



SIP Paging Server Operations Guide

*SIP Compliant
Part #011146*

Document Part #931073K
for Firmware Version 12.2.0

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

Operations Guide 931073K
SIP Compliant 011146

COPYRIGHT NOTICE:

© 2020, CyberData Corporation, ALL RIGHTS RESERVED.

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

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

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

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

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



Technical Support

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

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

Email: support@cyberdata.net

Fax: (831) 373-4193

Company and product information is at www.cyberdata.net.

Revision Information

Revision 931073K, which corresponds to firmware version 12.2.0, was released on May 30, 2020, and has the following changes:



- Updates [Figure 2-11, "Home Page"](#)
- Updates [Figure 2-12, "Device Page"](#)
- Updates [Figure 2-14, "Network Page"](#)
- Updates [Figure 2-15, "SIP Page"](#)
- Updates [Figure 2-16, "SIP Page Set to Point-to-Point Mode"](#)
- Updates [Figure 2-17, "PGROUPS Page"](#)
- Updates [Figure 2-18, "PGROUPS Page \(continued\)"](#)
- Updates [Figure 2-19, "PGROUPS Page \(continued\)"](#)
- Updates [Figure 2-28, "Fault Page"](#)
- Updates [Figure 2-29, "Audiofiles Page"](#)
- Updates [Figure 2-30, "Audiofiles Page"](#)
- Updates [Figure 2-35, "Events Page"](#)
- Updates [Figure 2-36, "Autoprovisioning Page"](#)
- Updates [Figure 2-38, "Firmware Page"](#)
- Updates [Figure 2-39, "Home Page"](#)
- Updates [Section 1.2, "Features"](#) to add [TLS 1.2](#) and [SRTP](#) enhanced security for IP endpoints in a local or cloud-based environment
- Updates [Table 1-1, "Specifications"](#)
- Updates [Table 2-3, "Web Page Navigation"](#)
- Updates [Table 2-11, "SIP Configuration Parameters"](#) to add the [SRTP](#) setting
- Adds [Section 2.4.10, "Configure the SSL Parameters"](#)

Browsers Supported

The following browsers have been tested against firmware version 12.2.0:

- Chrome (version 78.0.3904.70)
- Firefox (version 72.0.2)
- Microsoft Edge (80.0.361.50)
- Internet Explorer (version: 11)

Pictorial Alert Icons

	<p>General Alert</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>Ground</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.



Warning

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



Warning

Electrical Hazard: To prevent injury, this apparatus must be securely attached to the floor/wall in accordance with the installation instructions.



Warning

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

Chapter 1 Product Overview	1
1.1 How to Identify This Product	1
1.2 Features	2
1.3 Specifications	3
1.4 Compliance	4
1.4.1 Safety	4
1.4.2 FCC Statement	4
 Chapter 2 Setting Up the SIP Paging Server	 5
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
Poe	10
Non-Poe	10
Chassis Ground	10
2.3.7 Connect to the Network	11
2.3.8 Confirm that the SIP Paging Server is Up and Running	12
Confirm Power on, Network Connectivity, and Connection Speed	12
Verify Network Activity	12
2.3.9 Announcing the IP Address	13
2.3.10 Restore the Factory Default Settings	13
2.4 Configuring the SIP Paging Server	14
2.4.1 Gather the Required Configuration Information	14
Static or DHCP Addressing?	14
Username and Password for Configuration GUI	14
SIP Settings	14
2.4.2 SIP Paging Server Web Page Navigation	15
2.4.3 Using the Toggle Help Button	16
2.4.4 Log in to the Configuration GUI	18
2.4.5 Configure the Device Parameters	22
Polycom Paging	24
Time Zone Strings	26
2.4.6 Configure the Network Parameters	29
2.4.7 Configure the SIP Parameters	32
Point-to-Point Configuration	38
2.4.8 Configure the Paging Groups (PGROUPS) Parameters	39
2.4.9 Operating the Paging Server	46
DTMF Bypassed	46
DTMF Not Bypassed	46
2.4.10 Configure the SSL Parameters	47
Certificate Info Window	51
Remove Server Certificate Window	52

2.4.11 Configure the Schedules Parameters	53
2.4.12 Configure the Fault Detection Parameters	57
2.4.13 Configure the Audio Parameters	59
User-created Audio Files	63
2.4.14 Configure the Event Parameters	66
Example Packets for Events	68
2.4.15 Configure the Autoprovisioning Parameters	71
Autoprovisioning	73
Sample dhcpd.conf	81
Get Autoprovisioning Template Button	82
2.5 Upgrading the Firmware	83
2.5.1 Upgrade the Firmware	83
2.5.2 Reboot the SIP Paging Server	85
2.6.1 Command Interface Post Commands	86
 Appendix A Setting Up a TFTP Server	90
A.1 Set up a TFTP Server	90
A.1.1 In a LINUX Environment	90
A.1.2 In a Windows Environment	90
 Appendix B Troubleshooting/Technical Support	91
B.1 Frequently Asked Questions (FAQ)	91
B.2 Documentation	91
B.3 Contact Information	92
B.4 Warranty and RMA Information	92

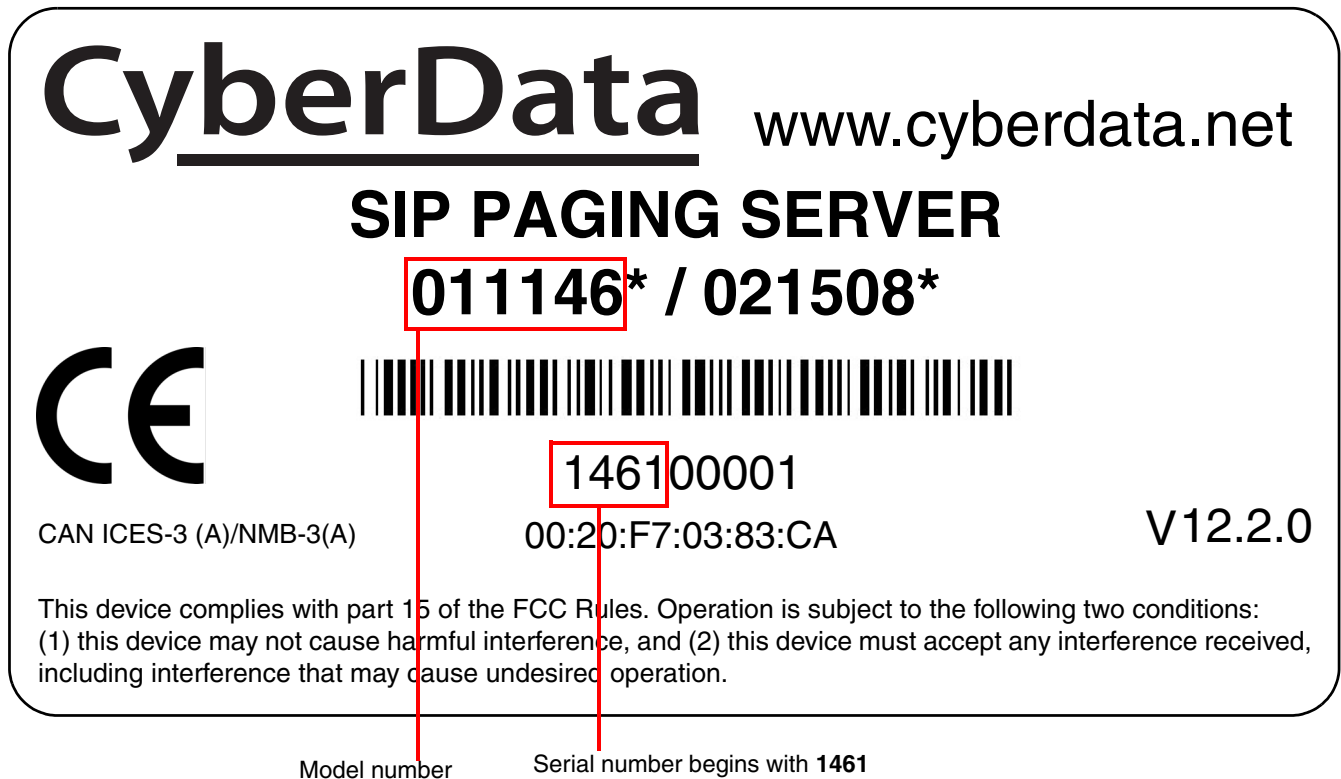
1 Product Overview

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 **1461**.

Figure 1-1. Model Number Label¹



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

1.2 Features

- Up to 25 unique bell files that can be used in up to 250 scheduled events
- Up to 25 stored messages that are utilized through paging groups
- Can page directly to Polycom phones
- Voice prompting and password controlled zones
- SIP RFC 3261 compatible
- NTP-based internal clock
- Multicast output
- Two SIP endpoints (one for Night Ringer)
- DTMF control of zone selection
- Delayed page support
- Line-In connection for background music multicasting
- Line-out connection to support analog amplifiers
- User uploadable audio files
- Web-based configuration and firmware upload
- PoE 802.3af enabled (Power-over-Ethernet)
- 19-inch Rack mount option
- TLS 1.2 and SRTP enhanced security for IP endpoints in a local or cloud-based environment

1.3 Specifications

Table 1-1. Specifications

Specifications	
Protocol	SIP RFC 3261 Compatible
Ethernet I/F	10/100 Mbps
Power Input	PoE 802.3af or 48VDC
Operating Temperature	-10° C to 50° C (14° F to 122° F)
Payload Types	G711, A-law and μ -law, G.722
Network Security	TLS/SSL 1.2 and SRTP
Page Port Output	Balanced 600 Ohm 5VPP
Line In:	
Input Signal Amplitudes	2.0 VPP maximum
Input Impedance	10k Ohm
Line Out:	
Output Signal Amplitudes	2.0 VPP maximum
Output Level	+2dBm nominal
Total Harmonic Distortion	0.5% maximum
Output Impedance	10k Ohm
Dimensions ^a	6.11 inches [155.19 mm] Length
	4.05 inches [102.87 mm] Width
	1.15 inches [29.21 mm] Height
Boxed Weight	1.8 lbs.
Compliance	UL 62368-1, RoHS Compliant, FCC; Part 15 Class A, IEEE 802.3 Compliant; Reference Number for UL: E129569 Vol 4 Sec 1
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 Safety

This product is listed by UL. Representative samples of this product have been evaluated by UL and meet applicable safety standards. (Standard: UL 62368-1). This applies to the following products: 011145, 011146, 011233, 011280, 011295, 011368, 011372

Note You can download the Declaration of Conformity document from the **Downloads** tab of the product's webpage.

1.4.2 FCC Statement

This equipment has been tested and found to comply with the limits for a Class B 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.



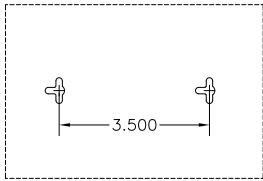

2 Setting Up the SIP Paging Server

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](#).

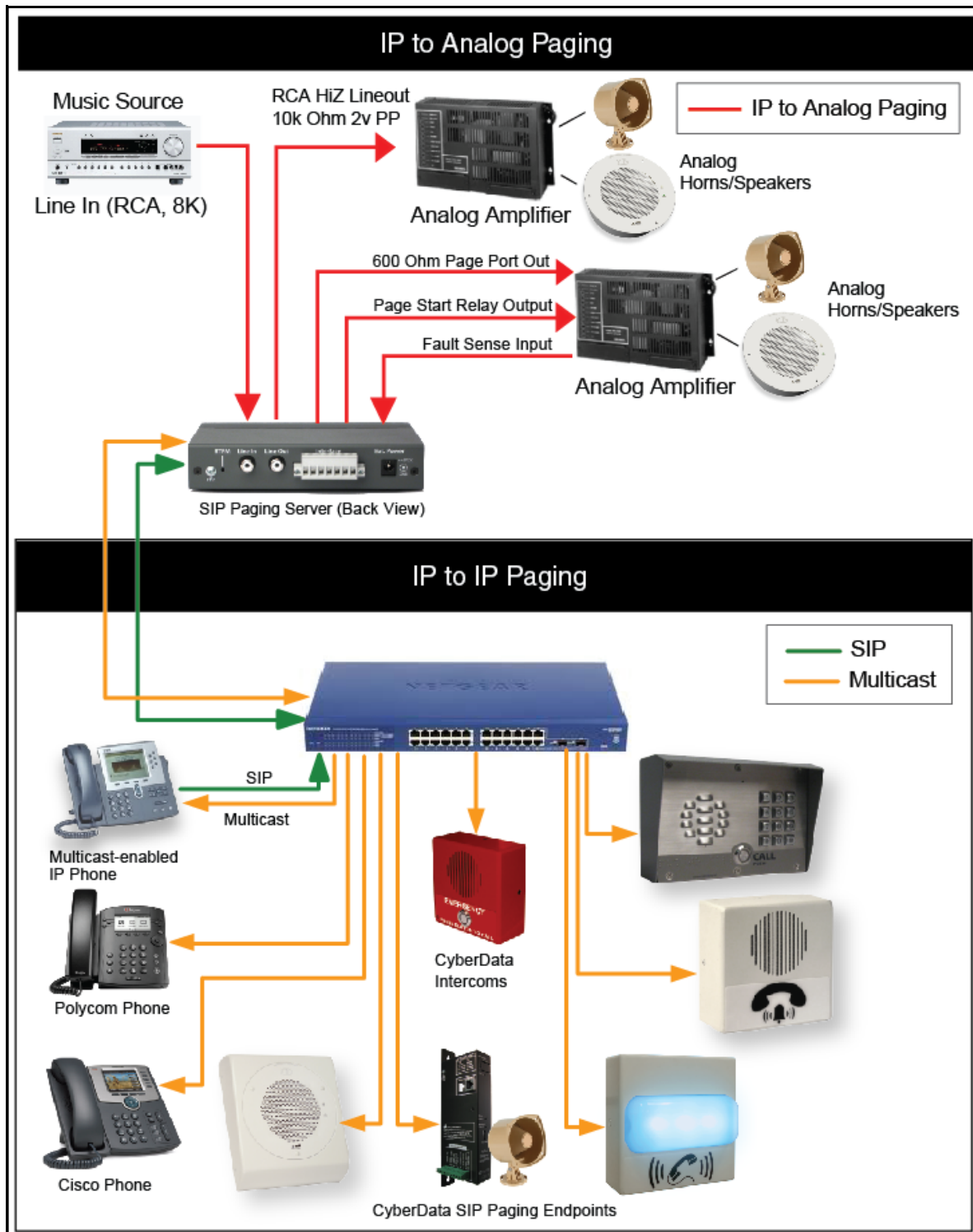
Table 2-1. Parts List

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

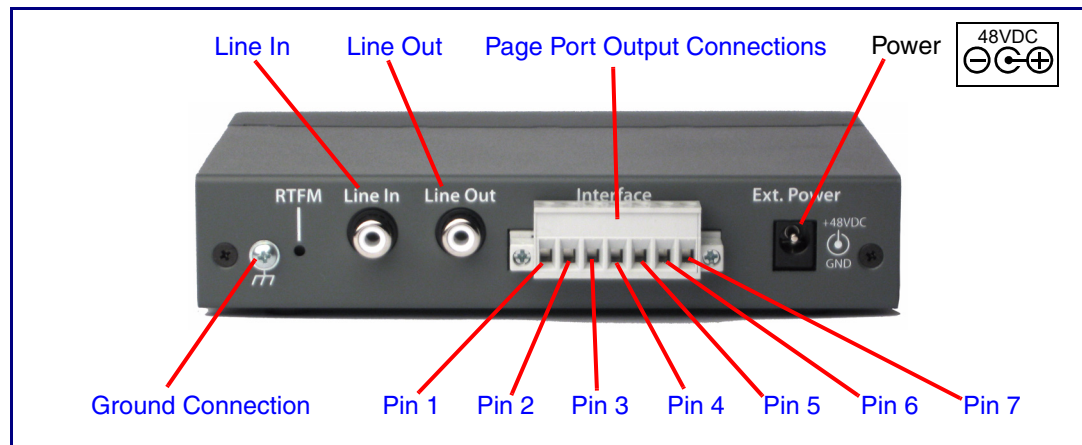


2.3 Connecting the SIP Paging Server

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



2.3.1 Ground Connection

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

2.3.2 Line In

This RCA 10K Ohm Hi-Z input connection allows you to connect the device to The RCA line-out (10K Ohm Hi-Z) of an external audio amplifier. The level of this input can be controlled by the potentiometer located on the front of the device (see [Section 2.4.12, "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 Section 2.3.4.1, "Pin 1 and 2—Fault Sense Input (Common/Sense)" .
Pin 2	Fault Sense Input (Sense). See Section 2.3.4.1, "Pin 1 and 2—Fault Sense Input (Common/Sense)" .
Pin 3	Positive 600-Ohm Audio Output ^a . See Section 2.3.4.2, "Pin 3, 4, and 5—Positive/Negative 600-Ohm Audio Output/Audio Ground Reference" .
Pin 4	Negative 600-Ohm Audio Output ^a . See Section 2.3.4.2, "Pin 3, 4, and 5—Positive/Negative 600-Ohm Audio Output/Audio Ground Reference" .
Pin 5	Audio Ground Reference. See Section 2.3.4.2, "Pin 3, 4, and 5—Positive/Negative 600-Ohm Audio Output/Audio Ground Reference" .
Pin 6	Relay Contact - Common ^b . See Section 2.3.4.3, "Pin 6 and 7—Relay Contact (Common/Normally Open)" .
Pin 7	Relay Contact - Normally Open ^b . See Section 2.3.4.3, "Pin 6 and 7—Relay Contact (Common/Normally Open)" .

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

b. 1 Amp at 30 VDC for continuous loads

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

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

When enabled via the web interface ([Section 2.4.12, "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.

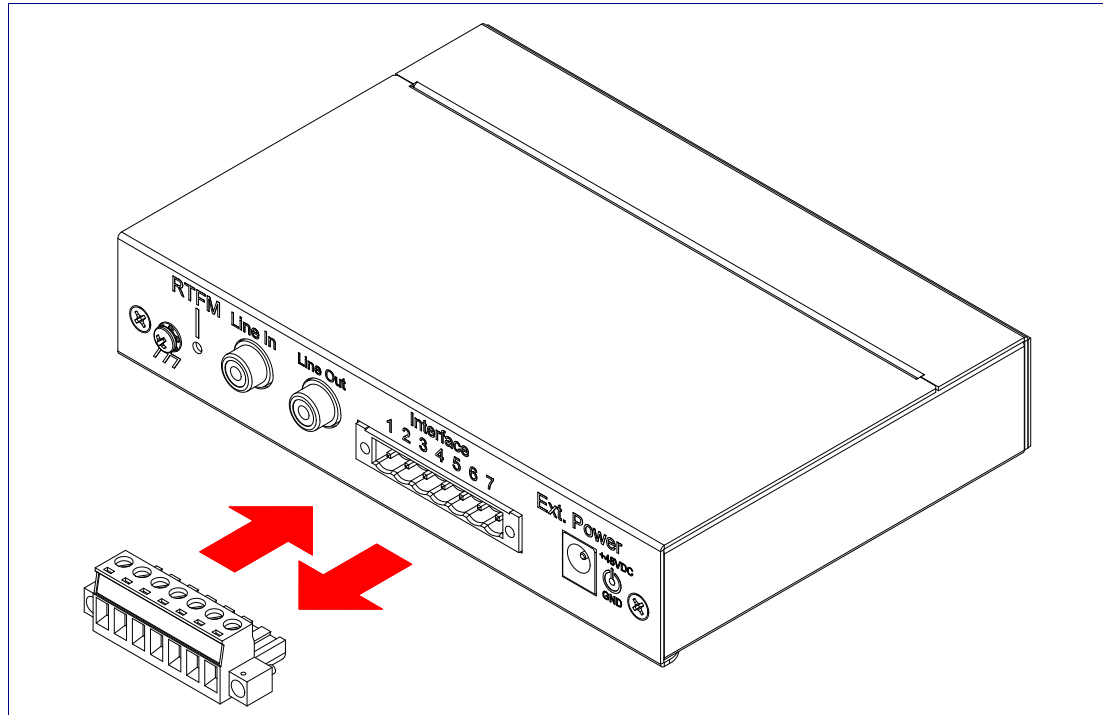
2.3.4.3 Pin 6 and 7—Relay Contact (Common/Normally Open)

When enabled on the web interface ([Section 2.4.5, "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.

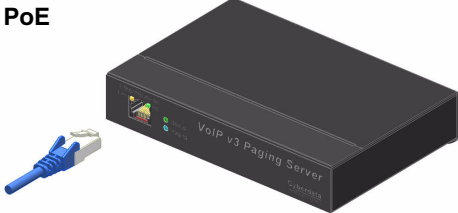


Figure 2-3. Removable Interface Connector



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>PoE</p> 	<p>To set up the SIP Paging Server, connect the device to your network:</p> <p>Poe</p> <ul style="list-style-type: none"> 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.
<p>Non PoE (with 48 VDC power supply)</p> 	<p>Non-Poe</p> <ul style="list-style-type: none"> For Non-PoE, connect the SIP Paging Server to a 48VDC power supply. See the figure on the left. Note: Do not use both PoE and external power. Alternatively, you can use our part# 010867 PoE Power Injector as a cost-effective option.
<p>Chassis Ground</p>  <p>Chassis Ground</p>	<p>Chassis Ground</p> <ul style="list-style-type: none"> If required, connect the earth grounding wire to the Chassis Ground. See the figure on the left.

2.3.7 Connect to the Network

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

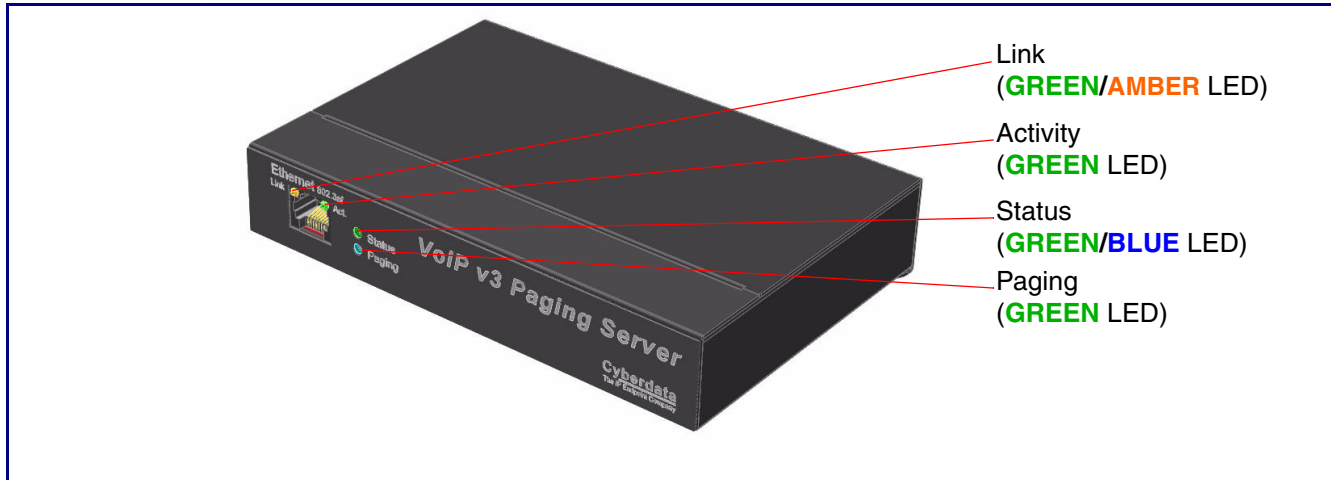
Figure 2-5. Connecting to the Network



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. Paging Server LEDs



2.3.8.1 Confirm Power on, Network Connectivity, and Connection Speed

When you plug in the Ethernet cable or power supply:

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

2.3.8.2 Verify Network Activity

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

2.3.9 Announcing the IP Address

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

Figure 2-7. RTFM Switch



2.3.10 Restore the Factory Default Settings

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

Use the RTFM switch (see [Figure 2-7](#)) on the back of the unit to restore these parameters to the factory default settings.

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

Table 2-2. Factory Default Settings

Parameter	Factory Default Setting
IP Addressing	DHCP
IP Address ^a	10.10.10.10
Web Access Username	admin
Web Access Password	admin
Subnet Mask ^a	255.0.0.0
Default Gateway ^a	10.0.0.1

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

To restore these parameters to the factory default settings:

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

2.4 Configuring the SIP Paging Server

Use this section to configure the VoIP paging server.

2.4.1 Gather the Required Configuration Information

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

2.4.1.1 Static or DHCP Addressing?

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

- IP Address
- Subnet Mask
- Default Gateway

2.4.1.2 Username and Password for Configuration GUI

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

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

2.4.1.3 SIP Settings

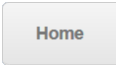



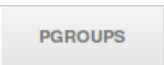

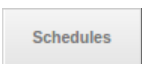
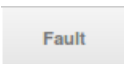
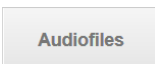
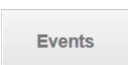


To configure the SIP parameters, determine whether you want to register with the server. If you do, determine the number of minutes the registration lease remains valid, and whether you want to automatically unregister when you reboot. To configure the SIP parameters, you also need to determine the values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

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

2.4.2 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

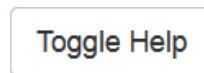
Web Page Item	Description
	Link to the Home page.
	Link to the Device page.
	Link to the Network page.
	Link to go to the SIP page.
	Link to the PGROUPS page.
	Link to the SSL page.
	Link to the Schedules page.
	Link to the Fault page.
	Link to the Audiofiles page.
	Link to the Events page.
	Link to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

2.4.3 Using the Toggle Help Button

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

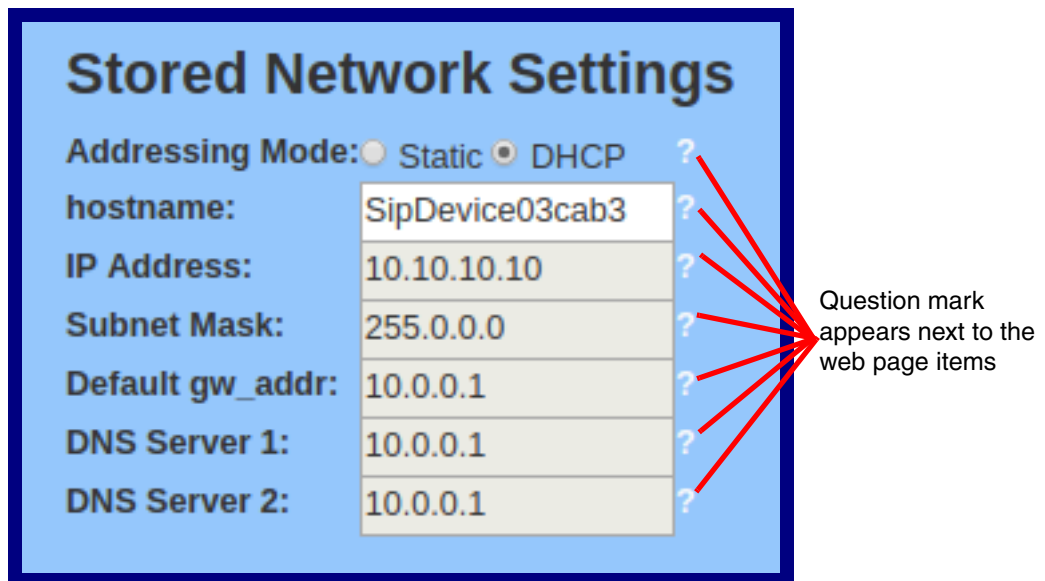
1. Click on the **Toggle Help** button that is on the UI webpage. See [Figure 2-8](#) and [Figure 2-9](#).

Figure 2-8. Toggle/Help Button



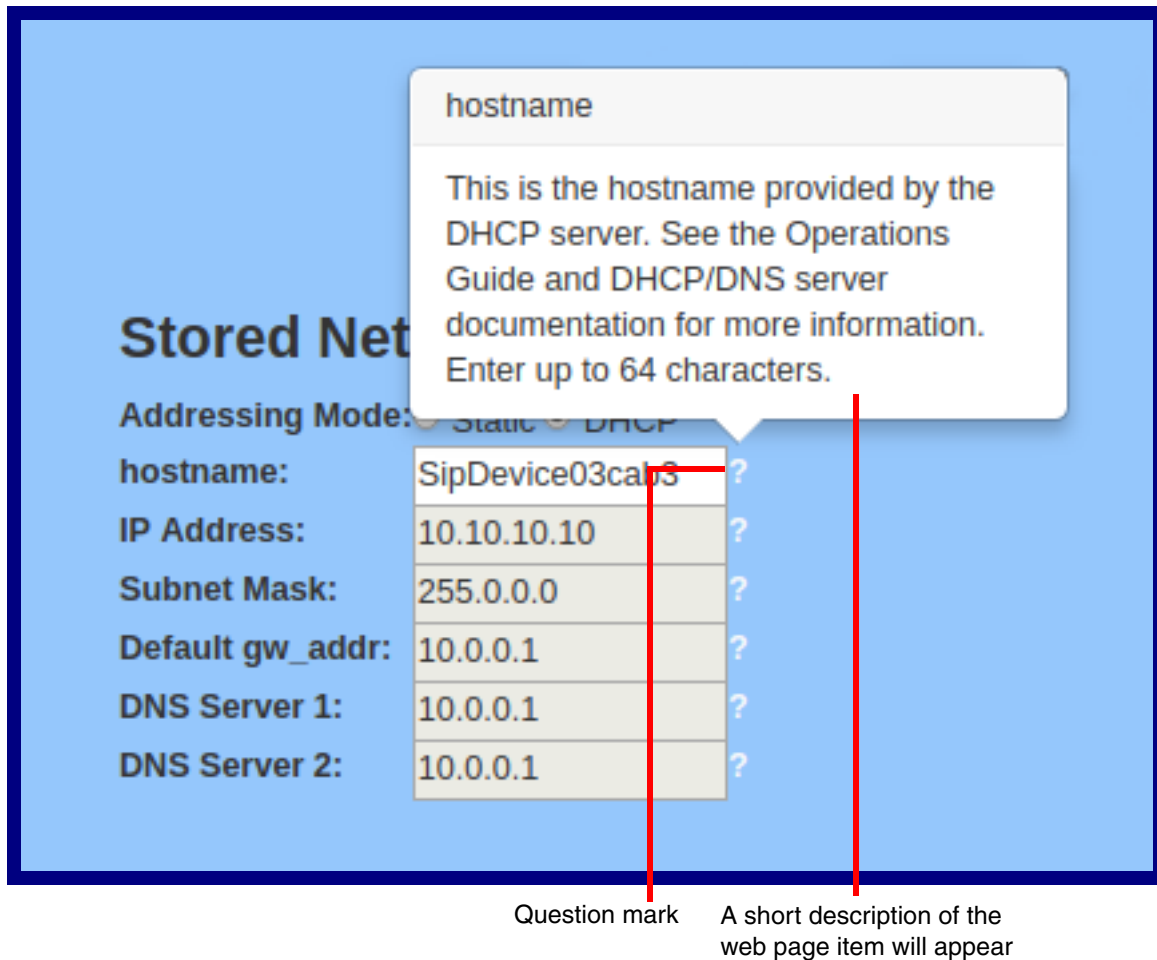
2. You will see a question mark (?) appear next to each web page item that has been provided with a short description by the Help feature. See [Figure 2-9](#).

Figure 2-9. 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 2-10](#).

Figure 2-10. Short Description Provided by the Help Feature



2.4.4 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 10.10.10.10.

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 2.4.6, "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 2-11. Home Page

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

CyberData v3.1 Paging Server

Current Status

Serial Number: 146100001
Mac Address: 00:20:f7:04:62:a9
Firmware Version: v12.2.0

IP Addressing: DHCP
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:

SIP Mode: Enabled
Event Reporting: Disabled
Nightringer: Disabled

Primary SIP Server: **Not registered**
Backup Server 1: Not registered
Backup Server 2: Not registered
Nightringer Server: Not registered

Admin Settings

Username:
Password:
Confirm Password:

Import Settings

No file chosen

Export Settings


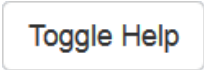
4. On the **Home Page**, review the setup details and navigation buttons described in [Table 2-4](#)

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
Admin Settings	
Username ?	The username to access the web interface. Enter up to 25 characters.
Password ?	The password to access the web interface. Enter up to 25 characters.
Confirm Password ?	Confirm the web interface password.
Current Status	
Serial Number	Shows the device serial number.
Mac Address	Shows the device Mac address.
Firmware Version	Shows the current firmware version.
IP Addressing	Shows the current IP addressing setting (DHCP or static).
IP Address	Shows the current IP address.
Subnet Mask	Shows the current subnet mask address.
Default Gateway	Shows the current default gateway address.
DNS Server 1	Shows the current DNS Server 1 address.
DNS Server 2	Shows the current DNS Server 2 address.
SIP 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.
Import Settings	
	Use this button to select a configuration file to import.
	After selecting a configuration file, click Import to import the configuration from the selected file. Then, click Save and Reboot to store changes.
Export Settings	
	Click Export to export the current configuration to a file.
	Click the Save button to save your configuration settings. Note: You need to reboot for changes to take effect.

Table 2-4. Home Page Overview (continued)

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

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

At this point you can:

- Review the SIP Paging Server's **Current Settings**. Use the RTFM switch to restore the factory default settings. See [Section 2.3.10, "Restore the Factory Default Settings"](#).
- Configure the device parameters. Click on the **Device** button and see [Section 2.4.5, "Configure the Device Parameters"](#) for instructions.
- Configure the network parameters. Click on the **Network** button and see [Section 2.4.6, "Configure the Network Parameters"](#) for instructions.
- Configure the SIP parameters. Click on the **SIP** button and see [Section 2.4.7, "Configure the SIP Parameters"](#) for instructions.
- Configure the PGROUPS parameters. Click on the **PGROUPS** button and see [Section 2.4.8, "Configure the Paging Groups \(PGROUPS\) Parameters"](#) for instructions.
- Configure the fault detection parameters. Click on the **Fault** button and see [Section 2.4.12, "Configure the Fault Detection Parameters"](#) for instructions.
- Configure the audio parameters. Click on the **Audiofiles** button and see [Section 2.4.13, "Configure the Audio Parameters"](#) for instructions.
- Configure the event parameters. Click on the **Events** button and see [Section 2.4.14, "Configure the Event Parameters"](#) for instructions.
- Configure the autoprovisioning parameters. Click on the **Autoprovisioning** button and see [Section 2.4.15, "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 2.5, "Upgrading the Firmware"](#) for instructions.

2.4.5 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 2-12](#).

Figure 2-12. Device Page

CyberData v3.1 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: ☐

Relay Settings

Activate Relay on Local Audio: ☐

Clock Settings

Set Time with NTP server on boot: ☐

NTP Server:

Posix Timezone String (see manual):

Periodically sync time with server: ☐

Time update period (in hours):

Current Time: 18:23:55

Misc Settings

Device Name:

Bypass DTMF: ☐

DTMF Duration:

Beep on Init: ☐

Beep on Page: ☒

Enable Polycom Paging on Multicast: ☐

Polycom Transmit Channel:

Disable HTTPS (NOT recommended): ☐

Buttons: Save, Reboot, Test Audio, Test Multicast, Test Relay, 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
Line-in Settings	
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 Play Line-in Audio via Multicast (Fault Detection)
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 silence is detected on line-input, the multicast stream will be stopped to reduce network traffic.
Relay Settings	
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.
Clock Settings	
Set Time with NTP Server on boot ?	When selected, the time is set with an external NTP server when the device restarts.
NTP Server ?	Use this field to set the address (in IPv4 dotted decimal notation or as a canonical name) for the NTP Server. This field can accept canonical names of up to 64 characters in length.
Posix Timezone String ?	See Section 2.4.5.2, "Time Zone Strings" for information about how to use the Posix Timezone String to specify time zone and daylight savings time where applicable. Enter up to 63 characters.
Periodically sync time with server ?	When selected, the time is periodically updated with the NTP server at the configured interval below.
Time update period (in hours) ?	The time interval after which the device will contact the NTP server to update the time. Enter up to 4 digits.
Current Time	Allows you to input the current time. (6 character limit)
Misc Settings	
Device Name ?	Type the device name. Enter up to 25 characters.
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).

Table 2-5. Device Configuration Parameters (continued)

Web Page Item	Description
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.
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 Test Audio button to do an audio test. When the Test Audio button is pressed, you will hear a voice message for testing the device audio quality and volume.
	This button will cause the device to send a 5 second ULAW multicast stream to 234.2.1.200:2200.
	Click on the Test Relay button to do a relay test.
	Click the Save button to save your configuration settings. Note: You need to reboot for changes to take effect.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

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

2.4.5.1 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. Save and reboot to store changes.

2.4.5.2 Time Zone Strings

The posix time zone string tells the internal date and time utilities how to handle daylight savings time for different time zones. [Table 2-6](#) shows some common strings.

Table 2-6. Common Time Zone Strings

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

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

[Table 2-7](#) shows a breakdown of the parts that constitute the following time zone string:

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

Table 2-7. Time Zone String Parts

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

Time Zone String
Examples

Table 2-8 has some more examples of time zone strings.

Table 2-8. Time Zone String Examples

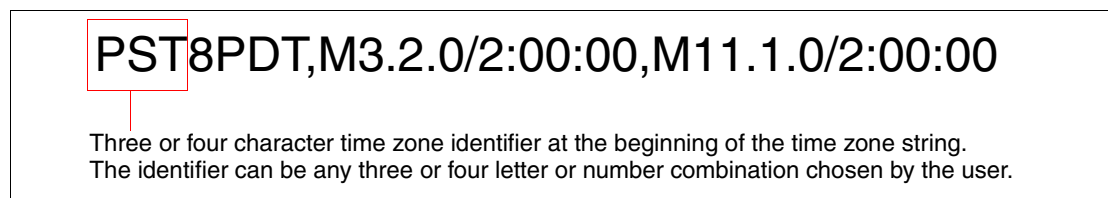
Time Zone	Time Zone String
Tokyo ^a	IST-9
Berlin ^b	CET-1MET,M3.5.0/1:00,M10.5.0/1:00

a. Tokyo does not use daylight savings time.

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

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

Figure 2-13. Three or Four Character Time Zone Identifier



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

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

World GMT Table

Table 2-9 has information about the GMT time in various time zones.

Table 2-9. World GMT Table

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

Table 2-9. World GMT Table (continued)

Time Zone	City or Area Zone Crosses
GMT+1	Berlin, Rome
GMT+2	Israel, Cairo
GMT+3	Moscow, Kuwait
GMT+4	Abu Dhabi, Muscat
GMT+5	Islamabad, Karachi
GMT+6	Almaty, Dhaka
GMT+7	Bangkok, Jakarta
GMT+8	Hong Kong, Beijing
GMT+9	Tokyo, Osaka
GMT+10	Sydney, Melbourne, Guam
GMT+11	Magadan, Soloman Is.
GMT+12	Fiji, Wellington, Auckland

2.4.6 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 v3.1 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



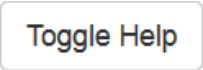
On the **Network** page, enter values for the parameters indicated in [Table 2-10](#).

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. Network Configuration Parameters

Web Page Item	Description
Stored Network Settings	
Addressing Mode ?	Select either DHCP IP Addressing or Static Addressing by marking the appropriate radio button. DHCP Addressing mode is enabled on default and the device will attempt to resolve network addressing with the local DHCP server upon boot. If DHCP Addressing fails, the device will revert to the last known IP address or the factory default address if no prior DHCP lease was established. See Section 2.3.10, "Restore the Factory Default Settings" for factory default settings. Be sure to click Save and Reboot to store changes when configuring a Static address.
Hostname ?	This is the hostname provided by the DHCP server. See the DHCP/DNS server documentation for more information. Enter up to 64 characters.
IP Address ?	Enter the Static IPv4 network address in dotted decimal notation.
Subnet Mask ?	Enter the Subnet Mask in dotted decimal notation.
Default Gateway ?	Enter the Default Gateway IPv4 address in dotted decimal notation.
DNS Server 1 ?	Enter the primary DNS Server IPv4 address in dotted decimal notation.
DNS Server 2 ?	Enter the secondary DNS Server IPv4 address in dotted decimal notation.
DHCP Timeout in seconds ?	Specify the desired time-out duration (in seconds) that the device will wait for a response from the DHCP server before reverting back to the stored static IP address. The stored static IP address may be the last known IP address or the factory default address if no prior DHCP lease was established. Enter up to 8 characters. A value of -1 will retry forever.
VLAN Settings	
VLAN ID (0-4095) ?	Specify the IEEE 802.1Q VLAN ID number. Enter up to 4 digits. Note: The device supports 802.1Q VLAN tagging support. The switch port connected to the device will need to be in "trunking mode" for the VLAN tags to propagate.
VLAN Priority (0-7) ?	Specify the IEEE 802.1p VLAN priority level. Enter 1 digit. A value of 0 may cause the VLAN ID tag to be ignored.
Current Network Settings	
IP Address	Shows the current Static IP address.
Subnet Mask	Shows the current Subnet Mask address.
Default Gateway	Shows the current Default Gateway address.
DNS Server 1	Shows the current DNS Server 1 address.
DNS Server 2	Shows the current DNS Server 2 address.

Table 2-10. Network Configuration Parameters (continued)

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

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**.

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

2.4.7 Configure the SIP 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 v3.1 Paging Server

SIP Settings

Enable SIP operation: ☒

SIP Transport Protocol: **UDP** ▼

TLS Version: **1.2 only (recommended)** ▼

Verify Server Certificate: ☒

Register with a SIP Server: ☒

Use Cisco SRST: ☐

Primary SIP Server: **10.0.0.253**

Primary SIP User ID: **199**

Primary SIP Auth ID: **199**

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

Backup SIP Server 1:

Backup SIP User ID 1:

Backup SIP Auth ID 1:

Backup SIP Auth Password 1:

Backup SIP Server 2:

Backup SIP User ID 2:

Backup SIP Auth ID 2:

Backup SIP Auth Password 2:

Remote SIP Port: **5060**

Local SIP Port: **5060**

Outbound Proxy:

Outbound Proxy Port: **0**

Disable rport Discovery: ☐

Buffer SIP Calls: ☐

Re-registration Interval (in seconds): **360**

Unregister on Boot: ☐

Keep Alive Period: **10000**

Nightringer Settings

Enable Nightringer: ☐

SIP Server: **10.0.0.253**

Remote SIP Port: **5060**

Local SIP Port: **5061**

Outbound Proxy:

Outbound Proxy Port: **0**

User ID: **241**

Authenticate ID: **241**

Authenticate 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**

Codec Selection

Force Selected Codec: ☐

Codec: **PCMU (G.711, u-law)** ▼

RTP Settings

RTP Port (even): **10500**

Jitter Buffer: **50**

SRTP: **Disabled** ▼

Save **Reboot** **Toggle Help**

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

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 2-11. SIP Configuration Parameters

Web Page Item	Description
SIP Settings	
Enable SIP Operation ?	When enabled, the device will transmit, receive, and process SIP messages according to the configured SIP settings below.
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.
Register with a SIP Server ?	When enabled, the device will attempt to register to the configured SIP Server(s) on this page. To configure the device to send and receive point-to-point SIP calls, enable SIP Operation and disable Register with a SIP Server (see Section 2.4.7.1, "Point-to-Point Configuration").
Use Cisco SRST ?	When enabled, the backup servers are handled according to Cisco SRST (Survivable Remote Site Telephony). It is required for use in clustered Cisco Unified Communications Manager topologies.
Primary SIP Server ?	Enter the SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the primary SIP server. This field can accept entries of up to 255 characters in length.
Primary SIP User ID ?	Specify the SIP User ID for the Primary SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the primary SIP server. Enter up to 64 alphanumeric characters.
Primary SIP Auth ID ?	Specify the Authenticate ID for the Primary SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Primary SIP Auth Password ?	Specify the Authenticate Password for the Primary SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Server 1 ?	Enter the backup SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the backup SIP server. This field can accept entries of up to 255 characters in length.
Backup SIP User ID 1 ?	Specify the SIP User ID for the first backup SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the first backup SIP server. Enter up to 64 alphanumeric characters.
Backup SIP Auth ID 1 ?	Specify the Authenticate ID for the first backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.



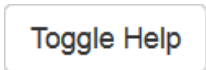
Table 2-11. SIP Configuration Parameters (continued)

Web Page Item	Description
Backup SIP Auth Password 1 ?	Specify the Authenticate Password for the first backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Server 2 ?	Enter a second backup SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the second backup SIP server. This field can accept entries of up to 255 characters in length.
Backup SIP User ID 2 ?	Specify the SIP User ID for the second backup SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the second backup SIP server. Enter up to 64 alphanumeric characters.
Backup SIP Auth ID 2 ?	Specify the Authenticate ID for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Auth Password 2 ?	Specify the Authenticate Password for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Remote SIP Port ?	The Remote SIP Port is the port number the device will use as the destination port when sending SIP messages. The default Remote SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
Local SIP Port ?	The Local SIP Port is the port number the device will use to receive SIP messages. The default Local SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
Outbound Proxy ?	Enter the Outbound Proxy address as an IPv4 address in dotted decimal notation or a fully qualified domain name (FQDN). When an IP address is configured, the device will send all SIP messages to this IP address. When an FQDN is configured, the device will run DNS NAPTR, SRV, and A queries on the FQDN to resolve an IP address to which it will send all SIP messages. This field can accept entries of up to 255 characters in length.
Outbound Proxy Port ?	The Outbound Proxy Port is port number used as the destination port when sending SIP messages to the outbound proxy. A value of 0 will default to 5060. The supported range is 0-65536. Enter up to 5 digits.
Disable rport Discovery ?	Disabling rport Discovery will prevent the device from including the public WAN IP address and port number in the contact information that is sent to the remote SIP servers. This will generally only need to be enabled when using an SBC or SIP ALG in conjunction with a remote SIP server.
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.
Re-registration Interval (in seconds) ?	The SIP Re-registration interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
Unregister on Boot ?	When enabled, the device will send one registration with an expiry of 0 on boot.
Keep Alive Period ?	The minimum time in milliseconds between keep-alive packets sent for nat traversal. A value of 0 will disable keep alive packets.
RTP Settings	
RTP Port (even) ?	Specify the port number used for the RTP stream after establishing a SIP call. This port number must be an even number and defaults to 10500. The supported range is 0-65536. Enter up to 5 digits.

Table 2-11. SIP Configuration Parameters (continued)

Web Page Item	Description
Jitter Buffer ?	Specify the size of the jitter buffer (in milliseconds) used for SIP calls. Valid values are 50-1000.
SRTP ?	When enabled, a SIP call's audio streams are encrypted using SRTP.
Nightringer Settings	
Enable Nightringer ?	When Nightringer is enabled, the device will attempt to register a second extension with the SIP server. Any calls made to this extension will play a ringtone (corresponds to Night Ring on the Audiofiles page). By design, it is not possible to answer a call to the Nightringer extension.
SIP Server ?	Enter the SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's Nightringer extension on the SIP server. This field can accept entries of up to 255 characters in length.
Remote SIP Port ?	The Remote SIP Port is the port number the device will use as the destination port when sending SIP messages for the Nightringer extension. The default Remote SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
Local SIP Port ?	The Local SIP Port is the port number the device will use to receive SIP messages for the Nightringer extension. This value cannot be the same as the Local SIP Port for the primary extension. The default Local SIP Port is 5061. The supported range is 0-65536. Enter up to 5 digits.
Outbound Proxy ?	Enter the Outbound Proxy address as an IPv4 address in dotted decimal notation or a fully qualified domain name (FQDN). When an IP address is configured, the device will send all SIP messages to this IP address for the Nightringer extension. When an FQDN is configured, the device will run DNS NAPTR, SRV, and A queries on the FQDN to resolve an IP address to which it will send all SIP messages for the Nightringer extension. This field can accept entries of up to 255 characters in length.
Outbound Proxy Port ?	The Outbound Proxy Port is port number used as the destination port when sending SIP messages to the outbound proxy for the Nightringer extension. A value of 0 will default to 5060. The supported range is 0-65536. Enter up to 5 digits.
User ID ?	Specify the SIP User ID for the SIP server. This parameter becomes the user portion of the SIP-URI for the device's Nightringer extension. Enter up to 64 alphanumeric characters.
Authenticate ID ?	Specify the Authenticate ID for the SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Authenticate Password ?	Specify the Authenticate Password for the SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Re-registration Interval (in seconds) ?	The SIP Re-registration Interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
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.
Call Disconnection	

Table 2-11. SIP Configuration Parameters (continued)

Web Page Item	Description
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.
Codec Selection	
Force Selected Codec ?	When configured, this option will allow you to force the device to negotiate for the selected codec [PCMU(G.711, u-law), PCMA(G.711, a-law), or G.722]. Otherwise, the device will perform codec negotiation using the default list of supported codecs.
Codec ?	Select desired codec (only one may be chosen).
	Click the Save button to save your configuration settings. Note: You need to reboot for changes to take effect.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

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

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

<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.

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

2.4.7.1 Point-to-Point Configuration

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

1. On the **SIP** page (Figure 2-16), make sure that the **Register with a SIP Server** parameter is not selected.
2. Type the IP address of the remote device that you want to contact into the **Dial out Extension** field

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

Figure 2-16. SIP Page Set to Point-to-Point Mode

The screenshot shows the 'SIP' configuration page of the CyberData v3.1 Paging Server. The page has a navigation bar at the top with tabs: Home, Device, Network, SIP (selected), PGROUPS, SSL, Schedules, Fault, Audiofiles, Events, Autoprov, and Firmware. The main title is 'CyberData v3.1 Paging Server'. Below the title, there are two main sections: 'SIP Settings' and 'Nightringer Settings'. In the 'SIP Settings' section, the 'Register with a SIP Server' checkbox is unchecked, and a red line points to it with the text 'Device is set to NOT register with a SIP server'. Other settings include 'Enable SIP operation' (checked), 'SIP Transport Protocol' (UDP), 'TLS Version' (1.2 only (recommended)), 'Verify Server Certificate' (checked), 'Use Cisco SRST' (unchecked), 'Primary SIP Server' (10.0.0.253), 'Primary SIP User ID' (199), 'Primary SIP Auth ID' (199), 'Primary SIP Auth Password' (*****), 'Backup SIP Server 1', 'Backup SIP User ID 1', 'Backup SIP Auth ID 1', and 'Backup SIP Auth Password 1'. The 'Nightringer Settings' section includes 'Enable Nightringer' (unchecked), 'SIP Server' (10.0.0.253), 'Remote SIP Port' (5060), 'Local SIP Port' (5061), 'Outbound Proxy', 'Outbound Proxy Port' (0), 'User ID' (241), 'Authenticate ID' (241), 'Authenticate Password' (*****), 'Re-registration Interval (in seconds)' (360), 'Relay rings to multicast' (unchecked), 'Multicast Address' (224.1.2.32), and 'Multicast Port' (2020). At the bottom, there is a 'Call Disconnection' section.

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

2.4.8 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 2-17](#).

Figure 2-17. PGROUPS Page

#	Address	Port	Name	Code	TTL	Lineout	
0	234.2.1.1	2000	PagingGroup00	255	Yes		Edit
1	234.2.1.2	2002	PagingGroup01	255	Yes		Edit
2	234.2.1.3	2004	PagingGroup02	255	Yes		Edit
3	234.2.1.4	2006	PagingGroup03	255	Yes		Edit
4	234.2.1.5	2008	PagingGroup04	255	Yes		Edit
5	234.2.1.6	2010	PagingGroup05	255	Yes		Edit
6	234.2.1.7	2012	PagingGroup06	255	Yes		Edit
7	234.2.1.8	2014	PagingGroup07	255	Yes		Edit
8	234.2.1.9	2016	PagingGroup08	255	Yes		Edit
9	234.2.1.10	2018	PagingGroup09	255	Yes		Edit
10	234.2.1.11	2020	PagingGroup10	255	Yes		Edit
11	234.2.1.12	2022	PagingGroup11	255	Yes		Edit
12	234.2.1.13	2024	PagingGroup12	255	Yes		Edit
13	234.2.1.14	2026	PagingGroup13	255	Yes		Edit
14	234.2.1.15	2028	PagingGroup14	255	Yes		Edit
15	234.2.1.16	2030	PagingGroup15	255	Yes		Edit
16	234.2.1.17	2032	PagingGroup16	255	Yes		Edit
17	234.2.1.18	2034	PagingGroup17	255	Yes		Edit
18	234.2.1.19	2036	PagingGroup18	255	Yes		Edit
19	234.2.1.20	2038	PagingGroup19	255	Yes		Edit
20	234.2.1.21	2040	PagingGroup20	255	Yes		Edit
21	234.2.1.22	2042	PagingGroup21	255	Yes		Edit
22	234.2.1.23	2044	PagingGroup22	255	Yes		Edit
23	234.2.1.24	2046	PagingGroup23	255	Yes		Edit
24	234.2.1.25	2048	PagingGroup24	255	Yes		Edit
25	234.2.1.26	2050	PagingGroup25	255	Yes		Edit
26	234.2.1.27	2052	PagingGroup26	255	Yes		Edit
27	234.2.1.28	2054	PagingGroup27	255	Yes		Edit

Figure 2-18. PGROUPS Page (continued)

19	234.2.1.20	2038	PagingGroup19	255	Yes	Edit
20	234.2.1.21	2040	PagingGroup20	255	Yes	Edit
21	234.2.1.22	2042	PagingGroup21	255	Yes	Edit
22	234.2.1.23	2044	PagingGroup22	255	Yes	Edit
23	234.2.1.24	2046	PagingGroup23	255	Yes	Edit
24	234.2.1.25	2048	PagingGroup24	255	Yes	Edit
25	234.2.1.26	2050	PagingGroup25	255	Yes	Edit
26	234.2.1.27	2052	PagingGroup26	255	Yes	Edit
27	234.2.1.28	2054	PagingGroup27	255	Yes	Edit
28	234.2.1.29	2056	PagingGroup28	255	Yes	Edit
29	234.2.1.30	2058	PagingGroup29	255	Yes	Edit
30	234.2.1.31	2060	PagingGroup30	255	Yes	Edit
31	234.2.1.32	2062	PagingGroup31	255	Yes	Edit
32	234.2.1.33	2064	PagingGroup32	255	Yes	Edit
33	234.2.1.34	2066	PagingGroup33	255	Yes	Edit
34	234.2.1.35	2068	PagingGroup34	255	Yes	Edit
35	234.2.1.36	2070	PagingGroup35	255	Yes	Edit
36	234.2.1.37	2072	PagingGroup36	255	Yes	Edit
37	234.2.1.38	2074	PagingGroup37	255	Yes	Edit
38	234.2.1.39	2076	PagingGroup38	255	Yes	Edit
39	234.2.1.40	2078	PagingGroup39	255	Yes	Edit
40	234.2.1.41	2080	PagingGroup40	255	Yes	Edit
41	234.2.1.42	2082	PagingGroup41	255	Yes	Edit
42	234.2.1.43	2084	PagingGroup42	255	Yes	Edit
43	234.2.1.44	2086	PagingGroup43	255	Yes	Edit
44	234.2.1.45	2088	PagingGroup44	255	Yes	Edit
45	234.2.1.46	2090	PagingGroup45	255	Yes	Edit
46	234.2.1.47	2092	PagingGroup46	255	Yes	Edit
47	234.2.1.48	2094	PagingGroup47	255	Yes	Edit

Figure 2-19. PGROUPS Page (continued)

47	234.2.1.48	2094	PagingGroup47	255	Yes	Edit
48	234.2.1.49	2096	PagingGroup48	255	Yes	Edit
49	234.2.1.50	2098	PagingGroup49	255	Yes	Edit
50	234.2.1.51	2100	PagingGroup50	255	Yes	Edit
51	234.2.1.52	2102	PagingGroup51	255	Yes	Edit
52	234.2.1.53	2104	PagingGroup52	255	Yes	Edit
53	234.2.1.54	2106	PagingGroup53	255	Yes	Edit
54	234.2.1.55	2108	PagingGroup54	255	Yes	Edit
55	234.2.1.56	2110	PagingGroup55	255	Yes	Edit
56	234.2.1.57	2112	PagingGroup56	255	Yes	Edit
57	234.2.1.58	2114	PagingGroup57	255	Yes	Edit
58	234.2.1.59	2116	PagingGroup58	255	Yes	Edit
59	234.2.1.60	2118	PagingGroup59	255	Yes	Edit
60	234.2.1.61	2120	PagingGroup60	255	Yes	Edit
61	234.2.1.62	2122	PagingGroup61	255	Yes	Edit
62	234.2.1.63	2124	PagingGroup62	255	Yes	Edit
63	234.2.1.64	2126	PagingGroup63	255	Yes	Edit
64	234.2.1.65	2128	PagingGroup64	255	Yes	Edit
65	234.2.1.66	2130	PagingGroup65	255	Yes	Edit
66	234.2.1.67	2132	PagingGroup66	255	Yes	Edit
67	234.2.1.68	2134	PagingGroup67	255	Yes	Edit
68	234.2.1.69	2136	PagingGroup68	255	Yes	Edit
69	234.2.1.70	2138	PagingGroup69	255	Yes	Edit
70	234.2.1.71	2140	PagingGroup70	255	Yes	Edit
71	234.2.1.72	2142	PagingGroup71	255	Yes	Edit
72	234.2.1.73	2144	PagingGroup72	255	Yes	Edit
73	234.2.1.74	2146	PagingGroup73	255	Yes	Edit
74	234.2.1.75	2148	PagingGroup74	255	Yes	Edit
75	234.2.1.76	2150	PagingGroup75	255	Yes	Edit

Figure 2-20. PGROUPS Page (continued)

77	234.2.1.78	2154	PagingGroup77	255	Yes	Edit
78	234.2.1.79	2156	PagingGroup78	255	Yes	Edit
79	234.2.1.80	2158	PagingGroup79	255	Yes	Edit
80	234.2.1.81	2160	PagingGroup80	255	Yes	Edit
81	234.2.1.82	2162	PagingGroup81	255	Yes	Edit
82	234.2.1.83	2164	PagingGroup82	255	Yes	Edit
83	234.2.1.84	2166	PagingGroup83	255	Yes	Edit
84	234.2.1.85	2168	PagingGroup84	255	Yes	Edit
85	234.2.1.86	2170	PagingGroup85	255	Yes	Edit
86	234.2.1.87	2172	PagingGroup86	255	Yes	Edit
87	234.2.1.88	2174	PagingGroup87	255	Yes	Edit
88	234.2.1.89	2176	PagingGroup88	255	Yes	Edit
89	234.2.1.90	2178	PagingGroup89	255	Yes	Edit
90	234.2.1.91	2180	PagingGroup90	255	Yes	Edit
91	234.2.1.92	2182	PagingGroup91	255	Yes	Edit
92	234.2.1.93	2184	PagingGroup92	255	Yes	Edit
93	234.2.1.94	2186	PagingGroup93	255	Yes	Edit
94	234.2.1.95	2188	PagingGroup94	255	Yes	Edit
95	234.2.1.96	2190	PagingGroup95	255	Yes	Edit
96	234.2.1.97	2192	PagingGroup96	255	Yes	Edit
97	234.2.1.98	2194	PagingGroup97	255	Yes	Edit
98	234.2.1.99	2196	PagingGroup98	255	Yes	Edit
99	234.2.1.100	2198	PagingGroup99	255	Yes	Edit

Reboot

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

Table 2-12. 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.
	Click on the Reboot button to reboot the system.
	<p>To make changes to the paging groups, complete the following steps:</p> <ol style="list-style-type: none"> 1. Click on the Edit button to open the Configure PGROUP window (Figure 2-21). 2. In the Configure PGROUP window (Figure 2-21), edit the PGROUP (see Table 2-13, "Configure PGROUP Window") and click on the Save Changes button. 3. On the PGROUPS page (Figure 2-19), click on the Reboot button.



Figure 2-21. Configure PGROUP Window

Configure PGROUP

PGROUP	0
Address	<input type="text" value="234.2.1.1"/>
Port	<input type="text" value="2000"/>
Name	<input type="text" value="PagingGroup00"/>
Security Code	<input type="text"/>
TTL	<input type="text" value="255"/>
Line-out	<input checked="" type="checkbox"/>
Play Stored Message	<input type="checkbox"/>
Audio File	<input type="text"/>
Times to Play	<input type="text" value="1"/>

The parameters for the **Configure PGROUP** window are shown in [Table 2-13](#).

Table 2-13. Configure PGROUP Window

Web Page Item	Description
PGROUP	Shows the paging group number.
Address	Enter the IP address of the PGROUP. Note: To disable a relay on a group, use an IP address of 0.0.0.0.
Port	Enter the port number of the PGROUP. Note: 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.
Lineout	The Lineout field determines whether or not the device will play audio out of the RCA output port and the 600 Ohm output port in addition to forwarding it to the PGROUP.
Play Stored Message	When selected, entering this paging group will play the stored message selected in Audio File .
Audio File	Select a file from the drop down list of audio files previously saved in the Stored Messages portion of the Audiofiles Page .
Times to Play	Enter the number of times the message will play (1-65535).
	Click the Save Changes button to save your configuration settings. Note: You need to reboot for changes to take effect.
	Click the Cancel button to close the Configure PGROUP window.

2.4.9 Operating the Paging Server

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

2.4.9.1 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.

2.4.9.2 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").

2.4.10 Configure the SSL Parameters

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

Figure 2-22. SSL Configuration Page

CyberData v3.1 Paging Server

Server CAs

Browse... No file chosen

Import CA Certificate

Restore Defaults **Remove All**

Apply/Reboot **Toggle Help**

Client Certificate

```
commonName = CyberData SIP Device
validFrom = Jul 10 17:56:03 2018 GMT
validTo = Jul 7 17:56:03 2028 GMT
```

[Client CA](#)

Test SSL Connection

Server: 10.0.0.253

Port: 5060

Test TLS connection

List of Trusted CAs

1	DST_ACES_CA_X6.crt	Info	Remove
2	DST_Root_CA_X3.crt	Info	Remove
3	Deutsche_Telekom_Root_CA_2.crt	Info	Remove
4	DigiCert_Assured_ID_Root_CA.crt	Info	Remove
5	DigiCert_Assured_ID_Root_G2.crt	Info	Remove
6	DigiCert_Assured_ID_Root_G3.crt	Info	Remove
7	DigiCert_Global_Root_CA.crt	Info	Remove
8	DigiCert_Global_Root_G2.crt	Info	Remove
9	DigiCert_Global_Root_G3.crt	Info	Remove
10	DigiCert_High_Assurance_EV_Root_CA.crt	Info	Remove

Figure 2-23. SSL Configuration Page

12	Equifax_Secure_CA.crt	Info	Remove
13	Equifax_Secure_Global_eBusiness_CA.crt	Info	Remove
14	Equifax_Secure_eBusiness_CA_1.crt	Info	Remove
15	GeoTrust_Global_CA.crt	Info	Remove
16	GeoTrust_Global_CA_2.crt	Info	Remove
17	GeoTrust_Primary_Certification_Authority.crt	Info	Remove
18	GeoTrust_Primary_Certification_Authority_-_G2.crt	Info	Remove
19	GeoTrust_Primary_Certification_Authority_-_G3.crt	Info	Remove
20	GeoTrust_Universal_CA.crt	Info	Remove
21	GeoTrust_Universal_CA_2.crt	Info	Remove
22	ISRG_Root_X1.crt	Info	Remove
23	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G4.crt	Info	Remove
24	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5.crt	Info	Remove
25	VeriSign_Universal_Root_Certification_Authority.crt	Info	Remove
26	Verisign_Class_1_Public_Primary_Certification_Authority.crt	Info	Remove
27	Verisign_Class_1_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
28	Verisign_Class_2_Public_Primary_Certification_Authority_-_G2.crt	Info	Remove
29	Verisign_Class_2_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
30	Verisign_Class_3_Public_Primary_Certification_Authority.crt	Info	Remove
31	Verisign_Class_3_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
32	thawte_Primary_Root_CA.crt	Info	Remove
33	thawte_Primary_Root_CA_-_G2.crt	Info	Remove
34	thawte_Primary_Root_CA_-_G3.crt	Info	Remove

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

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. SSL Configuration Parameters

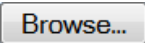

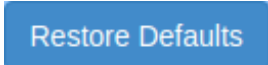





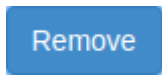
Web Page Item	Description
Server CAs	
	Use this button to select a configuration file to import.
	Click Browse to select a CA certificate to import. After selecting a server certificate authority (CA), click Import CA Certificate to import it to the list of trusted CAs. CAs are used to validate the certificate presented by the server when establishing a TLS connection.
	Restore Defaults will restore the default list of registered CAs and Remove All will remove all registered CAs.
	Restore Defaults will restore the default list of registered CAs and Remove All will remove all registered CAs.
	Reboots the device and applies settings and activates imported certificates.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.
Client Certificate	
Client CA ?	Right click and Save Link As... to get the Cyberdata CA used to sign this client certificate.
Test SSL Connection	
Server ?	The ssl test server address as a fully qualified domain name or in IPv4 dotted decimal notation.
Port ?	The ssl test server port. The supported range is 0-65536. SIP connections over TLS to port 5060 will do the same.
	Use this button to test a TLS connection to a remote server. 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.
List of Trusted CAs	
	Provides details of the certificate. After clicking on this button, the Certificate Info Window appears. See Section 2.4.10.1, "Certificate Info Window" .

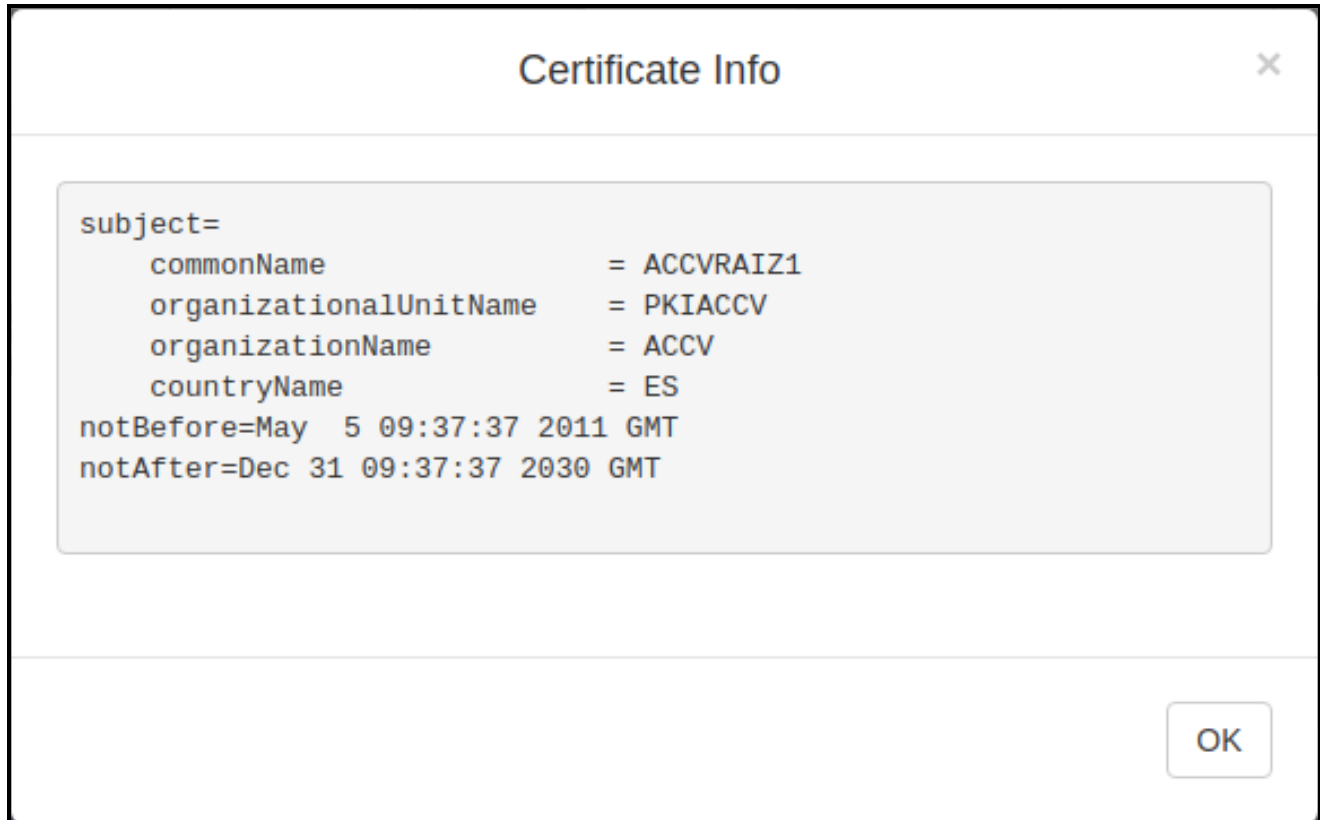
Table 2-14. SSL Configuration Parameters (continued)

Web Page Item	Description
	Removes this certificate from the list of trusted certificates. After clicking on this button, the Remove Server Certificate Window appears. See Section 2.4.10.2, "Remove Server Certificate Window" .

2.4.10.1 Certificate Info Window

The **Certificate Info Window** provides details of the certificate. This window appears after clicking on the **Info** button. See [Figure 2-24](#).

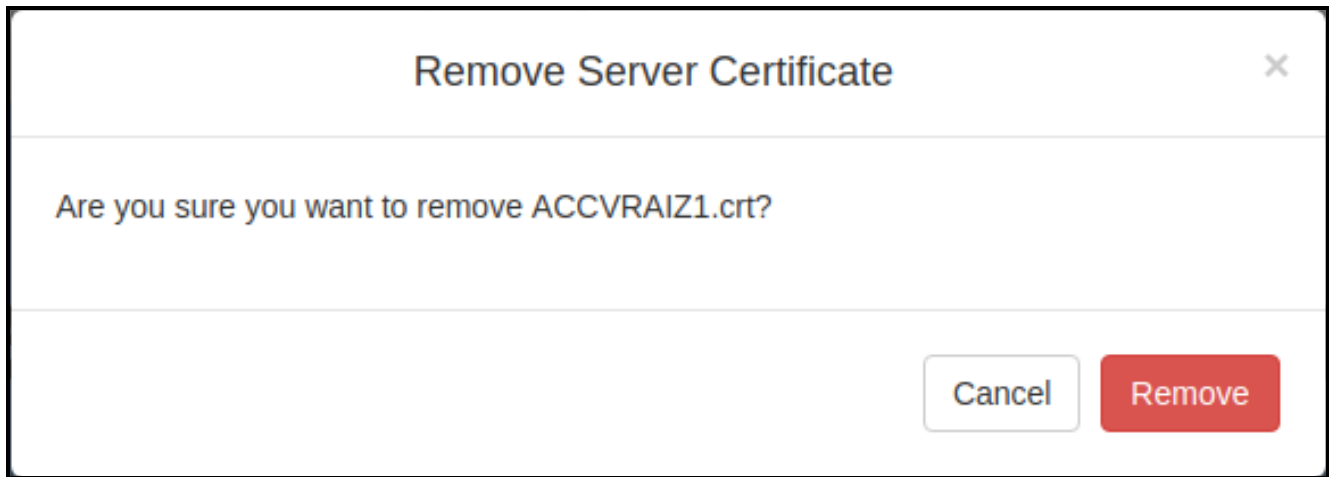
Figure 2-24. Certificate Info Window



2.4.10.2 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 2-25](#).

Figure 2-25. Remove Server Certificate Window



2.4.11 Configure the Schedules Parameters

1. Click on the **Schedules** button to open the **Schedules** page. See [Figure 2-26](#).

Figure 2-26. Schedules Page

CyberData v3.1 Paging Server




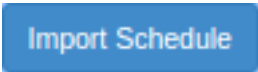


Scheduled Events

Days	Time	Audio File	PGROUP	Event Name	Edit	Delete
Mon Tue Wed Thu Fri	08:20	10_pulse_bell_tone.wav	0	Morning warning	Edit	Delete
Mon Tue Wed Thu Fri	08:40	Gong.wav	10	Morning	Edit	Delete
Mon Tue Wed Thu Fri	10:00	Dinner_Bell.wav	0	Recess start	Edit	Delete
Sun Mon Tue Wed	10:20	Dinner_Bell.wav	6	Recess ends	Edit	Delete
Mon Tue Wed Thu Fri	12:10	Westminster_chimes.wav	0	Lunch start	Edit	Delete
Mon Tue Wed Thu Fri	12:35	Gong.wav	0	Lunch ends	Edit	Delete
Thu	13:40	Gong.wav	6	Early Day	Edit	Delete
Mon Tue Wed Thu Fri	02:40	10_pulse_bell_tone.wav	0	End of Day	Edit	Delete
Sun Sat	16:00	Dinner_Bell.wav	0	Weekend event	Edit	Delete
						New

No file chosen

- On the **Schedules** page, enter values for the parameters indicated in [Table 2-17](#).

Table 2-15. Schedules Configuration Parameters

Web Page Item	Description
Scheduled Events	
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 Configure Scheduled Event window for the corresponding event. See Figure 2-27, "Configure Scheduled Event Window" and Table 2-16, "Configure Scheduled Event Window Parameters"
	Removes the event from the schedule.
	Opens a new Configure Scheduled Event window.
	After selecting a file, imports a schedule.
	Exports the current schedule.
	Reboots the device, which must be rebooted for changes to the schedule to take effect.

Note The schedule is not affected by restoring the factory defaults.

Figure 2-27. Configure Scheduled Event Window

Configure Scheduled Event

Event # 1

Days Sun Mon Tue Wed Thu Fri Sat

☐ ☒ ☒ ☒ ☒ ☒ ☐

Time

Audio

Times to Play

PGROUP

Name

Relay

No action

No action



Activate during bell

Activate indefinitely

Deactivate indefinitely

The parameters for the **Configure Scheduled Event** window are shown in [Table 2-16](#).

Table 2-16. Configure Scheduled Event Window Parameters

Web Page Item	Description
Days	Use the box beneath the day to select. Multiple days may be selected.
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.
Name	Enter the name of the event, using a maximum of 16 characters.
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>
	<p>Click the Save Changes button to save your configuration settings.</p> <p>Note: You need to reboot for changes to take effect.</p>
	Click the Cancel button to close the Configure Scheduled Event window.

- In addition to the bells, the user can have 25 stored messages that are utilized through paging groups.
- 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.

2.4.12 Configure the Fault Detection Parameters

1. Click on the **Fault** button to open the **Fault** page. See [Figure 2-28](#).

Figure 2-28. Fault Page

The screenshot shows the 'Fault' page of the CyberData v3.1 Paging Server web interface. At the top is a navigation bar with tabs: Home, Device, Network, SIP, PGROUPS, SSL, Schedules, Fault (selected), Audiofiles, Events, Autopro, and Firmware. Below the navigation bar is the title 'CyberData v3.1 Paging Server'. The main section is titled 'Fault Detection Settings' and contains the following configuration options:

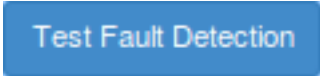


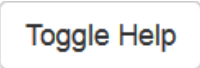
- Play Stored Audio Locally: ☐
- Make call to extension: ☐
- Dial Out Extension:
- Dial Out ID:
- Repeat Message:
- Play Stored Audio via Multicast: ☐
- Play Line-in Audio via Multicast: ☐
- Multicast Address:
- Multicast Port:

At the bottom of the settings section are three buttons: 'Save', 'Reboot', and 'Toggle Help'. Below these is a 'Test Fault Detection' button. The entire page has a light blue background and a dark blue border.

- On the **Fault Detection** page, enter values for the parameters indicated in [Table 2-17](#).

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

Table 2-17. Fault Detection Configuration Parameters

Web Page Item	Description
Triggered Settings	
Play Stored Audio 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 Dial Out Extension 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.
Repeat Message ?	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 Stored Audio via Multicast ?	When selected, the device will send the user-defined “sensor triggered” audio file to the specified multicast address and port. Cannot be combined with Play Line-in Audio via Multicast .
Play Line-in Audio via Multicast ?	When selected, the device will send line-in audio to the specified multicast address and port. Cannot be combined with Play Stored Audio via Multicast or Enable Line-in to Line-out Loopback .
Multicast Address ?	The multicast address used for fault detection audio.
Multicast Port ?	The multicast port used for fault detection audio.
	Click on the Test Fault Detection button to test the fault detection feature.
	Click the Save button to save your configuration settings. Note: You need to reboot for changes to take effect.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

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

2.4.13 Configure the Audio Parameters

Click on the **Audiofiles** button to open the **Audiofiles** page. See [Figure 2-29](#). 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 2-29. Audiofiles Page

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

CyberData v3.1 Paging Server

Available Space: 35.22MB

Built-in 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"/>

Figure 2-30. Audiofiles Page

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"/>
Enter PGROUP:	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 PGROUP:	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"/>
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"/>
Your IP Address Is:	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"/>
Rebooting:	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"/>
Restoring Default:	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"/>
Sensor Triggered:	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"/>
Night Ring:	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"/>

Bells

Stored Messages

Figure 2-31. Audiofiles Page

The screenshot displays the 'Audiofiles Page' with a light blue background. At the top, there are three tabs: 'Audiofiles', 'Messages', and 'Settings'. The 'Audiofiles' tab is active. Below the tabs, there are eight rows of configuration options, each with a label, a status, a file selection button, and action buttons.

Label	Status	File Selection	Play	Delete	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"/>
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"/>
Your IP Address Is:	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"/>
Rebooting:	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"/>
Restoring Default:	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"/>
Sensor Triggered:	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"/>
Night Ring:	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"/>

Below the configuration rows, there are two sections: 'Bells' and 'Stored Messages'.

Bells

File Name	Play	Delete
Gong.wav	<input type="button" value="Play"/>	<input type="button" value="Delete"/>
10_pulse_bell_tone.wav	<input type="button" value="Play"/>	<input type="button" value="Delete"/>
Dinner_Bell.wav	<input type="button" value="Play"/>	<input type="button" value="Delete"/>
Westminster_chimes.wav	<input type="button" value="Play"/>	<input type="button" value="Delete"/>
<input type="button" value="Browse..."/> No file chosen	<input type="button" value="Upload New Bell"/>	

Stored Messages

File Name	Play	Delete
Tsunami_Warning.wav	<input type="button" value="Play"/>	<input type="button" value="Delete"/>
<input type="button" value="Browse..."/> No file chosen	<input type="button" value="Upload Stored Message"/>	

On the **Audiofiles** page, enter values for the parameters indicated in [Table 2-18](#).

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 2-18. Audiofiles Configuration Parameters

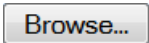



Web Page Item	Description
Audio Files	
0-9	The name of the audio configuration option is the same as the spoken audio that plays on the board (24 character limit). '0' corresponds to the spoken word "zero." '1' corresponds to the spoken word "one." '2' corresponds to the spoken word "two." '3' corresponds to the spoken word "three." '4' corresponds to the spoken word "four." '5' corresponds to the spoken word "five." '6' corresponds to the spoken word "six." '7' corresponds to the spoken word "seven." '8' corresponds to the spoken word "eight." '9' corresponds to the spoken word "nine."
Dot	Corresponds to the spoken word "dot." (24 character limit).
Audio Test	Corresponds to the message "This is the CyberData IP speaker test message..." (24 character limit).
Enter PGROUP	Corresponds to the message "Enter PGROUP" (24 character limit).
Invalid PGROUP	Corresponds to the message "Invalid PGROUP" (24 character limit).
Enter Code	Corresponds to the message "Enter Code" (24 character limit).
Invalid Code	Corresponds to the message "Invalid Code" (24 character limit).
Page Tone	Corresponds to a simple tone that is unused by default (24 character limit).
Your IP Address is	Corresponds to the message "Your IP address is..." (24 character limit).
Rebooting	Corresponds to the spoken word "Rebooting" (24 character limit).
Restoring Default	Corresponds to the message "Restoring default" (24 character limit).
Sensor Triggered	Corresponds to the message "Sensor Triggered" (24 character limit).
Night Ring	Specifies the ringtone for nightring. By default this parameter uses the same audio file that is selected for the Ring Tone parameter.
Bells	Upload files here to be used in scheduled events. Note: The user may upload a maximum of 25 files.
Stored Messages	Upload files here to be used as stored messages. Note: The user may upload a maximum of 25 files.
	The Browse button will allow you to navigate to and select an audio file.

Table 2-18. Audiofiles Configuration Parameters (continued)

Web Page Item	Description
	The Play button will play that audio file.
	The Delete button will delete any user uploaded audio and restore the stock audio file.
	The Save button will download a new user audio file to the board once you've selected the file by using the Browse button. The Save button will delete any pre-existing user-uploaded audio files.

2.4.13.1 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 2-32](#) through [Figure 2-34](#).

Figure 2-32. Audacity 1

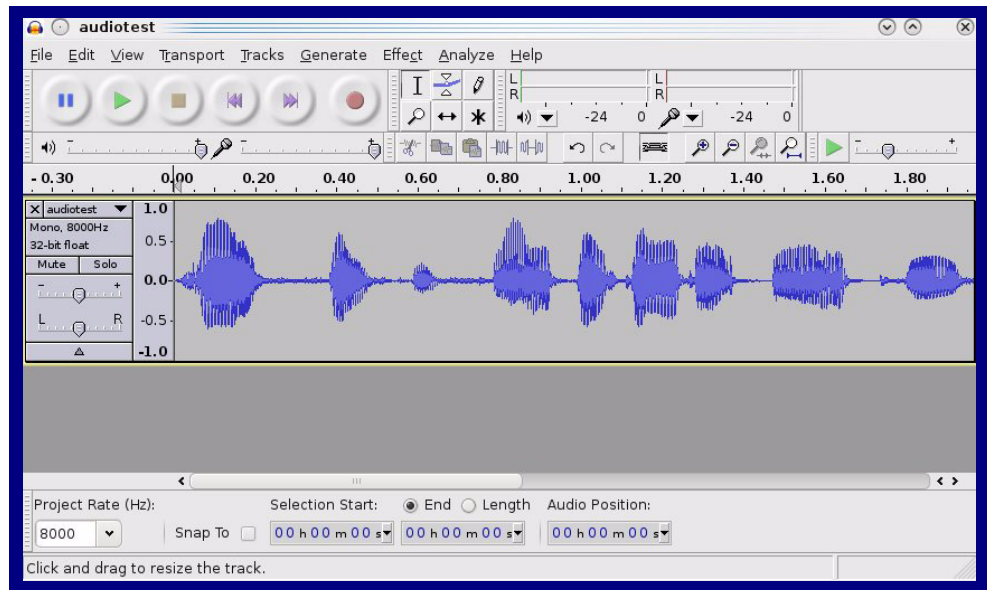


Figure 2-33. Audacity 2

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

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

Add Remove Clear

Genres Edit... Reset...

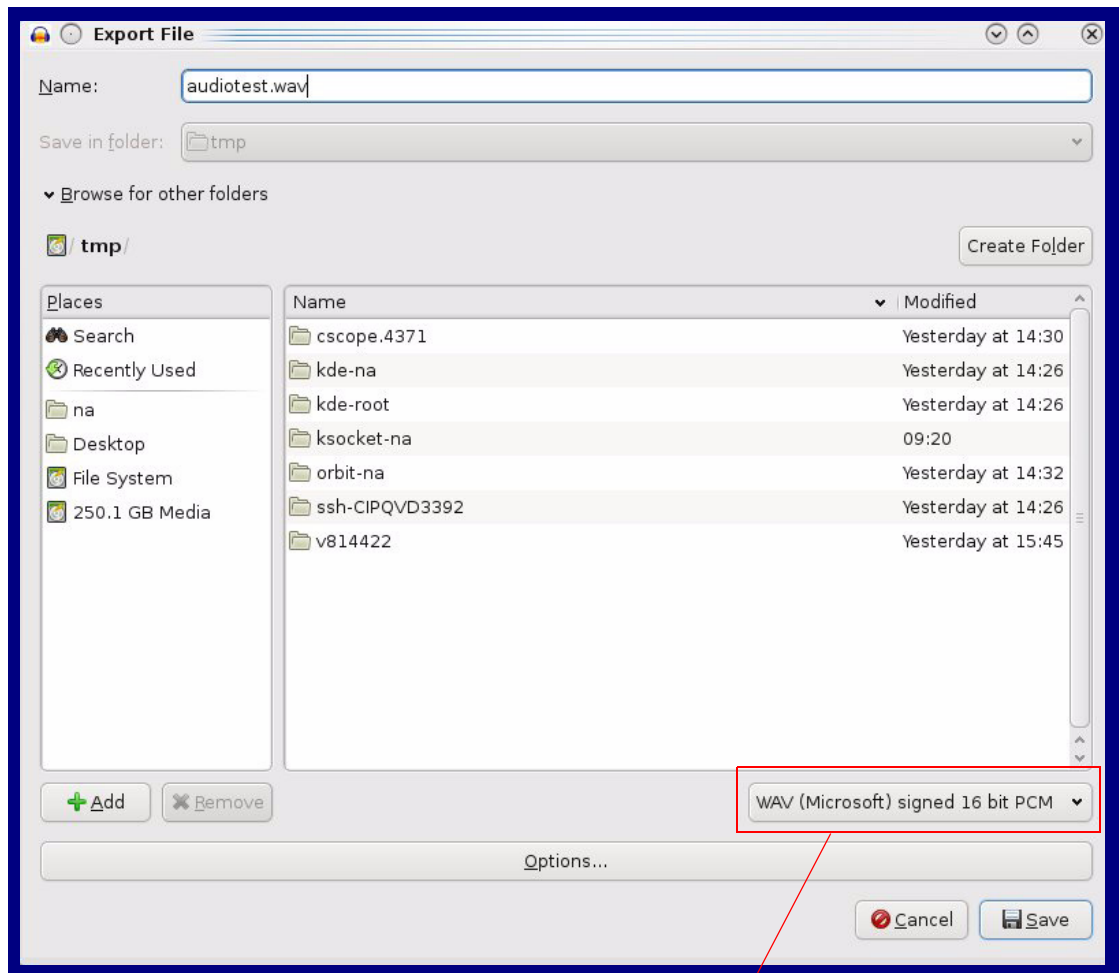
Template Load... Save... Set Default

Cancel OK

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

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

Figure 2-34. WAV (Microsoft) signed 16 bit PCM



WAV (Microsoft) signed 16 bit PCM

2.4.14 Configure the Event Parameters

Click on the **Events** button to open the **Events** page (Figure 2-35). The **Events** page specifies a remote server that can be used to receive HTTP POST events when actions take place on the board.

Figure 2-35. Events Page

The screenshot shows the 'Events' configuration page of the CyberData v3.1 Paging Server. At the top is a navigation bar with tabs: Home, Device, Network, SIP, PGROUPS, SSL, Schedules, Fault, Audiofiles, Events (selected), Autopro, and Firmware. The main title is 'CyberData v3.1 Paging Server'. Below the title, there is a section for 'Enable Event Generation' with a checkbox that is currently unchecked. To the left, under the heading 'Events', there is a list of event types with checkboxes: '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', and 'Enable 60 Second Heartbeat'. Below this list are two links: 'Check All' and 'Uncheck All'. To the right, under the heading 'Event Server', there are three input fields: 'Server IP Address' with the value '10.0.0.250', 'Server Port' with the value '8080', and 'Server URL' with the value 'xmlparse_engine'. At the bottom left, there are three buttons: 'Save', 'Reboot', and 'Toggle Help'.

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

CyberData v3.1 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: ☐

[Check All](#) [Uncheck All](#)

Event Server

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

[Save](#) [Reboot](#) [Toggle Help](#)

Table 2-19 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 2-19. 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 Section 2.4.14.1, "Example Packets for Events" for sample packets.
Events	
Enable Call Start Events ?	When selected, the device will report the start of a SIP call.
Enable Call Terminated Events ?	When selected, the device will report the end of a SIP call.
Enable Relay Activated Events ?	When selected, the device will report relay activation.
Enable Relay Deactivated Events ?	When selected, the device will report relay deactivation.
Enable 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.
Event Server	
Server IP Address ?	The IPv4 address of the event server in dotted decimal notation.
Server Port ?	Specify the event server port number. The supported range is 0-65536. Enter up to 5 digits.
Server URL ?	Generally, the destination URL is the name of the application that receives the events and the string in the HTTP POST command. It can be a script used to parse and process the HTTP POST events. Enter up to 127 characters.
Check All	Click on Check All to select all of the events on the page.
Uncheck All	Click on Uncheck All to de-select all of the events on the page.
Save	Click the Save button to save your configuration settings. Note: You need to reboot for changes to take effect.
Reboot	Click on the Reboot button to reboot the system.
Toggle Help	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

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

2.4.14.1 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>
```

2.4.15 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 2-36](#).

Figure 2-36. Autoprovisioning Page

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

CyberData v3.1 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 2-20](#).

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

Table 2-20. Autoprovisioning Configuration Parameters



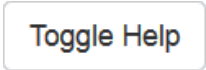

Web Page Item	Description
Disable Autoprovisioning ?	Prevent the device from automatically trying to download a configuration file. See Section 2.4.15.1, "Autoprovisioning" for more information.
Autoprovisioning Server ?	Enter the IPv4 address of the provisioning server in dotted decimal notation.
Autoprovisioning Filename ?	<p>The autoprovisioning filename is the configuration filename. The default autoprovisioning filename is in the format of <mac address>.xml.</p> <p>Supported filename extensions are ".txt", and ".xml." The current filename is denoted by an asterisk at the bottom of the Autoprovisioning Page. Enter up to 256 characters.</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>Note: To use the auto update options, enable the Set Time with NTP Server on boot setting on the Device Page (see Table 2-5).</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>Note: To use the auto update options, enable the Set Time with NTP Server on boot setting on the Device Page (see Table 2-5).</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>Note: To use the auto update options, enable the Set Time with NTP Server on boot setting on the Device Page (see Table 2-5).</p>
	<p>Click the Save button to save your configuration settings.</p> <p>Note: You need to reboot for changes to take effect.</p>

Table 2-20. Autoprovisioning Configuration Parameters (continued)

Web Page Item	Description
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.
	Press the Download Template button to create an autoprovisioning file for the device. See Section 2.4.15.3, "Get Autoprovisioning Template Button"
Autoprovisioning log	The autoprovisioning log provides information about the latest autoprovisioning attempt (i.e. dhcp options and server accessed and files parsed or not found).

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

2.4.15.1 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 2.4.15.2, "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 2-20](#)). This file contains every configuration option that can be set on the board.

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

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

```
<MiscSettings>
    <DeviceName>CyberData VoIP Intercom</DeviceName>
<!--    <AutoprovFile>common.xml</AutoprovFile>-->
<!--    <AutoprovFile>sip_reg[macaddress].xml</AutoprovFile>-->
<!--    <AutoprovFile>audio[macaddress]</AutoprovFile>-->
<!--    <AutoprovFile>device[macaddress].xml</AutoprovFile>-->
</MiscSettings>
```

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

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

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

The file 0020f7123456.xml contains:

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

1. The device will first set it's name to 'Newname'.
2. It will try to download <http://example.com/common.xml>.
3. It will try to download http://example.com/sip_reg0020f7123456.xml.
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 2-21. Autoprovisioning File Name

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

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

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

For example:

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

The autoprovisioning filename is set to “cyberdata/”

On boot, the device will try to download:

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

...and if this fails:

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

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

```
Autoprovisioning <FirmwareSettings>
Firmware Updates <FirmwareFile>505-ulmage-ceilingspeaker</FirmwareFile>
                  <FirmwareServer>10.0.1.3</FirmwareServer>
                  <OutdoorIntercom30>firmware_file_v9.3.0</OutdoorIntercom30>
                  <OutdoorIntercom31>firmware_file_v10.3.0</OutdoorIntercom31>
                  <CallButton31>firmware_file_v10.3.0</CallButton31>
                  </FirmwareSettings>
```

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

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

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

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

The list of valid product strings:

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

Autoprovisioning Example 1

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

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

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

000000cd.xml

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

sip_common.xml

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

sip_0020f7020001.xml

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

sip_0020f7020002.xml

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

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

1. Device1 changes its device name to **CyberData Autoprovisioned**.
2. Device1 finds an AutoprovFile element containing the filename **sip_common.xml**. The device downloads **sip_common.xml** from "https://autoprovtest.server.net," and imports this configuration, setting the sip server to **10.0.0.253** and the remote port to **5060.3**.
3. Device1 finds another AutoprovFile element containing the filename **sip_[macaddress].xml**. The device replaces the **[macaddress]** with its own mac address value creating **sip_0020f7020001.xml**, downloads this file from "https://autoprovtest.server.net," and imports this configuration. This sets the user ID to **198**, the password to **ext198**, and the dialout extension to **204**. Device1 is now finished with autoprovisioning.

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

Autoprovisioning Example 2

Here is another example of setting up your autoprovisioning files:

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

0020f7020001.xml

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

0020f7020002.xml

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

common_settings.xml

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

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

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

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

XML Files

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

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

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

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

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

From the common file, a pointer to sip_common.xml

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

Autoprovisioned Audio Files

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

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

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

2.4.15.2 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; }

```

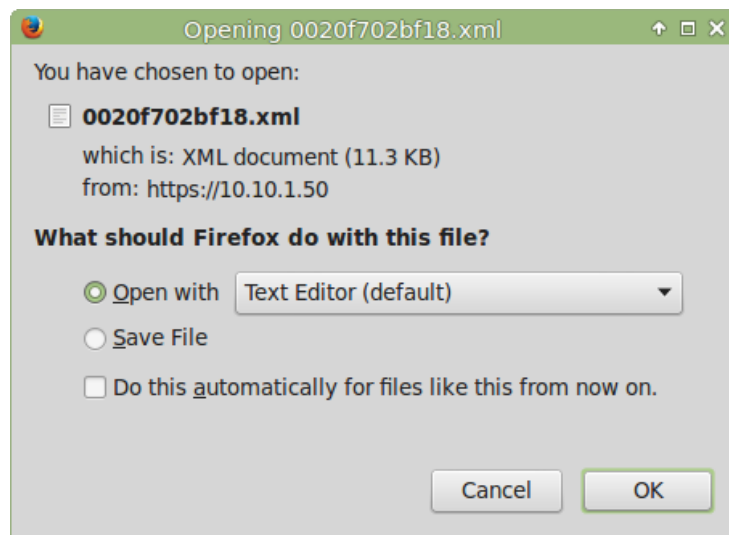
2.4.15.3 Get Autoprovisioning Template Button

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 2-37](#)). The configuration file is the basis for the default configuration settings for your unit).
3. Choose a location to save the configuration file and click on **OK**. See [Figure 2-37](#).

Figure 2-37. Configuration File



4. At this point, you can open and edit the autoprovisioning template to change the configuration settings in the template for the unit.
5. You can then upload the autoprovisioning file to a TFTP or HTTP server where the file can be loaded onto other devices.

2.5 Upgrading the Firmware



Caution


Equipment Hazard: Devices with a serial number that begins with 1461xxxxx can only run firmware versions 11.0.0 or later.

2.5.1 Upgrade the Firmware

To upload the firmware from your computer:

1. Retrieve the latest SIP Paging Server firmware from the SIP Paging Server **Downloads** page at:
<https://www.cyberdata.net/products/011146>
2. Unzip the firmware version file. This file may contain the following:
 - Firmware file
 - Release notes
3. Log in to the SIP Paging Server home page as instructed in [2.4.4 "Log in to the Configuration GUI"](#).

- Click on the **Firmware** menu button to open the **Firmware** page. See [Figure 2-38](#).



GENERAL ALERT

Caution

Equipment Hazard: CyberData strongly recommends that you first reboot the device before attempting to upgrade the firmware of the device. See [Section 2.5.2](#), "Reboot the SIP Paging Server".

Figure 2-38. Firmware Page





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

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

Note This starts the upgrade process. Once the SIP Paging Server has uploaded the file, the **Uploading Firmware** countdown page appears, indicating that the firmware is being written to flash. The SIP Paging Server will automatically reboot when the upload is complete. When the countdown finishes, the **Firmware** page will refresh. The uploaded firmware filename should be displayed in the system configuration (indicating a successful upload and reboot).

- [Table 2-22](#) shows the web page items on the **Firmware** page.

Table 2-22. Firmware Parameters

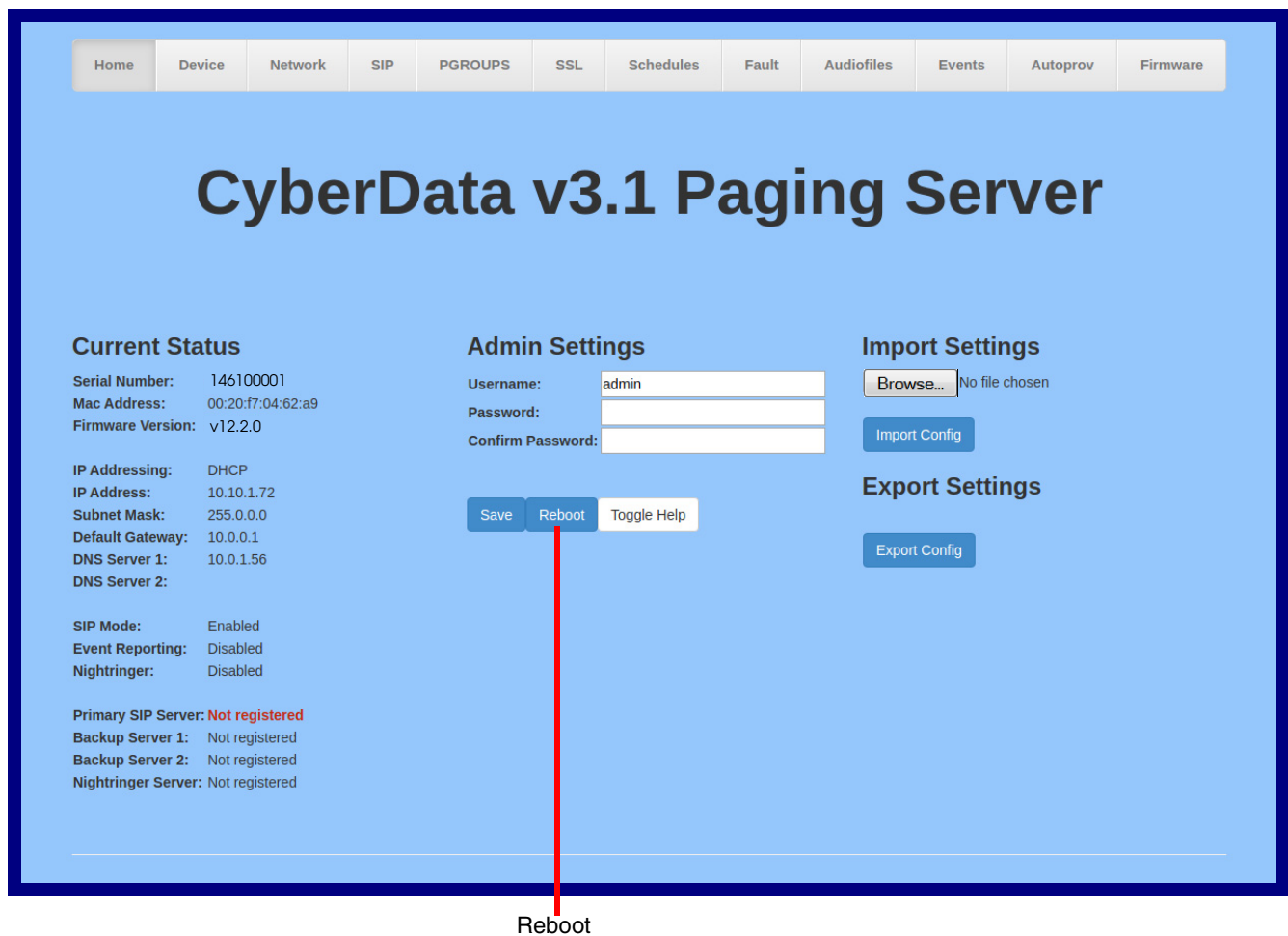
Web Page Item	Description
Current Firmware Version	Shows the current firmware version.
	Use the Browse button to navigate to the location of the Intercom firmware file that you want to upload.
	Click on the Upload button to automatically upload the selected firmware and reboot the system.

2.5.2 Reboot the SIP Paging Server

To reboot a SIP Paging Server, log in to the web page as instructed in [Section 2.4.4, "Log in to the Configuration GUI"](#).

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

Figure 2-39. Home Page



2.6 Command Interface

Some functions on the device can be activated using simple POST commands to the web interface. The examples in [Table 2-23](#) use the free unix utility, **wget** commands. However, any program that can send HTTP POST commands to the device should work.

2.6.1 Command Interface Post Commands

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

Table 2-23. Command Interface Post Commands^a

Device Action	HTTP Post Command
Trigger relay (fixed at 5 seconds)	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/command.cgi" --post-data "test_relay=yes"
Terminate active call	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/command.cgi" --post-data "terminate=yes"
Force reboot	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/command.cgi" --post-data "reboot=yes"
Play "audio test message"	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/command.cgi" --post-data "test_audio=yes"
Announce IP address	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/command.cgi" --post-data "speak_ip_address=yes"
Play the "0" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_0=yes"
Play the "1" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_1=yes"
Play the "2" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_2=yes"
Play the "3" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_3=yes"
Play the "4" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_4=yes"
Play the "5" audio file	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_5=yes"

Table 2-23. Command Interface Post Commands^a (continued)

Device Action	HTTP Post Command
Play the "6" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiosfiles.cgi" --post-data "play_6=yes"</code>
Play the "7" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiosfiles.cgi" --post-data "play_7=yes"</code>
Play the "8" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiosfiles.cgi" --post-data "play_8=yes"</code>
Play the "9" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiosfiles.cgi" --post-data "play_9=yes"</code>
Play the "Dot" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiosfiles.cgi" --post-data "play_d=yes"</code>
Play the "Page Tone" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiosfiles.cgi" --post-data "play_pagetone=yes"</code>
Play the "Your IP Address Is" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiosfiles.cgi" --post-data "play_youripaddressis=yes"</code>
Play the "Rebooting" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiosfiles.cgi" --post-data "play_rebooting=yes"</code>
Play the "Restoring Default" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiosfiles.cgi" --post-data "play_restoringdefault=yes"</code>
Play the "Sensor Triggered" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiosfiles.cgi" --post-data "play_sensortriggered=yes"</code>
Play the "Night Ring" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiosfiles.cgi" --post-data "play_nightring=yes"</code>
Play the "Enter PGROUP" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiosfiles.cgi" --post-data "play_enterpgroup=yes"</code>
Play the "Invalid PGROUP" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiosfiles.cgi" --post-data "play_invalidpgroup=yes"</code>
Play the "Enter Code" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiosfiles.cgi" --post-data "play_entercode=yes"</code>

Table 2-23. Command Interface Post Commands^a (continued)

Device Action	HTTP Post Command
Play the "Invalid Code" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "play_invalidcode=yes"</code>
Delete the "0" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_0=yes"</code>
Delete the "1" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_1=yes"</code>
Delete the "2" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_2=yes"</code>
Delete the "3" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_3=yes"</code>
Delete the "4" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_4=yes"</code>
Delete the "5" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_5=yes"</code>
Delete the "6" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_6=yes"</code>
Delete the "7" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_7=yes"</code>
Delete the "8" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_8=yes"</code>
Delete the "9" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_9=yes"</code>
Delete the "Audio Test" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_audiotest=yes"</code>
Delete the "Page Tone" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_pagetone=yes"</code>

Table 2-23. Command Interface Post Commands^a (continued)

Device Action	HTTP Post Command
Delete the "Your IP Address Is" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_youripaddressis=yes"</code>
Delete the "Rebooting" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_rebooting=yes"</code>
Delete the "Restoring Default" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_restoringdefault=yes"</code>
Delete the "Sensor Triggered" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_sensortriggered=yes"</code>
Delete the "Night Ring" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_nightring=yes"</code>
Delete the "Enter PGROUP" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_enterpgroup=yes"</code>
Delete the "Invalid PGROUP" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_invalidpgroup=yes"</code>
Delete the "Enter Code" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_entercode=yes"</code>
Delete the "Invalid Code" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/audiofiles.cgi" --post-data "delete_invalidcode=yes"</code>

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

Appendix A: Setting Up a TFTP Server

A.1 Set up a TFTP Server

Autoprovisioning requires a TFTP server for hosting the configuration file.

A.1.1 In a LINUX Environment

To set up a TFTP server on LINUX:

1. Create a directory dedicated to the TFTP server, and move the files to be uploaded to that directory.
2. Run the following command where `/tftpboot/` is the path to the directory you created in [Step 1](#): the directory that contains the files to be uploaded. For example:

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

A.1.2 In a Windows Environment

You can find several options online for setting up a Windows TFTP server. This example explains how to use the Solar Winds freeware TFTP server, which you can download at:

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

To set up a TFTP server on Windows:

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

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

Appendix B: Troubleshooting/Technical Support

B.1 Frequently Asked Questions (FAQ)

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>

B.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>

B.3 Contact Information

Contact	<p>CyberData Corporation 3 Justin Court Monterey, CA 93940 USA www.CyberData.net 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>http://support.cyberdata.net/</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 Comments section of the Support Form.</p> <p>Phone: (831) 373-2601, Extension 333</p>

B.4 Warranty and RMA Information

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

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

Index

Symbols

+48V DC power supply 10

Numerics

100 Mbps indicator light 12

A

activity light 12
 address, configuration login 18
 addressing
 DHCP 14, 31
 static 14, 31
 admin username and password 18
 audio configuration 59
 night ring tone parameter 62
 audio configuration page 59
 audio ground reference 8
 audio output 8
 authenticate ID and password for SIP server
 registration 36
 autoprovision at time (HHMMSS) 72
 autoprovision when idle (in minutes > 10) 72
 autoprovisioning 73
 download template button 73
 autoprovisioning autoupdate (in minutes) 72
 autoprovisioning configuration 71, 72
 autoprovisioning filename 72
 autoprovisioning server (IP Address) 72

B

backup SIP server 1 33
 backup SIP server 2 33
 backup SIP servers, SIP server
 backups 33

C

cat 5 ethernet cable 10
 changing
 the web access password 22

changing default username and password for
 configuration GUI 18
 Cisco SRST 33
 command interface 86
 commands 86
 configurable parameters 23, 30, 33
 configuration
 door sensor 47
 intrusion sensor 47
 configuration information 14
 configuration page
 configurable parameters 23, 30
 connecting the V3 paging server 7
 connection speed 12
 verifying 12
 connector (removable) 9
 contact information 92
 contact information for CyberData 92
 current network settings 30
 current settings, reviewing 21
 CyberData contact information 92

D

default
 gateway 13
 IP address 13
 subnet mask 13
 username and password 13
 default gateway 13, 30
 default gateway for static addressing 31
 default login address 18
 default password for configuration GUI 18
 default settings, restoring 13
 default username and password for configuration GUI 18
 device configuration 22
 device configuration parameters 72
 the device configuration page 71
 device configuration page 22
 device configuration parameters 23
 device configuration password
 changing for web configuration access 22
 DHCP addressing 14, 31
 dimensions 3
 discovery utility program 18
 DNS server 30
 door sensor 62
 download autoprovisioning template button 73

E

- enable night ring events 67
- ethernet port 10
- event configuration
 - enable night ring events 67
- expiration time for SIP server lease 34, 35, 36
- export settings 20

F

- fault sense input, sensor 8
- features 2
- firmware
 - where to get the latest firmware 83
- firmware, upgrade 83

G

- get autoprovisioning template 73
- GMT table 27
- GMT time 27
- ground connection 7
- GUI username and password 18

H

- hazard levels 4
- http POST command 86

I

- identifier names (PST, EDT, IST, MUT) 27
- identifying your product 1
- import settings 20
- import/export settings 20
- input specifications 3
- intercom configuration page
 - configurable parameters 33
- IP address 13, 30
 - SIP server 36
- IP addressing
 - default
 - IP addressing setting 13

L

- lease, SIP server expiration time 34, 35, 36
- line input specifications 3
- line output specifications 3
- line-in 7
- line-out 7
- link light 12
- Linux, setting up a TFTP server on 90
- local SIP port 34, 36
- log in address 18
- logging in to configuration GUI 18

M

- MGROUP 39
- multicast
 - play line-in audio via multicast 58
 - play stored audio via multicast 58
- multicast address 58
- multicast port 58
- multicast TTL 43, 45

N

- navigation (web page) 15
- navigation table 15
- network activity, verifying 12
- network configuration page 29
- network parameters, configuring 29
- network setup button 29
- network, connecting to 11
- Nightringer 82
- nightringer settings 35
- NTP server 23

O

- orange link LED 12
- out of band 46
- output specifications 3

P

- page port 8
- page port output connections 8
- paging server
 - configuration 14

- part number 3
- parts list 5
- password
 - configuration GUI 14, 18
 - for SIP server login 33
 - restoring the default 13
 - SIP server authentication 36
- pgroups 39
- pin descriptions and functions 8
- point-to-point configuration 38
- port
 - ethernet 10
 - local SIP 34, 36
 - remote SIP 34, 36
- posix timezone string
 - timezone string 23
- POST command 86
- power
 - connecting to 10
- product overview 1

R

- reboot 84, 85
 - unregistering from SIP server during 36
- registration and expiration, SIP server
 - lease expiration 36
- relay 8
- relay contact 8
- remote SIP port 34, 36
- required configuration for web access username and
 - password 14, 18
- resetting the IP address to the default 91
- restoring factory default settings 13
- RFC2833 RTP events 46
- rport discovery setting, disabling 34

S

- safety instructions 5
- sales 92
- sensor setup page 47
- sensor setup parameters 47
- server
 - TFTP 90
- server address, SIP 33
- service 92
- set time with external NTP server on boot 23
- SIP
 - enable SIP operation 33
 - local SIP port 34
 - user ID 33

- SIP configuration page 32
- SIP configuration parameters
 - outbound proxy 34, 35
 - registration and expiration, SIP server lease 34, 35
 - unregister on reboot 34
 - user ID, SIP 33
- SIP registration 33
- SIP remote SIP port 34
- SIP server 33
 - password for login 33
 - unregister from 34
 - user ID for login 33
- SIP server configuration 33
- SIP server parameters, configuring 14
- SIP setup button 32
- specifications 3
- SRST 33
- static addressing 14, 31
- status light 12
- subnet mask 13, 30
- subnet mask static addressing 31
- supported protocols 3

T

- tech support 92
- technical support, contact information 92
- TFTP server 90
- time zone string examples 27

U

- unregister from SIP server 36
- upgrade firmware 83
- user ID
 - for SIP server login 33
- user ID for SIP server registration 36
- username
 - changing for web configuration access 22
 - restoring the default 13
- username for configuration GUI 14, 18

V

- verifying
 - connection speed 12
 - network activity 12
 - network connectivity 12
- VLAN ID 30
- VLAN Priority 30
- VLAN tagging support 30

VLAN tags 30

W

warranty policy at CyberData 92

web access password 13

web access username 13

web configuration log in address 18

web page

 navigation 15

web page navigation 15

wget commands 86

wget, free unix utility 86

Windows, setting up a TFTP server on 90