CyberData

The IP Endpoint Company

SIP Office Ringer

Operations Guide

Part #011216, RAL 9003, Signal White Color

Pictorial Alert Icons

⚠️ GENERAL ALERT	**General Alert** *This pictoral alert indicates a potentially hazardous situation. This alert will be followed by a hazard level heading and more specific information about the hazard.*
⏚	**Ground** *This pictoral alert indicates the Earth grounding connection point.*

Hazard Levels

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

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

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

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

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

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. **WARNING: The device enclosure is not rated for any AC voltages!**

⚠ GENERAL ALERT	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.

Revision Information

Revision 930839D, which corresponds to firmware version 11.1.0., was released on January 14, 2015, and has the following changes:

- Adds Figure 1-3, "Typical Installation—Door Strike Intermediate Relay Module"
- Adds Figure 1-4, "Typical Installation—Networked Door Strike Intermediate Relay Module"
- Updates Figure 2-19, "Home Page"
- Updates Figure 2-20, "Device Configuration Page"
- Updates Figure 2-21, "Three or Four Character Time Zone Identifier"
- Updates Figure 2-22, "Network Configuration Page"
- Updates Figure 2-23, "SIP Configuration Page"
- Updates Figure 2-24, "SIP Page Set to Point-to-Point Mode"
- Updates Figure 2-25, "Multicast Configuration Page"
- Updates Figure 2-26, "Sensor Configuration Page"
- Updates Figure 2-27, "Audiofiles Configuration Page"
- Updates Figure 2-28, "Audiofiles Page"
- Updates Figure 2-32, "Event Configuration Page"
- Adds Figure 2-33, "DSR Page"
- Adds Figure 2-34, "Relay Status Section"
- Adds Figure 2-35, "DSR Page Configure Device Page"
- Updates Figure 2-36, "Autoprovisioning Page"
- Updates Figure 2-37, "Configuration File"
- Updates Figure 2-38, "Firmware Page"
- Updates Figure 2-39, "Home Page"
- Updates Table 2-6, "Home Page Overview"
- Updates Table 2-7, "Device Configuration Parameters"
- Updates Table 2-12, "Network Configuration Parameters"
- Updates Table 2-13, "SIP Configuration Parameters"
- Updates Table 2-16, "Multicast Configuration Parameters"
- Updates Table 2-17, "Sensor Configuration Parameters"
- Updates Table 2-18, "Audiofiles Configuration Parameters"
- Updates Table 2-19, "Events Configuration Parameters"
- Adds Table 2-20, "DSR Configuration Parameters"
- Adds Table 2-21, "DSR Page Configure Device Parameters"
- Updates Table 2-22, "Autoprovisioning Configuration Parameters"
- Updates Table 2-24, "Firmware Parameters"
- Updates Table 2-25, "Command Interface Post Commands"
- Updates Section 2.3.14.1, "Autoprovisioning"
- Updates Section 2.3.14.2, "Sample dhcpd.conf"

Abbreviations and Terms

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

Contents

1 Product Overview

1.1 How to Identify This Product

To identify the SIP Office Ringer, 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 **011216**.

- The serial number on the label should begin with **2161**.

Figure 1-1. Model Number Label

Model number

Serial number begins with **2161**
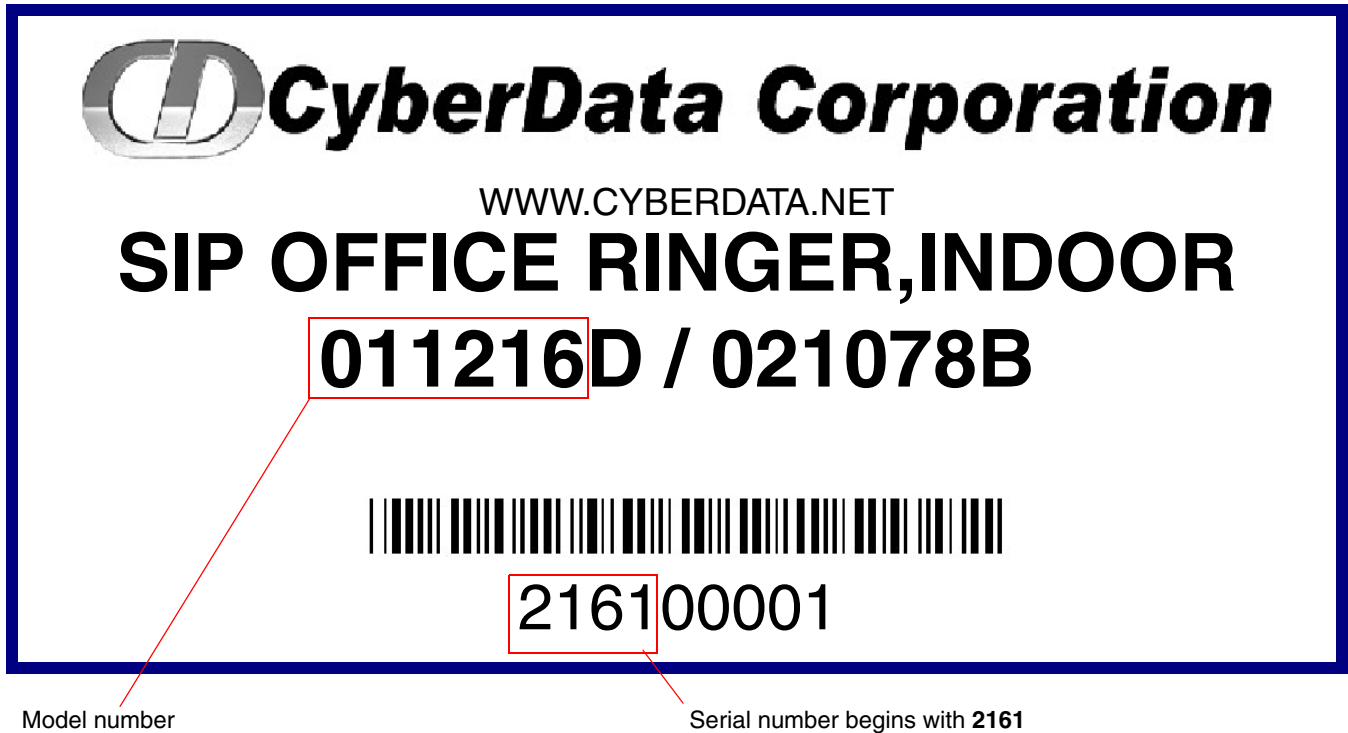
1.2 Typical System Installation

The SIP Office Ringer is a SIP endpoint designed to provide an audible ring tone or pre-recorded message when the device is called as part of a Ring Group.

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

Figure 1-2. Typical Installation
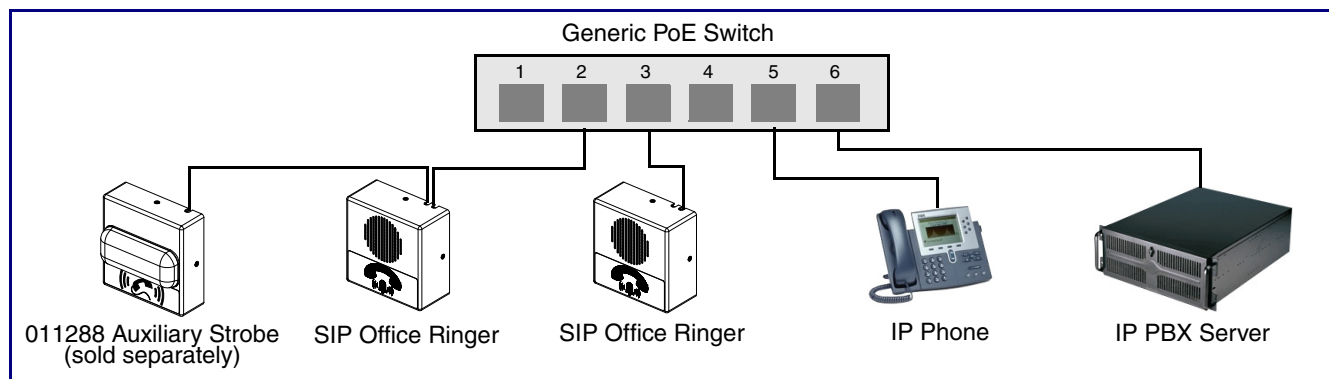
Figure 1-3. Typical Installation—Door Strike Intermediate Relay Module
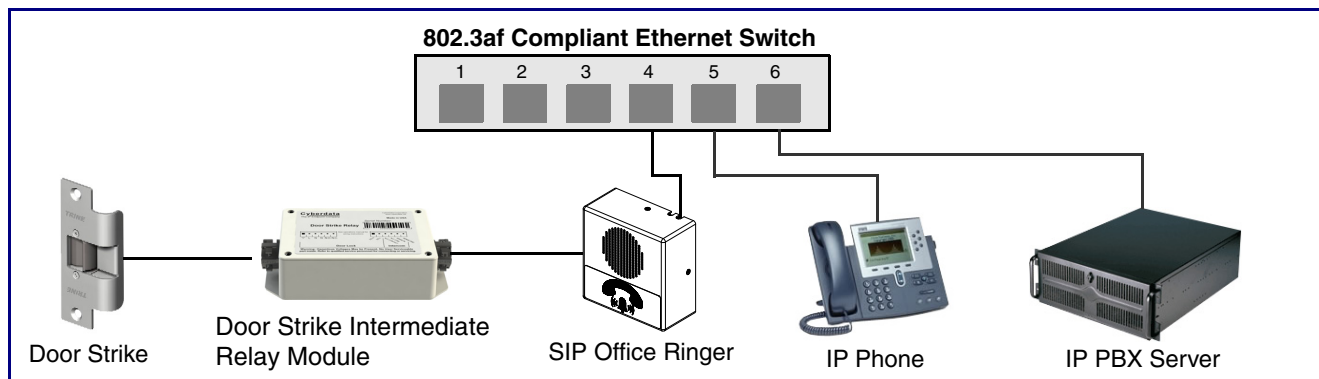
Figure 1-4. Typical Installation—Networked Door Strike Intermediate Relay Module
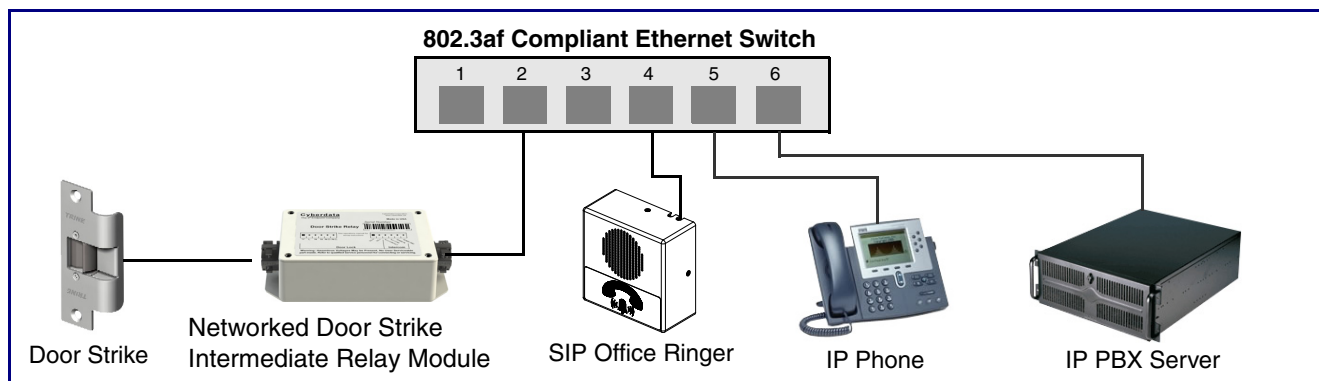
1.3 Product Features

- Cisco SRST (Survivable Remote Site Telephony)
- SIP
- Dual speeds of 10 Mbps and 100 Mbps
- 802.3af compliant
- Network/Web management
- Network adjustable speaker volume adjustment
- Network configurable relay activation settings
- Network downloadable product firmware
- Doubles as a paging speaker
- One dry contact relay for auxiliary control
- Autoprovisioning
- Configurable audio files
- Office Ringer

1.4 Supported Protocols

The Office Ringer supports:

- SIP
- HTTP Web-based configuration

  Provides an intuitive user interface for easy system configuration and verification of Office Ringer 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
- Packet Time 20 ms
- Audio Encodings

  PCMU (G.711 mu-law)

  PCMA (G.711 A-law)

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/support/server/index.html

1.6 Product Specifications
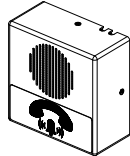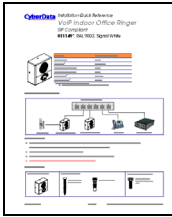
Category	Specification
Speaker Output	1 Watt Peak Power
Network Rate	10/100 Mbps
Power Requirement	PoE 802.3af compliant
	or 8 to 12 VDC at 1000 mA
Sound volume level	87db at 1 meter
Protocol	SIP
Part Number	011216
Dimensions	4.53" x 4.53" x 2.11" (H x W x D)
Weight	0.71 lbs./shipping weight of 1.1 lbs.
	(0.32 kg/shipping weight of 0.5 kg)
Auxiliary Relay	1 A at 30 VDC

2 Installing the SIP Office Ringer

2.1 Parts List

Table 2-1 illustrates the SIP Office Ringer parts.

Table 2-1. Parts List

Quantity	Part Name	Illustration
1	Office Ringer Assembly	
1	Installation Quick Reference Guide	
1	Office Ringer Mounting Accessory Kit	

2.2 Office Ringer Setup

2.2.1 Office Ringer Connections

Figure 2-5 shows the pin connections on the J3 (terminal block). This terminal block can accept 16 AWG gauge wire.

Note   As an alternative to using PoE power, you can supply 8 to 12 VDC at 1000 mA into the terminal block.

⚠️ **GENERAL ALERT**

Caution

Equipment Hazard: Contacts 1 and 2 on the J3 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 2-5. Connections

Alternate Power Input:
1 = 8 to 12 VDC at 1000 mA*
2 = Power Ground*

3   4

Relay Contact:
(1 A at 30 VDC for continuous loads)
3 = Relay Common
4 = Relay Normally Open Contact
5 = Sense Input
6 = Sense Ground
7 = Reserved for Future Use
8 = Reserved for Future Use

*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.

Wire (IN)

Use a 3.17 mm (1/8-inch) flat blade screwdriver for the terminal block screws

1

8

J3 Terminal Block can accept 16 AWG wire

2.2.2 Using the On-Board Relay

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

	Warning
⚠️ GENERAL ALERT	*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
⚠️ GENERAL ALERT	*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 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 have caused excessive "hum" and can interfere with 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 2.2.3.2, "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.

2.2.3 Wiring the Circuit

2.2.3.1 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 2-6 for the wiring diagram.

Figure 2-6. Wiring Diagram

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.

Strobe Light

1

8

J3 Terminal Block of the CyberData Device

Sense Input

DC Source
1 A @ 30 VDC
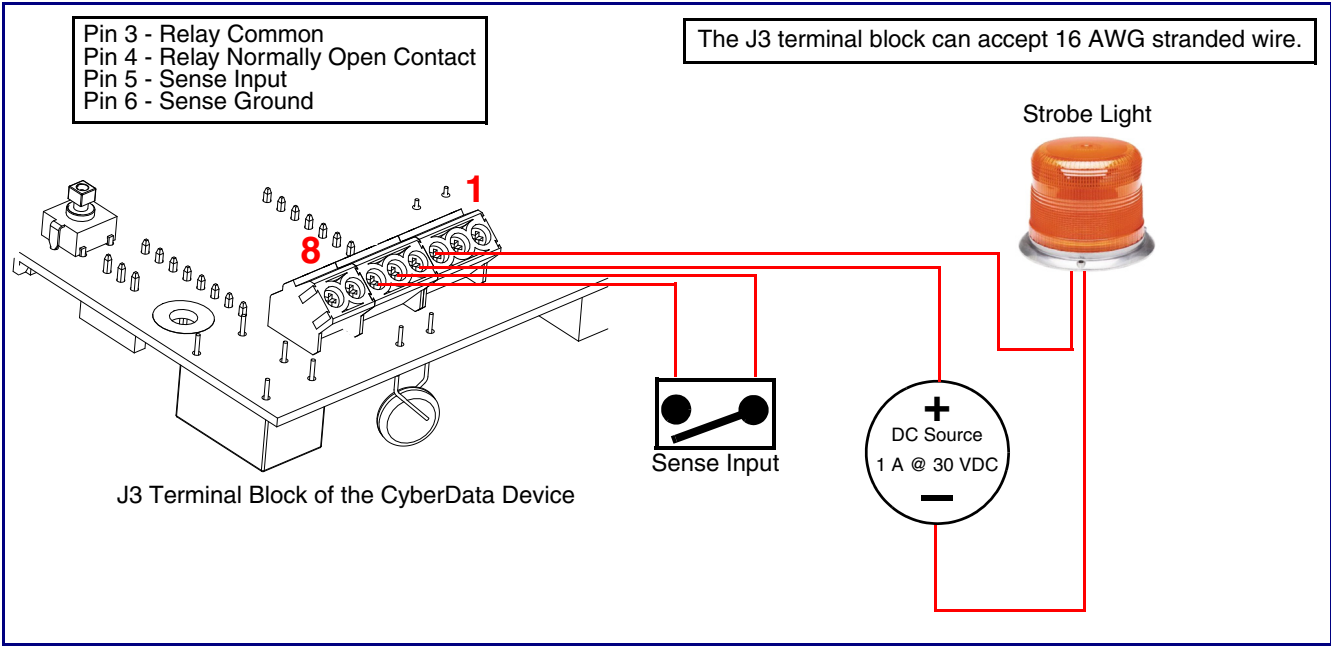
2.2.3.2 Connecting the Door Strike Intermediate Relay Module

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 2-7 for the wiring diagram.

Figure 2-7. Wiring Diagram
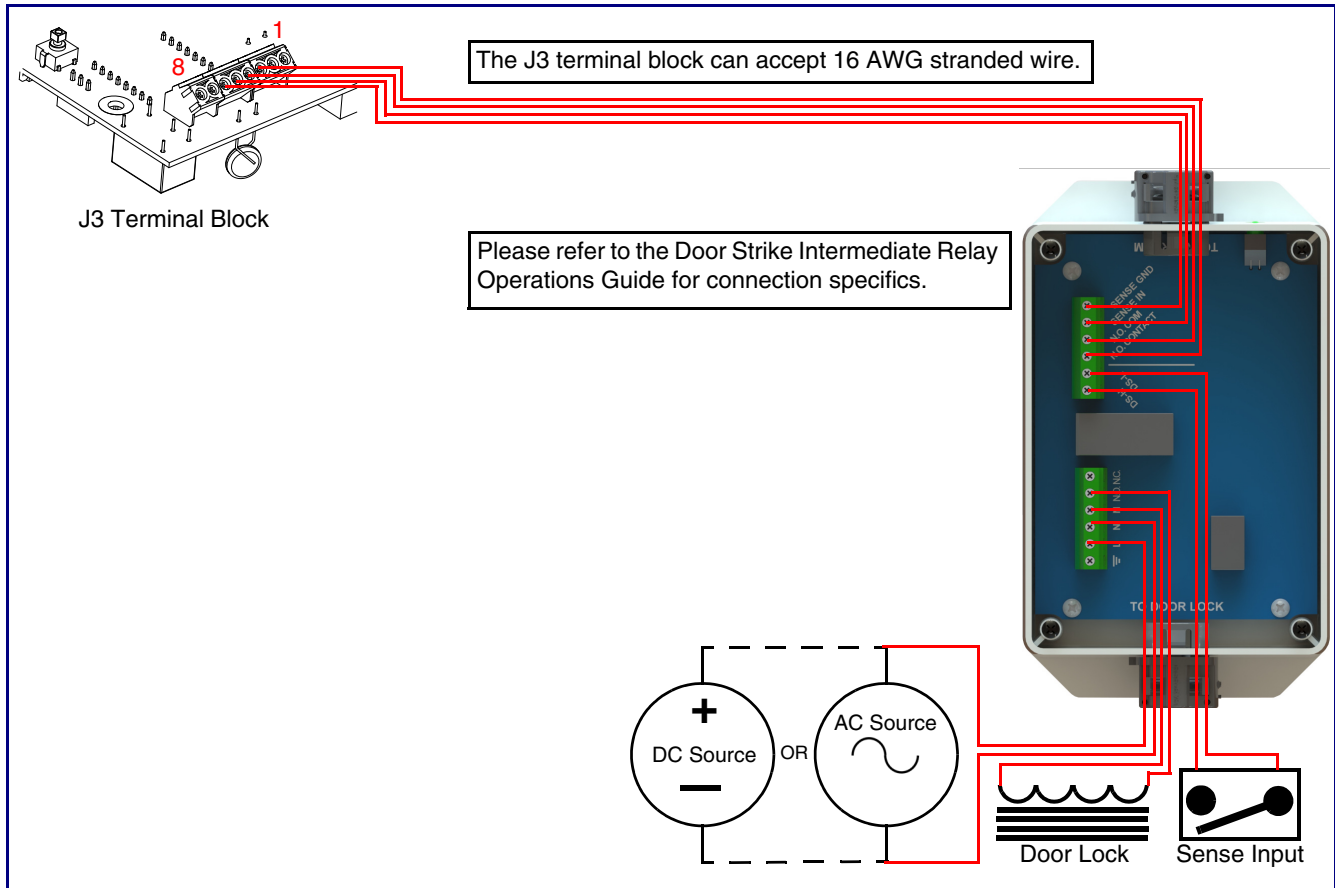
If you have questions about connecting door strikes or setting up the web configurable options, please contact our support department.

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

2.2.3.3 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 2-8 for the wiring diagram.

Figure 2-8. Wiring Diagram
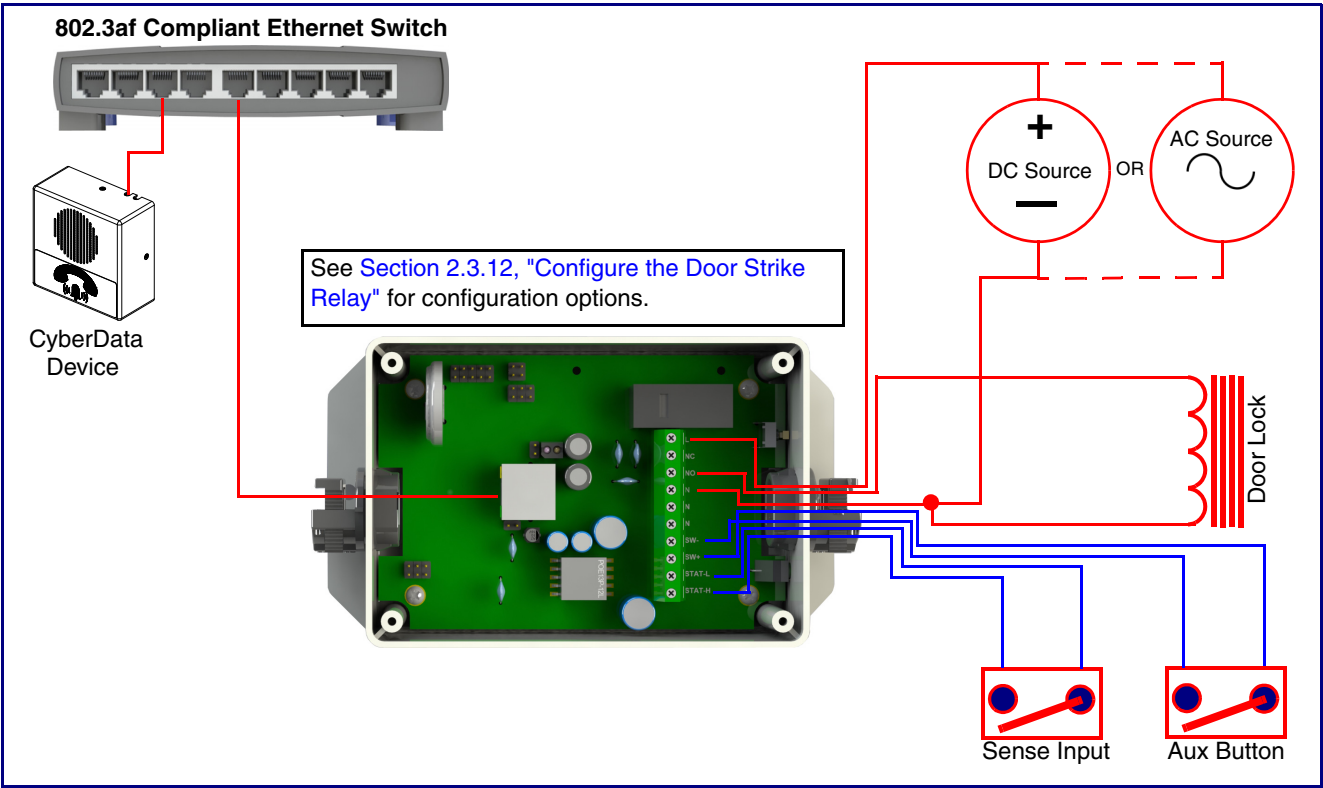
2.2.4 Identifying the Office Ringer Connectors

See the following Figures and Tables to identify the connectors and functions.

Figure 2-9. Connector Locations

.
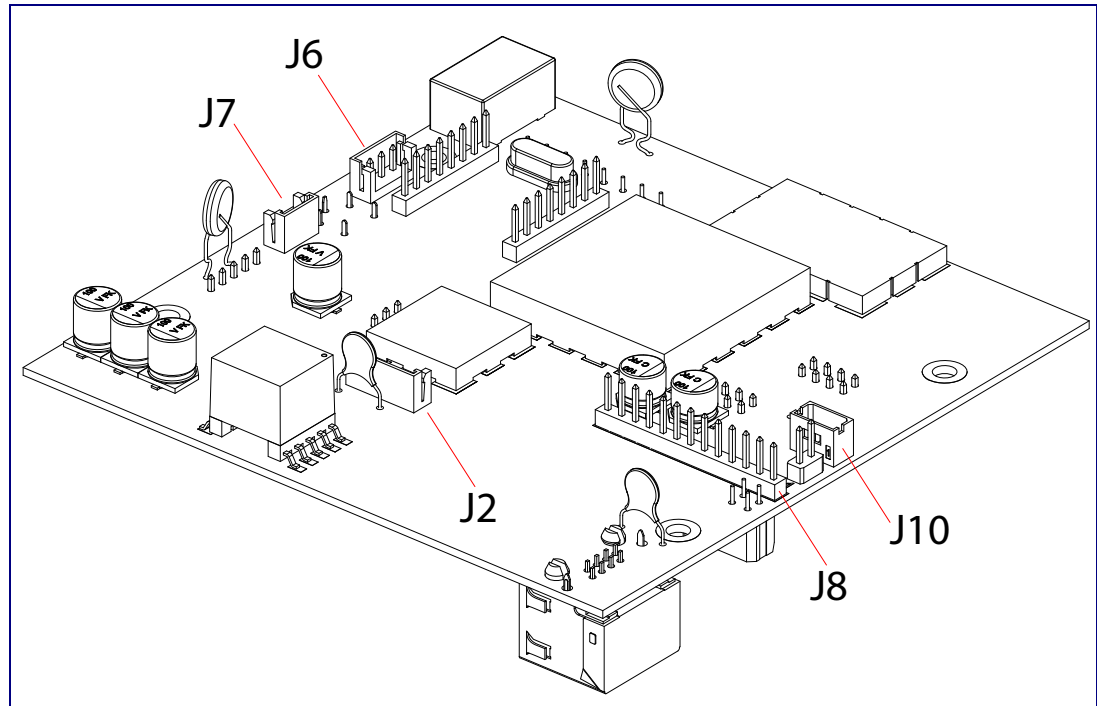
Table 2-2. Connector Functions

Connector	Function
J2	Call Button. LED Interface
J6	Microphone Interface — Not Used
J7	Speaker Interface
J8	Keypad Interface — Not Used
J10	Proximity Sensor Interface - N/A

Figure 2-10. Connector Locations
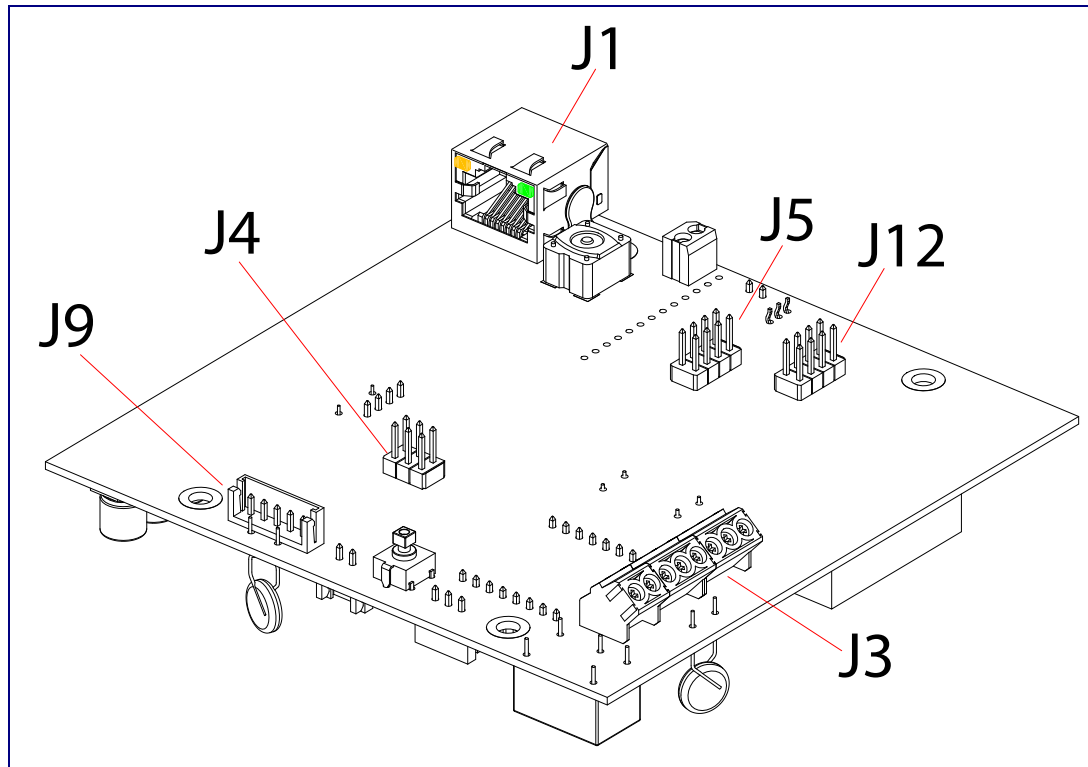
Table 2-3. Connector Functions

Connector	Function
J1	PoE Network Connection (RJ-45 ethernet)
J3	Terminal Block (see Figure 2-5)
J4	Factory Only—Console Port
J5	Factory Only—JTAG
J9	Auxiliary Strobe Connector (optional)
J12	Reserved for Factory Diagnostics

2.2.5 Auxiliary Strobe Connector

Figure 2-11 shows the location of the connector for the optional Auxiliary Strobe (sold separately).

Figure 2-11. Auxiliary Strobe Connector
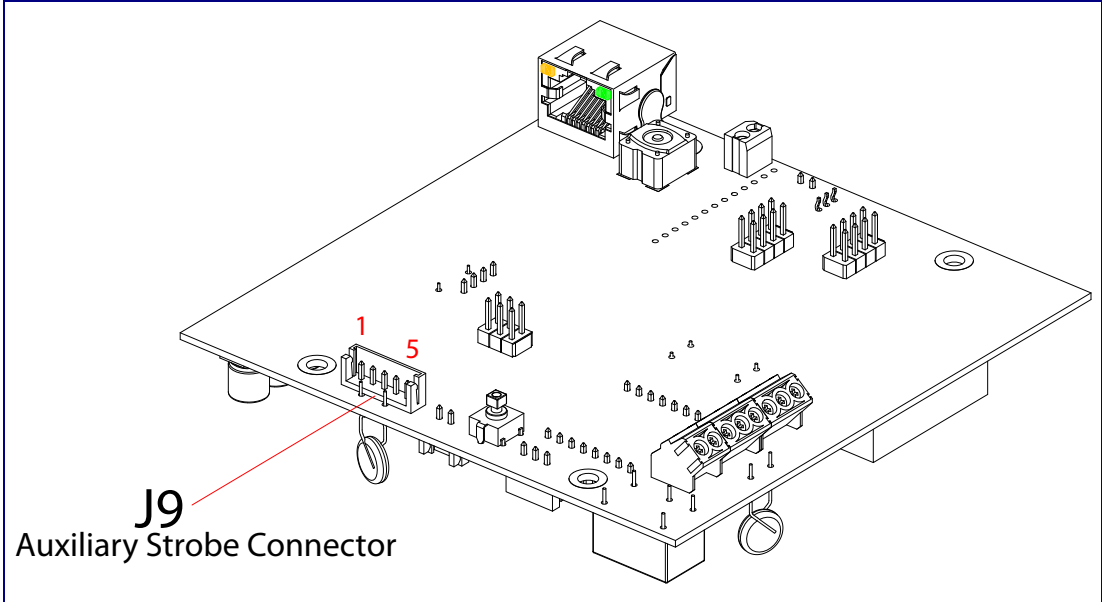
2.2.6 Activity and Link LEDs

2.2.6.1 Verifying the Network Connectivity and Data Rate

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

- The square, **YELLOW Activity** LED blinks when there is network activity (see Figure 2-12).

- The square, **GREEN Link** LED above the Ethernet port indicates that the network connection has been established (see Figure 2-12).

Figure 2-12. Activity and Link LED
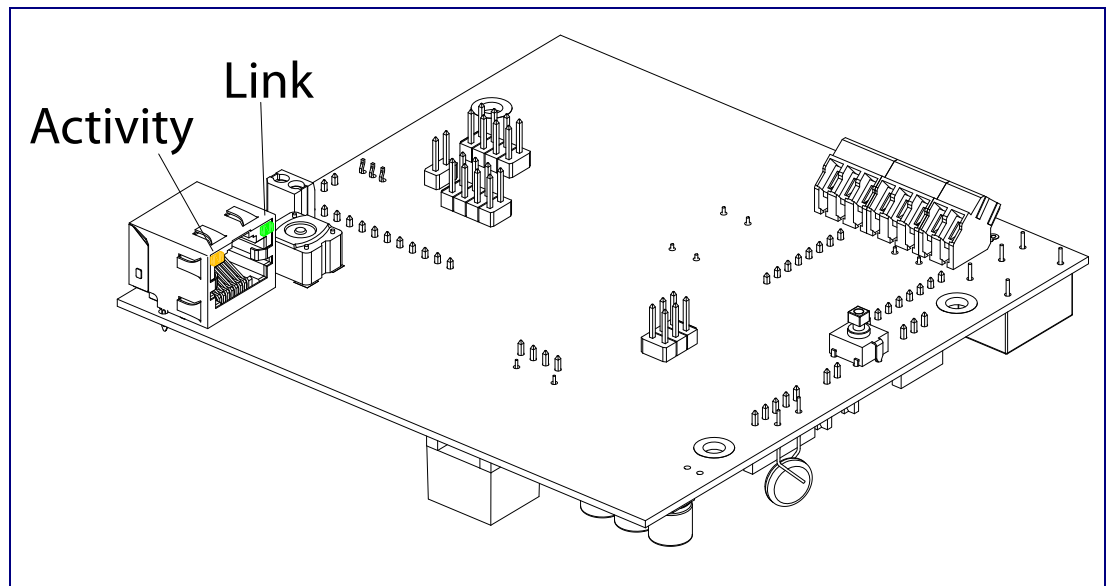
2.2.7 RTFM Button

When the Office Ringer is operational and linked to the network, you can use the Reset Test Function Management **(RTFM)** button (see Figure 2-13) on the Office Ringer board to announce and confirm the Office Ringer's IP Address and test to see if the audio is working.

Note   You must do these tests prior to final assembly.

Figure 2-13. RTFM Button (SW1)
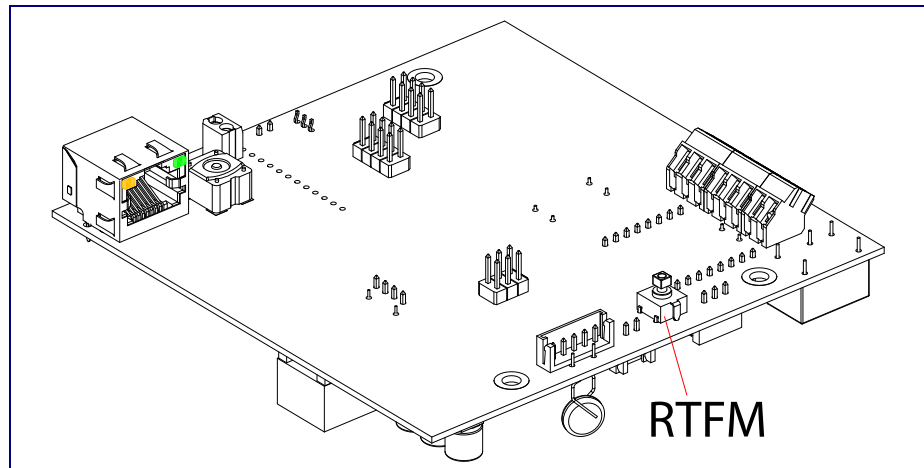
2.2.7.1 Announcing the IP Address

To announce a device's current IP address:

1. Press and release the RTFM button (see Figure 2-14) 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 2-14. RTFM Button (SW1)
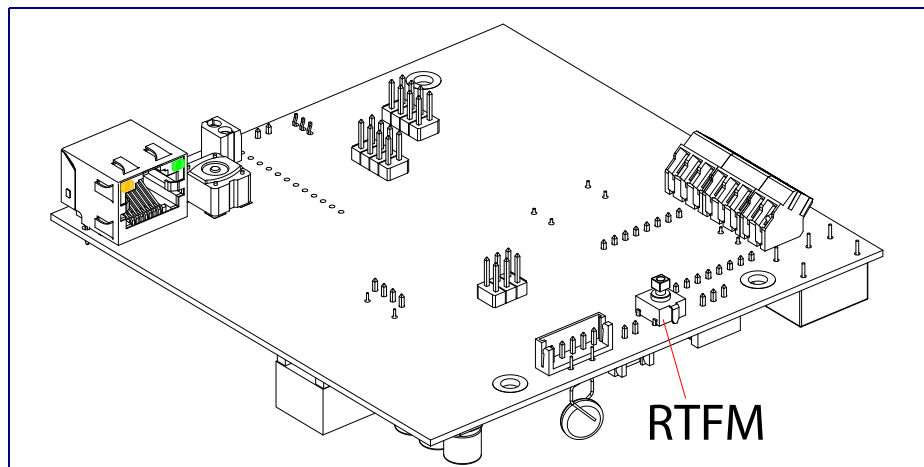
2.2.7.2 Restoring the Factory Default Settings

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

Note   Each Office Ringer is delivered with factory set default values.

To restore the factory default settings:

1. Press and hold the **RTFM button** (see **SW1** in Figure 2-15) 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 2-15. RTFM Button
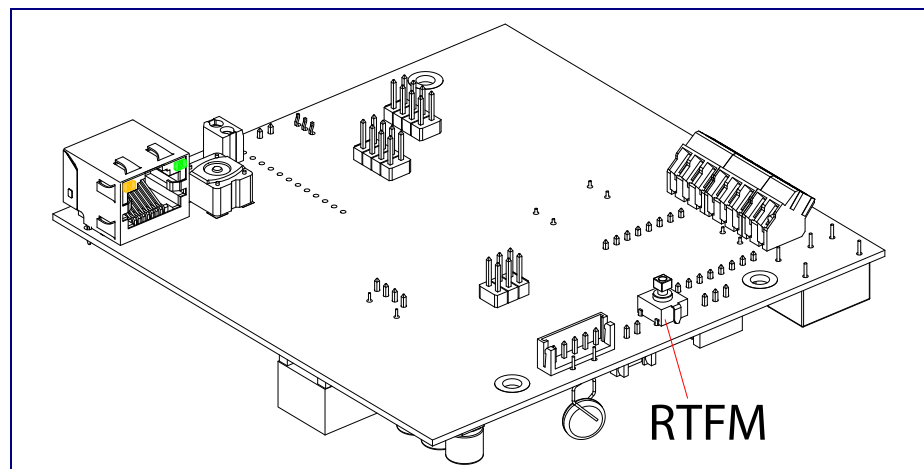
2.2.8 Adjust the Volume

You can adjust the volume through the SIP Volume setting on the Device Configuration Page.

2.3 Configure the Office Ringer Parameters

To configure the Office Ringer online, use a standard web browser.

Configure each Office Ringer and verify its operation *before* you mount it. When you are ready to mount an Office Ringer, refer to Section A.1, "Mount the Office Ringer" for instructions.

2.3.1 Factory Default Settings

All Office Ringers are initially configured with the following default IP settings:

When configuring more than one Office Ringer, attach the Office Ringers to the network and configure one at a time to avoid IP address conflicts.

Table 2-4. Factory Default Settings
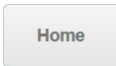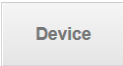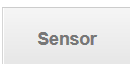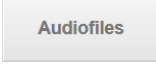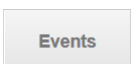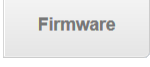
Parameter	Factory Default Setting
IP Addressing	DHCP
IP Address[a]	10.10.10.10
Web Access Username	admin
Web Access Password	admin
Subnet Mask[a]	255.0.0.0
Default Gateway[a]	10.0.0.1

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

2.3.2 Office Ringer Web Page Navigation

Table 2-5 shows the navigation buttons that you will see on every Office Ringer web page.

Table 2-5. Web Page Navigation

Web Page Item	Description
Home	Link to the **Home** page.
Device	Link to the **Device** page.
Network	Link to the **Network** page.
SIP	Link to go to the **SIP** page.
Multicast	Link to the **Multicast** page.
Sensor	Link to the **Sensor** page.
Audiofiles	Link to the **Audiofiles** page.
Events	Link to the **Events** page.
DSR	Link to the **Door Strike Relay** page.
Autoprov	Link to the **Autoprovisioning** page.
Firmware	Link to the **Firmware** page.

2.3.3 Using the Toggle Help Button

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

1. Click on the **Toggle Help** button that is on the UI webpage. See Figure 2-16 and Figure 2-17.

Figure 2-16. Toggle/Help Button
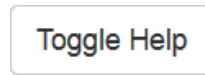
2. You will see a question mark (?) appear next to each web page item that has been provided with a short description by the Help feature. See Figure 2-17.

Figure 2-17. Toggle Help Button and Question Marks
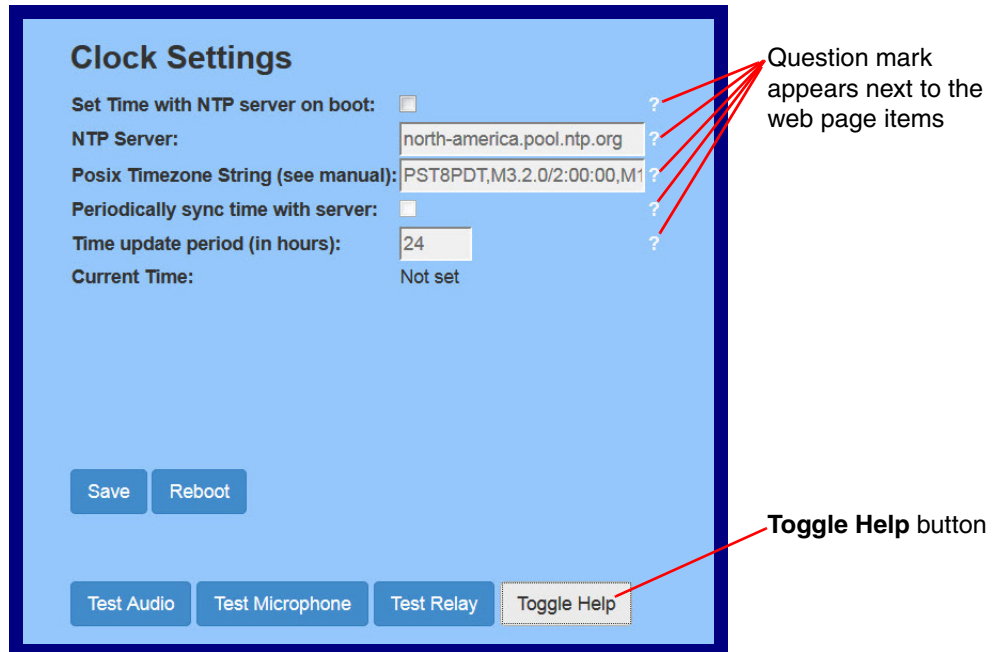
3. Move the mouse pointer to hover over the question mark (?), and a short description of the web page item will appear. See Figure 2-18.

Figure 2-18. Short Description Provided by the Help Feature

Question mark

A short description of the web page item will appear
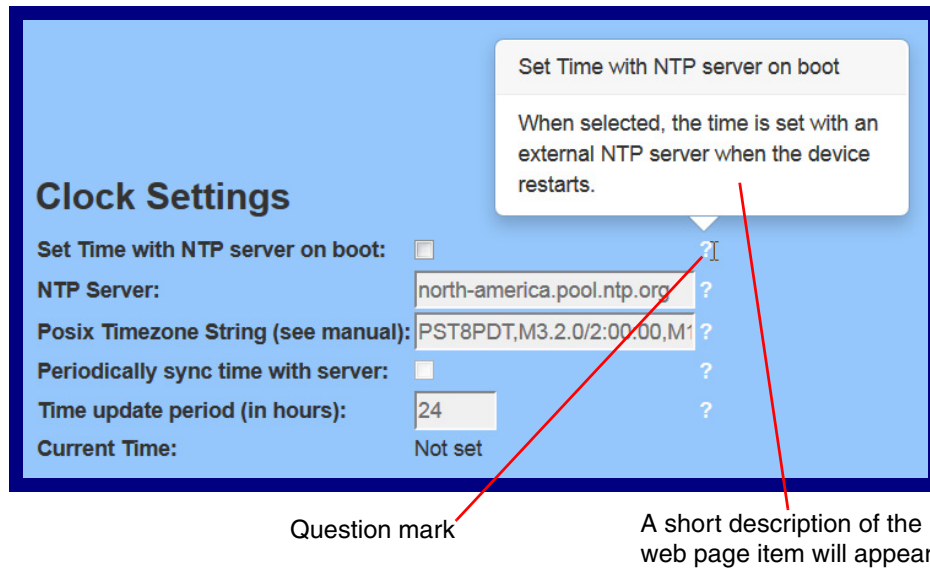
2.3.4 Log in to the Configuration Home Page

1. Open your browser to the Office Ringer 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 Office Ringer.

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/support/voip/discovery.html

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

2. When prompted, use the following default **Web Access Username** and **Web Access Password** to access the **Home Page** (Figure 2-19):

Web Access Username: **admin**

Web Access Password: **admin**

Figure 2-19. 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

Web Page Item	Description
Admin Settings	
Username ?	The username to access the web interface. Enter up to 25 characters.
Password ?	The password to access the web interface. Enter up to 25 characters.
Confirm Password ?	Confirm the web interface password.
Current Status	
Serial Number	Shows the device serial number.
Mac Address	Shows the device Mac address.
Firmware Version	Shows the current firmware version.
IP Addressing	Shows the current IP addressing setting (**DHCP** or **static**).
IP Address	Shows the current IP address.
Subnet Mask	Shows the current subnet mask address.
Default Gateway	Shows the current default gateway address.
DNS Server 1	Shows the current DNS Server 1 address.
DNS Server 2	Shows the current DNS Server 2 address.
SIP Volume	Shows the current SIP volume level.
Multicast Volume	Shows the current Multicast volume level.
Ring Volume	Shows the current Ring volume level.
Sensor Volume	Shows the current Sensor volume level.
Volume Boost	Shows the current Volume Boost level.
Microphone Gain	Shows the current microphone gain level.
SIP Mode	Shows the current status of the SIP mode.
Multicast Mode	Shows the current status of the Multicast mode.
Event Reporting	Shows the current status of the Event Reporting mode.
Nightringer	Shows the current status of the Nightringer mode.
Primary SIP Server	Shows the current status of the Primary SIP Server.
Backup Server 1	Shows the current status of Backup Server 1.
Backup Server 2	Shows the current status of Backup Server 2.
Nightringer Server	Shows the current status of Nightringer Server.
Import Settings	
Browse... ?	Use this button to select a configuration file to import.
Import Config ?	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)

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

2.3.5 Configure the Device

1. Click the **Device** menu button to open the **Device** page. See Figure 2-20.

Figure 2-20. Device Configuration Page

2. On the **Device** page, you may enter values for the parameters indicated in Table 2-7.

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

Table 2-7. Device Configuration Parameters

Web Page Item	Description
Volume Settings (0-9)	
SIP Volume ?	Set the speaker volume for a SIP call. A value of 0 will mute the speaker during SIP calls.
Multicast Volume ?	Set the speaker volume for multicast audio streams. A value of 0 will mute the speaker during multicasts.
Ring Volume ?	Set the ring volume for incoming calls. A value of 0 will mute the speaker instead of playing the ring tone when Auto-Answer Incoming Calls is disabled.
Sensor Volume ?	Set the speaker volume for playing sensor activated audio. A value of 0 will mute the speaker during sensor activated audio.
Relay Settings	
Activate Relay with DTMF Code ?	Activates the relay when the DTMF Activation Code is entered on the phone during a SIP call with the device. RFC2833 DTMF payload types are supported.
DTMF Activation Code ?	Activation code used to activate 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).
DTMF Activation Duration (in seconds) ?	The length of time (in seconds) during which the relay will be activated when the DTMF Activation Code is detected. Enter up to 5 digits. **NOTE**: A DTMF activation duration of 0 will toggle the relay indefinitely or until the activation code is sent again
Play tone during DTMF Activation ?	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).
Activate Relay During Ring ?	When selected, the relay will be activated for as long as the device is ringing. When Auto-Answer Incoming Calls is enabled, the device will not ring and this option does nothing.
Activate Relay During Night Ring ?	When selected, the relay will be activated as long as the Nightringer extension is ringing.
Activate Relay While Call Active ?	When selected, the relay will be activated as long as the SIP call is active.
Clock Settings	
Set Time with NTP Server on boot ?	When selected, the time is set with an external NTP server when the device restarts.
NTP Server ?	Use this field to set the address (in IPv4 dotted decimal notation or as a canonical name) for the NTP Server. This field can accept canonical names of up to 64 characters in length.
Posix Timezone String ?	See Section 2.3.5.1, "Time Zone Strings" for information about how to use the Posix Timezone String to specify time zone and daylight savings time where applicable. Enter up to 63 characters.

Table 2-7. Device Configuration Parameters (continued)

Web Page Item	Description
Periodically sync time with server ?	When selected, the time is periodically updated with the NTP server at the configured interval below.
Time update period (in hours) ?	The time interval after which the device will contact the NTP server to update the time. Enter up to 4 digits.
Current Time	Allows you to input the current time. (6 character limit)
Misc Settings	
Device Name ?	Type the device name. Enter up to 25 characters.
Auto-Answer Incoming Calls ?	When selected, the device will automatically answer incoming calls. When Auto-Answer Incoming Calls is disabled, the device will play a ring tone (corresponds to Ring Tone on the Audiofiles page) out of the speaker until the caller disconnects the call.
Play Ringback Tone ?	When selected, the device will play a ringback tone (corresponds to Ringback Tone on the Audiofiles page) out of the speaker while placing an outbound call. The Ringback Tone will play until the call is answered.
Disable HTTPS (NOT recommended) ?	Disables the encrypted connection to the webpage. We do not recommend disabling HTTPS for security reasons.
Test Audio	Click on the **Test Audio** button to do an audio test. When the **Test Audio** button is pressed, you will hear a voice message for testing the device audio quality and volume.
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**, and **Sensor Volume** without rebooting the device. You must save and reboot the device for other changes to take effect.

2.3.5.1 Time Zone Strings

The posix time zone string tells the internal date and time utilities how to handle daylight savings time for different time zones. Table 2-8 shows some common strings.

Table 2-8. Common Time Zone Strings

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

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

Table 2-9 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

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

Time Zone String
Examples

Table 2-10 has some more examples of time zone strings.

Table 2-10. Time Zone String Examples

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

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

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

Figure 2-21. Three or Four Character Time Zone Identifier

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

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

World GMT Table   Table 2-11 has information about the GMT time in various time zones.

Table 2-11. World GMT Table

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

Table 2-11. World GMT Table (continued)

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

2.3.6 Configure the Network Parameters

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

Figure 2-22. 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 2-12. Network Configuration Parameters

Web Page Item	Description
Stored Network Settings	
Addressing Mode ?	Select either DHCP IP Addressing or Static Addressing by marking the appropriate radio button. DHCP Addressing mode is enabled on default and the device will attempt to resolve network addressing with the local DHCP server upon boot. If DHCP Addressing fails, the device will revert to the last known IP address or the factory default address if no prior DHCP lease was established. See Section 2.3.1, "Factory Default Settings" for factory default settings. Be sure to click **Save** and **Reboot** to store changes when configuring a Static address.
Hostname ?	This is the hostname provided by the DHCP server. See the DHCP/DNS server documentation for more information. Enter up to 64 characters.
IP Address ?	Enter the Static IPv4 network address in dotted decimal notation.
Subnet Mask ?	Enter the Subnet Mask in dotted decimal notation.
Default Gateway ?	Enter the Default Gateway IPv4 address in dotted decimal notation.
DNS Server 1 ?	Enter the primary DNS Server IPv4 address in dotted decimal notation.
DNS Server 2 ?	Enter the secondary DNS Server IPv4 address in dotted decimal notation.
DHCP Timeout in seconds ?	Specify the desired time-out duration (in seconds) that the device will wait for a response from the DHCP server before reverting back to the stored static IP address. The stored static IP address may be the last known IP address or the factory default address if no prior DHCP lease was established. Enter up to 8 characters. A value of -1 will retry forever.
Current Network Settings	Shows the current network settings.
IP Address	Shows the current Static IP address.
Subnet Mask	Shows the current Subnet Mask address.
Default Gateway	Shows the current Default Gateway address.
DNS Server 1	Shows the current DNS Server 1 address.
DNS Server 2	Shows the current DNS Server 2 address.
VLAN Settings	
VLAN ID (0-4095) ?	Specify the IEEE 802.1Q VLAN ID number. Enter up to 4 digits. **Note**: The device supports 802.1Q VLAN tagging support. The switch port connected to the device will need to be in "trunking mode" for the VLAN tags to propagate.
VLAN Priority (0-7) ?	Specify the IEEE 802.1p VLAN priority level. Enter 1 digit. A value of 0 may cause the VLAN ID tag to be ignored.

Table 2-12. Network Configuration Parameters (continued)

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

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

2.3.7 Configure the SIP Parameters

1. Click on the **SIP** menu button to open the **SIP** page (Figure 2-23).

Figure 2-23. SIP Configuration Page

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

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

Table 2-13. SIP Configuration Parameters

Web Page Item	Description
SIP Settings	
Enable SIP Operation ?	When enabled, the device will transmit, receive, and process SIP messages according to the configured SIP settings below.
Register with a SIP Server ?	When enabled, the device will attempt to register to the configured SIP Server(s) on this page. To configure the device to send and receive point-to-point SIP calls, enable **SIP Operation** and disable **Register with a SIP Server** (see Section 2.3.7.2, "Point-to-Point Configuration").
Use Cisco SRST ?	When enabled, the backup servers are handled according to Cisco SRST (Survivable Remote Site Telephony). It is required for use in clustered Cisco Unified Communications Manager topologies.
Primary SIP Server ?	Enter the SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the primary SIP server. This field can accept entries of up to 255 characters in length.
Primary SIP User ID ?	Specify the SIP User ID for the Primary SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the primary SIP server. Enter up to 64 alphanumeric characters.
Primary SIP Auth ID ?	Specify the Authenticate ID for the Primary SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Primary SIP Auth Password ?	Specify the Authenticate Password for the Primary SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Server 1 ?	Enter the backup SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the backup SIP server. This field can accept entries of up to 255 characters in length.
Backup SIP User ID 1 ?	Specify the SIP User ID for the first backup SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the first backup SIP server. Enter up to 64 alphanumeric characters.
Backup SIP Auth ID 1 ?	Specify the Authenticate ID for the first backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Auth Password 1 ?	Specify the Authenticate Password for the first backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Server 2 ?	Enter a second backup SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the second backup SIP server. This field can accept entries of up to 255 characters in length.

Table 2-13. SIP Configuration Parameters (continued)

Web Page Item	Description
Backup SIP User ID 2 [?]	Specify the SIP User ID for the second backup SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the second backup SIP server. Enter up to 64 alphanumeric characters.
Backup SIP Auth ID 2 [?]	Specify the Authenticate ID for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Auth Password 2 [?]	Specify the Authenticate Password for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Remote SIP Port [?]	The Remote SIP Port is the port number the device will use as the destination port when sending SIP messages. The default Remote SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
Local SIP Port [?]	The Local SIP Port is the port number the device will use to receive SIP messages. The default Local SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
Outbound Proxy [?]	Enter the Outbound Proxy address as an IPv4 address in dotted decimal notation or a fully qualified domain name (FQDN). When an IP address is configured, the device will send all SIP messages to this IP address. When an FQDN is configured, the device will run DNS NAPTR, SRV, and A queries on the FQDN to resolve an IP address to which it will send all SIP messages. This field can accept entries of up to 255 characters in length.
Outbound Proxy Port [?]	The Outbound Proxy Port is port number used as the destination port when sending SIP messages to the outbound proxy. A value of 0 will default to 5060. The supported range is 0-65536. Enter up to 5 digits.
Disable rport Discovery [?]	Disabling rport Discovery will prevent the device from including the public WAN IP address and port number in the contact information that is sent to the remote SIP servers. This will generally only need to be enabled when using an SBC or SIP ALG in conjunction with a remote SIP server.
Re-registration Interval (in seconds) [?]	The SIP Re-registration interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
Unregister on Boot [?]	When enabled, the device will send one registration with an expiry of 0 on boot.
Keep Alive Period [?]	The minimum time in milliseconds between keep-alive packets sent for nat traversal. A value of 0 will disable keep alive packets.
RTP Settings	
RTP Port (even) [?]	Specify the port number used for the RTP stream after establishing a SIP call. This port number must be an even number and defaults to 10500. The supported range is 0-65536. Enter up to 5 digits.
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)

Web Page Item	Description
SIP Server ?	Enter the SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's Nightringer extension on the SIP server. This field can accept entries of up to 255 characters in length.
Remote SIP Port ?	The Remote SIP Port is the port number the device will use as the destination port when sending SIP messages for the Nightringer extension. The default Remote SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
Local SIP Port ?	The Local SIP Port is the port number the device will use to receive SIP messages for the Nightringer extension. This value cannot be the same as the **Local SIP Port** for the primary extension. The default Local SIP Port is 5061. The supported range is 0-65536. Enter up to 5 digits.
Outbound Proxy ?	Enter the Outbound Proxy address as an IPv4 address in dotted decimal notation or a fully qualified domain name (FQDN). When an IP address is configured, the device will send all SIP messages to this IP address for the Nightringer extension. When an FQDN is configured, the device will run DNS NAPTR, SRV, and A queries on the FQDN to resolve an IP address to which it will send all SIP messages for the Nightringer extension. This field can accept entries of up to 255 characters in length.
Outbound Proxy Port ?	The Outbound Proxy Port is port number used as the destination port when sending SIP messages to the outbound proxy for the Nightringer extension. A value of 0 will default to 5060. The supported range is 0-65536. Enter up to 5 digits.
User ID ?	Specify the SIP User ID for the SIP server. This parameter becomes the user portion of the SIP-URI for the device's Nightringer extension. Enter up to 64 alphanumeric characters.
Authenticate ID ?	Specify the Authenticate ID for the SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Authenticate Password ?	Specify the Authenticate Password for the SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Re-registration Interval (in seconds) ?	The SIP Re-registration Interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
Dial Out Settings	
Dial Out Extension ?	Specify the extension the device will call. Enter up to 64 alphanumeric characters. **Note**: For information about dial-out extension strings and DTMF tones, see Section 2.3.7.1, "Dial Out Extension Strings and DTMF Tones (using rfc2833)".
Extension ID ?	A Caller identification string added to outbound calls. Enter up to 64 alphanumeric characters.
Call Disconnection	
Terminate Call After Delay ?	Automatically terminate an active call after a given delay in seconds. A value of 0 will disable this function. Enter up to 8 digits.

Table 2-13. SIP Configuration Parameters (continued)

Web Page Item	Description
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/support/server/index.html

2.3.7.1 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

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

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

2.3.7.2 Point-to-Point Configuration

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

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

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

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

Device is set to NOT register with a SiP server

2.3.7.3 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

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

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

2.3.8 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 2-25. 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 2-16. Multicast Configuration Parameters

Web Page Item	Description
Enable Multicast Operation	Enables or disables multicast operation.
Priority	Indicates the priority for the multicast group. Priority **9** is the highest (emergency streams). **0** is the lowest (background music). SIP calls are considered priority **4.5**. See Section 2.3.8.1, "Assigning Priority" for more details.
Address	Enter the multicast IP Address for this multicast group (15 character limit).
Port	Enter the port number for this multicast group (5 character limit [range can be from 2000 to 65535]). **Note**: The multicast ports have to be even values. The webpage will enforce this restriction.
Name	Assign a descriptive name for this multicast group (25 character limit).
Beep	When selected, the device will play a beep before multicast audio is sent.
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.

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

2.3.8.1 Assigning Priority

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

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

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

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

Ringtones and Nightringtones

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

2.3.9 Configure the Sensor Configuration Parameters

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

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

Each sensor can trigger up to five different actions:

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

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

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

Figure 2-26. 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

Web Page Item	Description
Door Sensor Settings	
Door Sensor Normally Closed ?	Select the inactive state of the door sensor. The door sensor is also known as the Sense Input on the device's terminal block.
Door Open Timeout (in seconds) ?	The time (in seconds) the device will wait before it performs an action when the on-board door sensor is activated. The action(s) performed are based on the configured Door Sensor Settings below. Enter up to 5 digits.
Activate Relay ?	When selected, the device's on-board relay will be activated until the on-board door sensor is deactivated.
Play Audio Locally ?	When selected, the device will loop an audio file out of the speaker until the door sensor is deactivated.
Make call to extension ?	When selected, the device will call an extension when the on-board door sensor is activated. Use the **Dial Out Extension** field below to specify the extension the device will call.
Dial Out Extension ?	Specify the extension the device will call when the on-board door sensor is activated. Enter up to 64 alphanumeric characters.
Dial Out ID ?	An additional Caller identification string added to outbound calls. Enter up to 64 alphanumeric characters.
Play recorded audio ?	When selected, the device will call the **Dial Out Extension** and play an audio file to the phone answering the SIP call (corresponds to **Door Ajar** on the **Audiofiles** page).
Intrusion Sensor Settings	
Activate Relay ?	When selected, the device's on-board relay will be activated until the intrusion sensor is deactivated.
Play Audio Locally ?	When selected, the device will loop an audio file out of the speaker until the intrusion sensor is deactivated.
Make call to extension ?	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.
Dial Out Extension ?	Specify the extension the device will call when the intrusion sensor is activated. Enter up to 64 alphanumeric characters.
Dial Out ID ?	An additional Caller identification string added to outbound calls. Enter up to 64 alphanumeric characters.
Play recorded audio ?	When selected, the device will call the **Dial Out Extension** and play an audio file (corresponds to **Intrusion Sensor Triggered** on the **Audiofiles** page) to the phone answering the SIP call when the intrusion sensor is activated.
Test Door Sensor	Click the T**est Door Sensor** button to test the door sensor.

Table 2-17. Sensor Configuration Parameters (continued)

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

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

2.3.10 Configure the Audio Configuration Parameters

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

1. Click on the **Audiofiles** menu button to open the **Audiofiles** page (Figure 2-27).

Figure 2-27. Audiofiles Configuration Page
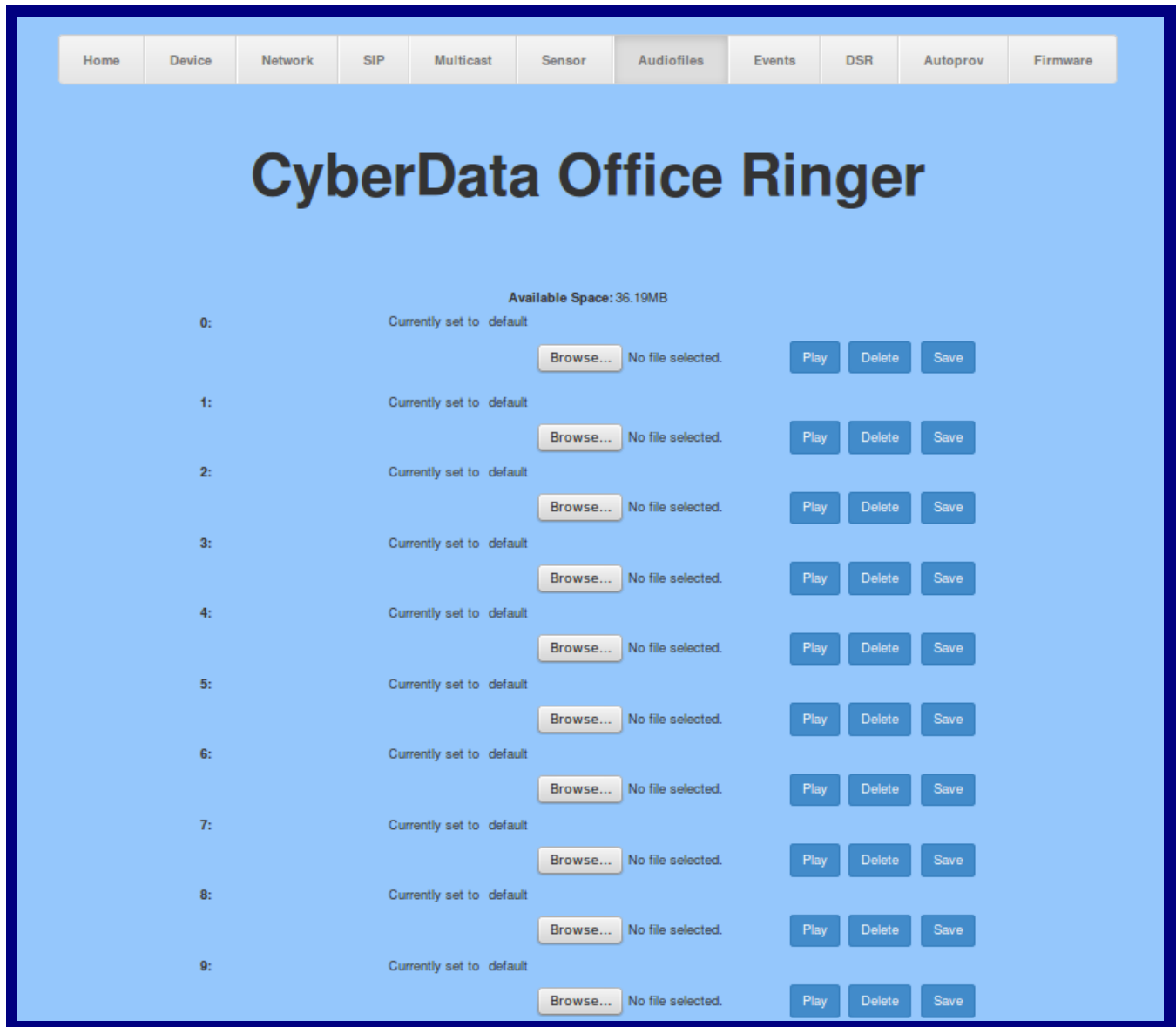
Figure 2-28. Audiofiles Page

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

Web Page Item	Description
Available Space	Shows the space available for the user to save custom audio files if they want to change the message when the door or sensor is triggered.
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)

Web Page Item	Description
0-9	'5' corresponds to the spoken word "five."
	'6' corresponds to the spoken word "six."
	'7' corresponds to the spoken word "seven."
	'8' corresponds to the spoken word "eight."
	'9' corresponds to the spoken word "nine."
Dot	Corresponds to the spoken word "dot." (24 character limit)
Audiotest	Corresponds to the message ***"This is the CyberData IP speaker test message..."*** (24 character limit)
Page tone	Corresponds to a simple tone used for beep on initialization and beep on page (24 character limit).
Your IP Address is	Corresponds to the message "Your IP address is..." (24 character limit).
Rebooting	Corresponds to the spoken word "Rebooting" (24 character limit).
Restoring default	Corresponds to the message "Restoring default" (24 character limit).
Ringback tone	This is the ringback tone that plays when calling a remote extension (24 character limit).
Ring Tone	This is the tone that plays when set to ring when receiving a call (24 character limit).
Intrusion Sensor Triggered	Corresponds to the message "Intrusion Sensor Triggered" (24 character limit).
Door Ajar	Corresponds to the message "Door Ajar" (24 character limit).
Night Ring	Specifies the ringtone for nightring. By default this parameter uses the same audio file that is selected for the **Ring Tone** parameter.
Browse...	Click on the **Browse** button to navigate to and select an audio file.
Play	The **Play** button will play that audio file.
Delete	The **Delete** button will delete any user uploaded audio and restore the stock audio file.
Save	The **Save** button will download a new user audio file to the board once you've selected the file by using the **Browse** button. The **Save** button will delete any pre-existing user-uploaded audio files.

2.3.10.1 User-created Audio Files

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

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

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

Figure 2-29. Audacity 1
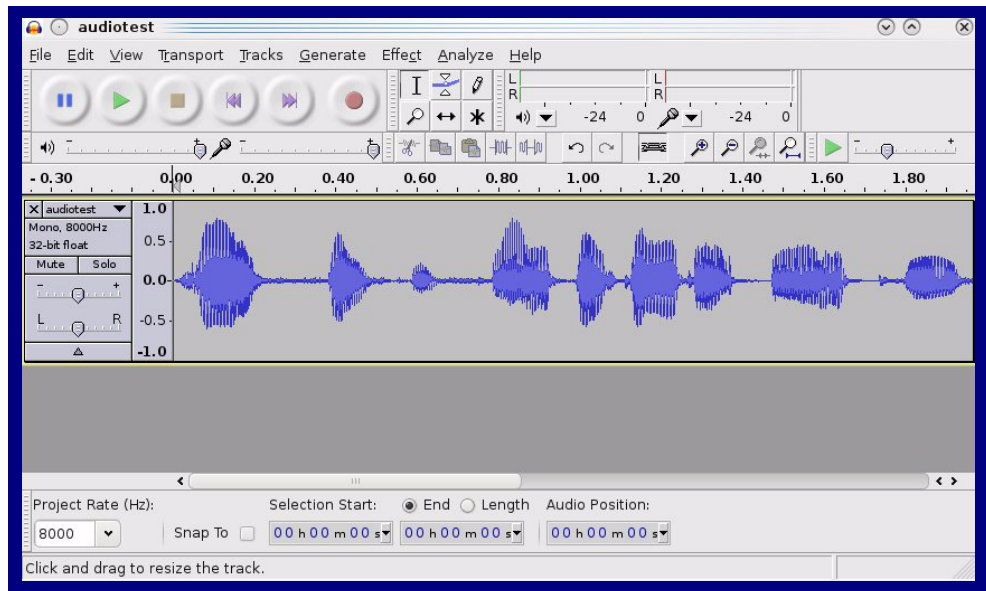
Figure 2-30. Audacity 2
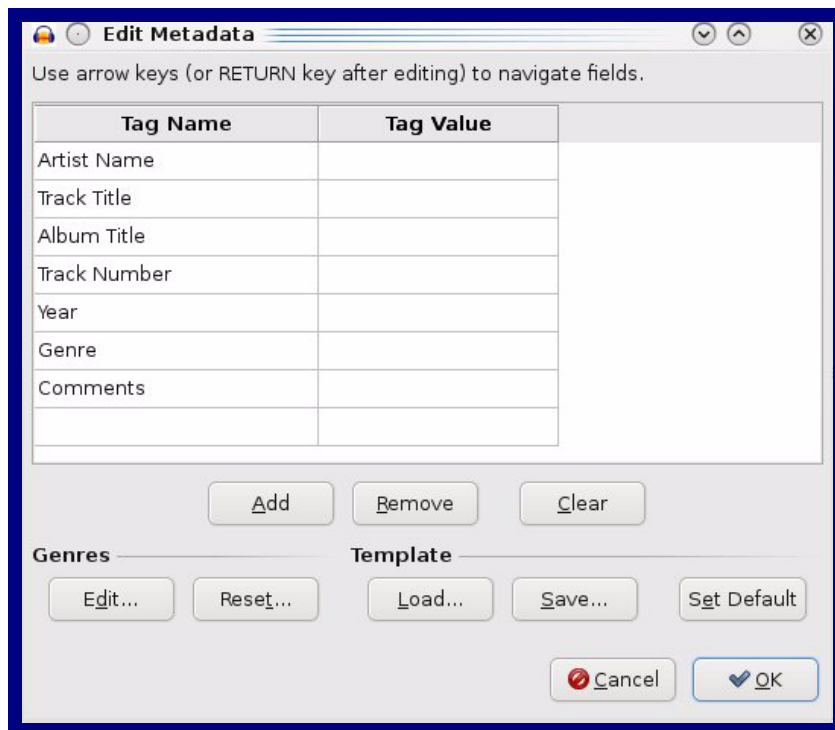
When you export an audio file with Audacity, save the output as:

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

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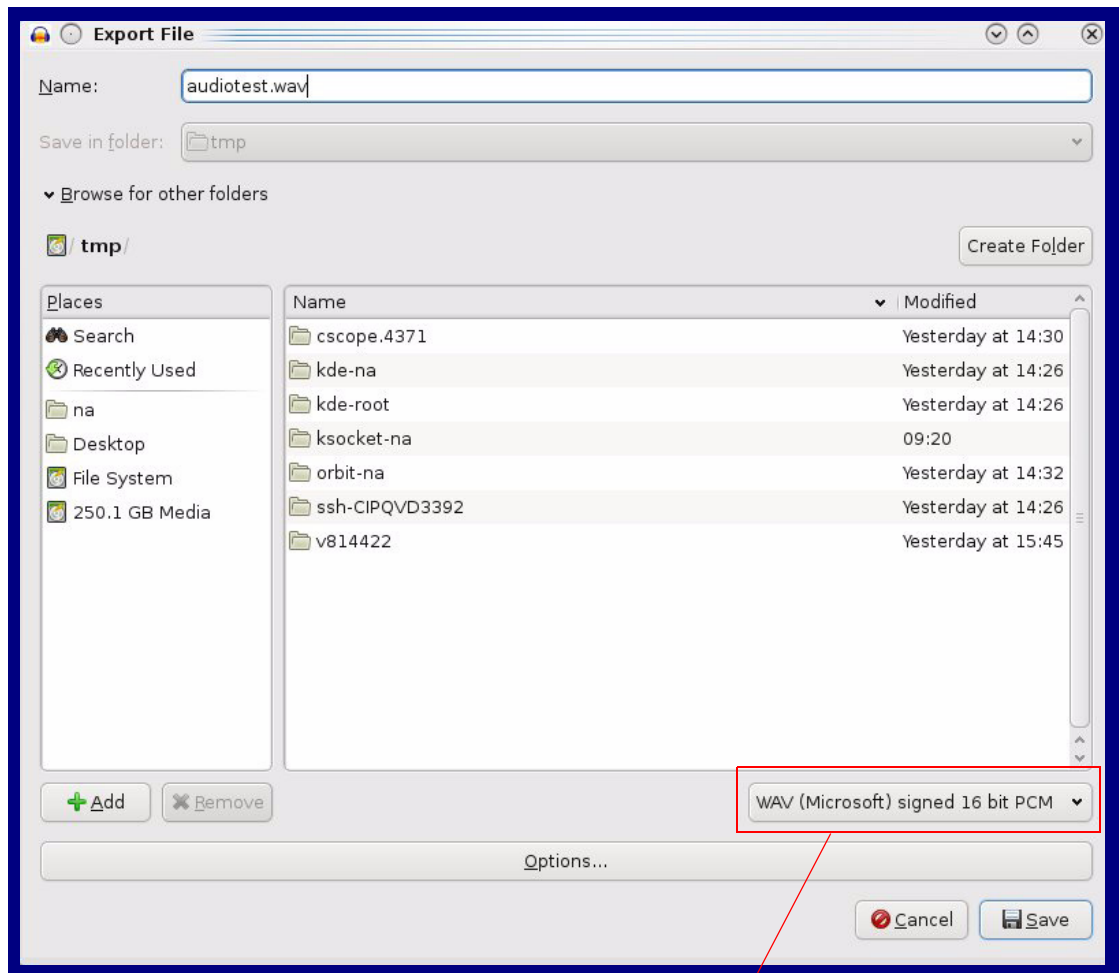
WAV (Microsoft) signed 16 bit PCM

2.3.11 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 2-32).

Figure 2-32. Event Configuration Page

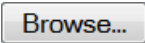2. On the **Events** page, enter values for the parameters indicated in Table 2-19.

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

Web Page Item	Description
Enable Event Generation ?	The device will send HTTP POST events to the specified remote server and port number whenever a certain action takes place. Select an event type below to generate an HTTP POST event.
Events	
Enable Call Start Events ?	When selected, the device will report the start of a SIP call.
Enable Call Terminated Events ?	When selected, the device will report the end of a SIP call.
Enable Relay Activated Events ?	When selected, the device will report relay activation.
Enable Relay Deactivated Events ?	When selected, the device will report relay deactivation.
Enable Ring Events ?	When selected, the device will report when it starts ringing upon an incoming SIP call. A Ring Event will not be generated when **Auto-Answer Incoming Calls** is enabled on the **Device** page.
Enable Night Ring Events ?	When selected, the device will report when it starts ringing upon an incoming SIP call to the Nightringer extension. As a reminder, the Nightringer extension always rings upon an incoming SIP call and it is not possible to alter this behavior.
Enable Multicast Start Events ?	When selected, the device will report when the device starts playing a multicast audio stream.
Enable Multicast Stop Events ?	When selected, the device will report when the device stops playing a multicast audio stream.
Enable Power On Events ?	When selected, the device will report when it boots.
Enable Sensor Events ?	When selected, the device will report when the on-board sensor is activated.
Enable Remote Relay Events ?	When selected, the device will report when the remote relay (DSR) is activated.
Enable Security Events ?	When enabled, the device will report when the intrusion sensor is activated.
Enable 60 Second Heartbeat Events ?	When enabled, the device will report a Heartbeat event every 60 seconds. SIP registration is not required to generate Heartbeat events.
Check All	Click on **Check All** to select all of the events on the page.
Uncheck All	Click on **Uncheck All** to de-select all of the events on the page.
Event Server	
Server IP Address ?	The IPv4 address of the event server in dotted decimal notation.
Server Port ?	Specify the event server port number. The supported range is 0-65536. Enter up to 5 digits.
Server URL ?	Generally, the destination URL is the name of the application that receives the events and the string in the HTTP POST command. It can be a script used to parse and process the HTTP POST events. Enter up to 127 characters.

Table 2-19. Events Configuration Parameters(continued)

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

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

2.3.11.1 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: 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>
POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 205
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData 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_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>
```

2.3.12 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 2-33).

Figure 2-33. DSR Page

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

Web Page Item	Description
Remote Relay Settings	The settings in this section will activate an associated door strike relay.
Activate Relay with DTMF Code ?	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.
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 (* and # are supported).
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 and 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.
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.
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.

Table 2-20. DSR Configuration Parameters (continued)
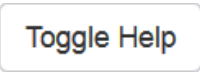
Web Page Item	Description
Dial Out ID [?]	An additional Caller identification string added to outbound calls. Enter up to 64 alphanumeric characters.
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Reboot	Click on the **Reboot** 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.
Discovered Remote Relays	
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.
Discover	Use this button to search for and find any remote relays that are available on the network.
View	Use this button to view the settings of a remote relay that has been "discovered" after pressing the **Discover** button.
Associate	Use this button to associate the remote relay with the device. Only one relay may be associated with a device.

Table 2-20. DSR Configuration Parameters (continued)

Web Page Item	Description
Relay Status	**Note**: The **Relay Status** section and settings (Figure 2-34) only appear on the webpage when there is an associated door strike relay.
Door	Shows the status of the door.
Relay	Shows the status of the remote relay.
Kick Remote Relay	Click on the **Kick Remote Relay** button to activate the remote relay for a specified time. The time is equal to the DTMF timeout.
Activate Remote Relay	Click on the **Activate Remote Relay** button to activate the remote relay until the **Deactivate Remote Relay** button is pressed.
Deactivate Remote Relay	Click on the **Deactivate Remote Relay** button to deactivate the remote relay.
Refresh	Click on the **Refresh** button to refresh the web page and accurately display the status of the remote relay (active/inactive) and door (open/closed).

Figure 2-34. Relay Status Section
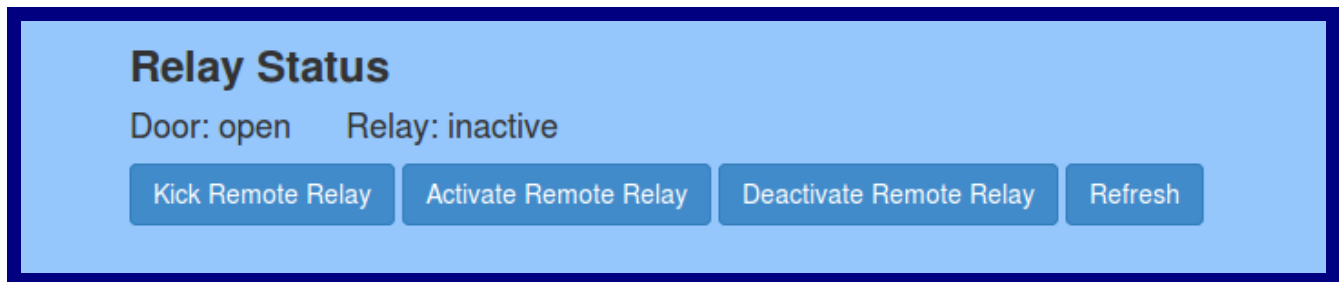
2.3.13 Configure the Device (on the DSR page)

1. Click the **View** button on the **DSR** page to open the **Configure Device** page (Figure 2-35).

Figure 2-35. DSR Page Configure Device Page

Configure Device

Serial Number	270000002
MAC Address	00:20:F7:02:6C:F8
Version	V1.2A
Device Name	LOCK270000003
Addressing Mode	○ Static ◉ DHCP
IP Address:	192.168.70.74
Subnet Mask:	255.255.240.0
Default Gateway:	192.168.64.1
Command Port:	59999
Send Events	◉ Off ○ On
Event IP Address:	192.168.79.255
Event Port:	49999
Energize Time:	
DST	◉ Off ○ On
DST Start:	M3.2.0/02.00.00
DST End:	M11.1.0/02.00.00
Current Time:	17:45:26 08182014
Encryption:	◉ None ○ AES-256
Encryption Key:	
Door State	open
Relay State	inactive
Button State	inactive
LED	red
Alarm State	alarm
JP4, 6, 9, 10	0000

Buttons: Refresh, Get Log, Clear Log, Reboot, Set Time, Save Changes, Cancel

Browse… No file selected. Upgrade

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 2-21. DSR Page Configure Device Parameters

Web Page Item	Description
Serial Number	Displays the serial number of the door strike relay.
MAC Address	Displays the mac address of the door strike relay.
Version	Displays the firmware version of the door strike relay.
Device Name	Displays the name of the door strike relay. The default name is "LOCK," followed by the 9 digit ASCII serial number. The maximum name length is 13 characters. The unit will always respond to its default name.
Addressing Mode	Determines whether an IP address will be manually assigned through Static mode or dynamically assigned through a DHCP server.
IP Address	Displays the IP address of the door strike relay.
Subnet Mask	Displays the subnet mask of the door strike relay.
Default Gateway	Displays the default gateway of the door strike relay.
Command Port	This shows the port on which the door strike relay sends status packets to the device (defaults to 49999).
Send Events	When enabled, events can be sent to the associated device.
Event IP Address	The IP address of the associated device.
Event Port	This is the port by which the door strike relay receives commands (defaults to 59999).
Energize Time	This is the number of seconds that the relay will be energized.
DST	Allows you to either enable or disable the Daylight Savings Time feature.
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.

Table 2-21. DSR Page Configure Device Parameters (continued)

Web Page Item	Description
Current Time	Sets the current time. **Note**: Be sure to save the current time by clicking on the **Set Time** button.
Encryption	Encryption can either be set to **None** or **AES-256**.
Encryption Key	Sets the AES encryption key. If encryption is currently enabled, the response to this command will be sent using the "old" key. The new key should be sent as 64 ASCII hexadecimal characters.
Door State	This field displays the current door state and is not configurable.
Relay State	This field displays the current relay state and is not configurable.
Button State	This field displays the current button state and is not configurable.
LED	This field displays the current LED state and is not configurable.
Alarm State	This field displays the current alarm state and is not configurable.
JP4, 6, 9, 10	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.
Refresh	Click on the **Refresh** button to refresh the **Device Configuration** page.
Get Log	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.
Clear Log	Click on the **Clear Log** button to clear the log from the door strike relay
Reboot	Click on the **Reboot** button to reboot any "discovered" remote relays and clear any associated devices.
Set Time	Click on the **Set Time** button to change the time.
Save Changes	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.
Cancel	Click on the **Cancel** button to cancel any changes that were made to the **Configure Device** page and return to the **DSR** page.
Browse...	Click on the **Browse** button to navigate through your computer and find firmware files.
Upgrade	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.

2.3.14 Configure the Autoprovisioning Parameters

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

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

1. Click the **Autoprov** menu button to open the **Autoprovisioning** page. See Figure 2-36.

Figure 2-36. 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
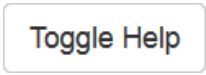
Web Page Item	Description
Disable Autoprovisioning ?	Prevent the device from automatically trying to download a configuration file. See Section 2.3.14.1, "Autoprovisioning" for more information.
Autoprovisioning Server ?	Enter the IPv4 address of the provisioning server in dotted decimal notation.
Autoprovisioning Filename ?	The autoprovisioning filename is the configuration filename. The default autoprovisioning filename is in the format of **<mac address>.xml**.
	Supported filename extensions are .txt, and .xml. The current filename is denoted by an asterisk at the bottom of the **Autoprovisioning Page**. Enter up to 256 characters.
	A file may have any name with an xml extension. If a file name is entered, the device will look for the specified file name, and only that file.
Use tftp	The device will use TFTP (instead of http) to download autoprovisioning files.
Autoprovisioning Autoupdate (in minutes) ?	The reoccurring time (in minutes) the device will wait before checking for new autoprovisioning files. Enter up to 6 digits. A value of 0 will disable this option.
	Note: To use the auto update options, enable the **Set Time with NTP Server on boot** setting on the **Device Configuration Page** page (see Table 2-7).
Autoprovision at time (HHMMSS) ?	The time of day the device will check for a new autoprovisioning file. The time must be 6 characters in length and in HHMMSS format. An empty value will disable this option.
	Note: To use the auto update options, enable the **Set Time with NTP Server on boot** setting on the **Device Configuration Page** page (see Table 2-7).
Autoprovision when idle (in minutes > 10) ?	The idle time (in minutes greater than 10) after which the device will check for a new autoprovisioning file. Enter up to 6 digits. A value of 0 will disable this option.
	Note: To use the auto update options, enable the **Set Time with NTP Server on boot** setting on the **Device Configuration Page** page (see Table 2-7).
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.

Table 2-22. Autoprovisioning Configuration Parameters (continued)

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

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

2.3.14.1 Autoprovisioning

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

1. The file configured on the autoprovisioning page.

2. A file named according to it's mac address (for example: 0020f7350058.xml).

3. The file 000000cd.xml

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

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

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

1. Option 43 - a FQDN or an IP address to an http server

2. Option 72 - an IP address to an http server

3. Option 150 - an IP address to a tftp server

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

You can download an autoprovisioning template file from the Autoprovisioning Page using the **Download Template** button (see Table 2-22). 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 Office Ringer</DeviceName>
<!--    <AutoprovFile>common.xml</AutoprovFile>-->
<!--    <AutoprovFile>sip_reg[macaddress].xml</AutoprovFile>-->
<!--    <AutoprovFile>audio[macaddress]</AutoprovFile>-->
<!--    <AutoprovFile>device[macaddress].xml</AutoprovFile>-->
    </MiscSettings>
```

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

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

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

The file 0020f7123456.xml contains:

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

1. The device will first set it's name to 'Newname'.

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

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

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

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

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

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

Checking for New Autoprovisioning Files after Boot

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

The
Autoprovisioning
Filename

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

Table 2-23. Autoprovisioning File Name

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

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

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

For example:

> The autoprovisioning server is set to "https://www.example.com"

> The autoprovisioning filename is set to "cyberdata/"

On boot, the device will try to download:

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

...and if this fails:

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

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

Autoprovisioning
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 **00:20:f7:02:00:01** and **00:20:f7:02:00:02** (Device1 and Device2).

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

000000cd.xml

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

sip_common.xml

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

sip_0020f7020001.xml

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

sip_0020f7020002.xml

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

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

1. Device1 changes its device name to **CyberData Autoprovisioned**.

2. Device1 finds an AutoprovFile element containing the filename **sip_common.xml**. The device downloads **sip_common.xml** from "https://autoprovtest.server.net," and imports this configuration, setting the sip server to **10.0.0.253** and the remote port to **5060.3**.

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

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

Autoprovisioning Example 2

Here is another example of setting up your autoprovisioning files:

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

0020f7020001.xml

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

0020f7020002.xml

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

common_settings.xml

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

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

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

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

XML Files

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

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

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

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

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

From the common file, a pointer to sip_common.xml

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

Autoprovisioned Audio Files

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

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

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

2.3.14.2 Sample dhcpd.conf

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

ddns-update-style none;

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

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

    option routers                10.0.0.1;
    option subnet-mask            255.0.0.0;

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

    option time-offset            -8;                    # Pacific Standard Time

#    option www-server              99.99.99.99;                    # OPTION 72

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

#    option option-150              10.0.0.252;                     # OPTION 150

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

    range 10.10.0.1 10.10.2.1; }
```

2.3.14.3 Download Template Button

The **Download Template** button allows the user to generate, download, edit, and then store an 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 2-37). 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 2-37.

Figure 2-37. Configuration File
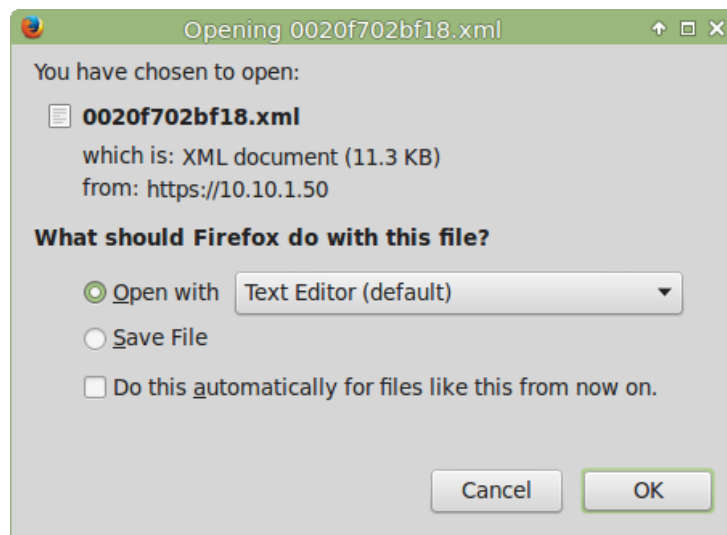
4. At this point, you can open and edit the autoprovisioning template to change the configuration settings in the template for the unit.

5. You can then upload the autoprovisioning file to a TFTP or HTTP server where the file can be loaded onto other devices.

2.4 Upgrade the Firmware and Reboot the Office Ringer

⚠ GENERAL ALERT	**Caution** *Equipment Hazard*: Devices with a serial number that begins with 2161xxxxx can only run firmware versions 10.0.0 or later.

2.4.1 Uploading the Firmware

To upload the firmware from your computer:

1. Retrieve the latest Office Ringer firmware file from the SIP Office Ringer **Downloads** page at:

   http://www.cyberdata.net/products/voip/digitalanalog/officeringerv3/downloads.html

2. Unzip the firmware version file. This file may contain the following:

- Firmware file

- Release notes

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

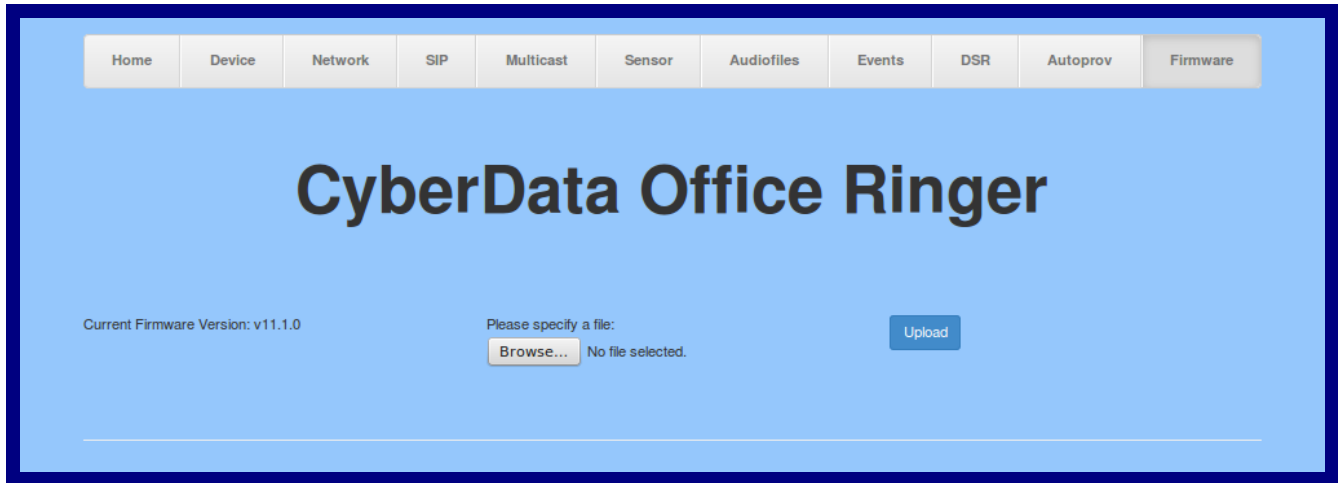4. Click on the **Firmware** menu button to open the **Firmware** page. See Figure 2-38.

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

Figure 2-38. Firmware Page

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

6. Select the firmware file.

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

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

Note   This starts the upgrade process. Once the Office Ringer has uploaded the file, the **Uploading Firmware** countdown page appears, indicating that the firmware is being written to flash. The Office Ringer 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 2-24. Firmware Parameters

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

2.4.2 Reboot the Device

To reboot a Office Ringer, log in to the web page as instructed in Section 2.3.4, "Log in to the Configuration Home Page".

1. Click on the **Reboot** button on the **Home** page (Figure 2-39). A normal restart will occur.

Figure 2-39. Home Page
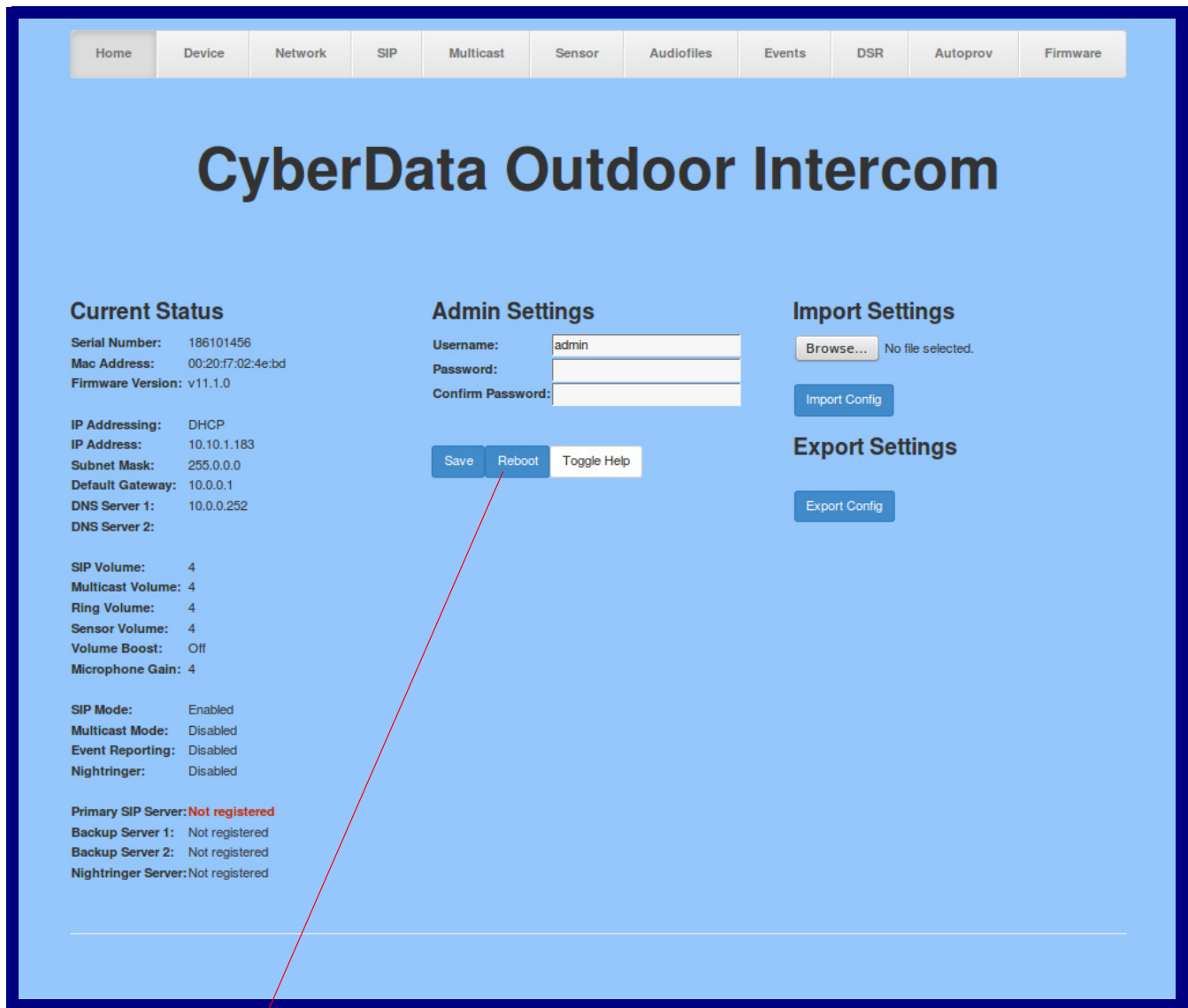
Reboot

2.5 Command Interface

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

2.5.1 Command Interface Post Commands

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

Table 2-25. Command Interface Post Commands

Device Action	HTTP Post Command[a]
Trigger relay (for configured delay)	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/command.cgi" --post-data "test_relay=yes"
Place call to extension (example: extension 130)	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/command.cgi" --post-data "call=130"
Place point-to-point call[b] (example: IP phone address = 10.0.3.72)	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/command.cgi" --post-data "call=10.0.3.72"
Terminate active call	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/command.cgi" --post-data "terminate=yes"
Force reboot	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/command.cgi" --post-data "reboot=yes"
Test Audio button	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/command.cgi" --post-data "test_audio=yes"
Announce IP address	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/command.cgi" --post-data "speak_ip_address=yes"
Play the "0" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_0=yes"
Play the "1" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_1=yes"
Play the "2" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_2=yes"
Play the "3" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_3=yes"

Table 2-25. Command Interface Post Commands (continued)

Device Action	HTTP Post Command[a]
Play the "4" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_4=yes"
Play the "5" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_5=yes"
Play the "6" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_6=yes"
Play the "7" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_7=yes"
Play the "8" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_8=yes"
Play the "9" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_9=yes"
Play the "Dot" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_d=yes"
Play the "Audio Test" audio file (from Audio Config)	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_audiotest=yes"
Play the "Page Tone" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_pagetone=yes"
Play the "Your IP Address Is" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_youripaddressis=yes"
Play the "Rebooting" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_rebooting=yes"
Play the "Restoring Default" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_restoringdefault=yes"
Play the "Ringback tone" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_ringback=yes"
Play the "Ring tone" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_ringtone=yes"
Play the "Intrusion Sensor Triggered" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_intrusionsensortriggered=yes"
Play the "Door Ajar" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_doorajar=yes"

Table 2-25. Command Interface Post Commands (continued)

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

Table 2-25. Command Interface Post Commands (continued)

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

a.Type and enter all of each http POST command on one line.
b. Must be in point-to-point mode see Section 2.3.7.2, "Point-to-Point Configuration"

Appendix A: Mounting the Indoor Office Ringer

A.1 Mount the Office Ringer

Before you mount the Office Ringer, make sure that you have received all the parts for each Office Ringer. Refer to Table A-1.

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

Quantity	Part Name	Illustration
4	#6 x 1" Pan head phillips wood screw	
4	Plastic-ribbed anchor	

Table A-1. Gang Box Mounting Components
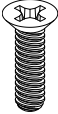
Quantity	Part Name	Illustration
4	6-32 x 0.5-inch flat undercut Phillips machine screw	

Figure A-1 shows how to properly connect the Office Ringer.

Figure A-1. Cable Connections
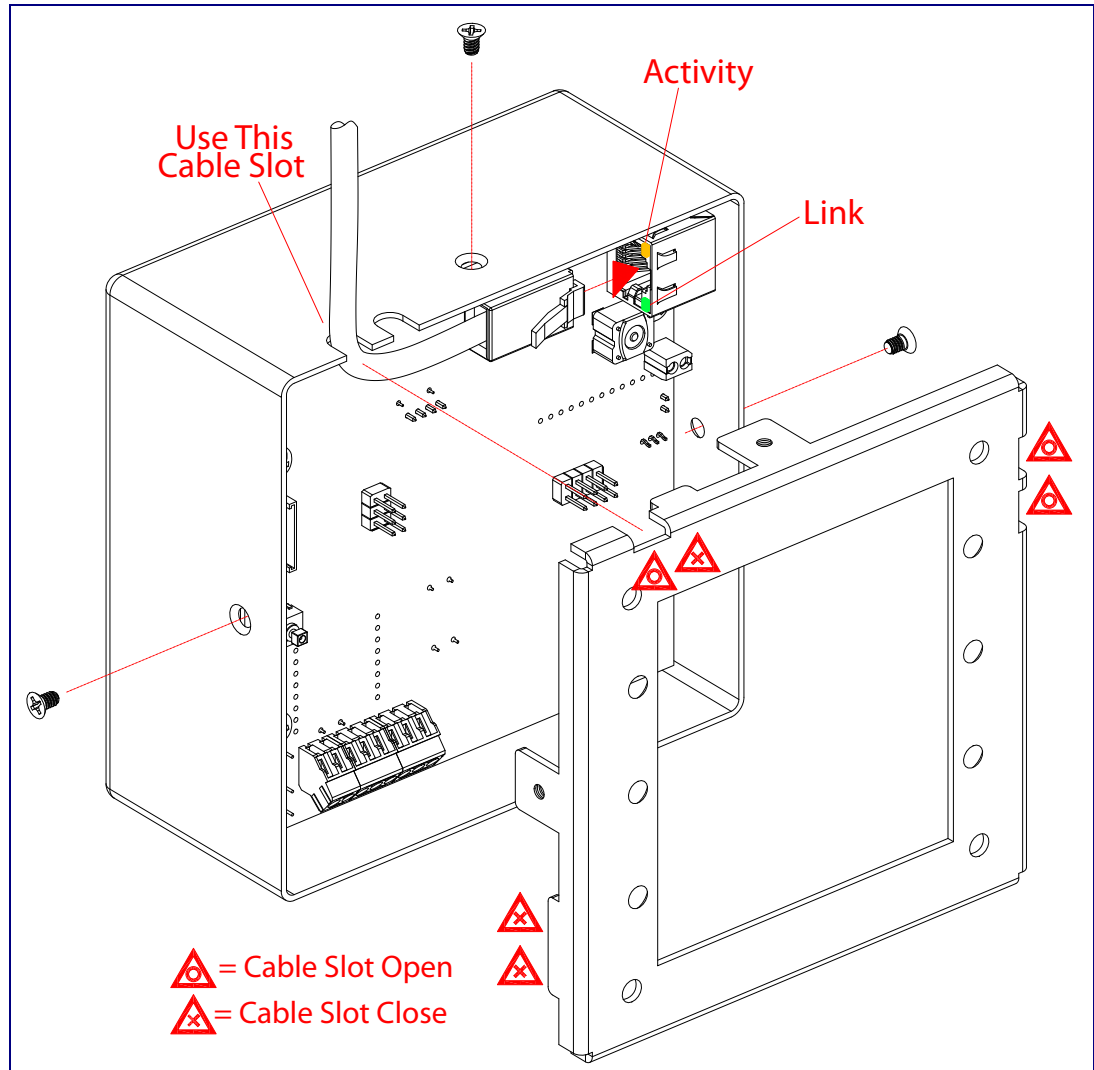
Figure A-2 shows a wall mounting option.

Note   Be sure to connect the SIP Office Ringer to the Earth Ground.

Figure A-2. Wall Mounting Option
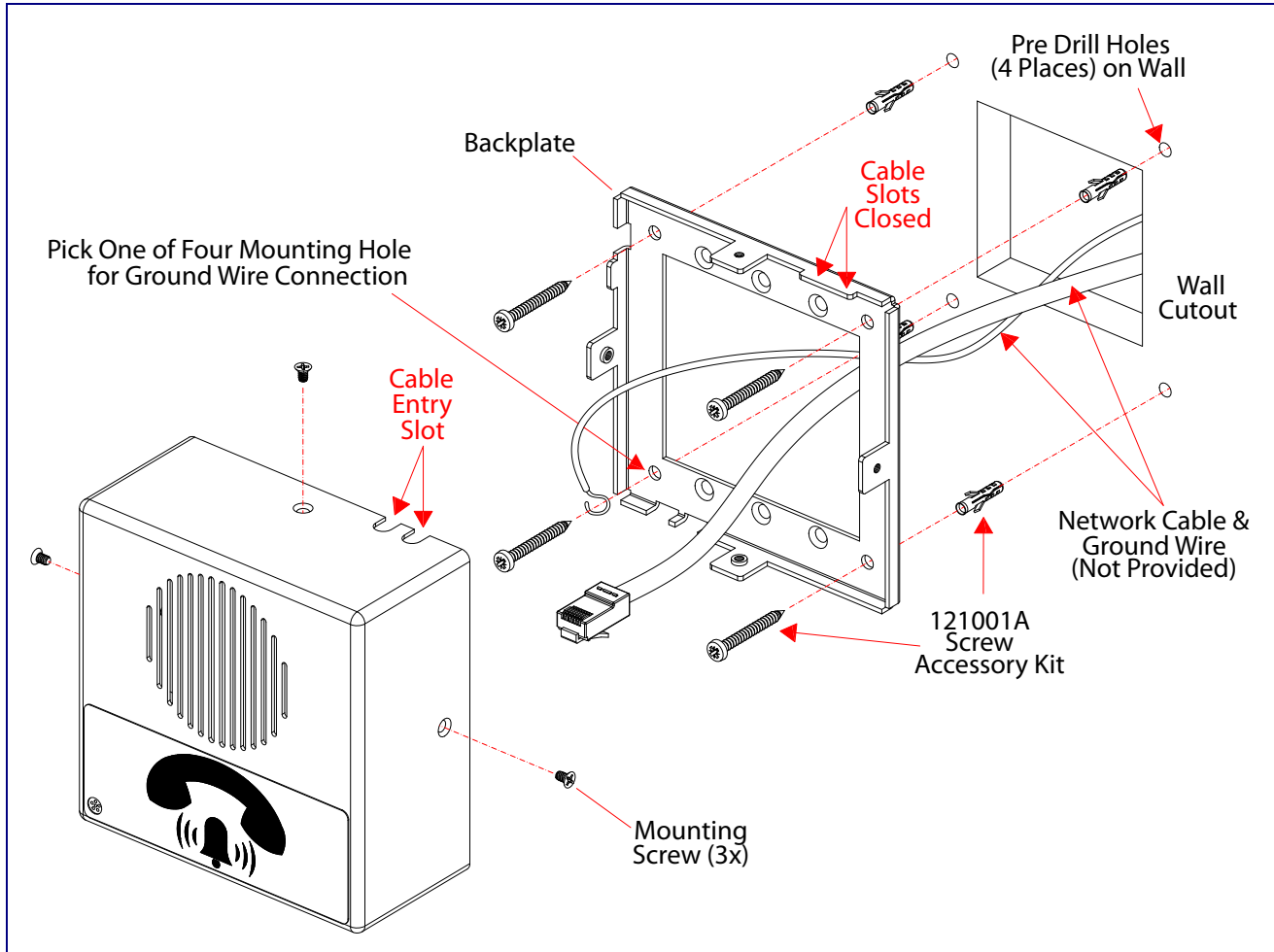
Figure A-3 shows a 1-Gang Box and a 2-Gang Box mounting option.

Note   Be sure to connect the SIP Office Ringer to the Earth Ground.
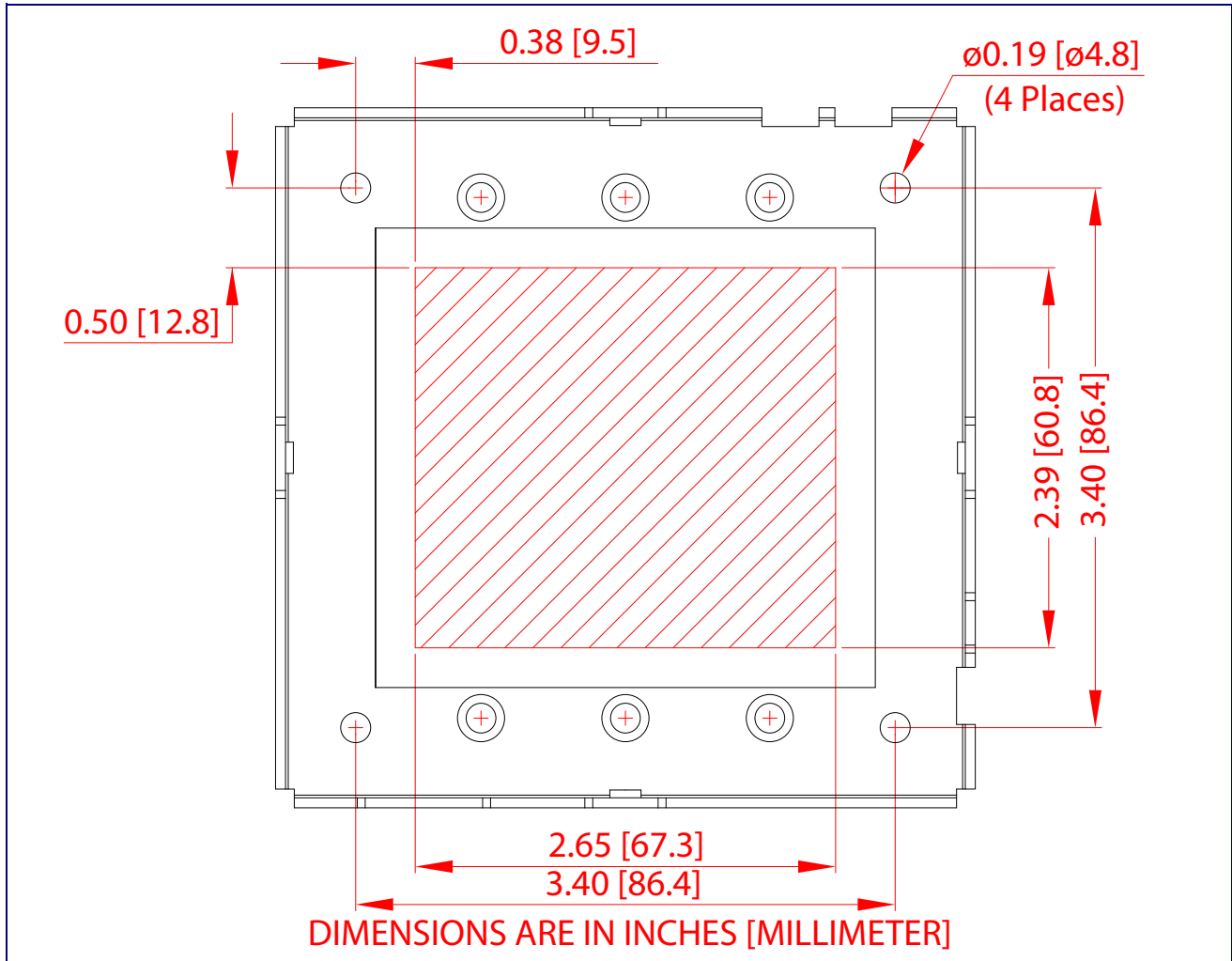
Figure A-3. Gang Box Mounting
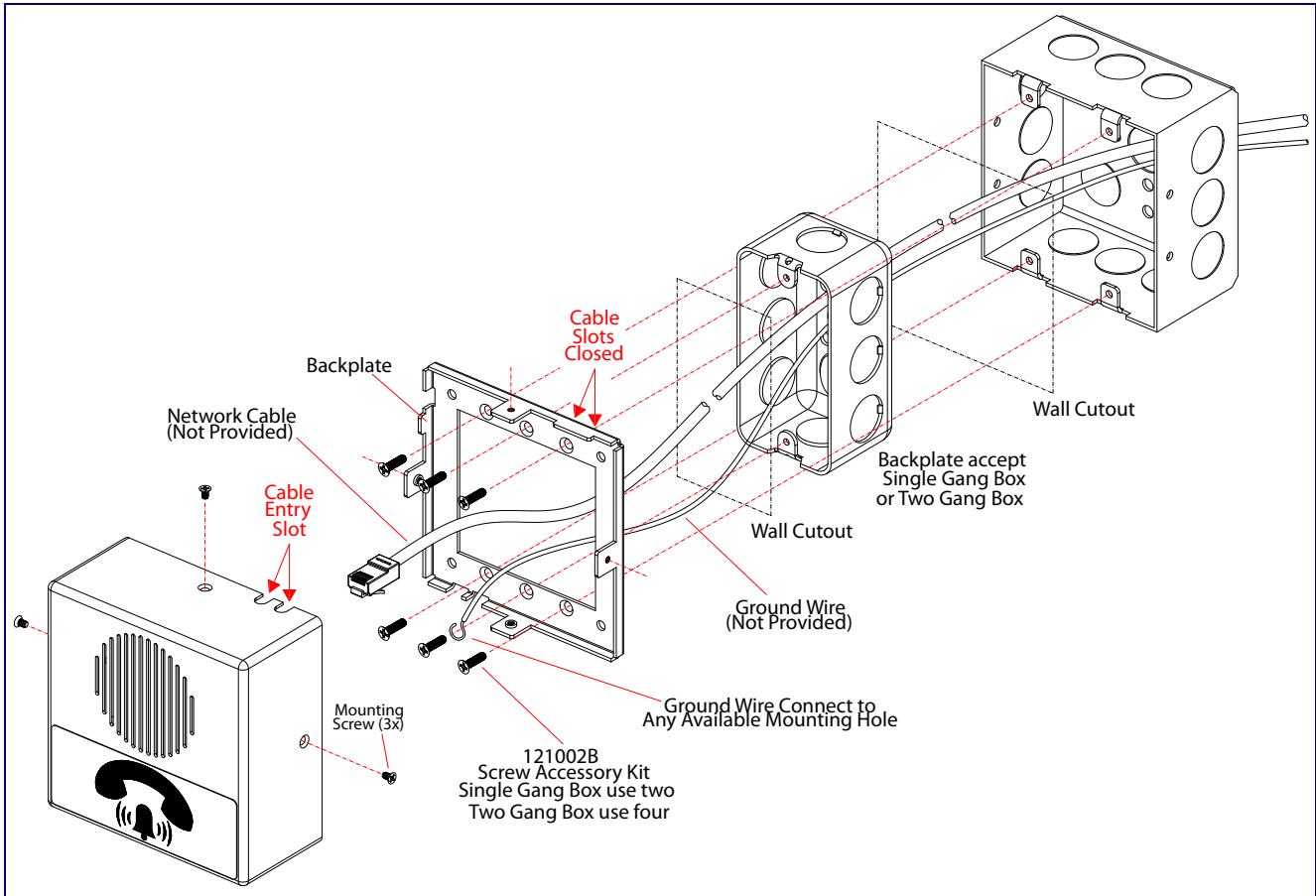
Figure A-4 shows the recommended wall cutout dimensions.

Figure A-4. Recommended Wall Cutout Dimensions

Appendix B: Setting up a TFTP Server

B.1 Set up a TFTP Server

Autoprovisioning requires a TFTP server for hosting the configuration file.

B.1.1 In a LINUX Environment

To set up a TFTP server on LINUX:

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

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

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

B.1.2 In a Windows Environment

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

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

To set up a TFTP server on Windows:

1. Install and start the software.

2. Select **File**/**Configure**/**Security** tab/**Transmit Only**.

3. Make a note of the default directory name, and then move the firmware files to be uploaded to that directory.

Appendix C: Troubleshooting/Technical Support

C.1 Frequently Asked Questions (FAQ)

A list of frequently asked questions (FAQs) are available on the SIP Office Ringer product page at:

http://www.cyberdata.net/products/voip/digitalanalog/officeringerv3/faqs.html

Select the support page for your product to see a list of frequently asked questions for the CyberData product:

C.2 Documentation

The documentation for this product is released in an English language version only.
You can download PDF copies of CyberData product documentation from the
SIP Office Ringer product page at:

http://www.cyberdata.net/products/voip/digitalanalog/officeringerv3/docs.html

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://www.cyberdata.net/support/contactsupportvoip.php

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, Ext. 333
Email: support@cyberdata.net

Returned
Materials
Authorization
To return the product, contact the Returned Materials Authorization (RMA) department:

Phone: 831-373-2601, Extension 136
Email: RMA@CyberData.net

When returning a product to CyberData, an approved CyberData RMA number must be printed on the outside of the original shipping package. Also, RMA numbers require an active VoIP Technical Support ticket number. A product will not be accepted for return without an approved RMA number. Send the product, in its original package, to the following address:

CyberData Corporation
3 Justin Court
Monterey, CA 93940
Attention: RMA "your RMA number"

RMA Status Form
If you need to inquire about the repair status of your product(s), please use the CyberData RMA Status form at the following web address:

http://www.cyberdata.net/support/rmastatus.html

C.4 Warranty

CyberData warrants its product against defects in material or workmanship for a period of two years from the date of purchase. Should the product fail Within Warranty, CyberData will repair or replace the product free of charge. This warranty includes all parts and labor.

Should the product fail Out of the Warranty period, a flat rate repair charge of one half of the purchase price of the product will be assessed. Repairs that are Within Warranty period but are damaged by improper installation, modification, or abuse are deemed Out of Warranty and will be charged at the Out of Warranty rate. A device is deemed Out of Warranty when its purchase date is longer than two years or when the device has been damaged due to human error during installation, modification, or abuse. A replacement unit will be offered at full cost if the device cannot be repaired.

End of Life Devices out of warranty are included under this policy. However, End of Life devices are not eligible for our Spare in the Air program. End of Life devices are devices that are no longer produced or sold. Therefore, we cannot offer a Spare in the Air replacement. Technical support is still available for these devices. However, no firmware revisions or updates will be scheduled. If an End of Life device cannot be repaired, a replacement of a current version of the device may be offered at MSRP.

Products shipped to CyberData, both within and out of warranty, are shipped at the expense of the customer. CyberData will pay return shipping charges for repaired products.

CyberData shall not under any circumstances be liable to any person for any special, incidental, indirect or consequential damages, including without limitation, damages resulting from use or malfunction of the products, loss of profits or revenues or costs of replacement goods, even if CyberData is informed in advance of the possibility of such damages.

C.4.1 Warranty & RMA Returns within the United States

If service is required, you must contact CyberData Technical Support prior to returning any products to CyberData. Our Technical Support staff will determine if your product should be returned to us for further inspection. If Technical Support determines that your product needs to be returned to CyberData, an RMA number will be issued to you at this point.

Your issued RMA number must be printed on the outside of the shipping box. No product will be accepted for return without an approved RMA number. The product in its original package should be sent to the following address:

CyberData Corporation

3 Justin Court.

Monterey, CA 93940

Attn: RMA "xxxxxx"

C.4.2 Warranty & RMA Returns outside of the United States

If you purchased your equipment through an authorized international distributor or reseller, please contact them directly for product repairs.

C.4.3 Spare in the Air Policy

CyberData now offers a *Spare in the Air* no wait policy for warranty returns within the United States and Canada. More information about the *Spare in the Air* policy is available at the following web address:

http://www.cyberdata.net/support/warranty/spareintheair.html

C.4.4 Return and Restocking Policy

For our authorized distributors and resellers, please refer to your CyberData Service Agreement for information on our return guidelines and procedures.

For End Users, please contact the company that you purchased your equipment from for their return policy.

C.4.5 Warranty and RMA Returns Page

The most recent warranty and RMA information is available at the CyberData Warranty and RMA Returns Page at the following web address:

http://www.cyberdata.net/support/warranty/index.html

Index

Numerics

16 AWG gauge wire 7

A

activate local relay (door sensor) 58
activate relay (door sensor) 45
activate relay (intrusion sensor) 45
activity LED 15
address, configuration login 22
alternative power input +12 to 24 VDC at 1000 mA (500
        mA minimum) 5
announcing a device's IP address 16
audio configuration 47
    night ring tone parameter 49
audio configuration page 47
audio encodings 4
audio files, user-created 50
Autoprovision at time (HHMMSS) 65
autoprovision at time (HHMMSS) 65
autoprovision when idle (in minutes > 10) 65
autoprovisioning 66
    download template button 66
    setting up a TFTP server 87
autoprovisioning autoupdate (in minutes) 65
autoprovisioning configuration 64, 65
autoprovisioning filename 65
autoprovisioning server (IP Address) 65
auxiliary relay, 1A at 30 VDC 5

B

backup SIP server 1 36
backup SIP server 2 36
backup SIP servers, SIP server
    backups 36
baud rate
    verifying 15

C

cable connections 83
changing
    the web access password 26
Cisco SRST 36

command interface 78
commands 78
configurable parameters 27, 33, 62
configuration
    audio 47
    default IP settings 18
    door sensor 44
    intrusion sensor 44
    SIP 35
    using Web interface 18
configuration home page 22
configuration page
    configurable parameters 27, 33, 62
contact information 89
contact information for CyberData 89
Current Network Settings 33
current network settings 33
CyberData contact information 89

D

default
    device settings 92
    gateway 18
    IP address 18
    subnet mask 18
    username and password 18
    web login username and password 22
default gateway 18, 33
default IP settings 18
default login address 22
default settings 17
device configuration 26
    default IP settings 18
    device configuration parameters 65
    the device configuration page 64
device configuration page 26
device configuration parameters 27
device configuration password
    changing for web configuration access 26
device setup 7
DHCP Client 4
dial out extension (door sensor) 45, 58
dial out extension (intrusion sensor) 45
dial out extension strings 39
dial-out extension strings 41
dimensions 5
discovery utility program 22
DNS server 33
door sensor 44, 45, 58

terminal block, 16 AWG gauge wire 7
TFTP server 4, 87
time zone string examples 30

U

user ID
    for SIP server login 36
username
    changing for web configuration access 26
    default for web configuration access 22
    restoring the default 18

V

verifying
    baud rate 15
    network connectivity 15
VLAN ID 33
VLAN Priority 33
VLAN tagging support 33
VLAN tags 33
volume
    multicast volume 27
    ring volume 27
    sensor volume 27
    SIP volume 27

W

wall mounting option 84
warranty 90
warranty & RMA returns outside of the United States 91
warranty and RMA returns page 91
warranty policy at CyberData 90
web access password 18
web access username 18
web configuration log in address 22
web page
    navigation 19
web page navigation 19
web-based configuration 18
weight 5
wget, free unix utility 78
Windows, setting up a TFTP server on 87
wiring the circuit 9
    devices less than 1A at 30 VDC 9