VoIP Outdoor Intercom
Operations Guide

Part #011186
Document Part #931293A
for Firmware Version 11.6.0

CyberData Corporation
3 Justin Court
Monterey, CA 93940
(831) 373-2601
COPYRIGHT NOTICE:
© 2016, 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 931293A, which corresponds to firmware version 11.6.0, was released on September 8, 2016, and has the following changes since document 930796T:

- Adds Section 2.3.3.4, "Connecting the Networked Dual Door Strike Intermediate Relay"
- Adds Section 2.3.3.5, "Connecting the Networked Dual Door Strike Intermediate Relay—12V Out"
- Updates Figure 2-3, "Devices Less than 1A at 30 VDC"
- Updates Figure 2-4, "Door Strike Intermediate Relay Wiring Diagram"
- Updates Figure 2-5, "Networked Door Strike Intermediate Relay Wiring Diagram"
- Updates Figure 2-8, "Connector Locations"
- Updates Figure 2-9, "Connector Locations"
- Updates Figure 2-10, "Activity and Link LED"
- Updates Figure 2-11, "RTFM Button"
- Updates Figure 2-12, "RTFM Button"
- Updates Figure 2-13, "RTFM Button"
- Updates Figure 2-18, "Home Page"
- Updates Figure 2-18, "Home Page"
- Updates Figure 2-19, "Device Configuration Page"
- Updates Table 2-7, "Device Configuration Parameters"
- Updates Figure 2-22, "SIP Configuration Page"
- Updates Table 2-13, "SIP Configuration Parameters"
- Updates Figure 2-23, "SIP Page Set to Point-to-Point Mode"
- Updates Figure 2-24, "Multicast Configuration Page"
- Updates Figure 2-37, "Firmware Page"
- Updates Figure 2-38, "Home Page"

Browsers Supported

The following browsers have been tested against firmware version 11.6.0:

- Internet Explorer (version: 10)
- Firefox (also called Mozilla Firefox) (version: 23.0.1 and 25.0)
- Chrome (version: 29.0.1547.66 m)
- Safari (version: 5.1.7)
Pictorial Alert Icons

<table>
<thead>
<tr>
<th>General Alert</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ground</th>
</tr>
</thead>
<tbody>
<tr>
<td>This pictorial alert indicates the Earth grounding connection point.</td>
</tr>
</tbody>
</table>

Hazard Levels

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

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

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

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

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

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

14. **WARNING:** The VoIP Intercom enclosure is not rated for any AC voltages!

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

1.1 How to Identify This Product

To identify the VoIP Outdoor Intercom, 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 **011186**.
- The serial number on the label should begin with **1861**.

![Model Number Label](image)

**Figure 1-1. Model Number Label**
1.2 Typical System Installation

The Voice-over-IP (VoIP) Intercom is a SIP endpoint designed to provide VoIP phone connectivity in a tamper-proof and secure package.

The following figures illustrate how the device can be installed as part of a VoIP phone system.

**Figure 1-2. Typical Installation—Door Strike Intermediate Relay Module**

**Figure 1-3. Typical Installation—Networked Door Strike Intermediate Relay Module**
Figure 1-4. Typical Installation—Networked Dual Door Strike Intermediate Relay Module

Figure 1-5. Typical Installation—Mass Notification

Figure 1-6. Typical Installation—Emergency Phone
1.3 Product Features

The VoIP Outdoor Intercom has the following features:

- Separately configurable volume and mic gain for push-to-talk operation
- Supports SRST (Survivable Remote Site Telephony) in a Cisco environment. SRST parameters are entered statically into the CyberData product's internal webpage.
- SIP
- Dual speeds of 10 Mbps and 100 Mbps
- 802.3af compliant
- 2 gang outlet box size
- Adaptive full duplex voice operation
- Network/Web management
- Network adjustable speaker volume adjustment
- Network configurable door or intrusion sensor settings
- Network configurable relay activation settings
- Dial Out Extension supports the addition of comma delimited pauses before sending additional DTMF tones
- Network configurable microphone input sensitivity adjustment
- Network downloadable product firmware
- Doubles as a paging speaker
- Call button
- Call activity indicator (light)
- Tamper proof design
- One dry contact relay for auxiliary control
- Autoprovisioning
- Configurable audio files
- Night Ringer
- Peer-to-peer capable
- Door closure and tamper alert signal
- Optional Torx screws with driver kit
- An active call is indicated by the Call Button LED blinking at one second intervals.
1.4 Supported Protocols

The Intercom supports the following protocols:

- **SIP (session initiation protocol)**
- **HTTP Web-based configuration**
  Provides an intuitive user interface for easy system configuration and verification of Intercom operations.
- **DHCP Client**
  Dynamically assigns IP addresses in addition to the option to use static addressing.
- **TFTP Client**
  Facilitates hosting for the Autoprovisioning configuration file.
- **RTP**
- **RTP/AVP - Audio Video Profile**
- **Facilitates autoprovisioning configuration values on boot**
- **Audio Encodings**
  - PCMU (G.711 mu-law)
  - PCMA (G.711 A-law)
  - G.722
  - Packet Time 20 ms

1.5 Supported SIP Servers

The following link contains information on how to configure the device 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>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet I/F</td>
<td>10/100 Mbps</td>
</tr>
<tr>
<td>Protocol</td>
<td>SIP RFC 3261 Compatible</td>
</tr>
<tr>
<td>Power Input</td>
<td>PoE 802.3af compliant or +8 to +12VDC @ 1000mA Regulated Power Supply&lt;sup&gt;a&lt;/sup&gt;</td>
</tr>
<tr>
<td>Speaker Output</td>
<td>1 Watt Peak Power</td>
</tr>
<tr>
<td>On-Board Relay</td>
<td>1A at 30 VDC</td>
</tr>
<tr>
<td>Operating Temperature</td>
<td>-10° C to 50° C (14° F to 122° F)</td>
</tr>
<tr>
<td>Payload Types</td>
<td>G711, A-law and μ-law</td>
</tr>
<tr>
<td>Regulatory Compliance</td>
<td>FCC Class A, UL 60950-1 / UL 60065-1</td>
</tr>
<tr>
<td>Dimensions&lt;sup&gt;b&lt;/sup&gt;</td>
<td>5.118 inches [130 mm] Length</td>
</tr>
<tr>
<td></td>
<td>2.252 inches [57.21 mm] Width</td>
</tr>
<tr>
<td></td>
<td>5.118 inches [130 mm] Height</td>
</tr>
<tr>
<td>Weight</td>
<td>2.0 lbs. (0.90 kg)</td>
</tr>
<tr>
<td>Boxed Weight</td>
<td>3.0 lbs. (1.36 kg)</td>
</tr>
<tr>
<td>Part Number</td>
<td>011186</td>
</tr>
<tr>
<td></td>
<td>011188 Weather Shroud (sold separately)</td>
</tr>
</tbody>
</table>

<sup>a</sup> Contacts 1 and 2 on the J3 terminal block are only for powering the device from a non-PoE 12VDC power source as an alternative to Network PoE power. Use of these contacts for any other purpose will damage the device and void the product warranty.

<sup>b</sup> Dimensions are measured from the perspective of the product being upright with the front of the product facing you.
2 Installing the VoIP Outdoor Intercom

2.1 Parts List

Table 2-1 illustrates the VoIP Outdoor Intercom parts.

**Note**  See Appendix A, "Mounting the Intercom" for physical mounting information.

<table>
<thead>
<tr>
<th>Table 2-1. Parts List</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Quantity</strong></td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>1</td>
</tr>
</tbody>
</table>
2.2 Intercom Components

Figure 2-1 shows the components of the Intercom.

Figure 2-1. Intercom Components

- Microphone Hole
- Speaker Drain Hole
- Call Button

See Section 2.3.8, "Call Button and the Call Button LED" for information about the functionality of the Call Button.
2.3 Intercom Setup

2.3.1 Intercom Connections

Figure 2-2 shows the pin connections on the terminal block. This terminal block can accept 16 AWG gauge wire.

**Note**  As an alternative to using PoE power, you can supply +8 to +12VDC @ 1000mA Regulated Power Supply into the terminal block.

**Caution**  
_Equipment Hazard:_ Contacts 1 and 2 on the terminal block are only for powering the device from a non-PoE 12 VDC power source as an alternative to Network PoE power. Use of these contacts for any other purpose will damage the device and void the product warranty.

**Figure 2-2. Intercom Connections**

<table>
<thead>
<tr>
<th>Alternate Power Input:</th>
<th>1 = +8 to +12VDC @ 1000mA Regulated Power Supply*</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2 = Power Ground*</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Relay Contact:</th>
<th>(1 A at 30 VDC for continuous loads)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 = Relay Common</td>
<td></td>
</tr>
<tr>
<td>4 = Relay Normally Open Contact</td>
<td></td>
</tr>
<tr>
<td>5 = Door Sense Input</td>
<td></td>
</tr>
<tr>
<td>6 = Door Sense Common</td>
<td></td>
</tr>
<tr>
<td>7 = Alternate Call Button Sense Input</td>
<td></td>
</tr>
<tr>
<td>8 = Alternate Call Button Sense Common</td>
<td></td>
</tr>
</tbody>
</table>

*Contacts 1 and 2 on the J3 terminal block are only for powering the device from a non-PoE 12VDC power source as an alternative to Network PoE power. Use of these contacts for any other purpose will damage the device and void the product warranty.
2.3.2 Using the On-Board Relay

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

Warning
**Electrical Hazard:** The relay contacts are dry and provided for a normally open and momentarily closed configuration. Neither the alternate power input nor PoE power can be used to drive a door strike.

Warning
**Electrical Hazard:** The relay does not support AC powered door strikes. Any use of this relay beyond its normal operating range can cause damage to the product and is not covered under our warranty policy.

The device has a built-in relay that can be activated by a web configurable DTMF string that can be received from a VoIP phone supporting out of band (RFC2833) DTMF as well as a number of other triggering events. See the [Device Configuration Page](#) on the web interface for relay settings.

This relay can be used to trigger low current devices like LED strobes and security camera input signals as long as the load is not an inductive type and the relay is limited to a maximum of 1 Amp @ 30 VDC. Inductive loads can cause excessive “hum” and can interfere with or damage the unit's electronics.

We highly recommend that inductive load and high current devices use our Door Strike Intermediate Relay product (CD# 011269) (see Section 2.3.3.2, “Connecting the Door Strike Intermediate Relay Module”).

This relay interface also has a general purpose input port that can be used to monitor an external switch and generate an event.

For more information on the sensor options, see the [Sensor Configuration Page](#) on the web interface.
2.3.3 Wiring the Circuit

2.3.3.1 Devices Less than 1A at 30 VDC

If the power for the device is less than 1A at 30 VDC and is not an inductive load, then see Figure 2-3 for the wiring diagram.

When configuring with an inductive load, please use an intermediary relay with a High PIV Ultrafast Switching Diode. We recommend using the CyberData Networked Dual Door Strike Intermediate Relay Module (CD# 011375) (see Section 2.3.3.4, "Connecting the Networked Dual Door Strike Intermediate Relay").

Figure 2-3. Devices Less than 1A at 30 VDC

- DC Source
- Sense Input
- LED Strobe Light
- Pin 3 - Relay Common
- Pin 4 - Relay Normally Open Contact
- Pin 5 - Sense Input
- Pin 6 - Sense Ground

The J3 terminal block can accept 16 AWG stranded wire.

The J3 terminal block can accept 16 AWG stranded wire.
2.3.3.2 Connecting the Door Strike Intermediate Relay Module

For wiring an electronic door strike, we recommend the use of our external Door Strike Intermediate Relay (CD# 011269).

This product provides an easier method of connecting standard door strikes as well as AC and higher voltage devices. See Figure 2-4 for the wiring diagram.

**Figure 2-4. Door Strike Intermediate Relay Wiring Diagram**

If you have questions about connecting door strikes or setting up the web configurable options, please contact our support department at the following website:

[http://support.cyberdata.net/](http://support.cyberdata.net/)
2.3.3.3 Connecting the Networked Door Strike Intermediate Relay

For wiring an electronic door strike to work over a network, we recommend the use of our external Networked Door Strike Intermediate Relay (CD# 011270).

This product provides an easier method of connecting standard door strikes as well as AC and higher voltage devices. See Figure 2-5 for the wiring diagram.

Figure 2-5. Networked Door Strike Intermediate Relay Wiring Diagram

If you have questions about connecting door strikes or setting up the web configurable options, please contact our support department at the following website:

http://support.cyberdata.net/
2.3.3.4 Connecting the Networked Dual Door Strike Intermediate Relay

For wiring an electronic door strike to work over a network, we recommend the use of our external Networked Dual Door Strike Intermediate Relay (CD# 011375).

This product provides an easier method of connecting standard door strikes as well as AC and higher voltage devices. See Figure 2-6 and Figure 2-7 (for 12V Out) for the wiring diagrams.

**Warning**

*Electrical Hazard:* Hazardous voltages may be present. No user serviceable part inside. Refer to qualified service personnel for connecting or servicing.

**Figure 2-6. Networked Dual Door Strike Intermediate Relay Wiring Diagram**

The relay connection maximum wire size is 12 gauge stranded wire.

*Equipment Hazard:* The door strike must have an internal or external MOV or diode (for over voltage protection) when connecting directly to the module.


See Section 2.4.12, "Configure the Door Strike Relay" for configuration options.
2.3.3.5 Connecting the Networked Dual Door Strike Intermediate Relay—12V Out

Figure 2-7. Networked Dual Door Strike Intermediate Relay Wiring Diagram—12V Out

The relay connection maximum wire size is 12 gauge stranded wire.

If you have questions about connecting door strikes or setting up the web configurable options, please contact our support department at the following website:

http://support.cyberdata.net/

*Caution

Equipment Hazard: The door strike must have an internal or external MOV or diode (for over voltage protection) when connecting directly to the module.


See Section 2.4.12, "Configure the Door Strike Relay" for configuration options.
2.3.4 Intercom Connectors

See the following figures and tables to identify the connectors and functions of the Intercom.

Figure 2-8. Connector Locations

Table 2-2. Connector Functions

<table>
<thead>
<tr>
<th>Connector</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>JBTN</td>
<td>Call Button LED Interface</td>
</tr>
<tr>
<td>JMIC1</td>
<td>Microphone Interface</td>
</tr>
<tr>
<td>JSPKR</td>
<td>Speaker Interface</td>
</tr>
<tr>
<td>JKPAD</td>
<td>Keypad Interface — Not Used</td>
</tr>
<tr>
<td>JX</td>
<td>Auxiliary Strobe Connector</td>
</tr>
<tr>
<td>JY</td>
<td>Proximity Sensor Interface — Not Used</td>
</tr>
<tr>
<td>JP10</td>
<td>Disables the intrusion sensor when installed.</td>
</tr>
<tr>
<td>JBT1</td>
<td>Touch Button -1 Interface — Not Used</td>
</tr>
<tr>
<td>JBT2</td>
<td>Touch Button -2 Interface — Not Used</td>
</tr>
</tbody>
</table>
Figure 2-9. Connector Locations

Table 2-3. Connector Functions

<table>
<thead>
<tr>
<th>Connector</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>JP1</td>
<td>Reset jumper&lt;sup&gt;a&lt;/sup&gt;</td>
</tr>
<tr>
<td>J1</td>
<td>PoE Network Connection (RJ-45 ethernet)</td>
</tr>
<tr>
<td>JAEC</td>
<td>AEC Configuration Interface (Factory Use Only)</td>
</tr>
<tr>
<td>JIO</td>
<td>Terminal Block (see Figure 2-2)</td>
</tr>
<tr>
<td>JCON</td>
<td>Console Port (Factory Use Only)</td>
</tr>
<tr>
<td>JTAG</td>
<td>JTAG (Factory Use Only)</td>
</tr>
<tr>
<td>JSPI</td>
<td>Reserved (Factory Use Only)</td>
</tr>
<tr>
<td>SW1</td>
<td>See Section 2.3.6, &quot;RTFM Button&quot;*</td>
</tr>
</tbody>
</table>

<sup>a</sup>Do not install a jumper. Momentary short to reset. Permanent installation of a jumper would prevent the board from running all together.
2.3.5 Activity and Link LEDs

2.3.5.1 Verifying the Network Connectivity and Data Rate

When you plug in the Ethernet cable or power supply to the Intercom, the following occurs:

- The square, **YELLOW Link/Activity** LED blinks when there is network activity (see Figure 2-10).
- The square, **GREEN 100Mb Link** LED above the Ethernet port indicates that the network connection has been established (see Figure 2-10).

![Figure 2-10. Activity and Link LED](image-url)
2.3.6 RTFM Button

When the Intercom is operational and linked to the network, you can use the Reset Test Function Management (RTFM) button (see SW1 in Figure 2-11) on the Intercom board to announce and confirm the Intercom's IP Address and test to see if the audio is working.

**Note** You must do these tests prior to final assembly.

Figure 2-11. RTFM Button
2.3.6.1 Announcing the IP Address

To announce a device's current IP address:

1. Press and release the RTFM button (see SW1 in Figure 2-12) within a five second window.

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

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

*Figure 2-12. RTFM Button*
2.3.6.2 Restoring the Factory Default Settings

When troubleshooting configuration problems, it is sometimes convenient to restore the device to a known state.

**Note**  Each Intercom is delivered with factory set default values.

To restore the factory default settings:

1. Press and hold the **RTFM button** (see SW1 in Figure 2-13) for more than five seconds.
2. The device announces that it is restoring the factory default settings.

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

---

**Figure 2-13. RTFM Button**

---

2.3.7 Adjusting the Intercom Volume

You can adjust the Intercom volume through the **SIP Volume**, **Multicast Volume**, **Ring Volume**, and **Sensor Volume** settings on the **Device Configuration Page**.
2.3.8 Call Button and the Call Button LED

2.3.8.1 Calling with the Call Button

- You may initiate a call by pressing the Call button.
- An active call is indicated by the Call Button LED blinking at one second intervals.
- The Intercom can automatically answer an incoming call.
- You can press the Call Button to terminate an active call.

2.3.8.2 Call Button LED Function

- Upon initial power or reset, the Call Button LED will illuminate.
- On boot, the Call Button LED will flash ten times a second while setting up the network and downloading autoprovisioning files.
- The device “autoprovisions” by default, and the initial process may take several minutes as the device searches for and downloads updates. The Call Button LED will blink during this process. During the initial provisioning, or after the factory defaults have been reset, the device may download firmware twice. The device will blink, remain solid for 10 to 20 seconds, and then resume blinking. This process will take longer if there are many audio files downloading.
- When the software has finished initialization, the Call Button LED will blink twice.
- When a call is established (not just ringing), the Call Button LED will blink.
- On the Device Configuration Page (see Section 2.4.5, “Configure the Device”), there is an option called Button Lit When Idle. This option sets the normal state for the indicator LED. The Call Button LED will still blink during initialization and calls.
- The Call Button LED flashes briefly at the beginning of RTFM mode.

Figure 2-14. Call Button and Call Button LED
2.4 Configure the Intercom Parameters

To configure the Intercom online, use a standard web browser.

Configure each Intercom and verify its operation before you mount it. When you are ready to mount an Intercom, refer to Appendix A, “Mounting the Intercom” for instructions.

2.4.1 Factory Default Settings

All Intercoms are initially configured with the following default IP settings:

When configuring more than one Intercom, attach the Intercoms 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.
### 2.4.2 Intercom Web Page Navigation

Table 2-5 shows the navigation buttons that you will see on every Intercom 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>Sensor</td>
<td>Link to the Sensor 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>DSR</td>
<td>Link to the Door Strike Relay 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>
2.4.3 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 2-15** and **Figure 2-16**.

**Figure 2-15. Toggle/Help Button**

2. You will see a question mark (❓) appear next to each webpage item that has been provided with a short description by the Help feature. See **Figure 2-16**.

**Figure 2-16. Toggle Help Button and Question Marks**
3. Move the mouse pointer to hover over the question mark (?), and a short description of the web page item will appear. See Figure 2-17.

Figure 2-17. Short Description Provided by the Help Feature
2.4.4 Log in to the Configuration Home Page

1. Open your browser to the Intercom 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 Intercom.

   **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 Intercom 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 2-18):

   Web Access Username: **admin**
   Web Access Password: **admin**
Figure 2-18. 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 2-6. Home Page Overview

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Admin Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Username</td>
<td>The username to access the web interface. Enter up to 25 characters.</td>
</tr>
<tr>
<td>Password</td>
<td>The password to access the web interface. Enter up to 25 characters.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Confirm the web interface password.</td>
</tr>
<tr>
<td><strong>Current Status</strong></td>
<td></td>
</tr>
<tr>
<td>Serial Number</td>
<td>Shows the device serial number.</td>
</tr>
<tr>
<td>Mac Address</td>
<td>Shows the device Mac address.</td>
</tr>
<tr>
<td>Firmware Version</td>
<td>Shows the current firmware version.</td>
</tr>
<tr>
<td>IP Addressing</td>
<td>Shows the current IP addressing setting (<strong>DHCP</strong> or <strong>static</strong>).</td>
</tr>
<tr>
<td>IP Address</td>
<td>Shows the current 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>SIP Volume</td>
<td>Shows the current SIP volume level.</td>
</tr>
<tr>
<td>Multicast Volume</td>
<td>Shows the current Multicast volume level.</td>
</tr>
<tr>
<td>Ring Volume</td>
<td>Shows the current Ring volume level.</td>
</tr>
<tr>
<td>Sensor Volume</td>
<td>Shows the current Sensor volume level.</td>
</tr>
<tr>
<td>Volume Boost</td>
<td>Shows the current Volume Boost level.</td>
</tr>
<tr>
<td>Microphone Gain</td>
<td>Shows the current microphone gain level.</td>
</tr>
<tr>
<td>SIP Mode</td>
<td>Shows the current status of the SIP mode.</td>
</tr>
<tr>
<td>Multicast Mode</td>
<td>Shows the current status of the Multicast mode.</td>
</tr>
<tr>
<td>Event Reporting</td>
<td>Shows the current status of the Event Reporting mode.</td>
</tr>
<tr>
<td>NightRinger</td>
<td>Shows the current status of the NightRinger mode.</td>
</tr>
<tr>
<td>Primary SIP Server</td>
<td>Shows the current status of the Primary SIP Server.</td>
</tr>
<tr>
<td>Backup Server 1</td>
<td>Shows the current status of Backup Server 1.</td>
</tr>
<tr>
<td>Backup Server 2</td>
<td>Shows the current status of Backup Server 2.</td>
</tr>
<tr>
<td>NightRinger Server</td>
<td>Shows the current status of NightRinger Server.</td>
</tr>
</tbody>
</table>

**Import Settings**

Use this button to select a configuration file to import.

After selecting a configuration file, click Import to import the configuration from the selected file. Then, click Save and Reboot to store changes.
Table 2-6. Home Page Overview (continued)

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export Settings</td>
<td>Click Export to export the current configuration to a file.</td>
</tr>
<tr>
<td>Export Config</td>
<td>Click Export to export the current configuration to a file.</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. |
2.4.5 Configure the Device

1. Click the **Device** menu button to open the **Device** page. See **Figure 2-19**.

**Figure 2-19. Device Configuration Page**

[Image of the Device Configuration Page]

- **Volume Settings (0-9)**
  - SIP Volume:
  - MediaStream Volume:
  - Sensor Volume:
  - Push to Talk Volume:

- **Microphone Settings (0-9)**
  - Microphone Gain:
  - Push to Talk Microphone Gain:

- **Clock Settings**
  - Synchronize with NTP server:
  - NTP server:
  - NTP Timezone String:
  - Periodically synchronize with server:
  - Time update period (in hours):

- **Relay Settings**
  - Activate relay with DTMF code:
  - Relay Pulse Code:
  - Relay Pulse Duration (in seconds):
  - Relay Activation Code:
  - Relay Deactivation Code:
  - Play tone during DTMF Activation:
  - Activate Relay During Ring:
  - Activate Relay During High Ring Tone:
  - Activate Relay When Call Audience:
  - Relay On Button Press Duration:

- **Misc Settings**
  - Device Name:
  - Auto-Answer incoming calls:
  - Button Lit when idle:
  - Button Brightness (0-255):
  - Play Ringback Tone:
  - Enable Push to Talk:
  - Enable DTMF Push to Talk:
  - Prevent Call Transfer:
  - Disable HTTPS (NOT recommended):
2. On the **Device** page, you may enter values for the parameters indicated in **Table 2-7**.

**Note**  The question mark icon (游戏玩家) 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>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 during SIP calls.</td>
</tr>
<tr>
<td>Multicast Volume</td>
<td>Set the speaker volume for multicast audio streams. A value of 0 will mute the speaker during multicasts.</td>
</tr>
<tr>
<td>Ring Volume</td>
<td>Set the ring volume for incoming calls. A value of 0 will mute the speaker instead of playing the ring tone when Auto-Answer Incoming Calls is disabled.</td>
</tr>
<tr>
<td>Sensor Volume</td>
<td>Set the speaker volume for playing sensor activated audio. A value of 0 will mute the speaker during sensor activated audio.</td>
</tr>
<tr>
<td>Push to Talk Volume</td>
<td>Set the speaker volume for Push to Talk operation. A value of 0 will mute the speaker in Push to Talk mode.</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 Volume Boost may introduce audio clips or cause the device to drop from full duplex to half duplex operation.</td>
</tr>
<tr>
<td>Volume Boost 1</td>
<td>Normal operation of the product can be met with volume levels 0 through 9. 0 being mute and 9 being the loudest volume that in a normal arm's length and average background noise, will enable full duplex operation and give the best quality of sound output. The volume boost options increase the output of the speaker by: 3db for Boost level 1 6db for Boost level 2 9db for Boost level 3 If the user would like a higher output from the speaker, the Boost settings are available. However, operation in <strong>Boost Mode</strong> may overdrive or clip the audio if, for example, the phone that is connected has a high microphone gain or if the person has a loud voice talking too close to the microphone. The acoustic echo canceller also has a harder time maintaining full duplex operation when in the <strong>Boost Mode</strong>. The product may drop from full duplex operation into half/duplex mode while in <strong>Boost Mode</strong>. Contact CyberData support for additional information if needed.</td>
</tr>
<tr>
<td>Volume Boost 2</td>
<td></td>
</tr>
<tr>
<td>Volume Boost 3</td>
<td></td>
</tr>
<tr>
<td>Microphone Settings</td>
<td></td>
</tr>
<tr>
<td>Microphone Gain</td>
<td>Set the microphone gain level.</td>
</tr>
<tr>
<td>Push to Talk Microphone Gain</td>
<td>Set the microphone gain level for Push to Talk operation.</td>
</tr>
</tbody>
</table>
# Installing the VoIP Outdoor Intercom

## Intercom Setup

### Clock Settings

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 2.4.5.1, &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>
</tbody>
</table>

### Relay Settings

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activate Relay with DTMF Code</td>
<td>Activates the relay when the DTMF Activation Code is entered on the phone during a SIP call with the device. RFC2833 DTMF payload types are supported.</td>
</tr>
<tr>
<td>Relay Pulse Code</td>
<td>DTMF code used to pulse the relay when entered on a phone during a SIP call with the device. Relay will activate for Relay Pulse Duration seconds then deactivate. Activate Relay with DTMF Code must be enabled. Enter up to 25 digits (* and # are supported).</td>
</tr>
<tr>
<td>Relay Pulse Duration (in seconds)</td>
<td>The length of time (in seconds) during which the relay will be activated when the DTMF Relay Activation Code is detected. Enter up to 5 digits.</td>
</tr>
<tr>
<td>Relay Activation Code</td>
<td>Activation code used to activate the relay when entered on a phone during a SIP call with the device. Relay will be active indefinitely, or until the DTMF Relay Deactivation code is entered. Activate Relay with DTMF Code must be enabled. Enter up to 25 digits (* and # are supported).</td>
</tr>
<tr>
<td>Relay Deactivation Code</td>
<td>Code used to deactivate the relay when entered on a phone during a SIP call with the device. Activate Relay with DTMF Code must be enabled. Enter up to 25 digits (* and # are supported).</td>
</tr>
<tr>
<td>Play tone during DTMF Activation</td>
<td>When selected, the device will play a tone out of the speaker upon DTMF relay activation. The tone plays for the DTMF Activation Duration (in seconds).</td>
</tr>
<tr>
<td>Activate Relay During Ring</td>
<td>When selected, the relay will be activated for as long as the device is ringing. When Auto-Answer Incoming Calls is enabled, the device will not ring and this option does nothing.</td>
</tr>
<tr>
<td>Activate Relay During Night Ring</td>
<td>When selected, the relay will be activated as long as the Nightringer extension is ringing.</td>
</tr>
</tbody>
</table>
## Table 2-7. Device Configuration Parameters (continued)

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activate Relay While Call Active</td>
<td>When selected, the relay will be activated as long as the SIP call is active.</td>
</tr>
<tr>
<td>Activate Relay on Button Press</td>
<td>When selected, the relay will be activated when the Call button is pressed.</td>
</tr>
<tr>
<td>Relay on Button Press Duration</td>
<td>The length of time (in seconds) during which the relay will be activated when the Call button is pressed. Enter up to 5 digits. <strong>A Relay on Button Press Duration</strong> value of 0 will pulse the relay once when the Call button is pressed.</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>Auto-Answer Incoming Calls</td>
<td>When selected, the device will automatically answer incoming calls. When Auto-Answer Incoming Calls is disabled, the device will play a ring tone (corresponds to Ring Tone on the Audiofiles page) out of the speaker until someone presses the Call button to answer the call or the caller disconnects before the call can be answered.</td>
</tr>
<tr>
<td>Button Lit When Idle</td>
<td>When selected, the Call button LED is illuminated while the device is idle (a call is not in progress).</td>
</tr>
<tr>
<td>Button Brightness (0-255)</td>
<td>The desired Call button LED brightness level. Acceptable values are 0-255, where 0 is the dimmest and 255 is the brightest. Enter up to three digits.</td>
</tr>
<tr>
<td>Play Ringback Tone</td>
<td>When selected, the device will play a ringback tone (corresponds to Ringback Tone on the Audiofiles page) out of the speaker while placing an outbound call. The Ringback Tone will play until the call is answered.</td>
</tr>
<tr>
<td>Enable Push to Talk</td>
<td>This option is for noisy environments. When enabled, the microphone will be muted normally. When the Call button is pressed and held, it will unmute the microphone and allow the operator to send audio back. Using Push to Talk prevents the operator from terminating a call by pressing the Call button. The call must be terminated by the phone user.</td>
</tr>
<tr>
<td>Enable DTMF Push to Talk</td>
<td>This option is for noisy environments. When enabled, in an active call, the remote phone can force receive only audio (setting the mic gain to max and muting the speaker) by pressing the * key. Pressing the # key will force send only audio (setting the max speaker volume and muting the mic). Pressing the 0 key will restore full duplex operation with the normal microphone and speaker volume.</td>
</tr>
<tr>
<td>Prevent Call Termination</td>
<td>When this option is enabled, a call cannot be terminated using the call button.</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>
</tbody>
</table>
### Table 2-7. Device Configuration Parameters (continued)

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Test Microphone** | Click on the **Test Microphone** button to do a microphone test. When the **Test Microphone** button is pressed, the following occurs:  
1. The device will immediately start recording 3 seconds of audio.  
2. The device will beep (indicating the end of recording).  
3. The device will play back the recorded audio. |
| **Test Relay** | Click on the **Test Relay** button to do a relay test. |
| **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 can change the **SIP Volume**, **Multicast Volume**, **Ring Volume**, **Sensor Volume**, and **Microphone Gain** without rebooting the device. You must save and reboot the device for other changes to take effect.
2.4.5.1 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 2-8 shows some common strings.

Table 2-8. Common Time Zone 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#</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>

Table 2-9 shows a breakdown of the parts that constitute the following time zone string:

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

Table 2-9. Time Zone String Parts

<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>

---

a. Phoenix, Arizona does not use daylight savings time.
Time Zone String Examples

Table 2-10 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>Tokyo(^a)</td>
<td>IST-9</td>
</tr>
<tr>
<td>Berlin(^b)</td>
<td>CET-1MET,M3.5.0/1:00,M10.5.0/1:00</td>
</tr>
</tbody>
</table>

\(^a\) Tokyo does not use daylight savings time.

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

Time Zone Identifier

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

Figure 2-20. 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 2-11 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>Time Zone</td>
<td>City or Area Zone Crosses</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>GMT+5</td>
<td>Islamabad, Karachi</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>
2.4.6 Configure the Network Parameters

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

Figure 2-21. Network Configuration 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 2</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 Section 2.4.1, &quot;Factory Default Settings&quot; 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 2</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 2</td>
<td>Enter the Static IPv4 network address in dotted decimal notation.</td>
</tr>
<tr>
<td>Subnet Mask 2</td>
<td>Enter the Subnet Mask in dotted decimal notation.</td>
</tr>
<tr>
<td>Default Gateway 2</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>VLAN Settings</strong></td>
<td></td>
</tr>
<tr>
<td>VLAN ID (0-4095) 2</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 &quot;trunking mode&quot; for the VLAN tags to propagate.</td>
<td></td>
</tr>
<tr>
<td>VLAN Priority (0-7) 2</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>
<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>
</tbody>
</table>
Table 2-12. Network Configuration 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.
2.4.7 Configure the SIP (Session Initiation Protocol) Parameters

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

---

**Figure 2-22. SIP Configuration Page**

![SIP Configuration Page](image-url)
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>
<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>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 Section 2.4.7.2, &quot;Point-to-Point Configuration&quot;).</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>
<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>
</tbody>
</table>
### Table 2-13. SIP Configuration Parameters (continued)

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>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>

#### RTP Settings

| RTP Port (even)                      | Specify the port number used for the RTP stream after establishing a SIP call. This port number must be an even number and defaults to 10500. The supported range is 0-65536. Enter up to 5 digits. |
| Jitter Buffer                        | Specify the size of the jitter buffer (in milliseconds) used for SIP calls. Valid values are 50-1000.                                          |

#### 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 Configuration 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 Local SIP Port for the primary extension. The default Local SIP Port is 5061. The supported range is 0-65536. Enter up to 5 digits.</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>Dial Out Settings</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Dial Out Extension</strong></td>
<td>Specify the extension the device will call when someone presses the Call button. Enter up to 64 alphanumeric characters.</td>
</tr>
<tr>
<td><strong>Note:</strong> For information about dial-out extension strings and DTMF tones, see Section 2.4.7.1, “Dial Out Extension Strings and DTMF Tones (using rfc2833)”</td>
<td></td>
</tr>
<tr>
<td><strong>Extension ID</strong></td>
<td>A Caller identification string added to outbound calls. Enter up to 64 alphanumeric characters.</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>
</tbody>
</table>
### Table 2-13. SIP Configuration Parameters (continued)

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Codec Selection</strong></td>
<td></td>
</tr>
<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>
</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. |

---

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

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

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

---

### 2.4.7.1 Dial Out Extension Strings and DTMF Tones (using rfc2833)

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

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

<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.
2.4.7.2 Point-to-Point Configuration

When the device is set to not register with a SIP server (see Figure 2-23), 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 2-23. SIP Page Set to Point-to-Point Mode*
2.4.7.3 Delayed DTMF

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

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

<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 25.
2.4.8 Configure the Multicast Parameters

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

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

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

1. Click on the Multicast menu button to open the Multicast page. See Figure 2-24.

Figure 2-24. Multicast Configuration 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>
<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 2.4.8.1, &quot;Assigning Priority&quot; 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>Beep</td>
<td>When selected, the device will play a beep before multicast audio is sent.</td>
</tr>
<tr>
<td>Relay</td>
<td>When selected, the device will activate a relay 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 <strong>Disabled</strong> 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 <strong>Disabled</strong> 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 <strong>Disabled</strong> 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.

**Note** You must click on the **Save** button and then the **Reboot** button for the changes to take effect.
2.4.8.1 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. 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.
2.4.9 Configure the Sensor Configuration Parameters

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

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

Each sensor can trigger up to five different actions:

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

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

1. Click Sensor menu button to open the Sensor page (Figure 2-25).
Figure 2-25. Sensor Configuration Page
2. On the Sensor page, enter values for the parameters indicated in Table 2-17.

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

### Table 2-17. Sensor Configuration Parameters

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Door Sensor Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Door Sensor Normally Closed</td>
<td>Select the inactive state of the door sensor. The door sensor is also known as the Sense Input on the device's terminal block.</td>
</tr>
<tr>
<td>Door Open Timeout (in seconds)</td>
<td>The time (in seconds) the device will wait before it performs an action when the on-board door sensor is activated. The action(s) performed are based on the configured Door Sensor Settings below. Enter up to 5 digits.</td>
</tr>
<tr>
<td>Flash Button LED</td>
<td>When selected, the Call button LED will flash until the on-board door sensor is deactivated (roughly 10 times/second).</td>
</tr>
<tr>
<td>Activate Relay</td>
<td>When selected, the device's on-board relay will be activated until the on-board door sensor is deactivated.</td>
</tr>
<tr>
<td>Play Audio Locally</td>
<td>When selected, the device will loop an audio file out of the speaker until the door sensor is deactivated.</td>
</tr>
<tr>
<td>Make call to extension</td>
<td>When selected, the device will call an extension when the on-board door sensor is activated. Use the Dial Out Extension field below to specify the extension the device will call.</td>
</tr>
<tr>
<td>Dial Out Extension</td>
<td>Specify the extension the device will call when the on-board door sensor is activated. Enter up to 64 alphanumeric characters.</td>
</tr>
<tr>
<td>Dial Out ID</td>
<td>An additional Caller identification string added to outbound calls. Enter up to 64 alphanumeric characters.</td>
</tr>
<tr>
<td>Play recorded audio</td>
<td>When selected, the device will call the Dial Out Extension and play an audio file to the phone answering the SIP call (corresponds to Door Ajar on the Audiofiles page).</td>
</tr>
<tr>
<td>Repeat Sensor Message</td>
<td>The number of times to repeat the audio message through the local speaker or to the remote endpoint. A value of 0 will repeat the message while the sensor is active. Enter a value from 0-65536.</td>
</tr>
<tr>
<td><strong>Intrusion Sensor Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Flash Button LED</td>
<td>When selected, the Call button LED will flash until the intrusion sensor is deactivated (roughly 10 times/second).</td>
</tr>
<tr>
<td>Activate Relay</td>
<td>When selected, the device's on-board relay will be activated until the intrusion sensor is deactivated.</td>
</tr>
<tr>
<td>Play Audio Locally</td>
<td>When selected, the device will loop an audio file out of the speaker until the intrusion sensor is deactivated.</td>
</tr>
<tr>
<td>Make call to extension</td>
<td>When selected, the device will call an extension when the intrusion sensor is activated. Use the Dial Out Extension field below to specify the extension the device will call.</td>
</tr>
<tr>
<td>Dial Out Extension</td>
<td>Specify the extension the device will call when the intrusion sensor is activated. Enter up to 64 alphanumeric characters.</td>
</tr>
<tr>
<td>Dial Out ID</td>
<td>An additional Caller identification string added to outbound calls. Enter up to 64 alphanumeric characters.</td>
</tr>
</tbody>
</table>
### Table 2-17. Sensor Configuration Parameters (continued)

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Play recorded audio</td>
<td>When selected, the device will call the Dial Out Extension and play an audio file (corresponds to Intrusion Sensor Triggered on the Audiofiles page) to the phone answering the SIP call when the intrusion sensor is activated.</td>
</tr>
<tr>
<td>Repeat Intrusion Message</td>
<td>The number of times to repeat the audio message through the local speaker or to the remote endpoint. A value of 0 will repeat forever. Enter a value from 0-65536.</td>
</tr>
<tr>
<td>Test Door Sensor</td>
<td>Click the Test Door Sensor button to test the door sensor.</td>
</tr>
<tr>
<td>Test Intrusion Sensor</td>
<td>Click the Test Intrusion Sensor button to test the Intrusion sensor.</td>
</tr>
<tr>
<td>Save</td>
<td>Click the Save button to save your configuration settings. Note: You need to reboot for changes to take effect.</td>
</tr>
<tr>
<td>Reboot</td>
<td>Click on the Reboot button to reboot the system.</td>
</tr>
<tr>
<td>Toggle Help</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.
2.4.10 Configure the Audio Configuration Parameters

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

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

**Figure 2-26. Audiofiles Configuration Page**
2. On the Audiofiles 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. Audiofiles Configuration 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>
</tbody>
</table>
| 0-9                 | The name of the audio configuration option is the same as the spoken audio that plays on the board (24 character limit).  
                      | '0' corresponds to the spoken word “zero.”  
                      | '1' corresponds to the spoken word “one.”  
                      | '2' corresponds to the spoken word “two.”  
                      | '3' corresponds to the spoken word “three.”  
                      | '4' corresponds to the spoken word “four.” |
Table 2-18. Audiofiles Configuration Parameters (continued)

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-9</td>
<td>'5' corresponds to the spoken word “five.”</td>
</tr>
<tr>
<td></td>
<td>'6' corresponds to the spoken word “six.”</td>
</tr>
<tr>
<td></td>
<td>'7' corresponds to the spoken word “seven.”</td>
</tr>
<tr>
<td></td>
<td>'8' corresponds to the spoken word “eight.”</td>
</tr>
<tr>
<td></td>
<td>'9' corresponds to the spoken word “nine.”</td>
</tr>
<tr>
<td>Dot</td>
<td>Corresponds to the spoken word “dot.” (24 character limit)</td>
</tr>
<tr>
<td>Audiotest</td>
<td>Corresponds to the message “<em>This is the CyberData IP speaker test message...</em>” (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>Ringback tone</td>
<td>This is the ringback tone that plays when calling a remote extension (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>Intrusion Sensor Triggered</td>
<td>Corresponds to the message “Intrusion Sensor Triggered” (24 character limit).</td>
</tr>
<tr>
<td>Door Ajar</td>
<td>Corresponds to the message “Door Ajar” (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 Ring Tone parameter.</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.
2.4.10.1 User-created Audio Files

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

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

You can use the free utility Audacity to convert audio files into this format. See Figure 2-28 through Figure 2-30.

Figure 2-28. Audacity 1

Figure 2-29. Audacity 2
When you export an audio file with Audacity, save the output as:

- WAV (Microsoft) signed 16 bit PCM.

**Figure 2-30. WAV (Microsoft) signed 16 bit PCM**
2.4.11 Configure the Events Parameters

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

1. Click on the **Events** menu button to open the **Events** page (Figure 2-31).

**Figure 2-31. Event Configuration Page**

![Event Configuration Page](image-url)

- **Enable Event Generation**: Enable this to configure events.
- **Events** section:
  - Enable Button Events
  - Enable Call Start Events
  - Enable Call Terminated Events
  - Enable Relay Activated Events
  - Enable Relay Deactivated Events
  - Enable Ring Events
  - Enable Night Ring Events
  - Enable Multicast Start Events
  - Enable Multicast Stop Events
  - Enable Power On Events
  - Enable Sensor Events
  - Enable Remote Relay Events
  - Enable Security Events
  - Enable 60 Second Heartbeat
- **Event Server**:
  - **Server IP Address**: 10.0.0.250
  - **Server Port**: 8080
  - **Server URL**: xmiparse_engine

**Save** | **Reboot** | **Toggle Help**
2. On the **Events** page, enter values for the parameters indicated in **Table 2-19**.

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

### Table 2-19. Events Configuration 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><strong>Events</strong></td>
<td></td>
</tr>
<tr>
<td>Enable Button Events ?</td>
<td>When selected, the device will report Call button presses.</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 Relay Activated Events ?</td>
<td>When selected, the device will report relay activation.</td>
</tr>
<tr>
<td>Enable Relay Deactivated Events ?</td>
<td>When selected, the device will report relay deactivation.</td>
</tr>
<tr>
<td>Enable Ring Events ?</td>
<td>When selected, the device will report when it starts ringing upon an incoming SIP call. A Ring Event will not be generated when <strong>Auto-Answer Incoming Calls</strong> is enabled on the <strong>Device</strong> page.</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 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 Power On Events ?</td>
<td>When selected, the device will report when it boots.</td>
</tr>
<tr>
<td>Enable Sensor Events ?</td>
<td>When selected, the device will report when the on-board sensor is activated.</td>
</tr>
<tr>
<td>Enable Remote Relay Events ?</td>
<td>When selected, the device will report when the remote relay (DSR) is activated.</td>
</tr>
<tr>
<td>Enable Security Events ?</td>
<td>When enabled, the device will report when the intrusion sensor is activated.</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><strong>Event Server</strong></td>
<td></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>
</tbody>
</table>
Table 2-19. Events Configuration Parameters (continued)

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td>Save</td>
<td>Click the Save button to save your configuration settings.</td>
</tr>
<tr>
<td>Note</td>
<td>You need to reboot for changes to take effect.</td>
</tr>
<tr>
<td>Reboot</td>
<td>Click on the Reboot button to reboot the system.</td>
</tr>
<tr>
<td>Toggle Help</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.
2.4.11.1 Example Packets for Events

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

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

Here are example packets for every event:

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

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP 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 VoIP 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 VoIP 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 VoIP Device' MAC='0020f70015b6'>
<event>CALL_ACTIVE</event>
</cyberdata>
Installing the VoIP Outdoor Intercom

Intercom Setup

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 VoIP 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 VoIP 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 VoIP 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 VoIP 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 VoIP Device' MAC='0020f70015b6'>
<event>RELAY_ACTIVATED</event>
</cyberdata>

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

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>RELAY_ACTIVATED</event>
</cyberdata>
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 VoIP 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 VoIP Device' MAC='0020f70015b6'>
  <event>NIGHTRINGING</event>
</cyberdata>
2.4.12 Configure the Door Strike Relay

The Door Strike Relay (DSR) is a network device designed to control an electronic door strike. The DSR is meant to be used as a replacement for (or an addition to) the on-board relay. In addition to being a drop-in 12 Amp relay, the DSR can monitor and record when the door is open or closed.

The DSR can be configured to trigger in the following ways: on the entry of a DTMF code, during different call events, manually through the web interface, or by using a Windows application.

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

![Figure 2-32. DSR Page](image)
2. On the **DSR** page, enter values for the parameters indicated in Table 2-20.

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

### Table 2-20. DSR Configuration Parameters

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Remote Relay Settings</strong></td>
<td>The settings in this section will activate an associated door strike relay.</td>
</tr>
<tr>
<td>Activate Relay with DTMF Code</td>
<td>Activates the remote relay (DSR) when the DTMF Activation Code is entered on the phone during a SIP call with the device. RFC2833 DTMF payload types are supported.</td>
</tr>
</tbody>
</table>
| DTMF Activation Code                 | Activation code used to activate the remote relay (DSR) when entered on a phone during a SIP call with the device. Activate Remote Relay with DTMF Code must be enabled. Enter up to 25 digits.
|                                       | **Note**: While **Enable DTMF Push to Talk** is enabled, the *, #, and 0 keys cannot be used in the DTMF activation code.                      |
| DTMF Activation Duration (in seconds)| The length of time (in seconds) during which the remote relay (DSR) will be activated when the DTMF Activation Code is detected. Enter up to 5 digits. |
| Activate Remote Relay During Ring    | When selected, the remote relay (DSR) will be activated for as long as the device is ringing. When Auto-Answer Incoming Calls is enabled, the device will not ring this option does nothing. When selected, the network relay will be activated for as long as the call is active. |
| Activate Remote Relay During Night Ring | When selected, the remote relay (DSR) will be activated as long as the Nightringer extension is ringing.                                      |
| Activate Remote Relay While Call Active | When selected, the remote relay (DSR) will be activated as long as the call is active.                                                     |
| Activate Remote Relay on Button Press | When selected, the remote relay (DSR) will be activated when the Call button is pressed.                                                    |
| Remote Relay on Button Press Duration (in seconds) | The length of time (in seconds) during which the remote relay (DSR) will be activated when the Call button is pressed. Enter up to 5 digits. A Remote Relay on Button Press Duration value of 0 will pulse the remote relay (DSR) once when the Call button is pressed. |
| Listen Port for Remote Relay Status  | Specify the port to listen for remote relay (DSR) status packets.                                                                            |
| **Remote Door Sensor Settings**      |                                                                                                                                              |
| Door Open Timeout (in seconds)       | The time (in seconds) the device will wait before it performs an action when the remote (DSR) door sensor is activated. The action(s) performed are based on the configured Remote Door Sensor Settings below. |
| Flash Button LED                     | When selected, the Call button LED will flash until the remote (DSR) door sensor is deactivated (roughly 10 times/second).                   |
| Activate Local Relay                 | When selected, the device's on-board relay will be activated until the remote (DSR) door sensor is deactivated.                              |
| Play Audio Locally                   | When selected, the device will loop an audio file out of the speaker until the remote (DSR) door sensor is deactivated.                    |
Make call to extension
When selected, the device will call an extension when the remote (DSR) door sensor is activated. Use the 'Dial Out Extension' field below to specify the extension the device will call.

Play recorded audio
When selected, the device will call the Dial Out Extension and play an audio file to the phone answering the SIP call (corresponds to Door Ajar on the Audiofiles page) when the remote (DSR) door sensor is activated.

Dial Out Extension
Specify the extension the device will call when the remote (DSR) door sensor is activated. Enter up to 64 alphanumeric characters.

Dial Out ID
An additional Caller identification string added to outbound calls. Enter up to 64 alphanumeric characters.

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.

Discovered Remote Relays
The Discovered Remote Relays section lists all of the networked door strike relays on the network. To associate your device with a door strike relay, click on the Associate button. This action allows the user to configure the door strike relay. Keep in mind that a device may only be associated with one door strike relay.

Product Type
Displays the product type of the remote relay.

IP Address
Displays the IP address of the remote relay.

MAC Address
Displays the MAC address of the remote relay.

Serial Number
Displays the serial number of the remote relay.

Name
Displays the name of the remote relay.

Version
Displays the version of the remote relay.

Use this button to search for and find any remote relays that are available on the network.

Use this button to view the settings of a remote relay that has been “discovered” after pressing the Discover button.

Use this button to associate the remote relay with the device. Only one relay may be associated with a device.
### Relay Status

**Door**: open 
**Relay**: inactive

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

**Figure 2-33. Relay Status Section**

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relay Status</td>
<td><strong>Note</strong>: The <strong>Relay Status</strong> section and settings (Figure 2-33) only appear on the webpage when there is an associated door strike relay.</td>
</tr>
<tr>
<td>Door</td>
<td>Shows the status of the door.</td>
</tr>
<tr>
<td>Relay</td>
<td>Shows the status of the remote relay.</td>
</tr>
<tr>
<td><strong>Kick Remote Relay</strong></td>
<td>Click on the <strong>Kick Remote Relay</strong> button to activate the remote relay for a specified time. The time is equal to the DTMF timeout.</td>
</tr>
<tr>
<td><strong>Activate Remote Relay</strong></td>
<td>Click on the <strong>Activate Remote Relay</strong> button to activate the remote relay until the <strong>Deactivate Remote Relay</strong> button is pressed.</td>
</tr>
<tr>
<td><strong>Deactivate Remote Relay</strong></td>
<td>Click on the <strong>Deactivate Remote Relay</strong> button to deactivate the remote relay.</td>
</tr>
<tr>
<td><strong>Refresh</strong></td>
<td>Click on the <strong>Refresh</strong> button to refresh the web page and accurately display the status of the remote relay (active/inactive) and door (open/closed).</td>
</tr>
</tbody>
</table>

Table 2-20. DSR Configuration Parameters (continued)
2.4.13 Configure the Device (on the DSR page)

1. Click the View button on the DSR page to open the Configure Device page (Figure 2-34).

Figure 2-34. DSR Page Configure Device Page
2. On the **Configure Device** page, enter values for the parameters indicated in Table 2-21.

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

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial Number</td>
<td>Displays the serial number of the door strike relay.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Displays the mac address of the door strike relay.</td>
</tr>
<tr>
<td>Version</td>
<td>Displays the firmware version of the door strike relay.</td>
</tr>
<tr>
<td>Device Name</td>
<td>Displays the name of the door strike relay. The default name is &quot;LOCK,&quot; followed by the 9 digit ASCII serial number. The maximum name length is 13 characters. The unit will always respond to its default name.</td>
</tr>
<tr>
<td>Addressing Mode</td>
<td>Determines whether an IP address will be manually assigned through Static mode or dynamically assigned through a DHCP server.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Displays the IP address of the door strike relay.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Displays the subnet mask of the door strike relay.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Displays the default gateway of the door strike relay.</td>
</tr>
<tr>
<td>Command Port</td>
<td>This shows the port on which the door strike relay sends status packets to the device (defaults to 49999).</td>
</tr>
<tr>
<td>Send Events</td>
<td>When enabled, events can be sent to the associated device.</td>
</tr>
<tr>
<td>Event IP Address</td>
<td>The IP address of the associated device.</td>
</tr>
<tr>
<td>Event Port</td>
<td>This is the port by which the door strike relay receives commands (defaults to 59999).</td>
</tr>
<tr>
<td>Energize Time</td>
<td>This is the number of seconds that the relay will be energized.</td>
</tr>
<tr>
<td>DST</td>
<td>Allows you to either enable or disable the Daylight Savings Time feature.</td>
</tr>
</tbody>
</table>
| DST Start           | Sets the Daylight Savings Time starting time in the following format:  
                      | M3.2.0/02:00:00  
                      | M3 is the third month (March).  
                      | .2 is the second occurrence of the day in the month.  
                      | .0 is Sunday.  
                      | /02:00:00 is the time.  
                      | **Note**: When the occurrence is set to 5, the final occurrence of the day in the specified month is used. |
| DST End             | Sets the Daylight Savings Time ending time in the following format:  
                      | M11.1.0/02:00:00  
                      | M11 is the eleventh month (November).  
                      | .1 is the first occurrence of the day in the month.  
                      | .0 is Sunday.  
                      | /02:00:00 is the time.  
                      | **Note**: When the occurrence is set to 5, the final occurrence of the day in the specified month is used. |
Installing the VoIP Outdoor Intercom

Intercom Setup

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Time</td>
<td>Sets the current time. <strong>Note</strong>: Be sure to save the current time by clicking on the <strong>Set Time</strong> button.</td>
</tr>
<tr>
<td>Encryption</td>
<td>Encryption can either be set to <strong>None</strong> or <strong>AES-256</strong>.</td>
</tr>
<tr>
<td>Encryption Key</td>
<td>Sets the AES encryption key. If encryption is currently enabled, the response to this command will be sent using the &quot;old&quot; key. The new key should be sent as 64 ASCII hexadecimal characters.</td>
</tr>
<tr>
<td>Door State</td>
<td>This field displays the current door state and is not configurable.</td>
</tr>
<tr>
<td>Relay State</td>
<td>This field displays the current relay state and is not configurable.</td>
</tr>
<tr>
<td>Button State</td>
<td>This field displays the current button state and is not configurable.</td>
</tr>
<tr>
<td>LED</td>
<td>This field displays the current LED state and is not configurable.</td>
</tr>
<tr>
<td>Alarm State</td>
<td>This field displays the current alarm state and is not configurable.</td>
</tr>
<tr>
<td>JP4, 6, 9, 10</td>
<td>This shows whether jumpers JP4, JP6, JP9, or JP10 are either enabled or disabled through the four digit sequence (0000). The 0 turns to 1 for an enabled jumper. For example, 0011 would mean jumpers JP9 and JP10 are activated, but JP4 and JP9 are not.</td>
</tr>
</tbody>
</table>

Click on the **Refresh** button to refresh the **Device Configuration** page.

Click on the **Get Log** button to get a log of the associated door strike relay activity. The door strike relay has 128Kb non-volatile storage for log data, storing an average of 10 days' worth of log data before it is overwritten.

Click on the **Clear Log** button to clear the log from the door strike relay.

Click on the **Reboot** button to reboot any "discovered" remote relays and clear any associated devices.

Click on the **Set Time** button to change the time.

Click on the **Save Changes** button to save any changes that are made to the **Device Configuration** page. **Note**: The time setting must be saved by pressing the **Set Time** button.

Click on the **Cancel** button to cancel any changes that were made to the **Configure Device** page and return to the **DSR** page.

Click on the **Browse** button to navigate through your computer and find firmware files.

Click on the **Upgrade** button to upgrade the firmware of the door strike relay.

**Note**: You must click on the **Save** button and then the **Reboot** button for the changes to take effect.
### 2.4.14 Configure the Autoprovisioning Parameters

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

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

1. Click the **Autoprov** menu button to open the **Autoprovisioning** page. See **Figure 2-35**.

**Figure 2-35. Autoprovisioning Page**
2. On the **Autoprovisioning** page, you may enter values for the parameters indicated in Table 2-22.

**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 2-22. Autoprovisioning Configuration Parameters

<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 2.4.14.1, “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. 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</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>(in minutes)</td>
<td><strong>Note</strong>: To use the auto update options, enable the <strong>Set Time with NTP Server on boot</strong> setting on the Device Configuration Page page (see Table 2-7).</td>
</tr>
<tr>
<td>Autoprovision at time</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>(HHMMSS)</td>
<td><strong>Note</strong>: To use the auto update options, enable the <strong>Set Time with NTP Server on boot</strong> setting on the Device Configuration Page page (see Table 2-7).</td>
</tr>
<tr>
<td>Autoprovision when idle</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>(in minutes &gt; 10)</td>
<td><strong>Note</strong>: To use the auto update options, enable the <strong>Set Time with NTP Server on boot</strong> setting on the Device Configuration Page page (see Table 2-7).</td>
</tr>
</tbody>
</table>

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

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

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

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

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

By default, the device will get its autoprovisioning server from the DHCP options. See Section 2.4.14.2, "Sample dhcpd.conf" for an example of how to configure dhcpd to offer autoprovisioning server addresses. If multiple options are set, the device will attempt to download autoprovisioning files from every server.

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

1. Option 43 - a FQDN or an IP address to an http server
2. Option 72 - an IP address to an http server
3. Option 150 - an IP address to a tftp server
4. Option 66 - an IP address to a tftp server or if the entry starts with 'http', a FQDN to a http server.
You can download an autoprovisioning template file from the Autoprovisioning Page using the Download Template button (see Table 2-22). This file contains every configuration option that can be set on the board.

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

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

```
<MiscSettings>
   <DeviceName>CyberData VoIP Intercom</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 its name to 'Newname'.

2. It will try to download http://example.com/common.xml.

3. It will try to download http://example.com/sip_reg0020f7123456.xml.

4. It will try to download http://example.com/audio0020f7123456.

5. It will try to download http://example.com/device.xml.

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

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

Checking for New Autoprositioning 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>
<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/000000cd.xml

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

Intercom Setup

Autoprovisioning

Firmware Updates

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

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

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

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

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

The list of valid product strings:

<ProductString>CallButton31</ProductString>
<ProductString>EmergencyIntercom31</ProductString>
<ProductString>EmergencyIntercom31SW</ProductString>
<ProductString>IndoorIntercom31</ProductString>
<ProductString>IndoorIntercom31SW</ProductString>
<ProductString>IndoorKeypad31</ProductString>
<ProductString>IndoorKeypad31SW</ProductString>
<ProductString>OfficeRinger31</ProductString>
<ProductString>OfficeRinger31SW</ProductString>
<ProductString>OutdoorIntercom31</ProductString>
<ProductString>OutdoorIntercom31SW</ProductString>
<ProductString>OutdoorKeypad31</ProductString>
<ProductString>OutdoorKeypad31SW</ProductString>
<ProductString>Strobe31</ProductString>
<ProductString>Strobe31SW</ProductString>
Autoprovisioning Example 1

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

We boot up two devices with mac addresses \textbf{00:20:17:02:00:01} and \textbf{00:20:17:02:00:02} (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:

\begin{verbatim}
000000cd.xml

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

sip_common.xml

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

sip_0020f7020001.xml

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

sip_0020f7020002.xml

<SIPSettings>
  <SIPUserID>500</SIPUserID>
  <SIPAuthPassword>ext500</SIPAuthPassword>
  <DialoutExtension0>555</DialoutExtension0>
</SIPSettings>
\end{verbatim}

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

1. Device1 changes its device name to \textbf{CyberData Autoprovisioned}.

2. Device1 finds an AutoprovFile element containing the filename \texttt{sip\_common.xml}. The device downloads \texttt{sip\_common.xml} from “https://autoprovtest.server.net,” and imports this configuration, setting the sip server to \texttt{10.0.0.253} and the remote port to \texttt{5060.3}.

3. Device1 finds another AutoprovFile element containing the filename \texttt{sip\_[macaddress].xml}. The device replaces the [\texttt{macaddress}] with its own mac address value creating \texttt{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.

Autoprosining Example 2

Here is another example of setting up your autoprovisioning files:

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

0020f7020001.xml

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

0020f7020002.xml

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

common_settings.xml

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

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

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

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

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

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

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

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

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

From the common file, a pointer to sip_common.xml

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

Autoprovisioned Audio Files

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

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

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

ddns-update-style none;

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

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

    option routers 10.0.0.1;
    option subnet-mask 255.0.0.0;

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

    option time-offset -8; # Pacific Standard Time

    # option www-server 99.99.99.99; # OPTION 72
    # option tftp-server-name "10.0.1.52"; # OPTION 66
    # option tftp-server-name "http://test.cyberdata.net"; # OPTION 66
    # option option-150 10.0.0.252; # OPTION 150

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

    range 10.10.0.1 10.10.2.1; }

2.4.14.3 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 2-36). 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 2-36.

   **Figure 2-36. Configuration File**

   ![Configuration File Window](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.
2.5 Upgrade the Firmware and Reboot the Intercom

2.5.1 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/011186/](http://www.cyberdata.net/voip/011186/)

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

3. Log in to the Intercom home page as instructed in Section 2.4.4, "Log in to the Configuration Home Page".

Caution

*Equipment Hazard:* Devices with a serial number that begins with 1861xxxxx can only run firmware versions 10.0.0 or later.
4. Click on the **Firmware** menu button to open the **Firmware** page. See Figure 2-37.

![Figure 2-37. Firmware Page](image)

**Caution**
*Equipment Hazard*: CyberData strongly recommends that you first reboot the device before attempting to upgrade the firmware of the device. See Section 2.5.2, “Reboot the Device”.

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

6. Select the firmware file.

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

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

**Note**  This starts the upgrade process. Once the Intercom has uploaded the file, the **Uploading Firmware** countdown page appears, indicating that the firmware is being written to flash. The Intercom 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 2-24 shows the web page items on the **Firmware** page.

<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><strong>Browse</strong></td>
<td>Use the <strong>Browse</strong> button to navigate to the location of the Intercom firmware file that you want to upload.</td>
</tr>
<tr>
<td><strong>Upload</strong></td>
<td>Click on the <strong>Upload</strong> button to automatically upload the selected firmware and reboot the system.</td>
</tr>
</tbody>
</table>
2.5.2 Reboot the Device

To reboot a Intercom, log in to the web page as instructed in Section 2.4.4, "Log in to the Configuration Home Page".

1. Click on the Reboot button on the Home page (Figure 2-38). A normal restart will occur.

Figure 2-38. Home Page
2.6 Command Interface

Some functions on the device can be activated using simple POST commands to the web interface. The examples in Table 2-25 use the free unix utility, `wget commands`. However, any program that can send HTTP POST commands to the device should work.

2.6.1 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 Commanda</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trigger relay (for configured delay)</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/command.cgi">https://10.0.3.71/cgi-bin/command.cgi</a>&quot; --post-data &quot;test_relay=yes&quot;</td>
</tr>
<tr>
<td>Place call to extension (example: extension 130)</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/command.cgi">https://10.0.3.71/cgi-bin/command.cgi</a>&quot; --post-data &quot;call=130&quot;</td>
</tr>
<tr>
<td>Place point-to-point callb (example: IP phone address = 10.0.3.72)</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/command.cgi">https://10.0.3.71/cgi-bin/command.cgi</a>&quot; --post-data &quot;call=10.0.3.72&quot;</td>
</tr>
<tr>
<td>Terminate active call</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/command.cgi">https://10.0.3.71/cgi-bin/command.cgi</a>&quot; --post-data &quot;terminate=yes&quot;</td>
</tr>
<tr>
<td>Force reboot</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/command.cgi">https://10.0.3.71/cgi-bin/command.cgi</a>&quot; --post-data &quot;reboot=yes&quot;</td>
</tr>
<tr>
<td>Test Audio button</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/command.cgi">https://10.0.3.71/cgi-bin/command.cgi</a>&quot; --post-data &quot;test_audio=yes&quot;</td>
</tr>
<tr>
<td>Announce IP address</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/command.cgi">https://10.0.3.71/cgi-bin/command.cgi</a>&quot; --post-data &quot;speak_ip_address=yes&quot;</td>
</tr>
<tr>
<td>Play the &quot;0&quot; audio file</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/audiofiles.cgi">https://10.0.3.71/cgi-bin/audiofiles.cgi</a>&quot; --post-data &quot;play_0=yes&quot;</td>
</tr>
<tr>
<td>Play the &quot;1&quot; audio file</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/audiofiles.cgi">https://10.0.3.71/cgi-bin/audiofiles.cgi</a>&quot; --post-data &quot;play_1=yes&quot;</td>
</tr>
<tr>
<td>Play the &quot;2&quot; audio file</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/audiofiles.cgi">https://10.0.3.71/cgi-bin/audiofiles.cgi</a>&quot; --post-data &quot;play_2=yes&quot;</td>
</tr>
<tr>
<td>Play the &quot;3&quot; audio file</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/audiofiles.cgi">https://10.0.3.71/cgi-bin/audiofiles.cgi</a>&quot; --post-data &quot;play_3=yes&quot;</td>
</tr>
</tbody>
</table>
### Table 2-25. 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;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;play_4=yes&quot;</code></td>
</tr>
<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</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;Intrusion Sensor Triggered&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_intrusionsensortriggered=yes&quot;</code></td>
</tr>
<tr>
<td>Play the &quot;Door Ajar&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_doorajar=yes&quot;</code></td>
</tr>
<tr>
<td>Device Action</td>
<td>HTTP Post Command</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------------------------------</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>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>
</tbody>
</table>
### Table 2-25. Command Interface Post Commands (continued)

<table>
<thead>
<tr>
<th>Device Action</th>
<th>HTTP Post Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete the &quot;Ringback tone&quot; audio file</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/audiofiles.cgi">https://10.0.3.71/cgi-bin/audiofiles.cgi</a>&quot; --post-data &quot;delete_ringback=yes&quot;</td>
</tr>
<tr>
<td>Delete the &quot;Ring tone&quot; audio file</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/audiofiles.cgi">https://10.0.3.71/cgi-bin/audiofiles.cgi</a>&quot; --post-data &quot;delete_ringtone=yes&quot;</td>
</tr>
<tr>
<td>Delete the &quot;Intrusion Sensor Triggered&quot; audio file</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/audiofiles.cgi">https://10.0.3.71/cgi-bin/audiofiles.cgi</a>&quot; --post-data &quot;delete_intrusionsensortriggered=yes&quot;</td>
</tr>
<tr>
<td>Delete the &quot;Door Ajar&quot; audio file</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/audiofiles.cgi">https://10.0.3.71/cgi-bin/audiofiles.cgi</a>&quot; --post-data &quot;delete_doorajar=yes&quot;</td>
</tr>
<tr>
<td>Delete the &quot;Night Ring&quot; audio file</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/audiofiles.cgi">https://10.0.3.71/cgi-bin/audiofiles.cgi</a>&quot; --post-data &quot;delete_nightring=yes&quot;</td>
</tr>
<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>
<tr>
<td>Trigger the Intrusion 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;intrusionevent=yes&quot;</td>
</tr>
</tbody>
</table>

---

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

b. Must be in point-to-point mode see Section 2.4.7.2, "Point-to-Point Configuration"
Appendix A: Mounting the Intercom

A.1 Mounting Components

Before you mount the Intercom, make sure that you have received all the parts for each Intercom. Refer to the following tables.

<table>
<thead>
<tr>
<th>Table A-1. Mounting Components (Part of the Accessory Kit)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quantity</td>
</tr>
<tr>
<td>----------</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table A-2. Optional Accessories (for gooseneck mounting)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quantity</td>
</tr>
<tr>
<td>----------</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table A-3. Optional Accessories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quantity</td>
</tr>
<tr>
<td>----------</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>1</td>
</tr>
</tbody>
</table>
A.2 Dimensions

Figure A-1. Unit Dimensions—Front and Side View

Figure A-2. Unit Dimensions—Rear View with Mounting Hole Locations

Dimensions are in Inches [Millimeter]

ø0.280 [ø7.11] (4 Places)

ø0.854 [ø21.69]
Figure A-3. Shroud Dimensions—Front and Side View with Mounting Hole Locations

Dimensions are in Inches [Millimeter]

Figure A-4. Unit Dimensions—Unit without the Gang Box

*Effective Range for Intrusion Sensor to Function
Affix Reflective Surface Above Intrusion Sensor from 3 mm (Minimum) to 14 mm (Maximum)
Figure A-5. PCB Dimensions and Intrusion Sensor Range

Dimensions are in inches [millimeter].

TOP SIDE
- JP10
- J10
- J8
- J7
- J9
- J2
- J10

BOTTOM SIDE
- J5
- J4
- J3
- SW1

DIMENSIONS ARE IN INCHES [MILLIMETER]
PROJECTION: THIRD ANGLE PROJECTION
A.3 Overview of Installation Types

An overview of the installation types and the required components are provided in Table A-4.

<table>
<thead>
<tr>
<th>Installation Type</th>
<th>What You Need</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Outdoor, on surface</strong></td>
<td>011186 Intercom only</td>
</tr>
</tbody>
</table>
| **Outdoor, on surface with shroud (increased resistance)** | 011186 Intercom  
|                                                       | 011188 Weather Shroud (sold separately)           |
A.4 Network Cable Entry Restrictions

A.4.1 Conduit Mounting Restrictions (Side Entry)

See Figure A-6 for the conduit mounting restrictions (side entry).

Figure A-6. Conduit Mounting Restrictions (Side Entry)
A.4.2 Conduit Mounting Restrictions (Rear Entry without Shroud)

See Figure A-7 for the conduit mounting restrictions (rear entry without shroud).

*Figure A-7. Conduit Mounting Restrictions (Rear Entry without Shroud)*

A.4.3 Conduit Mounting Restrictions (Rear Entry with Shroud)

See Figure A-8 for the conduit mounting restrictions (rear entry with shroud).

*Figure A-8. Conduit Mounting Restrictions (Rear Entry with Shroud)*
A.5 Ground Cable Installation

Figure A-9 illustrates how to connect a ground cable to the VoIP Outdoor Intercom.

**Note:** To mount the intercom, use methods compliant with local electrical codes.
A.6 Service Loop Cable Routing

Figure A-10 and Figure A-11 illustrate a service loop cable routing option for the VoIP Outdoor Intercom.

**Figure A-10. Ground Cable Service Loop Routing**

![Ground Cable Service Loop Routing Diagram]

- Ground Wire (not provided)
- Ground Lug
- Nut (to Ground Lug inside of the Gang Box)
- Route cable(s) inside of the Gang Box to create the service loop.

**Figure A-11. Network Cable Service Loop Routing**

![Network Cable Service Loop Routing Diagram]

- Network Cable (not provided)
- Route cable(s) inside of the Gang Box to create the service loop.
A.7 Securing the Intercom

Figure A-12 illustrates how to secure the VoIP Outdoor Intercom with Torx screws.

![Figure A-12. Securing the Intercom](image)

**Note:** To mount the intercom, use methods compliant with local electrical codes.

**Caution**

*Equipment Hazard:* Do not use an electric or power screwdriver to fasten the face plate and PCB assembly to the gang box. To prevent over-torque damage to the gasket, do not apply more than 10 inch-pounds force. Over-torquing will cause the gasket to tear, risk moisture intrusion, and effectively void the manufacturer's warranty.
A.8 Additional Mounting Options

A.8.1 Conduit Mounting Option (Not Provided)

*Figure A-13* illustrates a side and rear conduit mounting option for the VoIP Outdoor Intercom.

**Figure A-13. Optional Conduit Mounting**

*Note: To mount the intercom, use methods compliant with local electrical codes.*
A.8.2 Concrete Wall Mounting Option (Not Provided)

Figure A-14 illustrates a concrete wall mounting option for the VoIP Outdoor Intercom.

Figure A-14. Optional Concrete Wall Mounting

![Concrete Wall Mounting Diagram]

Note: To mount the intercom, use methods compliant with local electrical codes.
A.8.3 Goose Neck Mounting Option (Not Provided)

Figure A-15 illustrates a gooseneck mounting option for the VoIP Outdoor Intercom.

**Figure A-15. Optional Goose Neck Mounting**

**Note:** To mount the intercom, use methods compliant with local electrical codes.
A.8.4 Ground Cable Installation for Goose Neck Mounting Option

**Figure A-16** illustrates the correct ground cable installation for the gooseneck mounting option.

**Figure A-16. Ground Cable Installation for Goose Neck Mounting**

**Note:** To mount the intercom, use methods compliant with local electrical codes.
Appendix B: Setting up a TFTP Server

B.1 Set up a TFTP Server

Autoprovisioning requires a TFTP server for hosting the configuration file.

B.1.1 In a LINUX Environment

To set up a TFTP server on LINUX:

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

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

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

B.1.2 In a Windows Environment

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

   [http://www.cyberdata.net/support/voip/solarwinds.html](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/011186/

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/011186/
C.3 Contact Information

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

Sales
Sales 831-373-2601, Extension 334

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

http://support.cyberdata.net/

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

Phone: (831) 373-2601, Extension 333

C.4 Warranty and RMA Information

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

http://support.cyberdata.net/
Index

Numerics

16 AWG gauge wire 9

A
activate local relay (door sensor) 68
activate relay (door sensor) 54
activate relay (intrusion sensor) 54
activity LED 18
address, configuration login 27
alternative power input 6
announcing a device’s IP address 20
audio configuration 56
—night ring tone parameter 58
audio configuration page 56
audio encodings 5
audio files, user-created 59
autoprovision at time (HHMMSS) 75
autoprovision when idle (in minutes > 10) 75
autoprovisioning 76
—download template button 76
—setting up a TFTP server 107
autoprovisioning autoupdate (in minutes) 75
autoprovisioning configuration 74, 75
autoprovisioning filename 75
autoprovisioning server (IP Address) 75

B
backup SIP server 1 43
backup SIP server 2 43
backup SIP servers, SIP server backups 43
boost (volume) 32

c

call button 22
call button LED 22
call termination 34
changing
—the web access password 31
Cisco SRST 43
command interface 89
commands 89
concrete wall mounting option (not provided) 104
d conduit mounting option (not provided) 103
configurable parameters 32, 40, 43, 72
configuration
—audio 56
—default IP settings 23
door sensor 52
intrusion sensor 52
network 39
SIP 42
configuration home page 27
configuration page
—configurable parameters 32, 40, 72
contact information 109
contact information for CyberData 109
current network settings 40
CyberData contact information 109

default gateway 23
intercom settings 110
IP address 23
subnet mask 23
username and password 23
web login username and password 27
default gateway 23, 40
default intercom settings 21
default IP settings 23
default login address 27
device configuration 31
device configuration parameters 75
device configuration parameters 32
device configuration page
—changing for web configuration access 31
DHCP Client 5
dial out extension (door sensor) 54, 69
dial out extension (intrusion sensor) 54
dial out extension strings 46
dial-out extension strings 48
dimensions 6, 94
—pc board dimensions and intrusion sensor range 96
—shroud dimensions and mounting hole locations 95
unit dimensions and intrusion sensor range without
—the gang box 95
unit dimensions—front and side view 94
unit dimensions—rear view and mounting hole
Index

Operations Guide 931293A CyberData Corporation

locations 94
discovery utility program 27
DNS server 40
door sensor 52, 54, 68
activate local relay 68
activate relay 54
dial out extension 54, 69
door open timeout 54, 68
door sensor normally closed 54
flash button LED 54, 68
play audio locally 54, 68
door strike intermediate relay 12, 13, 14
download autoprovisioning template button 76
DTMF push to talk 34
DTMF tones 46, 48
DTMF tones (using rfc2833) 46

electric screwdriver 102
enable night ring events 62
ethernet I/F 6
event configuration
enable night ring events 62
expiration time for SIP server lease 44, 45
export settings 29, 30

factory default settings 21
fastening, gang box 102
firmware
where to get the latest firmware 86
flash button LED (door sensor) 54, 68
flash button LED (intrusion sensor) 54

gang box, fastening 102
gasket, avoid over-torque damage 102
get autoprovisioning template 76
GMT table 37
GMT time 37
goose neck mounting option (not provided) 105
ground cable installation 100
ground cable installation for goose neck mounting option 106

H
home page 27
http POST command 89
http web-based configuration 5

I
identifier names (PST, EDT, IST, MUT) 37
identifying your product 1
import settings 29, 30
import/export settings 29, 30
installation, typical intercom system 2
intercom configuration
default IP settings 23
intercom configuration page
configurable parameters 43
intrusion sensor 52, 54
activate relay 54
dial out extension 54
flash button LED 54
play audio locally 54
IP address 23, 40
IP addressing
default
IP addressing setting 23

J
J3 terminal block, 16 AWG gauge wire 9

L
lease, SIP server expiration time 44, 45
LED
green link LED 18
yellow activity LED 18
lengthy pages 51
link LED 18
Linux, setting up a TFTP server on 107
local SIP port 44
log in address 27

M
MGROUP
MGROUP Name 50
mounting 93
additional mounting options 103
concrete wall mounting option (not provided) 104
conduit mounting option (not provided) 103
goose neck mounting option (not provided) 105
ground cable installation 100
ground cable installation for goose neck mounting option 106
network cable entry restrictions 98
optional accessories 93
overview of installation types 93, 97
rear conduit network cable entry restrictions (with shroud) 99
rear conduit network cable entry restrictions (without shroud) 99
securing the intercom 102
service loop cable routing 101
side conduit network cable entry restrictions 98
mounting components 93
multicast configuration 56
Multicast IP Address 50

N

navigation (web page) 24
navigation table 24
network cable entry restrictions 98
network configuration 39
nightring tones 51
Nightringer 9, 85
nightringer settings 44
NTP server 33

O

on-board relay 6, 10
operating temperature 6
overview of installation types 97

P

packet time 5
pages (lengthy) 51
part number 6
parts list 7
password
  for SIP server login 43
  login 27
  restoring the default 23
payload types 6
pcb dimensions and intrusion sensor range 96
play audio locally (door sensor) 54, 68
play audio locally (intrusion sensor) 54
point-to-point configuration 47
polycom default channel 50
polycom emergency channel 50
polycom priority channel 50
port
  local SIP 44
  remote SIP 44
posix timezone string
timezone string 33
POST command 89
power input 6
  alternative 6
power screwdriver 102
priority
  assigning 51
product features 4
product overview
  product features 4
  product specifications 6
  supported protocols 5
  supported SIP servers 5
  typical system installation 2
product specifications 6
protocol 6
protocols supported 5
push to talk, DTMF 34

R

rear conduit network cable entry restrictions (with shroud) 99
rear conduit network cable entry restrictions (without shroud) 99
reboot 87, 88
remote SIP port 44
reset test function management button 19
resetting the IP address to the default 93, 108
restoring factory default settings 21, 110
ringtones 51
  lengthy pages 51
RJ-45 17
rport discovery setting, disabling 44
RTFM button 19
RTFM jumper 19, 20, 21
RTP/AVP 5

S

sales 109
securing the device 102
sensor setup page 53, 67
Index

sensor setup parameters 52
sensors 54, 68
server address, SIP 43
service 109
service loop cable routing 101
set time with external NTP server on boot 33
setting up the device 9
settings, default 21
shroud dimensions and mounting hole locations 95
side conduit network cable entry restrictions 98
SIP
  enable SIP operation 43
    local SIP port 44
    user ID 43
SIP configuration 42
SIP configuration parameters
  outbound proxy 44, 45
  registration and expiration, SIP server lease 44, 45
  unregister on reboot 44
  user ID, SIP 43
SIP registration 43
SIP remote SIP port 44
SIP server 43
  password for login 43
  SIP servers supported 5
  unregister from 44
  user ID for login 43
SIP server configuration 43
SIP volume 32
speaker output 6
SRST 43
subnet mask 23, 40
supported protocols 5

T

tech support 109
technical support, contact information 109
terminal block, 16 AWG gauge wire 9
TFTP server 5, 107
time zone string examples 37

U

unit dimensions and intrusion sensor range without the
  gang box 95
unit dimensions—front and side view 94
unit dimensions—rear view and mounting hole
  locations 94
user ID
  for SIP server login 43
username

V

VLAN ID 40
VLAN Priority 40
VLAN tagging support 40
VLAN tags 40
volume
  microphone gain 32
  multicast volume 32
  push to talk volume 32
  ring volume 32
  sensor volume 32
  SIP volume 32
  volume boost 32

W

warranty policy at CyberData 109
web access password 23
web access username 23
web configuration log in address 27
web page
  navigation 24
web page navigation 24
wget, free unix utility 89
Windows, setting up a TFTP server on 107
wiring the circuit 11
  devices less than 1A at 30 VDC 11