SIP IP66 Outdoor Horn
Operations Guide

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

CyberData Corporation
3 Justin Court
Monterey, CA 93940
(831) 373-2601
SIP IP66 Outdoor Horn Operations Guide 931508B
Part # 011457

COPYRIGHT NOTICE:
© 2018, CyberData Corporation, ALL RIGHTS RESERVED.

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

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

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

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

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

---

Technical Support

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

http://support.cyberdata.net/

Phone: (831) 373-2601, Ext. 333
Email: support@cyberdata.net
Fax: (831) 373-4193
Company and product information is at www.cyberdata.net.
Revision Information

Revision 931508B, which corresponds to firmware version 11.8.0, was released on May 4, 2018, and has the following changes:

- Updates Figure 2-1, "SIP IP66 Outdoor Horn Connections"
- Updates the following setting and description in Table 2-7, "Device Page Parameters":

<table>
<thead>
<tr>
<th>Volume Boost:</th>
<th>Set the Boost level to increase the volume output of the speaker. Using Volume Boost may introduce audio clipping or reduce intelligibility of the speaker audio. Boost will raise the volume above level 9, regardless of the digital volume settings.</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Volume Boost</td>
<td></td>
</tr>
<tr>
<td>Volume Boost 1</td>
<td></td>
</tr>
<tr>
<td>Volume Boost 2</td>
<td></td>
</tr>
<tr>
<td>Volume Boost 3</td>
<td></td>
</tr>
</tbody>
</table>

Browsers Supported

The following browsers have been tested against firmware version 11.8.0:

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

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

**Warning**

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

**Warning**

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

**Warning**

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

General Alert
This pictorial alert indicates a potentially hazardous situation. This alert will be followed by a hazard level heading and more specific information about the hazard.

Ground
This pictorial alert indicates the Earth grounding connection point.

Hazard Levels

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

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

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

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

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

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

## Chapter 1 Product Overview  
1.1 How to Identify This Product ..............................................................1  
1.2 Typical System Installation ...............................................................2  
1.3 Product Features ...............................................................................3  
1.4 Supported Protocols ..........................................................................4  
1.5 Supported SIP Servers .......................................................................4  
1.6 Specifications ....................................................................................5  
1.7 Typical Coverage ................................................................................6  
1.8 Compliance .........................................................................................6  
1.8.1 CE Testing .....................................................................................6  
1.8.2 FCC Statement ............................................................................6

## Chapter 2 Installing the SIP IP66 Outdoor Horn  
2.1 Parts List ..........................................................................................7  
2.2 SIP IP66 Outdoor Horn Setup .............................................................8  
2.2.1 SIP IP66 Outdoor Horn System Installation and Connection Options .................................................9  
2.2.2 Install the Network Cable Through Weatherproof Cable Gland .........................................................9  
2.2.3 Power Test and Status LED ............................................................10  
2.2.4 RTFM Switch ...............................................................................11  
2.3 Factory Default Settings .......................................................................14  
2.3.2 SIP IP66 Outdoor Horn Web Page Navigation ........................................15  
2.3.3 Using the Toggle Help Button .........................................................16  
2.3.4 Log in to the Home Page ...............................................................18  
2.3.5 Configure the Device ...................................................................22  
2.3.6 Configure the Network Parameters ............................................28  
2.3.7 Configure the SIP (Session Initiation Protocol) Parameters ................31  
2.3.8 Configure the Multicast Parameters ..........................................39  
2.3.9 Configure the Audiofiles Page Parameters ..................................43  
2.3.10 Configure the Events Parameters .............................................50  
2.3.11 Configure the Autoprovisioning Parameters ..............................55  
2.4.1 Downloading the Firmware .........................................................67  
2.4.2 Reboot the Device .......................................................................69  
2.5.1 Command Interface Post Commands ..........................................70

## Appendix A Mounting the Amplifier  
A.1 Dimensions .....................................................................................74

## Appendix B Setting up a TFTP Server  
B.1 Set up a TFTP Server ........................................................................75  
2.1.1 In a LINUX Environment .............................................................75  
2.1.2 In a Windows Environment .........................................................75

## Appendix C Troubleshooting/Technical Support  
C.1 Frequently Asked Questions (FAQ) ................................................76  
C.2 Documentation ................................................................................76  
C.3 Contact Information .........................................................................77  
C.4 Warranty and RMA Information .....................................................77

## Index  
78
1 Product Overview

1.1 How to Identify This Product

To identify the SIP IP66 Outdoor Horn (PoE), look for a model number label similar to the one shown in Figure 1-1. Confirm the following:

- The model number on the label should be 011457.

Figure 1-1. Model Number Label

![Image of model number label]

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.
1.2 Typical System Installation

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

**Figure 1-2. Typical Installation**

Compliant Non-PoE Ethernet Switch

- SIP IP66 Outdoor Horn
- VoIP Phone
- IP-PBX Server
1.3 Product Features

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

The SIP IP66 Outdoor Horn supports:

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

1.5 Supported SIP Servers

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

http://www.cyberdata.net/connecting-to-ip-pbx-servers/
## 1.6 Specifications

### Table 1-1. Specifications

<table>
<thead>
<tr>
<th>Specifications</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ethernet I/F</strong></td>
<td>10/100 Mbps</td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
<td>SIP RFC 3261 Compatible</td>
</tr>
<tr>
<td><strong>Power Input</strong></td>
<td>PoE 802.3at or 802.3af</td>
</tr>
<tr>
<td><strong>Audio Output</strong></td>
<td>802.3at: 107.7 (+/- 0.2) dBC @1M and 1kHz</td>
</tr>
<tr>
<td></td>
<td>802.3af: 104.8 (+/- 0.2) dBC @1M and 1kHz</td>
</tr>
<tr>
<td><strong>Operating Range</strong></td>
<td>Temperature: -40° C to 55° C (-40° F to 131° F)</td>
</tr>
<tr>
<td></td>
<td>Humidity: 5-95%, non-condensing</td>
</tr>
<tr>
<td><strong>Storage Temperature</strong></td>
<td>-40° C to 70° C (-40° F to 158° F)</td>
</tr>
<tr>
<td><strong>Storage Altitude</strong></td>
<td>Up to 15,000 ft. (4573 m)</td>
</tr>
<tr>
<td><strong>Payload Types</strong></td>
<td>G.711 a-law, G.711 u-law, and G.722, G.729</td>
</tr>
<tr>
<td><strong>Dimensions</strong>a</td>
<td>14.41 inches [366 mm] Length</td>
</tr>
<tr>
<td></td>
<td>10.71 inches [272 mm] Width</td>
</tr>
<tr>
<td></td>
<td>9.06 inches [230 mm] Height</td>
</tr>
<tr>
<td><strong>Weight</strong></td>
<td>6.6 lbs. [3 kg]</td>
</tr>
<tr>
<td><strong>Boxed Weight</strong></td>
<td>2.0 lbs. [0.90 kg]</td>
</tr>
<tr>
<td><strong>Compliance</strong></td>
<td>CE; EMC Directive – Class A EN 55032 &amp; EN 55024, LV</td>
</tr>
<tr>
<td></td>
<td>Safety Directive – EN 60950-1, RoHS Compliant, FCC; Part</td>
</tr>
<tr>
<td></td>
<td>15 Class A, Industry Canada; ICES-3 Class A, IEEE 802.3</td>
</tr>
<tr>
<td></td>
<td>Compliant</td>
</tr>
<tr>
<td><strong>Part Number</strong></td>
<td>011457</td>
</tr>
</tbody>
</table>

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

With one horn attached to Paging Amplifier under standard 802.3af PoE power, coverage is up to 5,000 square feet. With two horns attached to the Paging Amplifier under 802.3at PoE (high power), coverage is up to 10,000 square feet depending on ambient background noise levels.

1.8 Compliance

1.8.1 CE Testing

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

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

1.8.2 FCC Statement

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

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

<table>
<thead>
<tr>
<th>Quantity</th>
<th>Part Name</th>
<th>Illustration</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SIP IP66 Outdoor Horn Assembly</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Installation Quick Reference Guide</td>
<td></td>
</tr>
</tbody>
</table>

Table 2-2. Parts List
2.2 SIP IP66 Outdoor Horn Setup

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

CyberData delivers each SIP IP66 Outdoor Horn with the factory default values indicated in Table 2-3:

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Factory Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Addressing</td>
<td>DHCP</td>
</tr>
<tr>
<td>IP Address^a</td>
<td>10.10.10.10</td>
</tr>
<tr>
<td>Web Access Username</td>
<td>admin</td>
</tr>
<tr>
<td>Web Access Password</td>
<td>admin</td>
</tr>
<tr>
<td>Subnet Mask^a</td>
<td>255.0.0.0</td>
</tr>
<tr>
<td>Default Gateway^a</td>
<td>10.0.0.1</td>
</tr>
</tbody>
</table>

^a. Default if there is not a DHCP server present.
2.2.1 SIP IP66 Outdoor Horn System Installation and Connection Options

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

Figure 2-1. SIP IP66 Outdoor Horn Connections

**CLASS II WIRING**

- Mono(+)/Left Spkr (+) - 12
- Mono(-)/Right Spkr (-) - 9

**Internal Speaker Connections**

- White Speaker Cable to Circuit #12
- Black Speaker Cable to Circuit #9

2.2.2 Install the Network Cable Through Weatherproof Cable Gland

Install the network cable through weatherproof cable gland as shown in Figure 2-2.

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

- RJ45 Socket
- RJ45 Plug
- Weatherproof Network Cable Gland
- Cover Screw
- RTFM Access
2.2.3 Power Test and Status LED

1. Plug in the CyberData device and monitor the Status LED activity on the bottom side of the horn during the initialization process. See Figure 2-3.

Figure 2-3. Status LED

2. After about 20 seconds, the **GREEN Status** LED will blink fast to indicate that the device is acquiring an IP address and attempting to autoprovision. It will turn off thereafter until the device has finished booting. When the device has fully booted, the **GREEN Status** LED will turn on solid.

   If there is no DHCP server available on the network, it will try 12 times for 60 seconds and eventually fall back to the programmed static IP address (by default 10.10.10.10) or the previously used DHCP address if a prior lease was established. This process will take approximately 80 seconds.

3. When the device has completed the initialization process, pressing and holding the RTFM switch for a couple of seconds will announce the IP address. See Section 2.2.4, "RTFM Switch"

   This concludes the power test.
2.2.4 RTFM Switch

When the SIP IP66 Outdoor Horn is operational and linked to the network, use the Reset Test Function Management (RTFM) switch (Figure 2-5) (located behind the hole on the device) to announce and confirm the device’s IP Address and test the audio to verify that it is working.

2.2.4.1 RTFM Access

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

1. Remove the screw to gain access to the RTFM button (Figure 2-5).

Figure 2-4. RTFM Switch
2. Use a paper clip to feed through the hole to press the RTFM button. See Figure 2-5.

Figure 2-5. RTFM Switch
2.2.4.2 Announcing the IP Address

To announce a device’s current IP address:

- Use a bent paperclip or a similar object to press and hold the RTFM switch for a couple of seconds and then release it.

**Caution**

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

2.2.4.3 Restoring the Factory Default Settings

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

1. Use a bent paperclip or a similar object to press and hold the RTFM switch until you hear the device announce the words, “restoring defaults” and “rebooting”.

2. Release the RTFM switch. The device will be restored to the factory default settings.
2.3 Configure the SIP IP66 Outdoor Horn Parameters

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

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

2.3.1 Factory Default Settings

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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Factory Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Addressing</td>
<td>DHCP</td>
</tr>
<tr>
<td>IP Address(^a)</td>
<td>10.10.10.10</td>
</tr>
<tr>
<td>Web Access Username</td>
<td>admin</td>
</tr>
<tr>
<td>Web Access Password</td>
<td>admin</td>
</tr>
<tr>
<td>Subnet Mask(^a)</td>
<td>255.0.0.0</td>
</tr>
<tr>
<td>Default Gateway(^a)</td>
<td>10.0.0.1</td>
</tr>
</tbody>
</table>

\(^a\) Default if there is not a DHCP server present.
2.3.2 SIP IP66 Outdoor Horn Web Page Navigation

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

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home</td>
<td>Link to the Home page.</td>
</tr>
<tr>
<td>Device</td>
<td>Link to the Device page.</td>
</tr>
<tr>
<td>Network</td>
<td>Link to the Network page.</td>
</tr>
<tr>
<td>SIP</td>
<td>Link to go to the SIP page.</td>
</tr>
<tr>
<td>Multicast</td>
<td>Link to the Multicast page.</td>
</tr>
<tr>
<td>Audiofiles</td>
<td>Link to the Audiofiles page.</td>
</tr>
<tr>
<td>Events</td>
<td>Link to the Events page.</td>
</tr>
<tr>
<td>Autoprovisioning</td>
<td>Link to the Autoprovisioning page.</td>
</tr>
<tr>
<td>Firmware</td>
<td>Link to the Firmware page.</td>
</tr>
</tbody>
</table>
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](image)

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](image)
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 Home Page

1. Open your browser to the device IP address.

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

   **Note** Make sure that the PC is on the same IP network as the SIP IP66 Outdoor Horn.

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

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

   [http://www.cyberdata.net/assets/common/discovery.zip](http://www.cyberdata.net/assets/common/discovery.zip)

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

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

   Web Access Username: admin

   Web Access Password: admin
Figure 2-9. Home Page
3. On the **Home** page, review the setup details and navigation buttons described in Table 2-6.

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

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Admin Settings</strong></td>
<td><strong>Username</strong> The username to access the web interface. Enter up to 25 characters.</td>
</tr>
<tr>
<td></td>
<td><strong>Password</strong> The password to access the web interface. Enter up to 25 characters.</td>
</tr>
<tr>
<td></td>
<td><strong>Confirm Password</strong> Confirm the web interface password.</td>
</tr>
<tr>
<td><strong>Current Status</strong></td>
<td><strong>Serial Number</strong> Shows the device serial number.</td>
</tr>
<tr>
<td></td>
<td><strong>Mac Address</strong> Shows the device Mac address.</td>
</tr>
<tr>
<td></td>
<td><strong>Firmware Version</strong> Shows the current firmware version.</td>
</tr>
<tr>
<td></td>
<td><strong>IP Addressing</strong> Shows the current IP addressing setting (DHCP or static).</td>
</tr>
<tr>
<td></td>
<td><strong>IP Address</strong> Shows the current IP address.</td>
</tr>
<tr>
<td></td>
<td><strong>Subnet Mask</strong> Shows the current subnet mask address.</td>
</tr>
<tr>
<td></td>
<td><strong>Default Gateway</strong> Shows the current default gateway address.</td>
</tr>
<tr>
<td></td>
<td><strong>DNS Server 1</strong> Shows the current DNS Server 1 address.</td>
</tr>
<tr>
<td></td>
<td><strong>DNS Server 2</strong> Shows the current DNS Server 2 address.</td>
</tr>
<tr>
<td></td>
<td><strong>SIP Mode</strong> Shows the current status of the SIP mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Multicast Mode</strong> Shows the current status of the Multicast mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Event Reporting</strong> Shows the current status of the Event Reporting mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Nightringer</strong> Shows the current status of the Nightringer mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Primary SIP Server</strong> Shows the current status of the Primary SIP Server.</td>
</tr>
<tr>
<td></td>
<td><strong>Backup Server 1</strong> Shows the current status of Backup Server 1.</td>
</tr>
<tr>
<td></td>
<td><strong>Backup Server 2</strong> Shows the current status of Backup Server 2.</td>
</tr>
<tr>
<td></td>
<td><strong>Nightringer Server</strong> Shows the current status of Nightringer Server.</td>
</tr>
</tbody>
</table>

**Import Settings**

![Browse...](image)

Use this button to select a configuration file to import.

**Export Settings**

![Import Config](image)

After selecting a configuration file, click Import to import the configuration from the selected file. Then, click Save and Reboot to store changes.

![Export Config](image)

Click Export to export the current configuration to a file.

![Save](image)

Click the **Save** button to save your configuration settings. **Note:** You need to reboot for changes to take effect.
### Table 2-6. Home Page Overview (continued)

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reboot</strong></td>
<td>Click on the <strong>Reboot</strong> button to reboot the system.</td>
</tr>
<tr>
<td><strong>Toggle Help</strong></td>
<td>Click on the <strong>Toggle Help</strong> button to see a short description of some of the web page items. First click on the <strong>Toggle Help</strong> 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.</td>
</tr>
</tbody>
</table>
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**
2. On the **Device** page, you may enter values for the parameters indicated in Table 2-7.

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

**Table 2-7. Device Page Parameters**

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Volume Settings (0-9)</strong></td>
<td></td>
</tr>
<tr>
<td>SIP Volume</td>
<td>Set the speaker volume for a SIP call. A value of 0 will mute the speaker</td>
</tr>
<tr>
<td></td>
<td>during SIP calls.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You can change this setting without rebooting the device.</td>
</tr>
<tr>
<td>Multicast Volume</td>
<td>Set the speaker volume for multicast audio streams. A value of 0 will mute</td>
</tr>
<tr>
<td></td>
<td>the speaker during multicasts.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You can change this setting without rebooting the device.</td>
</tr>
<tr>
<td>Volume Boost:</td>
<td></td>
</tr>
<tr>
<td>No Volume Boost</td>
<td>Set the Boost level to increase the volume output of the speaker. Using</td>
</tr>
<tr>
<td></td>
<td>Volume Boost may introduce audio clipping or reduce intelligibility of the</td>
</tr>
<tr>
<td></td>
<td>speaker audio. Boost will raise the volume above level 9, regardless of</td>
</tr>
<tr>
<td></td>
<td>the digital volume settings.</td>
</tr>
<tr>
<td>Volume Boost 1</td>
<td></td>
</tr>
<tr>
<td>Volume Boost 2</td>
<td></td>
</tr>
<tr>
<td>Volume Boost 3</td>
<td></td>
</tr>
<tr>
<td><strong>Clock Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Set Time with NTP Server on boot</td>
<td>When selected, the time is set with an external NTP server when the device restarts.</td>
</tr>
<tr>
<td>NTP Server</td>
<td>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.</td>
</tr>
<tr>
<td>Posix Timezone String</td>
<td>See Section 2.3.5.1, &quot;Time Zone Strings&quot; for information about how to use the Posix Timezone String to specify time zone and daylight savings time where applicable. Enter up to 63 characters.</td>
</tr>
<tr>
<td>Periodically sync time with server</td>
<td>When selected, the time is periodically updated with the NTP server at the configured interval below.</td>
</tr>
<tr>
<td>Time update period (in hours)</td>
<td>The time interval after which the device will contact the NTP server to update the time. Enter up to 4 digits.</td>
</tr>
<tr>
<td>Current Time</td>
<td>Allows you to input the current time. (6 character limit)</td>
</tr>
<tr>
<td><strong>DTMF Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Require Security Code</td>
<td>When selected, the user will be prompted to enter a Security Code (entered on this page) before being able to execute a page when calling the device.</td>
</tr>
<tr>
<td>Security Code</td>
<td>Type the Security Code in this field. The Security Code must only use characters '0-9', '*', and '#'. Enter up to 25 characters.</td>
</tr>
<tr>
<td>Enable Stored Message Playback</td>
<td>When selected, the caller will be prompted to select one of nine stored messages to play through the speaker. Stored messages may be customized on the Audiofiles page.</td>
</tr>
<tr>
<td><strong>Power Settings</strong></td>
<td></td>
</tr>
</tbody>
</table>
### Table 2-7. Device Page Parameters (continued)

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>802.3AT Mode</strong></td>
<td>This device automatically detects if it is plugged into an 802.3AT (also known as PoE Plus) power source. 802.3AT provides more power than older 802.3AT power sources and allows this speaker to play audio at higher volumes. If you are sure this speaker is connected to an 802.3AT power source, but it is not being detected correctly, you can override the automatic settings below.</td>
</tr>
<tr>
<td>Force 802.3AT Mode (NOT recommended)</td>
<td>Enable this option if you are sure this speaker is connected to an 802.3AT power source, but it is not being detected correctly (not recommended).</td>
</tr>
<tr>
<td>Auxiliary Power Supply</td>
<td>This device can be connected to a +24VDC auxiliary power supply. Check this box if this is how this speaker is being powered.</td>
</tr>
<tr>
<td><strong>Misc Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Device Name</td>
<td>Type the device name. Enter up to 25 characters.</td>
</tr>
<tr>
<td>Beep on Init</td>
<td>Device will play the user-defined “pagetone” audio file when it boots.</td>
</tr>
<tr>
<td>Beep on Page</td>
<td>Device will play the user defined “pagetone” audio file before playing a SIP page.</td>
</tr>
<tr>
<td>Disable HTTPS (NOT recommended)</td>
<td>Disables the encrypted connection to the webpage. We do not recommend disabling HTTPS for security reasons.</td>
</tr>
<tr>
<td><strong>Test Audio</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Save</strong></td>
<td>Click the Save button to save your configuration settings.</td>
</tr>
<tr>
<td><strong>Reboot</strong></td>
<td>Click on the Reboot button to reboot the system.</td>
</tr>
<tr>
<td><strong>Toggle Help</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

**Note** You must click on the **Save** button and then the **Reboot** button for the changes to take effect.
### 2.3.5.1 Time Zone Strings

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

<table>
<thead>
<tr>
<th>Time Zone</th>
<th>Time Zone String</th>
</tr>
</thead>
<tbody>
<tr>
<td>US Pacific time</td>
<td>PST8PDT,M3.2.0/2:00:00,M11.1.0/2:00:00</td>
</tr>
<tr>
<td>US Mountain time</td>
<td>MST7MDT,M3.2.0/2:00:00,M11.1.0/2:00:00</td>
</tr>
<tr>
<td>US Eastern Time</td>
<td>EST5EDT,M3.2.0/2:00:00,M11.1.0/2:00:00</td>
</tr>
<tr>
<td>Phoenix Arizona(^a)</td>
<td>MST7</td>
</tr>
<tr>
<td>US Central Time</td>
<td>CST6DST,M3.2.0/2:00:00,M11.1.0/2:00:00</td>
</tr>
</tbody>
</table>

\(^a\) Phoenix, Arizona does not use daylight savings time.

Table 2-20 shows a breakdown of the parts that constitute the following time zone string:

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

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

Table 2-21 has some more examples of time zone strings.

Table 2-10. Time Zone String Examples

<table>
<thead>
<tr>
<th>Time Zone</th>
<th>Time Zone String</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tokyo³¹</td>
<td>IST-9</td>
</tr>
<tr>
<td>Berlin⁵²</td>
<td>CET-1MET,M3.5.0/1:00,M10.5.0/1:00</td>
</tr>
</tbody>
</table>

³ Tokyo does not use daylight savings time.
⁵ For Berlin, daylight savings time starts on the last Sunday in March at 01:00 UTC, and ends on the last Sunday in October at 01:00 UTC, and is one hour ahead of UTC.

Time Zone Identifier

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

Figure 2-11. Three or Four Character Time Zone Identifier

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


World GMT Table

Table 2-22 has information about the GMT time in various time zones.

Table 2-11. World GMT Table

<table>
<thead>
<tr>
<th>Time Zone</th>
<th>City or Area Zone Crosses</th>
</tr>
</thead>
<tbody>
<tr>
<td>GMT-12</td>
<td>Eniwetok</td>
</tr>
<tr>
<td>GMT-11</td>
<td>Samoa</td>
</tr>
<tr>
<td>GMT-10</td>
<td>Hawaii</td>
</tr>
<tr>
<td>GMT-9</td>
<td>Alaska</td>
</tr>
<tr>
<td>GMT-8</td>
<td>PST, Pacific US</td>
</tr>
<tr>
<td>GMT-7</td>
<td>MST, Mountain US</td>
</tr>
<tr>
<td>GMT-6</td>
<td>CST, Central US</td>
</tr>
<tr>
<td>GMT-5</td>
<td>EST, Eastern US</td>
</tr>
<tr>
<td>GMT-4</td>
<td>Atlantic, Canada</td>
</tr>
<tr>
<td>GMT-3</td>
<td>Brazilia, Buenos Aries</td>
</tr>
<tr>
<td>GMT-2</td>
<td>Mid-Atlantic</td>
</tr>
<tr>
<td>GMT-1</td>
<td>Cape Verdes</td>
</tr>
<tr>
<td>GMT</td>
<td>Greenwich Mean Time, Dublin</td>
</tr>
<tr>
<td>GMT+1</td>
<td>Berlin, Rome</td>
</tr>
<tr>
<td>GMT+2</td>
<td>Israel, Cairo</td>
</tr>
<tr>
<td>GMT+3</td>
<td>Moscow, Kuwait</td>
</tr>
<tr>
<td>GMT+4</td>
<td>Abu Dhabi, Muscat</td>
</tr>
<tr>
<td>GMT+5</td>
<td>Islamabad, Karachi</td>
</tr>
<tr>
<td>Time Zone</td>
<td>City or Area Zone Crosses</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>GMT+6</td>
<td>Almaty, Dhaka</td>
</tr>
<tr>
<td>GMT+7</td>
<td>Bangkok, Jakarta</td>
</tr>
<tr>
<td>GMT+8</td>
<td>Hong Kong, Beijing</td>
</tr>
<tr>
<td>GMT+9</td>
<td>Tokyo, Osaka</td>
</tr>
<tr>
<td>GMT+10</td>
<td>Sydney, Melbourne, Guam</td>
</tr>
<tr>
<td>GMT+11</td>
<td>Magadan, Solomon Is.</td>
</tr>
<tr>
<td>GMT+12</td>
<td>Fiji, Wellington, Auckland</td>
</tr>
</tbody>
</table>
2.3.6 Configure the Network Parameters

1. Click the **Network** menu button to open the **Network** page (Figure 2-12).

**Figure 2-12. Network Page**
2. On the **Network** page, enter values for the parameters indicated in **Table 2-12**.

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

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Stored Network Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Addressing Mode</td>
<td>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 <strong>Section 2.3.1, &quot;Factory Default Settings&quot;</strong> for factory default settings. Be sure to click <strong>Save</strong> and <strong>Reboot</strong> to store changes when configuring a Static address.</td>
</tr>
<tr>
<td>Hostname</td>
<td>This is the hostname provided by the DHCP server. See the DHCP/DNS server documentation for more information. Enter up to 64 characters.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the Static IPv4 network address in dotted decimal notation.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Enter the Subnet Mask in dotted decimal notation.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Enter the Default Gateway IPv4 address in dotted decimal notation.</td>
</tr>
<tr>
<td>DNS Server 1</td>
<td>Enter the primary DNS Server IPv4 address in dotted decimal notation.</td>
</tr>
<tr>
<td>DNS Server 2</td>
<td>Enter the secondary DNS Server IPv4 address in dotted decimal notation.</td>
</tr>
<tr>
<td>DHCP Timeout in seconds</td>
<td>Specify the desired time-out duration (in seconds) that the device will wait for a response from the DHCP server before reverting back to the stored static IP address. The stored static IP address may be the last known IP address or the factory default address if no prior DHCP lease was established. Enter up to 8 characters. A value of -1 will retry forever.</td>
</tr>
<tr>
<td><strong>Current Network Settings</strong></td>
<td>Shows the current network settings.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Shows the current Static IP address.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Shows the current Subnet Mask address.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Shows the current Default Gateway address.</td>
</tr>
<tr>
<td>DNS Server 1</td>
<td>Shows the current DNS Server 1 address.</td>
</tr>
<tr>
<td>DNS Server 2</td>
<td>Shows the current DNS Server 2 address.</td>
</tr>
<tr>
<td><strong>VLAN Settings</strong></td>
<td></td>
</tr>
<tr>
<td>VLAN ID (0-4095)</td>
<td>Specify the IEEE 802.1Q VLAN ID number. Enter up to 4 digits.</td>
</tr>
<tr>
<td><strong>Note</strong>: 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.</td>
<td></td>
</tr>
<tr>
<td>VLAN Priority (0-7)</td>
<td>Specify the IEEE 802.1p VLAN priority level. Enter 1 digit. A value of 0 may cause the VLAN ID tag to be ignored.</td>
</tr>
</tbody>
</table>
Table 2-12. Network Page Parameters (continued)

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

**Note** You must click on the **Save** button and then the **Reboot** button for the changes to take effect.
2.3.7 Configure the SIP (Session Initiation Protocol) Parameters

1. Click on the SIP menu button to open the SIP page (Figure 2-13).

Figure 2-13. SIP Page
2. On the **SIP** page, enter values for the parameters indicated in **Table 2-13**.

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

**Table 2-13. SIP Page Parameters**

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SIP Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Enable SIP Operation (?)</td>
<td>When enabled, the device will transmit, receive, and process SIP messages according to the configured SIP settings below.</td>
</tr>
<tr>
<td>SIP Transport Protocol (?)</td>
<td>Choose the transport protocol for SIP signaling. This will affect all extensions, including the Nightringer. Default is UDP.</td>
</tr>
<tr>
<td>Register with a SIP Server (?)</td>
<td>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 <strong>SIP Operation</strong> and disable <strong>Register with a SIP Server</strong> (see <strong>Section 2.3.7.2, “Point-to-Point Configuration”</strong>).</td>
</tr>
<tr>
<td>Use Cisco SRST (?)</td>
<td>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.</td>
</tr>
<tr>
<td>Primary SIP Server (?)</td>
<td>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.</td>
</tr>
<tr>
<td>Primary SIP User ID (?)</td>
<td>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.</td>
</tr>
<tr>
<td>Primary SIP Auth ID (?)</td>
<td>Specify the Authenticate ID for the Primary SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.</td>
</tr>
<tr>
<td>Primary SIP Auth Password (?)</td>
<td>Specify the Authenticate Password for the Primary SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.</td>
</tr>
<tr>
<td>Backup SIP Server 1 (?)</td>
<td>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.</td>
</tr>
<tr>
<td>Backup SIP User ID 1 (?)</td>
<td>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.</td>
</tr>
<tr>
<td>Backup SIP Auth ID 1 (?)</td>
<td>Specify the Authenticate ID for the first backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.</td>
</tr>
<tr>
<td>Backup SIP Auth Password 1 (?)</td>
<td>Specify the Authenticate Password for the first backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.</td>
</tr>
</tbody>
</table>
### Table 2-13. SIP Page Parameters (continued)

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup SIP Server 2</td>
<td>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.</td>
</tr>
<tr>
<td>Backup SIP User ID 2</td>
<td>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.</td>
</tr>
<tr>
<td>Backup SIP Auth ID 2</td>
<td>Specify the Authenticate ID for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.</td>
</tr>
<tr>
<td>Backup SIP Auth Password 2</td>
<td>Specify the Authenticate Password for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.</td>
</tr>
<tr>
<td>Remote SIP Port</td>
<td>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.</td>
</tr>
<tr>
<td>Local SIP Port</td>
<td>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.</td>
</tr>
<tr>
<td>Outbound Proxy</td>
<td>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.</td>
</tr>
<tr>
<td>Outbound Proxy Port</td>
<td>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.</td>
</tr>
<tr>
<td>Disable rport Discovery</td>
<td>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.</td>
</tr>
<tr>
<td>Buffer SIP Calls</td>
<td>Also referred to as delayed paging. Device will buffer up to 4 minutes of audio then play back the recording after hang up.</td>
</tr>
<tr>
<td>Re-registration Interval (in seconds)</td>
<td>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.</td>
</tr>
<tr>
<td>Unregister on Boot</td>
<td>When enabled, the device will send one registration with an expiry of 0 on boot.</td>
</tr>
<tr>
<td>Keep Alive Period</td>
<td>The minimum time in milliseconds between keep-alive packets sent for nat traversal. A value of 0 will disable keep alive packets.</td>
</tr>
</tbody>
</table>

### Nightringer Settings

| Enable Nightringer | When Nightringer is enabled, the device will attempt to register a second extension with the SIP server. Any calls made to this extension will play a ringtone (corresponds to Night Ring on the Audiofiles page). By design, it is not possible to answer a call to the Nightringer extension. |
### Table 2-13. SIP Page Parameters (continued)

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SIP Server</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Remote SIP Port</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Local SIP Port</strong></td>
<td>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 <strong>Local SIP Port</strong> for the primary extension. The default Local SIP Port is 5061. The supported range is 0-65536. Enter up to 5 digits.</td>
</tr>
<tr>
<td><strong>Outbound Proxy</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Outbound Proxy Port</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>User ID</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Authenticate ID</strong></td>
<td>Specify the Authenticate ID for the SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.</td>
</tr>
<tr>
<td><strong>Authenticate Password</strong></td>
<td>Specify the Authenticate Password for the SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.</td>
</tr>
<tr>
<td><strong>Re-registration Interval (in seconds)</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>RTP Settings</strong></td>
<td></td>
</tr>
<tr>
<td><strong>RTP Port (even)</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Jitter Buffer</strong></td>
<td>Specify the size of the jitter buffer (in milliseconds) used for SIP calls. Valid values are 50-1000.</td>
</tr>
<tr>
<td><strong>Call Disconnection</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Terminate Call After Delay</strong></td>
<td>Automatically terminate an active call after a given delay in seconds. A value of 0 will disable this function. Enter up to 8 digits.</td>
</tr>
<tr>
<td><strong>Codec Selection</strong></td>
<td></td>
</tr>
</tbody>
</table>
Table 2-13. SIP Page Parameters (continued)

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Force Selected Codec?</td>
<td>When configured, this option will allow you to force the device to negotiate for the selected codec. Otherwise, the device will perform codec negotiation using the default list of supported codecs.</td>
</tr>
<tr>
<td>Codec ?</td>
<td>Select the desired codec (only one may be chosen).</td>
</tr>
<tr>
<td></td>
<td>Click the <strong>Save</strong> button to save your configuration settings. <strong>Note:</strong> You need to reboot for changes to take effect.</td>
</tr>
<tr>
<td></td>
<td>Click on the <strong>Reboot</strong> button to reboot the system.</td>
</tr>
<tr>
<td></td>
<td>Click on the <strong>Toggle Help</strong> button to see a short description of some of the web page items. First click on the <strong>Toggle Help</strong> 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.</td>
</tr>
</tbody>
</table>

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

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

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

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

<table>
<thead>
<tr>
<th>Extension String</th>
<th>Resulting Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>302</td>
<td>Dial out extension 302 and establish a call</td>
</tr>
<tr>
<td>302,2</td>
<td>Dial out extension 302 and establish a call, wait 3 seconds then send the DTMF tone '2'</td>
</tr>
<tr>
<td>302,25,,4,,1</td>
<td>Dial out extension 302 and establish a call, wait 3 seconds then send the DTMF tone '2', send out DTMF tone 5, wait 6 seconds, send out DTMF tone 4, wait 4 seconds, send out DTMF tone 1</td>
</tr>
</tbody>
</table>

**Note** The maximum number of total characters in the dial-out field is 64.
2.3.7.2 Point-to-Point Configuration

When the device is set to not register with a SIP server (see Figure 2-14), it is possible to set the device to dial out to a single endpoint.

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

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

Figure 2-14. SIP Page Set to Point-to-Point Mode
2.3.7.3 Delayed DTMF

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

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

<table>
<thead>
<tr>
<th>Extension String</th>
<th>Resulting Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>302</td>
<td>Dial out extension 302 and establish a call</td>
</tr>
<tr>
<td>302,2</td>
<td>Dial out extension 302 and establish a call, wait 3 seconds then send the DTMF tone ‘2’</td>
</tr>
<tr>
<td>302,2,4,1</td>
<td>Dial out extension 302 and establish a call, wait 3 seconds then send the DTMF tone ‘2’, send out DTMF tone 5, wait 6 seconds, send out DTMF tone 4, wait 4 seconds, send out DTMF tone 1</td>
</tr>
</tbody>
</table>

Note: The maximum number of total characters in the dial-out field is 25.
2.3.8 Configure the Multicast Parameters

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

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

Each multicast group is assigned a priority, allowing simultaneously arriving pages to be serviced based on importance. Multicast groups are compatible with IGMP through version 3. The device supports simultaneous SIP and Multicast.
1. Click on the **Multicast** menu button to open the **Multicast** page. See **Figure 2-15**.

**Figure 2-15. Multicast Page**
2. On the Multicast page, enter values for the parameters indicated in Table 2-16.

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

### Table 2-16. Multicast Page Parameters

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Multicast Operation</td>
<td>Enables or disables multicast operation.</td>
</tr>
<tr>
<td>Priority</td>
<td>Indicates the priority for the multicast group. Priority 9 is the highest (emergency streams). 0 is the lowest (background music). SIP calls are considered priority 4.5. See Section 2.3.8.1, “Assigning Priority” for more details.</td>
</tr>
<tr>
<td>Address</td>
<td>Enter the multicast IP Address for this multicast group (15 character limit).</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port number for this multicast group (5 character limit [range can be from 2000 to 65535]).</td>
</tr>
<tr>
<td>Name</td>
<td>Assign a descriptive name for this multicast group (25 character limit).</td>
</tr>
<tr>
<td>Buffer</td>
<td>Device will buffer up to four minutes of audio and then play back the recording after the multicast stream finishes or after the buffer is full.</td>
</tr>
<tr>
<td>Beep</td>
<td>When selected, the device will play a beep before multicast audio is sent.</td>
</tr>
<tr>
<td>Polycom Default Channel</td>
<td>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.</td>
</tr>
<tr>
<td>Polycom Priority Channel</td>
<td>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.</td>
</tr>
<tr>
<td>Polycom Emergency Channel</td>
<td>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.</td>
</tr>
</tbody>
</table>

Click the **Save** button to save your configuration settings.

**Note**: You need to reboot for changes to take effect.

Click on the **Reboot** button to reboot the system.

Click on the **Toggle Help** button to see a short description of some of the web page items. First click on the **Toggle Help** button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.
Note You must click on the Save button and then the Reboot button for the changes to take effect.

2.3.8.1 Assigning Priority

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

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

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

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

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

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

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

   **Figure 2-16. Audiofiles Page**

   ![CyberData Outdoor Horn](image)
Figure 2-17. Audiofiles Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Current Setting</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dot</td>
<td>Currently set to default</td>
<td>Browse... No file chosen Play Delete Save</td>
</tr>
<tr>
<td>Audio Test</td>
<td>Currently set to default</td>
<td>Browse... No file chosen Play Delete Save</td>
</tr>
<tr>
<td>Enter Code</td>
<td>Currently set to default</td>
<td>Browse... No file chosen Play Delete Save</td>
</tr>
<tr>
<td>Invalid Code</td>
<td>Currently set to default</td>
<td>Browse... No file chosen Play Delete Save</td>
</tr>
<tr>
<td>Page Tone</td>
<td>Currently set to default</td>
<td>Browse... No file chosen Play Delete Save</td>
</tr>
<tr>
<td>Your IP Address To</td>
<td>Currently set to default</td>
<td>Browse... No file chosen Play Delete Save</td>
</tr>
<tr>
<td>Rebooting</td>
<td>Currently set to default</td>
<td>Browse... No file chosen Play Delete Save</td>
</tr>
<tr>
<td>Restoring Default</td>
<td>Currently set to default</td>
<td>Browse... No file chosen Play Delete Save</td>
</tr>
<tr>
<td>Ring Tone</td>
<td>Currently set to default</td>
<td>Browse... No file chosen Play Delete Save</td>
</tr>
<tr>
<td>Sensor Triggered</td>
<td>Currently set to default</td>
<td>Browse... No file chosen Play Delete Save</td>
</tr>
<tr>
<td>Night Ring</td>
<td>Currently set to default</td>
<td>Browse... No file chosen Play Delete Save</td>
</tr>
</tbody>
</table>
Figure 2-18. Audiofiles Page

Menu Audio Files

- Cancel: Currently set to default
- Currently Playing: Currently set to default
- Invalid Entry: Currently set to default
- Page: Currently set to default
- Play Stored Message: Currently set to default
- Pound (#): Currently set to default
- Press: Currently set to default
- Stored Message: Currently set to default
- Through: Currently set to default
- To: Currently set to default

Options: Browse, No file chosen, Play, Delete, Save
2. On the **Audiofiles** page, enter values for the parameters indicated in **Table 2-17**.

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

**Table 2-17. Audiofiles Page Parameters**

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available Space</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Stored Messages</strong></td>
<td></td>
</tr>
<tr>
<td>Stored Message 1 through 9</td>
<td><strong>Stored Message 1</strong> corresponds to the message played after pressing 1 on a phone keypad. <strong>Stored Message 2</strong> corresponds to the message played after pressing 2 on a phone keypad. <strong>Stored Message 3</strong> corresponds to the message played after pressing 3 on a phone keypad. <strong>Stored Message 4</strong> corresponds to the message played after pressing 4 on a phone keypad. <strong>Stored Message 5</strong> corresponds to the message played after pressing 5 on a phone keypad. <strong>Stored Message 6</strong> corresponds to the message played after pressing 6 on a phone keypad. <strong>Stored Message 7</strong> corresponds to the message played after pressing 7 on a phone keypad. <strong>Stored Message 8</strong> corresponds to the message played after pressing 8 on a phone keypad. <strong>Stored Message 9</strong> corresponds to the message played after pressing 9 on a phone keypad.</td>
</tr>
<tr>
<td>Dot</td>
<td>Corresponds to the spoken word “dot.” (24 character limit)</td>
</tr>
<tr>
<td>Audio Test</td>
<td>Corresponds to the message “This is the CyberData IP speaker test message...” (24 character limit)</td>
</tr>
<tr>
<td>Enter Code</td>
<td>Corresponds to the message “Enter Code” (24 character limit).</td>
</tr>
<tr>
<td>Invalid Code</td>
<td>Corresponds to the message “Invalid Code” (24 character limit).</td>
</tr>
<tr>
<td>Page Tone</td>
<td>Corresponds to a simple tone used for beep on initialization and beep on page (24 character limit).</td>
</tr>
<tr>
<td>Your IP Address is</td>
<td>Corresponds to the message “Your IP address is...” (24 character limit).</td>
</tr>
<tr>
<td>Rebooting</td>
<td>Corresponds to the spoken word “Rebooting” (24 character limit).</td>
</tr>
<tr>
<td>Restoring Default</td>
<td>Corresponds to the message “Restoring default” (24 character limit).</td>
</tr>
<tr>
<td>Ring Tone</td>
<td>This is the tone that plays when set to ring when receiving a call (24 character limit).</td>
</tr>
<tr>
<td>Sensor Triggered</td>
<td>Corresponds to the message “Sensor Triggered” (24 character limit).</td>
</tr>
<tr>
<td>Night Ring</td>
<td>Specifies the ringtone for nightring. By default this parameter uses the same audio file that is selected for the <strong>Ring Tone</strong> parameter.</td>
</tr>
<tr>
<td><strong>Menu Audio Files</strong></td>
<td><strong>Menu Audio Files</strong> are user-uploadable messages that create the audio menu played to the caller.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Corresponds to the word &quot;Cancel&quot; used in the audio menu played to the caller. (24 character limit).</td>
</tr>
<tr>
<td>Currently Playing</td>
<td>Corresponds to the words &quot;Currently Playing&quot; used in the audio menu played to the caller. (24 character limit).</td>
</tr>
<tr>
<td>Invalid Entry</td>
<td>Corresponds to the words &quot;Invalid Entry&quot; used in the audio menu played to the caller. (24 character limit).</td>
</tr>
<tr>
<td>Page</td>
<td>Corresponds to the word &quot;Page&quot; used in the audio menu played to the caller. (24 character limit).</td>
</tr>
</tbody>
</table>
Table 2-17. Audiofiles Page Parameters (continued)

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Play Stored Message</td>
<td>Corresponds to the words &quot;Play Stored Message&quot; used in the audio menu played to the caller. (24 character limit).</td>
</tr>
<tr>
<td>Pound (#)</td>
<td>Corresponds to whatever word or phrase the user wishes to call the pound key in the audio menu played to the caller (24 character limit).</td>
</tr>
<tr>
<td>Press</td>
<td>Corresponds to the word &quot;Press&quot; used in the audio menu played to the caller. (24 character limit).</td>
</tr>
<tr>
<td>Stored Message</td>
<td>Corresponds to the words &quot;Stored Message&quot; used in the audio menu played to the caller. (24 character limit).</td>
</tr>
<tr>
<td>Through</td>
<td>Corresponds to the word &quot;Through&quot; used in the audio menu played to the caller. (24 character limit).</td>
</tr>
<tr>
<td>To</td>
<td>Corresponds to the word &quot;To&quot; used in the audio menu played to the caller. (24 character limit).</td>
</tr>
</tbody>
</table>

Click on the Browse button to navigate to and select an audio file.

The Play button will play that audio file.

The Delete button will delete any user uploaded audio and restore the stock audio file.

The Save button will download a new user audio file to the board once you've selected the file by using the Browse button. The Save button will delete any pre-existing user-uploaded audio files.
2.3.9.1 User-created Audio Files

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

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

You can use the free utility Audacity to convert audio files into this format. See Figure 2-19 through Figure 2-21.

Figure 2-19. Audacity 1

![Figure 2-19. Audacity 1](image)

Figure 2-20. Audacity 2

![Figure 2-20. Audacity 2](image)
When you export an audio file with Audacity, save the output as:

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

Figure 2-21. WAV (Microsoft) signed 16 bit PCM
2.3.10 Configure the Events Parameters

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

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

**Figure 2-22. Event Page**

![CyberData Outdoor Horn events page](image)
2. On the **Events** page, enter values for the parameters indicated in **Table 2-18**.

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

### Table 2-18. Events Page Parameters

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Event Generation ?</td>
<td>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.</td>
</tr>
<tr>
<td>Enable Call Start Events ?</td>
<td>When selected, the device will report the start of a SIP call.</td>
</tr>
<tr>
<td>Enable Call Terminated Events ?</td>
<td>When selected, the device will report the end of a SIP call.</td>
</tr>
<tr>
<td>Enable Night Ring Events ?</td>
<td>When selected, the device will report when it starts ringing upon an incoming SIP call to the Nightringer extension. As a reminder, the Nightringer extension always rings upon an incoming SIP call and it is not possible to alter this behavior.</td>
</tr>
<tr>
<td>Enable Power On Events ?</td>
<td>When selected, the device will report when it boots.</td>
</tr>
<tr>
<td>Enable Multicast Start Events ?</td>
<td>When selected, the device will report when the device starts playing a multicast audio stream.</td>
</tr>
<tr>
<td>Enable Multicast Stop Events ?</td>
<td>When selected, the device will report when the device stops playing a multicast audio stream.</td>
</tr>
<tr>
<td>Enable 60 Second Heartbeat Events ?</td>
<td>When enabled, the device will report a Heartbeat event every 60 seconds. SIP registration is not required to generate Heartbeat events.</td>
</tr>
<tr>
<td>Check All</td>
<td>Click on <strong>Check All</strong> to select all of the events on the page.</td>
</tr>
<tr>
<td>Uncheck All</td>
<td>Click on <strong>Uncheck All</strong> to de-select all of the events on the page.</td>
</tr>
<tr>
<td>Server IP Address ?</td>
<td>The IPv4 address of the event server in dotted decimal notation.</td>
</tr>
<tr>
<td>Server Port ?</td>
<td>Specify the event server port number. The supported range is 0-65536. Enter up to 5 digits.</td>
</tr>
<tr>
<td>Server URL ?</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Save**

Click the **Save** button to save your configuration settings.

**Note**: You need to reboot for changes to take effect.

**Reboot**

Click on the **Reboot** button to reboot the system.

**Toggle Help**

Click on the **Toggle Help** button to see a short description of some of the web page items. First click on the **Toggle Help** button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.
2.3.10.1 Example Packets for Events

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

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

Here are example packets for every event:

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

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

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

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

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

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

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

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData Device' MAC='0020f70015b6'>
<event>LONGPRESS</event>
</cyberdata>
```
<event>CALL_ACTIVE</event>
</cyberdata>
POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 205
Content-Type: application/x-www-form-urlencoded

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

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

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

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

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

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

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

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

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

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

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

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

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

1. Click the **Autoprov** menu button to open the **Autoprovisioning** page. See Figure 2-23.

![Autoprovisioning Page](image)

**Figure 2-23. Autoprovisioning Page**
2. On the **Autoprovisioning** page, you may enter values for the parameters indicated in Table 2-19.

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

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable Autoprovisioning</td>
<td>Prevent the device from automatically trying to download a configuration file. See Section 2.3.11.1, “Autoprovisioning” for more information.</td>
</tr>
<tr>
<td>Autoprovisioning Server</td>
<td>Enter the IPv4 address of the provisioning server in dotted decimal notation.</td>
</tr>
<tr>
<td>Autoprovisioning Filename</td>
<td>The autoprovisioning filename is the configuration filename. The default autoprovisioning filename is in the format of <code>&lt;mac address&gt;.xml</code>.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Use tftp</td>
<td>The device will use TFTP (instead of http) to download autoprovisioning files.</td>
</tr>
<tr>
<td>Username</td>
<td>The username used to authenticate with an autoprovisioning server. Leave this field blank to disable authentication.</td>
</tr>
<tr>
<td>Password</td>
<td>The password used to authenticate with an autoprovisioning server. Leave this field blank to disable authentication.</td>
</tr>
<tr>
<td>Autoprovisioning Autoupdate (in minutes)</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Note</strong>: To use the auto update options, enable the Set Time with NTP Server on boot setting on the Device Page page (see Table 2-7).</td>
<td></td>
</tr>
<tr>
<td>Autoprovision at time (HHMMSS)</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Note</strong>: To use the auto update options, enable the Set Time with NTP Server on boot setting on the Device Page page (see Table 2-7).</td>
<td></td>
</tr>
<tr>
<td>Autoprovision when idle (in minutes &gt; 10)</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Note</strong>: To use the auto update options, enable the Set Time with NTP Server on boot setting on the Device Page page (see Table 2-7).</td>
<td></td>
</tr>
</tbody>
</table>

Click the **Save** button to save your configuration settings.

**Note**: You need to reboot for changes to take effect.
2.3.11.1 Autoprosionning

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

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

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

By default, the device will get its autoprovisioning server from the DHCP options. See Section 2.3.11.2, "Sample dhcpd.conf" for an example of how to configure dhcpd to offer autoprovisioning server addresses. If multiple options are set, the device will attempt to download autoprovisioning files from every server.

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

1. Option 43 - a FQDN or an IP address to an http server
2. Option 72 - an IP address to an http server
3. Option 150 - an IP address to a tftp server
4. Option 66 - an IP address to a tftp server or if the entry starts with 'http', a FQDN to a http server.
You can download an autoprovisioning template file from the Autoprovisioning Page using the Download Template button (see Table 2-19). This file contains every configuration option that can be set on the board.

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

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

```xml
  <MiscSettings>
    <DeviceName>CyberData Device</DeviceName>
    <!--    <AutoprovFile>common.xml</AutoprovFile>-->  
    <!--    <AutoprovFile>sip_reg[macaddress].xml</AutoprovFile>-->  
    <!--    <AutoprovFile>audio[macaddress].xml</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
<?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 can contain a file, a file path, or a directory.

### Table 2-20. Autoprovisioning File Name

<table>
<thead>
<tr>
<th>Autoprovisioning Filename</th>
<th>Autoprovisioning Server</th>
<th>File Downloaded</th>
</tr>
</thead>
<tbody>
<tr>
<td>config.xml</td>
<td>10.0.1.3</td>
<td>10.0.1.3/config.xml</td>
</tr>
<tr>
<td>/path/to/config.xml</td>
<td>10.0.1.3</td>
<td>10.0.1.3/path/to/config.xml</td>
</tr>
<tr>
<td>subdirectory/path/</td>
<td>10.0.1.3</td>
<td>10.0.1.3/subdirectory/path/0020f7020002.xml</td>
</tr>
</tbody>
</table>

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/0000000cd.xml

Audio files and firmware files will also add “cyberdata” to the URL before downloading.
The device 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>
```
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**

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

**sip_common.xml**

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

**sip_0020f7020001.xml**

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

**sip_0020f7020002.xml**

```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 Autoprovised**.

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**
  ```xml
  <MiscSettings>
  <AutoprovFile>common_settings.xml</AutoprovFile>
  </MiscSettings>
  <SIPSettings>
  <SIPUserID>198</SIPUserID>
  <SIPAuthPassword>ext198</SIPAuthPassword>
  <DialoutExtension0>204</DialoutExtension0>
  </SIPSettings>
  
  0020f7020002.xml
  ```

- **0020f7020002.xml**
  ```xml
  <MiscSettings>
  <AutoprovFile>common_settings.xml</AutoprovFile>
  </MiscSettings>
  <SIPSettings>
  <SIPUserID>500</SIPUserID>
  <SIPAuthPassword>ext500</SIPAuthPassword>
  <DialoutExtension0>555</DialoutExtension0>
  </SIPSettings>
  
  common_settings.xml
  ```

- **common_settings.xml**
  ```xml
  <MiscSettings>
  <DeviceName>CyberData Autoprovisioned</DeviceName>
  </MiscSettings>
  <SIPSettings>
  <SIPServer>10.0.0.253</SIPServer>
  <RemoteSIPPort>5060</RemoteSIPPort>
  </SIPSettings>
  
  1. On boot, Device1 downloads **0020f7020001.xml** from **10.0.1.3** and imports these values. The SIP User ID is **198**, the password is **ext198**, and the dialout extension is **204**.

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

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

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

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

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

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

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

From the common file, a pointer to sip_common.xml

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

Autoprovisioned Audio Files

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

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

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

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

ddns-update-style none;

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

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

  option routers                  10.0.0.1;
  option subnet-mask              255.0.0.0;

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

  option time-offset              -8;             # Pacific Standard Time

  # option www-server             99.99.99.99;    # OPTION 72
  # option tftp-server-name       "10.0.1.52";      # OPTION 66
  # option tftp-server-name       "http://test.cyberdata.net"; # OPTION 66

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

  range 10.10.0.1 10.10.2.1; }
```
2.3.11.3 Download Template Button

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

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

1. On the **Autoprovisioning** page, click on the **Download Template** button.

2. You will see a window prompting you to save a configuration file (.xml) to a location on your computer (Figure 2-24). 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 2-24.

   ![Figure 2-24. Configuration File](image)

4. At this point, you can open and edit the autoprovisioning template to change the configuration settings in the template for the unit.

5. You can then upload the autoprovisioning file to a TFTP or HTTP server where the file can be loaded onto other devices.
2.4 Upgrade the Firmware and Reboot the SIP IP66 Outdoor Horn

2.4.1 Downloading the Firmware

To download the firmware to your computer:

1. Download the latest firmware file from the Downloads tab at the following webpage:
   http://www.cyberdata.net/voip/011457/

2. Unzip the firmware version file. This file may contain the following:
   - Firmware file
   - Release notes

3. Log in to the home page as instructed in Section 2.3.4, "Log in to the Home Page”.

4. Click on the Firmware menu button to open the Firmware page. See Figure 2-25.

   **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 2-25. Firmware Page**

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

6. Select the firmware file.

7. Click on the **Upload** button.

   **Note**  Do not reboot the device after clicking on the **Upload** button.
Installing the SIP IP66 Outdoor Horn

Note
This starts the upgrade process. Once the SIP IP66 Outdoor Horn has uploaded the file, the Uploading Firmware countdown page appears, indicating that the firmware is being written to flash. The SIP IP66 Outdoor Horn will automatically reboot when the upload is complete. When the countdown finishes, the Firmware page will refresh. The uploaded firmware filename should be displayed in the system configuration (indicating a successful upload and reboot).

8. Table 2-21 shows the web page items on the Firmware page.

Table 2-21. Firmware Parameters

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Firmware Version</td>
<td>Shows the current firmware version.</td>
</tr>
<tr>
<td></td>
<td>Use the Browse button to navigate to the location of the firmware file that you want to upload.</td>
</tr>
<tr>
<td></td>
<td>Click on the Upload button to automatically upload the selected firmware and reboot the system.</td>
</tr>
</tbody>
</table>
2.4.2 Reboot the Device

To reboot a SIP IP66 Outdoor Horn, log in to the web page as instructed in Section 2.3.4, "Log in to the Home Page".

1. Click on the Reboot button on the Home page (Figure 2-26). A normal restart will occur.

Figure 2-26. Home Page
2.5 Command Interface

Some functions on the device can be activated using simple POST commands to the web interface. The examples in Table 2-22 use the free unix utility, *wget*, but any program that can send http POST commands to the device should work.

### 2.5.1 Command Interface Post Commands

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

<table>
<thead>
<tr>
<th>Device Action</th>
<th>HTTP Post Command</th>
</tr>
</thead>
</table>
| Trigger relay (for configured delay)   | wget --user admin --password admin --auth-no-challenge --no-
|                                        | check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-
|                                        | bin/command.cgi" --post-data "test_relay=yes"          |
| Place call to extension (example: extension 130) | wget --user admin --password admin --auth-no-challenge --no-
|                                        | check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-
|                                        | bin/command.cgi" --post-data "call=130"                |
| Terminate active call                  | wget --user admin --password admin --auth-no-challenge --no-
|                                        | check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-
|                                        | bin/command.cgi" --post-data "terminate=yes"           |
| Force reboot                           | wget --user admin --password admin --auth-no-challenge --no-
|                                        | check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-
|                                        | bin/command.cgi" --post-data "reboot=yes"              |
| Test Audio button                      | wget --user admin --password admin --auth-no-challenge --no-
|                                        | check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-
|                                        | bin/command.cgi" --post-data "test_audio=yes"          |
| Announce IP address                    | wget --user admin --password admin --auth-no-challenge --no-
|                                        | check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-
|                                        | bin/command.cgi" --post-data "speak_ip_address=yes"    |
| Play the "0" audio file                | wget --user admin --password admin --auth-no-challenge --no-
|                                        | check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-
|                                        | bin/audiofiles.cgi" --post-data "play_0=yes"           |
| Play the "1" audio file                | wget --user admin --password admin --auth-no-challenge --no-
|                                        | check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-
|                                        | bin/audiofiles.cgi" --post-data "play_1=yes"           |
| Play the "2" audio file                | wget --user admin --password admin --auth-no-challenge --no-
|                                        | check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-
|                                        | bin/audiofiles.cgi" --post-data "play_2=yes"           |
| Play the "3" audio file                | wget --user admin --password admin --auth-no-challenge --no-
|                                        | check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-
|                                        | bin/audiofiles.cgi" --post-data "play_3=yes"           |
| Play the "4" audio file                | wget --user admin --password admin --auth-no-challenge --no-
|                                        | check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-
|                                        | bin/audiofiles.cgi" --post-data "play_4=yes"           |
## Table 2-22. Command Interface Post Commands (continued)

<table>
<thead>
<tr>
<th>Device Action</th>
<th>HTTP Post Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Play the &quot;5&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;play_5=yes&quot;</code></td>
</tr>
<tr>
<td>Play the &quot;6&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;play_6=yes&quot;</code></td>
</tr>
<tr>
<td>Play the &quot;7&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;play_7=yes&quot;</code></td>
</tr>
<tr>
<td>Play the &quot;8&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;play_8=yes&quot;</code></td>
</tr>
<tr>
<td>Play the &quot;9&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;play_9=yes&quot;</code></td>
</tr>
<tr>
<td>Play the &quot;Dot&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;play_d=yes&quot;</code></td>
</tr>
<tr>
<td>Play the &quot;Audio Test&quot; audio file (from Audio Config)</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;play_audiotest=yes&quot;</code></td>
</tr>
<tr>
<td>Play the &quot;Page Tone&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;play_pagetone=yes&quot;</code></td>
</tr>
<tr>
<td>Play the &quot;Your IP Address Is&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;play_youripaddressis=yes&quot;</code></td>
</tr>
<tr>
<td>Play the &quot;Rebooting&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;play_rebooting=yes&quot;</code></td>
</tr>
<tr>
<td>Play the &quot;Restoring Default&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;play_restoringdefault=yes&quot;</code></td>
</tr>
<tr>
<td>Play the &quot;Ringback tone&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;play_ringback=yes&quot;</code></td>
</tr>
<tr>
<td>Play the &quot;Ring tone&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;play_ringtone=yes&quot;</code></td>
</tr>
<tr>
<td>Play the &quot;Night Ring&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;play_nightring=yes&quot;</code></td>
</tr>
<tr>
<td>Delete the &quot;0&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;delete_0=yes&quot;</code></td>
</tr>
<tr>
<td>Delete the &quot;1&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;delete_1=yes&quot;</code></td>
</tr>
<tr>
<td>Device Action</td>
<td>HTTP Post Command</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Delete the &quot;2&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;delete_2=yes&quot;</code></td>
</tr>
<tr>
<td>Delete the &quot;3&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;delete_3=yes&quot;</code></td>
</tr>
<tr>
<td>Delete the &quot;4&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;delete_4=yes&quot;</code></td>
</tr>
<tr>
<td>Delete the &quot;5&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;delete_5=yes&quot;</code></td>
</tr>
<tr>
<td>Delete the &quot;6&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;delete_6=yes&quot;</code></td>
</tr>
<tr>
<td>Delete the &quot;7&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;delete_7=yes&quot;</code></td>
</tr>
<tr>
<td>Delete the &quot;8&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;delete_8=yes&quot;</code></td>
</tr>
<tr>
<td>Delete the &quot;9&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;delete_9=yes&quot;</code></td>
</tr>
<tr>
<td>Delete the &quot;Audio Test&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;delete_audiotest=yes&quot;</code></td>
</tr>
<tr>
<td>Delete the &quot;Page Tone&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;delete_pagetone=yes&quot;</code></td>
</tr>
<tr>
<td>Delete the &quot;Your IP Address Is&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;delete_youripaddressis=yes&quot;</code></td>
</tr>
<tr>
<td>Delete the &quot;Rebooting&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;delete_rebooting=yes&quot;</code></td>
</tr>
<tr>
<td>Delete the &quot;Restoring Default&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;delete_restoringdefault=yes&quot;</code></td>
</tr>
<tr>
<td>Delete the &quot;Ringback tone&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;delete_ringback=yes&quot;</code></td>
</tr>
<tr>
<td>Delete the &quot;Ring tone&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;delete_ringtone=yes&quot;</code></td>
</tr>
<tr>
<td>Delete the &quot;Night Ring&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;delete_nightring=yes&quot;</code></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Device Action</th>
<th>HTTP Post Commanda</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trigger the Door Sensor Test (Sensor Config page)</td>
<td>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;<a href="https://10.0.3.71/cgi-bin/sensor.cgi">https://10.0.3.71/cgi-bin/sensor.cgi</a>&quot; --post-data &quot;doortest=yes&quot;</td>
</tr>
</tbody>
</table>

---

a. Type and enter all of each http POST command on one line.
Appendix A: Mounting the Amplifier

A.1 Dimensions

Figure A-1. Dimensions

- Dimensions (in millimeters):
  - Mounting holes: 3 places
  - Diameter: 6.772
  - Height: 14.404
  - Width: 6.730
  - Status LED: 9.291
  - Mounting holes fit thread size up to 3/8" or M10 fasteners

- Dimensions (in inches):
  - Diameter: 0.263
  - Height: 0.568
  - Width: 0.263
  - Status LED: 0.364

- Notes:
  - Mounting holes fit thread size up to 3/8" or M10 fasteners.
Appendix B: Setting up a TFTP Server

B.1 Set up a TFTP Server

Autoprosvisioning requires a TFTP server for hosting the configuration file.

2.1.1 In a LINUX Environment

To set up a TFTP server on LINUX:

1. Create a directory dedicated to the TFTP server, and move the files to be uploaded to that directory.

2. Run the following command where /tftpboot/ is the path to the directory you created in Step 1: the directory that contains the files to be uploaded. For example:

   in.tftpd -l -s /tftpboot/your_directory_name

2.1.2 In a Windows Environment

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

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

To set up a TFTP server on Windows:

1. Install and start the software.


3. Make a note of the default directory name, and then move the firmware files to be uploaded to that directory.
Appendix C: Troubleshooting/Technical Support

C.1 Frequently Asked Questions (FAQ)

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

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

C.2 Documentation

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

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

http://www.cyberdata.net/voip/011457/
## C.3 Contact Information

| Contact       | CyberData Corporation  
|               | 3 Justin Court  
|               | Monterey, CA 93940 USA  
|               | [www.CyberData.net](http://www.CyberData.net)  
|               | Phone: 800-CYBERDATA (800-292-3732)  
|               | Fax: 831-373-4193  
| Sales         | Sales 831-373-2601, Extension 334  
| Technical Support | The fastest way to get technical support for your VoIP product is to submit a VoIP Technical Support form at the following website:  
|               | [http://support.cyberdata.net/](http://support.cyberdata.net/)  
|               | The Support Form initiates a ticket which CyberData uses for tracking customer requests. Most importantly, the Support Form tells us which PBX system and software version that you are using, the make and model of the switch, and other important information. This information is essential for troubleshooting. Please also include as much detail as possible in the **Comments** section of the Support Form.  
|               | Phone: (831) 373-2601, Extension 333  

## C.4 Warranty and RMA Information

The most recent warranty and RMA information is available at the following website address:  
[http://support.cyberdata.net/](http://support.cyberdata.net/)
Index

A
address, configuration login 18
announcing an IP address 13
audio configuration 43
    night ring tone parameter 46
audio encodings 4
audio files, user-created 48
audio page 43
audio test 11
autoprovision at time (HHMMSS) 56
autoprovision when idle (in minutes > 10) 56
autoprovisioning 57
    download template button 57
autoprovisioning autoupdate (in minutes) 56
autoprovisioning configuration 55, 56
autoprovisioning filename 56
autoprovisioning server (IP Address) 56

B
backup SIP server 1 32
backup SIP server 2 32
backup SIP servers, SIP server backups 32

C
changing the web access password 22
Cisco SRST 32
command interface 70
commands 70
configurable parameters 32
configuration
    audio 43
    default IP settings 14
    network 28
    SIP 31
configuration home page 18
connection options 9
connections 9
contact information 77
contact information for CyberData 77
current network settings 29
CyberData contact information 77

d
default
    gateway 8, 14
    IP address 8, 14
    subnet mask 8, 14
    username and password 8, 14
    web login username and password 18
default gateway 8, 14, 29
default IP settings 14
default login address 18
device configuration 22
device configuration page 22
device configuration parameters 23
device configuration password
    changing for web configuration access 22
DHCP Client 4
dial out extension strings 36
dial-out extension strings 38
dimensions 5, 74
discovery utility program 18
DNS server 29
door sensor 46
download autoprovisioning template button 57
DTMF tones 36, 38
DTMF tones (using rfc2833) 36

E
enable night ring events 51
enclosure, mounting 74
ethernet I/F 5
event configuration
    enable night ring events 51
expiration time for SIP server lease 33, 34
export settings 20

F
factory defaults 13
firmware
    where to get the latest firmware 67

G
get autoprovisioning template 57
GMT table 26
GMT time 26

H
hazard levels 5
home page 18
http POST command 70
http web-based configuration 4

I
identifier names (PST, EDT, IST, MUT) 26
identifying your product 1
import settings 20
import/export settings 20
installation 2
IP address 8, 14, 29
IP address announcement 13
IP address confirmation 11
IP addressing
  default
  IP addressing setting 8, 14

L
lease, SIP server expiration time 33, 34
lengthy pages 42
Linux, setting up a TFTP server on 75
local SIP port 33
log in address 18

M
MGROUP
  MGROUP Name 41
multicast configuration 39, 43
Multicast IP Address 41

N
navigation (web page) 15
navigation table 15
network configuration 28
nightring tones 42
Nightringer 66
nightringer settings 33

P
packet time 4
pages (lengthy) 42
parts list 7
password
  for SIP server login 32
  login 18
  restoring the default 8, 14
payload types 5
point-to-point configuration 37
polycom default channel 41
polycom emergency channel 41
polycom priority channel 41
port
  local SIP 33
  remote SIP 33
posix timezone string
timezone string 23
POST command 70
power input 5
priority
  assigning 42
product
  parts list 7
product features 3
product overview
  product features 3
  product specifications 5
supported protocols 4
supported SIP servers 4
typical system installation 2
product specifications 5
protocols supported 4

R
reboot 68, 69
remote SIP port 33
reset test function management switch 11
resetting the IP address to the default 74
restoring the factory defaults 13
ringtones 42
  lengthy pages 42
rport discovery setting, disabling 33
RTFM switch 11
RTP/AVP 4
S
safety instructions 4
sales 77
server address, SIP 32
service 77
set time with external NTP server on boot 23
SIP
  enable SIP operation 32
  local SIP port 33
  user ID 32
SIP (session initiation protocol) 4
SIP configuration 31
SIP configuration parameters
  outbound proxy 33, 34
  registration and expiration, SIP server lease 33, 34
  unregister on reboot 33
  user ID, SIP 32
SIP registration 32
SIP remote SIP port 33
SIP server 32
  password for login 32
  SIP servers supported 4
  unregister from 33
  user ID for login 32
SIP server configuration 32
SIP volume 23
SRST 32
subnet mask 8, 14, 29
supported protocols 4

V
VLAN ID 29
VLAN Priority 29
VLAN tagging support 29
VLAN tags 29
volume
  multicast volume 23
  SIP volume 23

W
warranty policy at CyberData 77
web access password 8, 14
web access username 8, 14
web configuration log in address 18
web page
  navigation 15
web page navigation 15
wget, free unix utility 70
Windows, setting up a TFTP server on 75

T
technical support, contact information 77
test audio 11
TFTP server 4, 75
time zone string examples 26

U
user ID
  for SIP server login 32
username
  changing for web configuration access 22
  default for web configuration access 18
  restoring the default 8, 14