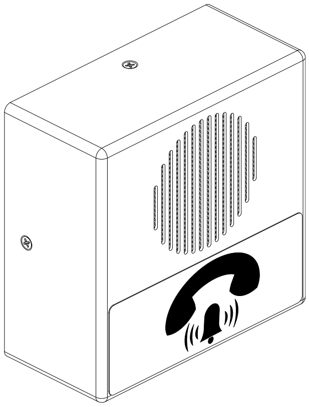
CyberData
The IP Endpoint Company



V3 SIP Office Ringer
Operations Guide

Part #011216, RAL 9003, Signal White Color

Document Part #930514G
for Firmware Version *7.1.7*

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

SIP Office Ringer Operations Guide 930514G
Part # 011216

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

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

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

CyberData
The IP Endpoint Company

Technical Support

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

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

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. Prior to installation, consult local building and electrical code requirements.
14. **WARNING: The SIP Office Ringer 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 930514G, which corresponds to firmware version 7.1.7., was released on October 30, 2015, and has the following changes:

- Updates the following specifications in Table 1-1, "Specifications":
  - Power Input: PoE 802.3af compliant or +8 to +12VDC @ 1000mA Regulated Power Supply
  - Speaker Output: 1 Watt Peak Power
  - On-Board Relay: 1A at 30 VDC
  - Dimensions: 5.118 inches [130 mm] Length, 2.252 inches [57.21 mm] Width, 5.118 inches [130 mm] Height
  - Weight: 1.0 lbs. (0.45 kg)
  - Boxed Weight: 2.0 lbs. (0.90 kg)
- Updates Figure 2-1, "Office Ringer Connections"
- Updates Section C.4, "Warranty and RMA Information"

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

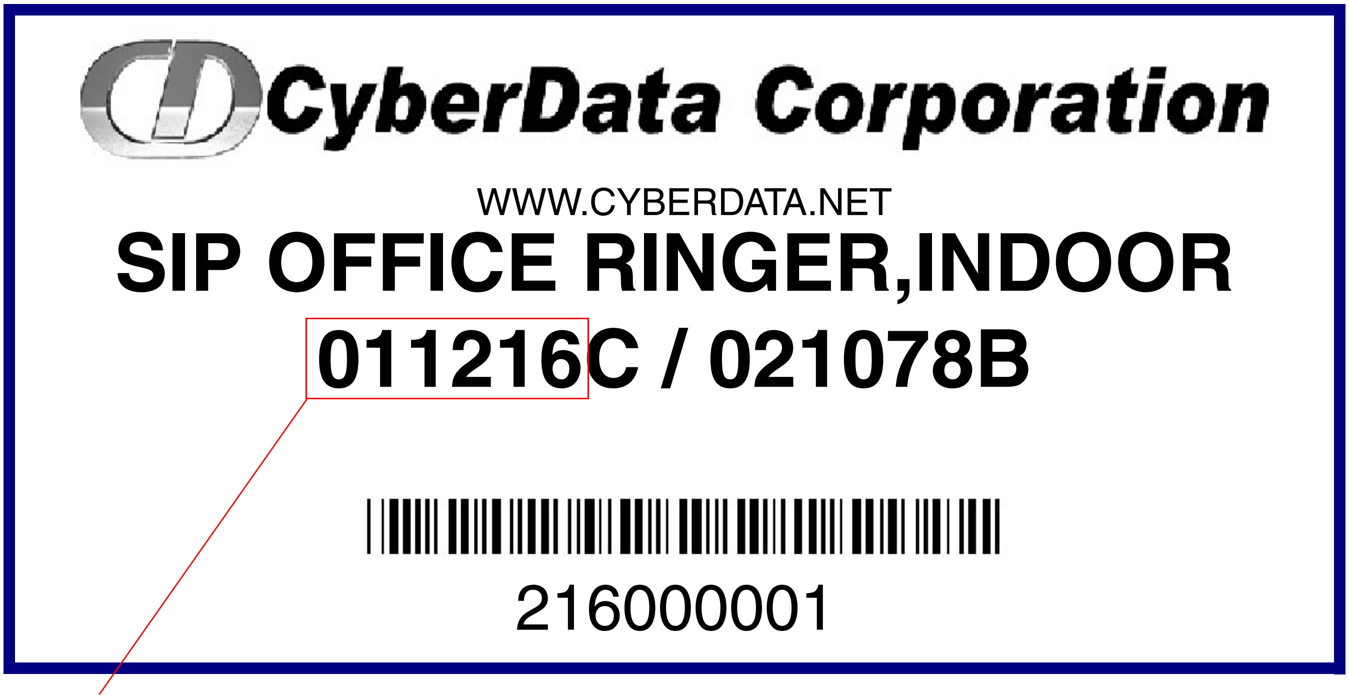
Contents

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. The model number on the label should be **011216.**

Figure 1-1. Model Number Label



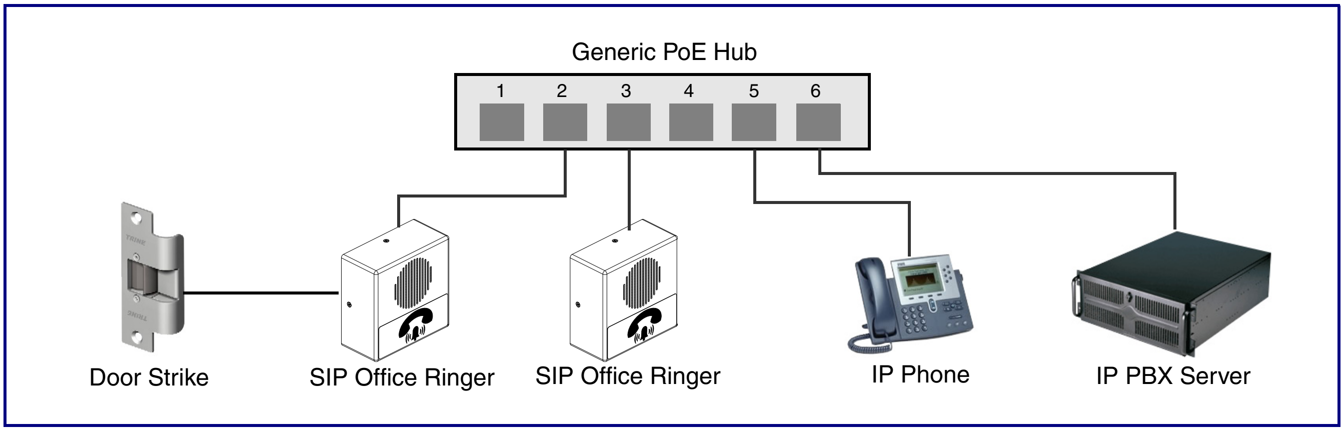
Model number

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.

Figure 1-2 illustrates how the SIP Office Ringer can be installed as part of a VoIP phone system.

Figure 1-2. Typical Installation—Door Entry/Access Control



⚠ GENERAL ALERT	Warning *Electrical Hazard:* The SIP Office Ringer 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.

1.3 Product Features

- Cisco SRST (Survivable Remote Site Telephony)
- SIP
- Dual speeds of 10 Mbps and 100 Mbps
- 802.3af compliant
- 2 gang outlet box size
- 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 Office Ringer for the supported SIP servers:

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

1.6 Specifications

Table 1-1. Specifications

Specifications	
Ethernet I/F	10/100 Mbps
Protocol	SIP RFC 3261 Compatible
Power Input	PoE 802.3af compliant or +8 to +12VDC @ 1000mA Regulated Power Supply[a]
Speaker Output	1 Watt Peak Power
On-Board Relay	1A at 30 VDC
Operating Temperature	-10° C to 50° C (14° F to 122° F)
Payload Types	G711, A-law and µ-law
Dimensions	4.53 inches [115 mm] Length 2.22 inches [56.3 mm] Width 4.53 inches [115 mm] Height
Weight Boxed Weight	1.0 lbs. (0.45 kg) 2.0 lbs. (0.90 kg)
Part Number	011216[b], RAL 9003, Signal White

[a] 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.

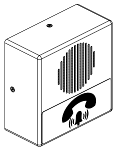
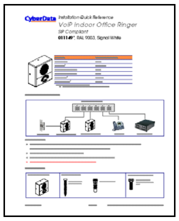
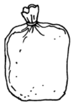
[b] This number replaces the 011149 number.

2 Installing the SIP Office Ringer

2.1 Parts List

Table 2-2 illustrates the V3 SIP Office Ringer parts.

Table 2-2. Parts List

Quantity	Part Name	Illustration
1	Office Ringer Assembly	
1	Installation Quick Reference Guide	 CyberData Installation Quick Reference VoIP Indoor Office Ringer SIP Compliant **011149***, RAL 9003, Signal White
1	Office Ringer Mounting Accessory Kit	

2.2 Office Ringer Setup

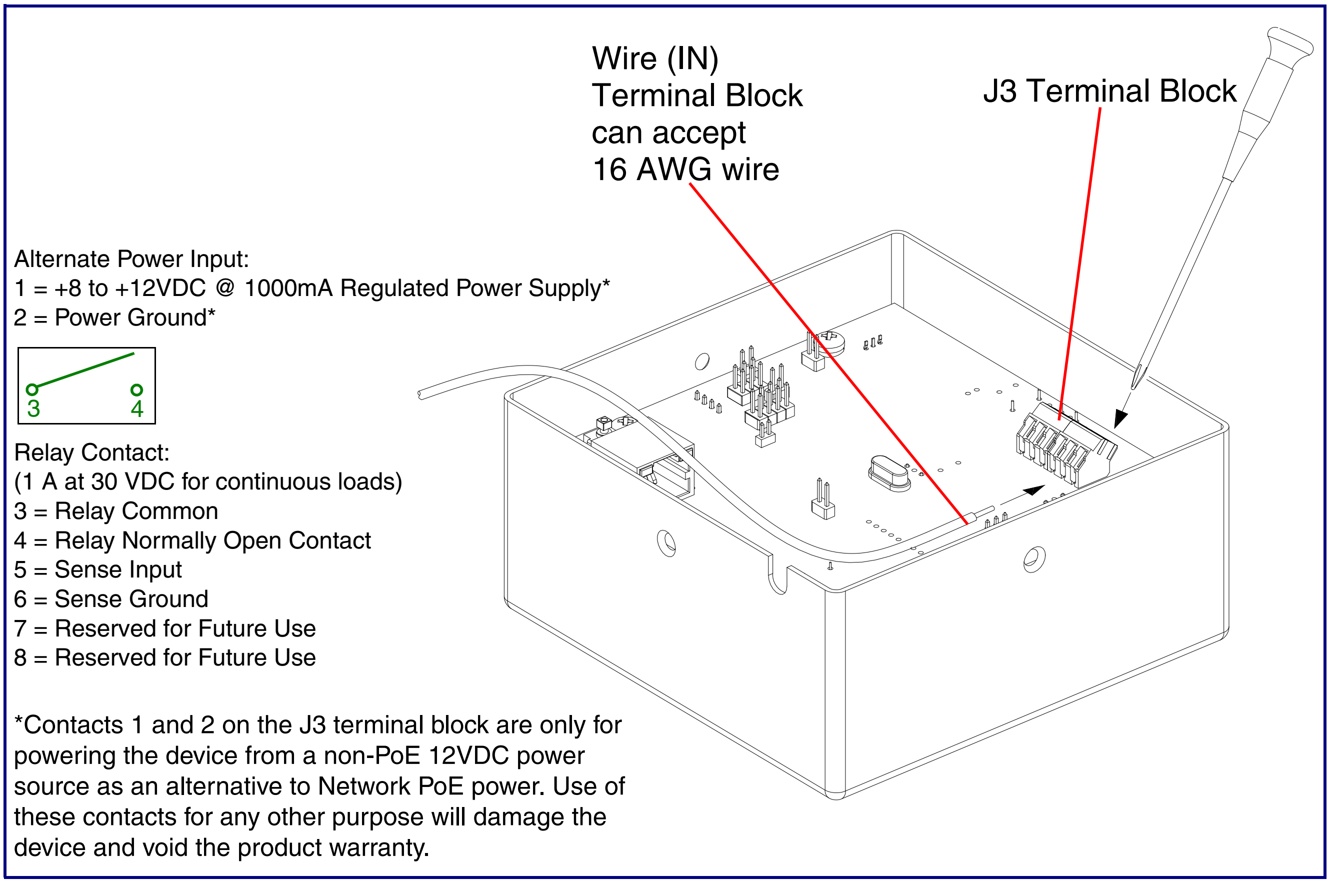
2.2.1 Office Ringer Connections

Figure 2-1 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 +12VDC @ 1000mA Regulated Power Supply 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 2-1. Office Ringer Connections



Alternate Power Input:
1 = +8 to +12VDC @ 1000mA Regulated Power Supply*
2 = Power Ground*

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.

2.2.2 Connecting the Office Ringer to the On-Board Relay

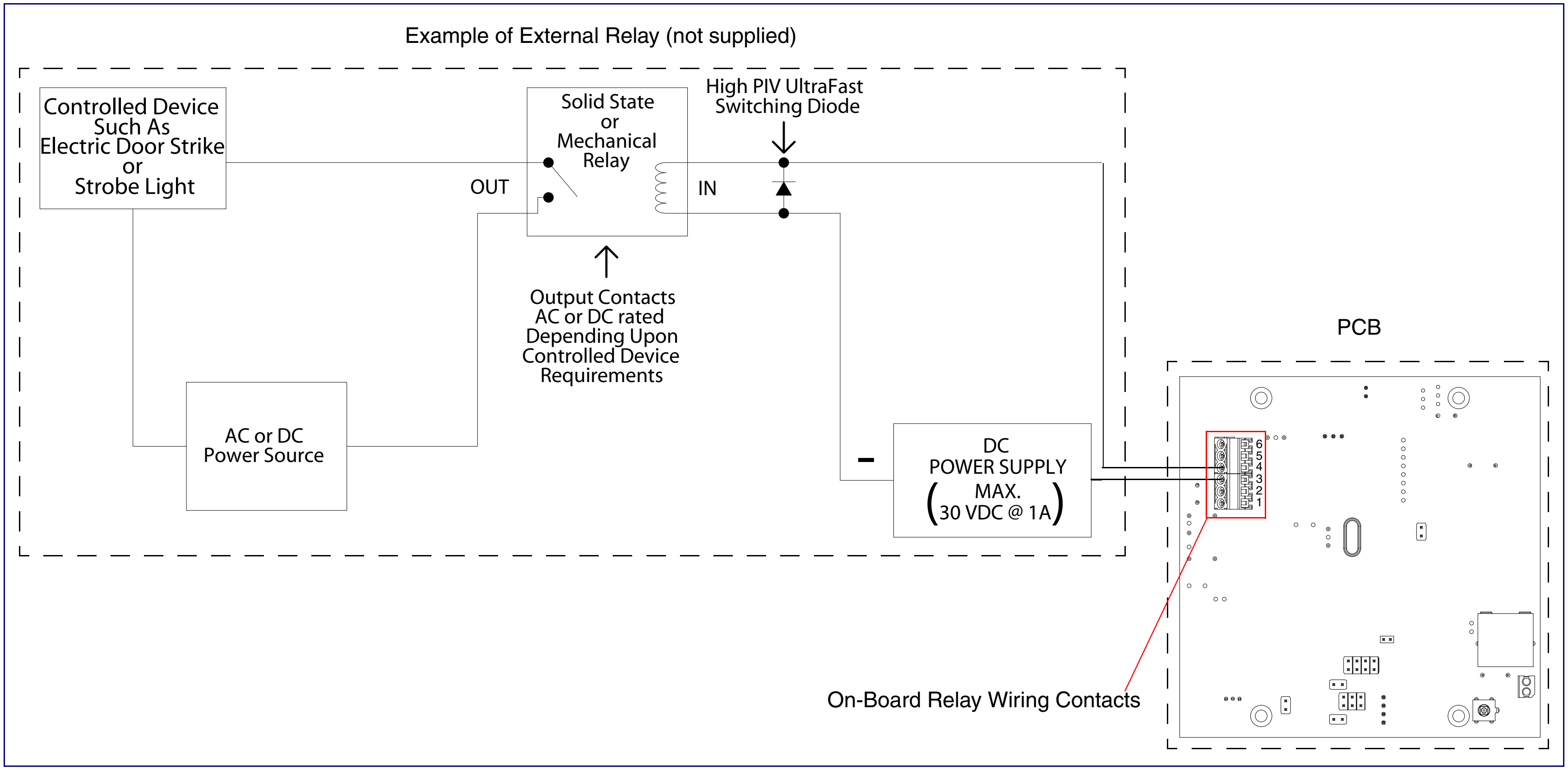
⚠ GENERAL ALERT	**Warning** *Electrical Hazard:* The SIP Office Ringer enclosure is not rated for any AC voltages.
⚠ GENERAL ALERT	**Warning** *Electrical Hazard:* This product should be installed by a licensed electrician according to all local electrical and building codes.
⚠ GENERAL ALERT	**Warning**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

The device incorporates an on-board relay which enables users to control an external relay for activating an auxiliary device such as an electric door strike (see Figure 2-2, "Wiring Diagram").

The relay contacts are limited to 1A at 30 VDC. The relay activation time is selectable through the web interface and is controlled by DTMF tones generated from the phone being called. The DTMF tones are selectable from the web interface as well.

Note The three digit code for the on-board relay must be sent in conformance with RFC2833 DTMF generation.

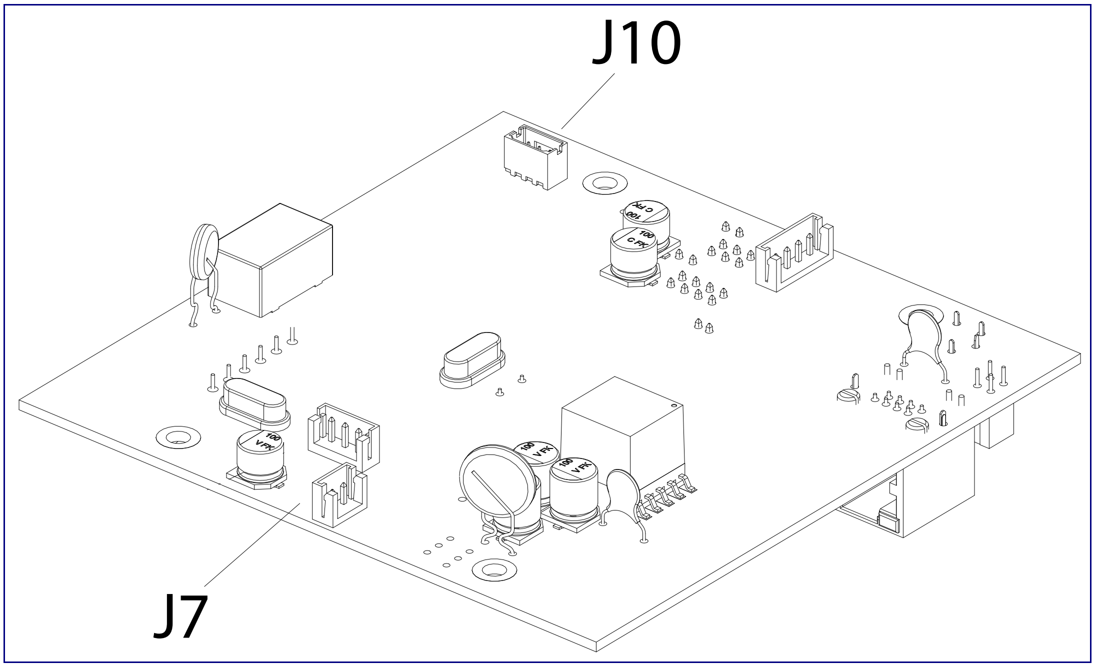
Figure 2-2. Wiring Diagram


Example of External Relay (not supplied)
Controlled Device Such As Electric Door Strike or Strobe Light
Solid State or Mechanical Relay
High PIV UltraFast Switching Diode
OUT
IN
Output Contacts AC or DC rated Depending Upon Controlled Device Requirements
AC or DC Power Source
–
DC POWER SUPPLY (MAX. 30 VDC @ 1A)
PCB
6
5
4
3
2
1
On-Board Relay Wiring Contacts

2.2.3 Identifying the Office Ringer Connectors

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

Figure 2-3. J2, J5, and J6 Connector Locations



.

Table 2-3. Connector Functions

Connector	Function
J7	Speaker Interface
J10	Proximity Sensor Interface - N/A

Figure 2-4. Connector Locations

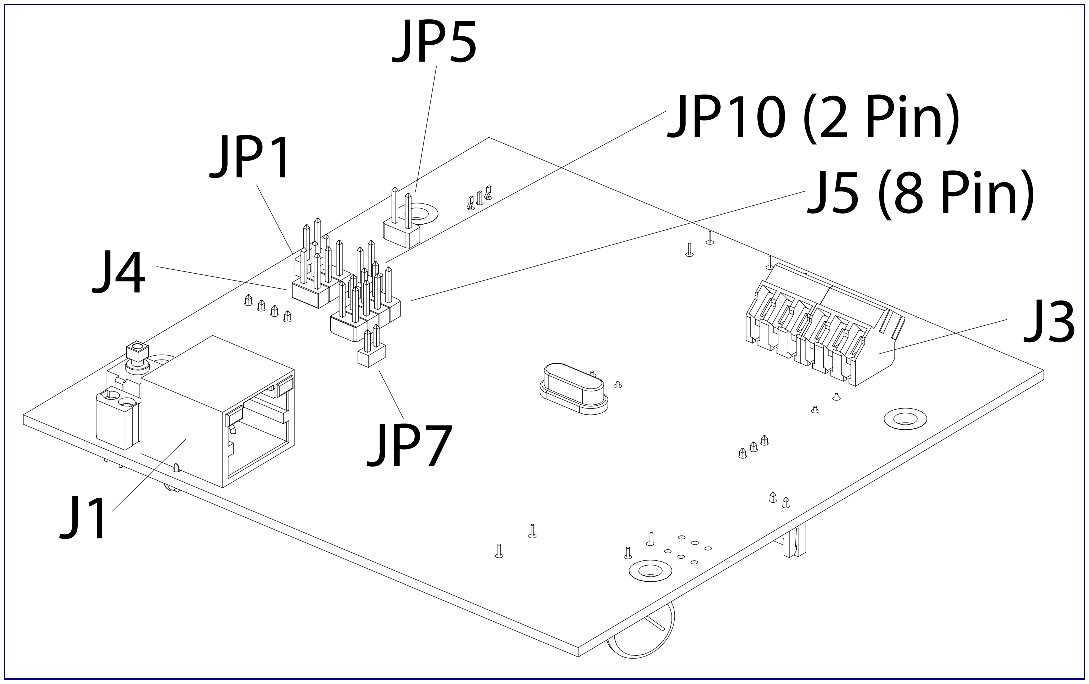


Table 2-4. Connector Functions

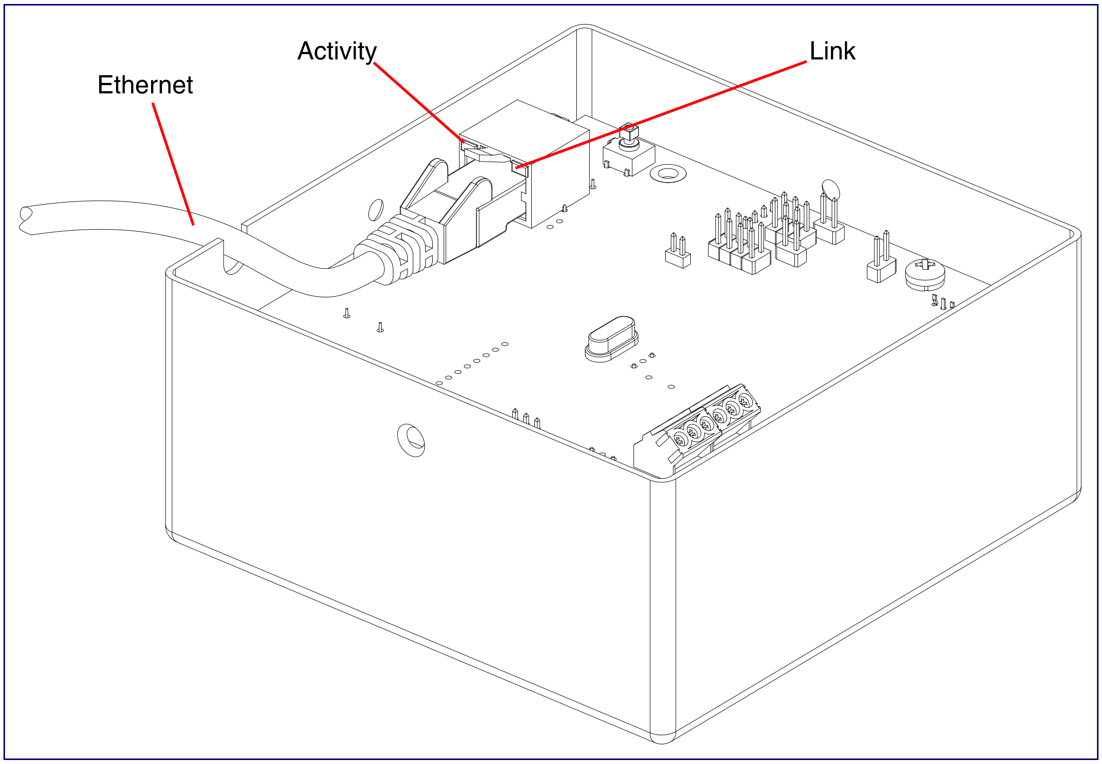
Connector	Function
J1	PoE Network Connection (RJ-45 ethernet)
J3	Terminal Block (see Figure 2-1)
J4	Factory Only—Console Port
J5	Factory Only—JTAG
JP1	Factory Only—Reset
JP5	Factory Only—Watch Dog
JP7	Factory Only—Boot Mode
JP10	Disables the intrusion sensor when installed.

2.2.4 Link and Activity LEDs

When you connect the Ethernet cable or power supply to the Office Ringer, the following occurs:

- The square, **GREEN Link** LED above the Ethernet port (Figure 2-5) indicates that the network connection has been established.
- The square, **YELLOW Activity** LED (see Figure 2-5) blinks when there is network activity.

Figure 2-5. Link and Activity LEDs

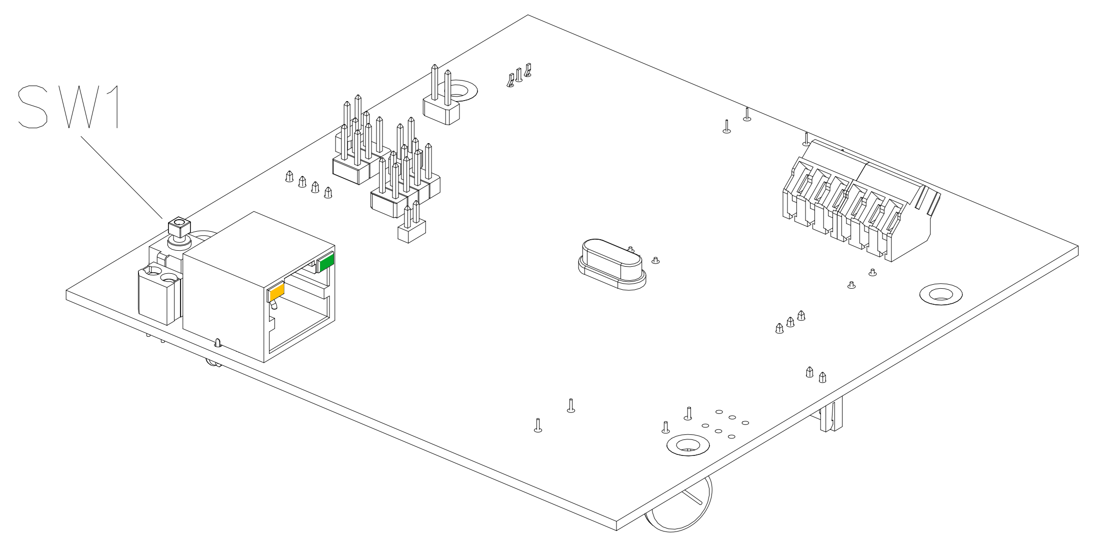


2.2.5 RTFM Button

When the Office Ringer is operational and linked to the network, use the Reset Test Function Management **(RTFM)** button (SW1) (Figure 2-6) on the Office Ringer board to announce and confirm the Office Ringer’s IP Address and test that the audio is working.

Note You must do these tests prior to final assembly.

Figure 2-6. RTFM Button



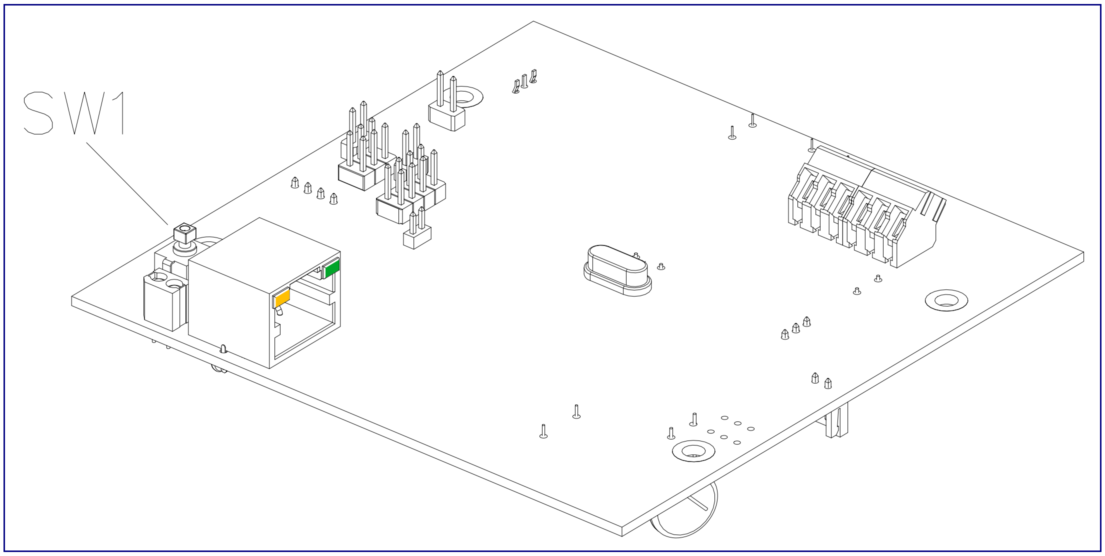
2.2.6 Announcing the IP Address

To announce an Office Ringer's current IP address, press and hold the RTFM button (SW1) (Figure 2-7) for one to two seconds.

Note The Office Ringer 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 Office Ringer to the factory default settings.

Figure 2-7. RTFM Button



2.2.7 Restore the Factory Default Settings

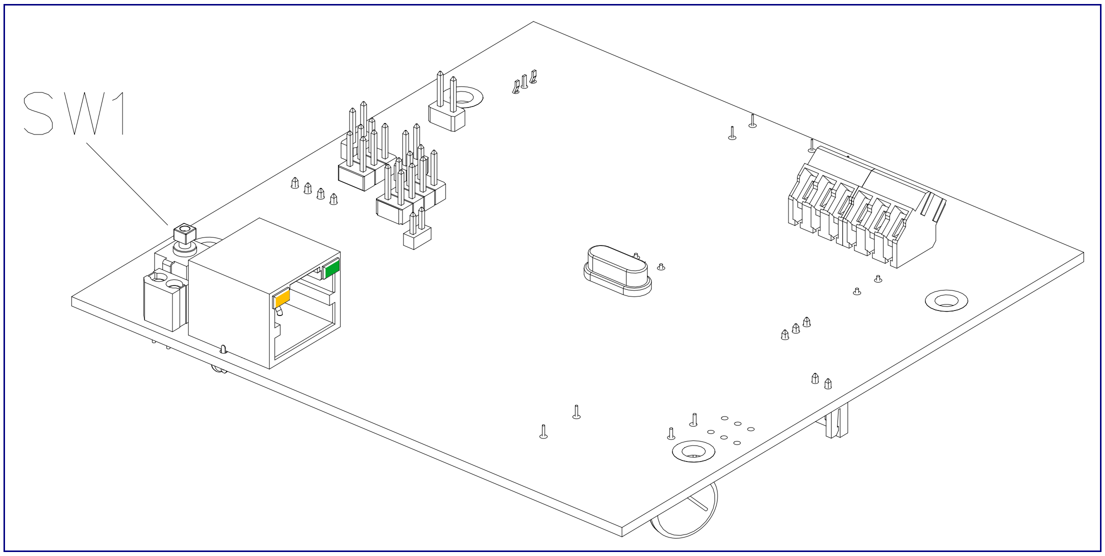
2.2.7.1 RTFM Button

When the Office Ringer is operational and linked to the network, use the Reset Test Function Management (RTFM) button (SW1) (Figure 2-8) to set the factory default settings.

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

Note The Office Ringer 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 2-8. RTFM Button



To set the factory default settings:

1. Press and hold the **RTFM** button (SW1) for more than five seconds.
2. The Office Ringer announces that it is restoring the factory default settings.

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

2.2.8 Adjust the Volume

You can adjust the volume through the Speaker 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 2-5. 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 2-6 shows the navigation buttons that you will see on every Office Ringer web page.

Table 2-6. Web Page Navigation

Web Page Item	Description
	Link to the **Home** page.
	Link to the **Device Configuration** page.
	Link to the **Networking** page.
	Link to go to the **SIP Configuration** page.
	Link to go to the **Officeringer** page.
	Link to the **Sensor Configuration** page.
	Link to the **Multicast Configuration** page.
	Link to the **Audio Configuration** page.
	Link to the **Event Configuration** page.
	Link to the **Autoprovisioning Configuration** page.
	Link to the **Update Firmware** page.

2.3.3 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 2-9):

   Web Access Username: **admin**

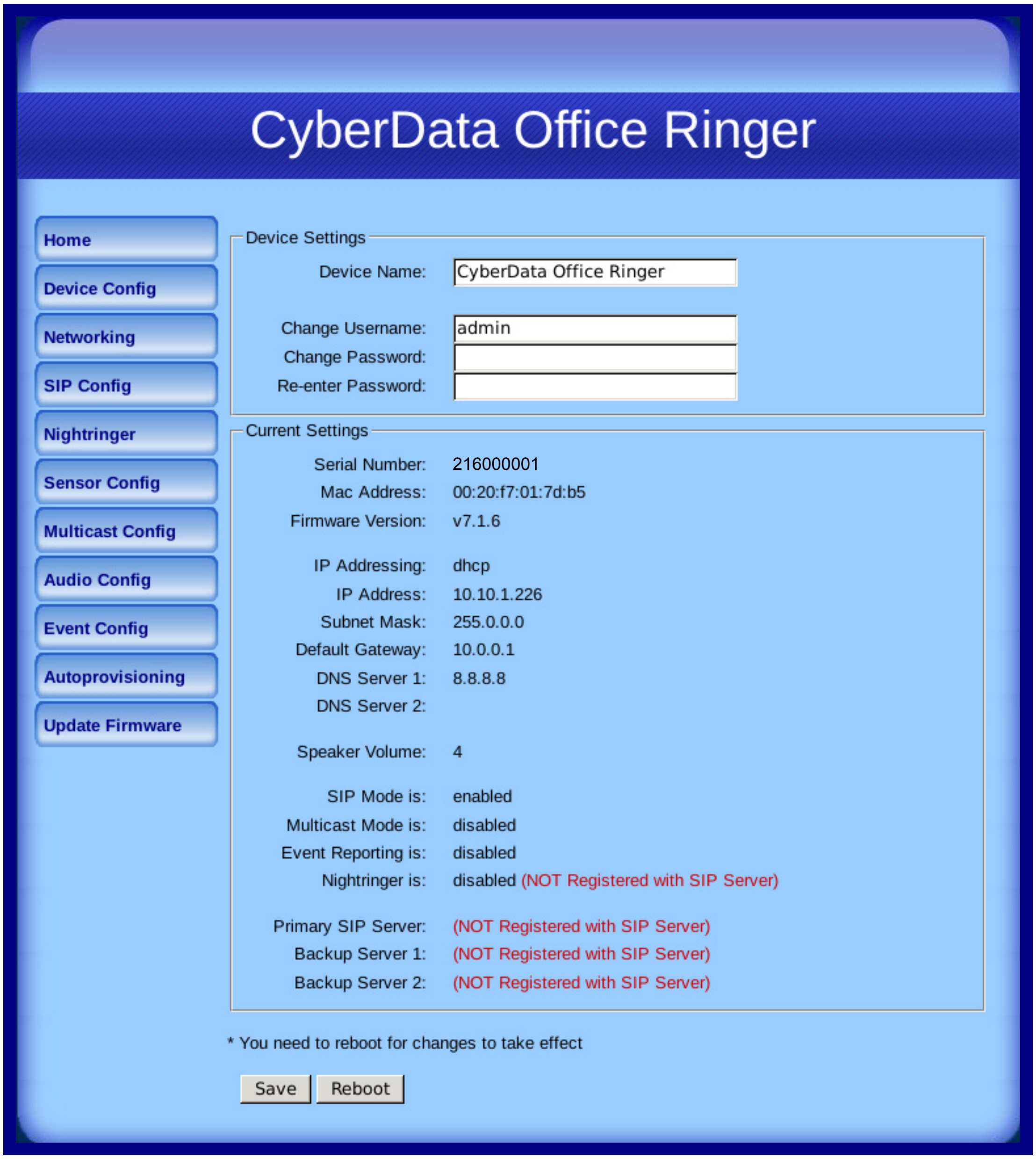
   Web Access Password: **admin**

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

   Web Access Username: **admin**

   Web Access Password: **admin**

Figure 2-9. Home Page



CyberData Office Ringer

Device Settings

Device Name: CyberData Office Ringer

Change Username: admin
Change Password:
Re-enter Password:

Current Settings

Serial Number: 216000001
Mac Address: 00:20:f7:01:7d:b5
Firmware Version: v7.1.6

IP Addressing: dhcp
IP Address: 10.10.1.226
Subnet Mask: 255.0.0.0
Default Gateway: 10.0.0.1
DNS Server 1: 8.8.8.8
DNS Server 2:

Speaker Volume: 4

SIP Mode is: enabled
Multicast Mode is: disabled
Event Reporting is: disabled
Nightringer is: disabled (NOT Registered with SIP Server)

Primary SIP Server: (NOT Registered with SIP Server)
Backup Server 1: (NOT Registered with SIP Server)
Backup Server 2: (NOT Registered with SIP Server)

* You need to reboot for changes to take effect

4. On the **Home Page**, review the setup details and navigation buttons described in Table 2-7.

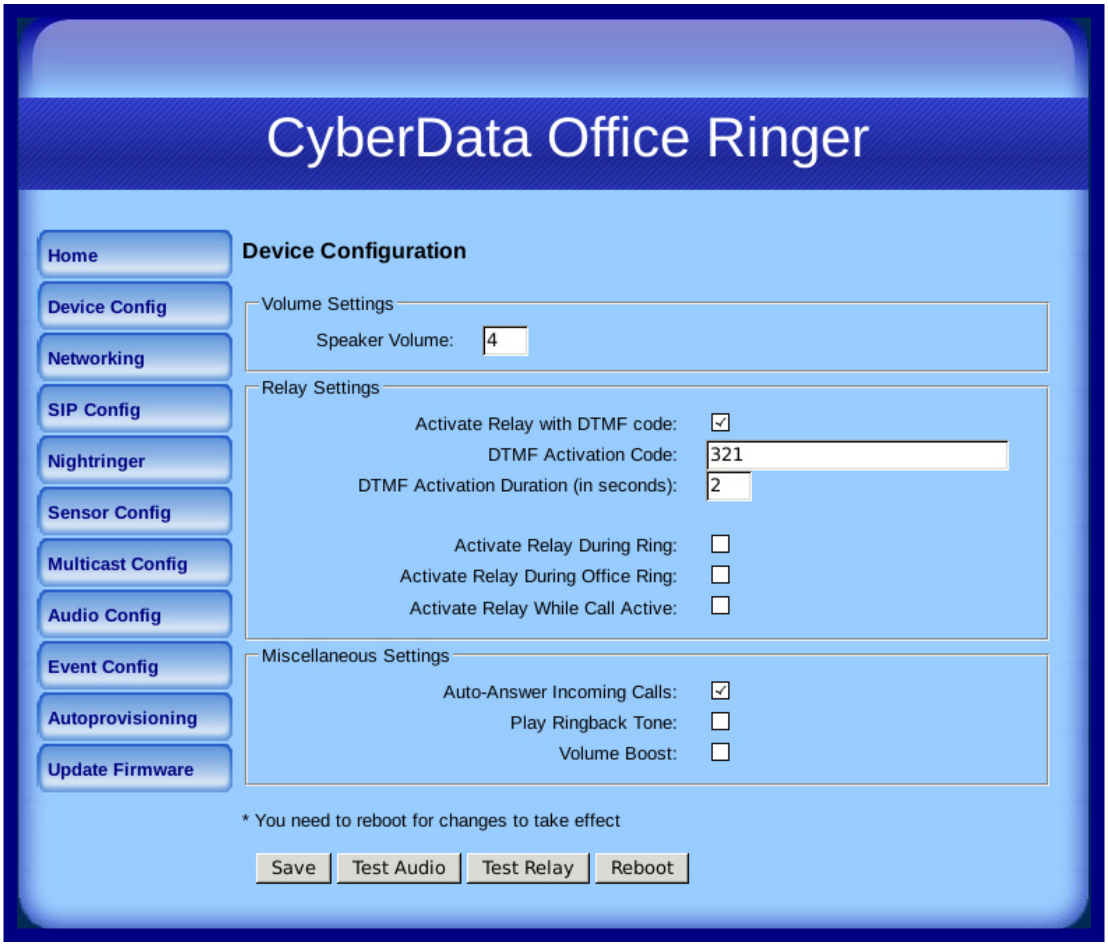
Table 2-7. Home Page Overview

Web Page Item	Description
Device Settings	
Device Name	Shows the device name.
Change Username	Type in this field to change the username.
Change Password	Type in this field to change the password.
Re-enter Password	Type the password again in this field to confirm the new password.
Current Settings	
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.
Speaker Volume	Shows the current speaker volume level.
SIP Mode is	Shows the current status of the SIP mode.
Multicast Mode is	Shows the current status of the Multicast mode.
Event Reporting is	Shows the current status of the Event Reporting mode.
Nightringer is	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.
	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
	Click on the **Reboot** button to reboot the system.

2.3.4 Configure the Device

1. Click the **Device Configuration** button to open the **Device Configuration** page. See Figure 2-10.

Figure 2-10. Device Configuration Page



Device Configuration

Volume Settings

Speaker Volume: 4

Relay Settings

Activate Relay with DTMF code: ☑

DTMF Activation Code: 321

DTMF Activation Duration (in seconds): 2

Activate Relay During Ring: □

Activate Relay During Office Ring: □

Activate Relay While Call Active: □

Miscellaneous Settings

Auto-Answer Incoming Calls: ☑

Play Ringback Tone: □

Volume Boost: □

* You need to reboot for changes to take effect

2. On the **Device Configuration** page, you may enter values for the parameters indicated in Table 2-8.

Table 2-8. Device Configuration Parameters

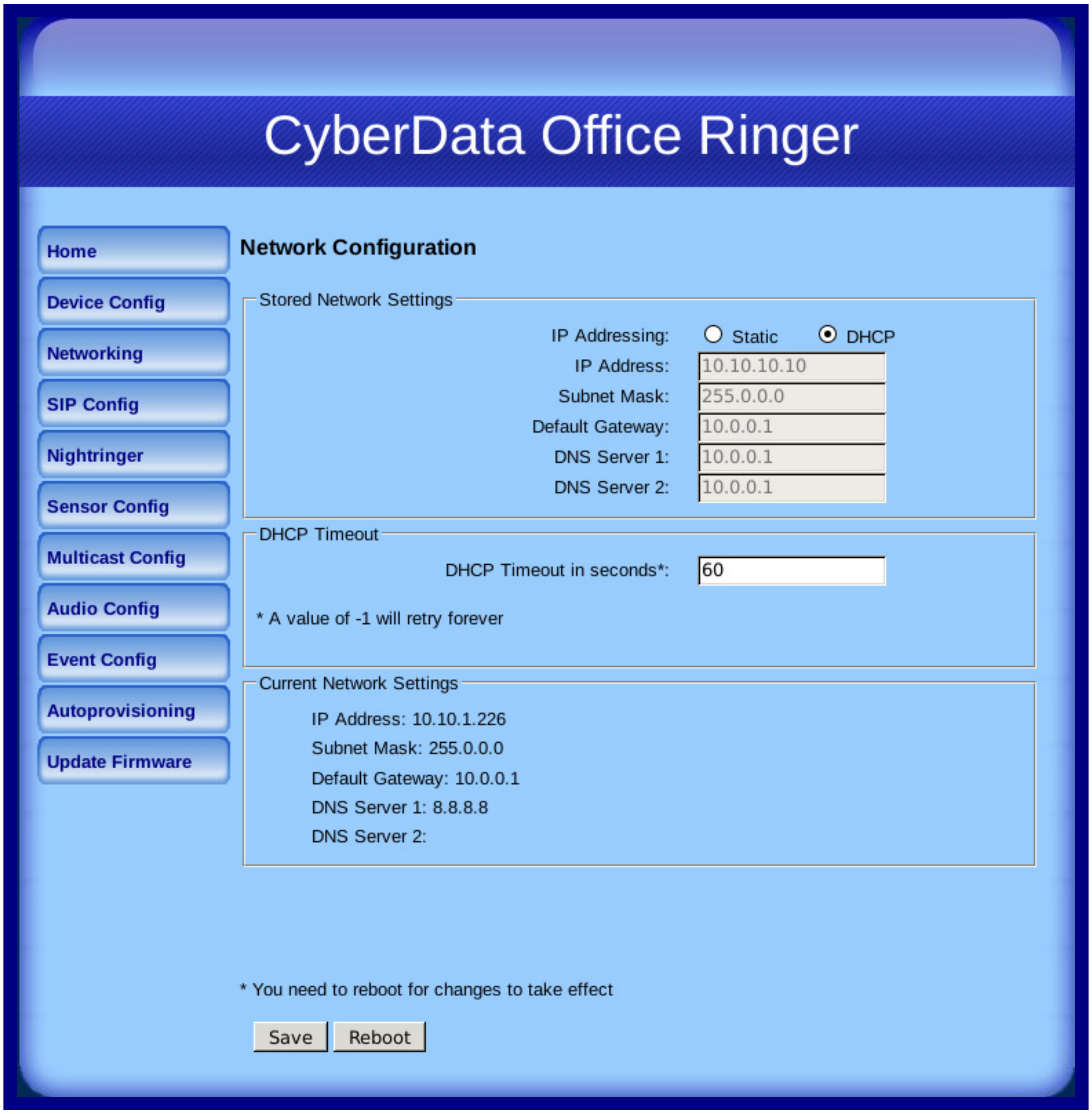
Web Page Item	Description
Volume Settings	
Speaker Volume	Type the desired volume level into this field.
Relay Settings	
Activate Relay with DTMF Code	When selected, the relay can be activated with a DTMF code.
DTMF Activation Code	Type the desired DTMF activation code (25 character limit).
DTMF Activation Duration (in seconds)	Type the desired DTMF activation duration (in seconds) (2 character limit [activation times now go up to 99 seconds]). **NOTE**: A DTMF activation duration of **0** will toggle the relay indefinitely or until the activation code is sent again
Activate Relay During Ring	When selected, the relay will be activated for as long as the call is active. **NOTE**: When the phone is set to **Auto Answer**, it will not ring and this option does nothing.
Activate Relay During Office Ring	Check this box to activate the relay for as long as a Night Ring tone is ringing.
Activate Relay While Call Active	When selected, the relay will be activated for as long as the call is active.
Miscellaneous Settings	
Auto-Answer Incoming Calls	When selected, the device will automatically answer incoming calls. When **Auto Answer** is Off, the device will play a ringtone through the speaker.
Play Ringback Tone	When selected, you will hear a ringback tone while making a call.
Volume Boost	When **Volume Boost** is enabled, the device will play at a higher volume at the risk of having the audio clip at very high levels.
	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
	Click on the **Test Audio** button to do an audio test. When the **Test Audio** button is pressed, you will hear a voice message for testing the device audio quality and volume.
	Click on the **Test Relay** button to do a relay test.
	Click on the **Reboot** button to reboot the system.

3. After changing the parameters, click the **Save** button.

2.3.5 Configure the Network Parameters

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

Figure 2-11. Network Configuration Page



Network Configuration

Stored Network Settings

IP Addressing: ○ Static ● DHCP
IP Address: 10.10.10.10
Subnet Mask: 255.0.0.0
Default Gateway: 10.0.0.1
DNS Server 1: 10.0.0.1
DNS Server 2: 10.0.0.1

DHCP Timeout

DHCP Timeout in seconds*: 60

* A value of -1 will retry forever

Current Network Settings

IP Address: 10.10.1.226
Subnet Mask: 255.0.0.0
Default Gateway: 10.0.0.1
DNS Server 1: 8.8.8.8
DNS Server 2:

* You need to reboot for changes to take effect

2. On the **Network Configuration** page, enter values for the parameters indicated in Table 2-9.

Table 2-9. Network Configuration Parameters

Web Page Item	Description
Stored Network Settings	
IP Addressing	Select either **DHCP IP Addressing** or **Static IP Addressing** by marking the appropriate radio button. If you select **Static**, configure the remaining parameters indicated in Table 2-9. If you select **DHCP**, go to Step 3.
IP Address	Enter the Static IP address.
Subnet Mask	Enter the Subnet Mask address.
Default Gateway	Enter the Default Gateway address.
DNS Server 1	Enter the DNS Server 1 address.
DNS Server 2	Enter the DNS Server 2 address.
DHCP Timeout	
DHCP Timeout in seconds	Enter the desired timeout duration (in seconds) that the device will wait for a response from the DHCP server before defaulting back to the stored static IP address. **Note**: A value of **-1** will cause the device to retry indefinitely and a value of **0** will cause the device to reset to a default of 60 seconds.
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.
	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
	Click on the **Reboot** button to reboot the system.

3. After changing the parameters, click **Save Settings**. This updates the changed parameters and reboots the Office Ringer if appropriate.

4. Connect the Office Ringer to the target network.

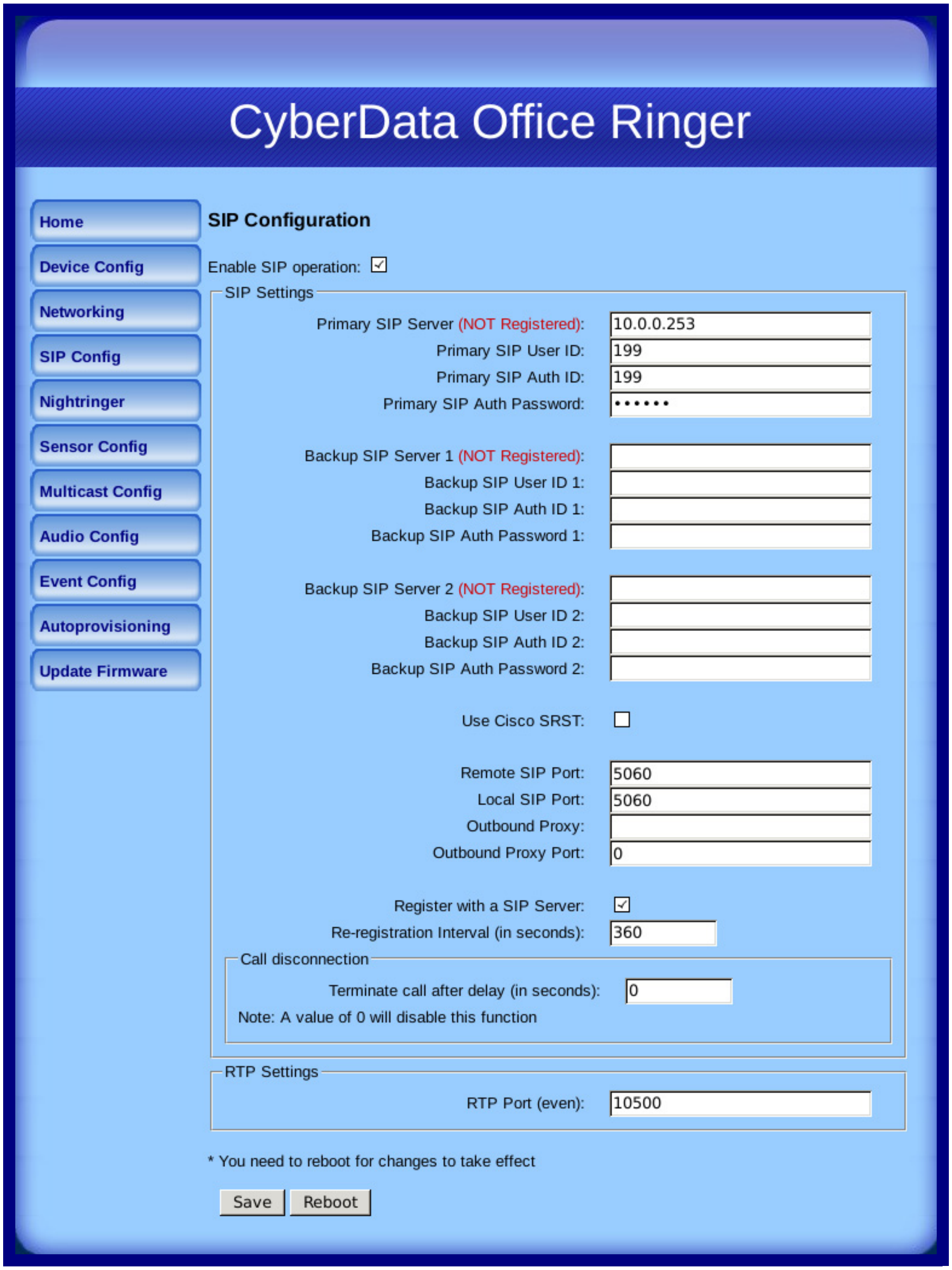
5. From a system on the same network as the Office Ringer, open a browser with the new IP address of the Office Ringer.

2.3.6 Configure the SIP Parameters

1. Click **SIP Config** to open the **SIP Configuration** page (Figure 2-12).

Note For specific server configurations, go to the following website address:
http://www.cyberdata.net/support/server/index.html

Figure 2-12. SIP Configuration Page



SIP Configuration

Enable SIP operation: ☑

SIP Settings

Primary SIP Server (NOT Registered): 10.0.0.253
Primary SIP User ID: 199
Primary SIP Auth ID: 199
Primary SIP Auth Password: ••••••

Backup SIP Server 1 (NOT Registered):
Backup SIP User ID 1:
Backup SIP Auth ID 1:
Backup SIP Auth Password 1:

Backup SIP Server 2 (NOT Registered):
Backup SIP User ID 2:
Backup SIP Auth ID 2:
Backup SIP Auth Password 2:

Use Cisco SRST: □

Remote SIP Port: 5060
Local SIP Port: 5060
Outbound Proxy:
Outbound Proxy Port: 0

Register with a SIP Server: ☑
Re-registration Interval (in seconds): 360

Call disconnection

Terminate call after delay (in seconds): 0
Note: A value of 0 will disable this function

RTP Settings

RTP Port (even): 10500

* You need to reboot for changes to take effect

2. On the **SIP Configuration** page, enter values for the parameters indicated in Table 2-10.

Table 2-10. SIP Configuration Parameters

Web Page Item	Description
Enable SIP Operation	Enables or disables SIP operation.
SIP Settings	
Primary SIP Server	Use this field to set the address (in dotted decimal notation or as a canonical name) for the Primary SIP Server. This field can accept canonical names of up to 255 characters in length.
Primary SIP User ID	Type the **SIP User ID** for the Primary SIP Server (up to 64 alphanumeric characters).
Primary Auth ID	Type the **Authenticate ID** for the Primary SIP Server (up to 64 alphanumeric characters).
Primary Auth Password	Type the **Authenticate Password** for the Primary SIP Server (up to 64 alphanumeric characters).
Backup SIP Server 1 Backup SIP Server 2	• If all of the **Primary SIP Server** and **Backup SIP Server** fields are populated, the device will attempt to stay registered with all three servers all of the time. You can leave the **Backup SIP Server 1** and **Backup SIP Server 2** fields blank if they are not needed. • In the event of a registration failure on the **Primary SIP Server**, the device will use the next highest priority server for outbound calls (**Backup SIP Server 1**). If **Backup SIP Server 1** fails, the device will use **Backup SIP Server 2**. • If a higher priority SIP Server comes back online, the device will switch back to this server.
Backup SIP User ID 1 Backup SIP User ID 2	Type the **SIP User ID** for the Backup SIP Server (up to 64 alphanumeric characters).
Backup SIP Auth ID 1 Backup SIP Auth ID 2	Type the **SIP Authenticate ID** for the Backup SIP Server (up to 64 alphanumeric characters).
Backup SIP Auth Password 1 Backup SIP Auth Password 2	Type the **SIP Authenticate Password** for the Backup SIP Server (up to 64 alphanumeric characters).
Use Cisco SRST	When selected, the backup servers are handled according to Cisco SRST (Survivable Remote Site Telephony).
Remote SIP Port	Type the **Remote SIP Port** number (default 5060) (8 character limit).
Local SIP Port*	Type the **Local SIP Port** number (default 5060) (8 character limit).
Outbound Proxy	Type the Outbound Proxy as either a numeric IP address in dotted decimal notation or the fully qualified host name (255 character limit [FQDN]).
Outbound Proxy Port	Type the Outbound Proxy Port number (8 character limit).
Register with a SIP Server	Check this box to enable SIP Registration.
Re-registration Interval (in seconds)	Type the SIP Registration lease time (in seconds)

Table 2-10. SIP Configuration Parameters

Web Page Item	Description
Call Disconnection	
Terminate call after delay (in seconds)	Type the desired number of seconds that you want to transpire after a connection delay before a call is terminated. Note: A value of **0** will disable this function.
RTP Settings	
RTP Port (even)	Specify the port number used for the RTP stream after establishing a SIP call. This port number has to be an even number and defaults to 10500.
	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
	Click on the **Reboot** button to reboot the system.

3. After changing the parameters, click **Save Settings**.

2.3.7 Configure the Nightringer Parameters

When the Nightringer is enabled, the device will register as a second SIP extension. Registration does not have to be to the same server as the primary SIP registration. Any calls made to the Nightringer extension will cause the device to play a ring tone. There is no way to answer this call. The Nightringer is designed to be used in buildings where calls made after hours are directed to a ring group.

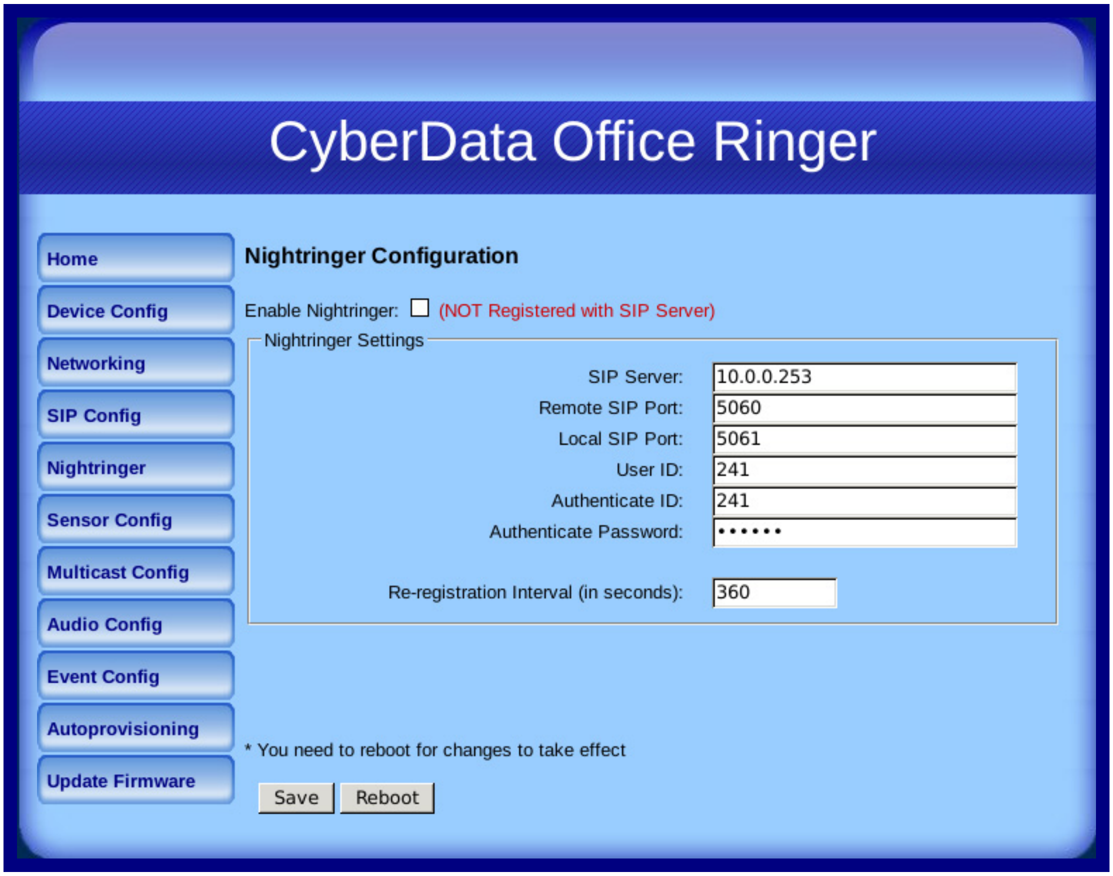
GENERAL ALERT

Caution

Nightringer requires SIP Registration. Nightringer cannot be used in peer to peer mode.

1. Click on the **Nightringer** button to open the **Nightringer Configuration** page. See Figure 2-13.

Figure 2-13. Nightringer Configuration Setup



Nightringer Configuration

Enable Nightringer: □ (NOT Registered with SIP Server)

Nightringer Settings

SIP Server: 10.0.0.253
Remote SIP Port: 5060
Local SIP Port: 5061
User ID: 241
Authenticate ID: 241
Authenticate Password: ••••••

Re-registration Interval (in seconds): 360

* You need to reboot for changes to take effect

2. On the **Nightringer Configuration** page, enter values for the parameters indicated in Table 2-11.

Table 2-11. Nightringer Configuration Parameters

Web Page Item	**Description**
Enable Nightringer	When the nightringer is enabled, the unit will attempt to register a second extension with the SIP server. Any calls made to this extension will play a ringtone.
Nightringer Settings	
SIP Server	Type the SIP server represented as either a numeric IP address in dotted decimal notation.
Remote SIP Port	Type the Remote SIP Port number (default 5060) (8 character limit).
Local SIP Port	Type the Local SIP Port number (default 5060) (8 character limit). **Note**: This value cannot be the same as the **Local SIP Port*** found on the **SIP Configuration Page**.
User ID	Type the **User ID** (up to 64 alphanumeric characters).
Authenticate ID	Type the **Authenticate ID** (up to 64 alphanumeric characters).
Authenticate Password	Type the **Authenticate Password** (up to 64 alphanumeric characters).
Re-registration Interval (in seconds)	Type the SIP Registration lease time in minutes (default is 60 minutes) (8 character limit). Re-registration Interval (in seconds)*
	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
	Click on the **Reboot** button to reboot the system.

3. After changing the parameters, click on the **Save** button.

2.3.8 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 Configuration** 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.

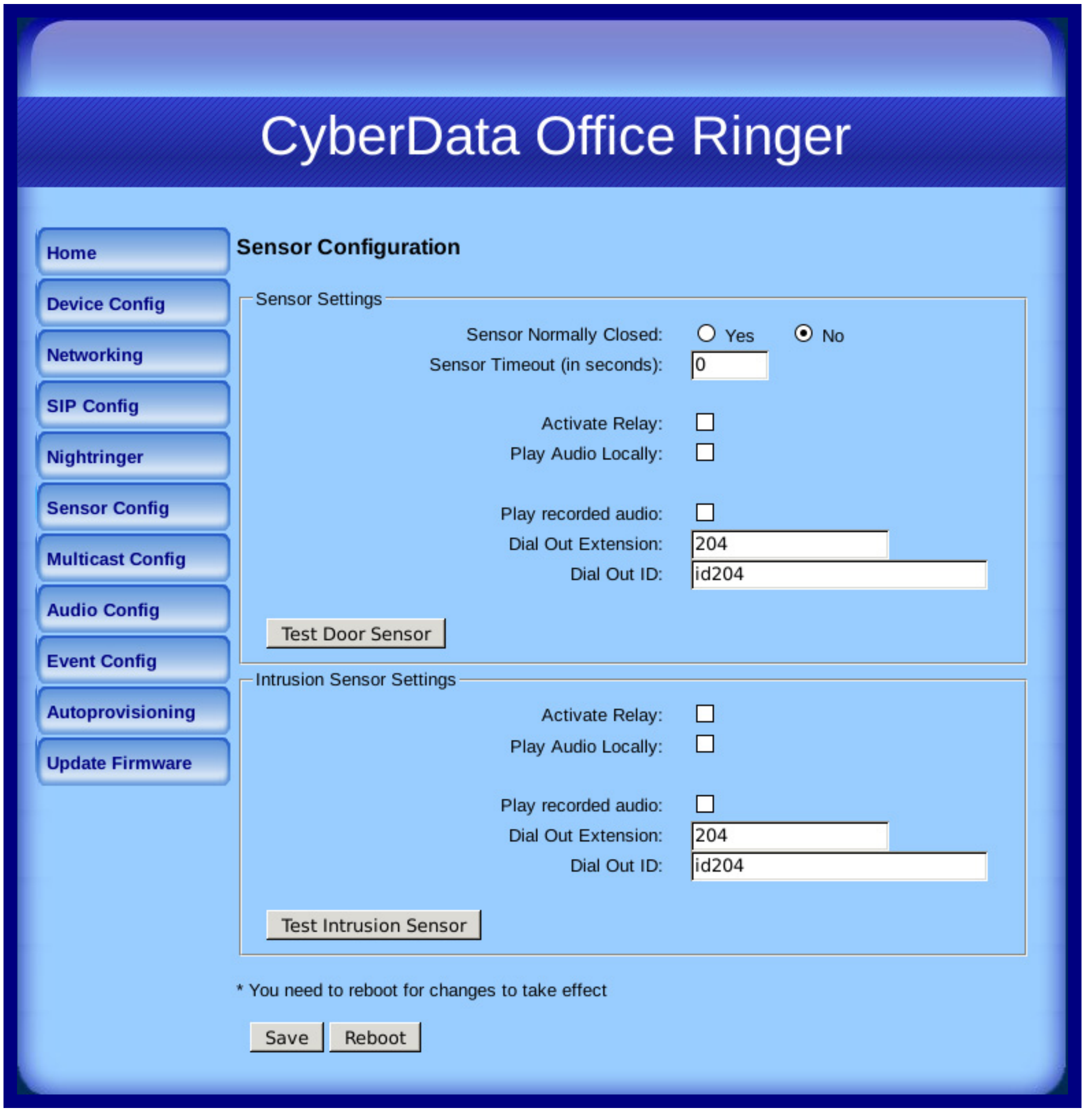
The intrusion sensor is an optical sensor installed on the board and will be activated when the device is removed from the case.

For each sensor, the device can take the following actions:

- Activate the relay until the sensor is deactivated
- Loop an audio file out of the speaker until the sensor is deactivated
- Call a preset extension and play a pre-recorded audio file (once)

1. Click **Sensor Config** to open the **Sensor Configuration** page (Figure 2-14).

Figure 2-14. Sensor Configuration Page



Sensor Configuration

Sensor Settings

Sensor Normally Closed: ○ Yes ● No
Sensor Timeout (in seconds): 0

Activate Relay: □
Play Audio Locally: □

Play recorded audio: □
Dial Out Extension: 204
Dial Out ID: id204

Test Door Sensor

Intrusion Sensor Settings

Activate Relay: □
Play Audio Locally: □

Play recorded audio: □
Dial Out Extension: 204
Dial Out ID: id204

Test Intrusion Sensor

* You need to reboot for changes to take effect

Save Reboot

2. On the **Sensor Configuration** page, enter values for the parameters indicated in Table 2-12.

Table 2-12. Sensor Configuration Parameters

Web Page Item	Description
Sensor Settings	
Sensor Normally Closed	Select the inactive state of the sensors.
Sensor Timeout (in seconds)	Select the number of seconds that you want to pass before the sensor is activated.
Activate Relay	Check this box to activate the relay until the sensor is deactivated.
Play Audio Locally	Check this box to loop an audio file out of the speaker until the sensor is deactivated.
Play recorded audio	Check this box to to make a call to the dial out extension and play pre-recorded audio.
Dial Out Extension	Enter the desired dial-out extension number.
Dial Out ID	Type the desired Extension ID (64 character limit).
	Use this button to test the sensor.
Intrusion Sensor Settings	
Activate Relay	Check this box to activate the relay until the sensor is deactivated.
Play Audio Locally	Check this box to loop an audio file out of the speaker until the sensor is deactivated.
Play recorded audio	Check this box to to make a call to the dial out extension and play pre-recorded audio.
Dial Out Extension	Enter the desired dial-out extension number.
Dial Out ID	Type the desired Extension ID (64 character limit).
	Use this button to test the Intrusion sensor.
	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
	Click on the **Reboot** button to reboot the system.

3. After changing the parameters, click **Save Settings**.

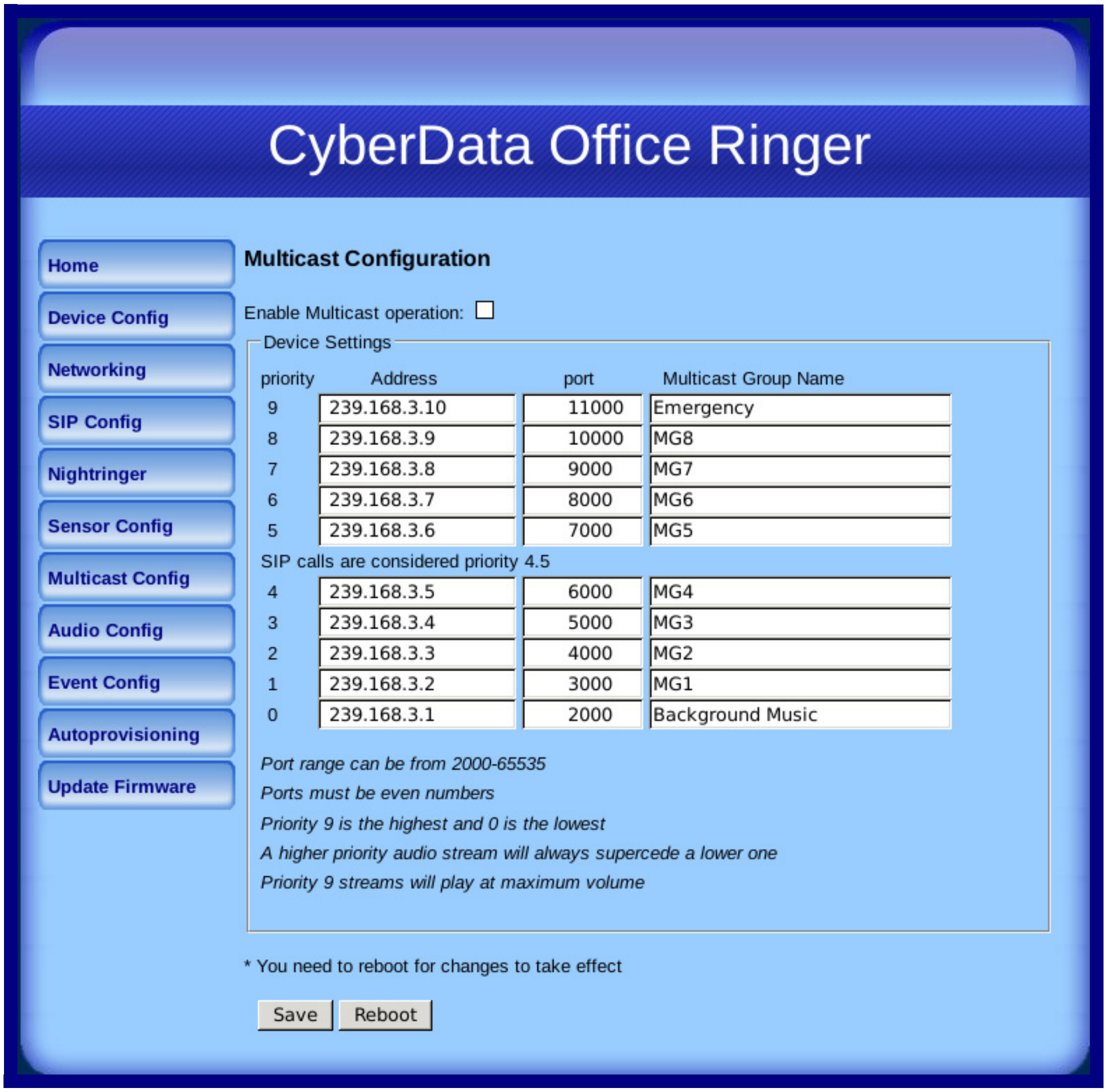
2.3.9 Configure the Multicast Parameters

Multicast groups use multicasting to create public address paging zones. Multicasting is based on the concept of a group. Multicast addresses specify an arbitrary group of IP hosts that have joined the group and want to receive traffic sent to the group. Group members send IGMP messages to their local multicast routers, allowing the group traffic traversal from the source.

The **Multicast Configuration** page allows the device to join up to 10 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 devices 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 three. The device supports simultaneous SIP and Multicast.

1. Click on the **Multicast Configuration** button to open the **Multicast Configuration** page. See Figure 2-15.

Figure 2-15. Multicast Configuration Page



Multicast Configuration

Enable Multicast operation: □

Device Settings

priority	Address	port	Multicast Group Name
9	239.168.3.10	11000	Emergency
8	239.168.3.9	10000	MG8
7	239.168.3.8	9000	MG7
6	239.168.3.7	8000	MG6
5	239.168.3.6	7000	MG5
SIP calls are considered priority 4.5			
4	239.168.3.5	6000	MG4
3	239.168.3.4	5000	MG3
2	239.168.3.3	4000	MG2
1	239.168.3.2	3000	MG1
0	239.168.3.1	2000	Background Music

Port range can be from 2000-65535
Ports must be even numbers
Priority 9 is the highest and 0 is the lowest
A higher priority audio stream will always supercede a lower one
Priority 9 streams will play at maximum volume

* You need to reboot for changes to take effect

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

Table 2-13. Multicast Configuration Parameters

Web Page Item	Description
Enable Multicast Operation	Enables or disables multicast operation.
Device Settings	
Priority	Indicates the priority for the multicast group. Priority **9** is the highest (emergency streams). **0** is the lowest (background music). SIP calls are considered priority **4.5**. See Section 2.3.9.1, "Assigning Priority" for more details.
Address	Enter the multicast IP Address for this multicast group (15 character limit).
Port (range can be from 2000 to 65535)	Enter the port number for this multicast group (5 character limit). **Note**: The multicast ports have to be even values. The webpage will enforce this restriction.
Multicast Group Name	Assign a descriptive name for this multicast group (25 character limit).
	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
	Click on the **Reboot** button to reboot the system.

3. After changing the parameters, click on the **Save** button.

2.3.9.1 Assigning Priority

When playing multicast streams, audio on different streams will preempt each other according to their priority in the list. An audio stream with a higher priority will interrupt a stream with a lower priority.

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 level is set to maximum.

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

Ringtones and Nightringtones

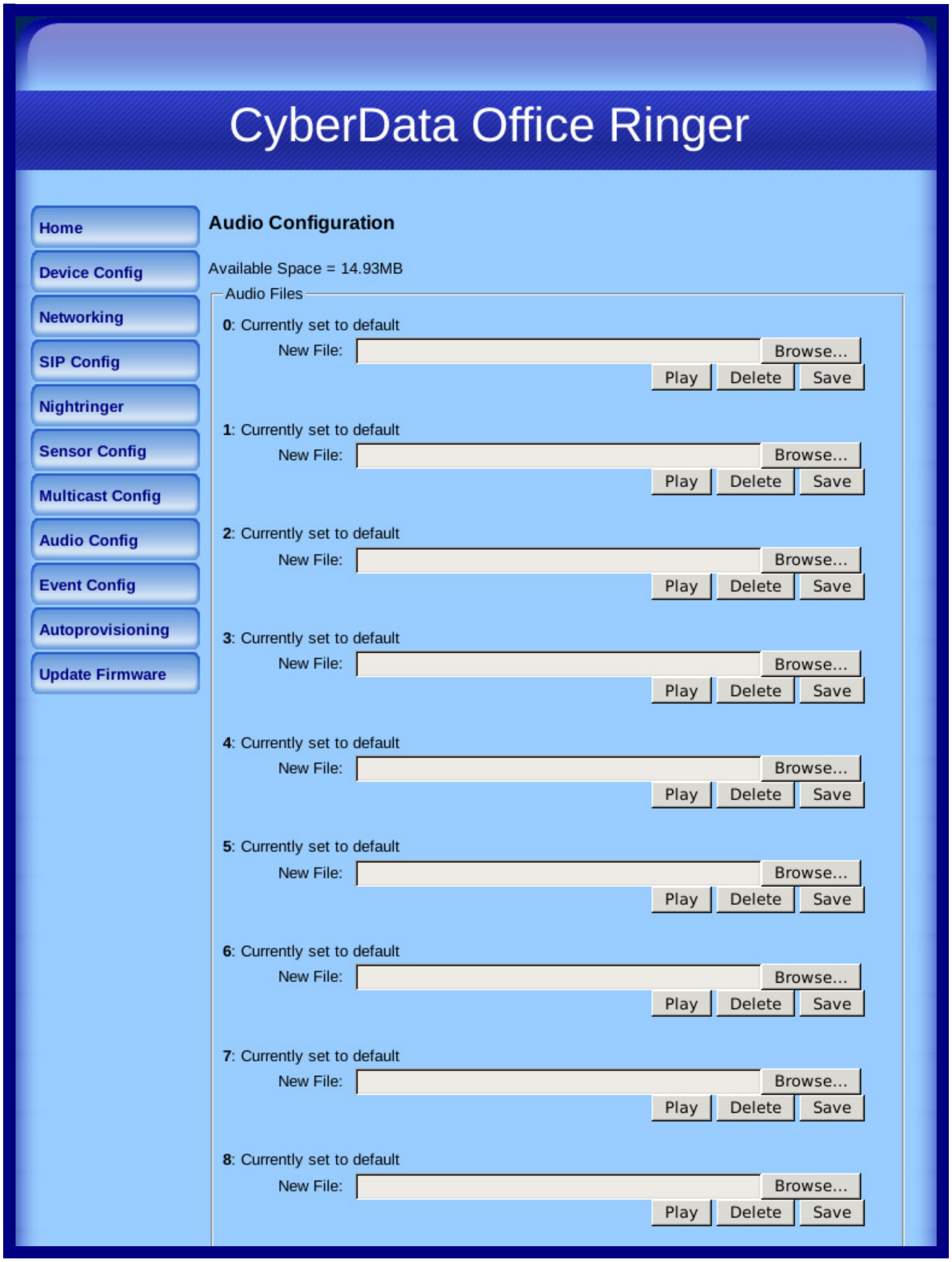
Ringtones all play at the same priority level. This means that it is possible to have a nightring tone and a normal ringtone playing at the same time.

2.3.10 Configure the Audio Configuration Parameters

The **Audio Configuration** 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 **Audio Config** to open the **Audio Configuration** page (Figure 2-16).

Figure 2-16. Audio Configuration Page



Audio Configuration

Available Space = 14.93MB

Audio Files

0: Currently set to default
New File:

1: Currently set to default
New File:

2: Currently set to default
New File:

3: Currently set to default
New File:

4: Currently set to default
New File:

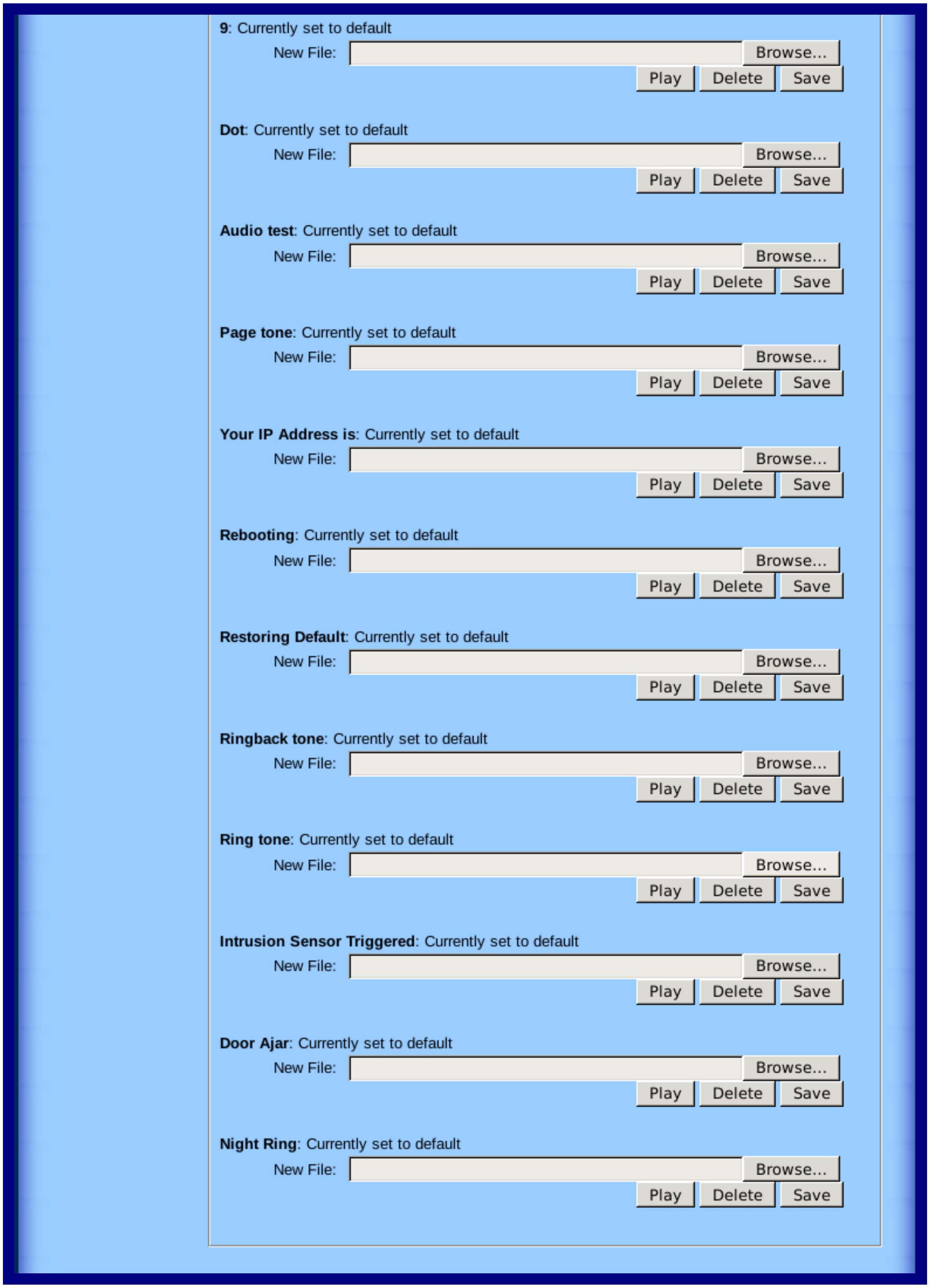
5: Currently set to default
New File:

6: Currently set to default
New File:

7: Currently set to default
New File:

8: Currently set to default
New File:

Figure 2-17. Audio Configuration Page (continued)



9: Currently set to default

New File:

Dot: Currently set to default

New File:

Audio test: Currently set to default

New File:

Page tone: Currently set to default

New File:

Your IP Address is: Currently set to default

New File:

Rebooting: Currently set to default

New File:

Restoring Default: Currently set to default

New File:

Ringback tone: Currently set to default

New File:

Ring tone: Currently set to default

New File:

Intrusion Sensor Triggered: Currently set to default

New File:

Door Ajar: Currently set to default

New File:

Night Ring: Currently set to default

New File:

2. On the **Audio Configuration** page, enter values for the parameters indicated in Table 2-14.

Table 2-14. Audio Configuration Parameters

Web Page Item	Description
Audio Files	
0-9	The name of the audio configuration option is the same as the spoken audio that plays on the board (24 character limit). '0' corresponds to the spoken word “zero.” '1' corresponds to the spoken word “one.” '2' corresponds to the spoken word “two.” '3' corresponds to the spoken word “three.” '4' corresponds to the spoken word “four.” '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.
	The **Browse** button will allow you to navigate to and select an audio file.
	The **Play** button will play that audio file.
	The **Delete** button will delete any user uploaded audio and restore the stock audio file.
	The **Save** button will download a new user audio file to the board once you've selected the file by using the **Browse** button. The **Save** button will delete any pre-existing user-uploaded audio files.

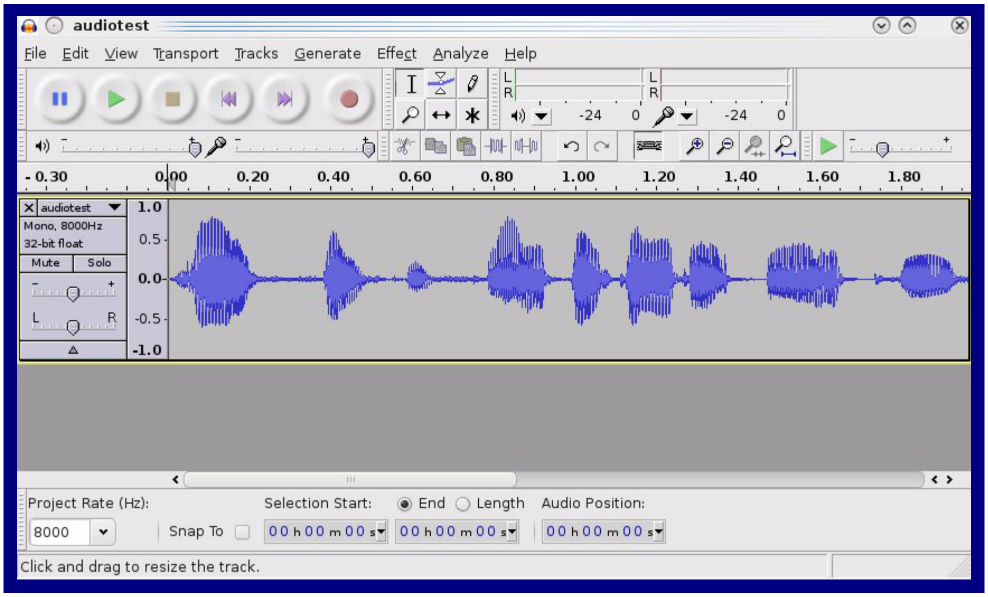
2.3.10.1 User-created Audio Files

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

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

You can use the free utility *Audacity* to convert audio files into this format. See Figure 2-18 through Figure 2-20.

Figure 2-18. Audacity 1



Mono, 8000Hz
32-bit float

Project Rate (Hz): 8000

Snap To □

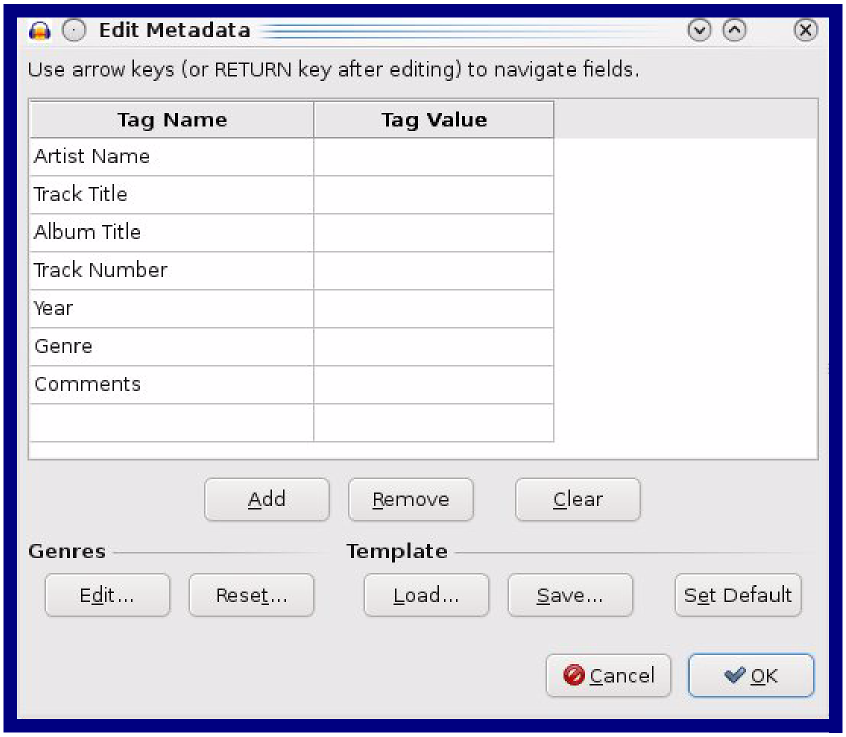
Selection Start: 00 h 00 m 00 s

● End ○ Length 00 h 00 m 00 s

Audio Position: 00 h 00 m 00 s

Click and drag to resize the track.

Figure 2-19. Audacity 2



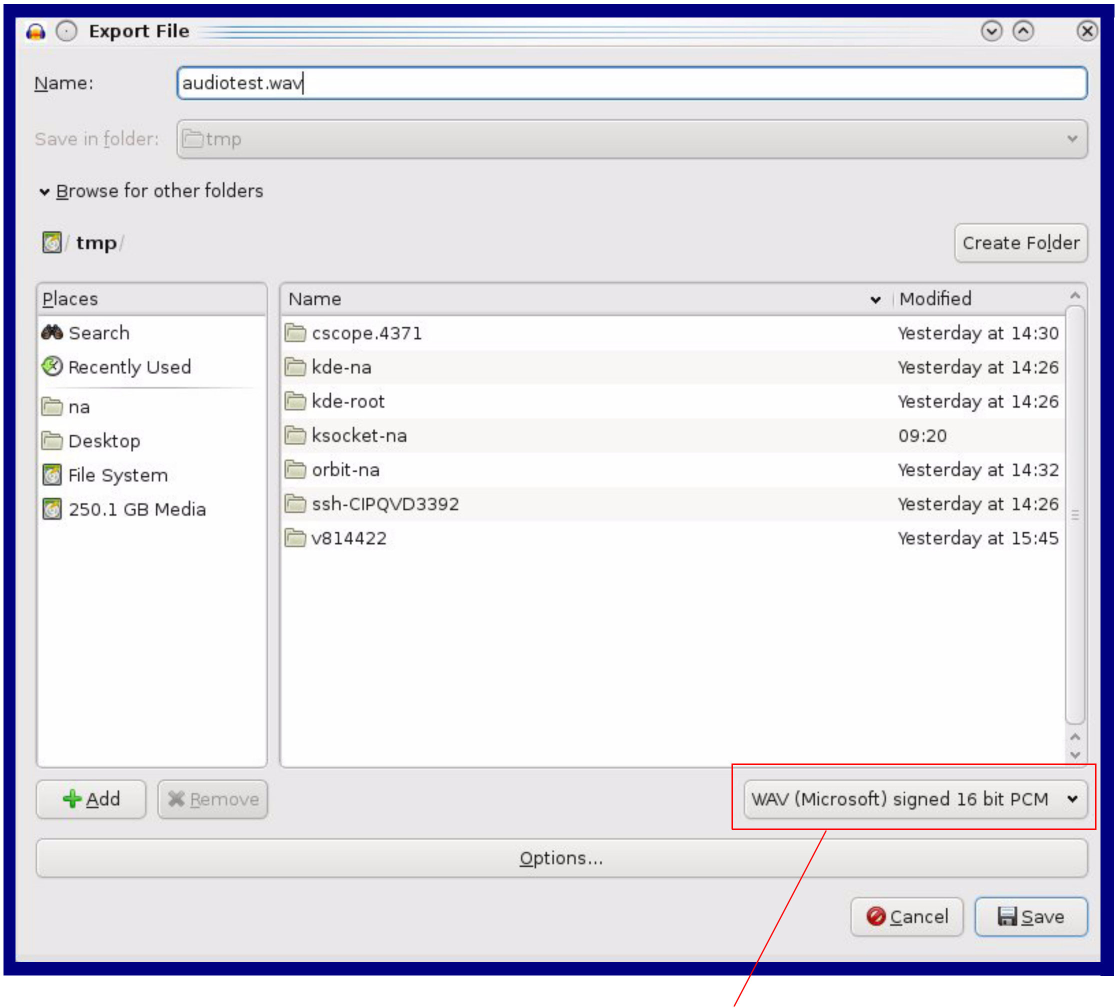
Use arrow keys (or RETURN key after editing) to navigate fields.

Tag Name	Tag Value
Artist Name	
Track Title	
Album Title	
Track Number	
Year	
Genre	
Comments	

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

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

Figure 2-20. WAV (Microsoft) signed 16 bit PCM



Export File

Name: audiotest.wav

Save in folder: tmp

Name	Modified
cscope.4371	Yesterday at 14:30
kde-na	Yesterday at 14:26
kde-root	Yesterday at 14:26
ksocket-na	09:20
orbit-na	Yesterday at 14:32
ssh-CIPQVD3392	Yesterday at 14:26
v814422	Yesterday at 15:45

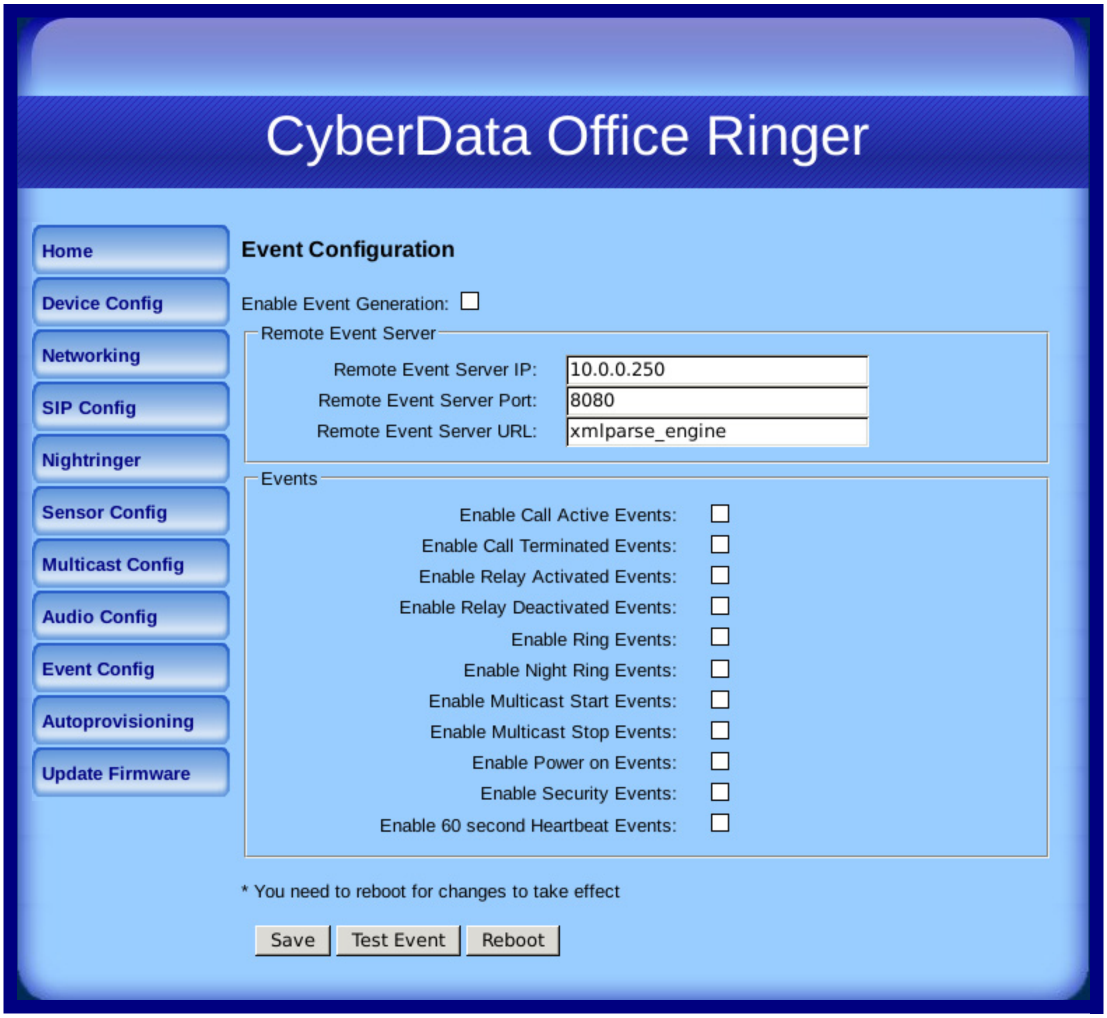
WAV (Microsoft) signed 16 bit PCM

WAV (Microsoft) signed 16 bit PCM

2.3.11 Configure the Event Parameters

Click the **Event Config** button to open the **Event Configuration** page (Figure 2-21). The **Event Configuration** page specifies a remote server that can be used to receive HTTP POST events when actions take place on the board.

Figure 2-21. Event Configuration Page



Event Configuration

Enable Event Generation: □

Remote Event Server

Remote Event Server IP: 10.0.0.250
Remote Event Server Port: 8080
Remote Event Server URL: xmlparse_engine

Events

Enable Call Active Events: □
Enable Call Terminated Events: □
Enable Relay Activated Events: □
Enable Relay Deactivated Events: □
Enable Ring Events: □
Enable Night Ring Events: □
Enable Multicast Start Events: □
Enable Multicast Stop Events: □
Enable Power on Events: □
Enable Security Events: □
Enable 60 second Heartbeat Events: □

* You need to reboot for changes to take effect

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

Table 2-15. Event Configuration

Web Page Item	Description
Enable Event Generation	When selected, Event Generation is enabled.
Remote Event Server	
Remote Event Server IP	Type the Remote Event Server IP address. (64 character limit)
Remote Event Server Port	Type the Remote Event Server port number. (8 character limit)
Remote Event Server URL	Type the Remote Event Server URL. (127 character limit)
Events	
Enable Call Active Events	When selected, Call Active Events are enabled.
Enable Call Terminated Events	When selected, Call Terminated Events are enabled.
Enable Relay Activated Events	When selected, Relay Activated Events are enabled.
Enable Relay Deactivated Events	When selected, Relay Deactivated Events are enabled.
Enable Ring Events	When selected, Ring Events are enabled.
Enable Night Ring Events	When selected, there is a notification when the unit receives a night ring.
Enable Multicast Start Events	When selected, Multicast Start Events are enabled.
Enable Multicast Stop Events	When selected, Multicast Stop Events are enabled.
Enable Power On Events	When selected, Power On Events are enabled.
Enable Security Events	When selected, Security Events are enabled.
Enable 60 Second Heartbeat Events	When selected, 60 Second Heartbeat Events are enabled.
	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
	Click on the **Test Event** button to test an event.
	Click on the **Reboot** button to reboot the system.

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
```

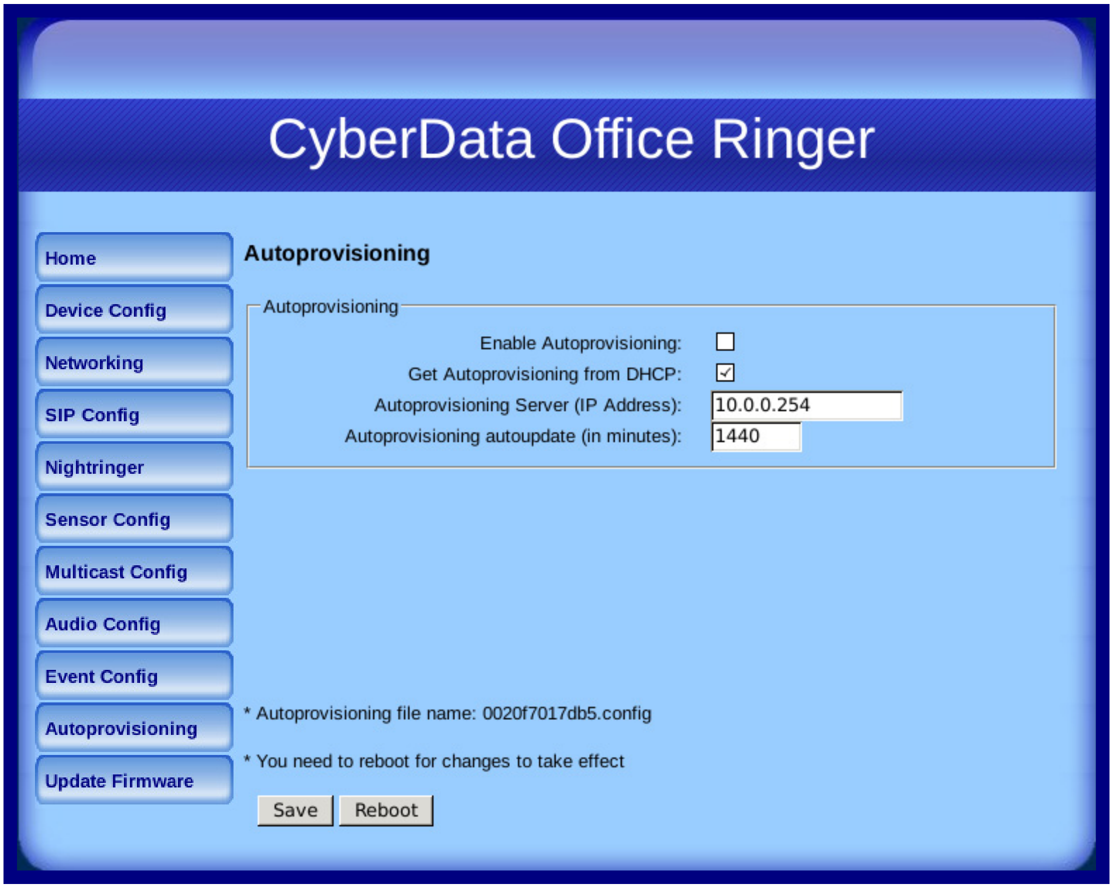
```
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 197
Content-Type: application/x-www-form-urlencoded

<?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 Autoprovisioning Parameters

1. Click the **Autoprovisioning** button to open the **Autoprovisioning Configuration** page. See Figure 2-22.

Figure 2-22. Autoprovisioning Configuration Page



Autoprovisioning

Autoprovisioning

Enable Autoprovisioning: □
Get Autoprovisioning from DHCP: ☑
Autoprovisioning Server (IP Address): 10.0.0.254
Autoprovisioning autoupdate (in minutes): 1440

* Autoprovisioning file name: 0020f7017db5.config

* You need to reboot for changes to take effect

2. On the **Autoprovisioning Configuration** page, you may enter values for the parameters indicated in Table 2-16.

Table 2-16. Autoprovisioning Configuration Parameters

Web Page Item	Description
Autoprovisioning	
Enable Autoprovisioning	See Section 2.3.12.1, "Autoprovisioning".
Get Autoprovisioning from DHCP	See Section 2.3.12.1, "Autoprovisioning".
Autoprovisioning Server (IP Address)	See Section 2.3.12.1, "Autoprovisioning" (15 character limit).
Autoprovisioning Autoupdate (in minutes)	Type the desired time (in minutes) that you want the Autoprovisioning feature to update (6 character limit).
	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
	Click on the **Reboot** button to reboot the system.

3. After changing the parameters, click the **Save** button.

2.3.12.1 Autoprovisioning

Enable Autoprovisioning Option

With autoprovisioning enabled, the board will get its configuration from a remote TFTP server on startup or periodically on a scheduled delay. Autoprovisioned values will override values stored in on-board memory and will be visible on the web page. The board gets its autoprovisioning information from an XML-formatted file hosted from a TFTP server. CyberData will provide a template for this XML file and the user can modify it for their own use.

To use autoprovisioning, create a copy of the autoprovisioning template with the desired settings and name this file with the mac address of the device to configure (for example: **0020f7350058.config**). Put this file into your TFTP server directory and manually set the TFTP server address on the board.

It is not necessary to set every option found in the autoprovisioning template. As long as the XML is valid, the file can contain any subset. Options not autoprovisioned will default to the values stored in the on board memory. For example if you only wanted to modify the device name, the following would be a valid autoprovisioning file:

```
<?xml version="1.0" encoding="utf-8" ?>
<specific>
    <MiscSettings>
        <DeviceName>auto Office Ringer</DeviceName>
    </MiscSettings>

</specific>
```

Networking

The board will only apply networking settings or firmware upgrades after a reboot.

Get Autoprovisioning from DHCP

When this option is checked, the device will automatically fetch its autoprovisioning server address from the DHCP server. The device will use the address specified in **OPTION 150** (TFTP-server-name) or **OPTION 66**. If both options are set, the device will use **OPTION 150**.

Refer to the documentation of your DHCP server for setting up **OPTION 150**.

To set up a Linux DHCPD server to serve autoprovisioning information (in this case using both option 66 and 150), here's an example dhcpd.conf:

```
# dhcpd.conf
#
# Configuration file for ISC dhcpd (see 'man dhcpd.conf')
#
ddns-update-style ad-hoc;

option option-150 code 150 = ip-address;

subnet 10.0.0.0 netmask 255.0.0.0 {
        max-lease-time 120;
        default-lease-time 120;

        option routers                  10.0.0.1;
        option subnet-mask              255.0.0.0;

        option domain-name              "voiplab";
        option domain-name-servers       10.0.0.1;

        option time-offset              -8;     # Pacific Standard Time

        option tftp-server-name         "10.0.0.254";

        option option-150               10.0.0.254;

        range 10.10.0.1 10.10.2.1;}
```

Autoprovisioning Server (IP Address)

Instead of using DHCP to provide the autoprovisioning tftp server address, you can specify an address manually.

Autoprovisioning Autoupdate

If **Autoprovisioning** is enabled and the **Autoprovisioning Autoupdate** value is something other than **0** minutes, a service is started on startup that will wait the configured number of minutes and then try to re-download its autoprovisioning file. It will compare its previously autoprovisioned file with this new file and if there are differences, it will reboot the board.

Autoprovisioned Firmware Upgrades

An Autoprovisioned firmware upgrade only happens after a reboot, will take roughly three minutes, and the web page will be unresponsive during this time.

The '**FirmwareVersion**' value in the xml file *must* match the version stored in the '**FirmwareFile**'.

```
<FirmwareVersion>v7.1.6</FirmwareVersion>
<FirmwareFile>716-officeringer-uImage</FirmwareFile>
```

If these values are mismatched, the board can get stuck in a loop where it goes through the following sequence of actions:

1. The board downloads and writes a new firmware file.
2. After the next reboot, the board recognizes that the firmware version does not match.
3. The board downloads and writes the firmware file again.

CyberData has timed a firmware upgrade at 140 seconds. Therefore, if you suspect the board is stuck in a loop, either remove or comment out the **FirmwareVersion** line in the XML file and let the board boot as it normally does.

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 the **Delete** button on the **Audio Configuration** page which will restore the default audio file. You can also change the autoprovisioning file with the word **default** set as the file name.

2.4 Upgrading the Firmware and Rebooting the Device

Note V3 Office Ringers can only run firmware versions 7.0.0 or later.

⚠ GENERAL ALERT	**Caution** When upgrading to firmware version 6.x.x from version 5.x.x or earlier, your device configuration settings will be lost because the way that the device stores the configuration settings is different in version 6.x.x.

2.4.1 Upgrading 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

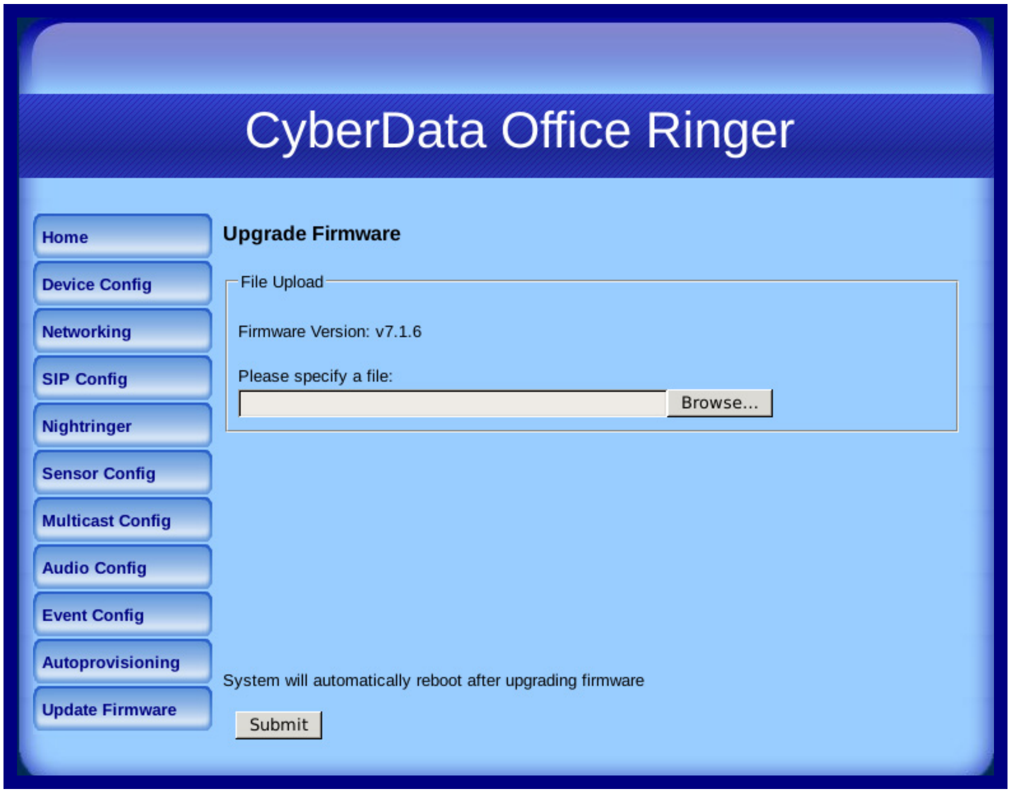
2. Unzip the firmware version file. This file may contain the following:

- Firmware file
- Release notes

3. Log in to the Office Ringer home page as instructed in Section 2.3.3, "Log in to the Configuration Home Page".

4. Click the **Update Firmware** button to open the **Upgrade Firmware** page. See Figure 2-23.

Figure 2-23. Upgrade Firmware Page



Upgrade Firmware

File Upload

Firmware Version: v7.1.6

Please specify a file:

System will automatically reboot after upgrading firmware

5. Select **Browse**, and then navigate to the location of the Office Ringer firmware file.

6. Click **Submit**.

Note Do not reboot the board after pressing the **Submit** 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 **Upgrade Firmware** page will refresh. The uploaded firmware filename should be displayed in the system configuration (indicating successful upload and reboot).

Table 2-17 shows the web page items on the **Upgrade Firmware** page.

Table 2-17. Firmware Upgrade Parameters

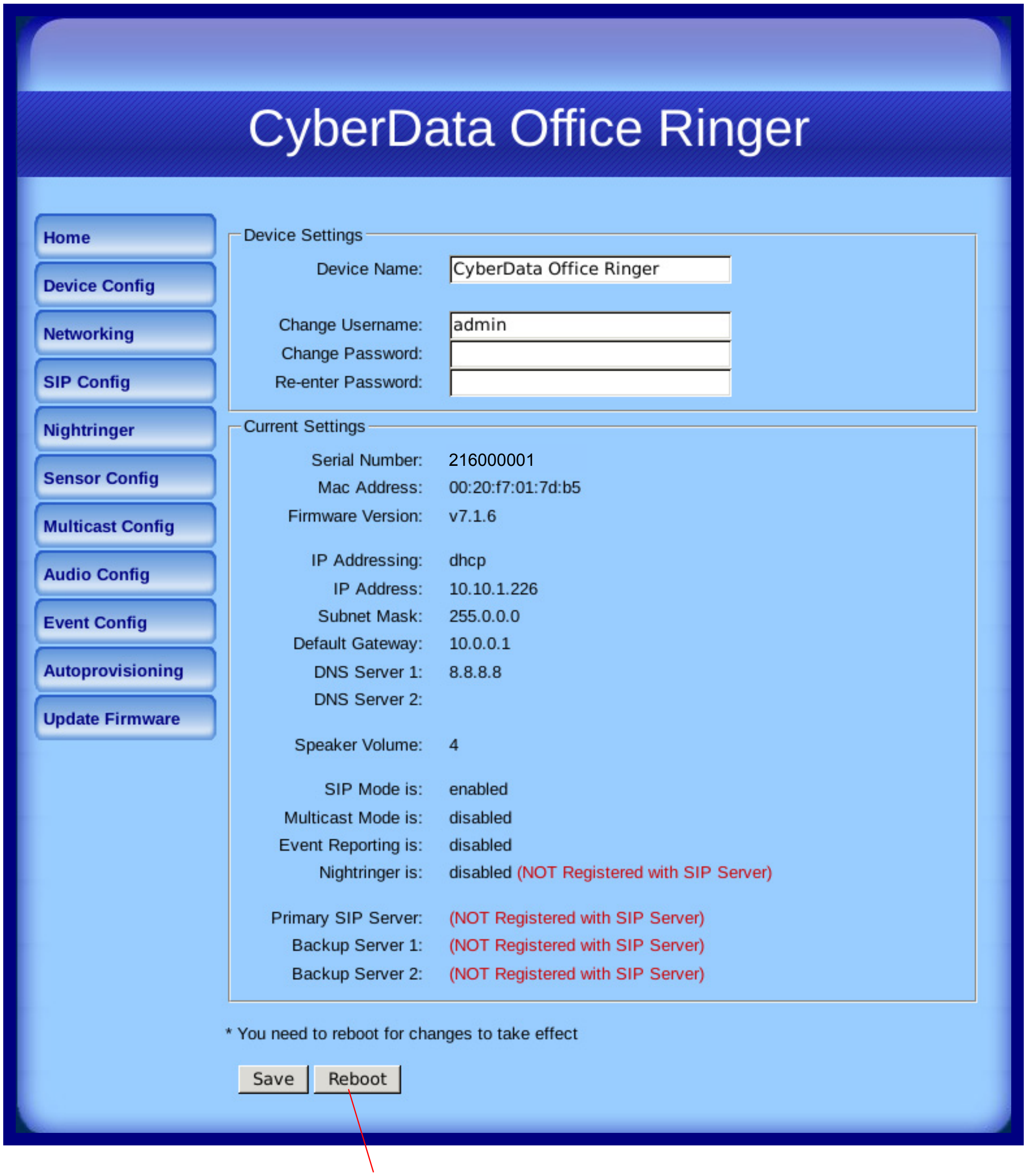
	Description
File Upload	
Firmware Version	Shows the current firmware version.
Browse...	Use the **Browse** button to navigate to the location of the firmware file that you want to upload.
Submit	Click on the **Submit** button to automatically upload the selected firmware and reboot the system.

2.4.2 Rebooting the Device

To reboot a Office Ringer, log in to the web page as instructed in Section 2.3.3, "Log in to the Configuration Home Page".

1. Click **Reboot** (Figure 2-24). A normal restart will occur.

Figure 2-24. Reboot System Section



Device Settings

Device Name:	CyberData Office Ringer
Change Username:	admin
Change Password:	
Re-enter Password:	

Current Settings

Serial Number:	216000001
Mac Address:	00:20:f7:01:7d:b5
Firmware Version:	v7.1.6
IP Addressing:	dhcp
IP Address:	10.10.1.226
Subnet Mask:	255.0.0.0
Default Gateway:	10.0.0.1
DNS Server 1:	8.8.8.8
DNS Server 2:	
Speaker Volume:	4
SIP Mode is:	enabled
Multicast Mode is:	disabled
Event Reporting is:	disabled
Nightringer is:	disabled (NOT Registered with SIP Server)
Primary SIP Server:	(NOT Registered with SIP Server)
Backup Server 1:	(NOT Registered with SIP Server)
Backup Server 2:	(NOT Registered with SIP Server)

* You need to reboot for changes to take effect

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 2-18 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 2-18. Command Interface Post Commands

Device Action	HTTP Post Command[a]
Trigger relay (for configured delay)	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://10.0.3.71/cgi-bin/command.cgi" --post-data "call=130"
Terminate active call	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/command.cgi" --post-data "terminate=yes"
Force reboot	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/command.cgi" --post-data "reboot=yes"
Test Audio button	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/command.cgi" --post-data "test_audio=yes"
Announce IP address	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_3=yes"
Play the "4" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_4=yes"

Table 2-18. Command Interface Post Commands

Device Action	HTTP Post Command[a]
Play the "5" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_doorajar=yes"
Play the "Night Ring" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_nightring=yes"

Table 2-18. Command Interface Post Commands

Device Action	HTTP Post Command[a]
Play the "5" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_doorajar=yes"
Play the "Night Ring" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "play_nightring=yes"

Table 2-18. Command Interface Post Commands

Device Action	HTTP Post Command[a]
Delete the "0" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_restoringdefault=yes"
Delete the "Ringback tone" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/audioconfig.cgi" --post-data "delete_ringback=yes"

Table 2-18. Command Interface Post Commands

Device Action	HTTP Post Command[a]
Delete the "Ring tone" audio file	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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 --quiet -O /dev/null "http://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.

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)

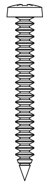
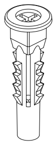
Quantity	Part Name	Illustration
4	#6 x 1" Pan head phillips wood screw	
4	Plastic-ribbed anchor	

Table A-1. Gang Box Mounting Components

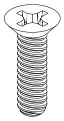
Quantity	Part Name	Illustration
4	6-32 x 0.5-inch flat undercut Phillips machine screw	

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

Figure A-1. Cable Connections

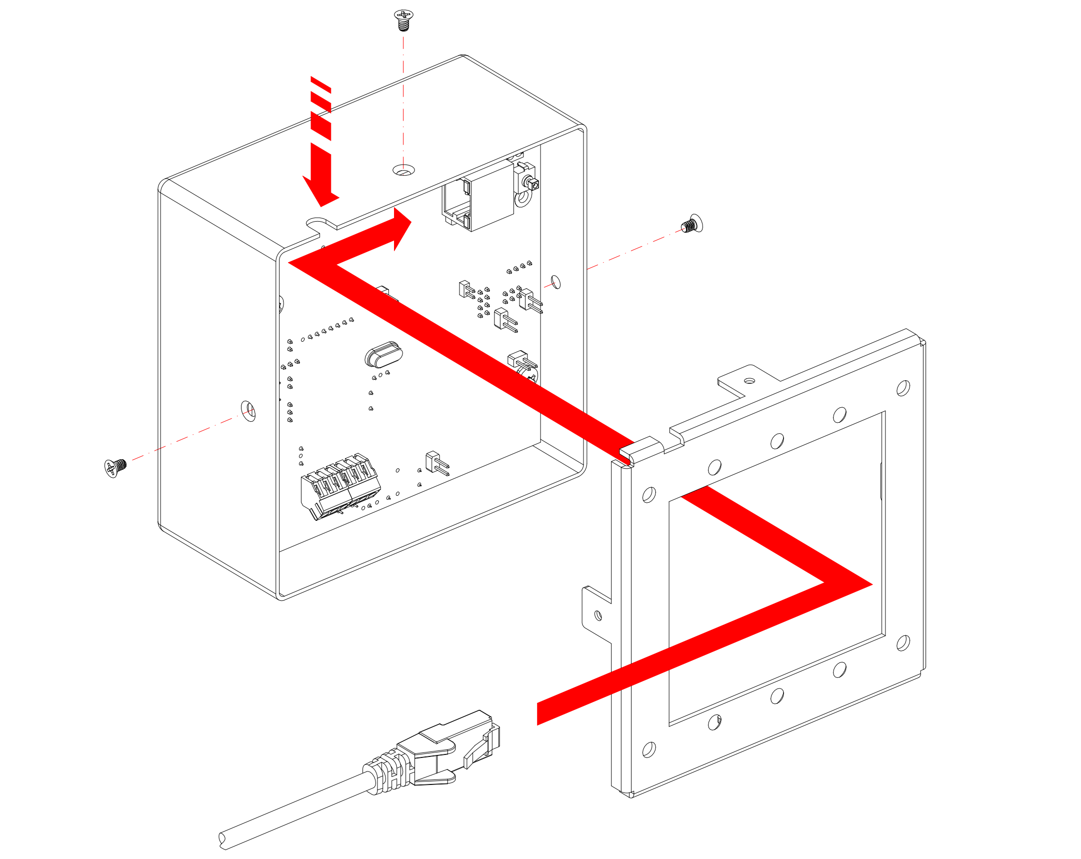


Figure A-2 shows a wall mounting option.

Figure A-2. Wall Mounting Option

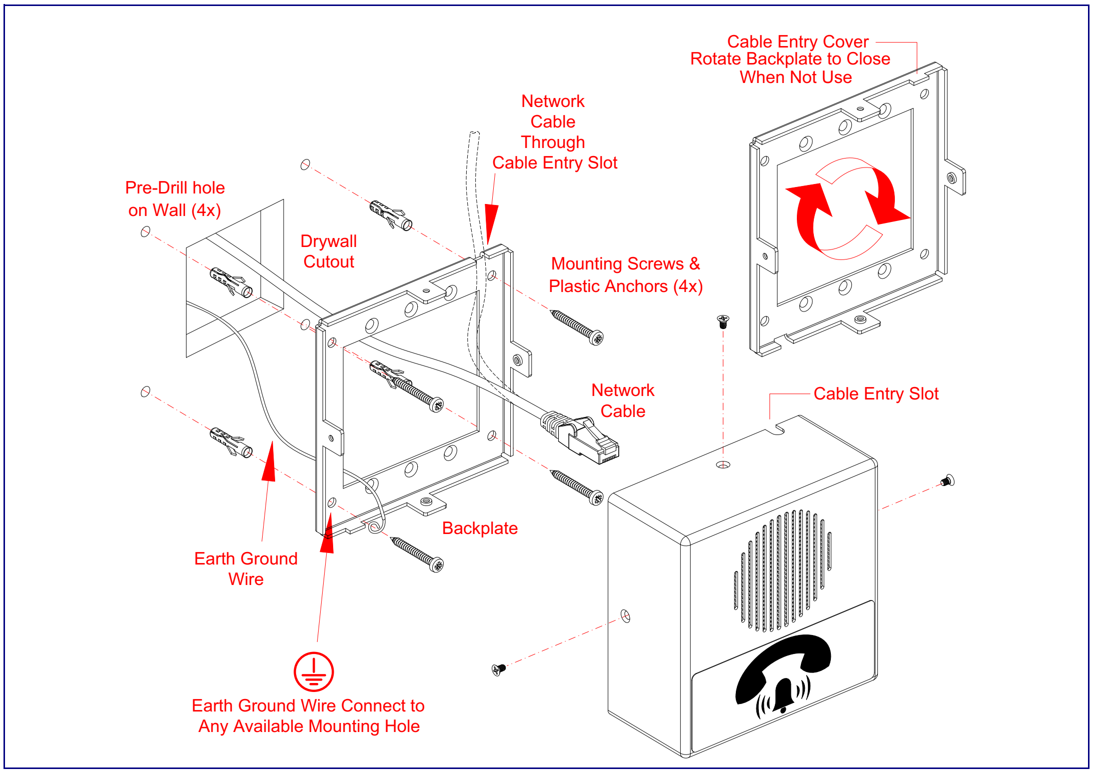


Figure A-3 shows a 1-Gang Box and a 2-Gang Box mounting option.

Figure A-3. Gang Box Mounting

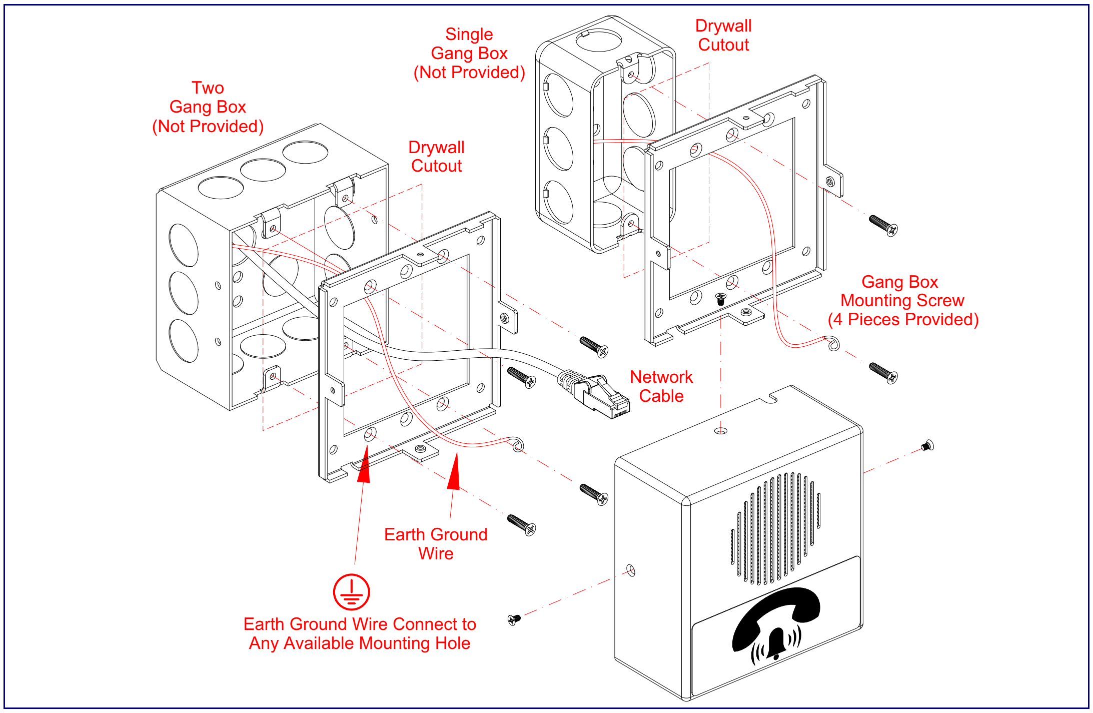
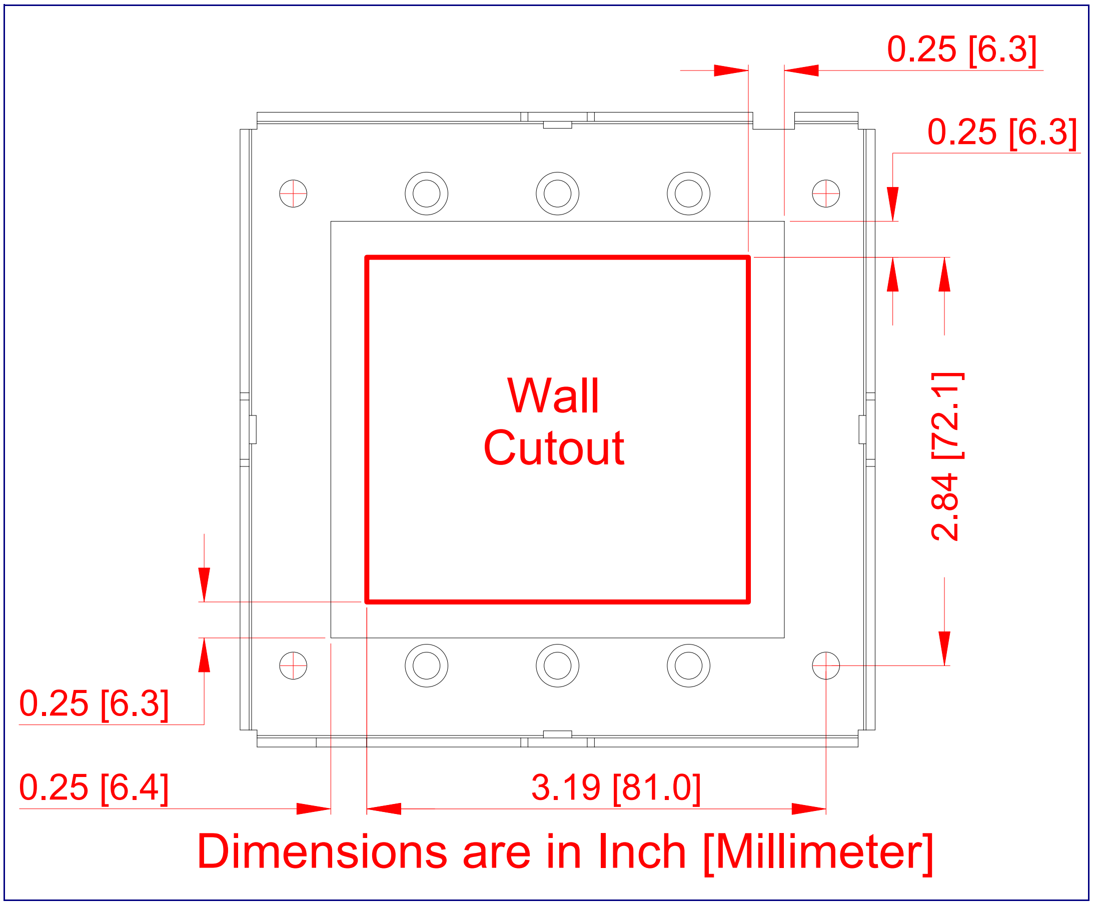


Figure A-4 shows the recommended wall cutout dimensions.

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://support.cyberdata.net/

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

Phone: (831) 373-2601, 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://support.cyberdata.net/

C.4 Warranty and RMA Information

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

http://support.cyberdata.net/

Index