registration**, designate whether you want the device to register with your SIP server.
5. At **Unregister on Reboot**:
 - a. Select **Yes** to automatically unregister the VoIP SIP/Multicast Ceiling Mount Speaker when you reboot it.

- b. Select **No** to keep the VoIP SIP/Multicast Ceiling Mount Speaker registered when you reboot it.
6. In the **Register Expiration** field, enter the number of seconds the VoIP SIP/Multicast Ceiling Mount Speaker registration lease remains valid with the SIP Server. The VoIP SIP/Multicast Ceiling Mount Speaker automatically re-registers with the SIP server before the lease expiration timeout.

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

2.3.7.1 Point-to-Point Configuration

It is possible to use the device as a paging endpoint without registering it with a SIP server by configuring it for Point-to-Point paging. To do this, complete the following steps:

1. On the **SIP** page (Figure 2-13), make sure of the following:
 - The **Register with a SIP Server** parameter is not selected.
 - The **Enable SIP Operation** parameter is selected
2. Click on the **Save** button to save the changes.
3. Click on the **Reboot** button to reboot the device.
4. Enter the device's IP address as a “speed dial” (also called “auto-dial”) key on the phone(s) from which you want to page.

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

Figure 2-13. SIP Page

SIP Settings

Enable SIP operation: ☒

Register with a SIP Server: ☐

Buffer SIP Calls:

Primary SIP Server: 0.0.0.253

Primary SIP User ID: 99

Primary SIP Auth ID: 99

Primary SIP Auth Password: *****

Re-registration Interval (in seconds): 360

Nightringer Settings

SIP Server: Host or IP address

SIP User ID: User ID

SIP Auth ID: Auth ID

SIP Auth Password: Password

Re-registration Interval (in seconds): 360

Call Disconnection

Register with a SIP Server is not selected

Enable SIP Operation is selected

2.3.8 Configure the SSL Parameters

1. Click **SSL** menu button to open the **SSL** page (Figure 2-14 and Figure 2-15).

Figure 2-14. SSL Configuration Page

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

CyberData VoIP Speaker

Web Server Certificate

```

subject=
countryName           = US
stateOrProvinceName   = California
localityName          = Monterey
organizationName      = Cyberdata
commonName             = 0020f704cbc5
notBefore=Dec  2 17:01:41 2021 GMT
notAfter=Nov 30 17:01:41 2031 GMT

```

Browse... No file chosen
Import Web Certificate
Restore Web Certificate

SIP Client Certificate

```

subject=
countryName           = US
stateOrProvinceName   = California
localityName          = Monterey
organizationName      = Cyberdata
commonName             = 0020f704cbc5
notBefore=Dec  2 17:01:41 2021 GMT
notAfter=Nov 30 17:01:41 2031 GMT

```

Browse... No file chosen
Import SIP Certificate
Restore SIP Certificate
Optional Password:

Autoprovisioning Client Certificate

```

subject=
countryName           = US
stateOrProvinceName   = California
localityName          = Monterey
organizationName      = Cyberdata
commonName             = 0020f704cbc5
notBefore=Dec  2 17:01:41 2021 GMT
notAfter=Nov 30 17:01:41 2031 GMT

```

Browse... No file chosen
Import Autoprovisioning Certificate
Restore Autoprovisioning Certificate
Optional Password:

Cyberdata CA Save Reboot Toggle Help

Test TLS Connection

Server: 10.0.0.253 Port: 5060 Test SIP Connection Test Autoprovisioning Connection

List of Trusted CAs

Browse... No file chosen Import CA Certificate Remove All Restore Defaults

1	CyberData_CA.pem	Info	Remove
2	DigiCert_Assured_ID_Root_CA.crt	Info	Remove
3	DigiCert_Assured_ID_Root_G2.crt	Info	Remove
4	DigiCert_Assured_ID_Root_G3.crt	Info	Remove
5	DigiCert_Global_Root_CA.crt	Info	Remove
6	DigiCert_Global_Root_G2.crt	Info	Remove
7	DigiCert_Global_Root_G3.crt	Info	Remove
8	DigiCert_High_Assurance_EV_Root_CA.crt	Info	Remove

Figure 2-15. SSL Configuration Page

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

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

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

Table 2-9. SSL Configuration Parameters

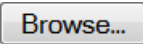
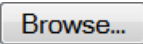
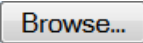
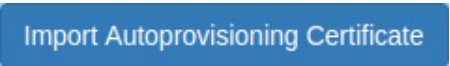
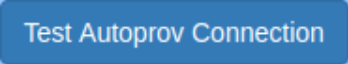
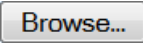
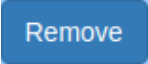
Web Page Item	Description
Web Server Certificate	Certificate used by the web server.
	Click Browse to select a certificate to import.
	After selecting a certificate, click Import Web Certificate to import it as the certificate used by this device's web server.
	Restore the device's default web server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

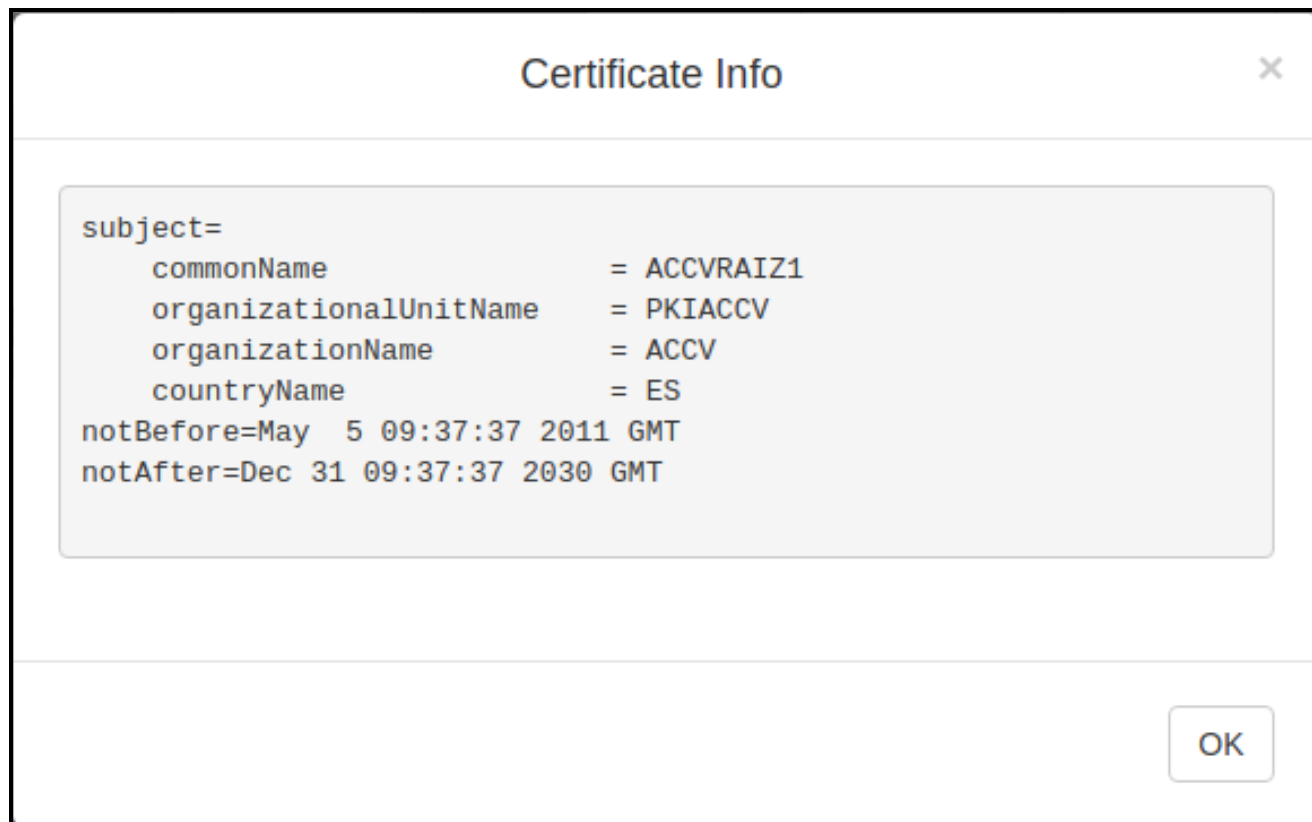
Table 2-9. SSL Configuration Parameters (continued)

Web Page Item	Description
	Click the Save button to save your configuration settings.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.
Test TLS Connection	
Server 	The ssl test server address as a fully qualified domain name or in IPv4 dotted decimal notation.
Port 	The supported range is 0-65536. SIP connections over TLS to port 5060 are modified to connect to port 5061. This test button will do the same.
	Use this button to test a TLS connection to a remote server using the sip client key and password. This will attempt to make a socket connection to the configured test server and port and report the success or failure. This can be used to debug TLS connection issues separate from SIP registration issues.
	Use this button to test a TLS connection to a remote server using the autoprovisioning client key and password. This will attempt to make a socket connection to the configured test server and port and report the success or failure. This can be used to debug TLS connection issues with secure autoprovisioning.
List of Trusted CAs	
	Use this button to select a configuration file to import.
	Click Browse to select a CA certificate to import. After selecting a server certificate authority (CA), click Import CA Certificate to import it to the list of trusted CAs. CAs are used to validate the certificate presented by the server when establishing a TLS connection.
	Restore Defaults will restore the default list of registered CAs and Remove All will remove all registered CAs.
	Restore Defaults will restore the default list of registered CAs and Remove All will remove all registered CAs.
	Provides details of the certificate. After clicking on this button, the Certificate Info Window appears. See Section 2.3.8.1, "Certificate Info Window" .
	Removes this certificate from the list of trusted certificates. After clicking on this button, the Remove Server Certificate Window appears. See Section 2.3.8.2, "Remove Server Certificate Window" .

2.3.8.1 Certificate Info Window

The **Certificate Info Window** provides details of the certificate. This window appears after clicking on the **Info** button. See [Figure 2-16](#).

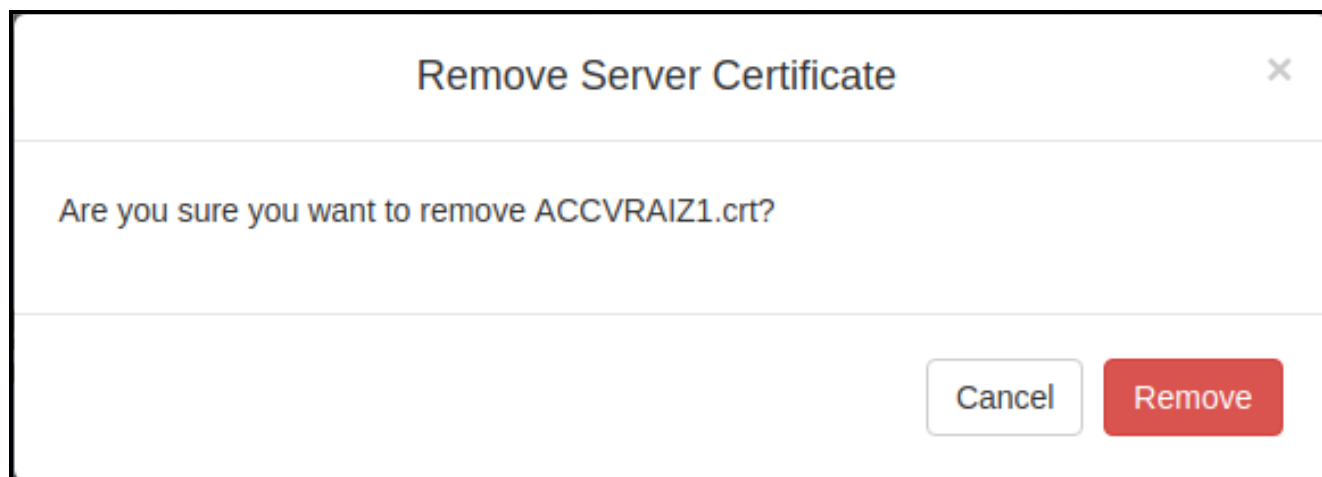
Figure 2-16. Certificate Info Window



2.3.8.2 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 2-17](#).

Figure 2-17. Remove Server Certificate Window



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.

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

Figure 2-18. Multicast Page

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

CyberData VoIP Speaker

Multicast Settings

Enable Multicast Operations: ☐

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

Polycom Default Channel: 1
Polycom Priority Channel: 24
Polycom 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
Priority 9 streams will play at maximum volume

Save Reboot

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

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

Table 2-10. Multicast Page Parameters

Web Page Item	Description
Priority	Indicates the priority for the multicast group. Priority 9 is the highest (emergency streams). 0 is the lowest (background music).
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 (length varies with codec) and then play back the recording after the multicast stream finishes or after the buffer is full.
Beep	When selected, the device will play a beep before multicast audio is sent.
Polycom Default Channel	When a default Polycom channel/group number is selected, the device will subscribe to the default channel for one-way group pages. Group Numbers 1-25 are supported. Or, select Disabled to disable this channel.
Polycom Priority Channel	When a priority Polycom channel/group number is selected, the device will subscribe to the priority channel for one-way group pages. Group Numbers 1-25 are supported. Or, select Disabled to disable this channel.
Polycom Emergency Channel	When an emergency Polycom channel/group number is selected, the device will subscribe to the default channel for one-way group pages. Group Numbers 1-25 are supported. Or, select Disabled to disable this channel.
	Click the Save button to save your configuration settings.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

2.3.10 Configure the Audio Configuration Parameters

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

1. Click on the **Audiofiles** menu button to open the **Audiofiles** page (Figure 2-19).

Figure 2-19. Audiofiles Page

Index	Name	Status	Actions
0:	Currently set to: default	No file chosen	Play Delete Save
1:	Currently set to: default	No file chosen	Play Delete Save
2:	Currently set to: default	No file chosen	Play Delete Save
3:	Currently set to: default	No file chosen	Play Delete Save
4:	Currently set to: default	No file chosen	Play Delete Save
5:	Currently set to: default	No file chosen	Play Delete Save
6:	Currently set to: default	No file chosen	Play Delete Save
7:	Currently set to: default	No file chosen	Play Delete Save
8:	Currently set to: default	No file chosen	Play Delete Save
9:	Currently set to: default	No file chosen	Play Delete Save
Dot:	Currently set to: default	No file chosen	Play Delete Save
Audio Test:	Currently set to: default	No file chosen	Play Delete Save
Page Tone:	Currently set to: default	No file chosen	Play Delete Save
Your IP Address Is:	Currently set to: default	No file chosen	Play Delete Save
Rebooting:	Currently set to: default	No file chosen	Play Delete Save

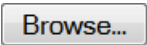
Figure 2-20. Audiofiles Page

0:	Currently set to: default	Browse...	No file chosen	Play	Delete	Save
1:	Currently set to: default	Browse...	No file chosen	Play	Delete	Save
2:	Currently set to: default	Browse...	No file chosen	Play	Delete	Save
3:	Currently set to: default	Browse...	No file chosen	Play	Delete	Save
4:	Currently set to: default	Browse...	No file chosen	Play	Delete	Save
5:	Currently set to: default	Browse...	No file chosen	Play	Delete	Save
6:	Currently set to: default	Browse...	No file chosen	Play	Delete	Save
7:	Currently set to: default	Browse...	No file chosen	Play	Delete	Save
8:	Currently set to: default	Browse...	No file chosen	Play	Delete	Save
9:	Currently set to: default	Browse...	No file chosen	Play	Delete	Save
Dot:	Currently set to: default	Browse...	No file chosen	Play	Delete	Save
Audio Test:	Currently set to: default	Browse...	No file chosen	Play	Delete	Save
Page Tone:	Currently set to: default	Browse...	No file chosen	Play	Delete	Save
Your IP Address Is:	Currently set to: default	Browse...	No file chosen	Play	Delete	Save
Rebooting:	Currently set to: default	Browse...	No file chosen	Play	Delete	Save
Restoring Default:	Currently set to: default	Browse...	No file chosen	Play	Delete	Save
Night Ring:	Currently set to: default	Browse...	No file chosen	Play	Delete	Save

2. On the **Audiofiles** page, enter values for the parameters indicated in [Table 2-11](#).

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

Table 2-11. 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.
Audio Files	
0-9	The name of the audio configuration option is the same as the spoken audio that plays on the board (24 character limit). '0' corresponds to the spoken word "zero." '1' corresponds to the spoken word "one." '2' corresponds to the spoken word "two." '3' corresponds to the spoken word "three." '4' corresponds to the spoken word "four."
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)
Your IP Address is	Corresponds to the message "Your IP address is..." (24 character limit).
Rebooting	Corresponds to the spoken word "Rebooting" (24 character limit).
Restoring Default	Corresponds to the message "Restoring default" (24 character limit).
	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.

2.3.10.1 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 2-21](#) through [Figure 2-23](#).

Figure 2-21. Audacity 1

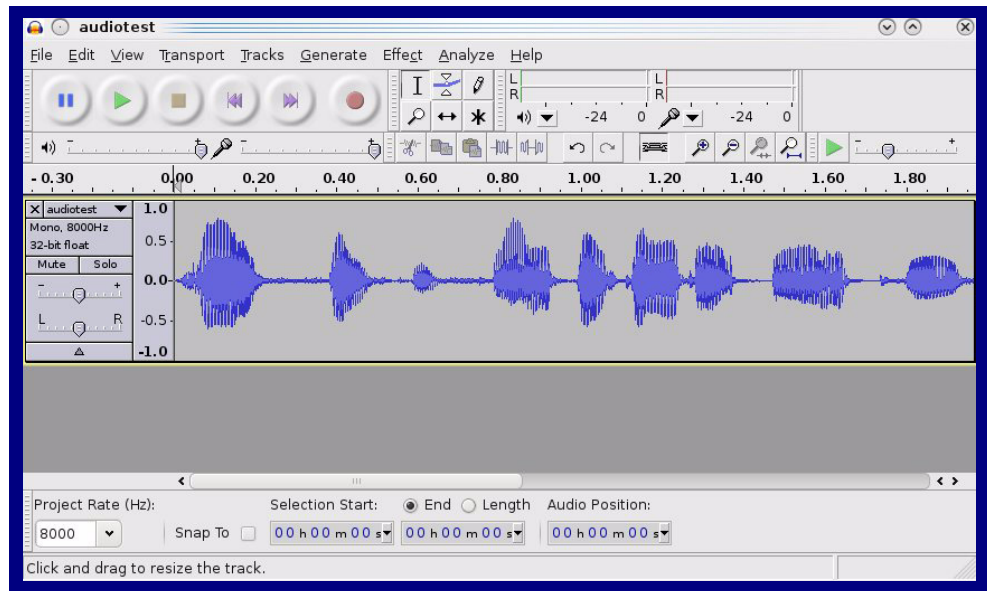
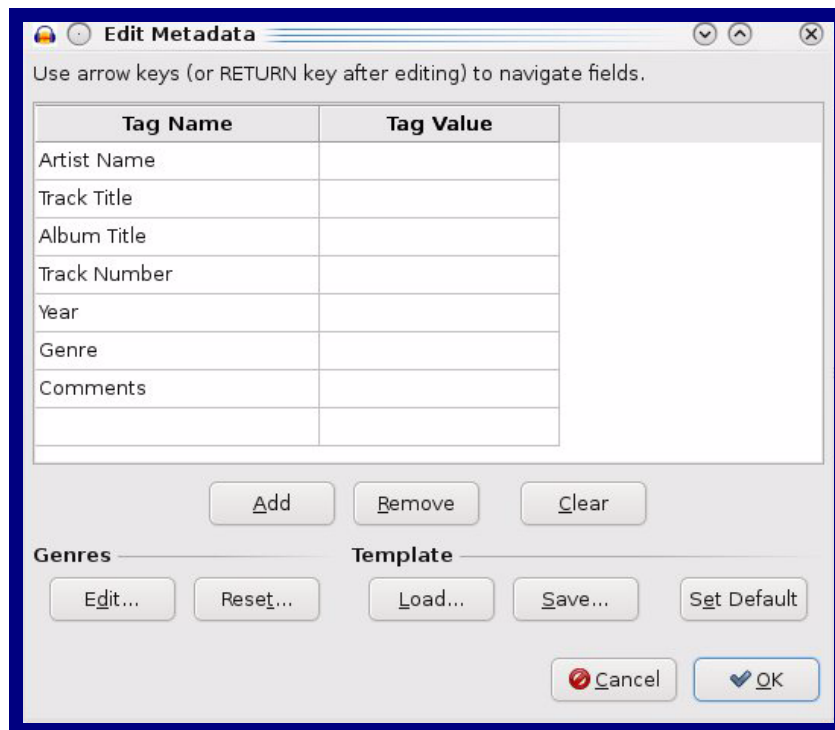


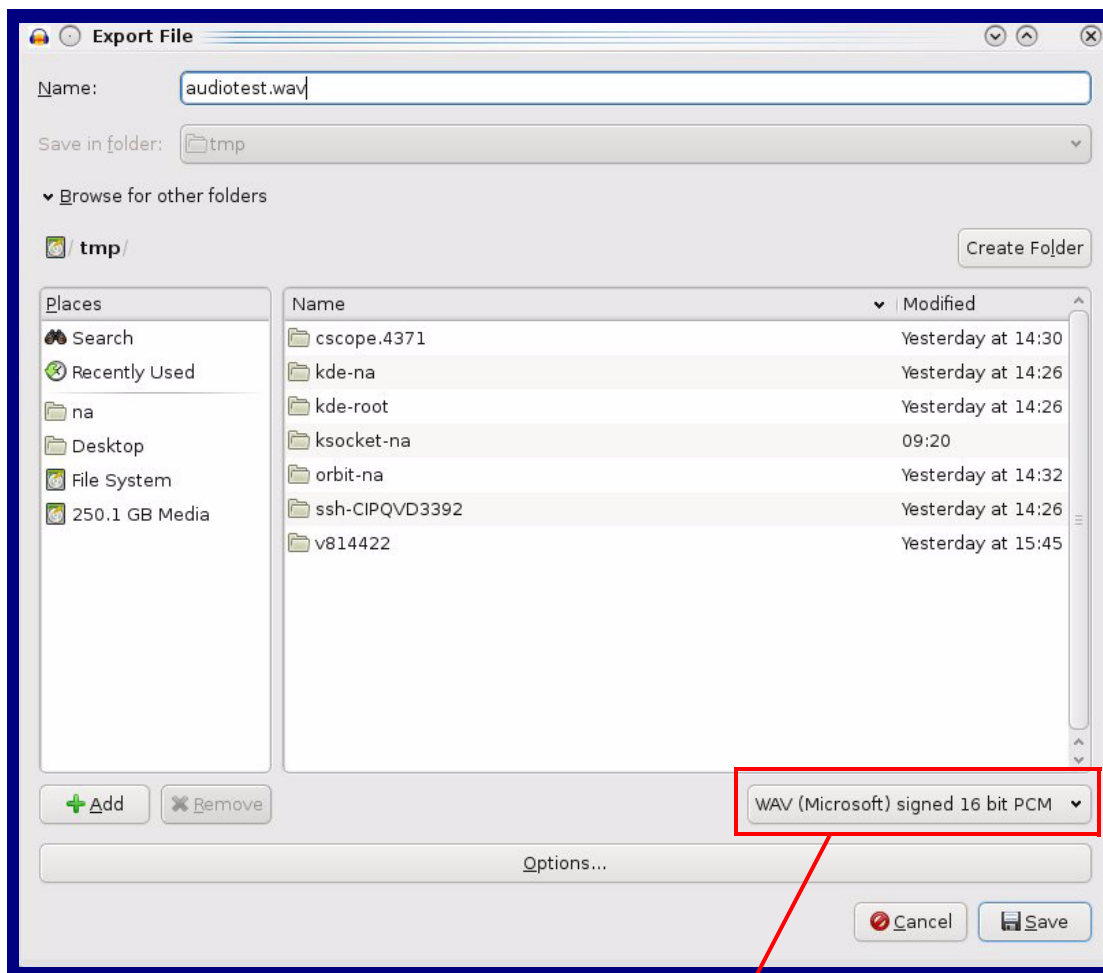
Figure 2-22. Audacity 2



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

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

Figure 2-23. WAV (Microsoft) signed 16 bit PCM



WAV (Microsoft) signed 16 bit PCM

2.3.11 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 2-24](#)).

Figure 2-24. Events Page

The screenshot shows the 'Events' configuration page for the CyberData VoIP Speaker. At the top is a navigation bar with buttons for Home, Device, Network, SIP, SSL, Multicast, Audiofiles, Events (highlighted), Autopro, and Firmware. The main title 'CyberData VoIP Speaker' is centered. Below it, there's a section 'Enable Event Generation' with a checkbox. To the left, under the 'Events' heading, are six checkboxes: 'Enable Multicast Start Events', 'Enable Multicast Stop Events', 'Enable Call Start Events', 'Enable Call Terminated Events', 'Enable Power On Events', and 'Enable 60 Second Heartbeat'. To the right, under the 'Event Server' heading, are three input fields: 'Server IP Address' (10.0.0.250), 'Server Port' (8080), and 'Server URL' (xmlparse_engine). At the bottom left are three buttons: 'Save', 'Reboot', and 'Toggle Help'.

CyberData VoIP Speaker	
Enable Event Generation: ☐	
Events	
Enable Multicast Start Events:	☐
Enable Multicast Stop Events:	☐
Enable Call Start Events:	☐
Enable Call Terminated Events:	☐
Enable Power On Events:	☐
Enable 60 Second Heartbeat:	☐
Event Server	
Server IP Address:	10.0.0.250
Server Port:	8080
Server URL:	xmlparse_engine
Save Reboot Toggle Help	

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

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. 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 Multicast Start Events ?	When selected, the device will report when the device starts playing a multicast audio stream.
Enable Multicast Stop Events ?	When selected, the device will report when the device stops playing a multicast audio stream.
Enable Call Start Events ?	When selected, the device will report the start of a SIP call.
Enable Call Terminated Events ?	When selected, the device will report the end of a SIP call.
Enable Power On Events ?	When selected, the device will report when it boots.
Enable 60 Second Heartbeat ?	When enabled, the device will report a Heartbeat event every 60 seconds. SIP registration is not required to generate Heartbeat events.
Event Server	
Server IP Address ?	The IPv4 address of the event server in dotted decimal notation.
Server Port ?	Specify the event server port number. The supported range is 0-65536. Enter up to 5 digits.
Server URL ?	Generally, the destination URL is the name of the application that receives the events and the string in the HTTP POST command. It can be a script used to parse and process the HTTP POST events. Enter up to 127 characters.
Save	Click the Save button to save your configuration settings.
Reboot	Click on the Reboot button to reboot the system.
Toggle Help	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

2.3.11.1 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/20.0.1
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/20.0.1
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/20.0.1
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/20.0.1
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/20.0.1
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/20.0.1
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/20.0.1
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/20.0.1
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/20.0.1
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/20.0.1
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/20.0.1
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>
```

2.3.12 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 2-25](#).

Figure 2-25. Autoprovisioning Page

Home Device Network SIP SSL Multicast Audiofiles Events Autoprov Firmware

CyberData VoIP Speaker

Enable Autoprovisioning: ☒

Autoprovisioning Server:

Autoprovisioning Filename:

Use tftp: ☐

Verify Server Certificate: ☐

Username:

Password:

Autoprovisioning autoupdate (in minutes):

Autoprovision at time (HHMM):

Autoprovision when idle (in minutes > 10):

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

Autoprovisioning happens on boot.

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

If these haven't been configured, it will look for an autoprovisioning server in your list of DHCP options and try to download '0020f704cbc5.xml' and if this fails, '000000cd.xml'.

Save Reboot Toggle Help

Download Template

Autoprovisioning log

```
2021-12-21 14:28:51 Autoprov: no autoprov triggers. Exiting...
2021-12-21 14:28:53 Autoprovisioning on boot
2021-12-21 14:28:53 Autoprov found server='http://10.0.0.242' in dhcp option 43
2021-12-21 14:28:53 Autoprov looking for 0020f704cbc5.xml at http://10.0.0.242
2021-12-21 14:28:53 Autoprov downloading http://10.0.0.242/0020f704cbc5.xml
2021-12-21 14:28:53 Got autoprov file. Parsing "0020f704cbc5.xml"
2021-12-21 14:28:53 Autoprov: Processing ssl certificates
2021-12-21 14:28:53 No certificate elements in SSLCertificates
2021-12-21 14:28:53 Autoprov: Processing audio files
2021-12-21 14:28:54 Autoprov found server='10.0.1.118' in dhcp option 72
```

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

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. Autoprovisioning Page Parameters

Web Page Item	Description
Enable Autoprovisioning ?	The device will automatically fetch a configuration file, also known as the 'autoprovisioning file', based on the configured settings below.
Autoprovisioning Server ?	Enter the IPv4 address of the provisioning server in dotted decimal notation.
Autoprovisioning Filename ?	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.
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.
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.
	Click the Save button to save your configuration settings.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.
	Press the Download Template button to create an autoprovisioning file for the device. See Section 2.3.12.3, "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 for the changes to take effect.

2.3.12.1 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 its 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 2.3.12.2, "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 2-13](#)). 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 VoIP Device</DeviceName>
<!--    <AutoprovFile>common.xml</AutoprovFile>-->
<!--    <AutoprovFile>sip_reg[macaddress].xml</AutoprovFile>-->
<!--    <AutoprovFile>audio[macaddress]</AutoprovFile>-->
<!--    <AutoprovFile>device[macaddress].xml</AutoprovFile>-->
</MiscSettings>
```

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

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

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

The file 0020f7123456.xml contains:

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

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

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

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

Checking for New Autoprovisioning Files after Boot

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

The
Autoprovisioning
Filename

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

Table 2-14. Autoprovisioning File Name

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

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

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

For example:

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

The autoprovisioning filename is set to “cyberdata/”

On boot, the device will try to download:

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

...and if this fails:

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

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

```

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

```

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

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

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

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

The list of valid product strings:

```

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

```

Autoprovisioning
Example 1

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

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

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

000000cd.xml

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

sip_common.xml

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

sip_0020f7020001.xml

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

sip_0020f7020002.xml

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

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

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

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

Autoprovisioning Example 2

Here is another example of setting up your autoprovisioning files:

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

0020f7020001.xml

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

0020f7020002.xml

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

common_settings.xml

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

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

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

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

XML Files

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

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

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

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

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

From the common file, a pointer to sip_common.xml

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

Autoprovisioned Audio Files

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

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

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

2.3.12.2 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; }
```

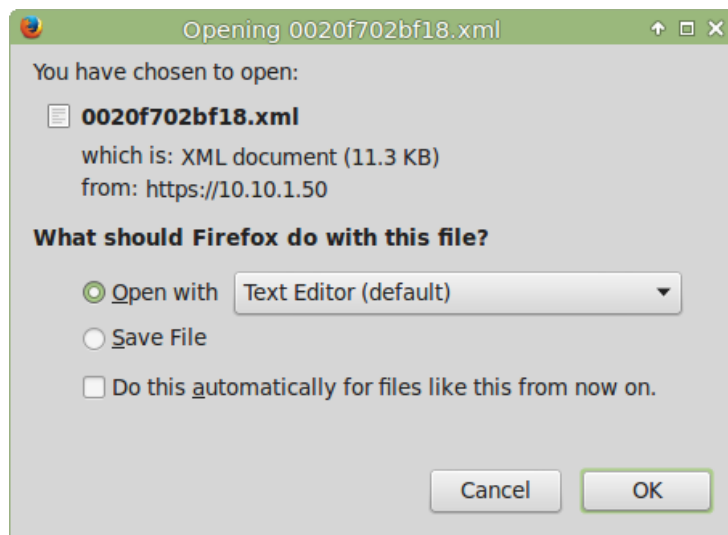
2.3.12.3 Download Template Button

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

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

1. On the **Autoprovisioning** page, click on the **Download Template** button.
2. You will see a window prompting you to save a configuration file (**.xml**) to a location on your computer ([Figure 2-26](#)). 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 2-26](#).

Figure 2-26. Configuration File



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

2.4 Upgrade the Firmware and Reboot the VoIP SIP/Multicast Ceiling Mount Speaker

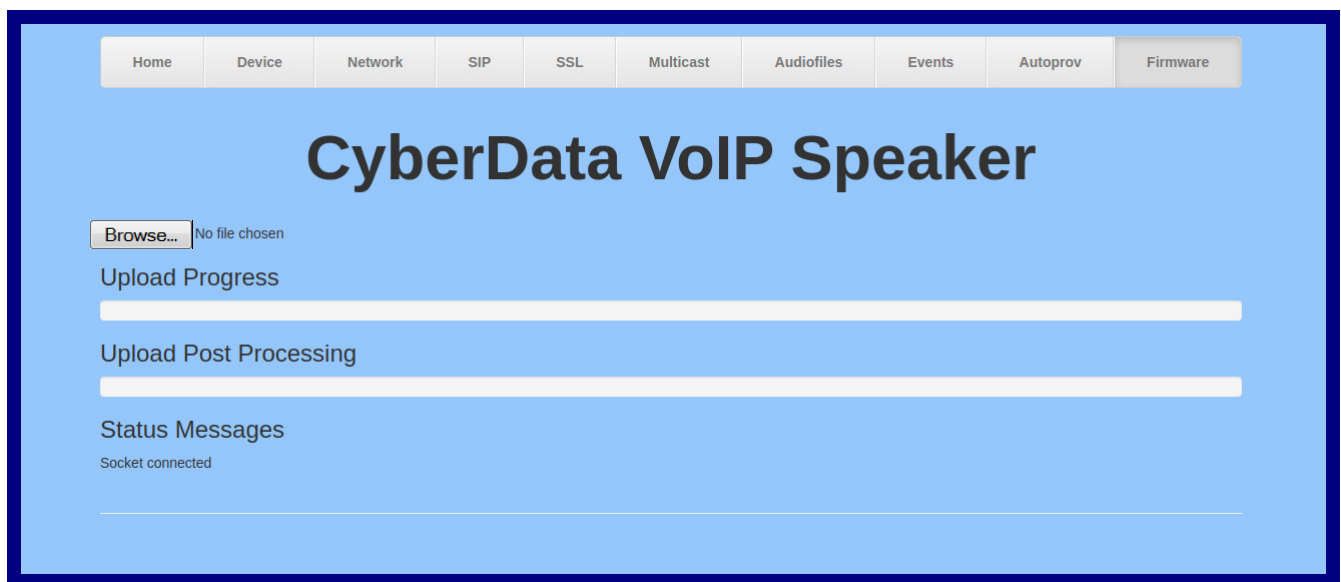
2.4.1 Downloading the Firmware

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/011511/>
2. Unzip the firmware version file. This file may contain the following:
 - Firmware file
 - Release notes
3. Log in to the VoIP SIP/Multicast Ceiling Mount Speaker home page as instructed in [Section 2.3.4, "Log in to the Configuration Home Page"](#).
4. Click on the **Firmware** menu button to open the **Firmware** page. See [Figure 2-27](#).

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

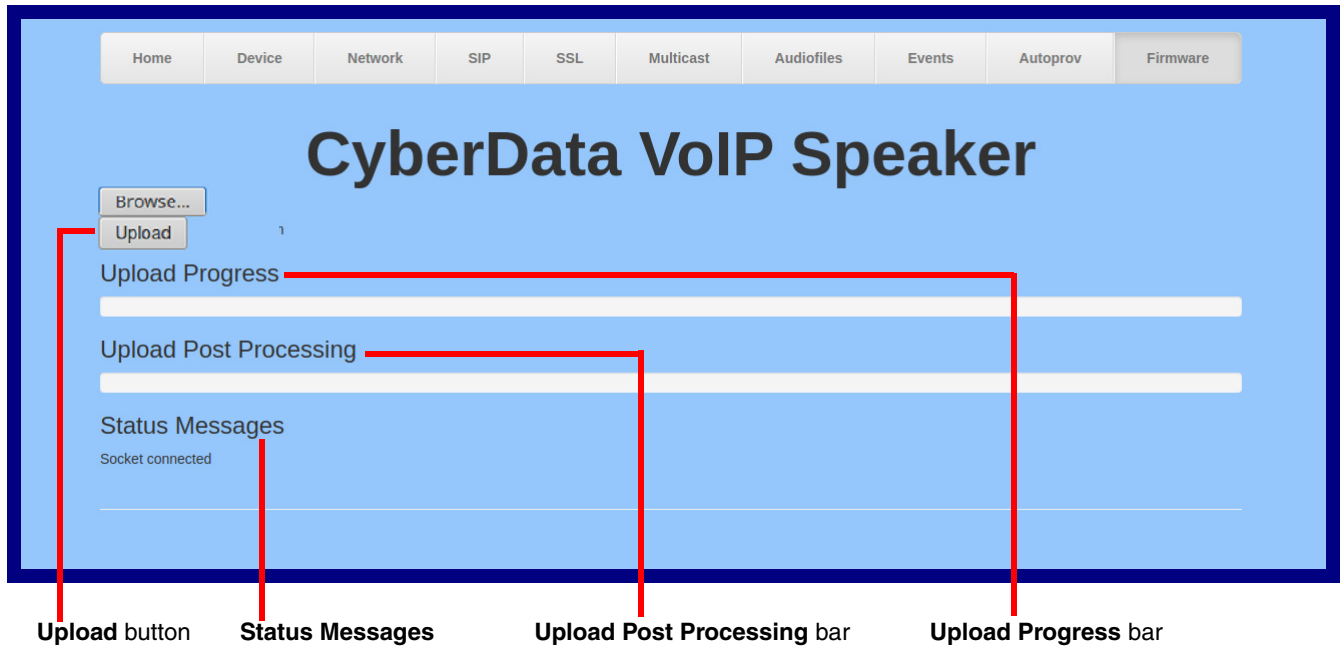
Figure 2-27. Firmware Page



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

6. Select the firmware file. This reveals the **Upload** button (Figure 2-28).

Figure 2-28. Upload Button



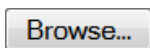
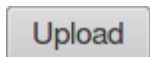
7. Click on the **Upload** button. After selecting the **Upload** button, you will see the progress of the upload in the **Upload Progress** bar.
8. When the upload is complete, you will see the words **Upload finished** under **Status Messages**.
9. At this point, you will see the progress of the upload's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

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

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

Table 2-15 shows the web page items on the **Firmware** page.

Table 2-15. Firmware Page Parameters

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

2.4.2 Reboot the Device

To reboot a VoIP SIP/Multicast Ceiling Mount 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 2-29](#)). A normal restart will occur.

Figure 2-29. Home Page

CyberData VoIP Speaker

Current Status

Serial Number: 511000001
 Mac Address: 00:20:f7:04:cf:33
 Firmware Version: v20.0.1
 Partition 2: v20.0.1
 Partition 3: v20.0.1
 Booting From: partition 2

Admin Settings

Username: admin
 Password: *****
 Confirm Password: *****

Import Settings

Browse... No file chosen
 Import Config

Export Settings

Export Config

Save Reboot Toggle Help

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 2-16](#) 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 2-16. Command Interface Post Commands

Device Action	HTTP Post Command ^a
Reboot	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.154/command" --post-data "request=reboot"
Test Audio	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.154/command" --post-data "request=test_audio"
Speak IP Address	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.154/command" --post-data "request=speak_ip_address"
Play the "0" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "0=Play"
Play the "1" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "1=Play"
Play the "2" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "2=Play"
Play the "3" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "3=Play"
Play the "4" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "4=Play"
Play the "5" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "5=Play"
Play the "6" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "6=Play"
Play the "7" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "7=Play"

Table 2-16. Command Interface Post Commands (continued)

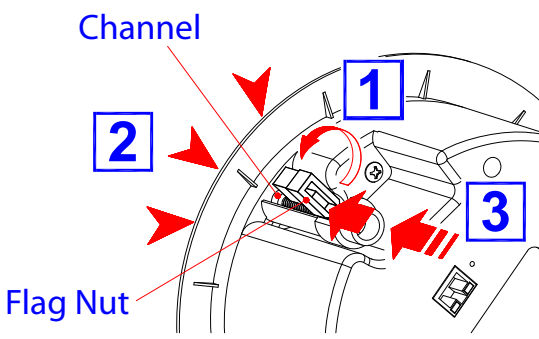
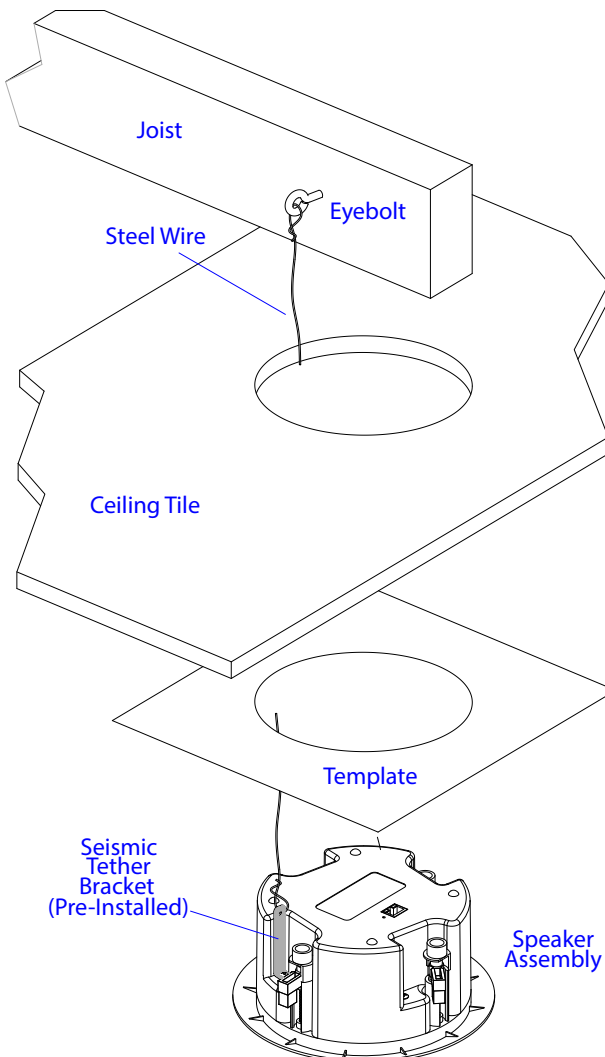
Device Action	HTTP Post Command^a
Play the "8" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "8=Play"
Play the "9" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "9=Play"
Play the "Dot" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "d=Play"
Play the Audio Test	wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "audiotest=Play"
Play the "Page Tone" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "pagetone=Play"
Play the "Your IP Address Is" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "youripaddressis=Play"
Play the "Rebooting" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "rebooting=Play"
Play the "Restoring Default" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "restoringdefault=Play"
Swap boot partitions	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.154/command" --post-data "request=swap_boot_partition"

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

A.1 Mounting

See [Figure A-1](#) to mount the speaker.

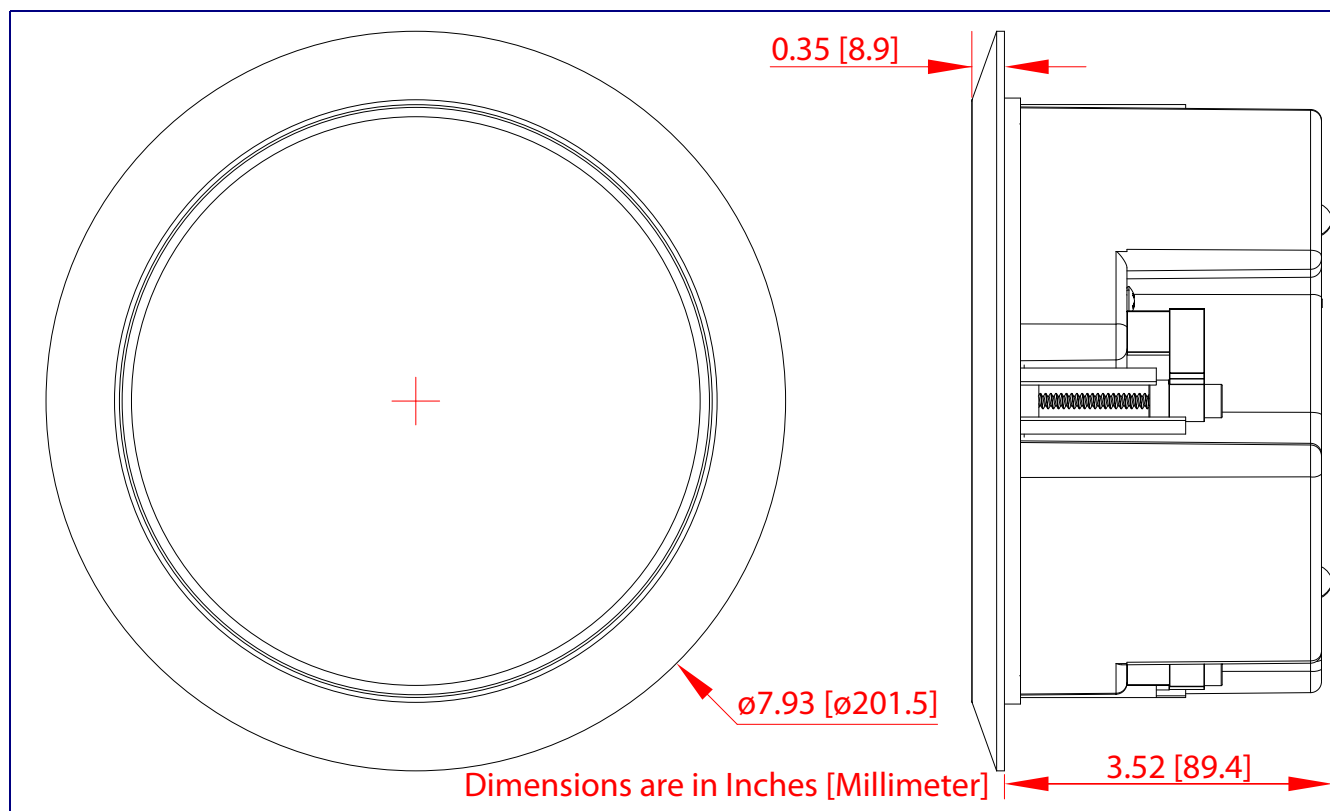
Figure A-1. Mounting the Speaker

 Channel Flag Nut 1 2 3	Remove the Speaker Grill out of the Speaker Housing: 1. Turn and line up at least two of the flag nuts with their channel. 2. Grasp the speaker grill with your index, middle, and ring fingers. 3. Place your thumb over the flag nut. At the same time, slowly push out the speaker grill.
 Joist Eyebolt Steel Wire Ceiling Tile Template Seismic Tether Bracket (Pre-Installed) Speaker Assembly	Tools Required for Installation: • (1) Sheetrock Saw or Drywall Cutter • (1) #2 Phillips Screw Driver or Powered Screw Driver with #2 Phillips Hex Bit To mount the speaker: 1. Loosen the Four (4) flag nuts with a #2 Phillip Screw Driver or Powered Screw Driver. 2. Use the TEMPLATE on the back of this document to cut a hole in the wall* or ceiling. *Skip the seismic tether mounting when mounting it to the wall. 3. Tighten the Four (4) flag nuts with a #2 Phillip Screw Driver or Powered Screw Driver. 4. Replace the speaker grill to the speaker housing.

A.2 Dimensions

Figure A-2 shows the dimensions for the VoIP SIP/Multicast Ceiling Mount Speaker.

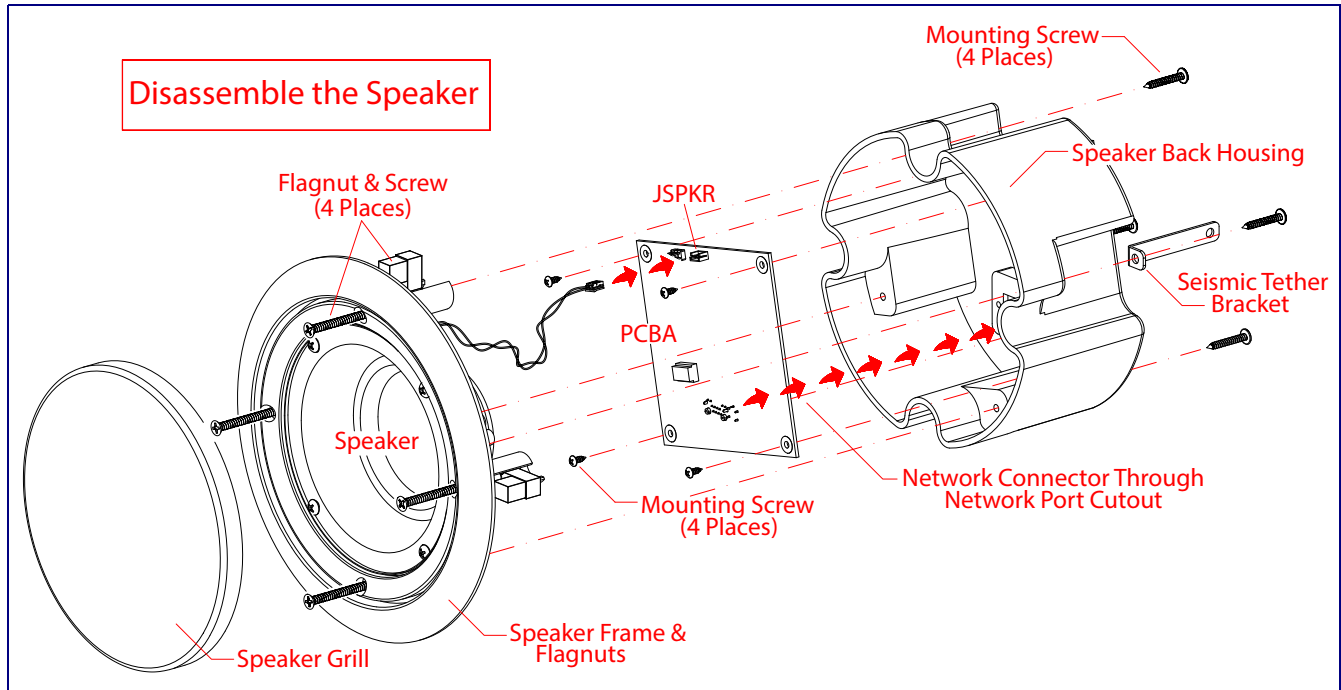
Figure A-2. Dimensions



A.3 Disassembling the Speaker

Figure A-3 shows how to disassemble the VoIP SIP/Multicast Ceiling Mount Speaker.

Figure A-3. Disassembling the Speaker



Appendix C: Setting up a TFTP Server

C.1 Set up a TFTP Server

C.1.1 Autoprovisioning requires a TFTP server for hosting the configuration file.

C.1.2 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
```

C.1.3 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/011511/>

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/011511/>

C.3 Contact Information

Contact	CyberData Corporation 3 Justin Court Monterey, CA 93940 USA www.CyberData.net Phone: 800-CYBERDATA (800-292-3732) Fax: 831-373-4193
Sales	Sales 831-373-2601, Extension 334
Technical Support	The fastest way to get technical support for your VoIP product is to submit a VoIP Technical Support form at the following website: https://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:

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

Index

A

- address, configuration login 17
- adjusting volume 12
- announcing a speaker's IP address 11, 12
- audio configuration 40
- audio configuration page 40
- audio files, user-created 43
- audio output 5
- audio test 11, 12
- authenticate ID and password for SIP server
 - registration 30
- autoprovision at time (HHMMSS) 51
- autoprovision when idle (in minutes > 10) 51
- autoprovisioning 51, 52
 - download template button 51
- autoprovisioning autoupdate (in minutes) 51
- autoprovisioning configuration 50, 51
- autoprovisioning filename 51
- autoprovisioning server (IP Address) 51

B

- backup SIP server 1 27
- backup SIP server 2 27
- backup SIP servers, SIP server
 - backups 27

C

- changing
 - the web access password 21
- Cisco SRST 27
- command interface 65
- commands 65
- configurable parameters 22, 24, 27
- configuration
 - audio 40
 - default IP settings 13
 - device 8
 - door sensor 32
 - intrusion sensor 32
 - network 23
- configuration home page 17
- configuration page
 - configurable parameters 22, 24
- confirming IP address 11, 12
- contact information 72

- contact information for CyberData 72
- current network settings 24
- CyberData contact information 72

D

- default
 - gateway 8, 13
 - IP address 8, 13
 - subnet mask 8, 13
 - username and password 8, 13
 - web login username and password 17
- default gateway 8, 13, 24
- default IP settings 13
- default login address 17
- device configuration 8, 21
 - device configuration parameters 51
 - the device configuration page 50
- device configuration page 21
- device configuration parameters 22
- device configuration password
 - changing for web configuration access 21
- dimensions 5
- discovery utility program 17
- DNS server 24
- download autoprovisioning template button 51

E

- expiration time for SIP server lease 28, 29, 31
- export settings 19, 20

F

- factory default settings
 - how to set 12
- features 3
- firmware
 - where to get the latest firmware 61

G

- get autoprovisioning template 51

H

hazard levels 3
home page 17
http POST command 65

I

identifying your product 1
import settings 19, 20
import/export settings 19, 20
intercom configuration page
 configurable parameters 27
IP address 8, 13, 24
 SIP server 30
IP addressing
 default
 IP addressing setting 8, 13

L

lease, SIP server expiration time 28, 29, 31
Linux, setting up a TFTP server on 70
local SIP port 28, 30
log in address 17

M

MGROUP
 MGROUP Name 39
multicast configuration 38, 40
Multicast IP Address 39

N

navigation (web page) 14
navigation table 14
network configuration 23
network link activity, verifying 10
Nightringer 60
nightringer settings 29
NTP server 22

O

overview 1

P

- password
 - for SIP server login 27
 - login 17
 - restoring the default 8, 13
 - SIP server authentication 30
- point-to-point configuration 31
- polycom default channel 39
- polycom emergency channel 39
- polycom priority channel 39
- port
 - local SIP 28, 30
 - remote SIP 28, 30
- POST command 65
- power input (J1) 5
- power requirement 5
- power, connecting to speaker 9
- product
 - parts list 7
- product features 3
- product overview 1
 - product features 3
 - product specifications 5
- product specifications 5

R

- reboot 63, 64
 - unregistering from SIP server during 30
- registration and expiration, SIP server
 - lease expiration 31
- remote SIP port 28, 30
- Reset Test Function Management (RTFM) button 11, 12
- restoring the factory default settings 12
- rport discovery setting, disabling 28
- RTFM button 11, 12

S

- sales 72
- sensor setup page 32
- sensor setup parameters 32
- server address, SIP 27
- service 72
- SIP
 - enable SIP operation 27
 - local SIP port 28
 - user ID 27
- SIP configuration page 26
- SIP configuration parameters
 - outbound proxy 28, 29
 - registration and expiration, SIP server lease 28, 29

- unregister on reboot 28
 - user ID, SIP 27
- SIP registration 27
- SIP remote SIP port 28
- SIP server 27
 - password for login 27
 - unregister from 28
 - user ID for login 27
- SIP server configuration 27
- SIP setup button 26
- SIP volume 22
- SRST 27
- subnet mask 8, 13, 24

T

- tech support 72
- technical support, contact information 72
- testing audio 11, 12
- TFTP server 70

U

- unregister from SIP server 30
- user ID
 - for SIP server login 27
- user ID for SIP server registration 30
- username
 - changing for web configuration access 21
 - default for web configuration access 17
 - restoring the default 8, 13

V

- verifying
 - network link and activity 10
 - power on to speaker 10
- VLAN ID 24
- VLAN Priority 24
- VLAN tagging support 24
- VLAN tags 24
- volume
 - multicast volume 22
 - SIP volume 22
- volume, adjusting 12

W

- warranty policy at CyberData 72

- web access password 8, 13
- web access username 8, 13
- web configuration log in address 17
- web page
 - navigation 14
- web page navigation 14
- weight 5
- wget, free unix utility 65
- Windows, setting up a TFTP server on 70