



# *SIP Paging Server Operations Guide*

*SIP Compliant  
Part #011146*

Document Part #931803C  
for Firmware Version 20.1.0

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

---

**Operations Guide 931803C**  
**SIP Compliant 011146**

**COPYRIGHT NOTICE:**

© 2022, 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:  
<https://support.cyberdata.net/>

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 931803C, which corresponds to firmware version 20.1.0, was released on May 16, 2022, and has the following changes:

- Updates [Section 1.2, "Features"](#) with the following changes:
  - Adds [Audio controlled relay/remote amplifier enable](#)
  - Adds [Web-based upgradeable firmware](#)
- Updates [Table 1-1, "Product Specifications"](#) with the following changes:
  - Updates [Network Security: TLS 1.2, SRTP, HTTPS](#)
  - Updates [Compliance: CE: EMC Directive – Class A EN 55032 & EN 55024, LV Safety Directive – EN 62368-1; RoHS Compliant; FCC Part 15 Class A; Industry Canada ICES-3 Class A; IEEE 802.3 Compliant; TAA Compliant](#)
- [IP Address: 192.168.1.23](#) Updates [Table 2-2, "Factory Default Settings"](#) with the following change:
  - [IP Address: 192.168.1.23](#)
  - [Subnet Mask: 255.255.255.0](#)
  - [Default Gateway: 192.168.1.1](#)
- Updates [Section 2.6.4, "Log in to the Configuration GUI"](#) with the following change:
  - [Note: If the network does not have access to a DHCP server, the device will default to an IP address of 192.168.1.23.](#)

---

## 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.

 GENERAL ALERT	<b>Warning</b> <i>Electrical Hazard:</i> This product should be installed by a licensed electrician according to all local electrical and building codes.
 GENERAL ALERT	<b>Warning</b> <i>Electrical Hazard:</i> To prevent injury, this apparatus must be securely attached to the floor/wall in accordance with the installation instructions.
 GENERAL ALERT	<b>Warning</b> 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
SRTP	Secure Real Time 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 .....	1
1.2 Features .....	2
1.3 Specifications .....	3
1.4 Compliance .....	4
1.4.1 CE Statement .....	4
1.4.2 FCC Statement .....	4
1.4.3 Industry Canada (IC) Compliance Statement .....	4
 <b>Chapter 2 Setting Up the SIP Paging Server</b>	 <b>5</b>
2.1 Parts List .....	5
2.2 Typical Installation .....	6
2.3 Connecting the SIP 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
Non-Poe .....	10
Chassis Ground .....	10
Poe .....	10
2.3.7 Connect to the Network .....	11
2.3.8 Confirm that the SIP Paging Server is Up and Running .....	12
Verify Network Activity .....	12
2.4 Announcing the IP Address .....	13
2.5 Restore the Factory Default Settings .....	14
2.6 Configuring the SIP Paging Server .....	15
2.6.1 Gather the Required Configuration Information .....	15
Static or DHCP Addressing? .....	15
Username and Password for Configuration GUI .....	15
SIP Settings .....	15
2.6.2 SIP Paging Server Web Page Navigation .....	16
2.6.3 Using the Toggle Help Button .....	17
2.6.4 Log in to the Configuration GUI .....	19
2.6.5 Configure the Device Parameters .....	23
Polycom Paging .....	25
2.6.6 Configure the Network Parameters .....	27
2.6.7 Configure the SIP Parameters .....	30
Point-to-Point Configuration .....	35
Point-to-Point Fault Sense Reporting .....	36
2.6.8 Configure the Paging Groups (PGROUPS) Parameters .....	38
2.6.9 Operating the Paging Server .....	42
DTMF Bypassed .....	42
DTMF Not Bypassed .....	42
2.6.10 Configure the SSL Parameters .....	43
Certificate Info Window .....	47
Remove Server Certificate Window .....	48

2.6.11 Configure the Schedules Parameters .....	49
2.6.12 Configure the Fault Detection Parameters .....	53
2.6.13 Configure the Audio Parameters .....	55
User-created Audio Files .....	60
2.6.14 Configure the Event Parameters .....	63
Example Packets for Events .....	65
2.6.15 Configure the Autoprovisioning Parameters .....	68
Autoprovisioning .....	70
Sample dhcpd.conf .....	78
Get Autoprovisioning Template Button .....	79
2.7 Upgrade the Firmware .....	80
2.7.1 Reboot the SIP Paging Server .....	83
2.8.1 Command Interface Post Commands .....	84

<b>Appendix A Troubleshooting/Technical Support .....</b>	<b>85</b>
A.1 Frequently Asked Questions (FAQ) .....	85
A.2 Documentation .....	85
A.3 Contact Information .....	86
A.4 Warranty and RMA Information .....	86



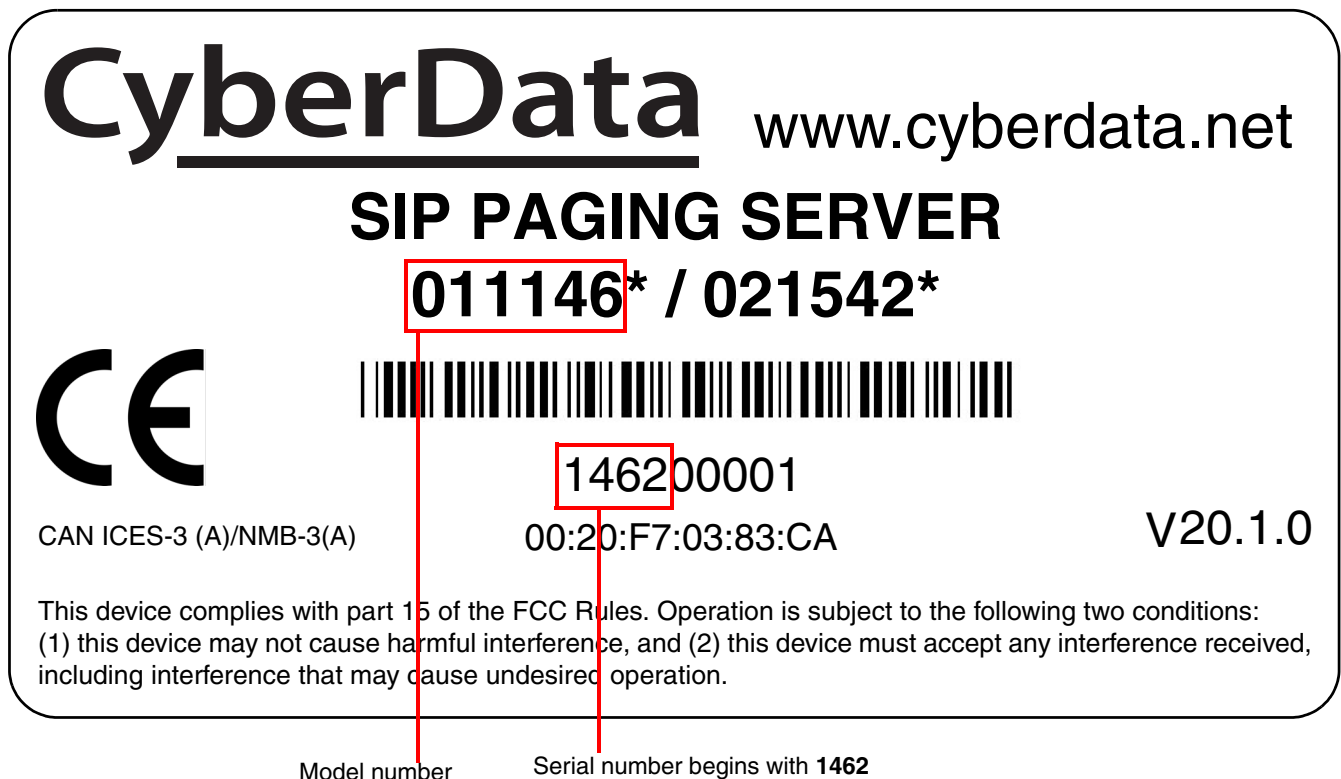
# 1 Product Overview

## 1.1 How to Identify This Product

To identify the SIP Paging Server, look for a model number label similar to the one shown in [Figure 1-1](#). Confirm the following:

- The model number on the label should be **011146**.
- The serial number on the label should begin with **1462**.

**Figure 1-1. Model Number Label<sup>1</sup>**



1. This figure is just an example. The information on your label may look different.

---

## 1.2 Features

- Up to 25 unique user uploadable bell files that can be used in up to 250 scheduled events
  - Up to 25 stored messages can be played through paging groups
  - Voice prompting and password controlled zones
  - DTMF control of zone selection
  - Paging Prioritization
  - Loud/Night Ringer function - second SIP extension
  - Supports user-uploadable ring and alert tones, with the option to send a stored message with each of the 100 page groups
  - Supports delayed pages with call buffering
  - Support for security code to prevent unwanted SIP calls
  - Can send multicast to Poly phones
- 
- Fault sense input
  - Line-in for background music
  - Line-out connector
  - NTP-based internal clock
  - Audio controlled relay/remote amplifier enable
  - DTMF pass-through
  - Rack mountable
- 
- TLS 1.2 and SRTP enhanced security for IP Endpoints in a local or cloud-based environment
  - Web-based upgradeable firmware
  - HTTPS or HTTP web based configuration. HTTPS is enabled by default.
  - Support for Cisco SRST resiliency
  - Autoprovisioning via HTTPS, HTTP or TFTP
  - Configurable event generation for device health and status monitoring
  - 802.11q VLAN tagging

## 1.3 Specifications

**Table 1-1. Product Specifications**

Specifications	
Ethernet I/F	10/100 Mbps
Protocol	SIP RFC 3261 Compatible
Power Input	PoE 802.3af or 48VDC
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
Page Port Output	Balanced 600 Ohm 5VPP
Payload Types	G.711 a-law, G.711 $\mu$ -law, G.722, and G.729
Network Security	TLS 1.2, SRTP, HTTPS
Operating Range	Temperature: -40° C to 55° C (-40° F to 131° F) Humidity: 5-95%, non-condensing
Storage Temperature	-40° C to 70° C (-40° F to 158° F)
Storage Altitude	Up to 15,000 ft. (4573 m)
Dimensions <sup>a</sup>	6.11 inches [155.19 mm] Length 4.05 inches [102.87 mm] Width 1.15 inches [29.21 mm] Height
Weight	1.2 lbs. [.54 kg]
Boxed Weight	1.8 lbs. [.82 kg]
Compliance	CE: EMC Directive – Class A EN 55032 & EN 55024, LV Safety Directive – EN 62368-1; RoHS Compliant; FCC Part 15 Class A; Industry Canada ICES-3 Class A; IEEE 802.3 Compliant; TAA Compliant
Warranty	2 Years Limited
Part Number	011146

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

---

## 1.4 Compliance

---

### 1.4.1 CE Statement



As of the date of manufacture, the Paging Series has been tested and found to comply with the specifications for CE marking and standards per EMC and Radio communications Compliance. This applies to the following products: 011145, 011146, 011233, 011280, 011295, 011314, 011368, and 011372.

EMC Directive - Class A Emissions, Immunity, and LV Safety Directive, RoHS Compliant.  
Flammability rating on all components is 94V-0.

---

### 1.4.2 FCC Statement



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

**CAUTION:** Changes or modifications not expressly approved by the manufacturer responsible for compliance could void the user's authority to operate the equipment.

---

### 1.4.3 Industry Canada (IC) Compliance Statement

Operation is subject to the following two conditions:

1. This device may not cause interference, and
2. This device must accept any interference, including interference that may cause undesired operations of the device.

ICES-3 Class A



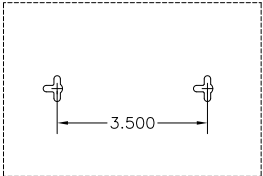

## 2 Setting Up the SIP Paging Server

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

### 2.1 Parts List

The packaging for the SIP Paging Server includes the parts in [Table 2-1](#).

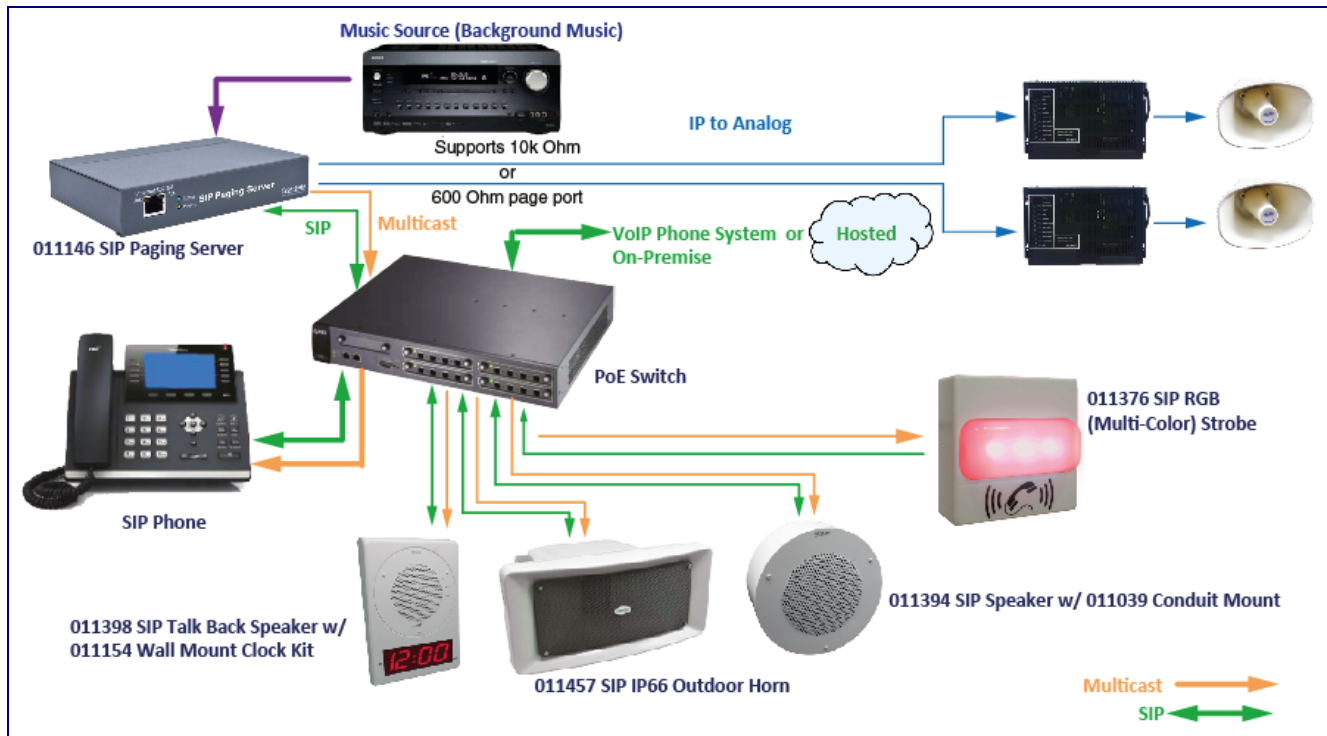
**Table 2-1. Parts List**

Quantity	Part Name	Illustration
1	SIP 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: (2) #4-6 x 7/8" Mounting Anchors (2) #4 x 1-1/4" Round Phillips Wood Screws	

## 2.2 Typical Installation

Figure 2-1 illustrates how the SIP Paging Server is normally installed as part of a paging system.

**Figure 2-1. Typical Installation**

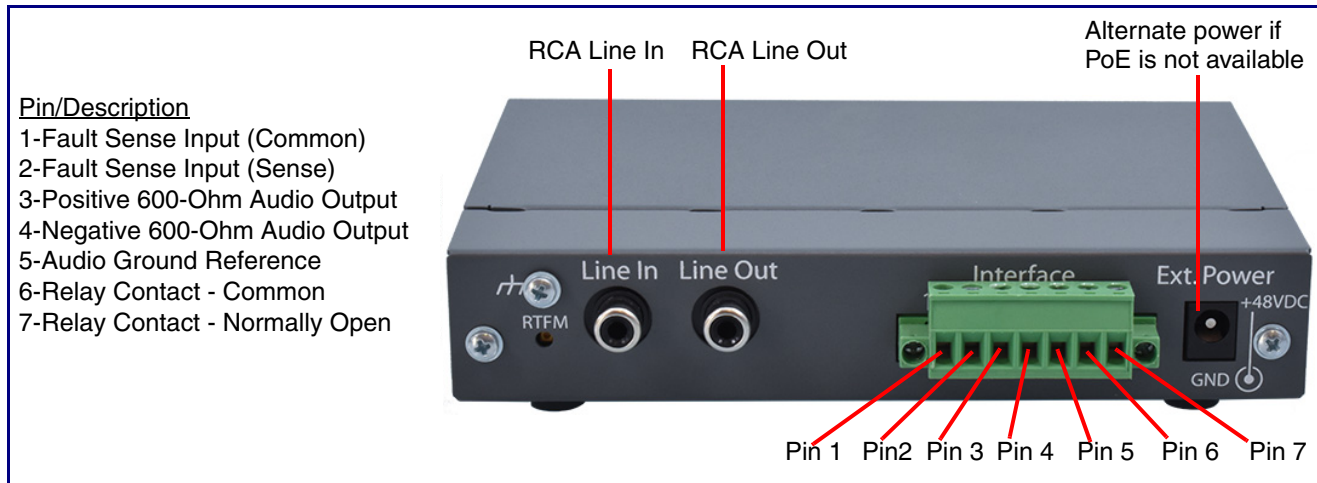


## 2.3 Connecting the SIP Paging Server

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

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

**Figure 2-2. Connection Options**



This equipment may be sensitive to ESD discharges. A certain level of performance might be impacted if this happens. Please take this precaution when installing and operating the equipment.

### 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 2.6.12, "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 2.6.12, "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)

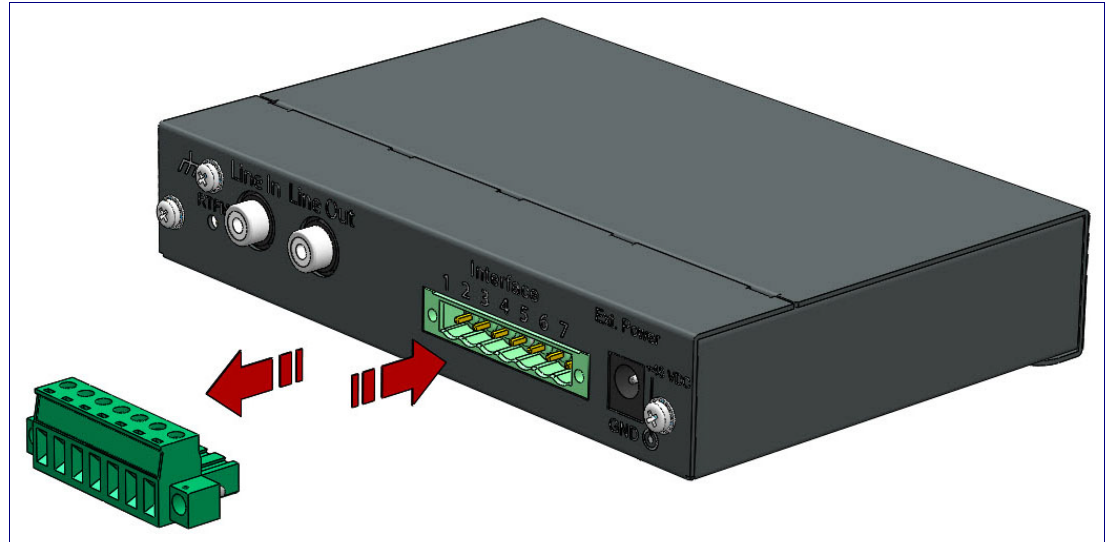
When enabled on the web interface ([Section 2.6.5, "Configure the Device Parameters"](#)), every time an audio file is played out of the local line-out or 600 Ohm output, the relay will close, thereby enabling amplifiers with a remote turn-on capability to become active.



## 2.3.5 Removable Interface Connector

Figure 2-3 shows the interface connector that is removable on the SIP Paging Server.

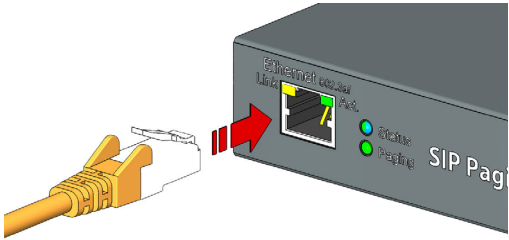
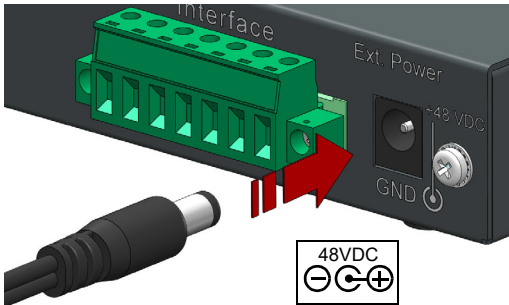
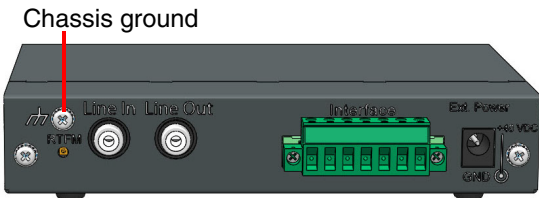
**Figure 2-3. Removable Interface Connector**



## 2.3.6 Connect to the Power Source

To use PoE, plug a Cat 5 Ethernet cable from the SIP 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 2-4](#).

**Figure 2-4. Connecting to the Power Source**

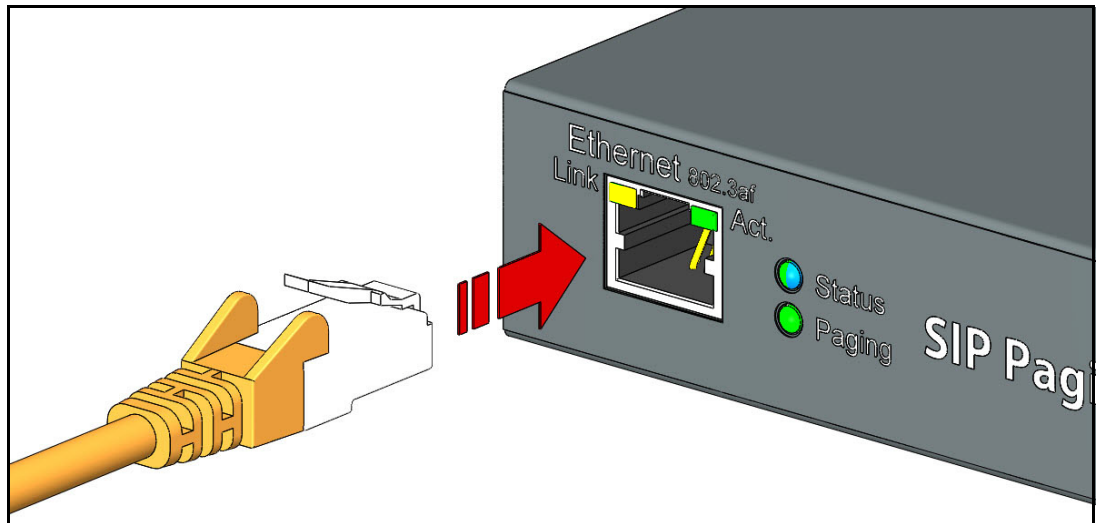
<p><b>PoE</b></p> 	<p>To set up the device, connect the device to your network:</p> <p><b>Poe</b></p> <ul style="list-style-type: none"> <li>For PoE, plug one end of an 802.3af Ethernet cable into the SIP Paging Server Ethernet port. Plug the other end of the Ethernet cable into your network. See the 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 Non-PoE, connect the SIP Paging Server to a 48VDC power supply. See the figure on the left.</li> <li><b>Note:</b> Do not use both PoE and external power.</li> </ul>
<p><b>Chassis Ground</b></p> 	<p><b>Chassis Ground</b></p> <ul style="list-style-type: none"> <li>If required, connect the earth grounding wire to the Chassis Ground. 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 SIP Paging Adapter **Ethernet** port. Plug the other end into your network.

**Figure 2-5. Connecting to the Network**



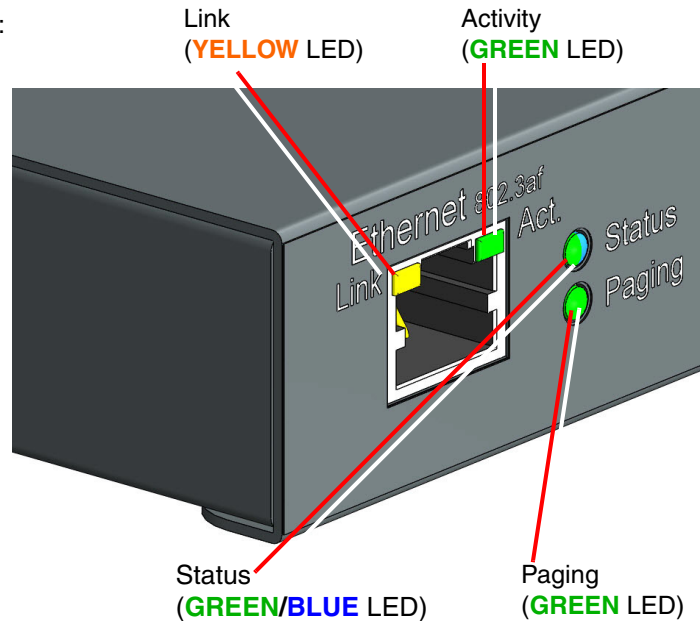
## 2.3.8 Confirm that the SIP Paging Server is Up and Running

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

**Figure 2-6. SIP Paging Adapter LEDs**

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 SIP 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, **YELLOW Link** LED above the Ethernet port indicates that the network connection has been established at 100Mbit speed.
- 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.



### 2.3.8.1 Verify Network Activity

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

## 2.4 Announcing the IP Address

To announce the IP address for the SIP Paging Server, briefly press and then quickly release the **RTFM** switch. See [Figure 2-7](#).

**Note** The IP address announcement can be heard if a speaker or amplified speaker is connected to the unit.

**Figure 2-7. RTFM Switch**



## 2.5 Restore the Factory Default Settings

The SIP Paging Server is delivered with factory set default values for the parameters in [Table 2-2](#). Use the **RTFM** switch (see [Figure 2-8](#)) on the back of the unit to restore these parameters to the factory default settings.

**Figure 2-8. RTFM Switch**



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

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

Parameter	Factory Default Setting
IP Addressing	DHCP
IP Address <sup>a</sup>	192.168.1.23
Web Access Username	admin
Web Access Password	admin
Subnet Mask <sup>a</sup>	255.255.255.0
Default Gateway <sup>a</sup>	192.168.1.1

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 switch until after the indicator lights go off, and then release it.

**Note** The “Restoring Defaults” announcement can be heard if a speaker or amplified speaker is connected to the unit.

3. The SIP Paging Server settings are restored to the factory defaults.

---

## 2.6 Configuring the SIP Paging Server

Use this section to configure the VoIP paging server.

---

### 2.6.1 Gather the Required Configuration Information

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

#### 2.6.1.1 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 SIP Paging Server parameters:

- IP Address
- Subnet Mask
- Default Gateway

#### 2.6.1.2 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.

#### 2.6.1.3 SIP Settings

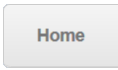
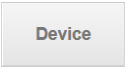
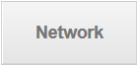

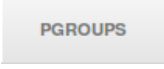

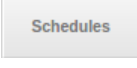
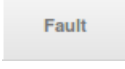
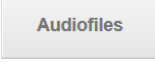

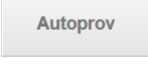
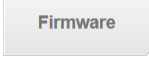
To configure the SIP parameters, determine whether you want to register with the server. If you do, determine the number of minutes the registration lease remains valid, and whether you want to automatically unregister when you reboot. To configure the SIP parameters, you also need to determine the values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

## 2.6.2 SIP Paging Server Web Page Navigation

Table 2-3 shows the navigation buttons that you will see on every SIP Paging Server web page.

**Table 2-3. Web Page Navigation**

Web Page Item	Description
	Link to the <b>Home</b> page.
	Link to the <b>Device</b> page.
	Link to the <b>Network</b> page.
	Link to go to the <b>SIP</b> page.
	Link to the <b>PGROUPS</b> page.
	Link to the <b>SSL</b> page.
	Link to the <b>Schedules</b> page.
	Link to the <b>Fault</b> page.
	Link to the <b>Audiofiles</b> page.
	Link to the <b>Events</b> page.
	Link to the <b>Autoprovisioning</b> page.
	Link to the <b>Firmware</b> page.



## 2.6.3 Using the Toggle Help Button

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

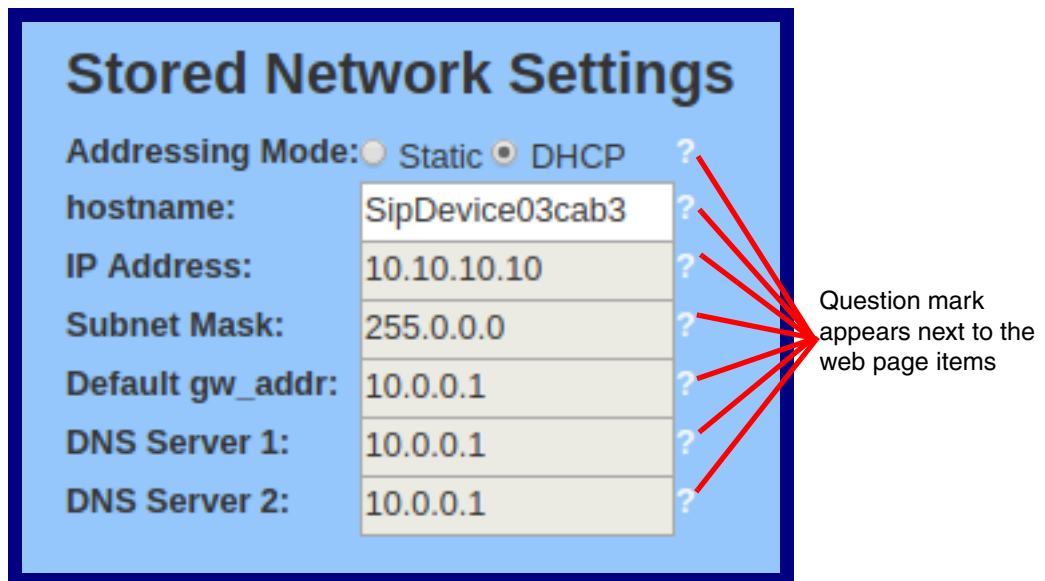
1. Click on the **Toggle Help** button that is on the UI webpage. See [Figure 2-9](#) and [Figure 2-10](#).

**Figure 2-9. Toggle/Help Button**



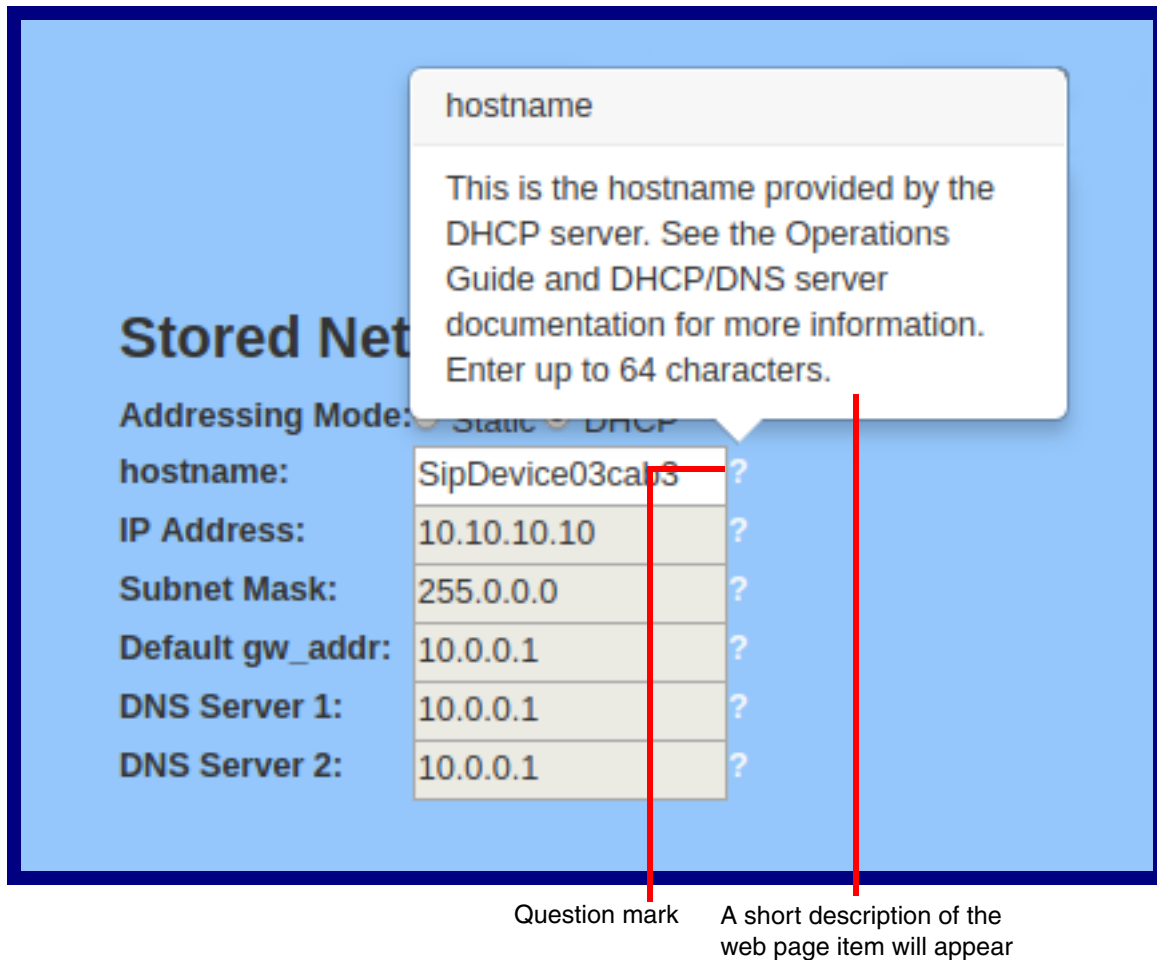
2. You will see a question mark (?) appear next to each web page item that has been provided with a short description by the Help feature. See [Figure 2-10](#).

**Figure 2-10. Toggle Help Button and Question Marks**



3. Move the mouse pointer to hover over the question mark (?), and a short description of the web page item will appear. See [Figure 2-11](#).

**Figure 2-11. Short Description Provided by the Help Feature**



---

## 2.6.4 Log in to the Configuration GUI

1. Open your browser to the SIP 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 192.168.1.23.

**Note** Make sure that the PC is on the same IP network as the SIP 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 **Downloads** tab on the following webpage:

<https://www.cyberdata.net/products/011146>

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 SIP Paging Server configuration *after* the initial configuration, log in using the IP address you assign to the device. [Section 2.6.6, "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 2-12. Home Page

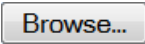


The screenshot shows the 'Home' page of the CyberData Paging Server configuration interface. At the top is a navigation bar with tabs: Home, Device, Network, SIP, PGROUPS, SSL, Schedules, Fault, Audiofiles, Events, Autoprovisioning, and Firmware. The 'Home' tab is selected. Below the navigation bar is a large heading 'CyberData Paging Server'. The main content area is divided into three columns. The left column, 'Current Status', displays system information: Serial Number (146200001), Mac Address (00:20:17:04:79:0d), Firmware Version (v20.1.0), Partition 2 (v20.1.0), Partition 3 (v20.1.0), and Booting From (partition 3). It includes a 'Boot From Other Partition' button. The middle column, 'Admin Settings', contains fields for Username (admin), Password (masked with asterisks), and Confirm Password (masked with asterisks), along with 'Save', 'Reboot', and 'Toggle Help' buttons. The right column has two sections: 'Import Settings' with a 'Browse...' button (showing 'No file chosen') and an 'Import Config' button; and 'Export Settings' with an 'Export Config' button. A bottom section of the left column lists network settings: IP Addressing (DHCP), IP Address (10.10.0.27), Subnet Mask (255.0.0.0), Default Gateway (10.0.0.1), DNS Server 1 (10.0.1.56), and DNS Server 2. Another section lists SIP-related settings: SIP Mode (Enabled), Multicast Mode (Disabled), Event Reporting (Disabled), Nightringer (Disabled), Primary SIP Server (Registered), Backup Server 1 (Not registered), Backup Server 2 (Not registered), and Nightringer Server (Not registered).

Category	Item	Value
Current Status	Serial Number:	146200001
	Mac Address:	00:20:17:04:79:0d
	Firmware Version:	v20.1.0
	Partition 2:	v20.1.0
	Partition 3:	v20.1.0
	Booting From:	partition 3
Admin Settings	Username:	admin
	Password:	*****
	Confirm Password:	*****
Network Settings	IP Addressing:	DHCP
	IP Address:	10.10.0.27
	Subnet Mask:	255.0.0.0
	Default Gateway:	10.0.0.1
	DNS Server 1:	10.0.1.56
	DNS Server 2:	
	SIP Settings	SIP Mode:
Multicast Mode:		Disabled
Event Reporting:		Disabled
Nightringer:		Disabled
Primary SIP Server:		Registered
Backup Server 1:		Not registered
Backup Server 2:		Not registered
Nightringer Server:		Not registered



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

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

**Table 2-4. Home Page Overview**

Web Page Item	Description
<b>Admin Settings</b>	
Username ?	The username to access the web interface. Enter up to 25 characters.
Password ?	The password to access the web interface. Enter up to 25 characters.
Confirm Password ?	Confirm the web interface password.
<b>Current Status</b>	
Serial Number	Shows the device serial number.
Mac Address	Shows the device Mac address.
Firmware Version	Shows the current firmware version.
IP Addressing	Shows the current IP addressing setting ( <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	Shows the current status of the SIP mode.
Event Reporting	Shows the current status of the Event Reporting mode.
Nightringer	Shows the current status of the Nightringer mode.
Primary SIP Server	Shows the current status of the Primary SIP Server.
Backup Server 1	Shows the current status of Backup Server 1.
Backup Server 2	Shows the current status of Backup Server 2.
Nightringer Server	Shows the current status of Nightringer Server.
<b>Import Settings</b>	
	Use this button to select a configuration file to import.
	After selecting a configuration file, click Import to import the configuration from the selected file.
<b>Export Settings</b>	
	Click Export to export the current configuration to a file.
	Click the <b>Save</b> button to save your configuration settings.

**Table 2-4. Home Page Overview (continued)**

Web Page Item	Description
	Click on the <b>Reboot</b> button to reboot the system.
	Click on the <b>Toggle Help</b> button to see a short description of some of the web page items. First click on the <b>Toggle Help</b> button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

At this point you can:

- Review the SIP Paging Server's **Current Settings**. Use the RTFM switch to restore the factory default settings. See [Section 2.5, "Restore the Factory Default Settings"](#).
- Configure the device parameters. Click on the **Device** button and see [Section 2.6.5, "Configure the Device Parameters"](#) for instructions.
- Configure the network parameters. Click on the **Network** button and see [Section 2.6.6, "Configure the Network Parameters"](#) for instructions.
- Configure the SIP parameters. Click on the **SIP** button and see [Section 2.6.7, "Configure the SIP Parameters"](#) for instructions.
- Configure the PGROUPS parameters. Click on the **PGROUPS** button and see [Section 2.6.8, "Configure the Paging Groups \(PGROUPS\) Parameters"](#) for instructions.
- Configure the fault detection parameters. Click on the **Fault** button and see [Section 2.6.12, "Configure the Fault Detection Parameters"](#) for instructions.
- Configure the audio parameters. Click on the **Audiofiles** button and see [Section 2.6.13, "Configure the Audio Parameters"](#) for instructions.
- Configure the event parameters. Click on the **Events** button and see [Section 2.6.14, "Configure the Event Parameters"](#) for instructions.
- Configure the autoprovisioning parameters. Click on the **Autoprov** button and see [Section 2.6.15, "Configure the Autoprovisioning Parameters"](#) for instructions.

**Note** Click on the **Firmware** button any time you need to upload new versions of the firmware. See [Section 2.7, "Upgrade the Firmware"](#) for instructions.

## 2.6.5 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** button to open the **Device** page. See [Figure 2-13](#).

**Figure 2-13. Device Page**

The screenshot shows the 'Device' configuration page for the CyberData Paging Server. The navigation bar at the top includes tabs for Home, Device, Network, SIP, PGROUPS, SSL, Schedules, Fault, Audiofiles, Events, Autoprov, and Firmware. The main heading is 'CyberData Paging Server'.

**Line-in Settings**

- Enable Line-in to Line-out Loopback: ☐
- Enable Line-in to Multicast: ☐
- Multicast Address:
- Multicast Port:
- Detect Line-in Silence: ☐
- Volume:

**Relay Settings**

- Activate Relay on Local Audio: ☐

**Clock Settings**

- Enable NTP: ☒
- NTP Server:
- Timezone:
- Current Time: Wed, 17 Nov 2021 08:54:43

**Misc Settings**

- Device Name:
- Bypass DTMF Menus: ☐
- Beep on Init: ☐
- Beep Before Page: ☐
- Enable Polycom Paging on Multicast: ☐
- Polycom Transmit Channel:
- Disable HTTPS (NOT recommended): ☐

At the bottom of the page, there are buttons for 'Test Audio', 'Test Relay', 'Test Multicast', 'Save', 'Reboot', and 'Toggle Help'.

2. On the **Device** page, you may enter values for the parameters indicated in [Table 2-5](#).









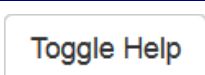

**Note** The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

**Table 2-5. Device Configuration Parameters**

Web Page Item	Description
<b>Line-in Settings</b>	
Enable Line-in to Line-out Loopback ?	Line-in audio will play back out the device's audio output ports. This is the lowest priority audio and will be preempted by any other audio stream.
Enable Line-in to Multicast ?	Line-in audio will be sent to the specified multicast address and port. Playback priority is determined by receiver(s) Cannot be combined with <b>Play Line-in Audio via Multicast (Fault Detection)</b>
Multicast Address ?	Address line-in audio will be sent to.
Multicast Port ?	Port line-in audio will be sent to (1-65535).
Detect Line-in Silence ?	If audio drops below a threshold on line-input, the fault line-in multicast stream will be stopped to reduce network traffic.
Volume	Volume setting for the line-in (0-127). <sup>a</sup>
<b>Relay Settings</b>	
Activate Relay on Local Audio ?	The relay will be activated (closed) when the device is playing audio. Use this to activate an external amplifier when the device is playing audio.
<b>Clock Settings</b>	
Enable NTP ?	Sync device's local time with the specified NTP Server.
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.
Timezone	Enter the tz database string of your timezone. Examples: America/Los_Angeles America/New_York Europe/London America/Toronto See <a href="https://en.wikipedia.org/wiki/List_of_tz_database_time_zones">https://en.wikipedia.org/wiki/List_of_tz_database_time_zones</a> for a full list of valid strings.
Current Time	Displays the current time.
<b>Misc Settings</b>	
Device Name ?	Type the device name. Enter up to 25 characters.
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
DTMF Duration ?	The duration, in milliseconds, of DTMF tones played out of the device's analog audio ports (1-65535).
Beep on Init ?	Device will play the user defined "pagetone" audio file when it boots.
Beep on Page ?	Device will play the user defined "pagetone" audio file before playing a SIP page.



**Table 2-5. Device Configuration Parameters (continued)**

Web Page Item	Description
Enable Polycom Paging on Multicast 	Enabling Polycom Paging will result in a standard RTP multicast being sent to the specified address and port and a Polycom Group Paging multicast being sent to the specified address and port+1.
Polycom Transmit Channel 	Destination channel for Polycom Group Paging multicast.
Disable HTTPS (NOT recommended) 	Disables the encrypted connection to the webpage. We do not recommend disabling HTTPS for security reasons.
	Click on the <b>Test Audio</b> button to do an audio test. When the <b>Test Audio</b> button is pressed, you will hear a voice message for testing the device audio quality and volume.
	This button will cause the device to send a 5 second ULAW multicast stream to 234.2.1.200:2200.
	Click on the <b>Test Relay</b> button to do a relay test.
	Click the <b>Save</b> button to save your configuration settings.
	Click on the <b>Reboot</b> button to reboot the system.
	Click on the <b>Toggle Help</b> button to see a short description of some of the web page items. First click on the <b>Toggle Help</b> button, and you will see a question mark (  ) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

a. This volume feature is only available on SIP Paging Servers with a serial number of 146202XXX or greater.

### 2.6.5.1 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 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 Page](#).
2. Specify the Polycom IP address and use the next lower even port number for the desired paging group on the [PGROUPS Page](#).
3. Click on the **Save** button to store changes.

## 2.6.6 Configure the Network Parameters

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

Figure 2-14. Network Page

HomeDeviceNetworkSIPPGROUPSSSLSchedulesFaultAudiofilesEventsAutoprovFirmware

CyberData Paging Server

Stored Network Settings

Addressing Mode:

Static

DHCP

Hostname:

SipDevice0462a9

IP Address:

10.10.10.10

Subnet Mask:

255.0.0.0

Default Gateway:

10.0.0.1

DNS Server 1:

10.0.0.1

DNS Server 2:

10.0.0.1

DHCP Timeout in seconds\*: 

60

\* A value of -1 will retry forever

VLAN Settings

VLAN ID (0-4095): 

0

VLAN Priority (0-7): 

0

Current Network Settings

IP Address: 10.10.1.72

Subnet Mask: 255.0.0.0

Default Gateway: 10.0.0.1

DNS Server 1: 10.0.1.56

DNS Server 2:

Save

Reboot

Toggle Help




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

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

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

Web Page Item	Description
<b>Stored Network Settings</b>	
Addressing Mode ?	Select either DHCP IP Addressing or Static Addressing by marking the appropriate radio button. DHCP Addressing mode is enabled on default and the device will attempt to resolve network addressing with the local DHCP server upon boot. If DHCP Addressing fails, the device will revert to the last known IP address or the factory default address if no prior DHCP lease was established. See <a href="#">Section 2.5, "Restore the Factory Default Settings"</a> for factory default settings. Be sure to click <b>Save</b> and <b>Reboot</b> to store changes when configuring a Static address.
Hostname ?	This is the hostname provided by the DHCP server. See the DHCP/DNS server documentation for more information. Enter up to 64 characters.
IP Address ?	Enter the Static IPv4 network address in dotted decimal notation.
Subnet Mask ?	Enter the Subnet Mask in dotted decimal notation.
Default Gateway ?	Enter the Default Gateway IPv4 address in dotted decimal notation.
DNS Server 1 ?	Enter the primary DNS Server IPv4 address in dotted decimal notation.
DNS Server 2 ?	Enter the secondary DNS Server IPv4 address in dotted decimal notation.
DHCP Timeout in seconds ?	Specify the desired time-out duration (in seconds) that the device will wait for a response from the DHCP server before reverting back to the stored static IP address. The stored static IP address may be the last known IP address or the factory default address if no prior DHCP lease was established. Enter up to 8 characters. A value of -1 will retry forever.
<b>VLAN Settings</b>	
VLAN ID (0-4095) ?	Specify the IEEE 802.1Q VLAN ID number. Enter up to 4 digits.  <b>Note:</b> The device supports 802.1Q VLAN tagging support. The switch port connected to the device will need to be in "trunking mode" for the VLAN tags to propagate.
VLAN Priority (0-7) ?	Specify the IEEE 802.1p VLAN priority level. Enter 1 digit. A value of 0 may cause the VLAN ID tag to be ignored.
<b>Current Network Settings</b>	
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.

Table 2-6. Network Configuration Parameters (continued)

Web Page Item	Description
	Click the <b>Save</b> button to save your configuration settings.
	Click on the <b>Reboot</b> button to reboot the system.
	Click on the <b>Toggle Help</b> button to see a short description of some of the web page items. First click on the <b>Toggle Help</b> button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

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 SIP Paging Server's **IP Address**: The SIP 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**.

## 2.6.7 Configure the SIP Parameters

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

Figure 2-15. SIP Page

**CyberData Paging Server**

**SIP Settings**

Enable SIP operation: ☒

Register with a SIP Server: ☒

Buffer SIP Calls: ☐

Primary SIP Server: 10.0.0.253

Primary SIP User ID: 199

Primary SIP Auth ID: 199

Primary SIP Auth Password: \*\*\*\*\*

Re-registration Interval (in seconds): 360

Backup SIP Server 1:

Backup SIP User ID:

Backup SIP Auth ID:

Backup SIP Auth Password:

Re-registration Interval (in seconds): 360

Backup SIP Server 2:

Backup SIP User ID:

Backup SIP Auth ID:

Backup SIP Auth Password:

Re-registration Interval (in seconds): 360

Remote SIP Port: 5060

Local SIP Port: 5060

SIP Transport Protocol: UDP

TLS Version: 1.2 only (recommended)

Verify Server Certificate: ☐

Outbound Proxy:

Outbound Proxy Port: 0

Use Cisco SRST: ☐

Disable rport Discovery: ☐

Unregister on Boot: ☐

Keep Alive Period: 10000

**Nightringer Settings**

SIP Server:

SIP User ID:

SIP Auth ID:

SIP Auth Password:

Re-registration Interval (in seconds): 360

Relay rings to multicast: ☐

Multicast Address: 224.1.2.32

Multicast Port: 2020

**Call Disconnection**

Terminate Call after delay: 0

**Audio Codec Selection**

Codec: Auto Select

**RTP Settings**

RTP Port (even): 10500

Asymmetric RTP: ☐

Jitter Buffer: 50

RTP Encryption (SRTP): Disabled

Save Reboot Toggle Help

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

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

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



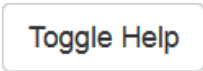
Web Page Item	Description
<b>SIP Settings</b>	
Enable SIP Operation ?	When enabled, the device will transmit, receive, and process SIP messages according to the configured SIP settings below.
Register with a SIP Server ?	When enabled, the device will attempt to register to the configured SIP Server(s) on this page. To configure the device to send and receive point-to-point SIP calls, enable <b>SIP Operation</b> and disable <b>Register with a SIP Server</b> (see <a href="#">Section 2.6.8, "Configure the Paging Groups (PGROUPS) Parameters"</a> ).
Buffer SIP Calls ?	Also referred to as "delayed paging." Device will buffer up to four minutes of audio then play back the recording after hang up or after the buffer is full.
Primary SIP Server ?	Enter the SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the primary SIP server. This field can accept entries of up to 255 characters in length.
Primary SIP User ID ?	Specify the SIP User ID for the Primary SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the primary SIP server. Enter up to 64 alphanumeric characters.
Primary SIP Auth ID ?	Specify the Authenticate ID for the Primary SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Primary SIP Auth Password ?	Specify the Authenticate Password for the Primary SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Re-registration Interval (in seconds) ?	The SIP Re-registration interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
Backup SIP Server 1 ?	Enter the backup SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the backup SIP server. This field can accept entries of up to 255 characters in length.
Backup SIP User ID ?	Specify the SIP User ID for the first backup SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the first backup SIP server. Enter up to 64 alphanumeric characters.
Backup SIP Auth ID ?	Specify the Authenticate ID for the first backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Auth Password ?	Specify the Authenticate Password for the first backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Re-registration Interval (in seconds) ?	The SIP Re-registration interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
Backup SIP Server 2 ?	Enter a second backup SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the second backup SIP server. This field can accept entries of up to 255 characters in length.
Backup SIP User ID ?	Specify the SIP User ID for the second backup SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the second backup SIP server. Enter up to 64 alphanumeric characters.

**Table 2-7. SIP Configuration Parameters (continued)**

Web Page Item	Description
Backup SIP Auth ID ?	Specify the Authenticate ID for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Auth Password ?	Specify the Authenticate Password for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Re-registration Interval (in seconds) ?	The SIP Re-registration interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
Remote SIP Port ?	The Remote SIP Port is the port number the device will use as the destination port when sending SIP messages. The default Remote SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
Local SIP Port ?	The Local SIP Port is the port number the device will use to receive SIP messages. The default Local SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
SIP Transport Protocol ?	Choose the transport protocol for SIP signaling. This will affect all extensions, including the Nightringer. Default is UDP.
TLS Version ?	Choose the TLS version for SIP over TLS. Modern security standards strongly recommend using TLS 1.2.
Verify Server Certificate ?	When enabled, the device will verify the authenticity of the server during the TLS handshake by its certificate and common name. The TLS handshake will be aborted if the server is deemed to be inauthentic and SIP registration will not proceed.
Outbound Proxy ?	Enter the Outbound Proxy address as an IPv4 address in dotted decimal notation or a fully qualified domain name (FQDN). When an IP address is configured, the device will send all SIP messages to this IP address. When an FQDN is configured, the device will run DNS NAPTR, SRV, and A queries on the FQDN to resolve an IP address to which it will send all SIP messages. This field can accept entries of up to 255 characters in length.
Outbound Proxy Port ?	The Outbound Proxy Port is port number used as the destination port when sending SIP messages to the outbound proxy. A value of 0 will default to 5060. The supported range is 0-65536. Enter up to 5 digits.
Use Cisco SRST ?	When enabled, the backup servers are handled according to Cisco SRST (Survivable Remote Site Telephony). It is required for use in clustered Cisco Unified Communications Manager topologies.
Disable rport Discovery ?	Disabling rport Discovery will prevent the device from including the public WAN IP address and port number in the contact information that is sent to the remote SIP servers. This will generally only need to be enabled when using an SBC or SIP ALG in conjunction with a remote SIP server.
Unregister on Boot ?	When enabled, the device will send one registration with an expiry of 0 on boot.
Keep Alive Period ?	The minimum time in milliseconds between keep-alive packets sent for nat traversal. A value of 0 will disable keep alive packets.
<b>Nightringer Settings</b>	
SIP Server ?	Enter the SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's Nightringer extension on the SIP server. This field can accept entries of up to 255 characters in length.
SIP User ID ?	Specify the SIP User ID for the SIP server. This parameter becomes the user portion of the SIP-URI for the device's Nightringer extension. Enter up to 64 alphanumeric characters.



**Table 2-7. SIP Configuration Parameters (continued)**

Web Page Item	Description
SIP Auth ID ?	Specify the Authenticate ID for the SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
SIP Auth Password ?	Specify the Authenticate Password for the SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Re-registration Interval (in seconds) ?	The SIP Re-registration Interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
Relay rings to multicast ?	When selected, the device will play ring tones to the specified multicast address and port.
Multicast Address ?	The multicast address used for nightring audio.
Multicast Port ?	The multicast port used for nightring audio.
<b>Call Disconnection</b>	
Terminate Call After Delay ?	Automatically terminate an active call after a given delay in seconds. A value of 0 will disable this function. Enter up to 8 digits.
<b>Audio Codec Selection</b>	
Codec ?	Select desired codec (only one may be chosen).
<b>RTP Settings</b>	
RTP Port (even) ?	Specify the port number used for the RTP stream after establishing a SIP call. This port number must be an even number and defaults to 10500. The supported range is 0-65536. Enter up to 5 digits.
Asymmetric RTP ?	<p>Specify if the remote endpoint will send and receive RTP packets on different ports. If set to false, the device will track the address/port that is sending RTP packets during a SIP call. If the address/port changes mid-stream, the device will disregard the SDP and send all further RTP packets to this new address.</p> <p>If set to true, this device will ignore the sending address/port and send RTP as specified in the SDP. Warning! Enabling asymmetric RTP can cause the RTP stream to be lost.</p> <p>Most installations should not enable asymmetric RTP.</p>
Jitter Buffer ?	Specify the size of the jitter buffer (in milliseconds) used for SIP calls. Valid values are 50-1000.
RTP Encryption (SRTP) ?	When enabled, a SIP call's audio streams are encrypted using SRTP.
	Click the <b>Save</b> button to save your configuration settings.
	Click on the <b>Reboot</b> button to reboot the system.
	Click on the <b>Toggle Help</b> button to see a short description of some of the web page items. First click on the <b>Toggle Help</b> button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

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

<https://www.cyberdata.net/pages/connecting-to-ip-pbx-servers>

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 SIP Paging Server when you reboot it.
  - b. Select **No** to keep the SIP Paging Server registered when you reboot it.
6. In the **Register Expiration** field, enter the number of seconds the SIP Paging Server registration lease remains valid with the SIP Server. The SIP Paging Server automatically re-registers with the SIP server before the lease expiration timeout.

## 2.6.7.1 Point-to-Point Configuration

It is possible to use the device as a paging endpoint without registering it with a SIP server by configuring it for Point-to-Point paging. To do this, complete the following steps:

1. On the **SIP** page (Figure 2-16), make sure of the following:
  - The **Register with a SIP Server** parameter is not selected.
  - The **Enable SIP Operation** parameter is selected
2. Click on the **Save** button to save the changes.
3. Click on the **Reboot** button to reboot the device.
4. Enter the device's IP address as a “speed dial” (also called “auto-dial”) key on the phone(s) from which you want to page.

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

Figure 2-16. SIP Page

**SIP Settings**

Enable SIP operation: ☒

Register with a SIP Server: ☐

Buffer SIP Calls: ☐

Primary SIP Server: 0.0.0.253

Primary SIP User ID: 99

Primary SIP Auth ID: 99

Primary SIP Auth Password: \*\*\*\*

Re-registration Interval (in seconds): 60

**Nightringer Settings**

SIP Server:

SIP User ID:

SIP Auth ID:

SIP Auth Password:

Re-registration Interval (in seconds): 360

Relay rings to multicast: ☐

Multicast Address: 224.1.2.32

Multicast Port: 2020

**Register with a SIP Server** is not selected

**Enable SIP Operation** is selected

## 2.6.7.2 Point-to-Point Fault Sense Reporting

It is possible to use the device to report faults detected at the device's Fault Sense Input without registering it with a SIP server by configuring it for Point-to-Point Fault Sense reporting. To do this, complete the following steps:

1. On the **SIP** page (Figure 2-17), make sure of the following:
  - The **Register with a SIP Server** parameter is not selected.
  - The **Enable SIP Operation** parameter is selected

Figure 2-17. SIP Page

**SIP Settings**

Enable SIP operation: ☒

Register with a SIP Server: ☐

Buffer SIP Calls: ☐

Primary SIP Server: 0.0.0.253

Primary SIP User ID: 99

Primary SIP Auth ID: 99

Primary SIP Auth Password: \*\*\*\*\*

Re-registration Interval (in seconds): 60

**Nightringer Settings**

SIP Server:

SIP User ID:

SIP Auth ID:

SIP Auth Password:

Re-registration Interval (in seconds): 360

Relay rings to multicast: ☐

Multicast Address: 224.1.2.32

Multicast Port: 2020

**Register with a SIP Server is not selected**

**Enable SIP Operation is selected**

2. Click on the **Save** button to save the changes.
3. Click on the **Reboot** button to reboot the device.

4. On the **Fault** page (Figure 2-18) in the **Dial Out Extension** field, enter the IP address of the phone that is to be called when a fault is detected at the Fault Sense Input.

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

**Figure 2-18. Fault Page**

Home Device Network SIP PGROUPS SSL Schedules Fault Audiofiles Events Autoprov Firmware

## CyberData Paging Server

### Fault Detection Settings

Message Playbacks: 0

Play Message Locally: ☐

Make Call to Extension: ☒

Dial Out Extension: 204

Dial Out ID: id204

Multicast Audio: Disabled

Multicast Address: 239.168.3.1

Multicast Port: 8888

Detect Line-in Silence: ☐

Test Fault Sensor

Save Reboot Toggle Help

In the **Dial Out Extension** field, enter the IP address of the phone that is to be called when a fault is detected at the Fault Sense Input.

## 2.6.8 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.

1. Click on the **PGROUPS** button to open the **PGROUPS** page. See [Figure 2-19](#).

**Figure 2-19. PGROUPS Page**

The screenshot displays the 'CyberData Paging Server' interface. At the top, there is a navigation bar with tabs: Home, Device, Network, SIP, **PGROUPS**, SSL, Schedules, Fault, Audiofiles, Events, Autoprov, and Firmware. The main heading is 'CyberData Paging Server'. Below it, the section is titled 'Paging Groups'. A table lists 10 paging groups, each with an 'Edit' button. The table columns are #, Address, Port, Name, Code, TTL, and Lineout. Below the table is a pagination bar with links for pages 1 through 10, and a 'Save' button at the bottom.



#	Address	Port	Name	Code	TTL	Lineout
0	234.2.1.1	2000	PagingGroup00		255	Yes
1	234.2.1.2	2002	PagingGroup01		255	Yes
2	234.2.1.3	2004	PagingGroup02		255	Yes
3	234.2.1.4	2006	PagingGroup03		255	Yes
4	234.2.1.5	2008	PagingGroup04		255	Yes
5	234.2.1.6	2010	PagingGroup05		255	Yes
6	234.2.1.7	2012	PagingGroup06		255	Yes
7	234.2.1.8	2014	PagingGroup07		255	Yes
8	234.2.1.9	2016	PagingGroup08		255	Yes
9	234.2.1.10	2018	PagingGroup09		255	Yes

« 1 2 3 4 5 6 7 8 9 10 »

Save

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

**Table 2-8. PGROUPS Parameters**

Web Page Item	Description
#	Shows the paging group number.
Address	Shows the IP address of the PGROUP.
Port	Shows the port number of the PGROUP.
Name	Shows the name of the PGROUP.
Code	Shows the security code of the PGROUP.
TTL	Shows the "time to live" of the PGROUP.
Lineout	Shows the Lineout setting of the PGROUP.
	<p>To make changes to the paging groups, complete the following steps:</p> <ol style="list-style-type: none"> <li>1. Click on the <b>Edit</b> button to open the <b>Configure PGROUP</b> window (<a href="#">Figure 2-20</a>).</li> <li>2. In the <b>Configure PGROUP</b> window (<a href="#">Figure 2-20</a>), edit the PGROUP (see <a href="#">Table 2-9</a>, "Configure PGROUP Window") and click on the <b>Save Changes</b> button.</li> <li>3. On the <b>PGROUPS</b> page (<a href="#">Figure 2-19</a>), click on the <b>Reboot</b> button.</li> </ol>
	Click the <b>Save</b> button to save your configuration settings.

**Figure 2-20. Configure PGROUP Window**

The screenshot shows a window titled "Configure PGROUP" with a close button (X) in the top right corner. The window contains the following configuration fields:


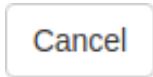

PGROUP	0
Address	234.2.1.164
Port	2078
Name	PagingGroup00
Security Code	0-9, *, #
TTL	255
Line-out	<input checked="" type="checkbox"/>
Play Stored Message	<input type="checkbox"/>
Audio File	<input type="text"/>
Times to Play	1

At the bottom right of the window, there are three buttons: "Toggle Help", "Cancel", and "Ok".



The parameters for the **Configure PGROUP** window are shown in [Table 2-9](#).

**Table 2-9. Configure PGROUP Window**

Web Page Item	Description
PGROUP	Shows the paging group number.
Address	Enter the IP address of the PGROUP. <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. <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.
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.
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.
Line-out	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.
Play Stored Message	When selected, entering this paging group will play the stored message selected in <a href="#">Audio File</a> .
Audio File	Select a file from the drop down list of audio files previously saved in the <a href="#">Stored Messages</a> portion of the <a href="#">Audiofiles Page</a> .
Times to Play	Enter the number of times the message will play (1-65535).
	Click on the <b>Toggle Help</b> button to see a short description of some of the web page items. First click on the <b>Toggle Help</b> button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.
	Click the <b>Cancel</b> button to close the <b>Configure PGROUP</b> window.
	Click the <b>OK</b> button to save your configuration settings.

---

## 2.6.9 Operating the Paging Server

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

### 2.6.9.1 DTMF Bypassed

- When the SIP 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.

### 2.6.9.2 DTMF Not Bypassed

- When the SIP 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 SIP 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 SIP 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 SIP 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 SIP 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 SIP 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 SIP Paging Server can negotiate the multicast stream via SIP regardless of the bypass state. However, if the SIP 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").

## 2.6.10 Configure the SSL Parameters

1. Click **SSL** menu button to open the **SSL** page (Figure 2-21 and Figure 2-22).

Figure 2-21. SSL Configuration Page

Home Device Network SIP PGROUPS **SSL** Schedules Fault Audiofiles Events Autoprovision Firmware

# CyberData Paging Server

**Web Server Certificate**

```

subject=
countryName           = US
stateOrProvinceName   = California
localityName          = Monterey
organizationName       = Cyberdata
commonName             = 0020f704790d
notBefore=Aug 28 23:26:06 2020 GMT
notAfter=Aug 26 23:26:06 2030 GMT

```

Browse... No file chosen
Import Web Certificate
Restore Web Certificate

**SIP Client Certificate**

```

subject=
countryName           = US
stateOrProvinceName   = California
organizationName       = CyberData
commonName             = 0020f704790d
notBefore=Aug  4 21:02:44 2021 GMT
notAfter=Aug  2 21:02:44 2031 GMT

```

Browse... No file chosen
Import SIP Certificate
Restore SIP Certificate
Optional Password:

**Autoprovisioning Client Certificate**

```

subject=
countryName           = US
stateOrProvinceName   = California
localityName          = Monterey
organizationName       = Cyberdata
commonName             = 0020f704790d
notBefore=Aug 28 23:26:06 2020 GMT
notAfter=Aug 26 23:26:06 2030 GMT

```

Browse... No file chosen
Import Autoprovisioning Certificate
Restore Autoprovisioning Certificate
Optional Password:

Cyberdata CA Save Reboot Toggle Help

**Test TLS Connection**
Server: 10.0.0.253 Port: 5060
Test SIP Connection Test Autoprovision Connection

**List of Trusted CAs**
Browse... No file chosen
Import CA Certificate Remove All Restore Defaults

1	CyberData_CA.pem	Info	Remove
2	DigiCert_Assured_ID_Root_CA.crt	Info	Remove
3	DigiCert_Assured_ID_Root_G2.crt	Info	Remove
4	DigiCert_Assured_ID_Root_G3.crt	Info	Remove
5	DigiCert_Global_Root_CA.crt	Info	Remove
6	DigiCert_Global_Root_G2.crt	Info	Remove
7	DigiCert_Global_Root_G3.crt	Info	Remove
8	DigiCert_High_Assurance_EV_Root_CA.crt	Info	Remove

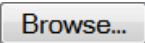


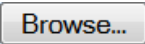


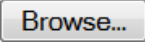
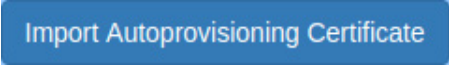
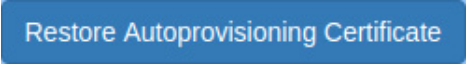
**Figure 2-22. SSL Configuration Page**

		Info	Remove
7	DigiCert_Global_Root_G3.crt	Info	Remove
8	DigiCert_High_Assurance_EV_Root_CA.crt	Info	Remove
9	DigiCert_Trusted_Root_G4.crt	Info	Remove
10	GeoTrust_Global_CA.crt	Info	Remove
11	GeoTrust_Primary_Certification_Authority.crt	Info	Remove
12	GeoTrust_Primary_Certification_Authority_-_G2.crt	Info	Remove
13	GeoTrust_Primary_Certification_Authority_-_G3.crt	Info	Remove
14	GeoTrust_Universal_CA.crt	Info	Remove
15	GeoTrust_Universal_CA_2.crt	Info	Remove
16	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G4.crt	Info	Remove
17	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5.crt	Info	Remove
18	VeriSign_Universal_Root_Certification_Authority.crt	Info	Remove
19	Verisign_Class_1_Public_Primary_Certification_Authority.crt	Info	Remove
20	Verisign_Class_1_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
21	Verisign_Class_2_Public_Primary_Certification_Authority_-_G2.crt	Info	Remove
22	Verisign_Class_2_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
23	Verisign_Class_3_Public_Primary_Certification_Authority.crt	Info	Remove
24	Verisign_Class_3_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
25	ca.crt	Info	Remove
26	cacert.pem	Info	Remove
27	thawte_Primary_Root_CA.crt	Info	Remove
28	thawte_Primary_Root_CA_-_G2.crt	Info	Remove
29	thawte_Primary_Root_CA_-_G3.crt	Info	Remove



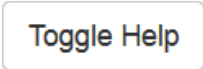





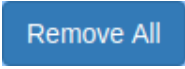

- On the **SSL** page, enter values for the parameters indicated in [Table 2-10](#).

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

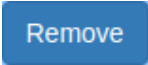
**Table 2-10. SSL Configuration Parameters**

Web Page Item	Description
<b>Web Server Certificate</b>	Certificate used by the web server.
	Click <b>Browse</b> to select a certificate to import.
	After selecting a certificate, click <b>Import Web Certificate</b> to import it as the certificate used by this device's web server.
	Restore the device's default web server certificate. This will remove the user-uploaded Web Server Certificate.(Server CAs and Trusted CAs are unaffected).
<b>SIP Client Certificate</b>	When doing mutual authentication this device will present a client certificate with these parameters.
	Click <b>Browse</b> to select a certificate to import.
	After selecting a certificate, click <b>Import SIP Certificate</b> to import it as the certificate used by the device during SIP transactions.
	Restore the device's default sip client certificate. This will remove any user-uploaded sip client certificates (Server CAs and Trusted CAs are unaffected).
Optional Password	Enter the optional password for the SIP certificate's private key. <b>Note:</b> When using a password, it must be entered and saved before importing the certificate.
<b>Autoprovisioning Client Certificate</b>	When doing mutual authentication this device will present a client certificate with these parameters.
	Click <b>Browse</b> to select a certificate to import.
	After selecting a certificate, click <b>Import Autoprovisioning Certificate</b> to import it as this device's certificate. This certificate will be used when requesting files during autoprovisioning.
	Restore the device's default autoprovisioning certificate. This will remove any user-uploaded autoprovisioning certificates. (Server CAs and Trusted CAs are unaffected).
Optional Password ?	Enter the optional password for the Autoprovisioning certificate's private key. <b>Note:</b> When using a password, it must be entered and saved before importing the certificate.
Cyberdata CA ?	Right click and <b>Save Link As...</b> to get the Cyberdata CA used to sign this client certificate.

**Table 2-10. SSL Configuration Parameters (continued)**

Web Page Item	Description
	Click the <b>Save</b> button to save your configuration settings.
	Click on the <b>Reboot</b> button to reboot the system.
	Click on the <b>Toggle Help</b> button to see a short description of some of the web page items. First click on the <b>Toggle Help</b> button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.
<b>Test TLS Connection</b>	
Server ?	The ssl test server address as a fully qualified domain name or in IPv4 dotted decimal notation.
Port ?	The supported range is 0-65536. SIP connections over TLS to port 5060 are modified to connect to port 5061. This test button will do the same.
	Use this button to test a TLS connection to a remote server using the sip client key and password. This will attempt to make a socket connection to the configured test server and port and report the success or failure. This can be used to debug TLS connection issues separate from SIP registration issues.
	Use this button to test a TLS connection to a remote server using the autoprovisioning client key and password. This will attempt to make a socket connection to the configured test server and port and report the success or failure. This can be used to debug TLS connection issues with secure autoprovisioning.
<b>List of Trusted CAs</b>	
	Use this button to select a configuration file to import.
	Click <b>Browse</b> to select a CA certificate to import. After selecting a server certificate authority (CA), click <b>Import CA Certificate</b> to import it to the list of trusted CAs. CAs are used to validate the certificate presented by the server when establishing a TLS connection.
	<b>Restore Defaults</b> will restore the default list of registered CAs and <b>Remove All</b> will remove all registered CAs.
	<b>Restore Defaults</b> will restore the default list of registered CAs and <b>Remove All</b> will remove all registered CAs.
	Provides details of the certificate. After clicking on this button, the <b>Certificate Info Window</b> appears. See <a href="#">Section 2.6.10.1, "Certificate Info Window"</a> .

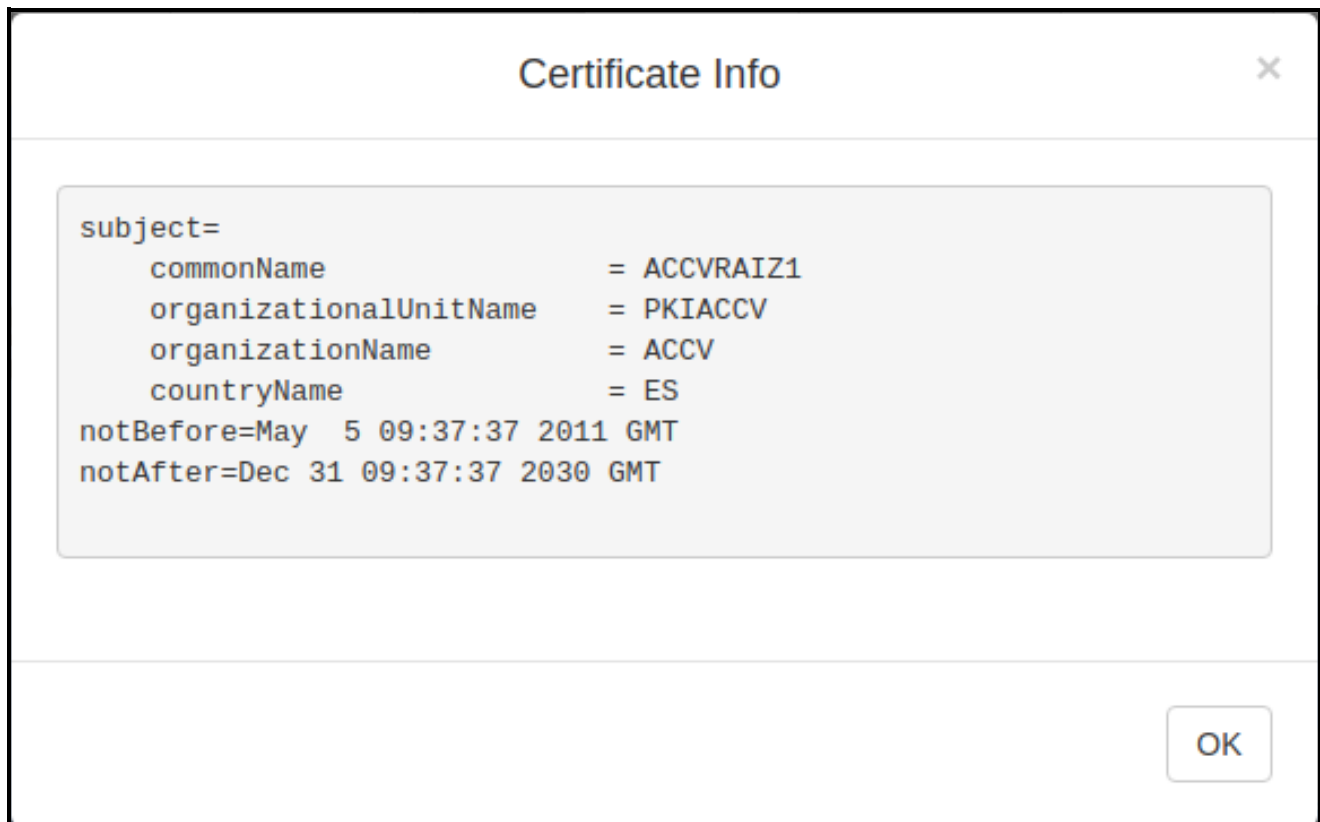
**Table 2-10. SSL Configuration Parameters (continued)**

Web Page Item	Description
	Removes this certificate from the list of trusted certificates. After clicking on this button, the <b>Remove Server Certificate Window</b> appears. See <a href="#">Section 2.6.10.2, "Remove Server Certificate Window"</a> .

### 2.6.10.1 Certificate Info Window

The **Certificate Info Window** provides details of the certificate. This window appears after clicking on the **Info** button. See [Figure 2-23](#).

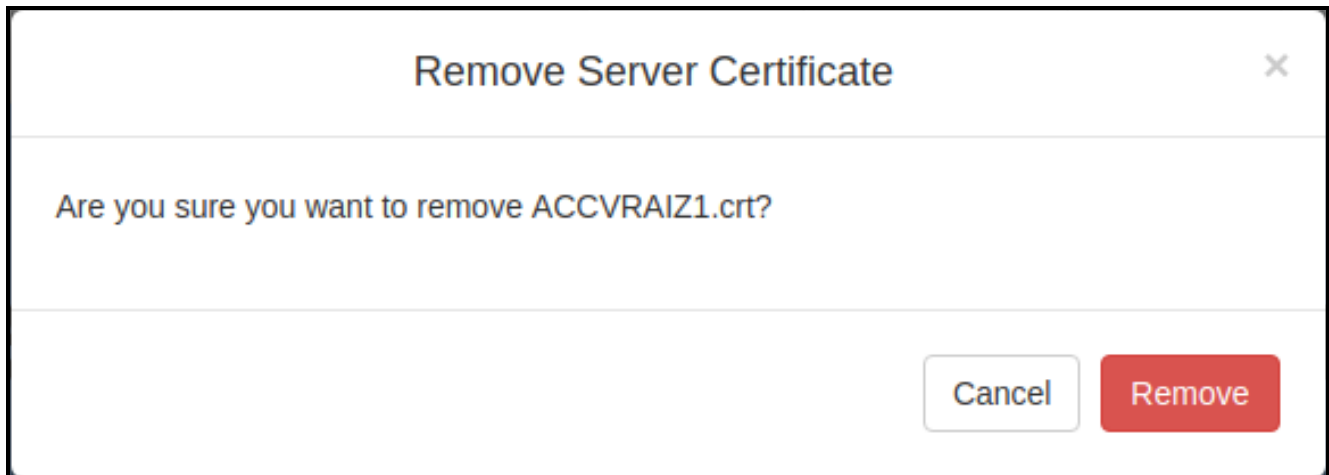
**Figure 2-23. Certificate Info Window**



## 2.6.10.2 Remove Server Certificate Window

The **Remove Server Certificate Window** will ask if the user wants to remove a certificate from the list of trusted certificates. This window appears after clicking on the **Remove** button. See [Figure 2-24](#).

**Figure 2-24. Remove Server Certificate Window**





## 2.6.11 Configure the Schedules Parameters

1. Click on the **Schedules** button to open the **Schedules** page. See [Figure 2-25](#).

**Figure 2-25. Schedules Page**




**CyberData Paging Server**

**Scheduled Events**

Event Name	Days	Time	Audio File	PGROUP		
am warning bell	Mon Tue Wed Thu Fri	08:40	Gong.wav	0	<a href="#">Edit</a>	<a href="#">Delete</a>
am bell	Mon Tue Wed Thu Fri Sat	08:45	Gong.wav	0	<a href="#">Edit</a>	<a href="#">Delete</a>
lunch bell	Mon Tue Wed Thu Fri	12:00	dingdong.wav	82	<a href="#">Edit</a>	<a href="#">Delete</a>
lunch end	Mon Tue Wed Thu Fri	12:40	dingdong.wav	82	<a href="#">Edit</a>	<a href="#">Delete</a>
recess	Mon Tue Wed Thu Fri	14:10	west.wav	21	<a href="#">Edit</a>	<a href="#">Delete</a>
recess end	Mon Tue Wed Thu Fri	14:25	west.wav	23	<a href="#">Edit</a>	<a href="#">Delete</a>
dismissal	Mon Tue Wed Thu Fri	15:10	french.wav	13	<a href="#">Edit</a>	<a href="#">Delete</a>
late bell	Mon Tue Wed Thu Fri	16:15	Gong.wav	0	<a href="#">Edit</a>	<a href="#">Delete</a>
weekend bell	Sun Fri Sat	11:30	Gong.wav	78	<a href="#">Edit</a>	<a href="#">Delete</a>
weekday 810	Mon Tue Wed Thu Fri	08:10	nuclear_explosion.wav	36	<a href="#">Edit</a>	<a href="#">Delete</a>
						<a href="#">New</a>

2. On the **Schedules** page, enter values for the parameters indicated in [Table 2-13](#).

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

Web Page Item	Description
<b>Scheduled Events</b>	
Days	Shows the days of the scheduled event.
Time	Shows the time of the scheduled event.
Audio File	Shows the audio file that is associated with the scheduled event.
Event Name	Shows the name of the scheduled event.
	Opens the <b>Configure Scheduled Event</b> window for the corresponding event. See <a href="#">Figure 2-26, "Configure Scheduled Event Window"</a> and <a href="#">Table 2-12, "Configure Scheduled Event Window Parameters"</a>
	Removes the event from the schedule.
	Opens a new <b>Configure Scheduled Event</b> window.

**Figure 2-26. Configure Scheduled Event Window**

**Configure Scheduled Event**

**Days**

Sun	Mon	Tue	Wed	Thu	Fri	Sat
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

**Name** am warning bell

**Time** 08:40

**Audio** Gong.wav

**PGROUP** 0

**Times to Play** 2



**Relay**

- No action
- Select a relay action
- No action
- Activate during bell
- Activate indefinitely
- Deactivate indefinitely

Cancel Save

The parameters for the **Configure Scheduled Event** window are shown in [Table 2-12](#).

**Table 2-12. Configure Scheduled Event Window Parameters**

Web Page Item	Description
Days	Use the box beneath the day to select. Multiple days may be selected.
Name	Enter the name of the event, using a maximum of 16 characters.
Time	Enter time of the event, in the form HH:MM, using the 24 hour clock.
Audio	Choose the audio file to be played from the drop down list, which displays files previously uploaded in the Bells section of the Audio Files web page.
PGROUP	Select the paging group from the drop down menu.
Times to Play	Number of times the audio file will play
Relay	<p>A relay can be activated or deactivated at the time of a scheduled bell.</p> <p>The relay options are :</p> <p>Activate during bell — The relay will be active while the bell is playing</p> <p>Activate indefinitely — The relay will be activated indefinitely.</p> <p>Deactivate indefinitely — The relay will be deactivated indefinitely.</p>
	Click the <b>Cancel</b> button to close the <b>Configure Scheduled Event</b> window.
	Click the <b>Save</b> button to save your configuration settings.

- In addition to the bells, the user can have 25 stored messages that are utilized through paging groups.
- [www.cyberdata.net/bell-download/](http://www.cyberdata.net/bell-download/) has a set of sounds that can be downloaded.
- The user can upload 25 unique bell files that can be used in up to 250 scheduled events.

## 2.6.12 Configure the Fault Detection Parameters

1. Click on the **Fault** button to open the **Fault** page. See [Figure 2-27](#).

**Figure 2-27. Fault Page**

The screenshot shows the 'Fault' page of the CyberData Paging Server web interface. At the top is a navigation bar with tabs: Home, Device, Network, SIP, PGROUPS, SSL, Schedules, Fault (selected), Audiofiles, Events, Autoprov, and Firmware. Below the navigation bar is the title 'CyberData Paging Server'. The main section is titled 'Fault Detection Settings' and contains the following configuration options:





- Message Playbacks: 0
- Play Message Locally: ☐
- Make Call to Extension: ☒
- Dial Out Extension: 204
- Dial Out ID: id204
- Multicast Audio: Disabled (dropdown menu)
- Multicast Address: 239.168.3.1
- Multicast Port: 8888
- Detect Line-in Silence: ☐

At the bottom of the settings section are three buttons: 'Test Fault Sensor', 'Save', 'Reboot', and 'Toggle Help'.

- On the **Fault Detection** page, enter values for the parameters indicated in [Table 2-13](#).

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

**Table 2-13. Fault Detection Configuration Parameters**

Web Page Item	Description
<b>Triggered Settings</b>	
Message Playbacks ?	The number of times to repeat the audio message through the local speaker or to the remote endpoint. A value of 0 will repeat forever. Enter a value from 0-65536.
Play Message Locally ?	When selected, the device will play the user defined “sensor triggered” audio file when the fault detection is triggered.
Make Call to Extension ?	When selected, the device will call an extension when fault detection is triggered. Use the <b>Dial Out Extension</b> field to specify the extension the device will call.
Dial Out Extension ?	Specify the extension the device will call when fault detection is triggered. Enter up to 64 alphanumeric characters.
Dial Out ID ?	An additional Caller identification string added to outbound calls. Enter up to 64 alphanumeric characters.
Multicast Audio ?	When enabled, the device will multicast audio to the specified multicast address and port while the fault sensor is activated.
Message ?	When set to <b>Message</b> , the device will multicast the user defined sensor triggered audio file.
Line-in ?	When set to Line-in, the device will multicast line-in audio.
Multicast Address ?	The multicast address used for fault detection audio.
Multicast Port ?	The multicast port used for fault detection audio.
Detect Line-in Silence ?	If audio drops below a threshold on line-input, the fault line-in multicast stream will be stopped to reduce network traffic.
	Click on the <b>Test Fault Sensor</b> button to test the fault detection feature.
	Click the <b>Save</b> button to save your configuration settings.
	Click on the <b>Reboot</b> button to reboot the system.
	Click on the <b>Toggle Help</b> button to see a short description of some of the web page items. First click on the <b>Toggle Help</b> button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

## 2.6.13 Configure the Audio Parameters

Click on the **Audiofiles** button to open the **Audiofiles** page. See [Figure 2-28](#). The **Audiofiles** page is used to add custom audio to the board. User uploaded audio will take precedence over the audio files shipped with the device.

**Figure 2-28. Audiofiles Page**

Home Device Network SIP PGROUPS SSL Schedules Fault **Audiofiles** Events Autoprov Firmware

# CyberData Paging Server

Available Space:1484MB

## Audio Files

0:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
1:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
2:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
3:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
4:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
5:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
6:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
7:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
8:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
9:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Dot:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Audio Test:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Page Tone:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>

**Figure 2-29. Audiofiles Page**

<b>Your IP Address Is:</b>	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
<b>Rebooting:</b>	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
<b>Restoring Default:</b>	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
<b>Ringback Tone:</b>	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
<b>Ring Tone:</b>	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
<b>Night Ring:</b>	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
<b>Sensor Triggered:</b>	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
<b>Stored Message File Not Found:</b>	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
<b>Enter Zone:</b>	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
<b>Confused:</b>	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>

Menu Audio Files						
<b>Cancel:</b>	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
<b>Currently Playing:</b>	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
<b>Invalid Entry:</b>	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
<b>Page:</b>	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
<b>Play Stored Message:</b>	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
<b>Pound (#):</b>	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
<b>Press:</b>	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
<b>Stored Message:</b>	Currently set to: default					



**Figure 2-30. Audiofiles Page**

Invalid Entry:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Page:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Play Stored Message:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Pound (#):	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Press:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Stored Message:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
To:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Enter Code:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Invalid Code:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>

### Stored Messages

No file chosen

Tsunami_Warning.wav	<input type="button" value="Play Stored Message"/>	<input type="button" value="Delete Stored Message"/>
Westminster_chimes.wav	<input type="button" value="Play Stored Message"/>	<input type="button" value="Delete Stored Message"/>

### Bells

No file chosen

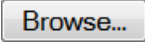

Gong.wav	<input type="button" value="Play Bell"/>	<input type="button" value="Delete Bell"/>
dingdong.wav	<input type="button" value="Play Bell"/>	<input type="button" value="Delete Bell"/>
explosion.wav	<input type="button" value="Play Bell"/>	<input type="button" value="Delete Bell"/>
french.wav	<input type="button" value="Play Bell"/>	<input type="button" value="Delete Bell"/>
west.wav	<input type="button" value="Play Bell"/>	<input type="button" value="Delete Bell"/>

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



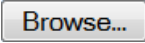

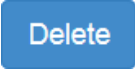

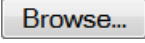

**Note** Each entry on the **Audiofiles** page replaces one of the stock audio files on the board. When the input box displays the word **default**, the SIP Paging Server is using the stock audio file. If that file is replaced with a user file, it will display the uploaded filename.

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



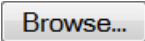



**Table 2-14. Audiofiles Configuration Parameters**

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). '0' corresponds to the spoken word "zero." '1' corresponds to the spoken word "one." '2' corresponds to the spoken word "two." '3' corresponds to the spoken word "three." '4' corresponds to the spoken word "four." '5' corresponds to the spoken word "five." '6' corresponds to the spoken word "six." '7' corresponds to the spoken word "seven." '8' corresponds to the spoken word "eight." '9' corresponds to the spoken word "nine."
Dot	Corresponds to the spoken word "dot."
Audio Test	Corresponds to the message "This is the CyberData IP speaker test message..."
Page Tone	Corresponds to a simple tone that is unused by default.
Your IP Address is	Corresponds to the message "Your IP address is..."
Rebooting	Corresponds to the spoken word "Rebooting."
Restoring Default	Corresponds to the message "Restoring default."
Ringback Tone	Specifies the Ringback Tone.
Ring Tone	Specifies the Ring Tone.
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.
Sensor Triggered	Corresponds to the message "Sensor Triggered."
Stored Message File Not Found	Corresponds to the message "Stored Message File Not Found."
Enter Zone	Corresponds to the words "Enter Zone" used in the audio menu played to the caller.
Confused	Corresponds to the message "Confused."
	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.

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

Web Page Item	Description
	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.
<b>Menu Audio Files</b>	<b>Menu Audio Files</b> are user-uploadable messages that create the audio menu played to the caller.
Cancel	Corresponds to the word "Cancel" used in the audio menu played to the caller.
Currently Playing	Corresponds to the words "Currently Playing" used in the audio menu played to the caller.
Invalid Entry	Corresponds to the words "Invalid Entry" used in the audio menu played to the caller.
Page	Corresponds to the word "Page" used in the audio menu played to the caller.
Play Stored Message	Corresponds to the words "Play Stored Message" used in the audio menu played to the caller.
Pound (#)	Corresponds to whatever word or phrase the user wishes to call the pound key in the audio menu played to the caller.
Press	Corresponds to the word "Press" used in the audio menu played to the caller.
Stored Message	Corresponds to the words "Stored Message" used in the audio menu played to the caller.
To	Corresponds to the word "To" used in the audio menu played to the caller.
Enter Code	Corresponds to the message "Enter Code."
Invalid Code	Corresponds to the message "Invalid Code."
	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.
<b>Stored Messages</b>	Upload files here to be used as stored messages. <b>Note:</b> The user may upload a maximum of 25 files.
	The <b>Browse</b> button will allow you to navigate to and select an audio file.
	The <b>Upload Stored Message</b> button will upload the stored message.

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

Web Page Item	Description
	The <b>Play Stored Message</b> button will play the stored message.
	The <b>Delete Stored Message</b> button will delete the stored message.
<b>Bells</b>	Upload files here to be used in scheduled events. <b>Note:</b> The user may upload a maximum of 25 files.
	The <b>Browse</b> button will allow you to navigate to and select an audio file.
	The <b>Upload Bell</b> button will upload the bell.
	The <b>Play Bell</b> button will play the bell.
	The <b>Delete Bell</b> button will delete the bell.

### 2.6.13.1 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 2-31](#) through [Figure 2-33](#).

Figure 2-31. Audacity 1

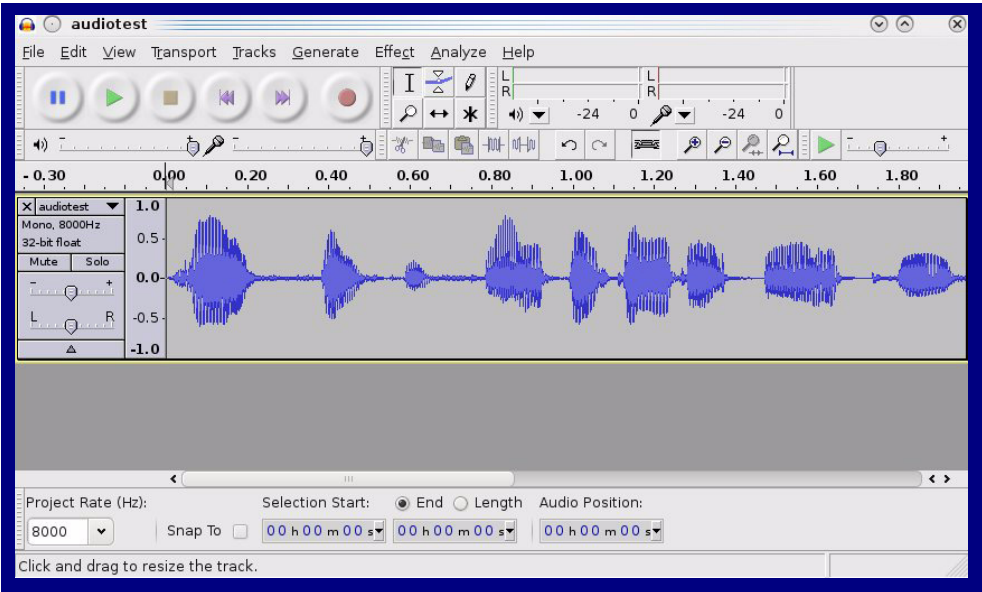
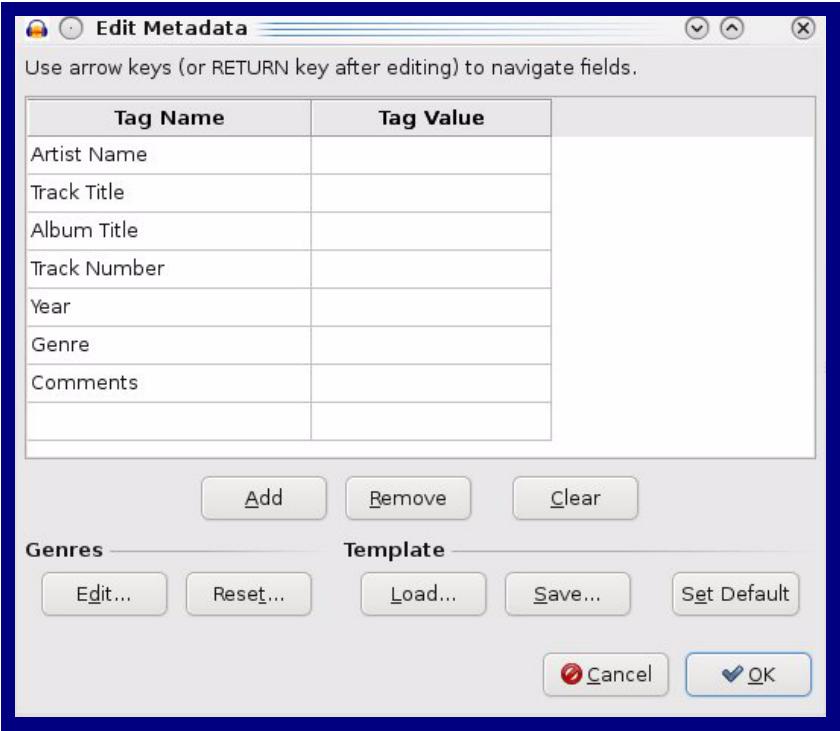


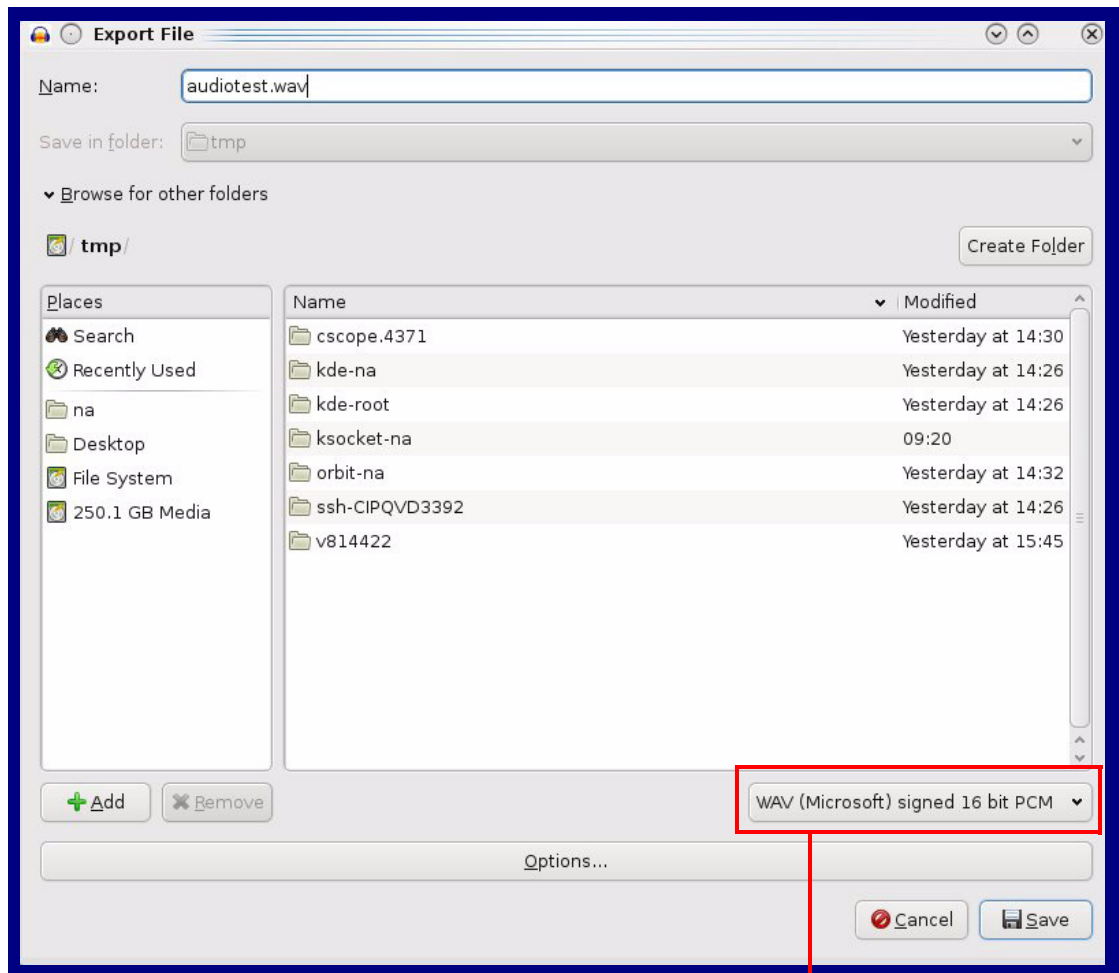
Figure 2-32. Audacity 2



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

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

**Figure 2-33. WAV (Microsoft) signed 16 bit PCM**



WAV (Microsoft) signed 16 bit PCM

## 2.6.14 Configure the Event Parameters

Click on the **Events** button to open the **Events** page (Figure 2-34). The **Events** page specifies a remote server that can be used to receive HTTP POST events when actions take place on the board.

**Figure 2-34. Events Page**

The screenshot shows the 'Events' configuration page of the CyberData Paging Server. At the top is a navigation bar with tabs: Home, Device, Network, SIP, PGROUPS, SSL, Schedules, Fault, Audiofiles, Events (selected), Autoprovisioning, and Firmware. The main header reads 'CyberData Paging Server'. Below this, there is a section for 'Enable Event Generation' with a checkbox. The 'Events' section contains a list of checkboxes for enabling various events: Call Start, Call Terminated, Relay Activated, Relay Deactivated, Night Ring, Power On, Fault, and 60 Second Heartbeat. To the right, the 'Event Server' section contains three input fields: 'Server IP Address' (10.0.0.250), 'Server Port' (8080), and 'Server URL' (xmlparse\_engine). At the bottom left are three buttons: 'Save', 'Reboot', and 'Toggle Help'.

Navigation
Home
Device
Network
SIP
PGROUPS
SSL
Schedules
Fault
Audiofiles
Events
Autoprovisioning
Firmware

# CyberData Paging Server

Enable Event Generation: ☐

### Events

- Enable Call Start Events: ☐
- Enable Call Terminated Events: ☐
- Enable Relay Activated Events: ☐
- Enable Relay Deactivated Events: ☐
- Enable Night Ring Events: ☐
- Enable Power On Events: ☐
- Enable Fault Events: ☐
- Enable 60 Second Heartbeat: ☐

### Event Server

Server IP Address:	10.0.0.250
Server Port:	8080
Server URL:	xmlparse_engine

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

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

**Table 2-15. Events Configuration**

Web Page Item	Description
Enable Event Generation ?	The device will send HTTP POST events to the specified remote server and port number whenever a certain action takes place. Select an event type below to generate an HTTP POST event. See <a href="#">Section 2.6.14.1, "Example Packets for Events"</a> for sample packets.
<b>Events</b>	
Enable Call Start Events ?	When selected, the device will report the start of a SIP call.
Enable Call Terminated Events ?	When selected, the device will report the end of a SIP call.
Enable Relay Activated Events ?	When selected, the device will report relay activation.
Enable Relay Deactivated Events ?	When selected, the device will report relay deactivation.
Enable Night Ring Events ?	When selected, the device will report when it starts ringing upon an incoming SIP call to the Nightringer extension. As a reminder, the Nightringer extension always rings upon an incoming SIP call and it is not possible to alter this behavior.
Enable Power On Events ?	When selected, the device will report when it boots.
Enable Fault Events ?	When selected, the device will report when the on-board fault detection is activated.
Enable 60 Second Heartbeat ?	When enabled, the device will report a Heartbeat event every 60 seconds. SIP registration is not required to generate Heartbeat events.
<b>Event Server</b>	
Server IP Address ?	The IPv4 address of the event server in dotted decimal notation.
Server Port ?	Specify the event server port number. The supported range is 0-65536. Enter up to 5 digits.
Server URL ?	Generally, the destination URL is the name of the application that receives the events and the string in the HTTP POST command. It can be a script used to parse and process the HTTP POST events. Enter up to 127 characters.
Check All	Click on <b>Check All</b> to select all of the events on the page.
Uncheck All	Click on <b>Uncheck All</b> to de-select all of the events on the page.
<b>Save</b>	Click the <b>Save</b> button to save your configuration settings.
<b>Reboot</b>	Click on the <b>Reboot</b> button to reboot the system.
<b>Toggle Help</b>	Click on the <b>Toggle Help</b> button to see a short description of some of the web page items. First click on the <b>Toggle Help</b> button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.



### 2.6.14.1 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>
```

## 2.6.15 Configure the Autoprovisioning Parameters

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

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

1. Click the **Autoprov** menu button to open the **Autoprovisioning** page. See [Figure 2-35](#).

**Figure 2-35. Autoprovisioning Page**

Home Device Network SIP PGROUPS SSL Schedules Fault Audiofiles Events Autoprov Firmware

# CyberData Paging Server

Disable Autoprovisioning: ☐

Autoprovisioning Server:

Autoprovisioning Filename:

Use tftp: ☐

Verify Server Certificate ☐

Username:

Password:

Autoprovisioning autoupdate (in minutes):

Autoprovision at time (HHMMSS):

Autoprovision when idle (in minutes > 10):

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 '0020f70462a9.xml' and if this fails, '000000cd.xml'.



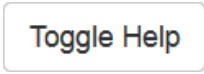
Autoprovisioning log

```
21:00 Autoprovisioning Device...
21:01 Autoprov found option 43 in DHCP server="http://10.0.0.242"
21:01 Autoprov looking for 0020f70462a9.xml at http://10.0.0.242
21:01 Got autoprov file. Parsing "0020f70462a9.xml"
21:09 Autoprov found option 72 in DHCP server="10.0.1.118"
21:09 Autoprov looking for 0020f70462a9.xml at 10.0.1.118
```


- On the **Autoprovisioning** page, you may enter values for the parameters indicated in [Table 2-16](#).

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

**Table 2-16. Autoprovisioning Configuration Parameters**

Web Page Item	Description
Disable Autoprovisioning ?	Prevent the device from automatically trying to download a configuration file. See <a href="#">Section 2.6.15.1, "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 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.
Username ?	The username used to authenticate with an autoprovisioning server. Leave this field blank to disable authentication.
Password ?	The password used to authenticate with an autoprovisioning server. Leave this field blank to disable authentication.
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, make sure that the <a href="#">Enable NTP</a> setting on the <a href="#">Device Page</a> is selected (see <a href="#">Table 2-5</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, make sure that the <a href="#">Enable NTP</a> setting on the <a href="#">Device Page</a> is selected (see <a href="#">Table 2-5</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, make sure that the <a href="#">Enable NTP</a> setting on the <a href="#">Device Page</a> is selected (see <a href="#">Table 2-5</a>).</p>
	Click the <b>Save</b> button to save your configuration settings.
	Click on the <b>Reboot</b> button to reboot the system.
	Click on the <b>Toggle Help</b> button to see a short description of some of the web page items. First click on the <b>Toggle Help</b> button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

**Table 2-16. Autoprovisioning Configuration Parameters (continued)**

Web Page Item	Description
	Press the <b>Download Template</b> button to create an autoprovisioning file for the device. See <a href="#">Section 2.6.15.3, "Get Autoprovisioning Template Button"</a>
Autoprovisioning log	The autoprovisioning log provides information about the latest autoprovisioning attempt (i.e. dhcp options and server accessed and files parsed or not found).

### 2.6.15.1 Autoprovisioning

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

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

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

By default, the device will get its autoprovisioning server from the DHCP options. See [Section 2.6.15.2, "Sample dhcpd.conf"](#) for an example of how to configure dhcpd to offer autoprovisioning server addresses. If multiple options are set, the device will attempt to download autoprovisioning files from every server.

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

1. Option 43 - a FQDN or an IP address to an http server
2. Option 72 - an IP address to an http server
3. Option 150 - an IP address to a tftp server
4. Option 66 - an IP address to a tftp server or if the entry starts with 'http', a FQDN to a http server.

You can download an autoprovisioning template file from the [Autoprovisioning Page](#) using the **Download Template** button (see [Table 2-16](#)). 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 <AutprovFile> 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 2-17. Autoprovisioning File Name**

<b>Autoprovisioning Filename</b>	<b>Autoprovisioning 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-uImage-ceilingspeaker</FirmwareFile>
                  <FirmwareServer>10.0.1.3</FirmwareServer>
                  <OutdoorIntercom30>firmware_file_v9.3.0</OutdoorIntercom30>
                  <OutdoorIntercom31>firmware_file_v10.3.0</OutdoorIntercom31>
                  <CallButton31>firmware_file_v10.3.0</CallButton31>
                  </FirmwareSettings>
```

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

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

The <FirmwareFile> name can contain path elements (i.e. /path/to/firmware/10.3.0-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.

## 2.6.15.2 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; }

```

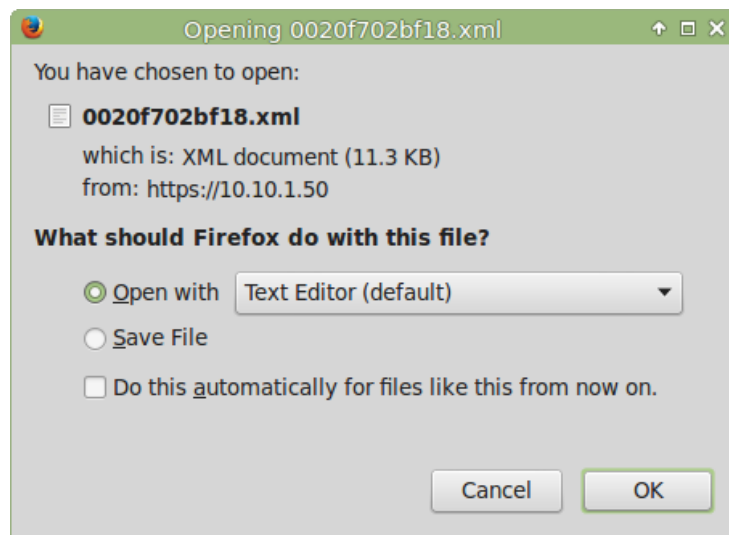
### 2.6.15.3 Get Autoprovisioning Template Button

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 2-36](#)). The configuration file is the basis for the default configuration settings for your unit).
3. Choose a location to save the configuration file and click on **OK**. See [Figure 2-36](#).

**Figure 2-36. Configuration File**



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.

## 2.7 Upgrade the Firmware

**Note** CyberData strongly recommends that you do not upgrade the firmware when the device is likely to be in use.

To upgrade the firmware of your device:

1. Download the latest firmware file from the **Downloads** tab at the following webpage:  
<https://www.cyberdata.net/products/011146>
2. Unzip the firmware version file. This file may contain the following:
  - Firmware file
  - Release notes
  - Autoprovisioning template
3. Log in to the **Home** page as instructed in [2.6.4 "Log in to the Configuration GUI"](#).
4. Click on the **Firmware** menu button to open the **Firmware** page ([Figure 2-37](#)).

**Figure 2-37. Firmware Page**

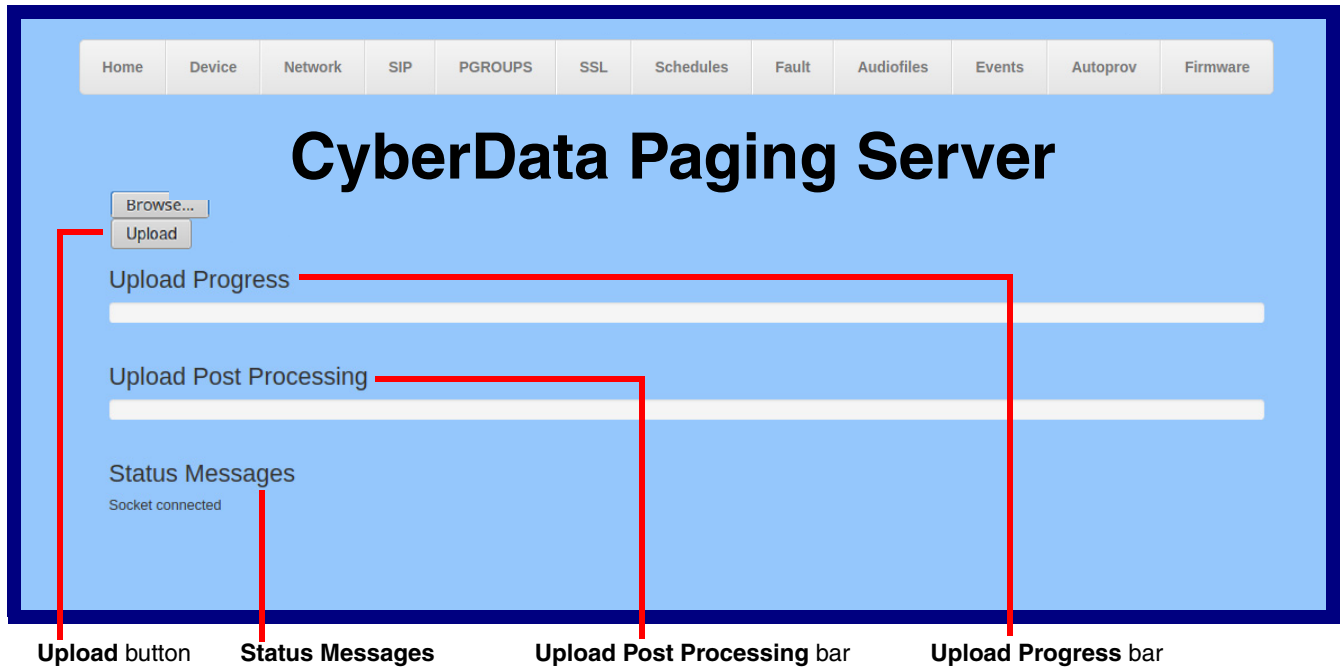


5. Click on the **Browse** button, and then navigate to the location of the firmware file.



6. Select the firmware file. This reveals the **Upload** button (Figure 2-38).

Figure 2-38. Upload Button



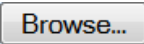

7. Click on the **Upload** button. After selecting the **Upload** button, you will see the progress of the upload in the **Upload Progress** bar.
8. When the upload is complete, you will see the words **Upload finished** under **Status Messages**.
9. At this point, you will see the progress of the upload's post processing in the **Upload Post Processing** bar.

**Note** Do not reboot the device before the upgrading process is complete.

10. When the process is complete, you will see the words **SWUPDATE Successful** under **Status Messages**.
11. The device will reboot automatically.
12. The **Home** page will display the version number of the firmware and indicate which boot partition is active.

Table 2-18 shows the web page items on the **Firmware** page.

**Table 2-18. Firmware Page Parameters**

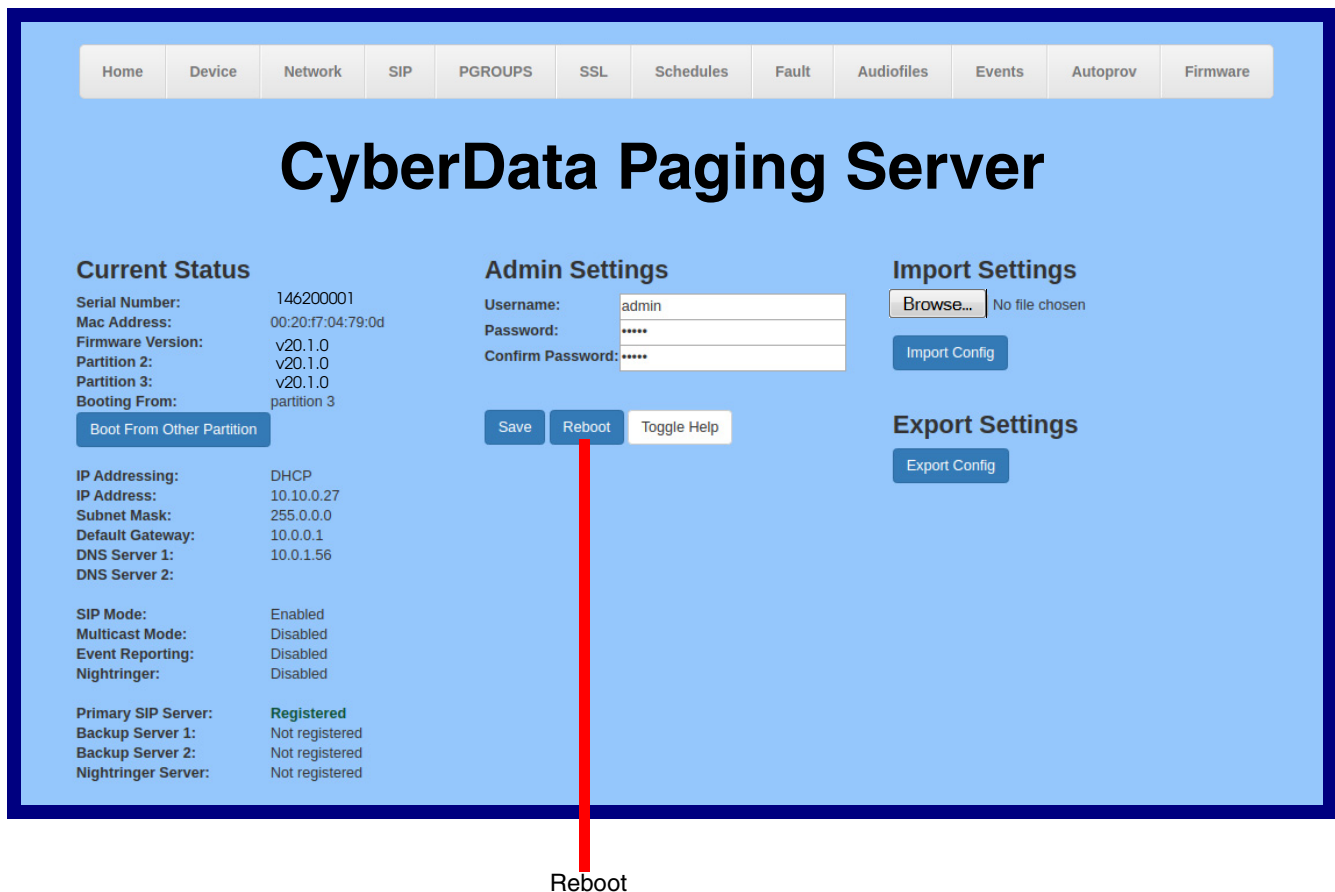
Web Page Item	Description
	Use the <b>Browse</b> button to navigate to the location of the firmware file that you want to upload.
	Click on the <b>Upload</b> button to automatically upload the selected firmware and reboot the system. <b>Note:</b> This button only appears after the user has selected a firmware file.
Upload progress	Status bar indicates the progress in uploading the file.
Upload Post Processing	Status bar indicates the progress of the software installation.
Status Messages	Messages relevant to the firmware update process appear here.

## 2.7.1 Reboot the SIP Paging Server

To reboot a SIP Paging Server, log in to the web page as instructed in [Section 2.6.4, "Log in to the Configuration GUI"](#).

1. Click **Reboot** ([Figure 2-39](#)). A normal restart will occur.

**Figure 2-39. Home Page**



## 2.8 Command Interface

Some functions on the device can be activated using simple POST commands to the web interface. The examples in [Table 2-19](#) use the free unix utility, **wget** commands. However, any program that can send HTTP POST commands to the device should work.

### 2.8.1 Command Interface Post Commands

The commands in [Table 2-19](#) require an authenticated session (a valid username and password to work).

**Table 2-19. Command Interface Post Commands**

Device Action	HTTP Post Command <sup>a</sup>
Reboot	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.247/command" --post-data "request=reboot"
Place call to extension (example: extension 600)	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.247/command" --post-data "request=call&extension=600"
Terminate a call	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.247/command" --post-data "request=terminate"
Test Relay	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.247/command" --post-data "request=test_relay"
Activate Relay	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.247/command" --post-data "request=activate_relay"
Deactivate Relay	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.247/command" --post-data "request=deactivate_relay"
Speak IP Address	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.247/command" --post-data "request=speak_ip_address"
Test Audio	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.247/command" --post-data "request=test_audio"
Swap Boot partitions	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.10.1.81/command" --post-data "request=swap_boot_partition"

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

# Appendix A: Troubleshooting/Technical Support

---

## A.1 Frequently Asked Questions (FAQ)

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

<https://www.cyberdata.net/products/011146>

---

## A.2 Documentation

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

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

<https://www.cyberdata.net/products/011146>

---

## A.3 Contact Information

Contact	<p>CyberData Corporation 3 Justin Court Monterey, CA 93940 USA <a href="http://www.CyberData.net">www.CyberData.net</a> Phone: 800-CYBERDATA (800-292-3732) 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="https://support.cyberdata.net/">https://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, Extension 333</p>

---

## A.4 Warranty and RMA Information

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

<https://support.cyberdata.net/>

# Index

---

## Symbols

+48V DC power supply 10

## A

activity light 12  
 address, configuration login 19  
 addressing  
     DHCP 15, 29  
     static 15, 29  
 admin username and password 19  
 audio configuration 55  
     night ring tone parameter 58  
 audio configuration page 55  
 audio ground reference 8  
 audio output 8  
 audio parameters 55  
 audiofiles 55  
 authenticate ID and password for SIP server  
     registration 34  
 autoprovision at time (HHMMSS) 69  
 autoprovision when idle (in minutes > 10) 69  
 autoprovisioning 70  
     download template button 70  
 autoprovisioning autoupdate (in minutes) 69  
 autoprovisioning configuration 68, 69  
 autoprovisioning filename 69  
 autoprovisioning server (IP Address) 69

## B

backup SIP server 1 31  
 backup SIP server 2 31  
 backup SIP servers, SIP server  
     backups 31

## C

cat 5 ethernet cable 10  
 changing  
     the web access password 23  
 changing default username and password for  
     configuration GUI 19  
 Cisco SRST 32  
 command interface 84

commands 84  
 configurable parameters 24, 28, 31  
 configuration information 15  
 configuration page  
     configurable parameters 24, 28  
 connecting the V3 paging server 7  
 connector (removable) 9  
 contact information 86  
 contact information for CyberData 86  
 current network settings 28  
 current settings, reviewing 22  
 CyberData contact information 86

## D

default gateway 28  
 default gateway for static addressing 29  
 default login address 19  
 default password for configuration GUI 19  
 default settings, restoring 14  
 default username and password for configuration GUI 19  
 device configuration 23  
     device configuration parameters 69  
     the device configuration page 68  
 device configuration page 23  
 device configuration parameters 24  
 device configuration password  
     changing for web configuration access 23  
 DHCP addressing 15, 29  
 dimensions 3  
 discovery utility program 19  
 DNS server 28  
 door sensor 58, 59  
 download autoprovisioning template button 70

## E

enable night ring events 64  
 ethernet port 10  
 event configuration  
     enable night ring events 64  
 expiration time for SIP server lease 31, 32, 33, 34  
 export settings 21

## F

- fault detection parameters 53
- fault sense input, sensor 8
- features 2
- firmware
  - where to get the latest firmware 80

## G

- get autoprovisioning template 70
- green link light 12
- ground connection 7
- GUI username and password 19

## H

- hazard levels 4
- http POST command 84

## I

- identifying your product 1
- import settings 21
- import/export settings 21
- input specifications 3
- intercom configuration page
  - configurable parameters 31
- IP address 28
  - SIP server 33

## L

- lease, SIP server expiration time 31, 32, 33, 34
- line input specifications 3
- line output specifications 3
- line-in 7
- line-out 7
- link light 12
- local SIP port 32, 34
- log in address 19
- logging in to configuration GUI 19

## M

- MGROUP 38

- multicast
  - play stored audio via multicast 54
- multicast address 54
- multicast port 24, 54
- multicast TTL 39, 41

## N

- navigation (web page) 16
- navigation table 16
- network activity, verifying 12
- network configuration page 27
- network parameters, configuring 27
- network setup button 27
- network, connecting to 11
- Nightringer 79
- nightringer settings 32
- NTP server 24

## O

- out of band 42
- output specifications 3

## P

- page port 8
- page port output connections 8
- paging server
  - configuration 15
- part number 3
- parts list 5
- password
  - configuration GUI 15, 19
  - for SIP server login 31
  - SIP server authentication 34
- payload types 3
- pgroups 38
- pin descriptions and functions 8
- point-to-point configuration 38
- port
  - ethernet 10
  - local SIP 32, 34
  - remote SIP 32, 34
- POST command 84
- power
  - connecting to 10
- product overview 1



## R

- reboot 82, 83
  - unregistering from SIP server during 34
- registration and expiration, SIP server
  - lease expiration 34
- relay 8
- relay contact 8
- remote SIP port 32, 34
- required configuration for web access username and
  - password 15, 19
- restoring factory default settings 14
- RFC2833 RTP events 42
- rport discovery setting, disabling 32

## S

- safety instructions 5
- sales 86
- scheduled events 50
- schedules parameters 49
- server address, SIP 31
- service 86
- SIP
  - enable SIP operation 31
  - local SIP port 32
  - user ID 31
- SIP configuration page 30
- SIP configuration parameters
  - outbound proxy 32
  - registration and expiration, SIP server lease 31, 32, 33
  - unregister on reboot 32
  - user ID, SIP 31
- SIP registration 31
- SIP remote SIP port 32
- SIP server 31
  - password for login 31
  - unregister from 32
  - user ID for login 31
- SIP server configuration 31
- SIP server parameters, configuring 15
- SIP setup button 30
- specifications 3
- SRST 32
- SSL parameters 43
- static addressing 15, 29
- status light 12
- subnet mask 28
- subnet mask static addressing 29
- supported protocols 3

## T

- tech support 86
- technical support, contact information 86

## U

- unregister from SIP server 34
- user ID
  - for SIP server login 31
- user ID for SIP server registration 34
- username
  - changing for web configuration access 23
- username for configuration GUI 15, 19

## V

- verifying
  - network activity 12
- VLAN ID 28
- VLAN Priority 28
- VLAN tagging support 28
- VLAN tags 28
- volume 24

## W

- warranty policy at CyberData 86
- web configuration log in address 19
- web page
  - navigation 16
- web page navigation 16
- wget, free unix utility 84