

# *VoIP V3 Paging Server Operations Guide*

*SIP Compliant  
Part #011146*

Document Part #9304270  
for Firmware Version 7.2.0

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

---

**Operations Guide 930427O**  
**SIP Compliant 011146**

**COPYRIGHT NOTICE:**

© 2015, CyberData Corporation, ALL RIGHTS RESERVED.

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

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

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

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

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



**Technical Support**

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

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

Email: [support@cyberdata.net](mailto:support@cyberdata.net)

Fax: (831) 373-4193

Company and product information is at [www.cyberdata.net](http://www.cyberdata.net).

---

## Revision Information

Revision 930427O, which corresponds to firmware version 7.2.0, was released on May 27, 2015, and has the following changes:

- Updates [Section 1.2, "Product features"](#)
- Adds [Section 2.3.1, "Ground Connection"](#)
- Adds [Section 2.3.2, "Line In"](#)
- Adds [Section 2.3.3, "Line Out"](#)
- Adds [Section 2.3.4, "Page Port Output Connections"](#)
- Updates [Figure 2-3, "Connection Options"](#)

---



## Browsers Supported

The following browsers have been tested against firmware version 7.2.0:

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

---

## Pictorial Alert Icons

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

---

## 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.

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

---

## Abbreviations and Terms

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

# Contents

---

|   |              |
|---|--------------|
| <b>Chapter 1 Product Overview</b>   | <b>1</b>     |
| 1.1 How to Identify This Product .....  | 2            |
| 1.2 Product features .....  | 3            |
| 1.3 Product Specifications .....  | 4            |
| <br><b>Chapter 2 Setting Up the V3 Paging Server</b>                                | <br><b>5</b> |
| 2.1 Parts List .....  | 5            |
| 2.2 Typical Installation .....  | 6            |
| 2.3 Connecting the V3 Paging Server .....   | 7            |
| 2.3.1 Ground Connection .....   | 7            |
| 2.3.2 Line In .....   | 7            |
| 2.3.3 Line Out .....  | 7            |
| 2.3.4 Page Port Output Connections .....  | 8            |
| Pin 1 and 2—Fault Sense Input (Common/Sense) .....                                  | 8            |
| Pin 3, 4, and 5—Positive/Negative 600-Ohm Audio Output/Audio Ground Reference ..... | 8            |
| Pin 6 and 7—Relay Contact (Common/Normally Open) .....                              | 8            |
| 2.3.5 Removable Interface Connector .....   | 9            |
| 2.3.6 Connect to the Power Source .....   | 10           |
| Poe .....   | 10           |
| Non-Poe .....   | 10           |
| Chassis Ground .....  | 10           |
| 2.3.7 Connect to the Network .....  | 11           |
| 2.3.8 Confirm that the V3 Paging Server is Up and Running .....                     | 12           |
| Confirm Power on, Network Connectivity, and Connection Speed .....                  | 12           |
| Verify Network Activity .....   | 12           |
| 2.3.9 Announcing the IP Address .....   | 13           |
| 2.3.10 Restore the Factory Default Settings .....                                   | 13           |
| 2.4 Configuring the V3 Paging Server .....  | 14           |
| 2.4.1 Gather the Required Configuration Information .....                           | 14           |
| Static or DHCP Addressing? .....  | 14           |
| Username and Password for Configuration GUI .....                                   | 14           |
| SIP Settings .....  | 14           |
| 2.4.2 V3 Paging Server Web Page Navigation .....                                    | 15           |
| 2.4.3 Log in to the Configuration GUI .....   | 16           |
| 2.4.4 Configure the Device Parameters .....   | 20           |
| Polycom Paging .....  | 22           |
| 2.4.5 Configure the Network Parameters .....  | 24           |
| 2.4.6 Configure the SIP Parameters .....  | 27           |
| Point-to-Point Configuration .....  | 30           |
| 2.4.7 Configure the Night Ringer Parameters .....                                   | 31           |
| 2.4.8 Configure the Fault Detection Parameters .....                                | 33           |
| 2.4.9 Configure the Paging Groups (PGROUPS) Parameters .....                        | 35           |
| 2.4.10 Operating the Paging Server .....  | 44           |
| DTMF Bypassed .....   | 44           |
| DTMF Not Bypassed .....   | 44           |
| 2.4.11 Configure the Audio Parameters .....   | 45           |
| User-created Audio Files .....  | 49           |
| 2.4.12 Configure the Event Parameters .....   | 52           |
| Example Packets for Events .....  | 54           |
| 2.4.13 Configure the Autoprovisioning Parameters .....                              | 57           |
| Autoprovisioning .....  | 59           |

|   |           |
|---|-----------|
| Sample dhcpd.conf .....   | 67        |
| Get Autoprovisioning Template Button .....                      | 68        |
| Time Zone Strings .....   | 69        |
| 2.5 Upgrading the Firmware .....                                | 72        |
| 2.5.1 Uploading the Firmware .....                              | 73        |
| Upgrade the Firmware .....                                      | 74        |
| 2.5.2 Reboot the V3 Paging Server .....                         | 75        |
| 2.6.1 Command Interface Post Commands .....                     | 76        |
| <br><b>Appendix A Setting Up a TFTP Server</b> .....            | <b>80</b> |
| A.1 Set up a TFTP Server .....                                  | 80        |
| A.1.1 In a LINUX Environment .....                              | 80        |
| A.1.2 In a Windows Environment .....                            | 80        |
| <br><b>Appendix B Troubleshooting/Technical Support</b> .....   | <b>81</b> |
| B.1 Frequently Asked Questions (FAQ) .....                      | 81        |
| B.2 Documentation .....   | 81        |
| B.3 Contact Information .....                                   | 82        |
| B.4 Warranty .....  | 83        |
| B.4.1 Warranty & RMA Returns within the United States .....     | 83        |
| B.4.2 Warranty & RMA Returns outside of the United States ..... | 83        |
| B.4.3 Spare in the Air Policy .....                             | 84        |
| B.4.4 Return and Restocking Policy .....                        | 84        |
| B.4.5 Warranty and RMA Returns Page .....                       | 84        |



# 1 Product Overview

---

The CyberData V3 VoIP Paging Server enables users through a single SIP phone extension, to access multiple zones for paging in a VoIP network and to connect to legacy analog overhead paging systems.

A second SIP extension can be configured as a night ringer playing a user-uploadable audio file.

The V3 Paging Server allows direct connection to legacy analog paging amplifiers that require a "Page Port" type of input that meets a balanced 600 Ohm 10Vpp signal or a 10k Ohm Hi-Z 2vpp signal. You can also take advantage of connections for a dry contact relay (page start output) and sense input (Fault Sense Input) for additional functionality.

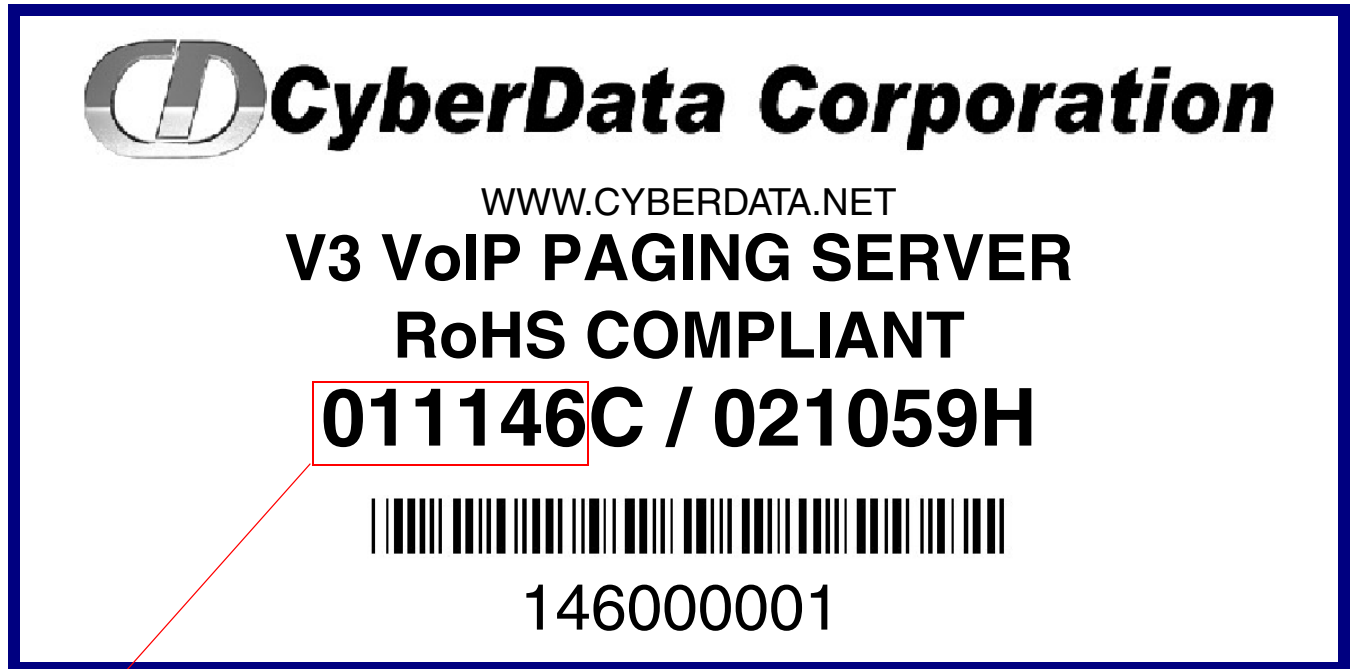
The easy-to-use, web-based configuration provides a graphical user interface to set up to 100 paging zones for IP paging with unique multicast address and port number combinations.

The V3 Paging Server connects via a single CAT 5 or 6 network cable to a standard PoE 802.3af compliant switch.

## 1.1 How to Identify This Product

To identify the VoIP V3 Paging Server, look for a model number label similar to the one shown in [Figure 1-1](#). The model number on the label should be **011146**.

Figure 1-1. Model Number Label



Model number

---

## 1.2 Product features

- SIP RFC 3261
- Two SIP endpoints (one for Night Ringer)
- Multicast output
- Polycom group paging
- DTMF control of zone selection (with optional security code per zone)
- RTP Version 2 Multicast and Unicast
- Delayed page support
- Line-In connection for background music multicasting
- Line-out connection to support analog Amps
- Audio Codecs
  - G.711 U-law
  - G.711 A-law
  - Speex
  - DTMF detection (via RFC 2833)
- Cisco SRST support
- 802.11Q VLAN support
- Ability to import and export configuration
- Autoprovisioning
- Added support for NTP server for time keeping
  - TFTP or HTTP
  - Update at certain times of day
  - Update after a certain amount of idle time
- HTTP command interface
- Outbound proxy support for night ringer
- Option to disable rport discovery
- DTMF tones can be played out of analog ports during a page
- User-configurable DTMF duration option
- Option to enable line-in audio to multicast on fault detection
- Remote amp fault sensor
- Web-based configuration and firmware upload
- User uploadable audio files
- PoE 802.3af enabled (Power-over-Ethernet)
- 19-inch rack mount option

## 1.3 Product Specifications

**Table 1-1. Product Specifications**

| <b>Specifications</b>     |                             |
|---------------------------|-----------------------------|
| Power Requirement         | PoE or 48V DC               |
| Connection Speed          | 10/100 Mbps                 |
| Protocol                  | SIP compliant               |
| Page Port Output          | Balanced 600 Ohm 5VPP       |
| Line In:                  |                             |
| Input Signal Amplitudes   | 2.0 VPP maximum             |
| Input Impedance           | 10k Ohm                     |
| Line Out:                 |                             |
| Output Signal Amplitudes  | 2.0 VPP maximum             |
| Output Level              | +2dBm nominal               |
| Total Harmonic Distortion | 0.5% maximum                |
| Output Impedance          | 10k Ohm                     |
| Part Number               | 011146                      |
| Dimensions                | 6.11" L x 4.05" W x 1.15" H |
| Weight                    | 1.2 pounds                  |



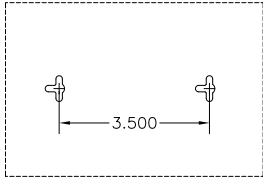

## 2 Setting Up the V3 Paging Server

The topics in this chapter provide information on setting up, configuring, and using the VoIP V3 Paging Server.

### 2.1 Parts List

The packaging for the V3 Paging Server includes the parts in [Table 2-2](#).

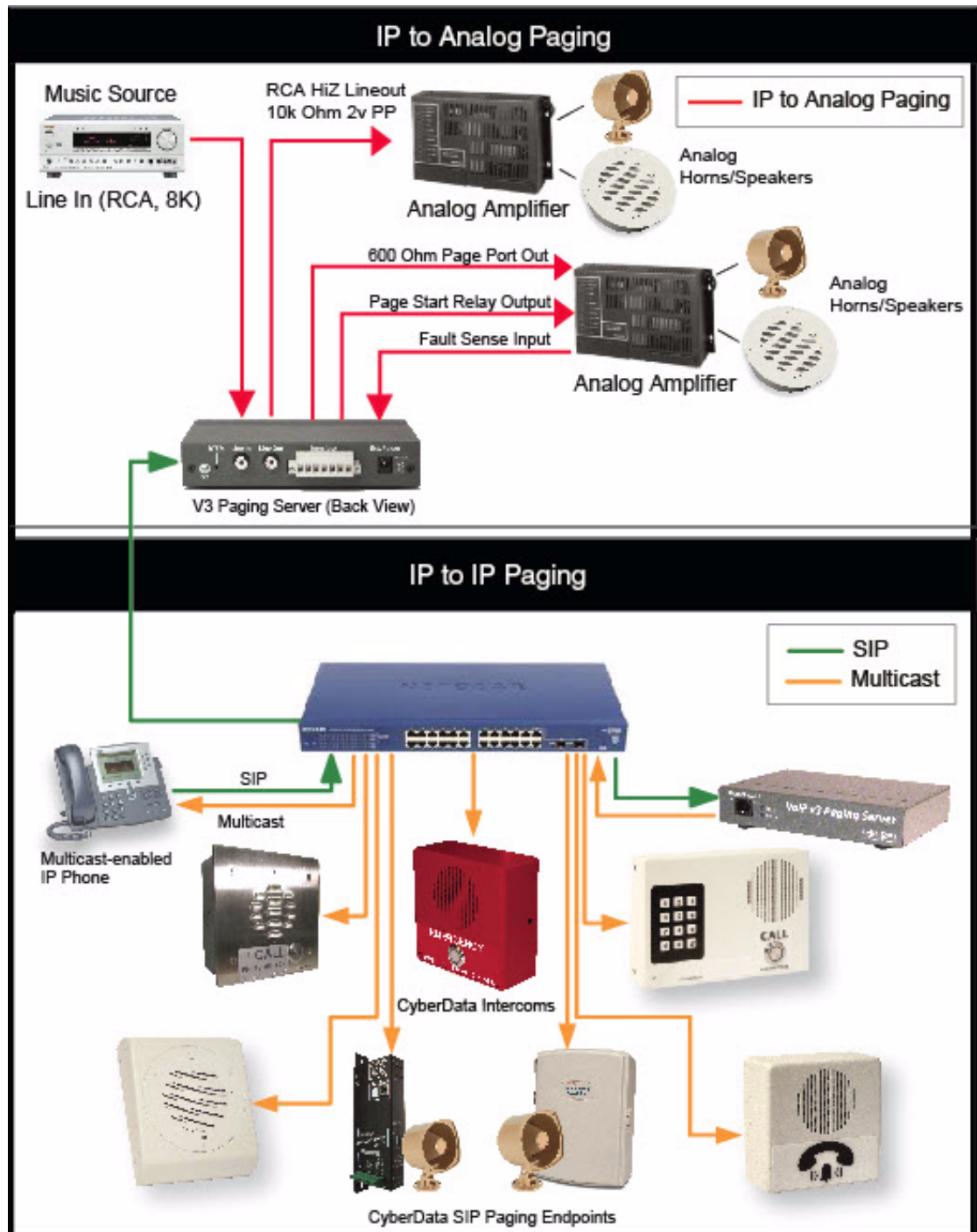
**Table 2-2. Parts List**

| Quantity | Part Name  | Illustration  |
|----------|--|---|
| 1        | V3 Paging Server   |    |
| 1        | Installation Quick Reference Guide   |   |
| 1        | Mounting Template (located on the last page of the <i>Installation Quick Reference</i> )                                       |  |
| 1        | Mounting Kit (part #070057A) which includes:<br>(2) #4-6 x 7/8" Mounting Anchors<br>(2) #4 x 1-1/4" Round Phillips Wood Screws |  |

## 2.2 Typical Installation

Figure 2-2 illustrates how the V3 Paging Server is normally installed as part of a paging system.

Figure 2-2. Typical Installation

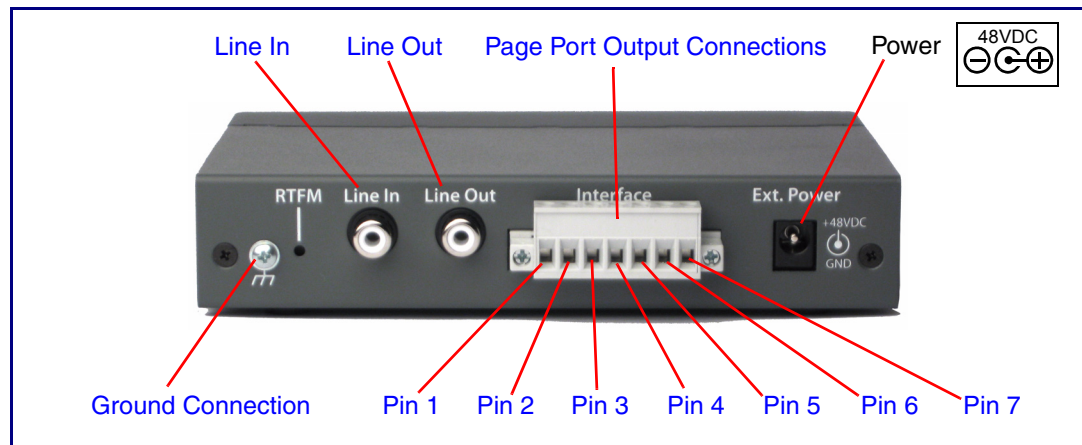


## 2.3 Connecting the V3 Paging Server

Before you connect the V3 Paging Server, be sure that you have received all of the parts described in [Section 2.1, "Parts List"](#).

See [Figure 2-3](#) for the connection options that are available for the V3 Paging Server.

**Figure 2-3. Connection Options**



### 2.3.1 Ground Connection

This connection allows you to connect the device to an electrical ground.

### 2.3.2 Line In

This RCA 10K Ohm Hi-Z input connection allows you to connect the device to The RCA line-out (10K Ohm Hi-Z) of an external audio amplifier. The level of this input can be controlled by the potentiometer located on the front of the device (see [Section 2.4.8, "Configure the Fault Detection Parameters"](#)).

### 2.3.3 Line Out

This RCA 10K Ohm Hi-Z output connection allows you to connect the device to The RCA line-in (10K Ohm Hi-Z) of an external audio amplifier.

## 2.3.4 Page Port Output Connections

**Table 2-1. Page Port Output Connections**

| Pin   | Description   |
|-------|---|
| Pin 1 | Fault Sense Input (Common). See <a href="#">Section 2.3.4.1, "Pin 1 and 2—Fault Sense Input (Common/Sense)"</a> .   |
| Pin 2 | Fault Sense Input (Sense). See <a href="#">Section 2.3.4.1, "Pin 1 and 2—Fault Sense Input (Common/Sense)"</a> .  |
| Pin 3 | Positive 600-Ohm Audio Output <sup>a</sup> . See <a href="#">Section 2.3.4.2, "Pin 3, 4, and 5—Positive/Negative 600-Ohm Audio Output/Audio Ground Reference"</a> . |
| Pin 4 | Negative 600-Ohm Audio Output <sup>a</sup> . See <a href="#">Section 2.3.4.2, "Pin 3, 4, and 5—Positive/Negative 600-Ohm Audio Output/Audio Ground Reference"</a> . |
| Pin 5 | Audio Ground Reference. See <a href="#">Section 2.3.4.2, "Pin 3, 4, and 5—Positive/Negative 600-Ohm Audio Output/Audio Ground Reference"</a> .                      |
| Pin 6 | Relay Contact - Common <sup>b</sup> . See <a href="#">Section 2.3.4.3, "Pin 6 and 7—Relay Contact (Common/Normally Open)"</a> .                                     |
| Pin 7 | Relay Contact - Normally Open <sup>b</sup> . See <a href="#">Section 2.3.4.3, "Pin 6 and 7—Relay Contact (Common/Normally Open)"</a> .                              |

a. The 600-Ohm audio output of the page port is also suited for interfaces with lower input impedances.

b. 1 Amp at 30 VDC for continuous loads

### 2.3.4.1 Pin 1 and 2—Fault Sense Input (Common/Sense)

This input was designed as a method of monitoring an external amplifier that is equipped with a fault sense relay.

When enabled via the web interface ([Section 2.4.8, "Configure the Fault Detection Parameters"](#)), this input (when closed) will play a user uploadable audio file out of the line-out connection and/or place a SIP call to a pre-determined extension and play that file.

### 2.3.4.2 Pin 3, 4, and 5—Positive/Negative 600-Ohm Audio Output/Audio Ground Reference

This output allows direct connection to paging amplifiers requiring a "Page Port" type input that meets a balanced 600 Ohm 5VPP signal.

### 2.3.4.3 Pin 6 and 7—Relay Contact (Common/Normally Open)

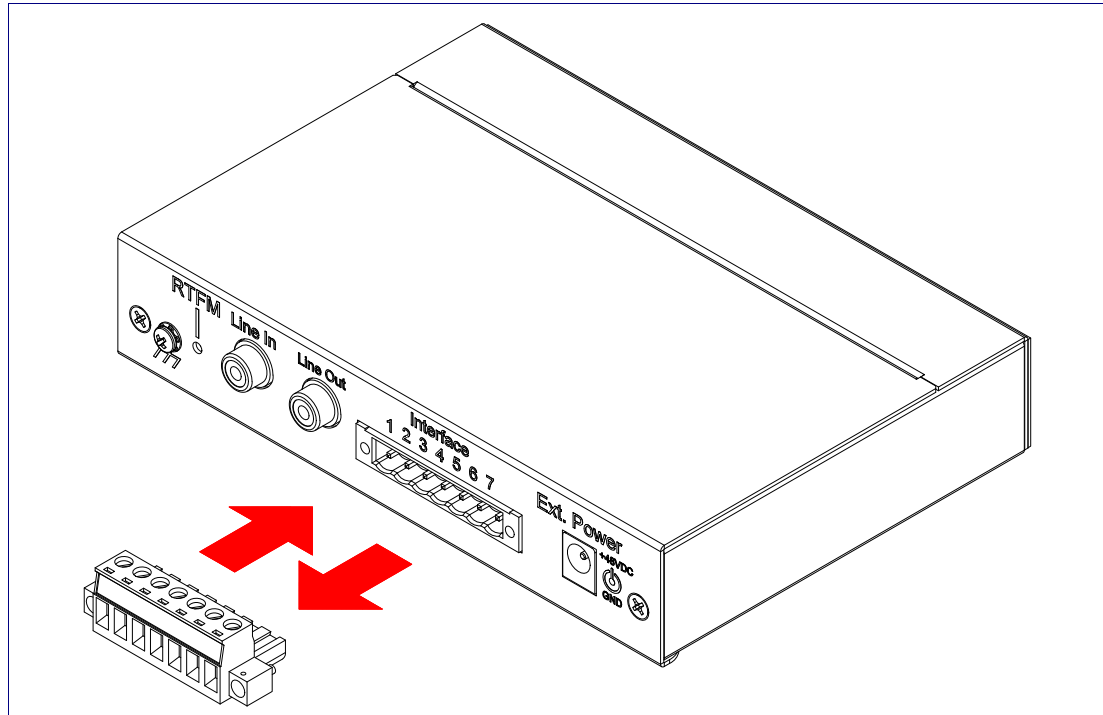
When enabled on the web interface ([Section 2.4.4, "Configure the Device Parameters"](#)), every time an audio file is played out of the local line-out or 600 Ohm output, the relay will close, thereby enabling amplifiers with a remote turn-on capability to become active.



## 2.3.5 Removable Interface Connector

Figure 2-4 shows the interface connector that is removable on the V3 Paging Server.

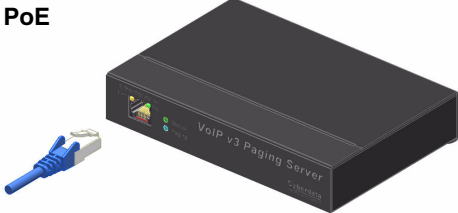


**Figure 2-4. Removable Interface Connector**



## 2.3.6 Connect to the Power Source

To use PoE, plug a Cat 5 Ethernet cable from the V3 Paging Server **Ethernet** port to your network. As an alternative to PoE, you can plug one end of a +48V DC power supply into the Paging Server, and plug the other end into a receptacle. If required, connect the earth grounding wire to the chassis ground on the back of the unit. See [Figure 2-5](#).

**Figure 2-5. Connecting to the Power Source**

|  |  |
|--|--|
| <p><b>PoE</b></p>                                     | <p>To set up the V3 Paging Server, connect the device to your network:</p> <p><b>Poe</b></p> <ul style="list-style-type: none"> <li>For <b>PoE</b>, plug one end of an 802.3af Ethernet cable into the V3 Paging Server Ethernet port. Plug the other end of the Ethernet cable into your network. See the figure on the left.</li> </ul>              |
| <p><b>Non PoE (with 48 VDC power supply)</b></p>     | <p><b>Non-Poe</b></p> <ul style="list-style-type: none"> <li>For <b>Non-PoE</b>, connect the V3 Paging Server to a <b>48VDC power supply</b>. See the figure on the left.</li> <li><b>Note:</b> Do not use both PoE and external power.</li> <li>Alternatively, you can use our part# 010867 PoE Power Injector as a cost-effective option.</li> </ul> |
| <p><b>Chassis Ground</b></p>  <p>Chassis Ground</p> | <p><b>Chassis Ground</b></p> <ul style="list-style-type: none"> <li>If required, connect the earth grounding wire to the <b>Chassis Ground</b>. See the figure on the left.</li> </ul>   |

---

## 2.3.7 Connect to the Network

Plug one end of a standard Ethernet cable into the Paging Server **Ethernet** port. Plug the other end into your network.

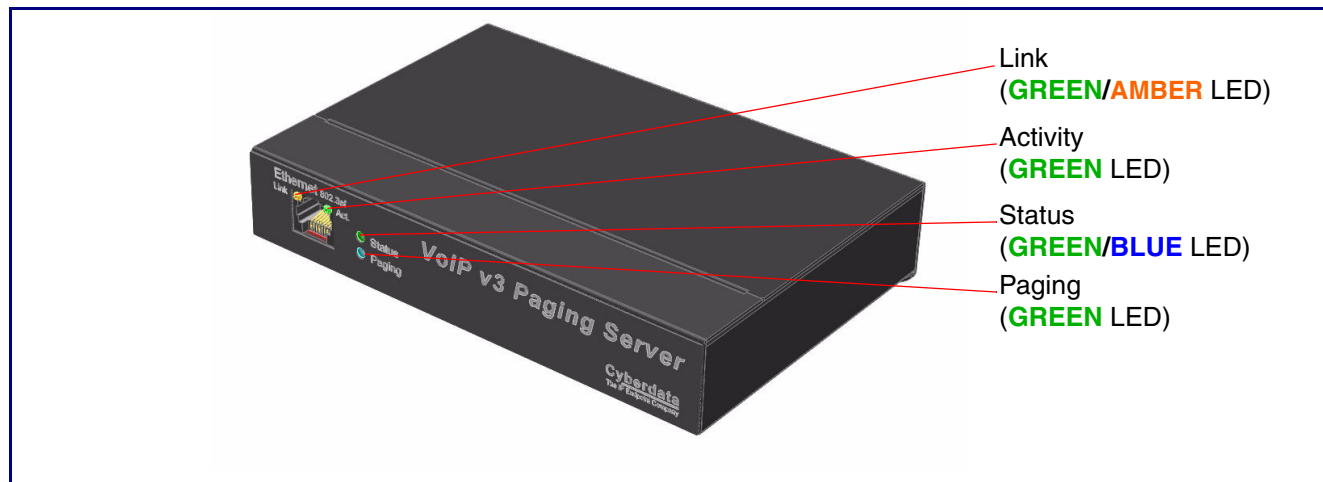
**Figure 2-6. Connecting to the Network**



## 2.3.8 Confirm that the V3 Paging Server is Up and Running

The LEDs on the front of the V3 Paging Server verify the unit's operations.

**Figure 2-7. Paging Server LEDs**



### 2.3.8.1 Confirm Power on, Network Connectivity, and Connection Speed

When you plug in the Ethernet cable or power supply:

- The **GREEN/BLUE Status** LED and the **GREEN Paging** LED both blink at a rate of 10 times per second during the initial network setup.
- The round, **GREEN/BLUE Status** LED on the front of the V3 Paging Server comes on indicating that the power is on. Once the device has been initialized, this LED blinks at one second intervals.
- The square, **GREEN/AMBER Link** LED above the Ethernet port indicates that the network connection has been established. The Link LED changes color to confirm the auto-negotiated connection speed:
  - The Link LED is **GREEN** at 10 Mbps.
  - The Link LED is **AMBER** at 100 Mbps.
- The **GREEN Paging** LED comes on after the device is booted and initialized. This LED blinks when a page is in progress. You can disable **Beep on Initialization** on the **Device Configuration** page.

### 2.3.8.2 Verify Network Activity

The square, **GREEN Activity** LED blinks when there is network traffic.

## 2.3.9 Announcing the IP Address

To announce the IP address for the V3 Paging Server, briefly press and then quickly release the RTFM switch. See [Figure 2-8](#).

**Figure 2-8. RTFM Switch**



## 2.3.10 Restore the Factory Default Settings

The V3 Paging Server is delivered with factory set default values for the parameters in [Table 2-3](#). In addition, the settings for various UI web pages (such as the [Device Configuration Page](#), [SIP Configuration Page](#), etc.) are delivered with the factory default settings and can be restored to these default settings when you use the RTFM switch. However, uploaded audio files are not restored to the factory default settings when you use the RTFM switch.

Use the RTFM switch (see [Figure 2-8](#)) on the back of the unit to restore these parameters to the factory default settings.

**Note** When you perform this procedure, the factory default settings are restored. The default parameters for access are shown in [Table 2-3](#).

**Table 2-3. Factory Default Settings**

| Parameter                    | Factory Default Setting |
|------------------------------|-------------------------|
| IP Addressing                | DHCP                    |
| IP Address <sup>a</sup>      | 10.10.10.10             |
| Web Access Username          | admin                   |
| Web Access Password          | admin                   |
| Subnet Mask <sup>a</sup>     | 255.0.0.0               |
| Default Gateway <sup>a</sup> | 10.0.0.1                |

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

To restore these parameters to the factory default settings:

1. Press and hold the RTFM switch until the status and paging lights come on.
2. Continue to press the RTFM switch until after you see the indicator lights go off and you hear the “restoring defaults” announcement.
3. Release the RTFM switch.
4. The V3 Paging Server settings are restored to the factory defaults.

---

## 2.4 Configuring the V3 Paging Server

Use this section to configure the VoIP paging server.

---

### 2.4.1 Gather the Required Configuration Information

Have the following information available before you configure the V3 Paging Server.

#### 2.4.1.1 Static or DHCP Addressing?

Know whether your system uses static or dynamic (DHCP) IP addressing. If it uses static addressing, you also need to know the values to assign to the following V3 Paging Server parameters:

- IP Address
- Subnet Mask
- Default Gateway

#### 2.4.1.2 Username and Password for Configuration GUI

Determine the Username and Password that will replace the defaults after you initially log in to the configuration GUI.

- The Username is case-sensitive, and must be from four to 25 alphanumeric characters long.
- The Password is case-sensitive, and must be from four to 20 alphanumeric characters long.

#### 2.4.1.3 SIP Settings



To configure the SIP parameters, determine whether you want to register with the server. If you do, determine the number of minutes the registration lease remains valid, and whether you want to automatically unregister when you reboot. To configure the SIP parameters, you also need to determine the values for these parameters:

- SIP Server IP Address
- Remote and Local SIP Port Numbers
- SIP User ID, and Authenticate ID and Password for this User ID

## 2.4.2 V3 Paging Server Web Page Navigation

Table 2-4 shows the navigation buttons that you will see on every V3 Paging Server web page.

**Table 2-4. V3 Paging Amplifier Web Page Navigation**

| Web Page Item   | Description  |
|---|--|
|    | Link to the <b>Home</b> page.                              |
|    | Link to the <b>Device Configuration</b> page.              |
|    | Link to the <b>Networking</b> page.                        |
|    | Link to go to the <b>SIP Configuration</b> page.           |
|    | Link to go to the <b>Nightringer</b> page.                 |
|    | Link to go to the <b>Fault Detection</b> page.             |
|  | Link to go to the <b>Paging Groups Configuration</b> page. |
|  | Link to the <b>Audio Configuration</b> page.               |
|  | Link to the <b>Event Configuration</b> page.               |
|  | Link to the <b>Autoprovisioning Configuration</b> page.    |
|  | Link to the <b>Upgrade Firmware</b> page.                  |

---

## 2.4.3 Log in to the Configuration GUI

1. Open your browser to the V3 Paging Server 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 V3 Paging Server.

**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\\_utility.html](http://www.cyberdata.net/support/voip/discovery_utility.html)

The unit 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.

**Note** To work with the V3 Paging Server configuration *after* the initial configuration, log in using the IP address you assign to the device. [Section 2.4.5, "Configure the Network Parameters"](#) provides instructions for entering the IP address.

2. When prompted, use the following default **Username** and **Password** to open the configuration Home page:

Username: **admin**

Password: **admin**

Change the  
Default Username  
and Password

To change the default Web access Username and Password:

1. Enter the new Username from four to 25 alphanumeric characters in the **Change Username** field. The Username is case-sensitive.
2. Enter the new Password from four to 20 alphanumeric characters in the **Change Password** field. The Password is case-sensitive.
3. Enter the new password again in the **Re-enter New Password** field.

Click **Save Settings**.



Figure 2-9. Home Page

The screenshot displays the 'CyberData v3 Paging Server' configuration interface. On the left is a vertical sidebar with buttons for 'Home', 'Device Config', 'Networking', 'SIP Config', 'Nightringer', 'Fault Detection', 'PGROUPs Config', 'Audio Config', 'Event Config', 'Autoprovisioning', and 'Update Firmware'. The main content area is divided into three sections: 'Device Settings', 'Current Settings', and 'Import/Export Settings'. The 'Device Settings' section includes fields for 'Device Name' (CyberData Paging Server), 'Change Username' (admin), 'Change Password', and 'Re-enter Password'. The 'Current Settings' section lists various parameters: Serial Number (146001452), Mac Address (00:20:f7:02:e5:8e), Firmware Version (v7.2.0), Part Number (011146), IP Addressing (dhcp), IP Address (10.10.0.105), Subnet Mask (255.0.0.0), Default Gateway (10.0.0.1), DNS Server 1 (10.0.0.252), DNS Server 2, SIP Mode (enabled), Event Reporting (disabled), Nightringer (disabled), and three SIP servers (Primary, Backup 1, Backup 2), all of which are marked as '(NOT Registered with SIP Server)'. The 'Import/Export Settings' section contains a 'Please specify a configuration file\*' label, a 'Browse...' button, a 'No file selected.' status, and buttons for 'Import Configuration' and 'Export Configuration'. At the bottom, a note states '\* You need to reboot for changes to take effect', followed by 'Save' and 'Reboot' buttons.

## CyberData v3 Paging Server

[Home](#)  
[Device Config](#)  
[Networking](#)  
[SIP Config](#)  
[Nightringer](#)  
[Fault Detection](#)  
[PGROUPs Config](#)  
[Audio Config](#)  
[Event Config](#)  
[Autoprovisioning](#)  
[Update Firmware](#)

**Device Settings**  
Device Name:   
Change Username:   
Change Password:   
Re-enter Password:


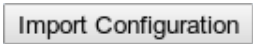
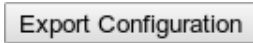

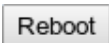
**Current Settings**  
Serial Number: 146001452  
Mac Address: 00:20:f7:02:e5:8e  
Firmware Version: v7.2.0  
Part Number: 011146  
IP Addressing: dhcp  
IP Address: 10.10.0.105  
Subnet Mask: 255.0.0.0  
Default Gateway: 10.0.0.1  
DNS Server 1: 10.0.0.252  
DNS Server 2:  
SIP Mode is: enabled  
Event 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)

**Import/Export Settings**  
Please specify a configuration file\*:  
 No file selected.

\* You need to reboot for changes to take effect

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

**Table 2-5. Home Page Overview**

| Web Page Item   | Description   |
|---|---|
| <b>Device Settings</b>  |   |
| Device Name   | Shows the device name (25 character limit).   |
| Change Username   | Type in this field to change the username (25 character limit).   |
| Change Password   | Type in this field to change the password (20 character limit).   |
| Re-enter Password   | Type the password again in this field to confirm the new password (20 character limit).   |
| <b>Current Settings</b>   |   |
| Serial Number   | Shows the serial number of the device.  |
| Part Number   | Shows the part number of the device.  |
| Mac Address   | Shows the Mac address of the device.  |
| Firmware Version  | Shows the current firmware version.   |
| IP Addressing   | Shows the current IP addressing setting ( <b>DHCP</b> or <b>Static</b> ).   |
| 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 Mode is   | Shows the current status of the SIP Mode.   |
| Event Reporting is  | Shows the current status of the Event Reporting.  |
| Nightring is  | Shows the current status of the Nightringer.  |
| 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.  |
| <b>Import/Export Settings</b>   | The user can export and edit the device's configuration (in XML format), and then reload it to a device (or devices) instead of making changes through the web interface. |
|  | Press the <b>Browse</b> button to select a configuration file to import.  |
|  | Press the <b>Import Configuration</b> button to save a board configuration to the board.<br><b>Note:</b> The board will have to be reset before changes will take effect. |
|  | Press the <b>Export Configuration</b> button to download the current board configuration.   |
|  | Click on the <b>Save</b> button to save your configuration settings.<br><b>Note:</b> You need to reboot for changes to take effect.                                       |
|  | Click on the <b>Reboot</b> button to reboot the system.   |

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

At this point you can:

- Review the V3 Paging Server's **Current Settings**. Use the RTFM switch to restore the factory default settings. See [Section 2.3.10, "Restore the Factory Default Settings"](#).
- Configure the device parameters. Click on the **Device Config** button and see [Section 2.4.4, "Configure the Device Parameters"](#).
- Configure the network parameters. Click on the **Networking** button and refer to [Section 2.4.5, "Configure the Network Parameters"](#) for instructions.
- Configure the SIP parameters. Click on the **SIP Config** button and see [Section 2.4.6, "Configure the SIP Parameters"](#).
- Configure the Night Ringer parameters. Click on the **Nightringer** button and see [Section 2.4.7, "Configure the Night Ringer Parameters"](#).
- Configure the fault detection parameters. Click on the **Fault Detection** button and see [Section 2.4.8, "Configure the Fault Detection Parameters"](#).
- Configure the PGROUPS parameters. Click on the **PGROUPS Config** button and see [Section 2.4.9, "Configure the Paging Groups \(PGROUPS\) Parameters"](#) for instructions.
- Configure the audio parameters. Click on the **Audio Config** button and see [Section 2.4.11, "Configure the Audio Parameters"](#) for instructions.
- Configure the event parameters. Click on the **Event Config** button and see [Section 2.4.12, "Configure the Event Parameters"](#) for instructions.
- Configure the autoprovisioning parameters. Click on the **Autoprovisioning** button and see [Section 2.4.13, "Configure the Autoprovisioning Parameters"](#) for instructions.

**Note** Click on the **Update Firmware** button any time you need to upload new versions of the firmware. See [Section 2.5, "Upgrading the Firmware"](#) for instructions.

## 2.4.4 Configure the Device Parameters

Miscellaneous device settings such as the page prompt and analog options are configured on this page. In addition, you may also enable Polycom Paging to page Polycom IP phones using their proprietary Polycom Paging protocol.

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

**Figure 2-10. Device Configuration Page**

**CyberData v3 Paging Server**

**Device Configuration**

Miscellaneous Settings

Beep on Initialization: ☐

Beep on page: ☒

Enable line-in to line-out loopback\*\*\*: ☐

Enable line-in to multicast\*\*\*: ☐

Multicast Address: 224.1.2.3

Multicast Port: 2000

Detect Line-in Silence: ☐

Enable relay on local audio: ☐

DTMF duration (milliseconds): 500

Enable Polycom Paging on Multicast\*\*\*\*: ☐

Polycom Transmit Channel: 1

\* You need to reboot for changes to take effect  
 \*\* "Test Multicast" will send a 5 second ULAW multicast stream to 234.2.1.200:2200  
 \*\*\* Cannot be combined with "Play Line-in Audio via Multicast (Fault Detection)"  
 \*\*\*\*Enabling Polycom Paging will result in a standard RTP multicast being sent to the specified address and port and a Polycom PTT Page multicast being sent to the specified address and port+1



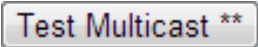


Save Test Audio Test Multicast \*\* Test Relay Reboot

2. On the **Device Configuration** page, you may enter values for the parameters indicated in [Table 2-6](#).

**Table 2-6. Device Configuration Parameters**

| Web Page Item                       | Description  |
|-------------------------------------|--|
| <b>Miscellaneous Settings</b>       |  |
| Beep on Initialization              | When selected, you will hear a beep when the device initializes.   |
| Beep on Page                        | When selected, the device will play a beep before a page is sent to the analog ports when "Lineout" is enabled on a paging group (works for both buffered and live pages).   |
| Enable Line In to Line Out Loopback | When selected, audio is sent from the line -in to the line-out output.<br><b>Note:</b> Cannot be combined with <b>Play Line-in Audio via Multicast (Fault Detection)</b>   |
| Enable Line-In to Multicast         | When selected, the line-in audio will be multicast to the address and port specified on the web page.<br><b>Note:</b> Cannot be combined with <b>Play Line-in Audio via Multicast (Fault Detection)</b><br><b>Note:</b> Ideally, the specified address and port will match that of a low priority MGROUP (such as background music) on the speakers or paging amplifiers.<br><b>Note:</b> When line-in to multicast is selected, do not set that multicast address and port to the same multicast address and port that is used by one of your PGROUPS. Otherwise, when you call the PGROUP, the Paging Server will be unable to send the new audio stream because the port will already be in use by the line-in to multicast stream. |
| Multicast Address                   | Type the Multicast address.  |
| Multicast Port                      | Type the Multicast port number.  |
| Detect Line-in Silence              | When selected, the device will detect when silence occurs in the line-in port. Also, the device will not relay line-in audio to multicast if this option is enabled and there is silence on the line-in port.<br><b>Note:</b> This option requires a 011146C/021059G/991034C or newer Paging Server.   |
| Enable Relay on Local Audio         | When selected, the relay will be closed any time that audio is played out of the line-out/page port. This setting is for legacy analog amplifiers that are often connected to the page port. Analog amplifiers will often have a noticeable hum if they are turned on while there is no audio being played. The relay closure causes these amplifiers to turn on only when audio is sent to them.  |
| DTMF duration (milliseconds)        | The duration of DTMF tones played out the analog ports. (in milliseconds)  |

**Table 2-6. Device Configuration Parameters (continued)**

| Web Page Item   | Description  |
|---|--|
| Enable Polycom Paging on Multicast  | <p>When selected, a Polycom Group Paging multicast will be sent to the specified Paging Group multicast address and [port number + 1]. The Polycom Group Paging multicast will be transmitted as a second, separate multicast transmission in addition to the standard multicast transmitted to the specified multicast address and even numbered port for the desired Paging Group (PGROUP). Be sure to configure an odd numbered port for the Polycom Paging/PTT Configuration setting on the Polycom phones. CyberData PGROUPS configuration settings are located on the <a href="#">PGROUPS Configuration Page</a>. The Polycom Paging/PTT Configuration setting for the multicast IP address on the Polycom phones must match the Paging Group multicast IP address on the Paging Server's <a href="#">PGROUPS Configuration Page</a>.</p> <p><b>Note: Enabling Polycom Paging</b> will result in a standard RTP multicast being sent to the specified address and port and a Polycom PTT Page multicast being sent to the specified address and [port number + 1].</p> |
| Polycom Transmit Channel  | Specify the Polycom channel/group number. Group Numbers 1 through 25 are supported. The Polycom phones must subscribe to this channel/group number to receive pages from the Paging Server.  |
|    | <p>Click on the <b>Save</b> button to save your configuration settings.</p> <p><b>Note:</b> You need to reboot for changes to take effect.</p>   |
|    | When the <b>Test Audio</b> button is pressed, you will hear a voice message for testing the device audio quality and volume.   |
|  | <p>When the <b>Test Multicast</b> button is pressed, the Paging Server will send a five second canned ULAW message to a predetermined multicast address and port.</p> <p><b>Note: Test Multicast</b> will send a 5 second ULAW multicast stream to 234.2.1.200:2200.</p>   |
|  | Click on the <b>Test Relay</b> button to do a relay test.  |
|  | Click on the <b>Reboot</b> button to reboot the system.  |

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

#### 2.4.4.1 Polycom Paging

The Polycom Paging feature is supported on Polycom IP phones using UC Software 4.0.0 and higher. The Polycom paging feature operates in two modes: Push-to-Talk (PTT) and Group Paging. Only Group Paging mode pages are supported by the Paging Server.

Polycom phones use the same multicast IP address and port number for both PTT and Group Paging multicasts. Make sure to note the Polycom multicast IP address and port number before configuring the CyberData V3 Paging Server. Polycom phones use a default multicast IP address of 224.0.1.116 and odd-numbered port 5001.

While the same multicast IP address and port number is used for all Polycom pages in both modes, Polycom uses numbered "groups" or "channels" to differentiate between each paging group. Each "group" or "channel" is numbered 1 through 25.

The Paging Server can transmit to Group Paging groups 1 through 25 only for one-way audio pages. The transmit channel is configurable. The Polycom phones must subscribe to this channel in order to receive one-way audio pages from the Paging Server.

When configuring Polycom phones for their Group Paging feature, be sure the following settings are configured:

- Payload Size = 20 ms (milliseconds)
- Codec = G.711Mu

The Polycom Group Paging multicast transmitted by the Paging Server is G.711Mu encoded with a payload size of 20 ms.

It is imperative to note the Paging Server assumes the Polycom phones will use an odd-numbered port. Since it is not possible to configure the V3 Paging Server to transmit multicasts on odd-numbered ports (which maintains conformance with RFC 1889), it is necessary to use the next lower even port number when specifying the Polycom multicast IP address and port number on the [PGROUPS Configuration Page](#). Using the Polycom default port 5001 will require you to configure the Paging Server to transmit on the next lower even port 5000.

Thus, configuring the Paging Server for Polycom Paging is a two-step process:

1. Enable Polycom Paging on the Paging Server by checking the box to [Enable Polycom Paging on Multicast](#) on the [Device Configuration Page](#).
2. Specify the Polycom IP address and use the next lower even port number for the desired paging group on the [PGROUPS Configuration Page](#).
3. Save and reboot to store changes.



## 2.4.5 Configure the Network Parameters

Configuring the network parameters enables your network to recognize the V3 Paging Server and communicate with it. Click the **Networking** button on the **Home** page to open the **Network Configuration** page.

Figure 2-11. Network Configuration Page

**CyberData v3 Paging Server**

**Home** **Device Config** **Networking** **SIP Config** **Nightringer** **Fault Detection** **PGROUPs Config** **Audio Config** **Event Config** **Autoprovisioning** **Update Firmware**

**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

VLAN ID (0-4095): 0

VLAN Priority (0-7): 0

DHCP Timeout

DHCP Timeout in seconds\*: 60

\* A value of -1 will retry forever

Current Network Settings

IP Address: 10.10.1.66

Subnet Mask: 255.0.0.0

Default Gateway: 10.0.0.1

DNS Server 1: 10.0.0.1

DNS Server 2:



\* You need to reboot for changes to take effect

Save Reboot



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

**Table 2-7. Network Configuration Parameters**

| Web Page Item   | Description   |
|---|---|
| <b>Stored Network Settings</b>  | Shows the settings stored in non-volatile memory.   |
| IP Addressing   | Select either <b>DHCP IP Addressing</b> or <b>Static IP Addressing</b> by marking the appropriate radio button. If you select <b>Static</b> , configure the remaining parameters indicated in <a href="#">Table 2-7</a> . If you select <b>DHCP</b> , go to <a href="#">Step Note</a> .   |
| 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.   |
| VLAN ID (0-4095)  | Enter the VLAN ID number.<br><br><b>Note:</b> The device supports 802.11Q 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)   | Enter the VLAN priority number.   |
| <b>DHCP Timeout</b>   |   |
| 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.<br><br><b>Note:</b> A value of <b>-1</b> will cause the device to retry indefinitely and a value of <b>0</b> will cause the device to reset to a default of 60 seconds. |
| <b>Current Network Settings</b>   | 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 on the <b>Save</b> button to save your configuration settings.<br><br><b>Note:</b> You need to reboot for changes to take effect.   |
|  | Click on the <b>Reboot</b> button to reboot the system.   |

On this page:

1. Specify whether you use **Static** or **DHCP IP Addressing** by marking the appropriate radio button. If you select **Static IP Addressing**, go to [Step 2](#).
2. For Static IP Addressing, also enter values for the following parameters:
  - The V3 Paging Server's **IP Address**: The V3 Paging Server is delivered with a factory default IP address. Change the default address to the correct IP address for your system.
  - The **Subnet Mask**.
  - The **Default Gateway**.

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

## 2.4.6 Configure the SIP Parameters

The SIP parameters enable the V3 Paging Server to contact and register with the SIP server. On the Home page, click **SIP Config** to open the **SIP Configuration** page.

Figure 2-12. SIP Configuration Page

**CyberData v3 Paging Server**

**SIP Configuration**

Enable SIP operation: ☒ (NOT Registered with SIP Server)

**SIP Settings**

SIP Server: 10.0.0.253

Backup SIP Server 1:

Backup SIP Server 2:

Use Cisco SRST: ☐

Remote SIP Port: 5060

Local SIP Port: 5060

Outbound Proxy:

Outbound Proxy Port: 0

SIP User ID: 199

Authenticate ID: 199

Authenticate Password: ••••••

Register with a SIP Server: ☒

Re-registration Interval (in seconds): 360

Unregister on Reboot: ☐

Disable rport Discovery: ☐

Buffer SIP Calls: ☐

**Call disconnection**

Terminate call after delay (in seconds): 0

Note: A value of 0 will disable this function

**Misc Settings**

RTP Port (even): 10500

\* You need to reboot for changes to take effect



Save Reboot

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

**Table 2-8. SIP Configuration Parameters**

| Web Page Item                              | Description   |
|--|---|
| Enable SIP Operation                       | Enables or disables SIP operation.  |
| <b>SIP Settings</b>                        |   |
| SIP Server                                 | Type the SIP server represented as either a numeric IP address in dotted decimal notation or the fully qualified host name (255 character limit [FQDN]).  |
| Backup SIP Server 1<br>Backup SIP Server 2 | <ul style="list-style-type: none"> <li>If all of the <b>SIP Server</b> and <b>Backup SIP Server</b> fields are populated, the device will attempt to stay registered with all three servers all of the time. You can leave the <b>Backup SIP Server 1</b> and <b>Backup SIP Server 2</b> fields blank if they are not needed.</li> <li>In the event of a registration failure on the <b>Primary SIP Server</b>, the device will use the next highest priority server for outbound calls (<b>Backup SIP Server 1</b>). If <b>Backup SIP Server 1</b> fails, the device will use <b>Backup SIP Server 2</b>.</li> <li>If a higher priority SIP Server comes back online, the device will switch back to this server.</li> </ul> |
| Use Cisco SRST                             | When selected, the backup servers are handled according to Cisco SRST (Survivable Remote Site Telephony).   |
| Remote SIP Port                            | Type the <b>Remote SIP Port</b> number (default 5060) (5 character limit [values from 1 to 65535]).   |
| Local SIP Port                             | Type the <b>Local SIP Port</b> number (default 5060) (5 character limit [values from 2000 to 65535]).   |
| 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 (5 character limit [values from 1 to 65535]).   |
| SIP User ID                                | Type the <b>SIP User ID</b> (up to 64 alphanumeric characters).   |
| Authenticate ID                            | Type the <b>Authenticate ID</b> (up to 64 alphanumeric characters).   |
| Authenticate Password                      | Type the <b>Authenticate Password</b> (up to 64 alphanumeric characters).   |
| Register with a SIP Server                 | <p>Enable or disable SIP Registration.</p> <p>For information about Point-to-Point Configuration, see <a href="#">Section 2.4.6.1, "Point-to-Point Configuration"</a>.</p>  |
| Re-registration Interval (in seconds)      | Type the SIP Registration lease time in seconds (default is 60 minutes) (4 character limit [values from 30 to 3600]). Re-registration Interval (in seconds)   |
| Unregister on Reboot                       | When selected, on boot, the device will first register with a SIP server with a expiration delay of 0 seconds. This has the effect of unregistering any current devices on this extension.  |
| Disable rport Discovery                    | Prevents the device from including the public WAN IP address in the contact information sent to remote SIP servers. This will generally only need to be enabled when using an SBC in conjunction with a remote SIP server.  |

**Table 2-8. SIP Configuration Parameters (continued)**

| Web Page Item   | Description   |
|---|---|
| Buffer SIP Calls  | When this is enabled, SIP calls to the device will be stored in memory and will play when either the call is terminated or the buffer is full. The receive buffer is 2MB in size and this is equal to about four minutes of ulaw encoded audio. |
| <b>Call Disconnection</b>   |   |
| 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.<br><br>Note: A value of <b>0</b> will disable this function.  |
| <b>Misc Settings</b>  |   |
| 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 (values from 2000 to 65534).   |
|  | Click on the <b>Save</b> button to save your configuration settings.<br><br><b>Note:</b> You need to reboot for changes to take effect.   |
|  | Click on the <b>Reboot</b> button to reboot the system.   |

1. Enter the IP address of the **SIP Server**.
2. Enter the port numbers used for SIP signaling:
  - a. **Remote SIP Port**
  - b. **Local SIP Port**
3. Enter the SIP registration parameters:
  - a. **SIP User ID**
  - b. **Authenticate ID**
  - c. **Authenticate Password**
4. For **SIP Registration**, designate whether you want the VoIP Paging Server to register with your SIP server.
5. At **Unregister on Reboot**:
  - a. Select **Yes** to automatically unregister the V3 Paging Server when you reboot it.
  - b. Select **No** to keep the V3 Paging Server registered when you reboot it.
6. In the **Register Expiration** field, enter the number of seconds the V3 Paging Server registration lease remains valid with the SIP Server. The V3 Paging Server automatically re-registers with the SIP server before the lease expiration timeout.

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

### 2.4.6.1 Point-to-Point Configuration

When the board is set to not register with a SIP server, it's possible to set the device to dial out to a single endpoint. To do this, do the following:

1. On the **SIP Configuration** page (Figure 2-13), make sure that the **Register with a SIP Server** parameter is not selected.
2. Type the IP address of the remote device that you want to contact into the **Dial out Extension** field

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

**Figure 2-13. SIP Configuration Page Set to Point-to-Point Mode**


The screenshot shows the 'SIP Configuration' page of the CyberData v3 Paging Server. The page has a sidebar with navigation links: Home, Device Config, Networking, SIP Config, Nightringer, Fault Detection, PGroups Config, Audio Config, Event Config, Autoprovisioning, and Update Firmware. The main content area is titled 'SIP Configuration' and contains the following settings:

- Enable SIP operation:** ☒ (NOT Registered with SIP Server)
- SIP Settings:**
  - SIP Server: 10.0.0.253
  - Backup SIP Server 1:
  - Backup SIP Server 2:
  - Use Cisco SRST: ☐
  - Remote SIP Port: 5060
  - Local SIP Port: 5060
  - Outbound Proxy:
  - Outbound Proxy Port: 0
  - SIP User ID: 199
  - Authenticate ID: 199
  - Authenticate Password:
- Register with a SIP Server:** ☐ (This checkbox is highlighted by a red arrow, indicating it is unchecked.)
- Re-registration Interval (in seconds):** 360
- Unregister on Reboot:** ☐
- Disable rport Discovery:** ☐
- Buffer SIP Calls:** ☐
- Call disconnection:**
  - Terminate call after delay (in seconds):** 0
  - Note: A value of 0 will disable this function
- Misc Settings:**
  - RTP Port (even):** 10500

At the bottom of the page, there is a note: '\* You need to reboot for changes to take effect' and two buttons: 'Save' and 'Reboot'.

Device is set to **NOT** register with a SIP server

## 2.4.7 Configure the Night Ringer Parameters



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 2-14](#).

**Figure 2-14. Nightringer Configuration Page**

CyberData v3 Paging Server

Home  
 Device Config  
 Networking  
 SIP Config  
 Nightringer  
 Fault Detection  
 PGROUPs Config  
 Audio Config  
 Event Config  
 Autoprovisioning  
 Update Firmware

### Nightringer Configuration

Enable Nightringer: ☐ (NOT Registered with SIP Server)

**Nightringer Settings**



|   |   |
|---|---|
| SIP Server:   | <input type="text" value="10.0.0.253"/> |
| Remote SIP Port:  | <input type="text" value="5060"/>       |
| Local SIP Port:   | <input type="text" value="5061"/>       |
| Outbound Proxy:   | <input type="text"/>                    |
| Outbound Proxy Port:  | <input type="text" value="0"/>          |
| User ID:  | <input type="text" value="241"/>        |
| Authenticate ID:  | <input type="text" value="241"/>        |
| Authenticate Password:  | <input type="password" value="•••••"/>  |
| Re-registration Interval (in seconds): <input type="text" value="360"/> |   |
| Relay rings to multicast: <input type="checkbox"/>                      |   |
| Multicast Address:  | <input type="text" value="224.1.2.32"/> |
| Multicast Port:   | <input type="text" value="2020"/>       |

*Multicast port range can be from 2000-65534 and must be even*

\* You need to reboot for changes to take effect

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

**Table 2-9. 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.  |
| <b>Nightringer Settings</b>   |  |
| 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) (5 character limit [values from 1 to 65535]).   |
| Local SIP Port  | Type the Local SIP Port number (default 5061) (5 character limit [values from 2000 to 65535]).<br><br><b>Note:</b> This value cannot be the same as the <a href="#">Local SIP Port</a> found on the <a href="#">SIP Configuration Page</a> . |
| 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 (5 character limit [values from 1 to 65535]).  |
| User ID   | Type the <b>User ID</b> (up to 64 alphanumeric characters).  |
| Authenticate ID   | Type the <b>Authenticate ID</b> (up to 64 alphanumeric characters).  |
| Authenticate Password   | Type the <b>Authenticate Password</b> (up to 64 alphanumeric characters).  |
| Re-registration Interval (in seconds)   | Type the SIP Registration lease time in seconds (default is 60 minutes) (4 character limit [values from 30 to 3600]). Re-registration Interval (in seconds)  |
| Relay Rings to Multicast  | When selected, a user-defined audio file is sent to the specified multicast address and port when the night ringer is activated.   |
| Multicast Address   | Type the Multicast address.  |
| Multicast Port  | Type the Multicast port number.  |
|  | Click on the <b>Save</b> button to save your configuration settings.<br><br><b>Note:</b> You need to reboot for changes to take effect.  |
|  | Click on the <b>Reboot</b> button to reboot the system.  |

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



## 2.4.8 Configure the Fault Detection Parameters

1. Click on the **Fault Detection** button to open the **Fault Detection Configuration** page. See [Figure 2-15](#).

Figure 2-15. Fault Detection Configuration Page

**CyberData v3 Paging Server**

**Fault Detection**

Triggered Settings

Play Stored Audio Locally: ☒

Make Call to Extension: ☐

Dial Out Extension:

Dial Out ID:

Play Stored Audio via Multicast: ☐

Play Line-in Audio via Multicast\*\*: ☐

Multicast Address:




Multicast Port:

\* You need to reboot for changes to take effect

\*\* Cannot be combined with "Enable line-in to line-out loopback", "Enable line-in to multicast", or "Play Stored Audio via Multicast"

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

**Table 2-10. Fault Detection Configuration Parameters**

| Web Page Item   | Description   |
|---|---|
| <b>Triggered Settings</b>   |   |
| Play Audio Locally  | When selected, when the sensor is triggered, the audio file for "Sensor Triggered" will play out of the line-out and 600-Ohm connectors.  |
| Make Call to Extension  | When selected, when the sensor is triggered, the device will call the <b>Dial Out Extension</b> and play the "Sensor Triggered" audio file when someone answers.  |
| Dial Out Extension  | Enter the Dial Out Extension that you want the device to call when the sensor is triggered.   |
| Dial Out ID   | Enter the caller ID for the <b>Dial Out Extension</b> .   |
| Play Stored Audio via Multicast   | When selected, the device will play the stored audio file via multicast when the sensor is triggered.   |
| Play Line-in Audio via Multicast  | When selected, the device will play the line-in audio via multicast when the sensor is triggered.<br><br><b>Note:</b> You cannot combine this setting with any of the following settings: <b>Enable line-in to line-out loopback</b> , <b>Enable line-in to multicast</b> , or <b>Play Stored Audio via Multicast</b> |
| Multicast Address   | Enter the multicast IP address (15 character limit).  |
| Multicast Port  | Enter the multicast port number (5 character limit).  |
|  | Click on the <b>Test Fault</b> button to test the fault detection feature.  |
|  | Click on the <b>Save</b> button to save your configuration settings.<br><b>Note:</b> You need to reboot for changes to take effect.   |
|  | Click on the <b>Reboot</b> button to reboot the system.   |

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

## 2.4.9 Configure the Paging Groups (PGROUPS) Parameters

**Note** A PGROUP is a way of assigning multicast addresses and port numbers when configuring multicast paging speakers.

To assign a multicast address, you must first configure the speakers that you want to put into a paging zone by entering a particular multicast address and port number combination in the web configuration for these speakers.

**Note** The PGROUPS Configuration page consists of four pages. Each page must be saved independently.

1. Click on the **PGROUPS Config** button to open the **PGROUPS Configuration** page. See [Figure 2-16](#).

Figure 2-16. PGROUPS Configuration Page

**CyberData v3 Paging Server**

**PGROUPS Configuration (00-24)**

Bypass DTMF ☐  
*Bypassing DTMF will result in all calls being relayed to PGROUP 0  
 Any security code entered for PGROUP 0 will be ignored if DTMF is bypassed*

| #                 | Address    | Port | Name          | TTL | Lineout                             |
|-------------------|------------|------|---------------|-----|-------------------------------------|
| 00                | 234.2.1.1  | 2000 | PagingGroup00 | 255 | <input checked="" type="checkbox"/> |
| Security Code: .. |            |      |               |     |                                     |
| 01                | 234.2.1.2  | 2002 | PagingGroup01 | 255 | <input checked="" type="checkbox"/> |
| Security Code:    |            |      |               |     |                                     |
| 02                | 234.2.1.3  | 2004 | PagingGroup02 | 255 | <input checked="" type="checkbox"/> |
| Security Code:    |            |      |               |     |                                     |
| 03                | 234.2.1.4  | 2006 | PagingGroup03 | 255 | <input checked="" type="checkbox"/> |
| Security Code:    |            |      |               |     |                                     |
| 04                | 234.2.1.5  | 2008 | PagingGroup04 | 255 | <input checked="" type="checkbox"/> |
| Security Code:    |            |      |               |     |                                     |
| 05                | 234.2.1.6  | 2010 | PagingGroup05 | 255 | <input checked="" type="checkbox"/> |
| Security Code:    |            |      |               |     |                                     |
| 06                | 234.2.1.7  | 2012 | PagingGroup06 | 255 | <input checked="" type="checkbox"/> |
| Security Code:    |            |      |               |     |                                     |
| 07                | 234.2.1.8  | 2014 | PagingGroup07 | 255 | <input checked="" type="checkbox"/> |
| Security Code:    |            |      |               |     |                                     |
| 08                | 234.2.1.9  | 2016 | PagingGroup08 | 255 | <input checked="" type="checkbox"/> |
| Security Code:    |            |      |               |     |                                     |
| 09                | 234.2.1.10 | 2018 | PagingGroup09 | 255 | <input checked="" type="checkbox"/> |
| Security Code:    |            |      |               |     |                                     |
| 10                | 234.2.1.11 | 2020 | PagingGroup10 | 255 | <input checked="" type="checkbox"/> |
| Security Code:    |            |      |               |     |                                     |

**Figure 2-17. PGROUPS Configuration Page (continued)**

|                                     |            |      |               |     |                                     |
|-------------------------------------|------------|------|---------------|-----|-------------------------------------|
| <b>11</b>                           | 234.2.1.12 | 2022 | PagingGroup11 | 255 | <input checked="" type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                                     |
| <b>12</b>                           | 234.2.1.13 | 2024 | PagingGroup12 | 255 | <input checked="" type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                                     |
| <b>13</b>                           | 234.2.1.14 | 2026 | PagingGroup13 | 255 | <input checked="" type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                                     |
| <b>14</b>                           | 234.2.1.15 | 2028 | PagingGroup14 | 255 | <input checked="" type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                                     |
| <b>15</b>                           | 234.2.1.16 | 2030 | PagingGroup15 | 255 | <input checked="" type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                                     |
| <b>16</b>                           | 234.2.1.17 | 2032 | PagingGroup16 | 255 | <input checked="" type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                                     |
| <b>17</b>                           | 234.2.1.18 | 2034 | PagingGroup17 | 255 | <input checked="" type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                                     |
| <b>18</b>                           | 234.2.1.19 | 2036 | PagingGroup18 | 255 | <input checked="" type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                                     |
| <b>19</b>                           | 234.2.1.20 | 2038 | PagingGroup19 | 255 | <input checked="" type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                                     |
| <b>20</b>                           | 234.2.1.21 | 2040 | PagingGroup20 | 255 | <input checked="" type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                                     |
| <b>21</b>                           | 234.2.1.22 | 2042 | PagingGroup21 | 255 | <input checked="" type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                                     |
| <b>22</b>                           | 234.2.1.23 | 2044 | PagingGroup22 | 255 | <input checked="" type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                                     |
| <b>23</b>                           | 234.2.1.24 | 2046 | PagingGroup23 | 255 | <input checked="" type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                                     |
| <b>24</b>                           | 234.2.1.25 | 2048 | PagingGroup24 | 255 | <input checked="" type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                                     |

Port range can be from 2000-65534 and must be even  
Use IP address of "0.0.0.0" to disable relay on a group

\* You need to reboot for changes to take effect

Page: 1, 2, 3, 4

Figure 2-18. PGROUPS Configuration Page (continued)

## CyberData v3 Paging Server

- Home
- Device Config
- Networking
- SIP Config
- Nightringer
- Fault Detection
- PGROUPS Config**
- Audio Config
- Event Config
- Autoprovisioning
- Update Firmware

### PGROUPS Configuration (25-49)

Paging Groups

| #                                   | Address    | Port | Name          | TTL | Lineout                  |
|-------------------------------------|------------|------|---------------|-----|--------------------------|
| 25                                  | 234.2.1.26 | 2050 | PagingGroup25 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                          |
| 26                                  | 234.2.1.27 | 2052 | PagingGroup26 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                          |
| 27                                  | 234.2.1.28 | 2054 | PagingGroup27 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                          |
| 28                                  | 234.2.1.29 | 2056 | PagingGroup28 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                          |
| 29                                  | 234.2.1.30 | 2058 | PagingGroup29 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                          |
| 30                                  | 234.2.1.31 | 2060 | PagingGroup30 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                          |
| 31                                  | 234.2.1.32 | 2062 | PagingGroup31 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                          |
| 32                                  | 234.2.1.33 | 2064 | PagingGroup32 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                          |
| 33                                  | 234.2.1.34 | 2066 | PagingGroup33 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                          |
| 34                                  | 234.2.1.35 | 2068 | PagingGroup34 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                          |
| 35                                  | 234.2.1.36 | 2070 | PagingGroup35 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                          |
| 36                                  | 234.2.1.37 | 2072 | PagingGroup36 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                          |

**Figure 2-19. PGROUPS Configuration Page (continued)**

|           |                |      |                      |     |                          |
|-----------|----------------|------|----------------------|-----|--------------------------|
| <b>37</b> | 234.2.1.38     | 2074 | PagingGroup37        | 255 | <input type="checkbox"/> |
|           | Security Code: |      | <input type="text"/> |     |                          |
| <b>38</b> | 234.2.1.39     | 2076 | PagingGroup38        | 255 | <input type="checkbox"/> |
|           | Security Code: |      | <input type="text"/> |     |                          |
| <b>39</b> | 234.2.1.40     | 2078 | PagingGroup39        | 255 | <input type="checkbox"/> |
|           | Security Code: |      | <input type="text"/> |     |                          |
| <b>40</b> | 234.2.1.41     | 2080 | PagingGroup40        | 255 | <input type="checkbox"/> |
|           | Security Code: |      | <input type="text"/> |     |                          |
| <b>41</b> | 234.2.1.42     | 2082 | PagingGroup41        | 255 | <input type="checkbox"/> |
|           | Security Code: |      | <input type="text"/> |     |                          |
| <b>42</b> | 234.2.1.43     | 2084 | PagingGroup42        | 255 | <input type="checkbox"/> |
|           | Security Code: |      | <input type="text"/> |     |                          |
| <b>43</b> | 234.2.1.44     | 2086 | PagingGroup43        | 255 | <input type="checkbox"/> |
|           | Security Code: |      | <input type="text"/> |     |                          |
| <b>44</b> | 234.2.1.45     | 2088 | PagingGroup44        | 255 | <input type="checkbox"/> |
|           | Security Code: |      | <input type="text"/> |     |                          |
| <b>45</b> | 234.2.1.46     | 2090 | PagingGroup45        | 255 | <input type="checkbox"/> |
|           | Security Code: |      | <input type="text"/> |     |                          |
| <b>46</b> | 234.2.1.47     | 2092 | PagingGroup46        | 255 | <input type="checkbox"/> |
|           | Security Code: |      | <input type="text"/> |     |                          |
| <b>47</b> | 234.2.1.48     | 2094 | PagingGroup47        | 255 | <input type="checkbox"/> |
|           | Security Code: |      | <input type="text"/> |     |                          |
| <b>48</b> | 234.2.1.49     | 2096 | PagingGroup48        | 255 | <input type="checkbox"/> |
|           | Security Code: |      | <input type="text"/> |     |                          |
| <b>49</b> | 234.2.1.50     | 2098 | PagingGroup49        | 255 | <input type="checkbox"/> |
|           | Security Code: |      | <input type="text"/> |     |                          |

Port range can be from 2000-65534 and must be even  
Use IP address of "0.0.0.0" to disable relay on a group

\* You need to reboot for changes to take effect

Save Reboot

Page: 1, 2, 3, 4

Figure 2-20. PGROUPS Configuration Page (continued)

## CyberData v3 Paging Server

- Home
- Device Config
- Networking
- SIP Config
- Nightringer
- Fault Detection
- PGROUPS Config**
- Audio Config
- Event Config
- Autoprovisioning
- Update Firmware

### PGROUPS Configuration (50-74)

Paging Groups

| #                                   | Address    | Port | Name          | TTL | Lineout                  |
|-------------------------------------|------------|------|---------------|-----|--------------------------|
| 50                                  | 234.2.1.51 | 2100 | PagingGroup50 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                          |
| 51                                  | 234.2.1.52 | 2102 | PagingGroup51 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                          |
| 52                                  | 234.2.1.53 | 2104 | PagingGroup52 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                          |
| 53                                  | 234.2.1.54 | 2106 | PagingGroup53 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                          |
| 54                                  | 234.2.1.55 | 2108 | PagingGroup54 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                          |
| 55                                  | 234.2.1.56 | 2110 | PagingGroup55 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                          |
| 56                                  | 234.2.1.57 | 2112 | PagingGroup56 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                          |
| 57                                  | 234.2.1.58 | 2114 | PagingGroup57 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                          |
| 58                                  | 234.2.1.59 | 2116 | PagingGroup58 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                          |
| 59                                  | 234.2.1.60 | 2118 | PagingGroup59 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                          |
| 60                                  | 234.2.1.61 | 2120 | PagingGroup60 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                          |
| 61                                  | 234.2.1.62 | 2122 | PagingGroup61 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                          |

**Figure 2-21. PGROUPS Configuration Page (continued)**

|           |                                     |      |               |     |                          |
|-----------|-------------------------------------|------|---------------|-----|--------------------------|
| <b>62</b> | 234.2.1.63                          | 2124 | PagingGroup62 | 255 | <input type="checkbox"/> |
|           | Security Code: <input type="text"/> |      |               |     |                          |
| <b>63</b> | 234.2.1.64                          | 2126 | PagingGroup63 | 255 | <input type="checkbox"/> |
|           | Security Code: <input type="text"/> |      |               |     |                          |
| <b>64</b> | 234.2.1.65                          | 2128 | PagingGroup64 | 255 | <input type="checkbox"/> |
|           | Security Code: <input type="text"/> |      |               |     |                          |
| <b>65</b> | 234.2.1.66                          | 2130 | PagingGroup65 | 255 | <input type="checkbox"/> |
|           | Security Code: <input type="text"/> |      |               |     |                          |
| <b>66</b> | 234.2.1.67                          | 2132 | PagingGroup66 | 255 | <input type="checkbox"/> |
|           | Security Code: <input type="text"/> |      |               |     |                          |
| <b>67</b> | 234.2.1.68                          | 2134 | PagingGroup67 | 255 | <input type="checkbox"/> |
|           | Security Code: <input type="text"/> |      |               |     |                          |
| <b>68</b> | 234.2.1.69                          | 2136 | PagingGroup68 | 255 | <input type="checkbox"/> |
|           | Security Code: <input type="text"/> |      |               |     |                          |
| <b>69</b> | 234.2.1.70                          | 2138 | PagingGroup69 | 255 | <input type="checkbox"/> |
|           | Security Code: <input type="text"/> |      |               |     |                          |
| <b>70</b> | 234.2.1.71                          | 2140 | PagingGroup70 | 255 | <input type="checkbox"/> |
|           | Security Code: <input type="text"/> |      |               |     |                          |
| <b>71</b> | 234.2.1.72                          | 2142 | PagingGroup71 | 255 | <input type="checkbox"/> |
|           | Security Code: <input type="text"/> |      |               |     |                          |
| <b>72</b> | 234.2.1.73                          | 2144 | PagingGroup72 | 255 | <input type="checkbox"/> |
|           | Security Code: <input type="text"/> |      |               |     |                          |
| <b>73</b> | 234.2.1.74                          | 2146 | PagingGroup73 | 255 | <input type="checkbox"/> |
|           | Security Code: <input type="text"/> |      |               |     |                          |
| <b>74</b> | 234.2.1.75                          | 2148 | PagingGroup74 | 255 | <input type="checkbox"/> |
|           | Security Code: <input type="text"/> |      |               |     |                          |

*Port range can be from 2000-65534 and must be even  
Use IP address of "0.0.0.0" to disable relay on a group*

\* You need to reboot for changes to take effect

Page: [1](#), [2](#), [3](#), [4](#)



Figure 2-22. PGROUPS Configuration Page (continued)

## CyberData v3 Paging Server

- Home
- Device Config
- Networking
- SIP Config
- Nightringer
- Fault Detection
- PGROUPS Config**
- Audio Config
- Event Config
- Autoprovisioning
- Update Firmware

### PGROUPS Configuration (75-99)

Paging Groups

| #                                   | Address    | Port | Name          | TTL | Lineout                  |
|-------------------------------------|------------|------|---------------|-----|--------------------------|
| 75                                  | 234.2.1.76 | 2150 | PagingGroup75 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                          |
| 76                                  | 234.2.1.77 | 2152 | PagingGroup76 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                          |
| 77                                  | 234.2.1.78 | 2154 | PagingGroup77 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                          |
| 78                                  | 234.2.1.79 | 2156 | PagingGroup78 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                          |
| 79                                  | 234.2.1.80 | 2158 | PagingGroup79 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                          |
| 80                                  | 234.2.1.81 | 2160 | PagingGroup80 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                          |
| 81                                  | 234.2.1.82 | 2162 | PagingGroup81 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                          |
| 82                                  | 234.2.1.83 | 2164 | PagingGroup82 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                          |
| 83                                  | 234.2.1.84 | 2166 | PagingGroup83 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                          |
| 84                                  | 234.2.1.85 | 2168 | PagingGroup84 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                          |
| 85                                  | 234.2.1.86 | 2170 | PagingGroup85 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                          |
| 86                                  | 234.2.1.87 | 2172 | PagingGroup86 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |            |      |               |     |                          |

**Figure 2-23. PGROUPS Configuration Page (continued)**

|                                     |             |      |               |     |                          |
|-------------------------------------|-------------|------|---------------|-----|--------------------------|
| 87                                  | 234.2.1.88  | 2174 | PagingGroup87 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |             |      |               |     |                          |
| 88                                  | 234.2.1.89  | 2176 | PagingGroup88 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |             |      |               |     |                          |
| 89                                  | 234.2.1.90  | 2178 | PagingGroup89 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |             |      |               |     |                          |
| 90                                  | 234.2.1.91  | 2180 | PagingGroup90 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |             |      |               |     |                          |
| 91                                  | 234.2.1.92  | 2182 | PagingGroup91 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |             |      |               |     |                          |
| 92                                  | 234.2.1.93  | 2184 | PagingGroup92 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |             |      |               |     |                          |
| 93                                  | 234.2.1.94  | 2186 | PagingGroup93 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |             |      |               |     |                          |
| 94                                  | 234.2.1.95  | 2188 | PagingGroup94 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |             |      |               |     |                          |
| 95                                  | 234.2.1.96  | 2190 | PagingGroup95 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |             |      |               |     |                          |
| 96                                  | 234.2.1.97  | 2192 | PagingGroup96 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |             |      |               |     |                          |
| 97                                  | 234.2.1.98  | 2194 | PagingGroup97 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |             |      |               |     |                          |
| 98                                  | 234.2.1.99  | 2196 | PagingGroup98 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |             |      |               |     |                          |
| 99                                  | 234.2.1.100 | 2198 | PagingGroup99 | 255 | <input type="checkbox"/> |
| Security Code: <input type="text"/> |             |      |               |     |                          |

*Port range can be from 2000-65534 and must be even  
Use IP address of "0.0.0.0" to disable relay on a group*

\* You need to reboot for changes to take effect

Save Reboot

Page: 1, 2, 3, 4

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

**Table 2-11. PGROUPS Configuration Parameters**

| Web Page Item   | Description   |
|---|---|
| Bypass DTMF   | When selected, bypassing the DTMF will result in all calls being relayed to PGROUP 0.   |
| #   | Shows the paging group number.  |
| Address   | Enter the IP address of the PGROUP.<br><b>Note:</b> To disable a relay on a group, use an IP address of 0.0.0.0.  |
| Port  | Enter the port number of the PGROUP.<br><b>Note:</b> The port range can be from 2000 to 65534 and must be even. When configuring a Paging Group for Polycom Group Paging using an odd-numbered port, configure the next lower even port number. For example, when using the default Polycom paging port 5001 on Polycom phones, configure the next lower even port 5000 for the desired V3 Paging Server's Paging Group port. |
| Name  | Enter a name for the PGROUP.  |
| TTL   | The TTL field allows you to adjust the TTL. TTL is "time to live" and it describes how many networks (routers) a packet will go through before it is discarded.   |
| Lineout   | The Lineout field determines whether or not the device will play audio out of the RCA output port and the 600 Ohm output port in addition to forwarding it to the PGROUP.   |
| Security Code   | This field allows the user to add a security code to prevent unauthorized paging to the PGROUP. Code must be between two to five numeric digits (0 through 9). Leave the field empty for no security code. Any security code entered for PGROUP 0 will be ignored if DTMF is bypassed.  |
| <div>Page: 1 2 3 4</div> Click on 1, 2, 3, or 4 to navigate through the pages of PGROUPS. |   |

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

---

## 2.4.10 Operating the Paging Server

Call behavior changes based on the configuration of the **PGROUPs Configuration** page.

### 2.4.10.1 DTMF Bypassed

- When the V3 Paging Server is called, it will send the "page tone" audio message to the caller.
- When the caller hears this message, the caller should begin speaking.

### 2.4.10.2 DTMF Not Bypassed

- When the V3 Paging Server is called, it sends the "Enter PGROUP" audio message to the caller. By default, this message is "Enter the two digit zone number."
- When the caller hears this message, the caller should enter the two-digit code for the zone that the caller wants to page.
- If the zone is invalid or not configured, the V3 Paging Server sends the "Invalid PGROUP" audio message to the caller. By default this message is "Invalid zone number. Enter the two digit zone number." The caller should repeat the previous step.
- If a security code is enabled on the zone, the V3 Paging Server sends the "Enter Code" audio message to the caller. By default this message is "Enter the security code." When the caller hears this message, the caller should enter the security code for the selected zone. If no security code is enabled on the zone, the V3 Paging Server will send the "page tone" audio message to the caller. The caller should begin speaking when this message is heard.
- If the security code is invalid, the V3 Paging Server will send the "Invalid Code" audio message to the caller. By default this message is "Invalid Security code. Enter the security code." The caller should repeat the previous step. When a valid security code is entered, the V3 Paging Server will send the "page tone" audio message to the caller. The caller should begin speaking when this message is heard.
- For *page-all*, you simply configure *all* speakers with a particular multicast address and port number combination, which represents one of the 100 zones that the paging server will initially support. Each speaker can still be part of 100 other paging zones in addition to the one *page-all* zone.
- The V3 Paging Server can negotiate the multicast stream via SIP regardless of the bypass state. However, if the V3 Paging Server is not in bypass mode (or the multicast sender does not send any DTMF), the device will not play or relay any audio because the device will be waiting at the zone entry prompt. The DTMF from the sender would have to be sent as RFC2833 RTP events (i.e. "out of band").

## 2.4.11 Configure the Audio Parameters

Click on the **Audio Config** button to open the **Audio Configuration** page. See [Figure 2-24](#). 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.

**Figure 2-24. Audio Configuration Page**

**CyberData v3 Paging Server**

**Audio Configuration**

Available Space = 14.95MB

Audio Files

|                             |  |   |
|-----------------------------|--|---|
| 0: Currently set to default | New File: <input type="button" value="Browse..."/> No file selected. | <input type="button" value="Play"/> <input type="button" value="Delete"/> <input type="button" value="Save"/> |
| 1: Currently set to default | New File: <input type="button" value="Browse..."/> No file selected. | <input type="button" value="Play"/> <input type="button" value="Delete"/> <input type="button" value="Save"/> |
| 2: Currently set to default | New File: <input type="button" value="Browse..."/> No file selected. | <input type="button" value="Play"/> <input type="button" value="Delete"/> <input type="button" value="Save"/> |
| 3: Currently set to default | New File: <input type="button" value="Browse..."/> No file selected. | <input type="button" value="Play"/> <input type="button" value="Delete"/> <input type="button" value="Save"/> |
| 4: Currently set to default | New File: <input type="button" value="Browse..."/> No file selected. | <input type="button" value="Play"/> <input type="button" value="Delete"/> <input type="button" value="Save"/> |
| 5: Currently set to default | New File: <input type="button" value="Browse..."/> No file selected. | <input type="button" value="Play"/> <input type="button" value="Delete"/> <input type="button" value="Save"/> |
| 6: Currently set to default | New File: <input type="button" value="Browse..."/> No file selected. | <input type="button" value="Play"/> <input type="button" value="Delete"/> <input type="button" value="Save"/> |
| 7: Currently set to default | New File: <input type="button" value="Browse..."/> No file selected. | <input type="button" value="Play"/> <input type="button" value="Delete"/> <input type="button" value="Save"/> |
| 8: Currently set to default | New File: <input type="button" value="Browse..."/> No file selected. | <input type="button" value="Play"/> <input type="button" value="Delete"/> <input type="button" value="Save"/> |

**Figure 2-25. Audio Configuration Page**

The screenshot displays the Audio Configuration Page with a light blue background and a dark blue border. It contains ten rows of configuration options, each with a label, a status message, a file selection button, and three action buttons (Play, Delete, Save).

| Parameter           | Status                   | File Selection   | Play                                | Delete                                | Save                                |
|---------------------|--------------------------|--|-------------------------------------|---------------------------------------|-------------------------------------|
| 9:                  | Currently set to default | New File: <input type="button" value="Browse..."/> No file selected. | <input type="button" value="Play"/> | <input type="button" value="Delete"/> | <input type="button" value="Save"/> |
| Dot:                | Currently set to default | New File: <input type="button" value="Browse..."/> No file selected. | <input type="button" value="Play"/> | <input type="button" value="Delete"/> | <input type="button" value="Save"/> |
| Audio test:         | Currently set to default | New File: <input type="button" value="Browse..."/> No file selected. | <input type="button" value="Play"/> | <input type="button" value="Delete"/> | <input type="button" value="Save"/> |
| Page tone:          | Currently set to default | New File: <input type="button" value="Browse..."/> No file selected. | <input type="button" value="Play"/> | <input type="button" value="Delete"/> | <input type="button" value="Save"/> |
| Enter PGROUP:       | Currently set to default | New File: <input type="button" value="Browse..."/> No file selected. | <input type="button" value="Play"/> | <input type="button" value="Delete"/> | <input type="button" value="Save"/> |
| Invalid PGROUP:     | Currently set to default | New File: <input type="button" value="Browse..."/> No file selected. | <input type="button" value="Play"/> | <input type="button" value="Delete"/> | <input type="button" value="Save"/> |
| Enter Code:         | Currently set to default | New File: <input type="button" value="Browse..."/> No file selected. | <input type="button" value="Play"/> | <input type="button" value="Delete"/> | <input type="button" value="Save"/> |
| Invalid Code:       | Currently set to default | New File: <input type="button" value="Browse..."/> No file selected. | <input type="button" value="Play"/> | <input type="button" value="Delete"/> | <input type="button" value="Save"/> |
| Your IP Address is: | Currently set to default | New File: <input type="button" value="Browse..."/> No file selected. | <input type="button" value="Play"/> | <input type="button" value="Delete"/> | <input type="button" value="Save"/> |
| Rebooting:          | Currently set to default | New File: <input type="button" value="Browse..."/> No file selected. | <input type="button" value="Play"/> | <input type="button" value="Delete"/> | <input type="button" value="Save"/> |
| Restoring Default:  | Currently set to default | New File: <input type="button" value="Browse..."/> No file selected. | <input type="button" value="Play"/> | <input type="button" value="Delete"/> | <input type="button" value="Save"/> |

**Figure 2-26. Audio Configuration Page**

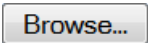



The screenshot displays the Audio Configuration Page with a light blue background and a dark blue border. It contains two main sections: **Sensor Triggered** and **Night Ring**. Each section indicates it is currently set to default and provides a 'New File' field with a 'Browse...' button and the text 'No file selected.' To the right of each section are three buttons: 'Play', 'Delete', and 'Save'.

| Configuration Item | Current Setting          | New File          | Buttons            |
|--------------------|--------------------------|-------------------|--------------------|
| Sensor Triggered   | Currently set to default | No file selected. | Play, Delete, Save |
| Night Ring         | Currently set to default | No file selected. | Play, Delete, Save |

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

**Note** Each entry on the **Audio Configuration** page replaces one of the stock audio files on the board. When the input box displays the word **default**, the V3 Paging Server is using the stock audio file. If that file is replaced with a user file, it will display the uploaded filename.

**Table 2-12. Audio Configuration Parameters**

| Web Page Item   | Description  |
|---|--|
| <b>Audio Files</b>  |  |
| 0-9   | The name of the audio configuration option is the same as the spoken audio that plays on the board (24 character limit).<br><br>'0' corresponds to the spoken word "zero."<br>'1' corresponds to the spoken word "one."<br>'2' corresponds to the spoken word "two."<br>'3' corresponds to the spoken word "three."<br>'4' corresponds to the spoken word "four."<br>'5' corresponds to the spoken word "five."<br>'6' corresponds to the spoken word "six."<br>'7' corresponds to the spoken word "seven."<br>'8' corresponds to the spoken word "eight."<br>'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 that is unused by default (24 character limit).   |
| Enter PGROUP  | Corresponds to the message "Enter PGROUP" (24 character limit).  |
| Invalid PGROUP  | Corresponds to the message "Invalid PGROUP" (24 character limit).  |
| Enter Code  | Corresponds to the message "Enter Code" (24 character limit).  |
| Invalid Code  | Corresponds to the message "Invalid Code" (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).   |
| Sensor Triggered  | Corresponds to the message "Sensor Triggered" (24 character limit).  |
| Night Ring  | Specifies the ringtone for nightring. By default this parameter uses the same audio file that is selected for the <b>Ring Tone</b> parameter.  |
|  | The <b>Browse</b> button will allow you to navigate to and select an audio file.   |
|  | The <b>Play</b> button will play that audio file.  |
|  | The <b>Delete</b> button will delete any user uploaded audio and restore the stock audio file.   |
|  | The <b>Save</b> button will download a new user audio file to the board once you've selected the file by using the <b>Browse</b> button. The <b>Save</b> button will delete any pre-existing user-uploaded audio files.  |



### 2.4.11.1 User-created Audio Files

User-created audio files must be saved in one of the following formats:

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

**Note** These audio format restrictions are enforced by the webpage.

You can use the free utility *Audacity* to convert audio files into this format. See [Figure 2-27](#) through [Figure 2-29](#).

**Figure 2-27. Audacity 1**

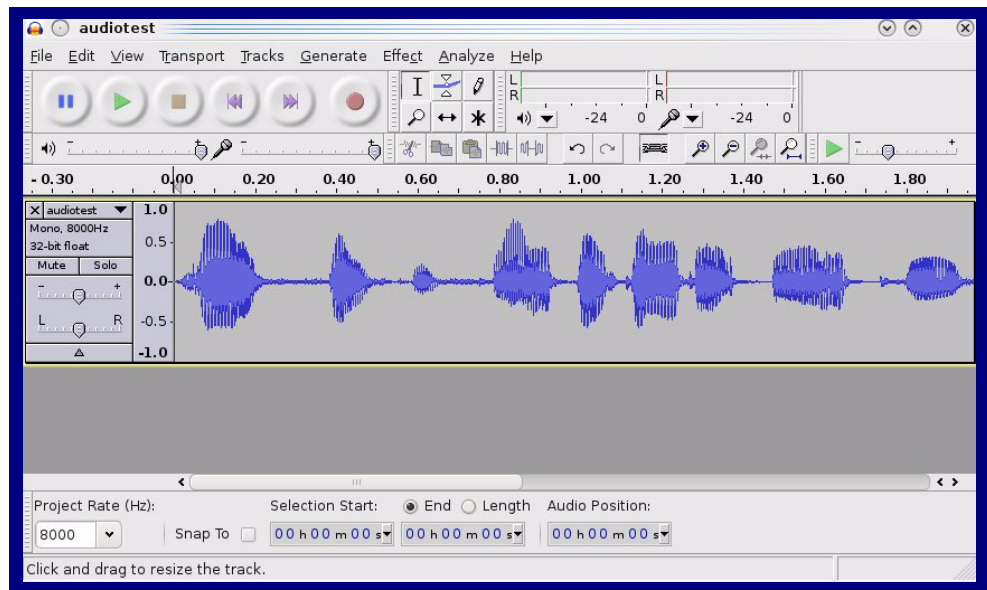
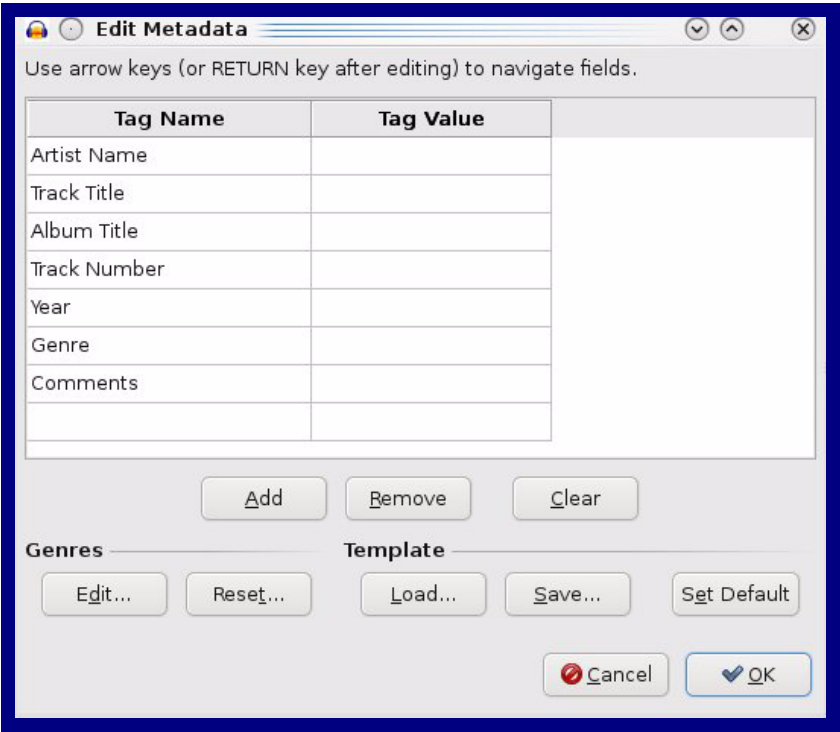


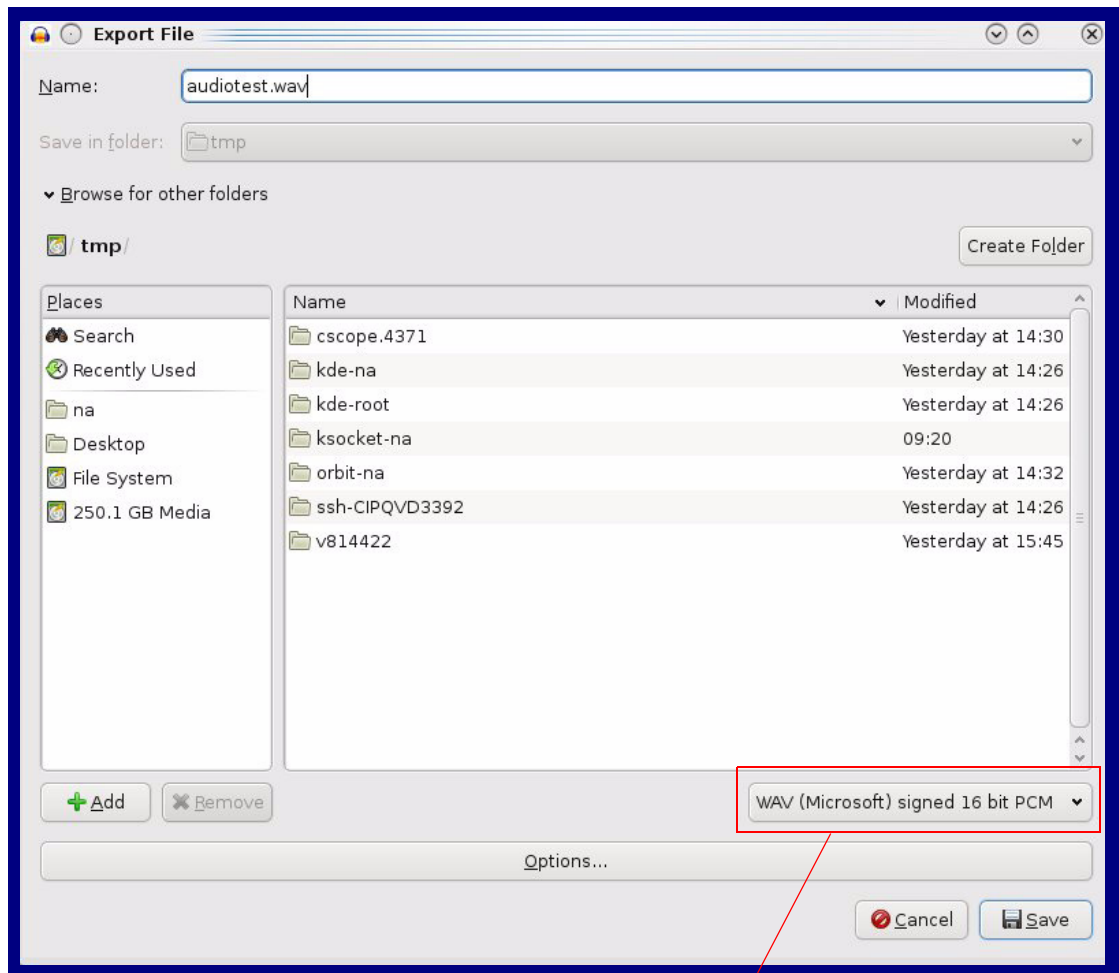
Figure 2-28. Audacity 2



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

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

**Figure 2-29. WAV (Microsoft) signed 16 bit PCM**



WAV (Microsoft) signed 16 bit PCM

## 2.4.12 Configure the Event Parameters

Click on the **Event Config** button to open the **Event Configuration** page (Figure 2-30). 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 2-30. Event Configuration Page

**CyberData v3 Paging Server**

**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 Night Ring Events: ☐

Enable Power on Events: ☐

Enable Security Events: ☐




Enable 60 second Heartbeat Events: ☐

\* You need to reboot for changes to take effect

Save Test Event Reboot

Table 2-13 shows the web page items on the **Event Configuration** page.

**Table 2-13. Event Configuration**

| Web Page Item   | Description   |
|---|---|
| Enable Event Generation   | When selected, Event Generation is enabled.   |
| <b>Remote Event Server</b>  |   |
| Remote Event Server IP  | Type the Remote Event Server IP address.<br>(64 character limit)  |
| Remote Event Server Port  | Type the Remote Event Server port number.<br>(8 character limit)  |
| Remote Event Server URL   | Type the Remote Event Server URL.<br>(127 character limit)  |
| <b>Events</b>   |   |
| 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 Night Ring Events  | When selected, there is a notification when the unit receives a night ring.   |
| 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 on the <b>Save</b> button to save your configuration settings.<br><br><b>Note:</b> You need to reboot for changes to take effect. |
|  | Click on the <b>Test Event</b> button to test an event.   |
|  | Click on the <b>Reboot</b> button to reboot the system.   |

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

### 2.4.12.1 Example Packets for Events

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

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

Here are example packets for every event:

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

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

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

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

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

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

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

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



## 2.4.13 Configure the Autoprovisioning Parameters

1. Click on the **Autoprovisioning** button to open the **Autoprovisioning Configuration** page.  
See [Figure 2-31](#).

Figure 2-31. Autoprovisioning Configuration Page

**CyberData v3 Paging Server**

**Autoprovisioning**

Autoprovisioning

Disable Autoprovisioning: ☐

Autoprovisioning Server:

Autoprovisioning Filename:

Use TFTP: ☐

Autoprovisioning autoupdate (in minutes):

Autoprovision at time (HHMMSS):

Autoprovision when idle (in minutes > 10):

Get Autoprovisioning Template

Clock

NTP Server:

Posix Timezone String (see manual):

Set Time with external NTP server on boot: ☐

Periodically update with time server: ☐

Time update period (in hours):

Set time from NTP Server

Current Time

Current Time (UTC) in 24 hour format (HHMMSS):

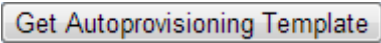
Set Time

See the manual to learn how to use autoprovisioning to configure your device. Autoprovisioning happens on boot. The device will first look for a configured server address and filename. If these haven't been configured, it will look for an autoprovisioning server in your list of DHCP options and try to download '0020f702e58e.xml' and if this fails, '000000cd.xml'.





Save Reboot

2. On the **Autoprovisioning Configuration** page, you may enter values for the parameters indicated in [Table 2-14](#).

**Table 2-14. Autoprovisioning Configuration Parameters**

| Web Page Item   | Description   |
|---|---|
| <b>Autoprovisioning</b>   |   |
| Disable Autoprovisioning  | Prevent the device from automatically trying to download a configuration file. See <a href="#">Section 2.4.13.1, "Autoprovisioning"</a> for more information.   |
| Autoprovisioning Server   | Enter the IPv4 address of the provisioning server in dotted decimal notation.   |
| Autoprovisioning Filename   | <p>The autoprovisioning filename is the configuration filename. The default autoprovisioning filename is in the format of <b>&lt;mac address&gt;.xml</b>.</p> <p>Supported filename extensions are .txt, and .xml. The current filename is denoted by an asterisk at the bottom of the <a href="#">Autoprovisioning Configuration Page</a>. Enter up to 256 characters.</p> <p>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.</p> |
| Use tftp  | The device will use TFTP (instead of http) to download autoprovisioning files.  |
| Autoprovisioning Autoupdate (in minutes)  | <p>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.</p> <p><b>Note:</b> To use the auto update options, enable the <a href="#">Set Time with NTP Server on boot</a> setting on the <a href="#">Device Configuration Page</a> (see <a href="#">Table 2-6</a>).</p>  |
| Autoprovision at time (HHMMSS)  | <p>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.</p> <p><b>Note:</b> To use the auto update options, enable the <a href="#">Set Time with NTP Server on boot</a> setting on the <a href="#">Device Configuration Page</a> (see <a href="#">Table 2-6</a>).</p>  |
| Autoprovision when idle (in minutes > 10)   | <p>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.</p> <p><b>Note:</b> To use the auto update options, enable the <a href="#">Set Time with NTP Server on boot</a> setting on the <a href="#">Device Configuration Page</a> (see <a href="#">Table 2-6</a>).</p>   |
|  | Press the <b>Get Autoprovisioning Template</b> button to create an autoprovisioning file for this unit. See <a href="#">Section 2.4.13.3, "Get Autoprovisioning Template Button"</a>  |
| <b>Clock</b>  |   |
| 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.  |

**Table 2-14. Autoprovisioning Configuration Parameters (continued)**

| Web Page Item   | Description  |
|---|--|
| Posix Timezone String   | See <a href="#">Section 2.4.13.4, "Time Zone Strings"</a> 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. |
| Set Time with NTP Server on boot  | When selected, the time is set with an external NTP server when the device restarts.   |
| Periodically update with time 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.   |
|    | Allows you to set the time from the NTP server.  |
| <b>Current Time</b>   |  |
| Current Time (UTC) in 24 hour format (HHMMSS)                                       | Allows you to input the current time in the 24 hour format. (6 character limit)  |
|    | Click on this button to set the clock after entering the current time.   |
|    | Click on the <b>Save</b> button to save your configuration settings.<br><b>Note:</b> You need to reboot for changes to take effect.  |
|  | Click on the <b>Reboot</b> button to reboot the system.  |

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

### 2.4.13.1 Autoprovisioning

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

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

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

By default, the device will get its autoprovisioning server from the DHCP options. See [Section 2.4.13.2, "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 Configuration Page](#) using the **Download Template** button (see [Table 2-14](#)). This file contains every configuration option that can be set on the board.

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

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

```
<MiscSettings>
    <DeviceName>CyberData VoIP Intercom</DeviceName>
<!--    <AutoprovFile>common.xml</AutoprovFile>-->
<!--    <AutoprovFile>sip_reg[macaddress].xml</AutoprovFile>-->
<!--    <AutoprovFile>audio[macaddress]</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](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 2-15. Autoprovisioning File Name**

| <b>Autoprovisioning<br/>Filename</b> | <b>Autoprovisioning<br/>Server</b> | <b>File Downloaded</b>                      |
|--------------------------------------|------------------------------------|---|
| config.xml                           | 10.0.1.3                           | 10.0.1.3/config.xml                         |
| /path/to/config.xml                  | 10.0.1.3                           | 10.0.1.3/path/to/config.xml                 |
| subdirectory/path/                   | 10.0.1.3                           | 10.0.1.3/subdirectory/path/0020f7020002.xml |

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

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

For example:

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

The autoprovisioning filename is set to “cyberdata/”

On boot, the device will try to download:

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

...and if this fails:

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

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

```
Autoprovisioning <FirmwareSettings>
Firmware Updates <FirmwareFile>505-ulmage-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-ulmage-[device\_file\_name]).

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

The list of valid product strings:

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

## Autoprovisioning Example 1

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

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

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

**000000cd.xml**

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

**sip\_common.xml**

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

**sip\_0020f7020001.xml**

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

**sip\_0020f7020002.xml**

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

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

1. Device1 changes its device name to **CyberData Autoprovisioned**.
2. Device1 finds an AutoprovFile element containing the filename **sip\_common.xml**. The device downloads **sip\_common.xml** from "https://autoprovtest.server.net," and imports this configuration, setting the sip server to **10.0.0.253** and the remote port to **5060.3**.
3. Device1 finds another AutoprovFile element containing the filename **sip\_[macaddress].xml**. The device replaces the **[macaddress]** with its own mac address value creating **sip\_0020f7020001.xml**, downloads this file from "https://autoprovtest.server.net," and imports this configuration. This sets the user ID to **198**, the password to **ext198**, and the dialout extension to **204**. Device1 is now finished with autoprovisioning.



Device2 goes through the same steps by setting its device name to **CyberData Autoprovisioned**, its SIP server to **10.0.0.253**, and its port to **5060**. When Device2 “sees” **sip\_[macaddress].xml**, Device2 replaces it with its own mac address and downloads **sip\_0020f7020002.xml** from “https://autoprovtest.server.net.” Device2 sets the SIP User ID to **500**, the password to **ext500**, and the dialout extension to **555**.

#### Autoprovisioning Example 2

Here is another example of setting up your autoprovisioning files:

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

##### **0020f7020001.xml**

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

##### **0020f7020002.xml**

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

##### **common\_settings.xml**

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

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

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

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

## XML Files

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

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

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

From the device specific xml, a pointer to a sip\_common file

From the device specific xml, a pointer to the device specific sip\_[macaddress].xml

From the common file, a pointer to sip\_common.xml

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

## Autoprovisioned Audio Files

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

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

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

### 2.4.13.2 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; }

```

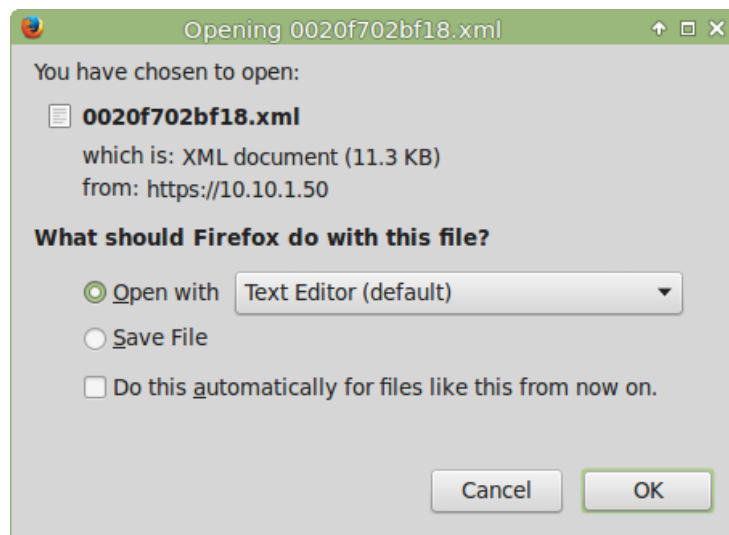
### 2.4.13.3 Get Autoprovisioning Template Button

The **Get Autoprovisioning 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 **Get Autoprovisioning Template** button.
2. You will see a window prompting you to save a configuration file (.xml) to a location on your computer (Figure 2-32). 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 2-32.

**Figure 2-32. 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.

## 2.4.13.4 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 2-16](#) shows some common strings.

**Table 2-16. 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 <sup>a</sup> | 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 2-17](#) 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 2-17. 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 2-18](#) has some more examples of time zone strings.

**Table 2-18. Time Zone String Examples**

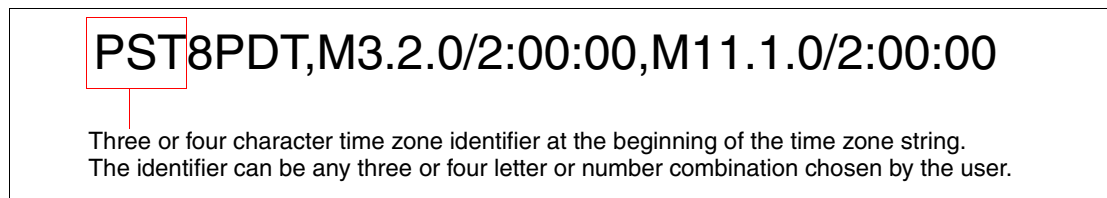
| Time Zone           | Time Zone String                  |
|---------------------|-----------------------------------|
| Tokyo <sup>a</sup>  | IST-9                             |
| Berlin <sup>b</sup> | CET-1MET,M3.5.0/1:00,M10.5.0/1:00 |

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 2-33. 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 2-19](#) has information about the GMT time in various time zones.

**Table 2-19. 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 |

**Table 2-19. World GMT Table (continued)**

| <b>Time Zone</b> | <b>City or Area Zone Crosses</b> |
|------------------|----------------------------------|
| GMT+1            | Berlin, Rome                     |
| GMT+2            | Israel, Cairo                    |
| GMT+3            | Moscow, Kuwait                   |
| GMT+4            | Abu Dhabi, Muscat                |
| 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       |

## 2.5 Upgrading the Firmware

**Note** A new firmware signature prevents users from loading firmware intended for one device to a different device. See [Table 2-20](#).

**Table 2-20. Firmware**

| Firmware File Name       | Description  |
|--------------------------|--|
| 700-ulmage-pserver_nosig | Must be used to upgrade from previous versions to v7.0.0.    |
| 700-ulmage-pserver_sig   | Must be used to downgrade from versions greater than v7.0.0. |
| 631-ulmage-pserver_sig   | Must be used to downgrade from v7.0.0 only to v6.3.1.        |



### Caution

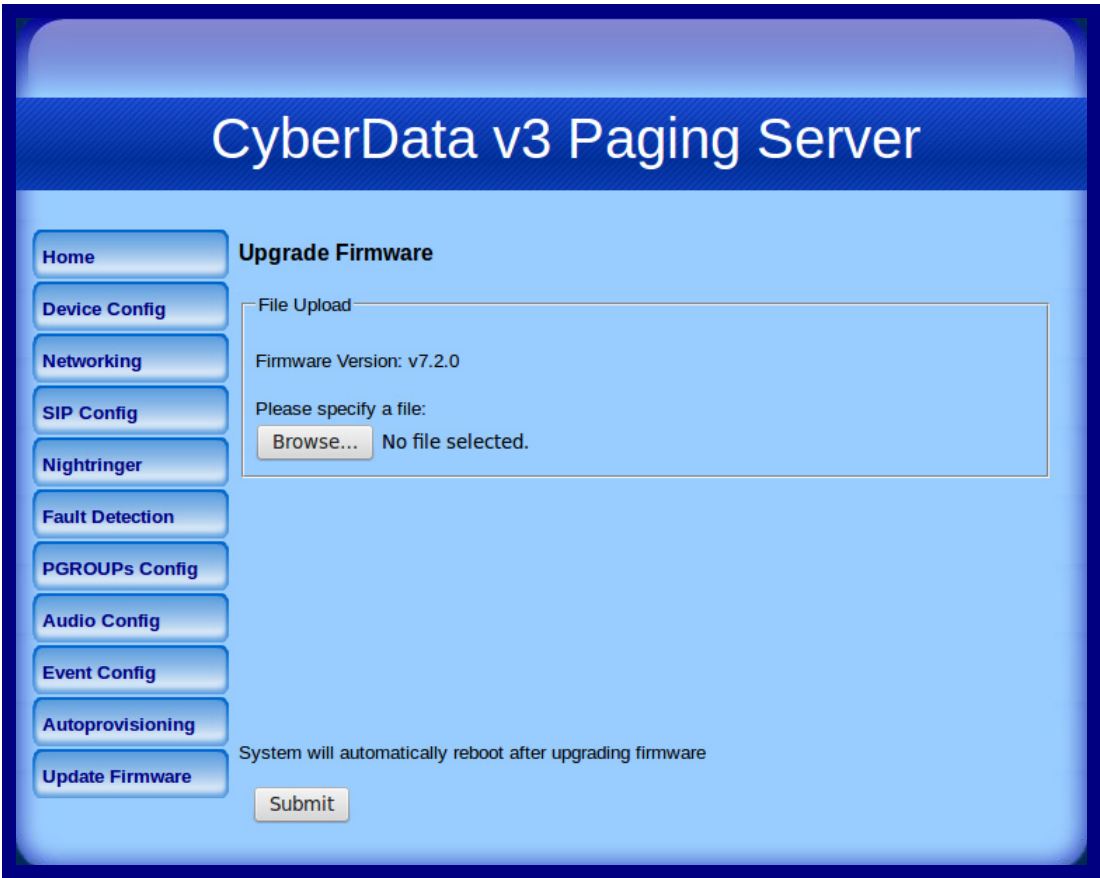
*Equipment Hazard:* Users will not be able to upgrade directly from versions older than v7.0.0 to versions greater than v7.0.0. Users will have to upgrade to v7.0.0 then move on from there.



## 2.5.1 Uploading the Firmware

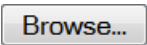

1. Click on the **Update Firmware** button to open the **Upgrade Firmware** page. See [Figure 2-34](#).

Figure 2-34. Upgrade Firmware Page



[Table 2-21](#) shows the web page items on the **Upgrade Firmware** page.

Table 2-21. Upgrade Firmware Parameters

| Web Page Item   | Description   |
|---|---|
| <b>File Upload</b>  |   |
| Firmware Version  | Shows the current firmware version.   |
| Please specify a file   | Click on the <b>Browse</b> button to navigate to the application firmware file that you want to upload. |
|  | The <b>Browse</b> button will allow you to navigate to and select an application firmware file.         |
|  | Click on the <b>Submit</b> button to automatically upload the selected firmware and reboot the system.  |

### 2.5.1.1 Upgrade the Firmware

To upload the firmware from your computer:

1. Retrieve the latest V3 Paging Server firmware from the VoIP V3 Paging Server **Downloads** page at:  
<http://www.cyberdata.net/products/voip/digitalanalog/pagingserverv3/downloads.html>
2. Unzip the V3 Paging Server version file. This file may contain the following:
  - Firmware file
  - Release notes
3. Log in to the V3 Paging Server home page as instructed in [Section 2.4.3, "Log in to the Configuration GUI"](#).
4. Click on the **Update Firmware** button to open the **Upgrade Firmware** page. See [Figure 2-34](#).
5. Click **Browse**, and then navigate to the location of the V3 Paging Server firmware file.
6. Click **Submit**.

**Note** This starts the upload process. Once the V3 Paging Server has uploaded the file, the **Uploading Firmware** countdown page appears, indicating that the firmware is being written to flash. The V3 Paging Server 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).

## 2.5.2 Reboot the V3 Paging Server

To reboot a V3 Paging Server, log in to the web page as instructed in [Section 2.4.3, "Log in to the Configuration GUI"](#).

1. Click **Reboot** ([Figure 2-35](#)). A normal restart will occur.

**Figure 2-35. Home Page**

**CyberData v3 Paging Server**

**Home**

**Device Config**

**Networking**

**SIP Config**

**Nightringer**

**Fault Detection**

**PGROUPs Config**

**Audio Config**

**Event Config**

**Autoprovisioning**

**Update Firmware**

**Device Settings**

Device Name: CyberData Paging Server

Change Username: admin

Change Password:

Re-enter Password:

**Current Settings**

Serial Number: 146001452

Mac Address: 00:20:f7:02:e5:8e

Firmware Version: v7.2.0

Part Number: 011146

IP Addressing: dhcp

IP Address: 10.10.0.105

Subnet Mask: 255.0.0.0

Default Gateway: 10.0.0.1

DNS Server 1: 10.0.0.252

DNS Server 2:

SIP Mode is: enabled

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)

**Import/Export Settings**

Please specify a configuration file\*:

Browse... No file selected. Import Configuration

Export Configuration

\* You need to reboot for changes to take effect

Save Reboot

Reboot

## 2.6 Command Interface

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

### 2.6.1 Command Interface Post Commands

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

**Table 2-22. Command Interface Post Commands<sup>a</sup>**

| Device Action                      | HTTP Post Command <sup>1</sup>   |
|------------------------------------|--|
| Trigger relay (fixed at 5 seconds) | wget --user admin --password admin --auth-no- challenge --quiet -<br>O /dev/null "http://10.0.3.71/cgi- bin/command.cgi" --post-data "test_relay=yes"          |
| Terminate active call              | wget --user admin --password admin --auth-no- challenge --quiet -<br>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 -<br>O /dev/null "http://10.0.3.71/cgi- bin/command.cgi" --post-data "reboot=yes"              |
| Play "audio test message"          | wget --user admin --password admin --auth-no- challenge --quiet -<br>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 -<br>O /dev/null "http://10.0.3.71/cgi- bin/command.cgi" --post-data<br>"speak_ip_address=yes" |
| Play the "0" audio file            | wget --user admin --password admin --auth-no- challenge --quiet -<br>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 -<br>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 -<br>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 -<br>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 -<br>O /dev/null "http://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 --quiet -<br>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 -<br>O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "play_6=yes"          |

**Table 2-22. Command Interface Post Commands<sup>a</sup> (continued)**

|  |   |
|--|---|
| Play the "7" audio file                  | wget --user admin --password admin --auth-no- challenge --quiet -<br>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 -<br>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 -<br>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 -<br>O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data "play_d=yes"                   |
| Play the "Page Tone" audio file          | wget --user admin --password admin --auth-no- challenge --quiet -<br>O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data<br>"play_pagetone=yes"         |
| Play the "Your IP Address Is" audio file | wget --user admin --password admin --auth-no- challenge --quiet -<br>O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data<br>"play_youripaddressis=yes"  |
| Play the "Rebooting" audio file          | wget --user admin --password admin --auth-no- challenge --quiet -<br>O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data<br>"play_rebooting=yes"        |
| Play the "Restoring Default" audio file  | wget --user admin --password admin --auth-no- challenge --quiet -<br>O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data<br>"play_restoringdefault=yes" |
| Play the "Sensor Triggered" audio file   | wget --user admin --password admin --auth-no- challenge --quiet -<br>O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data<br>"play_sensortriggered=yes"  |
| Play the "Night Ring" audio file         | wget --user admin --password admin --auth-no- challenge --quiet -<br>O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data<br>"play_nightring=yes"        |
| Play the "Enter PGROUP" audio file       | wget --user admin --password admin --auth-no- challenge --quiet -<br>O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data<br>"play_enterpgroup=yes"      |
| Play the "Invalid PGROUP" audio file     | wget --user admin --password admin --auth-no- challenge --quiet -<br>O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data<br>"play_invalidpgroup=yes"    |
| Play the "Enter Code" audio file         | wget --user admin --password admin --auth-no- challenge --quiet -<br>O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data<br>"play_entercode=yes"        |
| Play the "Invalid Code" audio file       | wget --user admin --password admin --auth-no- challenge --quiet -<br>O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data<br>"play_invalidcode=yes"      |

**Table 2-22. Command Interface Post Commands<sup>a</sup> (continued)**

|  |   |
|--|---|
| Delete the "0" audio file                  | wget --user admin --password admin --auth-no- challenge --quiet -<br>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 -<br>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 -<br>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 -<br>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 -<br>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 -<br>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 -<br>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 -<br>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 -<br>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 -<br>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 -<br>O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data<br>"delete_audiotest=yes"        |
| Delete the "Page Tone" audio file          | wget --user admin --password admin --auth-no- challenge --quiet -<br>O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data<br>"delete_pagetone=yes"         |
| Delete the "Your IP Address Is" audio file | wget --user admin --password admin --auth-no- challenge --quiet -<br>O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data<br>"delete_youripaddressis=yes"  |
| Delete the "Rebooting" audio file          | wget --user admin --password admin --auth-no- challenge --quiet -<br>O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data<br>"delete_rebooting=yes"        |
| Delete the "Restoring Default" audio file  | wget --user admin --password admin --auth-no- challenge --quiet -<br>O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data<br>"delete_restoringdefault=yes" |

**Table 2-22. Command Interface Post Commands<sup>a</sup> (continued)**

|  |  |
|--|--|
| Delete the "Sensor Triggered" audio file                   | wget --user admin --password admin --auth-no- challenge --quiet -<br>O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data<br>"delete_sensortriggered=yes" |
| Delete the "Night Ring" audio file                         | wget --user admin --password admin --auth-no- challenge --quiet -<br>O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data<br>"delete_nightring=yes"       |
| Delete the "Enter PGROUP" audio file                       | wget --user admin --password admin --auth-no- challenge --quiet -<br>O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data<br>"delete_enterpgroupl=yes"    |
| Delete the "Invalid PGROUP" audio file                     | wget --user admin --password admin --auth-no- challenge --quiet -<br>O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data<br>"delete_invalidpgroup=yes"   |
| Delete the "Enter Code" audio file                         | wget --user admin --password admin --auth-no- challenge --quiet -<br>O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data<br>"delete_entercode=yes"       |
| Delete the "Invalid Code" audio file                       | wget --user admin --password admin --auth-no- challenge --quiet -<br>O /dev/null "http://10.0.3.71/cgi- bin/audioconfig.cgi" --post-data<br>"delete_invalidcode=yes"     |
| Trigger the Fault Detection Test (Fault<br>Detection page) | wget --user admin --password admin --auth-no- challenge --quiet -<br>O /dev/null "http://10.0.3.71/cgi- bin/sensorconfig.cgi" --post-data<br>"intrusiontest=yes"         |

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

# Appendix A: Setting Up a TFTP Server

---

## A.1 Set up a TFTP Server

Autoprovisioning requires a TFTP server for hosting the configuration file.

---

### A.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
```

---

### A.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 Solar Winds freeware TFTP server, which you can download at:

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

To set up a TFTP server on Windows:

1. Install and start the software.
2. Select **File/Configure/Security** tab/**Transmit Only**.

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



# Appendix B: Troubleshooting/Technical Support

---

## B.1 Frequently Asked Questions (FAQ)

Go to the following URL to see CyberData's list of frequently asked questions:

<http://www.cyberdata.net/products/voip/digitalanalog/pagingserverv3/faqs.html>

---

## B.2 Documentation

The documentation for this product is released in an English language version only. You can download PDF copies of CyberData product documentation at:

<http://www.cyberdata.net/products/voip/digitalanalog/pagingserverv3/docs.html>

## B.3 Contact Information

|                                  |   |
|----------------------------------|---|
| Contact                          | <p>CyberData Corporation<br/> 3 Justin Court<br/> Monterey, CA 93940 USA<br/> <a href="http://www.CyberData.net">www.CyberData.net</a><br/> Phone: 800-CYBERDATA (800-292-3732)<br/> Fax: 831-373-4193</p>  |
| Sales                            | <p>Sales 831-373-2601 Extension 334</p>   |
| Technical Support                | <p>The fastest way to get technical support for your VoIP product is to submit a VoIP Technical Support form at the following website:</p> <p><a href="http://support.cyberdata.net/">http://support.cyberdata.net/</a></p> <p>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 <b>Comments</b> section of the Support Form.</p> <p>Phone: (831) 373-2601, Ext. 333<br/> Email: support@cyberdata.net</p> |
| Returned Materials Authorization | <p>To return the product, contact the Returned Materials Authorization (RMA) department:</p> <p>Phone: 831-373-2601, Extension 136<br/> Email: RMA@CyberData.net</p> <p>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:</p> <p>CyberData Corporation<br/> 3 Justin Court<br/> Monterey, CA 93940<br/> Attention: RMA "your RMA number"</p>  |
| RMA Status Form                  | <p>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:</p> <p><a href="http://support.cyberdata.net/">http://support.cyberdata.net/</a></p>   |

---

## B.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** are included under this policy. End of Life devices are devices that are no longer produced or sold. Technical support is still available for these devices. However, no firmware revisions or updates will be provided. If an End of Life device cannot be repaired, the replacement offered may be the current version of the device.

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.

---

### B.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"

---

### B.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.

---

### B.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://support.cyberdata.net/>

---

### B.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.

---

### B.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://support.cyberdata.net/>

# Index

---

## Symbols

+48V DC power supply 10

## Numerics

100 Mbps indicator light 12

## A

activity light 12  
 address, configuration login 16  
 addressing  
     DHCP 14, 26  
     static 14, 26  
 admin username and password 16  
 audio configuration 45  
     night ring tone parameter 48  
 audio configuration page 45  
 audio ground reference 8  
 audio output 8  
 authenticate ID and password for SIP server  
     registration 29  
 Autoprovision at time (HHMMSS) 58  
 autoprovision at time (HHMMSS) 58  
 autoprovision when idle (in minutes > 10) 58  
 autoprovisioning 58, 59  
     get autoprovisioning template button 58  
 autoprovisioning autoupdate (in minutes) 58  
 autoprovisioning configuration 57, 58  
 autoprovisioning filename 58  
 autoprovisioning server (IP Address) 58

## B

backup SIP server 1 28  
 backup SIP server 2 28  
 backup SIP servers, SIP server  
     backups 28  
 beep on page setting 21

## C

cat 5 ethernet cable 10

changing  
     the web access password 20  
 changing default username and password for  
     configuration GUI 16  
 Chrome (web browser) 3  
 Cisco SRST 28  
 command interface 76  
 commands 76  
 configurable parameters 18, 21, 25  
 configuration 18  
     beep on page setting 21  
 configuration information 14  
 configuration page  
     configurable parameters 18, 21, 25  
 connecting the V3 paging server 7  
 connection speed 12  
     specification 4  
     verifying 12  
 connector (removable) 9  
 contact information 82  
 contact information for CyberData 82  
 Current Network Settings 25  
 current network settings 25  
 current settings, reviewing 19  
 CyberData contact information 82

## D

default  
     gateway 13  
     IP address 13  
     subnet mask 13  
     username and password 13  
 default gateway 13, 25  
 default gateway for static addressing 26  
 default login address 16  
 default password for configuration GUI 16  
 default settings, restoring 13  
 default username and password for configuration GUI 16  
 device configuration 20  
     beep on page setting 21  
     device configuration parameters 58  
     the device configuration page 57  
 device configuration page 20  
 device configuration parameters 21  
 device configuration password  
     changing for web configuration access 20  
 DHCP addressing 14, 26  
 DHCP IP addressing 25  
 dimensions 4

- discovery utility program 16
- DNS server 25
- door sensor 48
- DTMF duration (milliseconds) 21

## E

- enable night ring events 53
- ethernet port 10
- event configuration
  - enable night ring events 53
- expiration time for SIP server lease 28, 29, 32
- export configuration button 18
- export settings 18

## F

- fault sense input, sensor 8
- features 3
- Firefox (web browser) 3
- firmware
  - where to get the latest firmware 74
- firmware signature 72
- firmware upgrade parameters 73
- firmware, upgrade 72

## G

- get autoprovisioning template 58
- get autoprovisioning template button 58
- GMT table 70
- GMT time 70
- ground connection 7
- GUI username and password 16

## H

- hazard levels 4
- http POST command 76

## I

- identifier names (PST, EDT, IST, MUT) 70
- identifying your product 2
- import configuration button 18
- import settings 18
- import/export settings 18

- importing and exporting the device's configuration 18
- input specifications 4
- Internet Explorer (web browser) 3
- IP address 13, 25
  - SIP server 29
- IP addressing 25
  - default
    - IP addressing setting 13

## L

- lease, SIP server expiration time 28, 29, 32
- line input specifications 4
- line output specifications 4
- line-in 7
- line-in to multicast setting
  - multicast, line-in to multicast setting
    - line-in, line-in to multicast setting 21
- line-out 7
- link light 12
- Linux, setting up a TFTP server on 80
- local SIP port 28, 29
- log in address 16
- logging in to configuration GUI 16

## M

- MGROUP 35
- Mozilla Firefox (web browser) 3
- multicast
  - play line-in audio via multicast 34
  - play stored audio via multicast 34
- multicast address 34
- multicast port 34
- multicast TTL 43

## N

- navigation (web page) 15
- navigation table 15
- network activity, verifying 12
- network configuration page 24
- network parameters, configuring 24
- network setup button 24
- network, connecting to 11
- Nightringer 31, 68
- Nightringer in peer to peer mode (cannot be used) 31
- nightringer settings 32
- Nightringer, SIP registration required 31
- NTP server 58, 59

## O

orange link LED 12  
out of band 44  
output specifications 4

## P

page port 8  
page port output connections 8  
paging server  
    configuration 14  
part number 4  
parts list 5  
password  
    configuration GUI 14, 16  
    for SIP server login 28  
    restoring the default 13  
    SIP server authentication 29  
pgroups 35  
pin descriptions and functions 8  
point-to-point configuration 30  
polycom transmit channel 22  
polycom, enable polycom paging on multicast 22  
port  
    ethernet 10  
    local SIP 28, 29  
    remote SIP 28, 29  
posix timezone string  
    timezone string 59  
POST command 76  
power  
    connecting to 10  
    requirement 4  
product overview 1

## R

reboot 73, 75  
    unregistering from SIP server during 29  
registration and expiration, SIP server  
    lease expiration 29  
regulatory compliance 4  
relay 8  
relay contact 8  
remote SIP port 28, 29  
required configuration for web access username and  
    password 14, 16  
resetting the IP address to the default 81  
restoring factory default settings 13  
return and restocking policy 84  
RFC2833 RTP events 44

RMA returned materials authorization 82  
RMA status 82  
rport discovery 28

## S

Safari (web browser) 3  
safety instructions 5  
sales 82  
server  
    TFTP 80  
server address, SIP 28  
service 82  
set the time from the NTP server 59  
SIP  
    enable SIP operation 28  
    local SIP port 28  
    user ID 28  
SIP configuration  
    SIP Server 28  
SIP configuration page 27  
SIP configuration parameters 28  
    outbound proxy 28, 32  
    registration and expiration, SIP server lease 28, 32  
    unregister on reboot 28  
    user ID, SIP 28  
SIP registration 28  
SIP remote SIP port 28  
SIP server 28  
    password for login 28  
    unregister from 28  
    user ID for login 28  
SIP server parameters, configuring 14  
SIP settings 28, 29  
SIP setup button 27  
Spare in the Air Policy 84  
specifications 4  
SRST 28  
static addressing 14, 26  
static IP addressing 25  
status light 12  
Stored Network Settings 25  
subnet mask 13, 25  
subnet mask static addressing 26  
supported protocols 4

## T

tech support 82  
technical support, contact information 82  
TFTP server 80  
time zone string examples 70

## U

- unregister from SIP server 29
- upgrade firmware 72
- user ID
  - for SIP server login 28
- user ID for SIP server registration 29
- username
  - changing for web configuration access 20
  - restoring the default 13
- username for configuration GUI 14, 16

## V

- verifying
  - connection speed 12
  - network activity 12
  - network connectivity 12
- VLAN ID 25
- VLAN Priority 25
- VLAN tagging support 25
- VLAN tags 25

## W

- warranty 83
- warranty & RMA returns outside of the United States 83
- warranty and RMA returns page 84
- warranty policy at CyberData 83
- web access password 13
- web access username 13
- web configuration log in address 16
- web page
  - navigation 15
- web page navigation 15
- weight 4
- wget, free unix utility 76
- Windows, setting up a TFTP server on 80