



SIP Paging Server Operations Guide

*SIP Compliant
Part #011146*

Document Part #931803D
for Firmware Version 21.0.0

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

Operations Guide 931803D
SIP Compliant 011146

COPYRIGHT NOTICE:

© 2023, CyberData Corporation, ALL RIGHTS RESERVED.

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

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

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

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

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



Technical Support

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

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

Email: support@cyberdata.net

Fax: (831) 373-4193

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



Revision Information

Revision 931803D, which corresponds to firmware version 21.0.0, was released on March 20, 2023, and has the following changes:

- Updates [Figure 1-1, "Model Number Label"](#)
- Updates [Section 1.2, "Features"](#)
- Updates [Table 1-1, "Product Specifications"](#)
- Updates [Table 2-3, "Web Page Navigation"](#)
- Updates [Figure 2-13, "Home Page"](#)
- Updates [Table 2-4, "Home Page Overview"](#)
- Adds [Figure 2-14, "Users List"](#)
- Adds [Table 2-5, "Users List"](#)
- Adds [Figure 2-15, "Add New User"](#)
- Adds [Table 2-6, "Add New User"](#)
- Updates [Figure 2-18, "Device Page"](#)
- Updates [Figure 2-19, "Network Page"](#)
- Updates [Figure 2-20, "SIP Page"](#)
- Updates [Figure 2-21, "SIP Page"](#)
- Updates [Figure 2-22, "SIP Page"](#)
- Updates [Table 2-9, "SIP Configuration Parameters"](#)
- Updates [Figure 2-23, "Fault Page"](#)
- Updates [Figure 2-24, "PGROUPS Page"](#)
- Updates [Figure 2-25, "PGROUPS Page"](#)
- Updates [Table 2-10, "PGROUPS Parameters"](#)
- Adds [Figure 2-26, "Warning"](#)
- Updates [Figure 2-28, "SSL Configuration Page"](#)
- Updates [Figure 2-29, "SSL Configuration Page"](#)
- Updates [Figure 2-32, "Schedules Page"](#)
- Updates [Table 2-13, "Schedules Configuration Parameters"](#)
- Updates [Figure 2-40, "Fault Page"](#)
- Adds [Figure 2-41, "WiFi-Buttons Page"](#)
- Adds [Table 2-20, "WiFi-Buttons Configuration Parameters"](#)
- Adds [Figure 2-42, "Button Settings Page"](#)
- Adds [Figure 2-43, "Button Settings Page"](#)
- Adds [Table 2-21, "Button Settings Page Parameters"](#)
- Updates [Figure 2-44, "Audiofiles Page"](#)
- Updates [Figure 2-45, "Audiofiles Page"](#)
- Updates [Figure 2-46, "Audiofiles Page"](#)
- Updates [Figure 2-47, "Audiofiles Page"](#)

- Updates [Figure 2-51, "Events Page"](#)
- Updates [Figure 2-52, "Autoprovisioning Page"](#)
- Updates [Figure 2-54, "Firmware Page"](#)
- Updates [Figure 2-55, "Upload Button"](#)
- Updates [Figure 2-56, "Home Page"](#)

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.

 GENERAL ALERT	Warning <i>Electrical Hazard:</i> This product should be installed by a licensed electrician according to all local electrical and building codes.
 GENERAL ALERT	Warning <i>Electrical Hazard:</i> To prevent injury, this apparatus must be securely attached to the floor/wall in accordance with the installation instructions.
 GENERAL ALERT	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 CE Statement	4
1.4.2 FCC Statement	4
1.4.3 Industry Canada (IC) Compliance 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
Non-Poe	10
Chassis Ground	10
Poe	10
2.3.7 Connect to the Network	11
2.3.8 Confirm that the SIP Paging Server is Up and Running	12
Verify Network Activity	12
2.4 Announcing the IP Address	13
2.5 Restore the Factory Default Settings	14
2.6 Configuring the SIP Paging Server	15
2.6.1 Gather the Required Configuration Information	15
Static or DHCP Addressing?	15
Username and Password for Configuration GUI	15
SIP Settings	15
2.6.2 SIP Paging Server Web Page Navigation	16
2.6.3 Using the Toggle Help Button	17
2.6.4 Log in to the Configuration GUI	19
2.6.5 Configure the Device Parameters	30
Polycom Paging	32
2.6.6 Configure the Network Parameters	34
2.6.7 Configure the SIP Parameters	37
Point-to-Point Configuration	42
Point-to-Point Fault Sense Reporting	43
2.6.8 Configure the Paging Groups (PGROUPS) Parameters	45
2.6.9 Operating the Paging Server	51
DTMF Bypassed	51
DTMF Not Bypassed	51
2.6.10 Configure the SSL Parameters	52
Certificate Info Window	56
Remove Server Certificate Window	57

2.6.11 Configure the Schedules Parameters	58
Configure the Calendar	62
New Event Window	66
2.6.12 Configure the Fault Detection Parameters	69
2.6.13 Configure the WiFi-Buttons Parameters	71
2.6.14 Configure the Audio Parameters	77
User-created Audio Files	83
2.6.15 Configure the Event Parameters	86
Example Packets for Events	88
2.6.16 Configure the Autoprovisioning Parameters	91
Autoprovisioning	93
Sample dhcpd.conf	101
Get Autoprovisioning Template Button	102
2.7 Upgrade the Firmware	103
2.7.1 Reboot the SIP Paging Server	106
2.8.1 Command Interface Post Commands	107

Appendix A Troubleshooting/Technical Support	108
A.1 Frequently Asked Questions (FAQ)	108
A.2 Documentation	108
A.3 Contact Information	109
A.4 Warranty and RMA Information	109

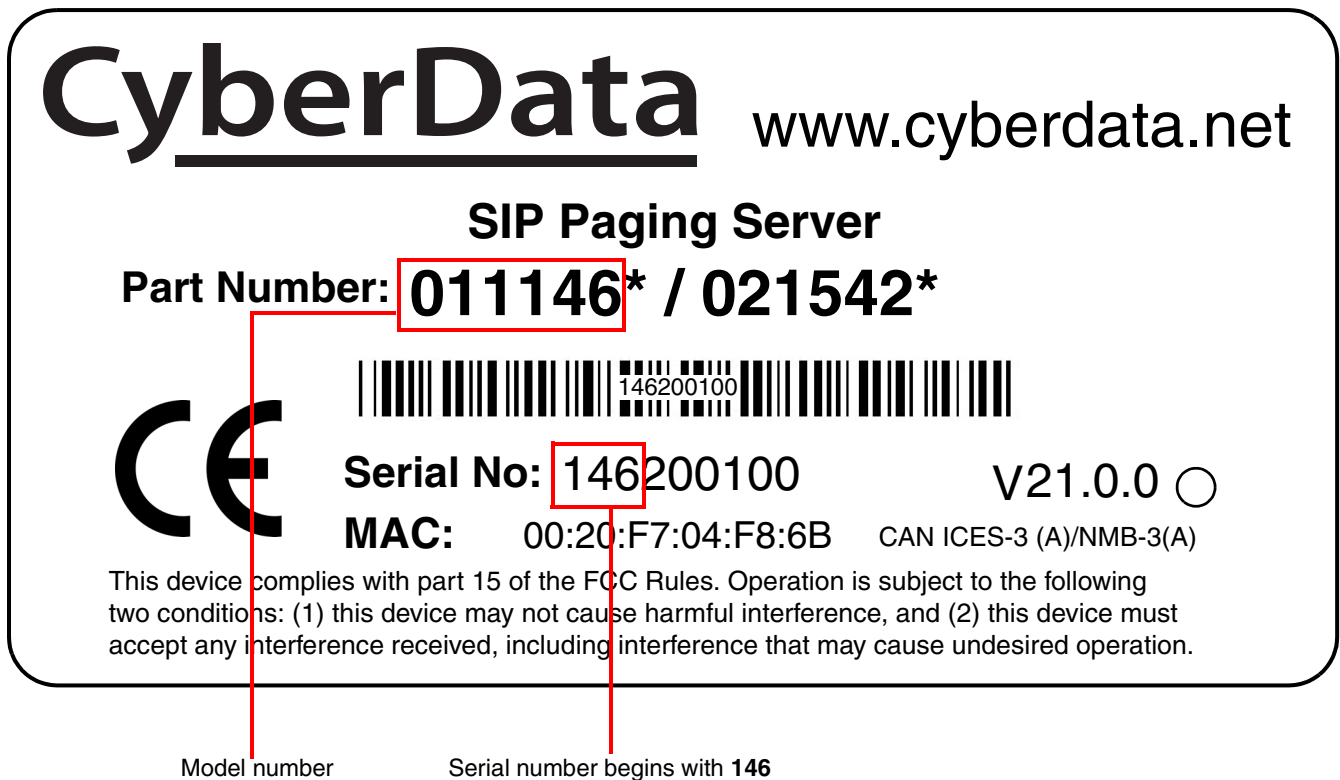
1 Product Overview

1.1 How to Identify This Product

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

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

Figure 1-1. Model Number Label¹



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

1.2 Features

- 1485 MB available for user uploaded audio: up to 135 files for stored messages, bells, and other audio created by the user
 - Calendar-based bell scheduler supporting multiple schedule files and time-based recurring event management
 - Supports call-in stored message recording
 - Voice prompting and password controlled zones
 - Supports 100 paging groups accessed via DTMF
 - Paging Prioritization
 - Loud/Night Ringer function - second SIP extension
 - Supports user-uploadable ring and alert tones, with the option to send a stored message with each of the 100 page groups
 - Supports delayed pages with call buffering
 - Support for security code to prevent unwanted SIP calls
 - Supports multiple user accounts, with distinct log in credentials
 - Can send multicast to all Poly channels
 - The Paging Server supports up to 100 buttons, but network infrastructure could impact the number of attached devices¹
-
- Fault sense input
 - Line-in for background music
 - Line-out connector
 - NTP-based internal clock
 - Audio-controlled onboard relay for amplifier mute control
 - Rack mountable
-
- TLS 1.2 and SRTP enhanced security for IP Endpoints in a local or cloud-based environment
 - HTTP command interface
 - HTTPS web based configuration
 - Support for Cisco SRST resiliency
 - Autoprovisioning via HTTPS, HTTP or TFTP
 - Configurable event generation for device health and status monitoring
 - 802.11q VLAN tagging

1. The Paging Server supports up to 100 buttons, but network infrastructure could impact the number of attached devices

1.3 Specifications

Table 1-1. Product Specifications

Specifications	
Ethernet I/F	10/100 Mbps
Protocol	SIP RFC 3261 Compatible
Power Input	PoE 802.3af or 48VDC
Line In:	
Input Signal Amplitudes	2.0 VPP maximum
Input Impedance	10k Ohm
Line Out:	
Output Signal Amplitudes	2.0 VPP maximum
Output Level	+2dBm nominal
Total Harmonic Distortion	0.5% maximum
Output Impedance	10k Ohm
Page Port Output	Balanced 600 Ohm 5VPP
Payload Types	G.711 a-law, G.711 μ -law, G.722, and G.729
Network Security	TLS 1.2, SRTP, HTTPS
Operating Range	Temperature: -40° C to 55° C (-40° F to 131° F)
	Humidity: 5-95%, non-condensing
Storage Temperature	-40° C to 70° C (-40° F to 158° F)
Storage Altitude	Up to 15,000 ft. (4573 m)
Dimensions ^a	6.11 inches [155.19 mm] Length
	4.05 inches [102.87 mm] Width
	1.15 inches [29.21 mm] Height
Weight	1.2 lbs. [.54 kg]
Boxed Weight	1.8 lbs. [.82 kg]
Compliance	CE: EMC Directive – Class A EN 55032 & EN 55024, LV Safety Directive – EN 62368-1; RoHS Compliant; FCC Part 15 Class A; Industry Canada ICES-3 Class A; IEEE 802.3 Compliant; TAA Compliant
Warranty	2 Years Limited
Part Number	011146

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

1.4 Compliance

1.4.1 CE Statement



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

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

1.4.2 FCC Statement



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

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

1.4.3 Industry Canada (IC) Compliance Statement

Operation is subject to the following two conditions:

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

ICES-3 Class A


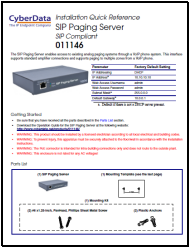
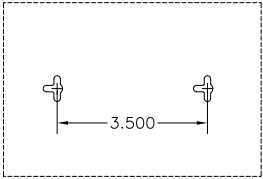

2 Setting Up the SIP Paging Server

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

2.1 Parts List

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

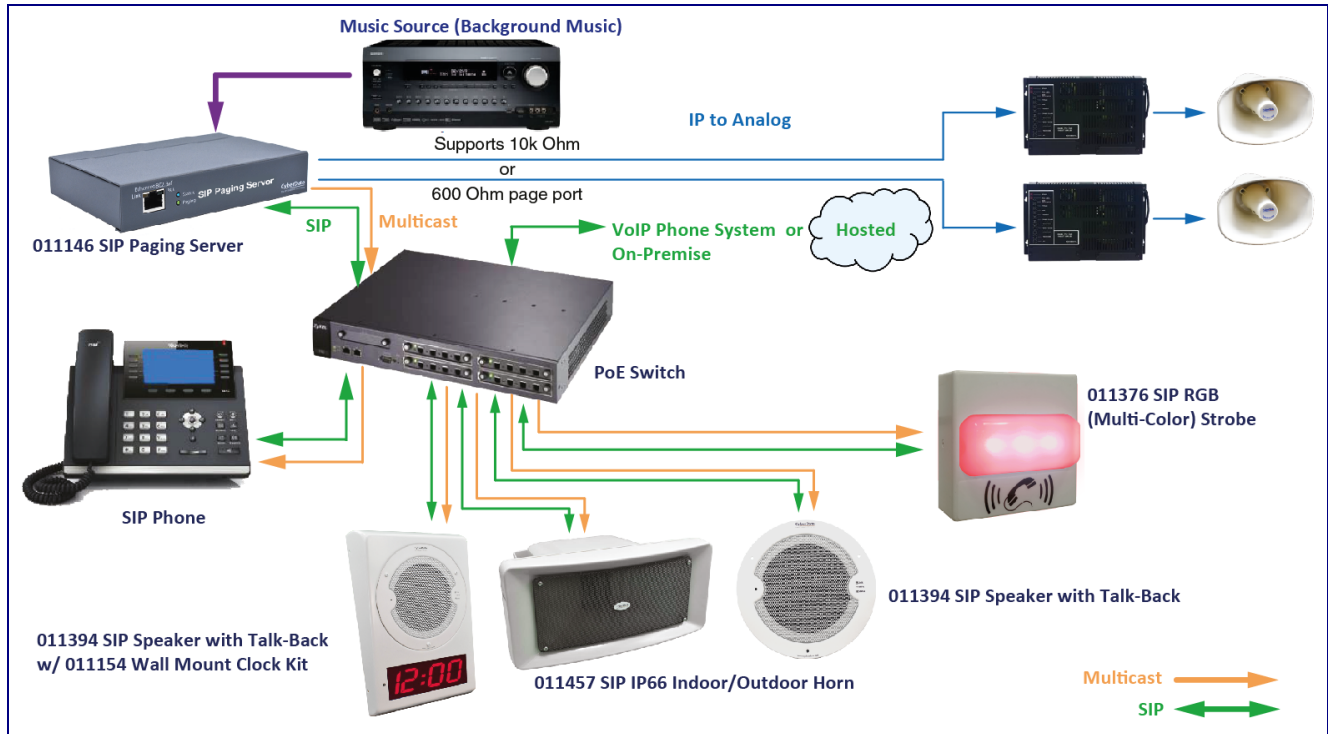
Table 2-1. Parts List

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

2.2 Typical Installation

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

Figure 2-1. Typical Installation

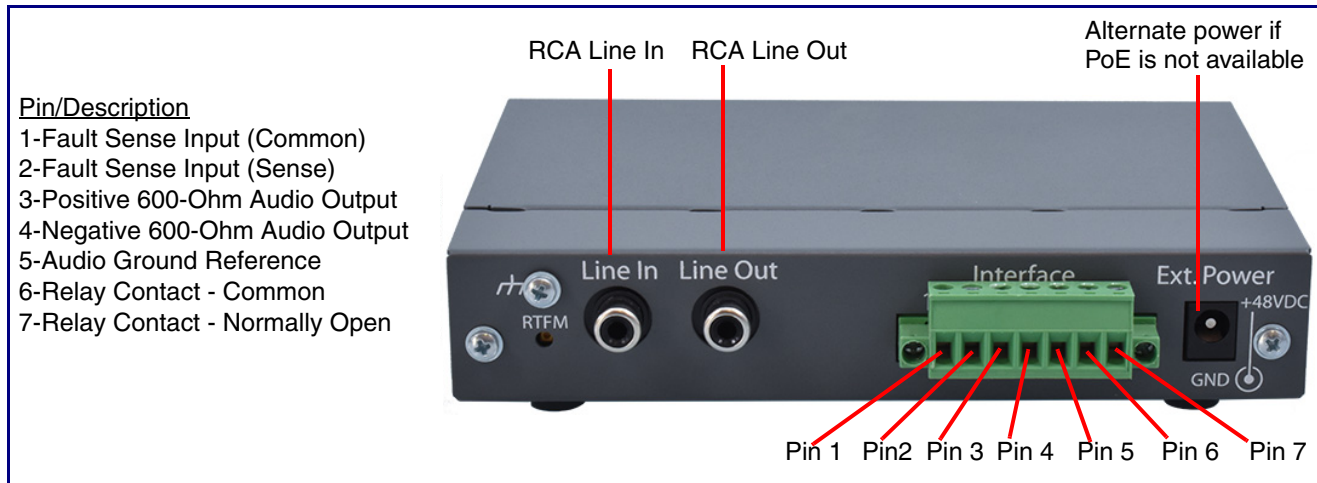


2.3 Connecting the SIP Paging Server

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

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

Figure 2-2. Connection Options



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

2.3.1 Ground Connection

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

2.3.2 Line In

This RCA 10K Ohm Hi-Z input connection allows you to connect the device to The RCA line-out (10K Ohm Hi-Z) of an external audio amplifier. The level of this input can be controlled by the potentiometer located on the front of the device (see [Section 2.6.12, "Configure the Fault Detection Parameters"](#)).

2.3.3 Line Out

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

2.3.4 Page Port Output Connections

Table 2-1. Page Port Output Connections

Pin	Description
Pin 1	Fault Sense Input (Common). See 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 2.6.12, "Configure the Fault Detection Parameters"](#)), this input (when closed) will play a user uploadable audio file out of the line-out connection and/or place a SIP call to a pre-determined extension and play that file.

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

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

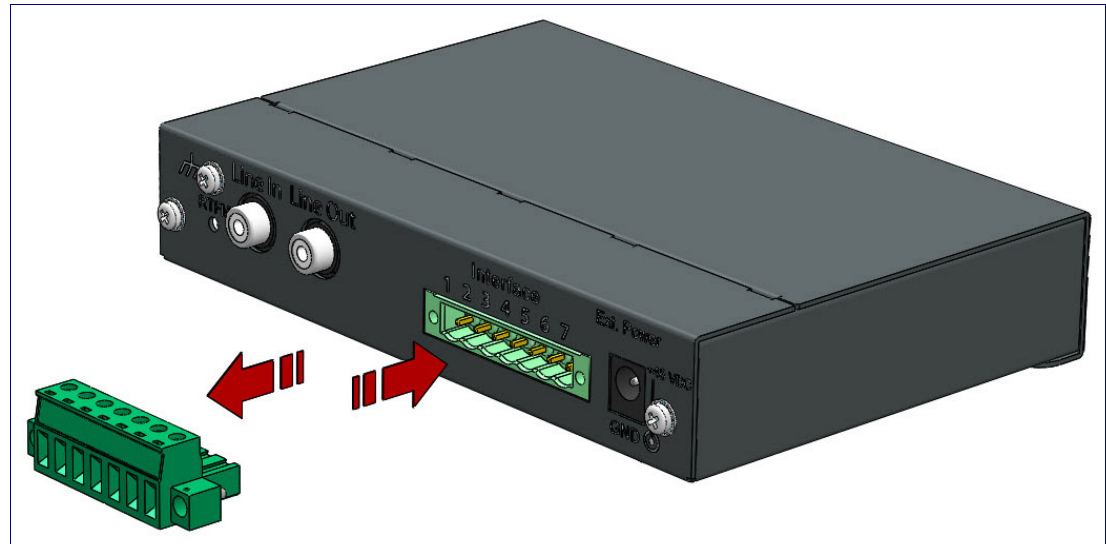
2.3.4.3 Pin 6 and 7—Relay Contact (Common/Normally Open)

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

2.3.5 Removable Interface Connector

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

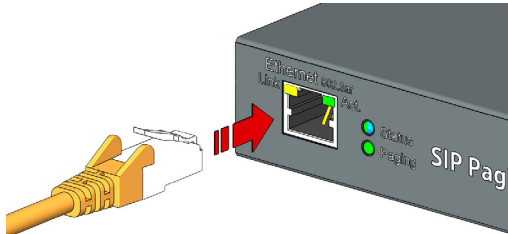
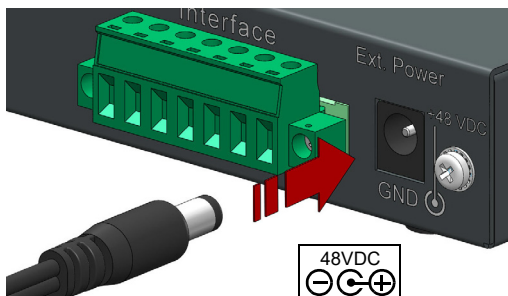
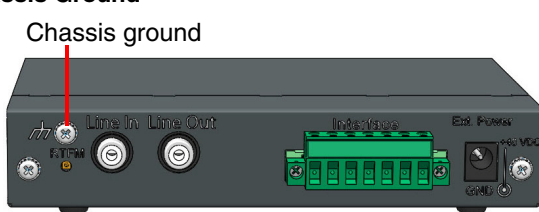
Figure 2-3. Removable Interface Connector



2.3.6 Connect to the Power Source

To use PoE, plug a Cat 5 Ethernet cable from the SIP Paging Server **Ethernet** port to your network. As an alternative to PoE, you can plug one end of a +48V DC power supply into the Paging Server, and plug the other end into a receptacle. If required, connect the earth grounding wire to the chassis ground on the back of the unit. See [Figure 2-4](#).

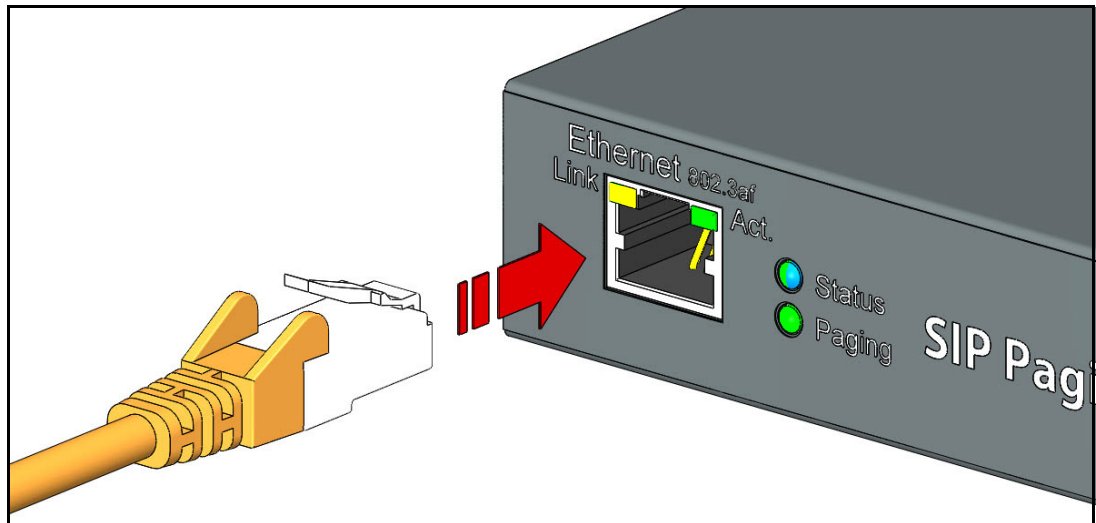
Figure 2-4. Connecting to the Power Source

<p>PoE</p> 	<p>To set up the device, 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.
<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 SIP Paging Adapter **Ethernet** port. Plug the other end into your network.

Figure 2-5. Connecting to the Network



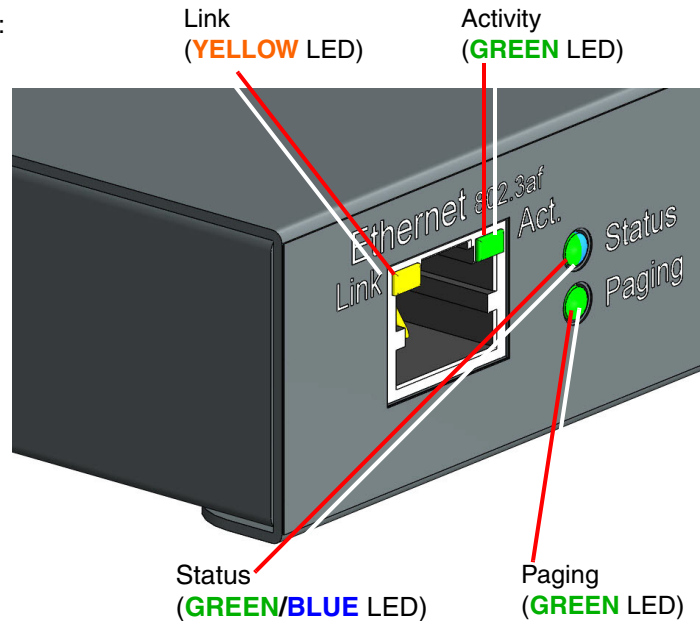
2.3.8 Confirm that the SIP Paging Server is Up and Running

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

Figure 2-6. SIP Paging Adapter LEDs

When you plug in the Ethernet cable or power supply:

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



2.3.8.1 Verify Network Activity

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

2.4 Announcing the IP Address

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

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

Figure 2-7. RTFM Switch



2.5 Restore the Factory Default Settings

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

Figure 2-8. RTFM Switch



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

Table 2-2. Factory Default Settings

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

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

To restore these parameters to the factory default settings:

1. Press and hold the **RTFM** switch until the status and paging lights come on.
2. Continue to press the switch until after the indicator lights go off, and then release it.

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

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

2.6 Configuring the SIP Paging Server

Use this section to configure the VoIP paging server.

2.6.1 Gather the Required Configuration Information

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

2.6.1.1 Static or DHCP Addressing?

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

- IP Address
- Subnet Mask
- Default Gateway

2.6.1.2 Username and Password for Configuration GUI

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

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

2.6.1.3 SIP Settings

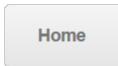
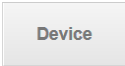
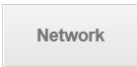

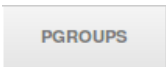

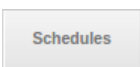
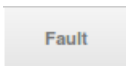

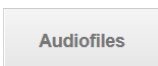



To configure the SIP parameters, determine whether you want to register with the server. If you do, determine the number of minutes the registration lease remains valid, and whether you want to automatically unregister when you reboot. To configure the SIP parameters, you also need to determine the values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

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

2.6.2 SIP Paging Server Web Page Navigation

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

Table 2-3. Web Page Navigation

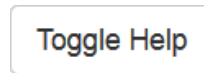
Web Page Item	Description
	Link to the Home page.
	Link to the Device page.
	Link to the Network page.
	Link to go to the SIP page.
	Link to the PGROUPS page.
	Link to the SSL page.
	Link to the Schedules page.
	Link to the Fault page.
	Link to the WiFi-Buttons page.
	Link to the Audiofiles page.
	Link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

2.6.3 Using the Toggle Help Button

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

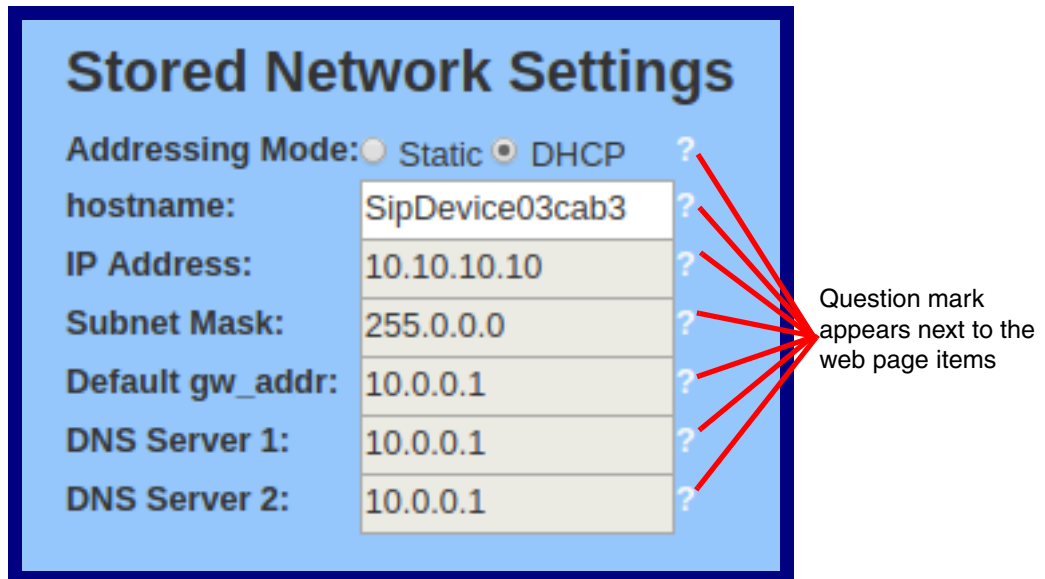
1. Click on the **Toggle Help** button that is on the UI webpage. See [Figure 2-9](#) and [Figure 2-10](#).

Figure 2-9. Toggle/Help Button



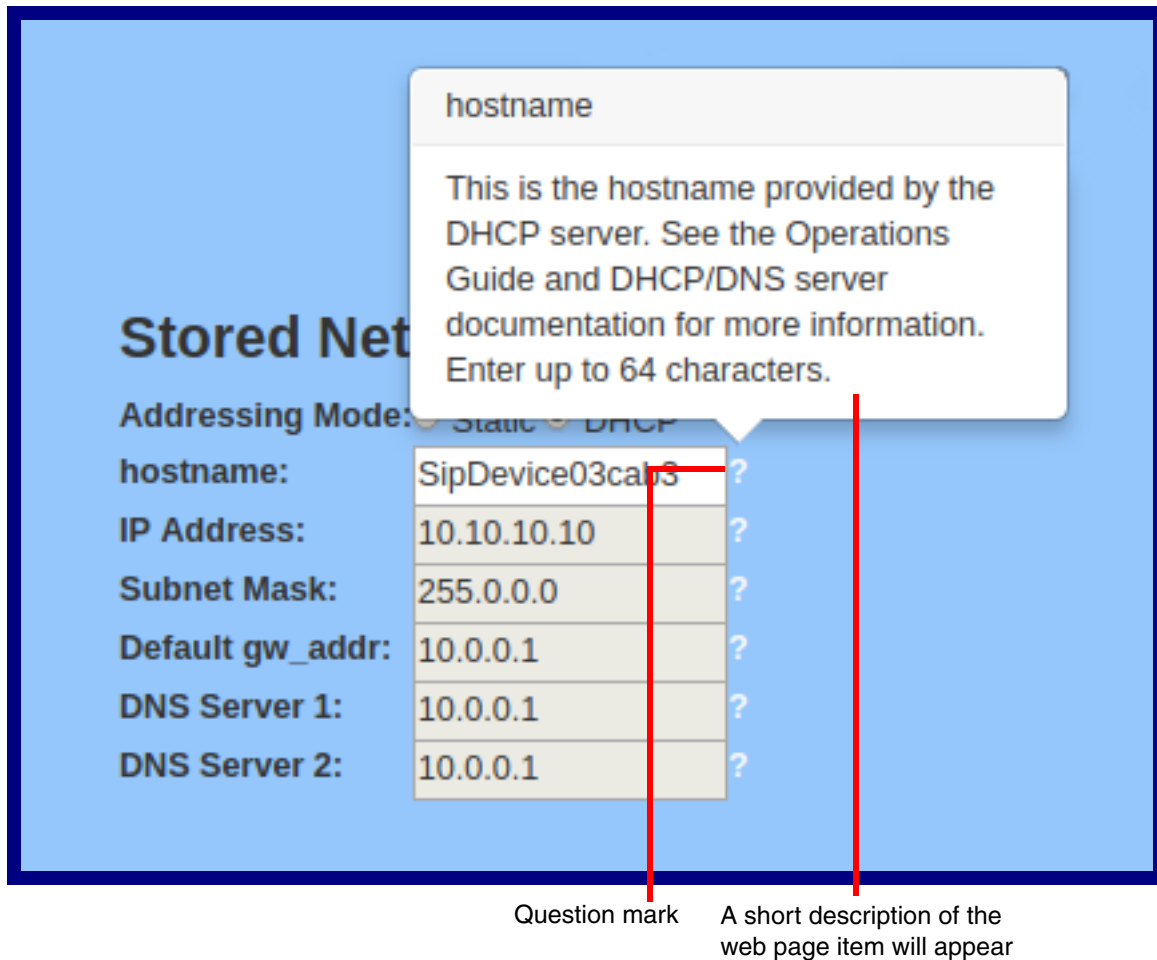
2. You will see a question mark (?) appear next to each web page item that has been provided with a short description by the Help feature. See [Figure 2-10](#).

Figure 2-10. Toggle Help Button and Question Marks



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

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



2.6.4 Log in to the Configuration GUI

1. Open your browser to the SIP Paging Server IP address.

Note If the network does not have access to a DHCP server, the device will default to an IP address of 192.168.1.23.

Note Make sure that the PC is on the same IP network as the SIP Paging Server.

Note You may also download CyberData's VoIP Discovery Utility program which allows you to easily find and configure the default web address of the CyberData VoIP products.

CyberData's VoIP Discovery Utility program is available at the **Downloads** tab on the following webpage:

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

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

Note To work with the SIP Paging Server configuration *after* the initial configuration, log in using the IP address you assign to the device. [Section 2.6.6, "Configure the Network Parameters"](#) provides instructions for entering the IP address.

2. Use the following default username and password on the **User Login** page. ([Figure 2-12](#)):

username: **admin**

password: **admin**

Change the
Default Username
and Password

To change the default web access username and password from the **Home** page ([Figure 2-13](#)):

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.
4. Click **Save Settings**.

Figure 2-12. User Login Page



The image shows a web browser window with a light blue background. At the top center, the text "CyberData Paging Server" is displayed in a large, bold, black font. Below this text, there is a small red message that says "User logged out". Underneath the message, there are three input fields: a "Username" field, a "Password" field, and a "Login" button. The "Username" and "Password" fields are white with black text, and the "Login" button is a light gray rectangle with the word "Login" in black text.

Figure 2-13. Home Page

The screenshot shows the 'Home' page of the CyberData Paging Server configuration interface. At the top is a navigation bar with tabs: Home, Device, Network, SIP, PGROUPS, SSL, Schedules, Fault, WiFi-Buttons, Audiofiles, Events, Autopro, and Firmware. The main title 'CyberData Paging Server' is centered. Below the title, the page is divided into three main sections: Current Status, Admin Settings, and Import/Export Settings.

Current Status

Serial Number:	146200001
Mac Address:	00:20:f7:04:79:0d
Firmware Version:	v21.0.0
Partition 2:	v21.0.0
Partition 3:	v21.0.0
Booting From:	partition 2

IP Addressing: DHCP
IP Address: 192.168.0.71
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.0.1
DNS Server 1: 192.168.0.1
DNS Server 2:

SIP Mode: Enabled
Event Reporting: 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

Figure 2-14. Users List

CyberData Paging Server

Users List

[Add New User](#)
[Delete All](#)
[Import Users](#)
[Export Users](#)
[Logout](#)

Username	Home	Device	Network	SIP	PGROUPS	SSL	Schedules	Fault	WiFi-Buttons	Audiofiles	Events	Autopro	Firmware		
Olivia	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Edit	Delete
Liam	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Edit	Delete
Emma	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Edit	Delete
Noah	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Edit	Delete
Amelia	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Edit	Delete
Oliver	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Edit	Delete
Ava	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Edit	Delete
Elijah	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Edit	Delete
Sophia	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Edit	Delete
Mateo	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Edit	Delete
Isabella	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Edit	Delete
Lucas	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Edit	Delete
Luna	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Edit	Delete

Figure 2-15. Add New User

Add New User

Username:

Password:

Confirm Password:

Authorized Pages

Home

Device

Network

SIP

PGROUPS

SSL

Schedules

Fault

WiFi-Buttons

Audiofiles

Events

Autoprov

Firmware

☐

☐

☐

☐

☐

☐

☐

☐

☐

☐

☐

☐

☐

Save

Cancel

5. 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.
Export Settings	
	Click Export to export the current configuration to a file.
	Click the Save button to save your configuration settings.

Table 2-4. Home Page Overview (continued)


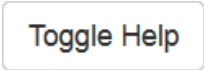
Web Page Item	Description
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse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

Figure 2-16. Users List



Table 2-5. Users List

Web Page Item	Description
Users List	
Add New User	Adds an authorized user to the user list
Delete All	Deletes all users from the current list
Import Users	Imports a previously exported user list
Export Users	Saves the current user list as a .json file. Please note that the data is encrypted and cannot be edited outside of the Paging Server Users dialog box.
Logout	Logs out the current user and returns to the user log in page
Edit	Allows administrator to modify the user's profile
Delete	Deletes the profile
Username	Name of the user

Table 2-5. Users List


Web Page Item	Description
Home	Authorizes a user to view the Home page, allowing the user to see status, but does not grant administrative privileges.
Device	Authorizes a user to view and edit the Device web page.
Network	Authorizes a user to view and edit the Network web page.
SIP	Authorizes a user to view and edit the SIP web page.
PGROUPS	Authorizes a user to view and edit the PGROUPS web page.
SSL	Authorizes a user to view and edit the SSL web page.
Schedules	Authorizes a user to view and edit the Schedules web page.
Fault	Authorizes a user to view and edit the Fault web page.
WiFi-Button	Authorizes a user to view and edit the WiFi-Button web page.
Audiofiles	Authorizes a user to view and edit the Audiofiles web page.
Events	Authorizes a user to view and edit the Events web page.
Autoprov	Authorizes a user to view and edit the Autoprov web page.
Firmware	Authorizes a user to view and edit the Firmware web page.

Figure 2-17. Add New User

Table 2-6. Add New User

Web Page Item	Description
Add New User	
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.
Authorized Pages	
Home	Authorizes a user to view the Home page, allowing the user to see status, but does not grant administrative privileges.
Device	Authorizes a user to view and edit the Device web page.
Network	Authorizes a user to view and edit the Network web page.
SIP	Authorizes a user to view and edit the SIP web page.
PGROUPS	Authorizes a user to view and edit the PGROUPS web page.
SSL	Authorizes a user to view and edit the SSL web page.
Schedules	Authorizes a user to view and edit the Schedules web page.
Fault	Authorizes a user to view and edit the Fault web page.
WiFi-Button	Authorizes a user to view and edit the WiFi-Button web page.
Audiofiles	Authorizes a user to view and edit the Audiofiles web page.
Events	Authorizes a user to view and edit the Events web page.
Autoproov	Authorizes a user to view and edit the Autoproov web page.
Firmware	Authorizes a user to view and edit the Firmware web page.
Save	Click the Save button to save your configuration settings.
Cancel	Closes the dialog box without saving changes

Table 2-6. Add New User(continued)

Web Page Item	Description
	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.

At this point you can:

- Review the SIP Paging Server's **Current Settings**. Use the RTFM switch to restore the factory default settings. See [Section 2.5, "Restore the Factory Default Settings"](#).
- Configure the device parameters. Click on the **Device** button and see [Section 2.6.5, "Configure the Device Parameters"](#) for instructions.
- Configure the network parameters. Click on the **Network** button and see [Section 2.6.6, "Configure the Network Parameters"](#) for instructions.
- Configure the SIP parameters. Click on the **SIP** button and see [Section 2.6.7, "Configure the SIP Parameters"](#) for instructions.
- Configure the PGROUPS parameters. Click on the **PGROUPS** button and see [Section 2.6.8, "Configure the Paging Groups \(PGROUPS\) Parameters"](#) for instructions.
- Configure the fault detection parameters. Click on the **Fault** button and see [Section 2.6.12, "Configure the Fault Detection Parameters"](#) for instructions.
- Configure the audio parameters. Click on the **Audiofiles** button and see [Section 2.6.14, "Configure the Audio Parameters"](#) for instructions.
- Configure the event parameters. Click on the **Events** button and see [Section 2.6.15, "Configure the Event Parameters"](#) for instructions.
- Configure the autoprovisioning parameters. Click on the **Autoprov** button and see [Section 2.6.16, "Configure the Autoprovisioning Parameters"](#) for instructions.

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

2.6.5 Configure the Device Parameters

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

1. Click on the **Device** button to open the **Device** page. See [Figure 2-18](#).

Figure 2-18. Device Page

Home Device Network SIP PGROUPS SSL Schedules Fault WiFi-Buttons Audiofiles Events Autoprovisioning Firmware

CyberData Paging Server

Line-in Settings

Enable Line-in to Line-out Loopback: ☐

Enable Line-in to Multicast: ☐

Multicast Address:

Multicast Port:

Enable Polycom Paging: ☐

Polycom Channel:

Detect Line-in Silence: ☐

Relay Settings

Activate Relay on Local Audio: ☐

Time Settings

Enable NTP: ☒

NTP Server:

Timezone:

Current Time: Thu, 09 Mar 2023 16:49:44

Misc Settings

Device Name:

Bypass DTMF Menus: ☐

Beep on Init: ☐

Beep Before Page: ☐

Multicast TTL:

Test Audio Test Relay Test Multicast

Save Reboot Toggle Help Logout









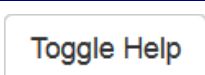

2. On the **Device** page, you may enter values for the parameters indicated in [Table 2-7](#).

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

Table 2-7. Device Configuration Parameters

Web Page Item	Description
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 audio drops below a threshold on line-input, the fault line-in multicast stream will be stopped to reduce network traffic.
Volume	Volume setting for the line-in (0-127). ^a
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	
Enable NTP ?	Sync device's local time with the specified NTP Server.
NTP Server ?	Use this field to set the address (in IPv4 dotted decimal notation or as a canonical name) for the NTP Server. This field can accept canonical names of up to 64 characters in length.
Timezone	Enter the tz database string of your timezone. Examples: America/Los_Angeles America/New_York Europe/London America/Toronto See https://en.wikipedia.org/wiki/List_of_tz_database_time_zones for a full list of valid strings.
Current Time	Displays the current time.
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).
Beep on Init ?	Device will play the user defined "pagetone" audio file when it boots.
Beep on Page ?	Device will play the user defined "pagetone" audio file before playing a SIP page.

Table 2-7. Device Configuration Parameters (continued)

Web Page Item	Description
Enable Polycom Paging on Multicast 	Enabling Polycom Paging will result in a standard RTP multicast being sent to the specified address and port and a Polycom Group Paging multicast being sent to the specified address and port+1.
Polycom Transmit Channel 	Destination channel for Polycom Group Paging multicast.
Disable HTTPS (NOT recommended) 	Disables the encrypted connection to the webpage. We do not recommend disabling HTTPS for security reasons.
	Click on the 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.
	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.

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

2.6.5.1 Polycom Paging

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

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

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

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

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

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

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

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

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

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

2.6.6 Configure the Network Parameters

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

Figure 2-19. Network Page

HomeDeviceNetworkSIPPGROUPSSSLSchedulesFaultWiFi-ButtonsAudiofilesEventsAutoprovFirmware

CyberData Paging Server

Stored Network Settings

Addressing Mode:

Static

☒ DHCP

Hostname:

SipDevice04790d

IP Address:

192.168.0.43

Subnet Mask:

255.0.0.0

Default Gateway:

192.168.0.1

DNS Server 1:

192.168.0.1

DNS Server 2:

10.0.0.1

DHCP Timeout in seconds:

60

VLAN Settings

VLAN ID (0-4095):

0

VLAN Priority (0-7):

0

Save

Reboot

Toggle Help

Logout

Current Network Settings

IP Address:

192.168.0.71

Subnet Mask:

255.255.255.0

Default Gateway:

192.168.0.1

DNS Server 1:

192.168.0.1

DNS Server 2:



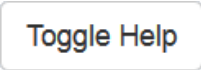
On the **Network** page, enter values for the parameters indicated in [Table 2-8](#).

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 2-8. 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 2.5, "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 2-8. Network Configuration Parameters (continued)

Web Page Item	Description
	Click the Save button to save your configuration settings.
	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**.

2.6.7 Configure the SIP Parameters

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

Figure 2-20. SIP Page

CyberData Paging Server

SIP Settings

Enable SIP operation: ☒

Register with a SIP Server: ☒

Buffer SIP Calls: ☐

Primary SIP Server: 10.0.0.253

Primary SIP User ID: 199

Primary SIP Auth ID: 199

Primary SIP Auth Password: *****

Re-registration Interval (in seconds): 360

Backup SIP Server 1:

Backup SIP User ID:

Backup SIP Auth ID:

Backup SIP Auth Password:

Re-registration Interval (in seconds): 360

Backup SIP Server 2:

Backup SIP User ID:

Backup SIP Auth ID:

Backup SIP Auth Password:

Re-registration Interval (in seconds): 360

Remote SIP Port: 5060

Local SIP Port: 5060

SIP Transport Protocol: UDP

TLS Version: 1.2 only (recommended)

Verify Server Certificate: ☐

Outbound Proxy:

Outbound Proxy Port: 0

Use Cisco SRST: ☐

Disable rport Discovery: ☐

Unregister on Boot: ☐

Keep Alive Period: 10000

Nightringer Settings

SIP Server:

SIP User ID:

SIP Auth ID:

SIP Auth Password:

Re-registration Interval (in seconds): 360

Relay rings to multicast: ☐

Multicast Address: 224.1.2.32

Multicast Port: 2020

Call Disconnection

Terminate Call after delay: 0

Audio Codec Selection

Codec: Auto Select

RTP Settings

RTP Port (even): 10500

Asymmetric RTP: ☐

Jitter Buffer: 50

RTP Encryption (SRTP): Disabled

Save Reboot Toggle Help

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

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



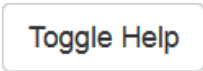
Table 2-9. SIP Configuration Parameters

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

Table 2-9. SIP Configuration Parameters (continued)

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

Table 2-9. SIP Configuration Parameters (continued)

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

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

1. Enter the IP address of the **SIP Server**.

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

2.6.7.1 Point-to-Point Configuration

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

1. On the **SIP** page (Figure 2-21), make sure of the following:
 - The **Register with a SIP Server** parameter is not selected.
 - The **Enable SIP Operation** parameter is selected
2. Click on the **Save** button to save the changes.
3. Click on the **Reboot** button to reboot the device.
4. Enter the device's IP address as a “speed dial” (also called “auto-dial”) key on the phone(s) from which you want to page.

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

Figure 2-21. SIP Page

SIP Settings

Enable SIP operation: ☒

Register with a SIP Server: ☐

Buffer SIP Calls: ☐

Primary SIP Server: 0.0.0.253

Primary SIP User ID: 99

Primary SIP Auth ID: 99

Primary SIP Auth Password: ****

Re-registration Interval (in seconds): 60

Nightringer Settings

SIP Server:

SIP User ID:

SIP Auth ID:

SIP Auth Password:

Re-registration Interval (in seconds): 360

Relay rings to multicast: ☐

Multicast Address: 224.1.2.32

Multicast Port: 2020

Register with a SIP Server is not selected

Enable SIP Operation is selected

2.6.7.2 Point-to-Point Fault Sense Reporting

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

1. On the **SIP** page (Figure 2-22), make sure of the following:
 - The **Register with a SIP Server** parameter is not selected.
 - The **Enable SIP Operation** parameter is selected

Figure 2-22. SIP Page

SIP Settings

Enable SIP operation: ☒

Register with a SIP Server: ☐

Buffer SIP Calls: ☐

Primary SIP Server: 0.0.0.253

Primary SIP User ID: 99

Primary SIP Auth ID: 99

Primary SIP Auth Password: *****

Re-registration Interval (in seconds): 60

Nightringer Settings

SIP Server:

SIP User ID:

SIP Auth ID:

SIP Auth Password:

Re-registration Interval (in seconds): 360

Relay rings to multicast: ☐

Multicast Address: 224.1.2.32

Multicast Port: 2020

Register with a SIP Server is not selected

Enable SIP Operation is selected

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

4. On the **Fault** page (Figure 2-23) in the **Dial Out Extension** field, enter the IP address of the phone that is to be called when a fault is detected at the Fault Sense Input.

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

Figure 2-23. Fault Page

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

CyberData Paging Server

Fault Detection Settings

Message Playbacks:

Play Message Locally: ☐

Make Call to Extension: ☐

Dial Out Extension:

Dial Out ID:

Multicast Audio:

Multicast Address:

Multicast Port:

Enable Polycom Paging: ☐

Polycom Channel:

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

2.6.8 Configure the Paging Groups (PGROUPS) Parameters

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

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

1. Click on the **PGROUPS** button to open the **PGROUPS** page. See [Figure 2-24](#).

Figure 2-24. 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

Figure 2-25. PGROUPS Page

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

[«](#)
[1](#)
[2](#)
[3](#)
[4](#)
[5](#)
[6](#)
[7](#)
[8](#)
[9](#)
[10](#)
[»](#)

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

Table 2-10. PGROUPS Parameters




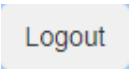


Web Page Item	Description
Stored message recording:	Enabling stored message recording allows a user to call into the device and record a stored message. Note: When recording is enabled, a warning pops up (Figure 2-26): Remember to de-select stored message recording feature once finished recording.
Recording Security Code:	Set the recording security code value, which must ONLY use digit characters '0-9'. The security code max length is 25 characters
	Click the Save button to save your configuration settings.
	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.
	Logs out the current user and returns to the user log in page
#	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.
	To make changes to the paging groups, complete the following steps: 1. Click on the Edit button to open the Configure PGROUP window (Figure 2-27). 2. In the Configure PGROUP window (Figure 2-27), edit the PGROUP (see Table 2-11 , " Configure PGROUP Window ") and click on the Save Changes button. 3. On the PGROUPS page (Figure 2-24), click on the Reboot button.
	Click the Save button to save your configuration settings.

Figure 2-26. Warning

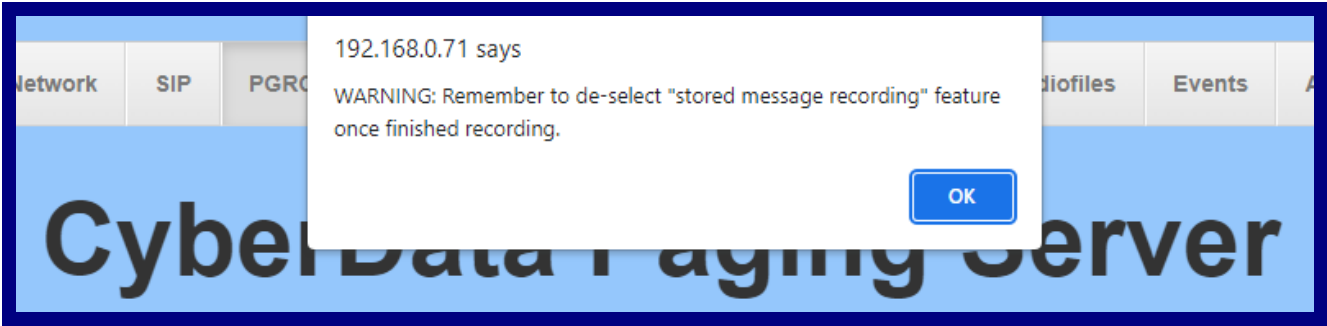


Figure 2-27. Configure PGROUP Window


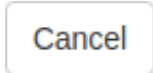

The screenshot shows a window titled "Configure PGROUP" with a close button (X) in the top right corner. The window contains the following configuration fields:

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

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

The parameters for the **Configure PGROUP** window are shown in [Table 2-11](#).

Table 2-11. 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 <i>0.0.0.0</i> .
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.
Line-out	The Lineout field determines whether or not the device will play audio out of the RCA output port and the 600 Ohm output port in addition to forwarding it to the PGROUP.
Play Stored Message	When selected, entering this paging group will play the stored message selected in 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 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.
	Click the Cancel button to close the Configure PGROUP window.
	Click the OK button to save your configuration settings.

2.6.9 Operating the Paging Server

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

2.6.9.1 DTMF Bypassed

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

2.6.9.2 DTMF Not Bypassed

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

2.6.10 Configure the SSL Parameters

1. Click **SSL** menu button to open the **SSL** page (Figure 2-28 and Figure 2-29).

Figure 2-28. SSL Configuration Page

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

CyberData Paging Server

Web Server Certificate

```

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

```

Browse... No file chosen

Import Web Certificate

Restore Web Certificate

SIP Client Certificate

```

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

```

Browse... No file chosen

Import SIP Certificate

Restore SIP Certificate

Optional Password:

Autoprovisioning Client Certificate

```

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

```

Browse... No file chosen

Import Autoprovisioning Certificate

Restore Autoprovisioning Certificate

Optional Password:

Cyberdata CA Save Reboot Toggle Help

Test TLS Connection

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

List of Trusted CAs

Browse... No file chosen Import CA Certificate Remove All Restore Defaults

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

Figure 2-29. SSL Configuration Page

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

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

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

Table 2-12. SSL Configuration Parameters

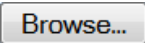


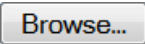


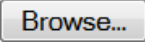
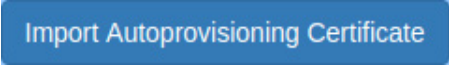
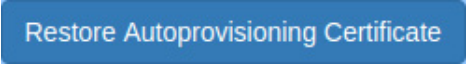
Web Page Item	Description
Web Server Certificate	Certificate used by the web server.
	Click Browse to select a certificate to import.
	After selecting a certificate, click Import Web Certificate to import it as the certificate used by this device's web server.
	Restore the device's default web server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

Table 2-12. SSL Configuration Parameters (continued)



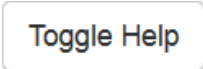





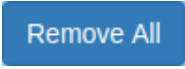

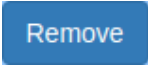
Web Page Item	Description
	Click the Save button to save your configuration settings.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) 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.
Test TLS Connection	
Server ?	The ssl test server address as a fully qualified domain name or in IPv4 dotted decimal notation.
Port ?	The supported range is 0-65536. SIP connections over TLS to port 5060 are modified to connect to port 5061. This test button will do the same.
	Use this button to test a TLS connection to a remote server using the sip client key and password. This will attempt to make a socket connection to the configured test server and port and report the success or failure. This can be used to debug TLS connection issues separate from SIP registration issues.
	Use this button to test a TLS connection to a remote server using the autoprovisioning client key and password. This will attempt to make a socket connection to the configured test server and port and report the success or failure. This can be used to debug TLS connection issues with secure autoprovisioning.
List of Trusted 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.
	Provides details of the certificate. After clicking on this button, the Certificate Info Window appears. See Section 2.6.10.1, "Certificate Info Window" .

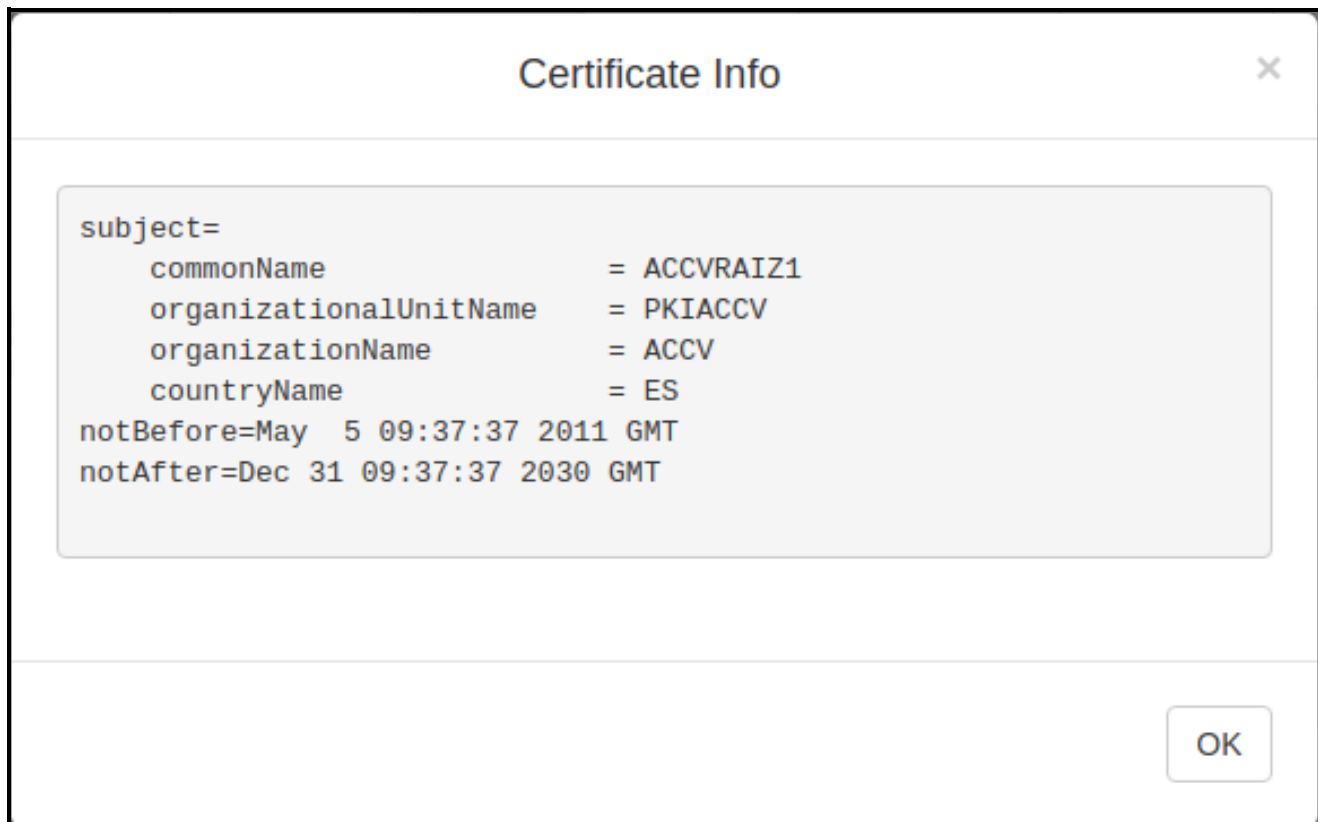
Table 2-12. SSL Configuration Parameters (continued)

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 2.6.10.2, "Remove Server Certificate Window" .

2.6.10.1 Certificate Info Window

The **Certificate Info Window** provides details of the certificate. This window appears after clicking on the **Info** button. See [Figure 2-30](#).

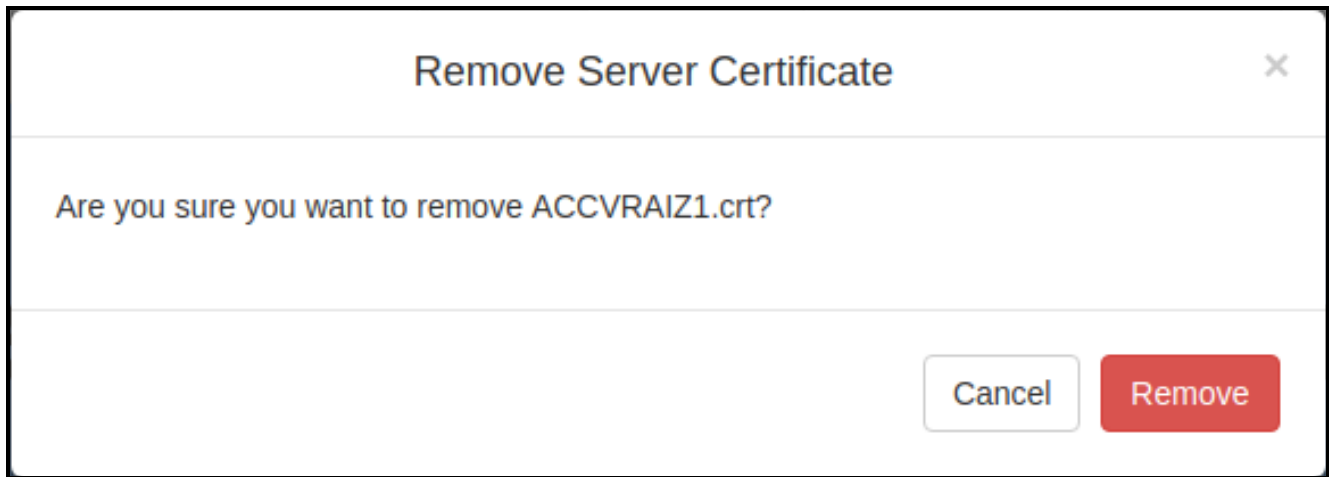
Figure 2-30. Certificate Info Window



2.6.10.2 Remove Server Certificate Window

The **Remove Server Certificate Window** will ask if the user wants to remove a certificate from the list of trusted certificates. This window appears after clicking on the **Remove** button. See [Figure 2-31](#).

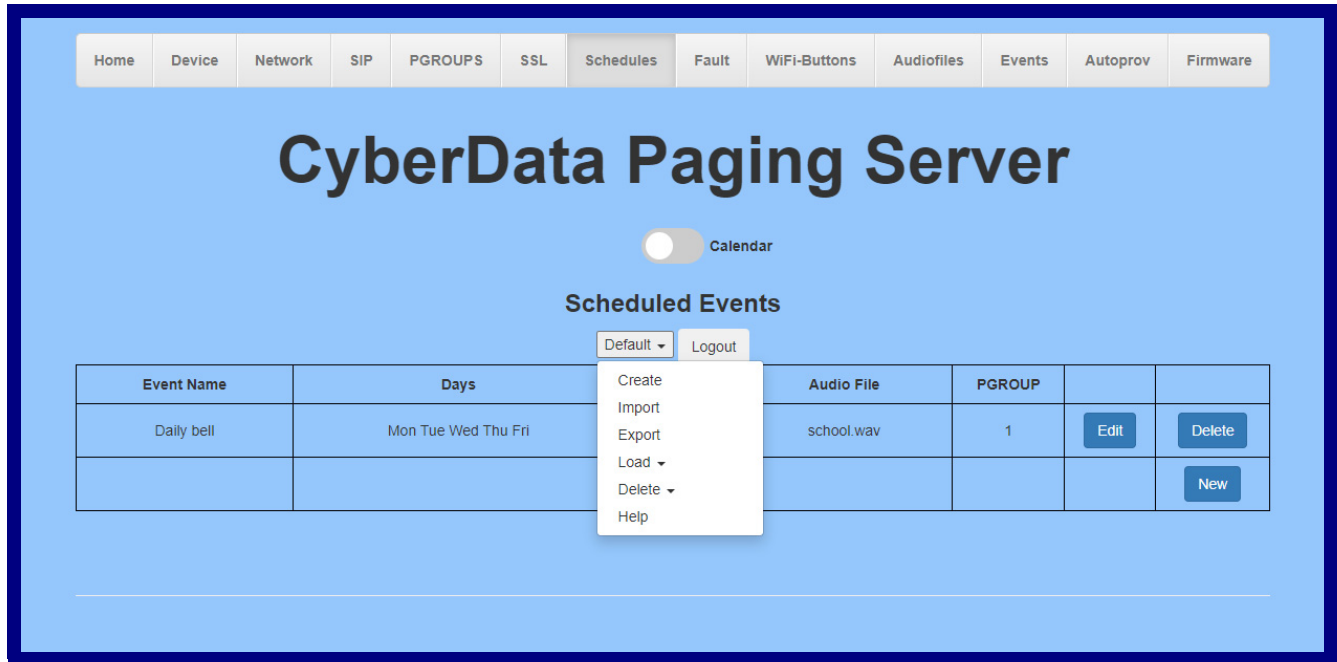
Figure 2-31. Remove Server Certificate Window



2.6.11 Configure the Schedules Parameters

1. Click on the **Schedules** button to open the **Schedules** page. See [Figure 2-32](#).

Figure 2-32. Schedules Page



2. On the **Schedules** page, enter values for the parameters indicated in [Table 2-19](#).

Table 2-13. Schedules Configuration Parameters

Web Page Item	Description
Calendar	Switches to Calendar mode, with augmented scheduling functionality. Note that scheduled events do not populate across the two modes. See Section 2.6.11.1, "Configure the Calendar"
Scheduled Events	
<div>Default ▾</div> <div> Create Import Export Load ▾ Delete ▾ Help </div>	<p>Default: Default, unnamed schedule available for editing</p> <p>Create: Used to create a new schedule. Upon saving, the new schedule will be loaded as the active schedule. Duplicate schedule names are not allowed.</p> <p>Import: Import a schedule previously exported. Imported schedules will need to be loaded to be set as the active schedule. Duplicate schedule names are not allowed.</p> <p>Export: Export currently active schedule.</p> <p>Load: Load imported or created schedules. This makes the loaded schedule active.</p> <p>Delete: Delete imported or created schedules. Deleting currently active schedule is not allowed.</p> <p>Help: Launches the help text</p>

Table 2-13. Schedules Configuration Parameters (continued)

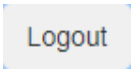



Web Page Item	Description
	Logs out the current user and returns to the user log in page
Event Name	Shows the name of the scheduled event.
Days	Shows the days of the scheduled event.
Time	Shows the time of the scheduled event.
Audio File	Shows the audio file that is associated with the scheduled event.
PGROUP	Select the paging group from the drop down menu.
	Opens the Configure Scheduled Event window for the corresponding event. See Figure 2-33, "Configure Scheduled Event Window" and Table 2-14, "Configure Scheduled Event Window Parameters"
	Removes the event from the schedule.
	Opens a new Configure Scheduled Event window.

Figure 2-33. Configure Scheduled Event Window

The screenshot shows a window titled "Configure Scheduled Event" with a close button (X) in the top right corner. The window contains several configuration fields and a dropdown menu.

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

Name: Daily bell

Time: 0900

Audio: school.wav

PGROUP: 01

Times to Play: 1

Relay: No action

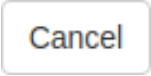

The "Relay" dropdown menu is open, showing the following options:

- Select a relay action
- No action (highlighted)
- Activate during bell
- Activate indefinitely
- Deactivate indefinitely

At the bottom right, there are two buttons: "Cancel" and "Save".

The parameters for the **Configure Scheduled Event** window are shown in [Table 2-14](#).

Table 2-14. Configure Scheduled Event Window Parameters

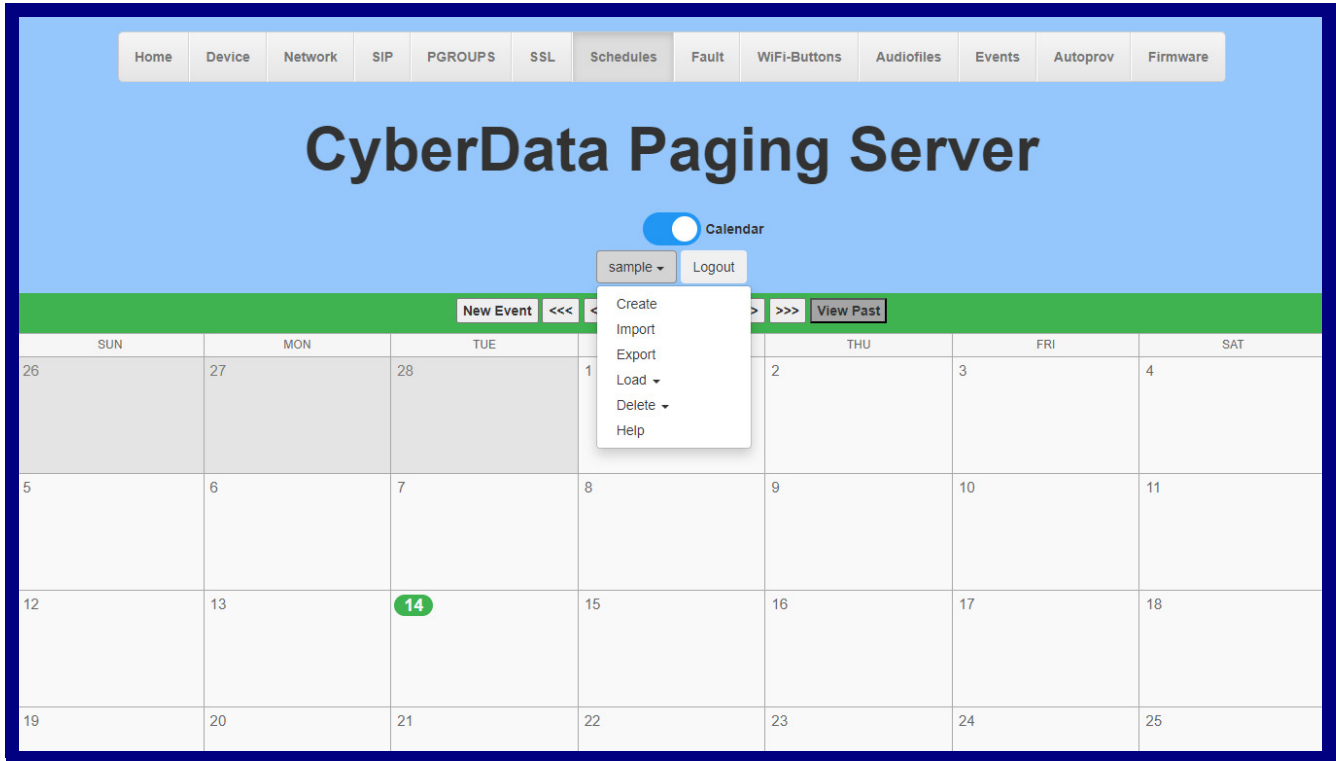
Web Page Item	Description
Days	Use the box beneath the day to select. Multiple days may be selected.
Name	Enter the name of the event, using a maximum of 16 characters.
Time	Enter time of the event, in the form HH:MM, using the 24 hour clock.
Audio	Choose the audio file to be played from the drop down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

Note www.cyberdata.net/bell-download/ has a set of sounds that can be downloaded.

2.6.11.1 Configure the Calendar

1. Enable the **Calendar** setting to open its configuration options. See [Figure 2-34](#).

Figure 2-34. Calendar Setting



The parameters for the **Calendar** are shown in [Table 2-15](#).

Table 2-15. Calendar Parameters

Web Page Item	Description
	<p>Sample: This is the default calendar</p> <p>Create: Used to create a new schedule. See Figure 2-35, "Create Schedule Window". Upon saving, the new schedule will be loaded as the active schedule (see Figure 2-38, "Populated Calendar"). Duplicate schedule names are not allowed.</p> <p>Import: Import a schedule previously exported. Imported schedules will need to be loaded to be set as the active schedule. Duplicate schedule names are not allowed.</p> <p>Export: Export currently active schedule.</p> <p>Load: Load imported or created schedules. This makes the loaded schedule active.</p> <p>Delete: Delete imported or created schedules. Deleting currently active schedule is not allowed.</p> <p>Help: Launches the help text. See Figure 2-36, "Help Window"</p>
	<p>Logs out the current user and returns to the user log in page</p>

Table 2-15. Calendar Parameters




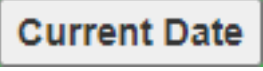



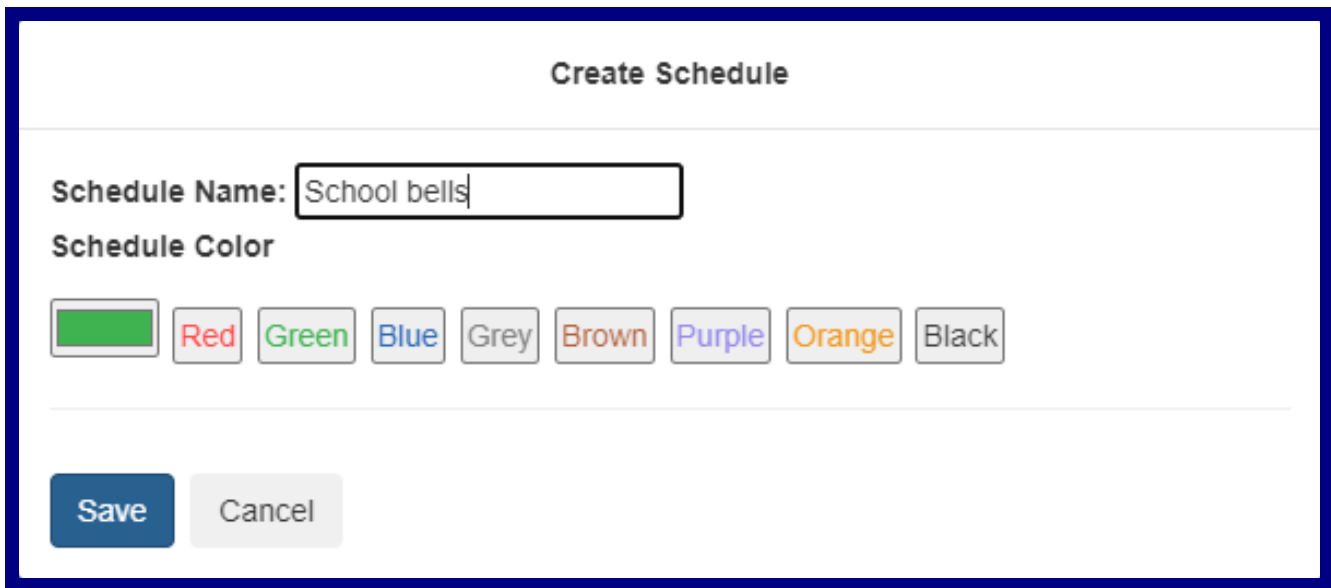
Web Page Item	Description
	Launches the dialog box to create an event. See Section 2.6.11.2, "New Event Window"
	Navigates back 1 year or to the first month of the calendar
	Navigates to the previous month
	Navigates to the current date.
	Navigates to the next month
	Navigates to one year in the future
	Displays the schedule for past days

Figure 2-35. Create Schedule Window



The parameters for the **Create Schedule** window are shown in [Table 2-15](#).

Table 2-16. Create Schedule Parameters


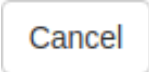
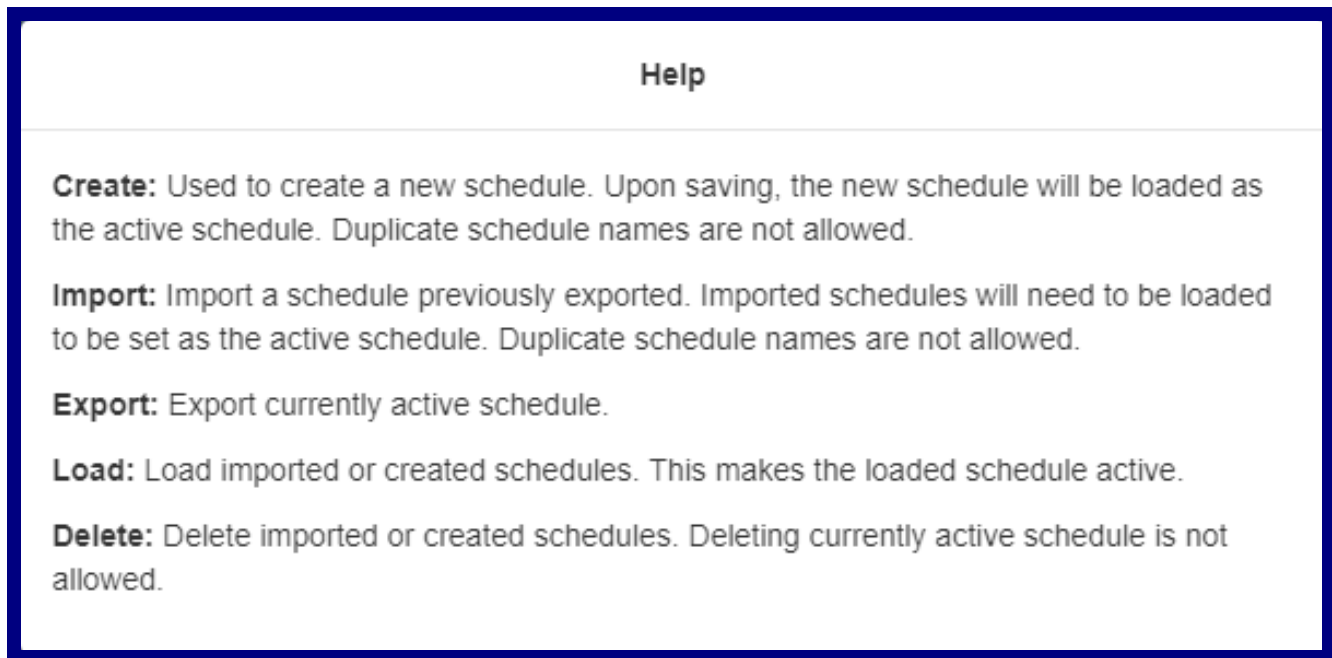
Window Item	Description
Schedule Name	Name of the schedule.
Schedule Color	Color of the schedule.
	Click the Save button to save your configuration settings.
	Click the Cancel button to close the Create Schedule window.

Figure 2-36. Help Window



2.6.11.2 New Event Window

1. Click on the **New Event** button (Figure 2-34) to open the **New Event** window. See Figure 2-37.


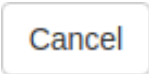
Figure 2-37. New Event Window

The 'New Event' window is a form for configuring a new event. It includes the following fields and options:

- Title:** Text input field containing 'Morning bell'.
- Start date:** Date picker showing '04/01/2023'.
- End date:** Date picker showing '04/01/2024'.
- Start time:** Time picker showing '09:00 AM'.
- End time:** Time picker showing '11:59 PM'.
- Audio:** Dropdown menu showing 'school.wav'.
- PGroup:** Dropdown menu showing '0: PagingGroup00'.
- Times to play:** Dropdown menu showing '1'.
- Relay:** Dropdown menu showing 'Activate during bell'.
- Recurring:** Checkmark is checked.
- Occurs:** Dropdown menu with options: Daily, Weekdays (highlighted), Weekly, Monthly.
- Day of Week:** Dropdown menu (empty).
- Day of Month:** Dropdown menu showing '1'.
- Every:** Input field showing '0'.
- Minute(s):** Input field showing '0'.
- Details:** Text area for additional information.
- Color:** Selection buttons for color: Green (selected), Red, Green, Blue, Grey, Brown, Purple, Orange, Black.
- Buttons:** 'Save' and 'Cancel' buttons at the bottom.

The parameters for the **New Event** window are shown in [Table 2-15](#).

Table 2-17. New Event Window Parameters

Window Item	Description
Title	The name of the event.
Start date	The start date of the event defaults to the current date; selecting the calendar allows the user to select a different date.
End Date	The end date defaults to the current date; selecting the calendar allows the user to select a different date.
Start time	Type a date or select the clock icon to indicate the start time.
End time	End time becomes enabled for a recurring event. Type a date or select the clock icon to indicate the start time.
Audio	Choose the audio file to be played from the drop down list, which displays files previously uploaded in the Bells section of the Audio Files web page.
PGROUP	Select the paging group from the drop down menu.
Times to Play	Number of times the audio file will play
Relay	<p>A relay can be activated or deactivated at the time of a scheduled bell.</p> <p>The relay options are:</p> <p>Activate during bell — The relay will be active while the bell is playing</p> <p>Activate indefinitely — The relay will be activated indefinitely.</p> <p>Deactivate indefinitely — The relay will be deactivated indefinitely.</p>
Recurring	Select this box to schedule a recurring event. Events may occur daily, only weekdays, weekly, monthly, or repeated after minutes or hours have elapsed.
Day of Week	From the drop down list, select the day of the week for a weekly recurring event.
Day of month	From the drop down list, select the day of the month for a recurring monthly event.
Every Hour(s)/Minute(s)	Type the number of hours or minutes to specify the interval of the recurring bell.
Details	This field is optional, and allows the user to provide details.
Color	Select the background color of the display of the bell.
	Click the Save button to save your configuration settings.
	Click the Cancel button to close the New Event window.

On a populated calendar (Figure 2-38), hovering over an individual bell reveals the bell menu drop down menu. (Figure 2-39).

Figure 2-38. Populated Calendar

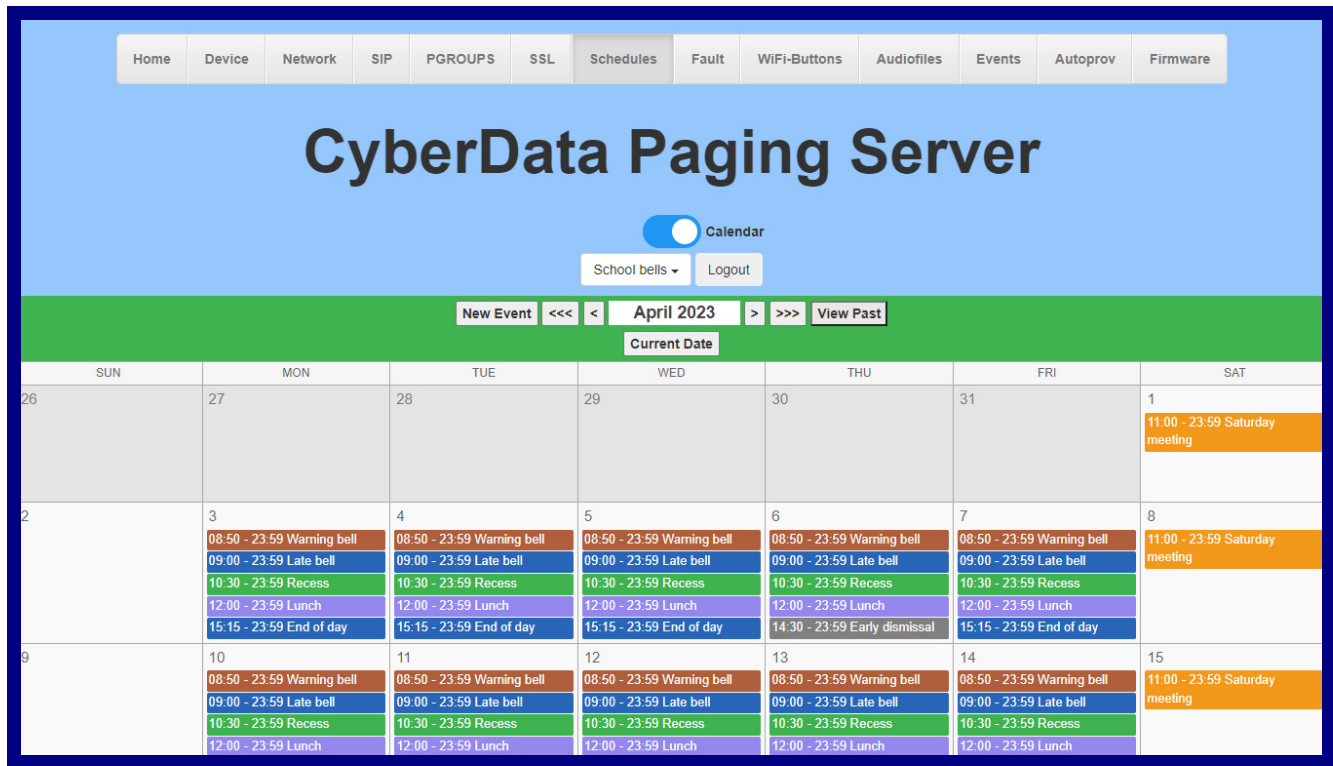
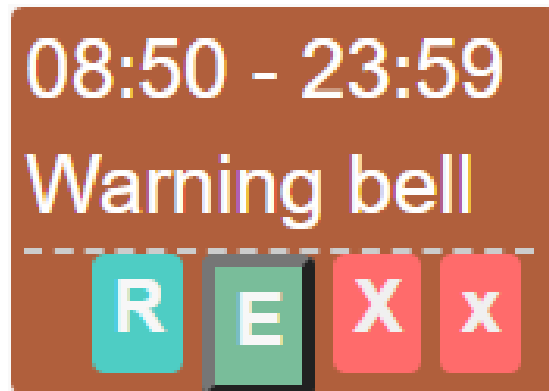


Figure 2-39. Hovering over an individual bell reveals the bell menu drop down menu



The parameters for the bell menu drop down menu are shown in Table 2-18.

Table 2-18. Bell Menu Drop Down Menu Parameters

Menu Item	Description
R	Indicates a recurring event
E	Launches the Edit Event window
X	Deletes all occurrences of this event.
x	Deletes the current occurrence of this event.

2.6.12 Configure the Fault Detection Parameters

1. Click on the **Fault** button to open the **Fault** page. See [Figure 2-40](#).

Figure 2-40. Fault Page

The screenshot shows the 'Fault' page of the CyberData Paging Server web interface. The page has a light blue background and a dark blue border. At the top, there is a navigation bar with buttons for Home, Device, Network, SIP, PGROUPS, SSL, Schedules, Fault (highlighted), WiFi-Buttons, Audiofiles, Events, Autopro, and Firmware. Below the navigation bar, the title 'CyberData Paging Server' is displayed in a large, bold, black font. Underneath the title, the section 'Fault Detection Settings' is shown. This section contains several configuration fields: 'Message Playbacks' (a text input with '0'), 'Play Message Locally' (a checkbox), 'Make Call to Extension' (a checkbox), 'Dial Out Extension' (a text input with '204'), 'Dial Out ID' (a text input with 'id204'), 'Multicast Audio' (a dropdown menu with 'Disabled' selected), 'Multicast Address' (a text input with '239.168.3.1'), 'Multicast Port' (a text input with '8888'), 'Enable Polycom Paging' (a checkbox), and 'Polycom Channel' (a dropdown menu with '1' selected). Below these fields, there is a 'Test Fault Sensor' button. At the bottom of the page, there are four buttons: 'Save', 'Reboot', 'Toggle Help', and 'Logout'.

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

CyberData Paging Server

Fault Detection Settings

Message Playbacks:

Play Message Locally: ☐

Make Call to Extension: ☐

Dial Out Extension:

Dial Out ID:

Multicast Audio:

Multicast Address:

Multicast Port:





Enable Polycom Paging: ☐

Polycom Channel:

- On the **Fault Detection** page, enter values for the parameters indicated in [Table 2-19](#).

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

Table 2-19. Fault Detection Configuration Parameters

Web Page Item	Description
Triggered Settings	
Message Playbacks ?	The number of times to repeat the audio message through the local speaker or to the remote endpoint. A value of 0 will repeat forever. Enter a value from 0-65536.
Play Message Locally ?	When selected, the device will play the user defined “sensor triggered” audio file when the fault detection is triggered.
Make Call to Extension ?	When selected, the device will call an extension when fault detection is triggered. Use the 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.
Multicast Audio ?	When enabled, the device will multicast audio to the specified multicast address and port while the fault sensor is activated.
Message ?	When set to Message , the device will multicast the user defined sensor triggered audio file.
Line-in ?	When set to Line-in, the device will multicast line-in audio.
Multicast Address ?	The multicast address used for fault detection audio.
Multicast Port ?	The multicast port used for fault detection audio.
Detect Line-in Silence ?	If audio drops below a threshold on line-input, the fault line-in multicast stream will be stopped to reduce network traffic.
	Click on the Test Fault Sensor button to test the fault detection feature.
	Click the Save button to save your configuration settings.
	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.

2.6.13 Configure the WiFi-Buttons Parameters

1. Click on the **WiFi-Buttons** button to open the **WiFi-Buttons** page. See [Figure 2-41](#).
1. Before WiFi Buttons become available to be associated with the Paging Server, WiFi network settings must be configured using the WiFi Utility. Please see the *011527 WiFi Alert Button Operations Guide* at the **Downloads** tab at the following webpage:
<https://www.cyberdata.net/products/011527/>

Figure 2-41. WiFi-Buttons Page

Name	IP Address	MAC Address	Serial Number	Firmware Version	Battery SoC		
WiFi Button	192.168.0.251	00:20:f7:04:e0:78	527000226	v2.4.2	100%	View/Config	Disassociate
WiFi Button	192.168.0.10	00:20:f7:04:e0:83	527000237	v2.4.2	99%	View/Config	Disassociate
WiFi Button	192.168.0.8	00:20:f7:04:e0:81	527000235	v2.4.2	52%	View/Config	Disassociate
WiFi Button	192.168.0.17	00:20:f7:04:e0:8a	527000244	v2.4.2	98%	View/Config	Disassociate

2. On the WiFi-Buttons page, enter values for the parameters indicated in [Table 2-20](#).

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

Table 2-20. WiFi-Buttons Configuration Parameters

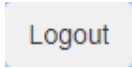
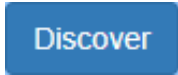


Web Page Item	Description
Discovered WiFi Buttons	
	Logs out the current user and returns to the user log in page
	Discovers WiFi Buttons on the network
Name ?	Button's name (recommended to have a unique name for each)
IP Address ?	Button's IP Address
MAC Address: ?	MAC address of the button
Serial Number ?	Serial number of the button
Firmware Version ?	Firmware version being used by the button
Battery SoC ?	Battery State of Charge (SoC) of the button
	Opens the Buttons Settings Page . See Figure 2-42 and Figure 2-43 .
	Severs the association with the SIP Paging Server, erasing fields pertaining the button press and the heartbeat timeout.

Figure 2-42. Button Settings Page

Button Settings

Serial Number:	527000235	<div style="margin-bottom: 5px;">Save</div> <div style="margin-bottom: 5px;">Get Log</div> <div style="margin-bottom: 5px;">Clear Log</div> <div style="margin-bottom: 5px;">Restart Button</div> <div style="margin-bottom: 5px;">Cancel</div> <div style="margin-bottom: 5px;">Toggle Help</div>
MAC Address:	00:20:f7:04:e0:81	
Firmware Version:	v2.4.2	
Battery SoC	52%	
Power Source	Line	
Addressing Mode	<input type="radio"/> Static <input checked="" type="radio"/> DHCP	
IP Address:	192.168.0.8	
Subnet Mask:	255.255.255.0	
Default Gateway:	192.168.0.1	
DNS Server:	192.168.0.1	
SSID:	TP-Link_FC70	
NTP Server:	pool.ntp.org	
Time Zone:	PST+8PDT,M3.2.0,M	
Device Name:	WiFi Button	
Logging IP Address:	239.255.255.255	

Button Press Duration (ms):

Button press PGROUP: Choose a PGROUP ▼

Button press MSG: Choose a MSG ▼

Times to play MSG:

Button press Ext:



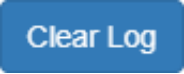


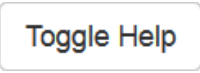
Figure 2-43. Button Settings Page

Heartbeat timeout (seconds):	<input type="text"/>
Heartbeat timeout PGROUP:	<input type="text" value="Choose a PGROUP"/>
Heartbeat timeout MSG:	<input type="text" value="Choose a MSG"/>
Times to play MSG:	<input type="text" value="1"/>
Heartbeat timeout Ext:	<input type="text"/>
Buzzer Volume (Line 0-10):	<input type="text"/>
Buzzer Pattern (Line):	<input type="text" value="v"/>
Buzzer Volume (Batt 0-10):	<input type="text"/>
Buzzer Pattern (Batt):	<input type="text" value="v"/>
LED Brightness (Line 0-10):	<input type="text"/>
LED Pattern (Line):	<input type="text" value="v"/>
LED Brightness (Batt 0-10):	<input type="text"/>
LED Pattern (Batt):	<input type="text" value="v"/>

Table 2-21. Button Settings Page Parameters

Web Page Item	Description
Discovered WiFi Buttons	
Serial Number ?	Serial number of the button
MAC Address: ?	MAC address of the button
Firmware Version ?	Firmware version being used by the button
Battery SoC ?	Battery State of Charge (SoC) of the button
Power Source ?	Power source of the button
Addressing Mode ?	Indicates if the button is using DHCP or Static
IP Address ?	Button's IP Address
Subnet Mask ?	Subnet mask of the network
SSID ?	Service Set Identifier (SSID) of the network
NTP Server ?	Network Time Protocol (NTP) Server of the network
Time Zone ?	Time Zone
Device Name ?	Button's name (recommended to have a unique name for each)
Logging IP Address ?	Logging IP Address
ButtonPress Duration (ms) ?	The time in milliseconds the button must be pressed before an event is registered
Button press PGROUP ?	Paging Group to multicast an audio message on a button press
Button press MSG ?	Audio message to play on button press. To upload a message, please go the Stored Messages section of the Audiofiles page.
Times to play MSG ?	Times to play audio message on button press
Button press extension ?	SIP extension to dial on button press
Heartbeat timeout ?	Buttons send a heartbeat message every 60 seconds. This is the timeout in seconds after which a failure to receive a heartbeat message will raise an event.
Heartbeat timeout PGROUP ?	Paging Group used to multicast an audio message on a heartbeat timeout
Heartbeat timeout MSG ?	Audio file to play on heartbeat timeout. TO upload a message, please go to the Stored Messages section of the Audiofiles page.
Times to play MSG ?	Times to play the audio message on heartbeat timeout
Heartbeat timeout extension ?	SIP extension to dial on heartbeat timeout.
Buzzer Volume ?	Set the buzzer power volume when the device is plugged in, where 0 is min power volume and 10 is the max power volume.
Buzzer Pattern ?	Set the buzzer pattern used when the device is plugged in.
Buzzer Volume ?	Set the buzzer power volume when the device is running on battery, where 0 is min power volume and 10 is the max power volume.
Buzzer Pattern ?	Set the buzzer pattern used when the device is running on battery.
LED Brightness ?	Set the LED brightness when the device is plugged in.
LED Pattern ?	Set the LED pattern used when the device is plugged in.
LED Brightness ?	Set the LED brightness when the device is running on battery.
Battery Power Pattern ?	Set the LED pattern used when the device is running on battery.

Table 2-21. Button Settings Page Parameters (continued)

Web Page Item	Description
	Click the Save button to save your configuration settings.
	Downloads the WiFi Button's log
	Erases the Wifi Button's Log from the log partition
	Restarts the WiFi Button
	Closes the Button Settings window without saving changes
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

2.6.14 Configure the Audio Parameters

Click on the **Audiofiles** button to open the **Audiofiles** page. See [Figure 2-44](#). 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 2-44. Audiofiles Page

HomeDeviceNetworkSIPPGROUPSSLSchedulesFaultWiFi-ButtonsAudiofilesEventsAutoprovFirmware

CyberData Paging Server

Logout

Available Space: 1483MB

Audio Files

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

Figure 2-45. 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"/>
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"/>
Confused:	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"/>
Enter Zone:	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"/>
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"/>
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"/>
Ringback 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"/>
Ring 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"/>
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"/>
Stored Message File Not Found:	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"/>

Menu Audio Files

Cancel:	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"/>
Currently Playing:	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 2-46. Audiofiles Page

Page:	Currently set to:	default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Play Stored Message:	Currently set to:	default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Pound (#):	Currently set to:	default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Press:	Currently set to:	default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Stored Message:	Currently set to:	default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
To:	Currently set to:	default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Enter Code:	Currently set to:	default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Enter Recording Security 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"/>
Press Start To Record Message:	Currently set to:	default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Or:	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"/>
Record Message Prompt:	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"/>
Save Record Message Prompt:	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"/>
Assign Zone To Message:	Currently set to:	default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Message Saved Successfully:	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"/>
Message Not Saved Successfully:	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"/>
You Recorded:	Currently set to:	default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>

Stored Messages

Figure 2-47. Audiofiles Page

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"/>
Press Start To Record Message:	Currently set to:	default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Or:	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"/>
Record Message Prompt:	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"/>
Save Record Message Prompt:	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"/>
Assign Zone To Message:	Currently set to:	default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Message Saved Successfully:	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"/>
Message Not Saved Successfully:	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"/>
You Recorded:	Currently set to:	default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Delete"/>	<input type="button" value="Save"/>

Stored Messages

No file chosen

Bells

No file chosen

On the **Audiofiles** page, enter values for the parameters indicated in [Table 2-22](#).

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 2-22. Audiofiles Configuration Parameters

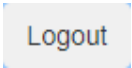

Web Page Item	Description
Audio Files	
	Logs out the current user and returns to the user log in page
0-9	<p>The name of the audio configuration option is the same as the spoken audio that plays on the board (24 character limit).</p> <p>'0' corresponds to the spoken word "zero."</p> <p>'1' corresponds to the spoken word "one."</p> <p>'2' corresponds to the spoken word "two."</p> <p>'3' corresponds to the spoken word "three."</p> <p>'4' corresponds to the spoken word "four."</p> <p>'5' corresponds to the spoken word "five."</p> <p>'6' corresponds to the spoken word "six."</p> <p>'7' corresponds to the spoken word "seven."</p> <p>'8' corresponds to the spoken word "eight."</p> <p>'9' corresponds to the spoken word "nine."</p>
Dot	Corresponds to the spoken word "dot."
Audio Test	Corresponds to the message "This is the CyberData IP speaker test message..."
Page Tone	Corresponds to a simple tone that is unused by default.
Your IP Address is	Corresponds to the message "Your IP address is..."
Rebooting	Corresponds to the spoken word "Rebooting."
Restoring Default	Corresponds to the message "Restoring default."
Ringback Tone	Specifies the Ringback Tone.
Ring Tone	Specifies the Ring Tone.
Night Ring	Specifies the ringtone for nightring. By default this parameter uses the same audio file that is selected for the Ring Tone parameter.
Sensor Triggered	Corresponds to the message "Sensor Triggered."
Stored Message File Not Found	Corresponds to the message "Stored Message File Not Found."
Enter Zone	Corresponds to the words "Enter Zone" used in the audio menu played to the caller.
Confused	Corresponds to the message "Confused."
	The Browse button will allow you to navigate to and select an audio file.

Table 2-22. Audiofiles Configuration Parameters (continued)




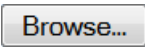



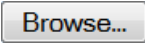


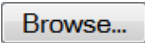


Web Page Item	Description
	The Play button will play that audio file.
	The Delete button will delete any user uploaded audio and restore the stock audio file.
	The Save button will download a new user audio file to the board once you've selected the file by using the Browse button. The Save button will delete any pre-existing user-uploaded audio files.
Menu Audio Files	Menu Audio Files are user-uploadable messages that create the audio menu played to the caller.
Cancel	Corresponds to the word "Cancel" used in the audio menu played to the caller.
Currently Playing	Corresponds to the words "Currently Playing" used in the audio menu played to the caller.
Invalid Entry	Corresponds to the words "Invalid Entry" used in the audio menu played to the caller.
Page	Corresponds to the word "Page" used in the audio menu played to the caller.
Play Stored Message	Corresponds to the words "Play Stored Message" used in the audio menu played to the caller.
Pound (#)	Corresponds to whatever word or phrase the user wishes to call the pound key in the audio menu played to the caller.
Press	Corresponds to the word "Press" used in the audio menu played to the caller.
Stored Message	Corresponds to the words "Stored Message" used in the audio menu played to the caller.
To	Corresponds to the word "To" used in the audio menu played to the caller.
Enter Code	Corresponds to the message "Enter Code."
Invalid Code	Corresponds to the message "Invalid Code."
Press Start to Record Message	Corresponds to the message "Press Start to Record Message."
Or	Corresponds to the message "Or."
Record Message Prompt	Corresponds to the message "Record Message Prompt."
Save Record Message Prompt	Corresponds to the message "Save Record Message Prompt."
Assign Zone to Message	Corresponds to the message "Assign Zone to Message."
Message Saved Successfully	Corresponds to the message "Message Saved Successfully."
Message Not Saved Successfully	Corresponds to the message "Message Not Saved Successfully."
You Recorded	Corresponds to the message "You Recorded."
	The Browse button will allow you to navigate to and select an audio file.
	The Play button will play that audio file.

Table 2-22. Audiofiles Configuration Parameters (continued)

Web Page Item	Description
	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.
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.
	The Upload Message button will upload the stored message.
	The Delete All Messages button will delete all of the stored messages.
Bells	Upload files here to be used in scheduled events. Note: The user may upload a maximum of 25 files.
	The Browse button will allow you to navigate to and select an audio file.
	The Upload Bell button will upload the bell.
	The Delete All Bells button will delete all of the bells.

2.6.14.1 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 2-48](#) through [Figure 2-50](#).

Figure 2-48. Audacity 1

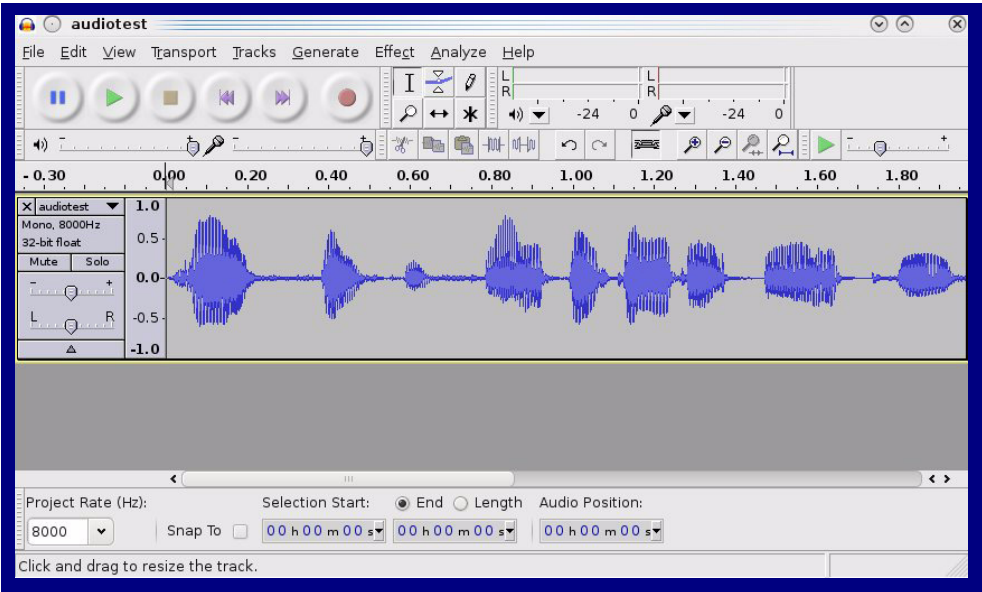
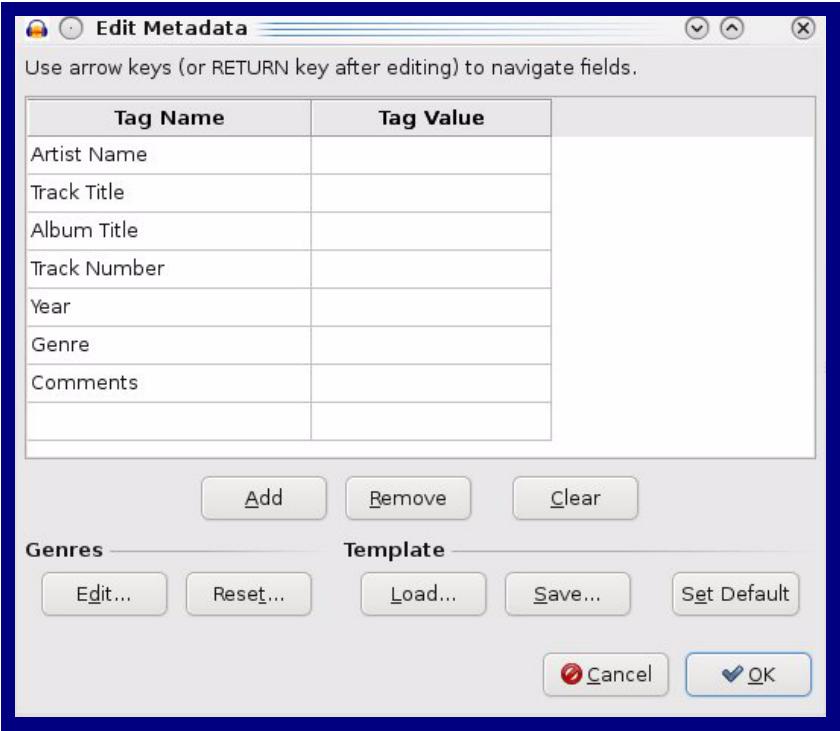


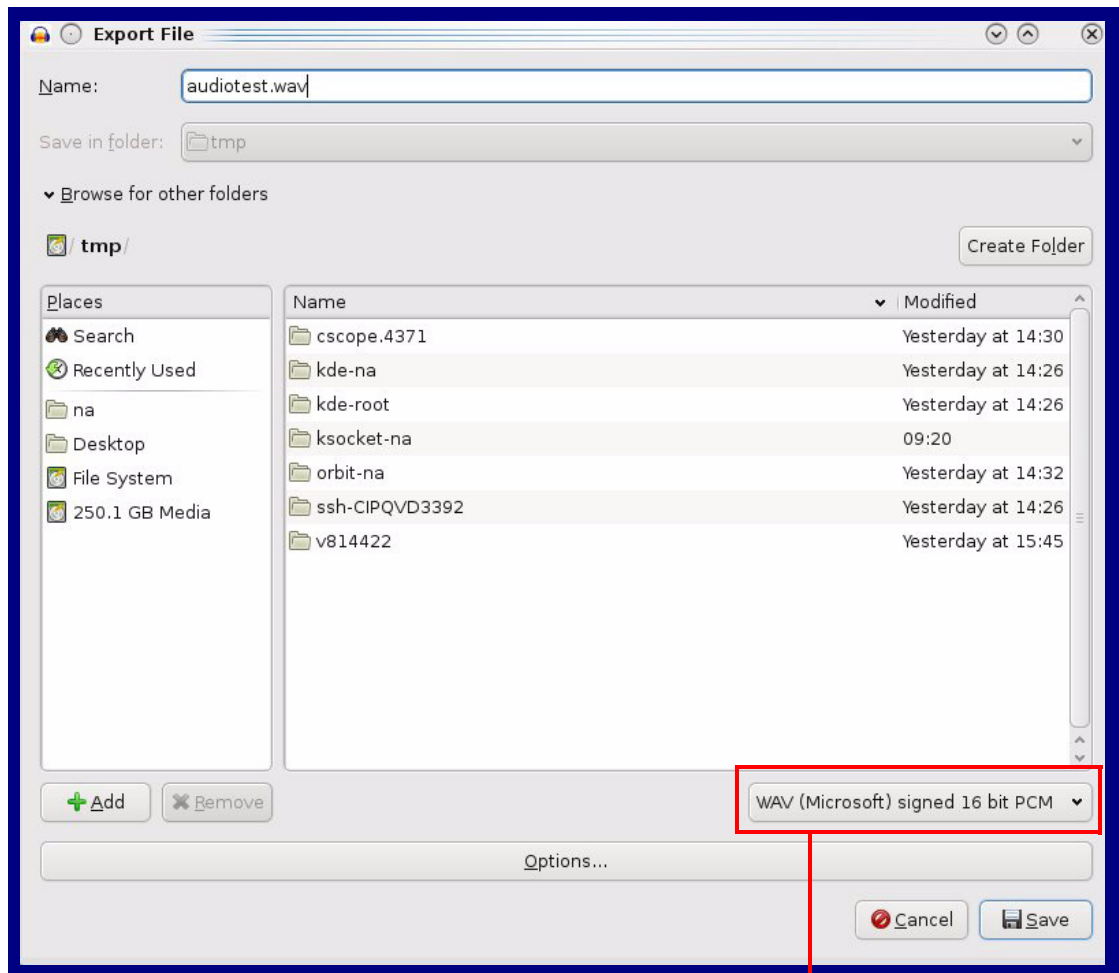
Figure 2-49. Audacity 2



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

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

Figure 2-50. WAV (Microsoft) signed 16 bit PCM



WAV (Microsoft) signed 16 bit PCM

2.6.15 Configure the Event Parameters

Click on the **Events** button to open the **Events** page (Figure 2-51). The **Events** page specifies a remote server that can be used to receive HTTP POST events when actions take place on the board.

Figure 2-51. Events Page

The screenshot shows the 'Events' configuration page of the CyberData Paging Server. At the top is a navigation bar with tabs: Home, Device, Network, SIP, PGROUPS, SSL, Schedules, Fault, WiFi-Buttons, Audiofiles, Events (selected), Autoprov, and Firmware. The main title 'CyberData Paging Server' is centered. Below it, on the left, is a section 'Events' with a toggle 'Enable Event Generation:' (unchecked) and a list of checkboxes for various 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, and Enable 60 Second Heartbeat. On the right is the 'Event Server' section with input fields for 'Server IP Address' (10.0.0.250), 'Server Port' (8080), and 'Server URL' (xmlparse_engine). At the bottom right are four buttons: Save, Reboot, Toggle Help, and Logout.

Table 2-23 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 2-23. 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 2.6.15.1, "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.
Reboot	Click on the Reboot button to reboot the system.
Toggle Help	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

2.6.15.1 Example Packets for Events

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

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

Here are example packets for every event:

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

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

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

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

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

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

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

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>CALL_ACTIVE</event>
</cyberdata>
POST xmlparse_engine HTTP/1.1
```

```
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 205
Content-Type: application/x-www-form-urlencoded

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

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

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

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>MULTICAST_START</event>
<index>8</index>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 233
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>MULTICAST_STOP</event>
<index>8</index>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>RELAY_ACTIVATED</event>
</cyberdata>
POST xmlparse_engine HTTP/1.1
```

```
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>RELAY_DEACTIVATED</event>
</cyberdata>
```

```
POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>NIGHTRINGING</event>
</cyberdata>
```

2.6.16 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 2-52](#).

Figure 2-52. Autoprovisioning Page

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

CyberData Paging Server

Enable Autoprovisioning: ☒

Autoprovisioning Server:

Autoprovisioning Filename:

Use tftp: ☐

Verify Server Certificate ☐

Username:

Password:

Autoprovisioning autoupdate (in minutes):

Autoprovision at time (HHMM):

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 '0020f704790d.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
```

2. On the **Autoprovisioning** page, you may enter values for the parameters indicated in [Table 2-24](#).

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 2-24. Autoprovisioning Configuration Parameters



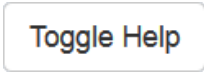

Web Page Item	Description
Disable Autoprovisioning ?	Prevent the device from automatically trying to download a configuration file. See Section 2.6.16.1, "Autoprovisioning" for more information.
Autoprovisioning Server ?	Enter the IPv4 address of the provisioning server in dotted decimal notation.
Autoprovisioning 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, make sure that the Enable NTP setting on the Device Page is selected (see Table 2-7).</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, make sure that the Enable NTP setting on the Device Page is selected (see Table 2-7).</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, make sure that the Enable NTP setting on the Device Page is selected (see Table 2-7).</p>
	Click the Save button to save your configuration settings.
	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.

Table 2-24. Autoprovisioning Configuration Parameters (continued)

Web Page Item	Description
	Press the Download Template button to create an autoprovisioning file for the device. See Section 2.6.16.3, "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).

2.6.16.1 Autoprovisioning

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

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

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

By default, the device will get its autoprovisioning server from the DHCP options. See [Section 2.6.16.2, "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 2-24](#)). 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 2-25. 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.

2.6.16.2 Sample dhcpd.conf

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

ddns-update-style none;

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

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

    option routers                10.0.0.1;
    option subnet-mask            255.0.0.0;

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

    option time-offset            -8;          # Pacific Standard Time

#    option www-server            99.99.99.99;          # OPTION 72

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

#    option option-150            10.0.0.252;          # OPTION 150

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

    range 10.10.0.1 10.10.2.1; }
```

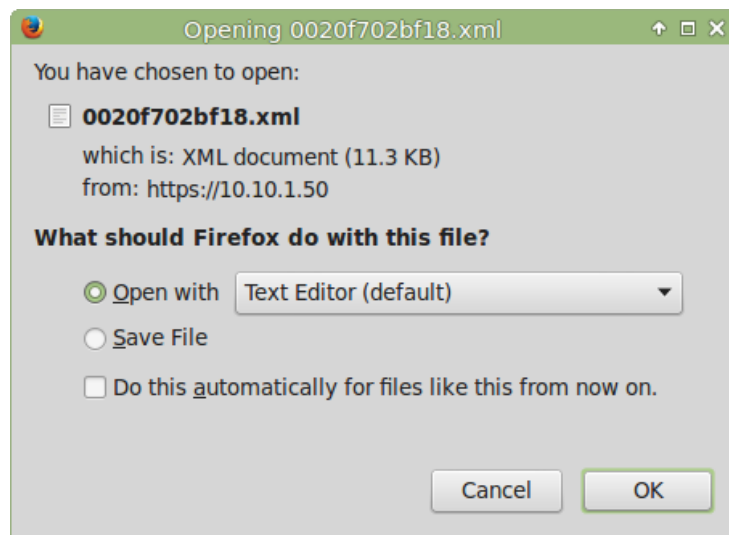
2.6.16.3 Get Autoprovisioning Template Button

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 2-53). 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 2-53.

Figure 2-53. Configuration File



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

2.7 Upgrade the Firmware

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

To upgrade the firmware of your device:

1. Download the latest firmware file from the **Downloads** tab at the following webpage:
<https://www.cyberdata.net/products/011146>
2. Unzip the firmware version file. This file may contain the following:
 - Firmware file
 - Release notes
 - Autoprovisioning template
3. Log in to the **Home** page as instructed in [2.6.4 "Log in to the Configuration GUI"](#).
4. Click on the **Firmware** menu button to open the **Firmware** page ([Figure 2-54](#)).

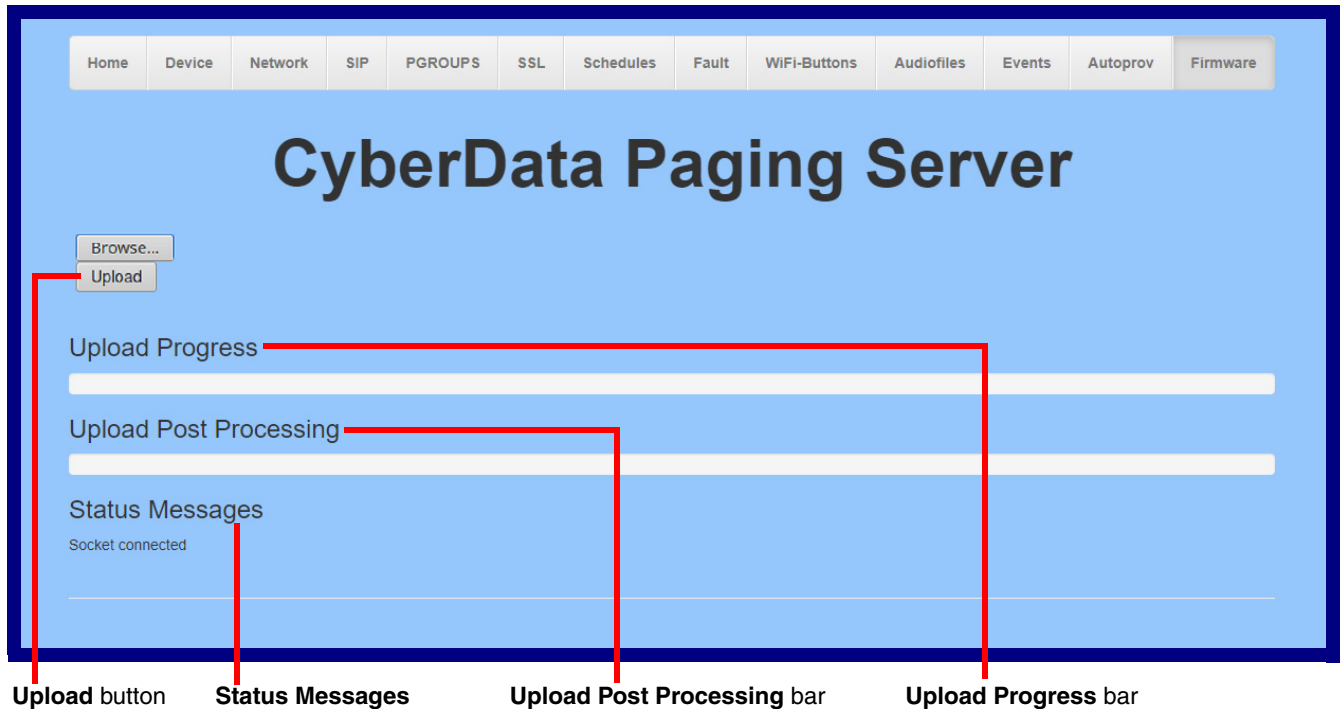
Figure 2-54. Firmware Page



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

6. Select the firmware file. This reveals the **Upload** button (Figure 2-55).

Figure 2-55. Upload Button



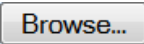

7. Click on the **Upload** button. After selecting the **Upload** button, you will see the progress of the upload in the **Upload Progress** bar.
8. When the upload is complete, you will see the words **Upload finished** under **Status Messages**.
9. At this point, you will see the progress of the upload's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

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

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

Table 2-26 shows the web page items on the **Firmware** page.

Table 2-26. Firmware Page Parameters

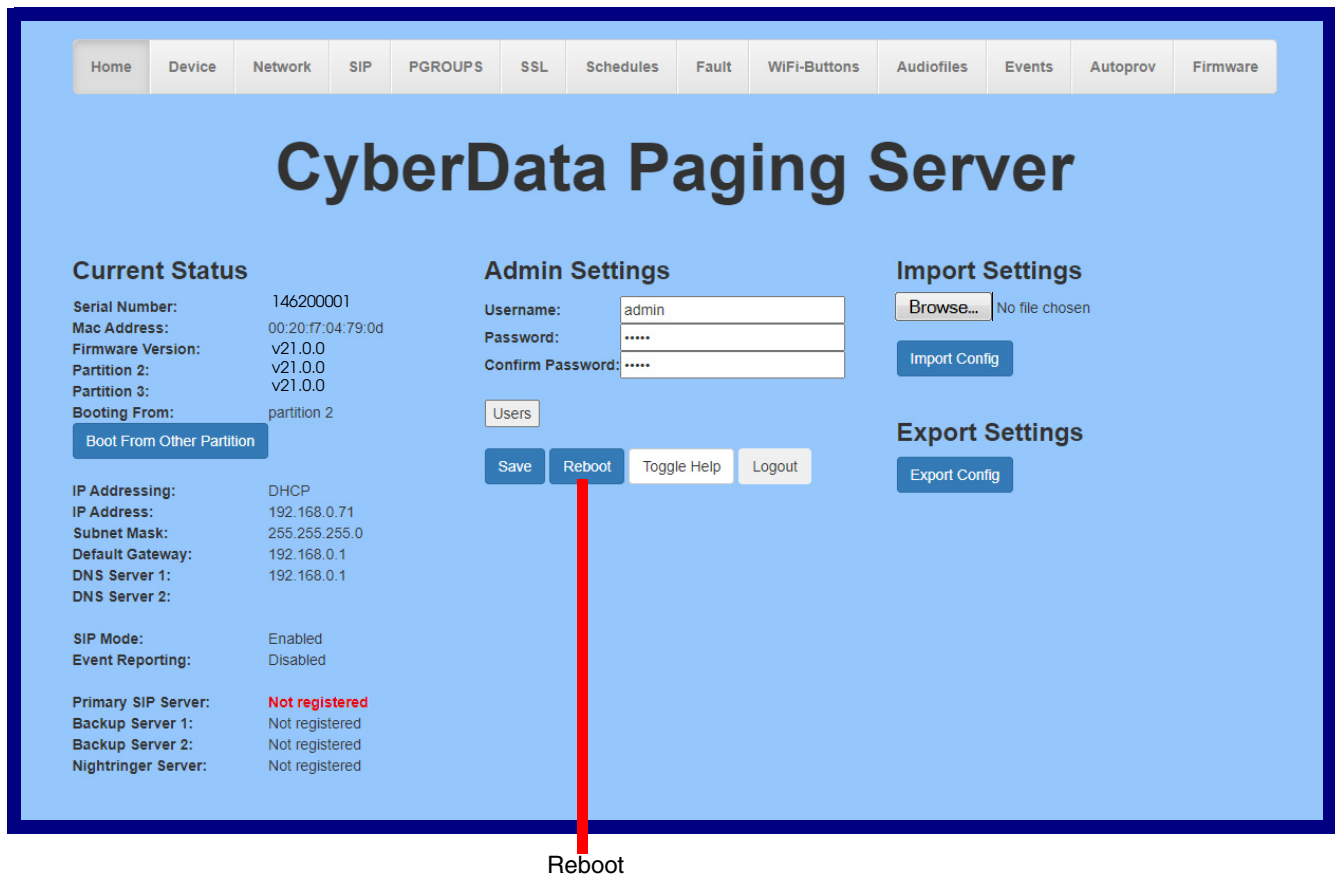
Web Page Item	Description
	Use the Browse button to navigate to the location of the firmware file that you want to upload.
	Click on the Upload button to automatically upload the selected firmware and reboot the system. Note: This button only appears after the user has selected a firmware file.
Upload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

2.7.1 Reboot the SIP Paging Server

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

1. Click **Reboot** ([Figure 2-56](#)). A normal restart will occur.

Figure 2-56. Home Page



2.8 Command Interface

Some functions on the device can be activated using simple POST commands to the web interface. The examples in [Table 2-27](#) use the free unix utility, **wget** commands. However, any program that can send HTTP POST commands to the device should work.

2.8.1 Command Interface Post Commands

The commands in [Table 2-27](#) require an authenticated session (a valid username and password to work).

Table 2-27. Command Interface Post Commands

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

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

Appendix A: Troubleshooting/Technical Support

A.1 Frequently Asked Questions (FAQ)

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

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

A.2 Documentation

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

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

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

A.3 Contact Information

Contact	<p>CyberData Corporation 3 Justin Court Monterey, CA 93940 USA 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>https://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>

A.4 Warranty and RMA Information

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

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

Index

Symbols

+48V DC power supply 10

A

activity light 12
 address, configuration login 19
 addressing
 DHCP 15, 36
 static 15, 36
 admin username and password 19
 audio configuration 77
 night ring tone parameter 81
 audio configuration page 77
 audio ground reference 8
 audio output 8
 audio parameters 77
 audiofiles 77
 authenticate ID and password for SIP server
 registration 41
 autoprovision at time (HHMMSS) 92
 autoprovision when idle (in minutes > 10) 92
 autoprovisioning 93
 download template button 93
 autoprovisioning autoupdate (in minutes) 92
 autoprovisioning configuration 91, 92
 autoprovisioning filename 92
 autoprovisioning server (IP Address) 92

B

backup SIP server 1 38
 backup SIP server 2 38
 backup SIP servers, SIP server
 backups 38

C

cat 5 ethernet cable 10
 changing
 the web access password 30
 changing default username and password for
 configuration GUI 19
 Cisco SRST 39
 command interface 107

commands 107
 configurable parameters 31, 35, 38
 configuration information 15
 configuration page
 configurable parameters 31, 35
 connecting the V3 paging server 7
 connector (removable) 9
 contact information 109
 contact information for CyberData 109
 current network settings 35
 current settings, reviewing 29
 CyberData contact information 109

D

default gateway 35
 default gateway for static addressing 36
 default login address 19
 default settings, restoring 14
 device configuration 30
 device configuration parameters 92
 the device configuration page 91
 device configuration page 30
 device configuration parameters 31
 device configuration password
 changing for web configuration access 30
 DHCP addressing 15, 36
 dimensions 3
 discovery utility program 19
 DNS server 35
 door sensor 81, 82
 download autoprovisioning template button 93

E

enable night ring events 87
 ethernet port 10
 event configuration
 enable night ring events 87
 expiration time for SIP server lease 38, 39, 40, 41
 export settings 24

F

fault detection parameters 69
 fault sense input, sensor 8

features 2
 firmware
 where to get the latest firmware 103

G

get autoprovisioning template 93
 green link light 12
 ground connection 7
 GUI username and password 19

H

hazard levels 5
 http POST command 107

I

identifying your product 1
 import settings 24
 import/export settings 24
 input specifications 3
 intercom configuration page
 configurable parameters 38
 IP address 35
 SIP server 40

L

lease, SIP server expiration time 38, 39, 40, 41
 line input specifications 3
 line output specifications 3
 line-in 7
 line-out 7
 link light 12
 local SIP port 39, 41
 log in address 19
 logging in to configuration GUI 19

M

MGROUP 45
 multicast
 play stored audio via multicast 70
 multicast address 70, 72, 75
 multicast port 31, 70
 multicast TTL 47, 50

N

navigation (web page) 16
 navigation table 16
 network activity, verifying 12
 network configuration page 34
 network parameters, configuring 34
 network setup button 34
 network, connecting to 11
 Nightringer 102
 nightringer settings 39
 NTP server 31

O

out of band 51
 output specifications 3

P

page port 8
 page port output connections 8
 paging server
 configuration 15
 part number 3
 parts list 5
 password
 configuration GUI 15, 19
 for SIP server login 38
 SIP server authentication 41
 payload types 3
 pgroups 45
 pin descriptions and functions 8
 point-to-point configuration 45
 port
 ethernet 10
 local SIP 39, 41
 remote SIP 39, 41
 POST command 107
 power
 connecting to 10
 product overview 1

R

reboot 105, 106
 unregistering from SIP server during 41
 registration and expiration, SIP server
 lease expiration 41
 relay 8

- relay contact 8
- remote SIP port 39, 41
- required configuration for web access username and password 15, 19
- restoring factory default settings 14
- RFC2833 RTP events 51
- rport discovery setting, disabling 39

S

- safety instructions 6
- sales 109
- scheduled events 58
- schedules parameters 58
- server address, SIP 38
- service 109
- SIP
 - enable SIP operation 38
 - local SIP port 39
 - user ID 38
- SIP configuration page 37
- SIP configuration parameters
 - outbound proxy 39
 - registration and expiration, SIP server lease 38, 39, 40
 - unregister on reboot 39
 - user ID, SIP 38
- SIP registration 38
- SIP remote SIP port 39
- SIP server 38
 - password for login 38
 - unregister from 39
 - user ID for login 38
- SIP server configuration 38
- SIP server parameters, configuring 15
- SIP setup button 37
- specifications 3
- SRST 39
- SSL parameters 52
- static addressing 15, 36
- status light 12
- subnet mask 35
- subnet mask static addressing 36
- supported protocols 3

T

- tech support 109
- technical support, contact information 109

U

- unregister from SIP server 41
- user ID
 - for SIP server login 38
- user ID for SIP server registration 41
- username
 - changing for web configuration access 30
- username for configuration GUI 15, 19

V

- verifying
 - network activity 12
- VLAN ID 35
- VLAN Priority 35
- VLAN tagging support 35
- VLAN tags 35
- volume 31

W

- warranty policy at CyberData 109
- web configuration log in address 19
- web page
 - navigation 16
- web page navigation 16
- wget, free unix utility 107