

Paging Amplifier Operations Guide

Part #011324, 011403, 011405, 011407

Document Part #932064A
for Firmware Version 22.0

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

Paging Amplifier Operations Guide 932064A
Part # 011324, 011403, 011405, 011407

COPYRIGHT NOTICE:

© 2024, 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



Fax: (831) 373-4193

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

Revision Information

Revision 932064A, which corresponds to firmware version 22.0, was released on November 19, 2024.

Pictorial Alert Icons

	<p>General Alert <i>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.</i></p>
	<p>Ground <i>This pictorial alert indicates the Earth grounding connection point.</i></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.

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

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

Chapter 1 Installing the Paging Amplifier	1
1.1 Connecting the Device	1
1.1.1 Using the Amplified Outputs	1
1.1.2 System Installation and Connection Options	4
1.1.3 Strobe Connections Behind the Port Cover	6
1.1.4 Connecting the 011288 Auxiliary RGB (Multi-Color) Strobe Kit	7
1.1.5 Ethernet Connection	9
1.1.6 Confirm Operation	10
Chapter 2 Configure the Device	11
2.2 Log In Page	11
2.2.1 Announcing the IP Address	12
2.2.2 Restoring Factory Defaults	12
2.3 Home Page	13
2.4 Device	15
2.5 Audio	16
2.6 Network	17
2.7 SIP (Session Initiation Protocol)	18
2.7.1 Dial Out Extension Strings and DTMF Tones (using rfc2833)	19
2.7.2 Point-to-Point Configuration	19
2.8 SSL	20
2.9 Multicast	23
2.10 Sensor	24
2.11 Audiofiles	25
2.12 Events	27
2.12.1 Example Packets for Events	28
2.13 Terminus	31
2.14 Autoprovisioning	32
2.15 Firmware	33
2.16 Admin	34
2.17 Command Interface	35
2.17.1 Command Interface Post Commands	35
Appendix A Troubleshooting/Technical Support	36
A.1 Contact Information	36
A.2 Warranty and RMA Information	36
Index	37

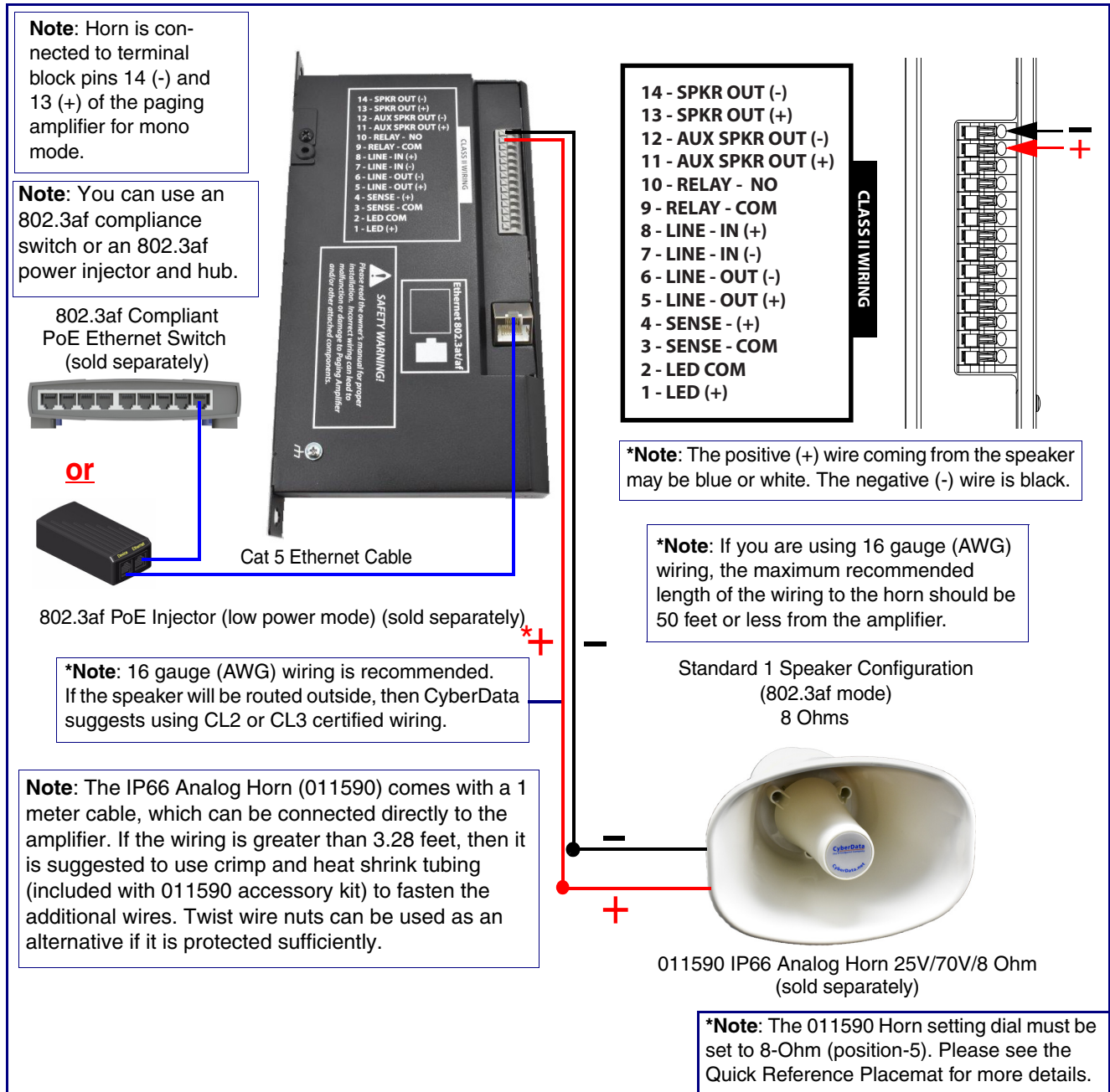
1 Installing the Paging Amplifier

1.1 Connecting the Device

1.1.1 Using the Amplified Outputs

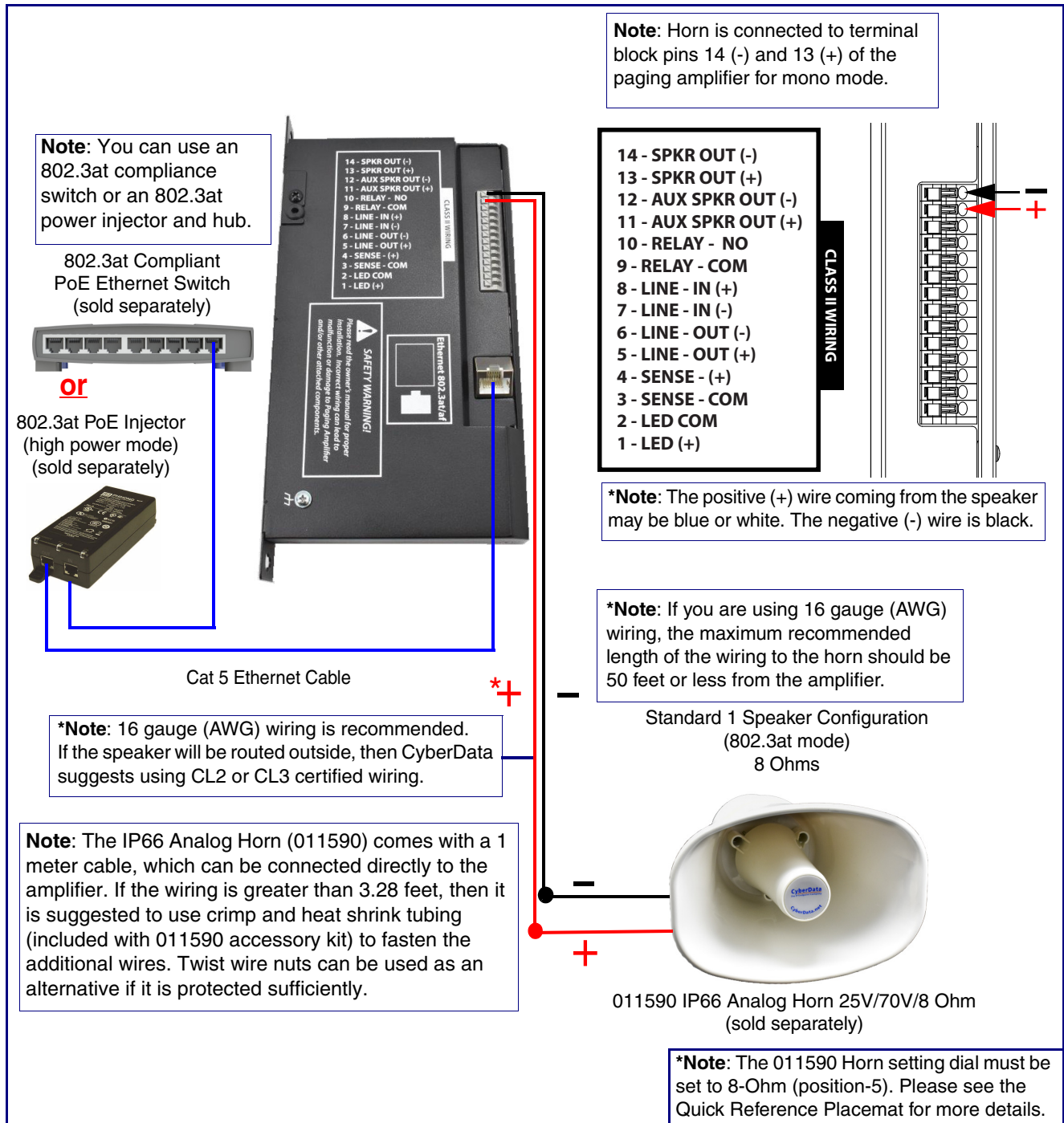
Low Power Mode (One Speaker) The following figure illustrates how to connect the Paging Amplifier and use the amplified outputs in low power mode to one speaker or horn.

Figure 1-1. Low Power Mode with One Speaker



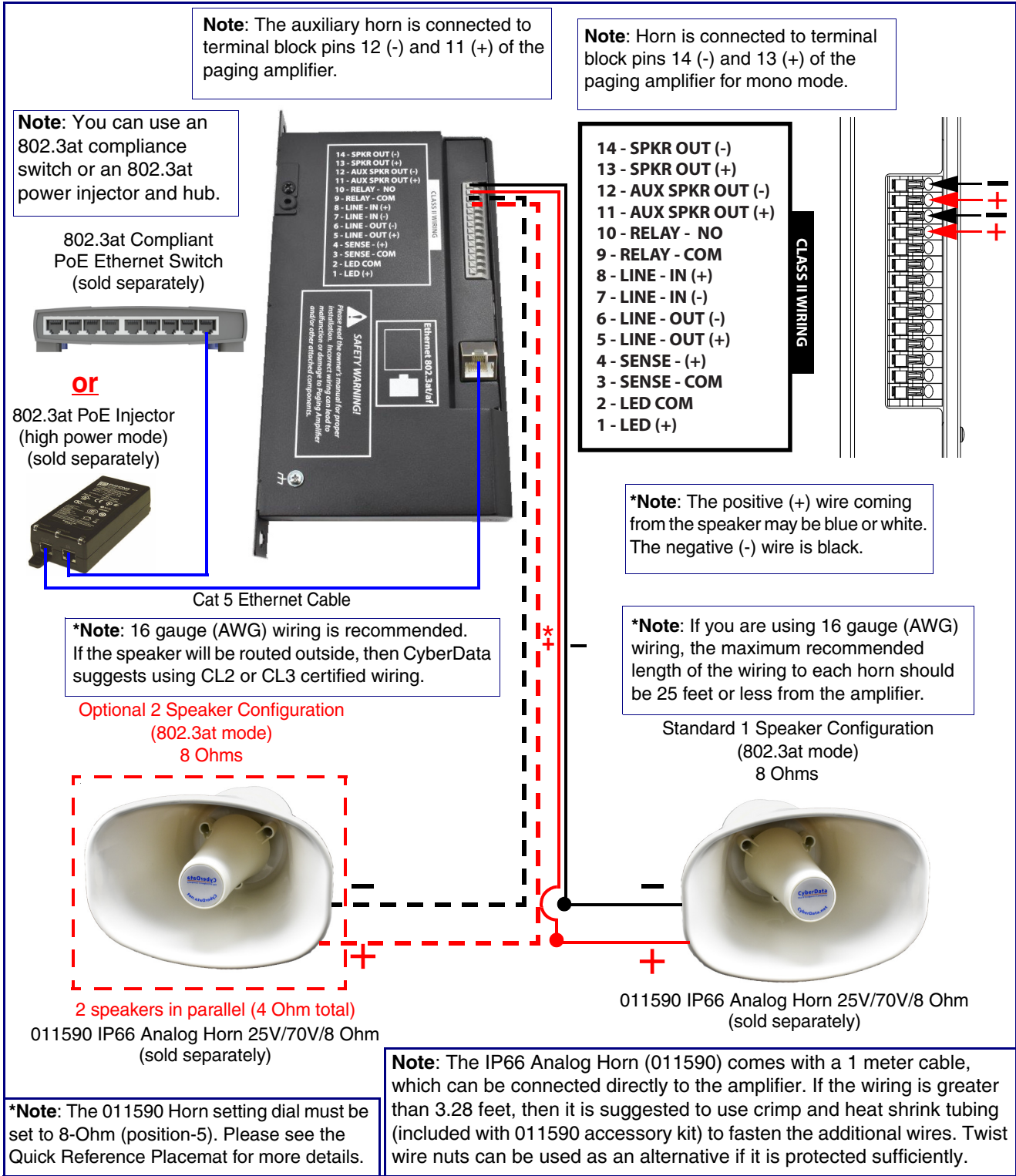
High Power Mode (One Speaker) The following figure illustrates how to connect the Paging Amplifier and use the amplified outputs in high power mode to one speaker or horn.

Figure 1-2. High Power Mode with One Speaker



High Power Mode (Two Speakers) The following figure illustrates how to connect the Paging Amplifier and use the amplified outputs in high power mode to two speakers or horns.

Figure 1-3. High Power Mode with Two Speakers



1.1.2 System Installation and Connection Options

The following figures show the connection options for the Paging Amplifier.

Figure 1-4. Paging Amplifier Connections

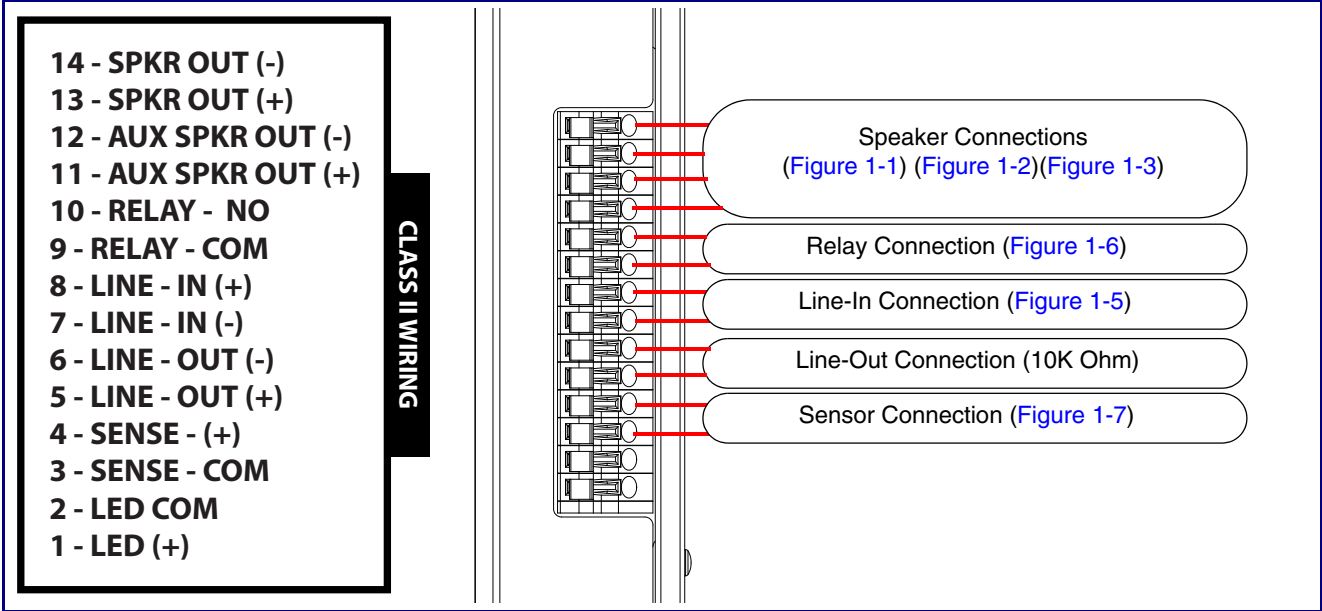


Figure 1-5. Line-In Connection

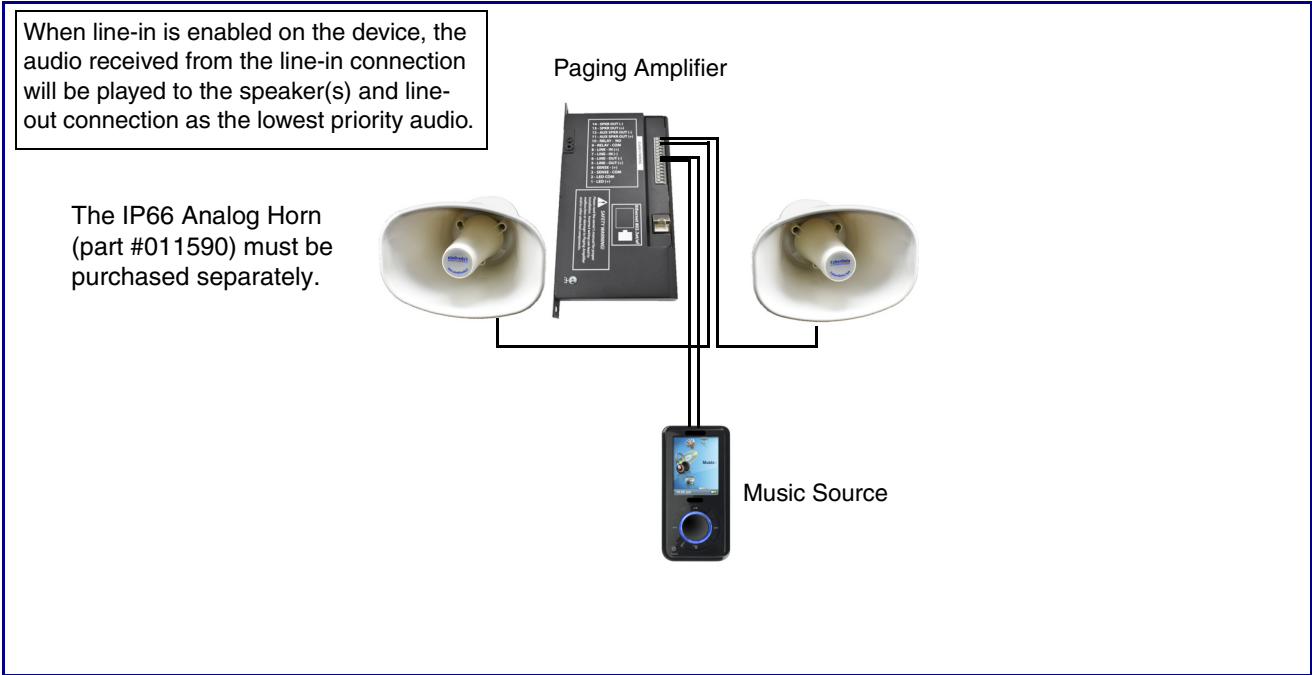


Figure 1-6. Relay or LED Strobe Connection

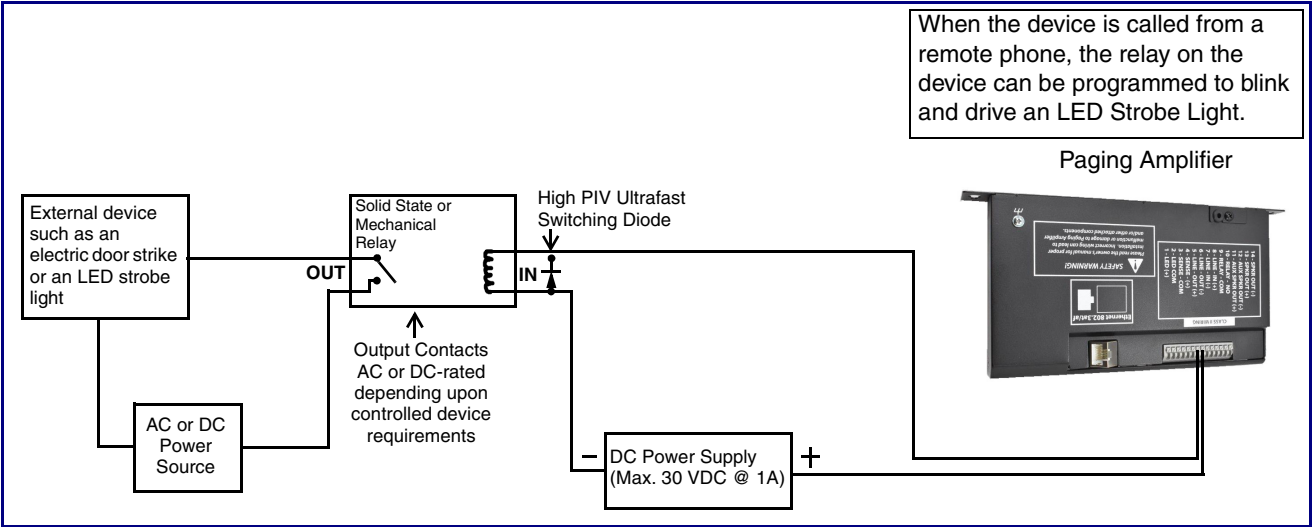
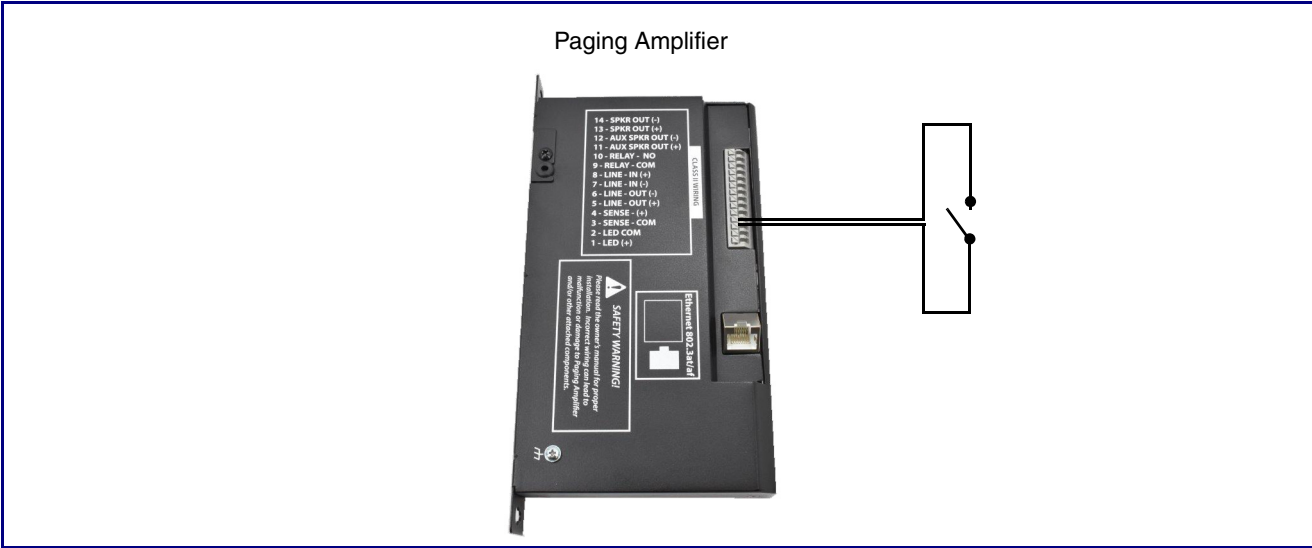


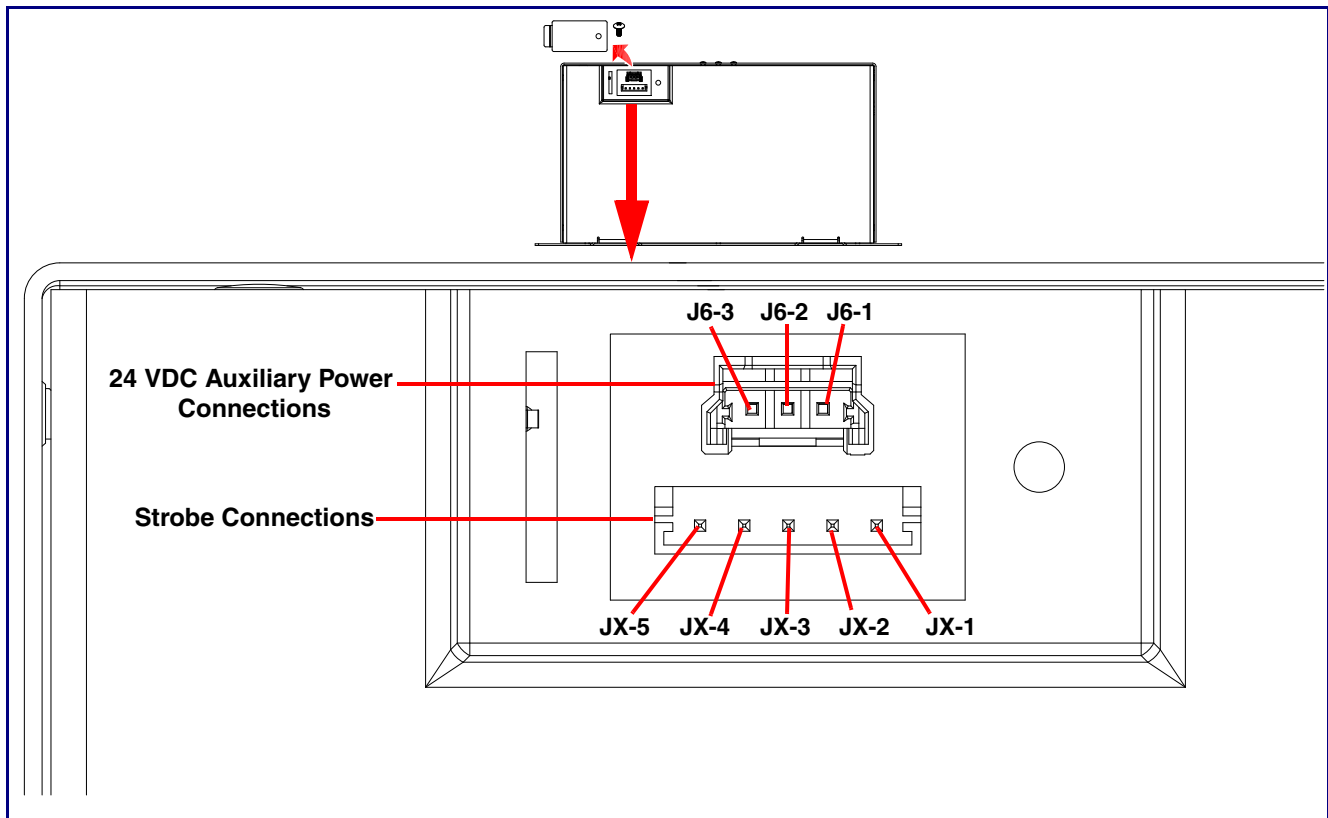
Figure 1-7. Sensor Connection



1.1.3 Strobe Connections Behind the Port Cover

See [Figure 1-8](#) for the additional connection options for the Paging Amplifier.

Figure 1-8. Connections Behind the Port Cover



See [Table 1-1](#) for the descriptions of the connections behind the port cover.

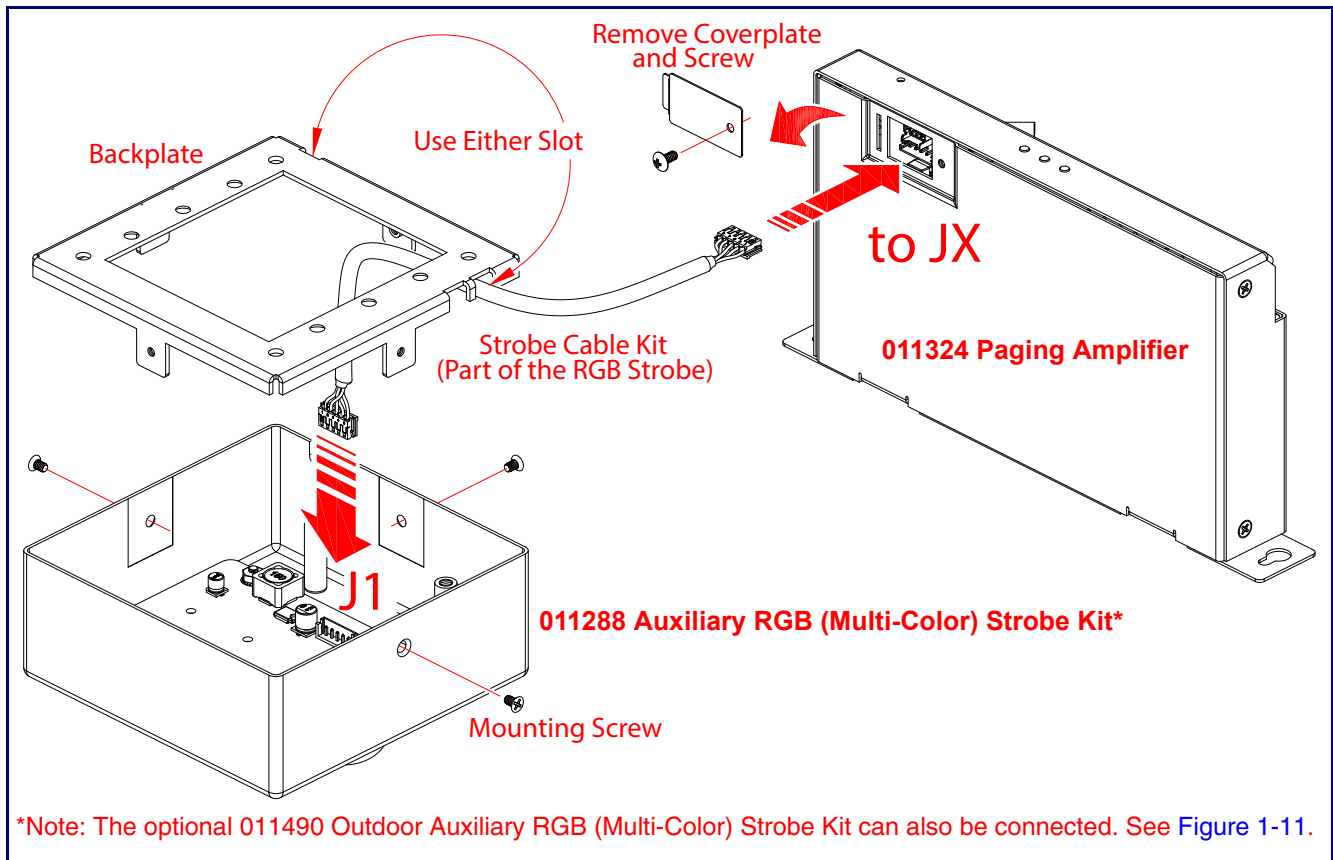
Table 1-1. Connections Behind the Port Cover

Connections Behind the Port Cover	
Connection	Description
J6-1	+24VDC
J6-2	Ground
J6-3	Chassis Ground
Strobe Connections	
Connection	Description
JX-1	Ground
JX-2	Strobe positive power (+24V)
JX-3	Ground
JX-4	I2C data
JX-5	I2C clock

1.1.4 Connecting the 011288 Auxiliary RGB (Multi-Color) Strobe Kit¹

1. Remove the mounting screw to remove the cover plate. See [Figure 1-9](#).
2. Remove the hole plug and grommet. See [Figure 1-9](#).
3. Slide the cover plate through the slot on the cable grommet. See [Figure 1-9](#).
4. Install the mounting screw to secure the cover plate. See [Figure 1-9](#).

Figure 1-9. Connecting the 011288 Auxiliary RGB (Multi-Color) Strobe Kit



1. The optional 011490 Outdoor Auxiliary RGB (Multi-Color) Strobe Kit can also be connected. See [Figure 1-11](#).

Figure 1-10. Connecting the 011288 Auxiliary RGB (Multi-Color) Strobe Kit

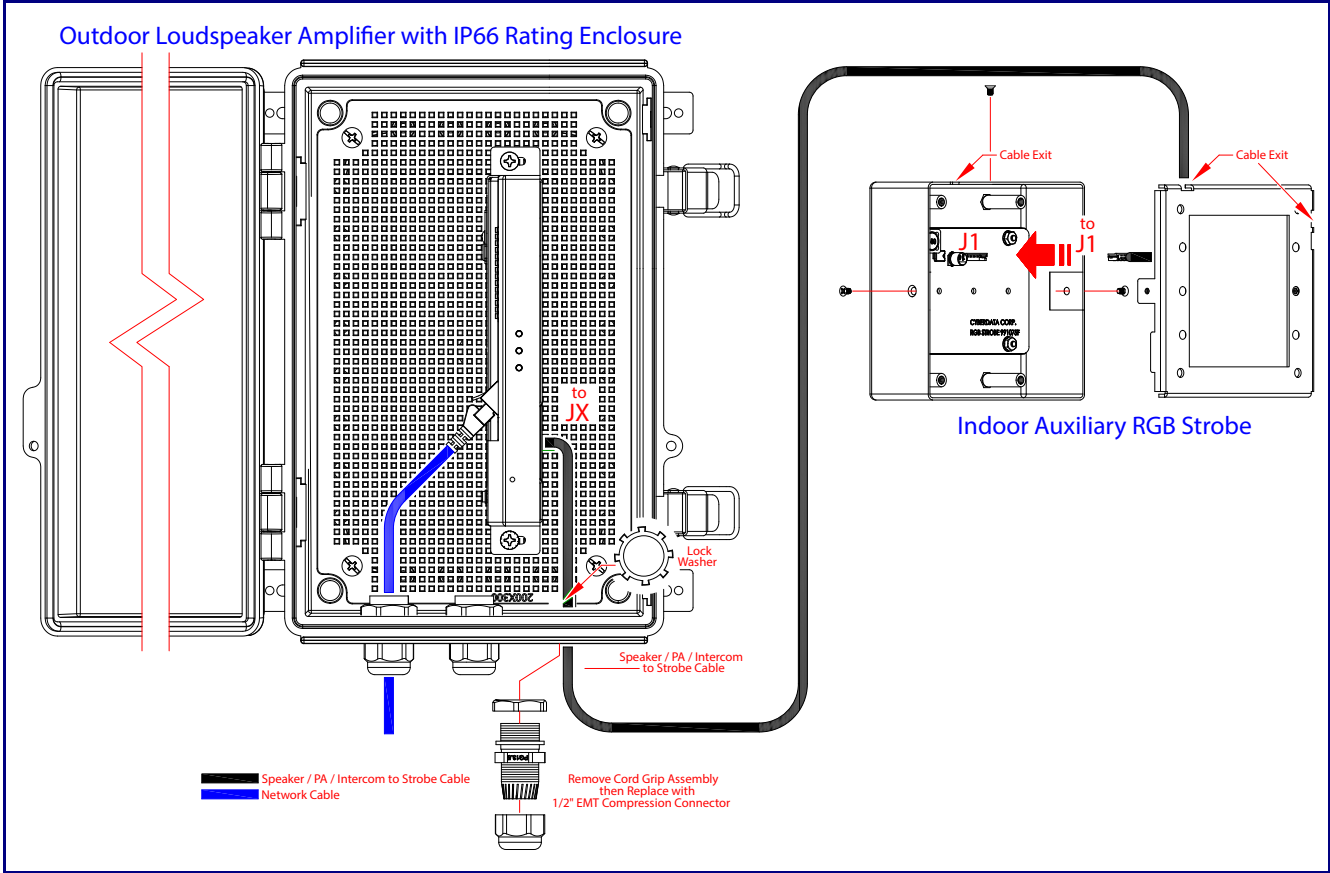
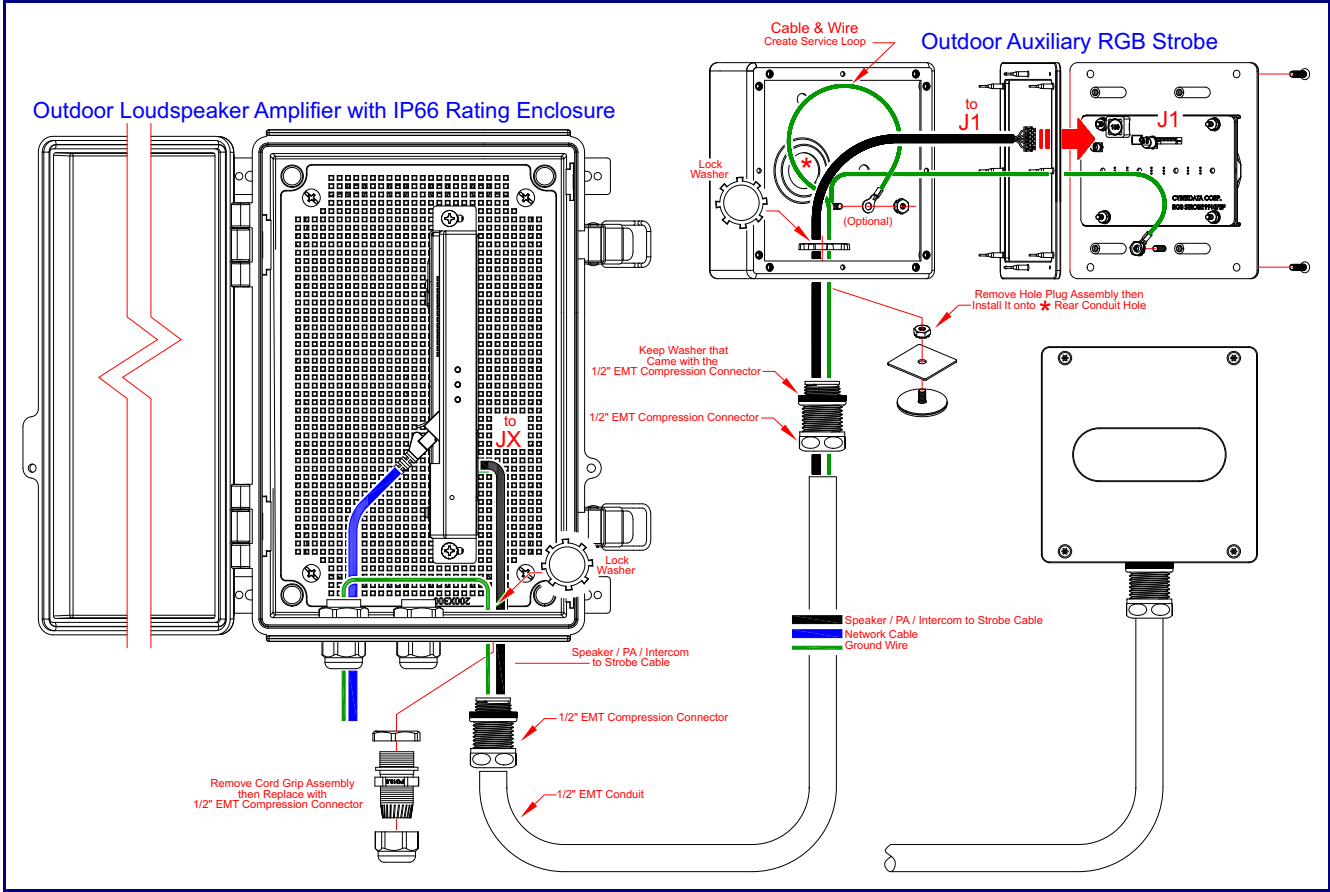


Figure 1-11. Connecting the 011490 Outdoor Auxiliary RGB (Multi-Color) Strobe Kit



1.1.5 Ethernet Connection

See [Table 1-2](#) for details about the Paging Amplifier connection.

Table 1-2. Paging Amplifier Connection

Connection	Connection Details	Location
Ethernet	Use a RJ 45 cable.	Paging Amplifier

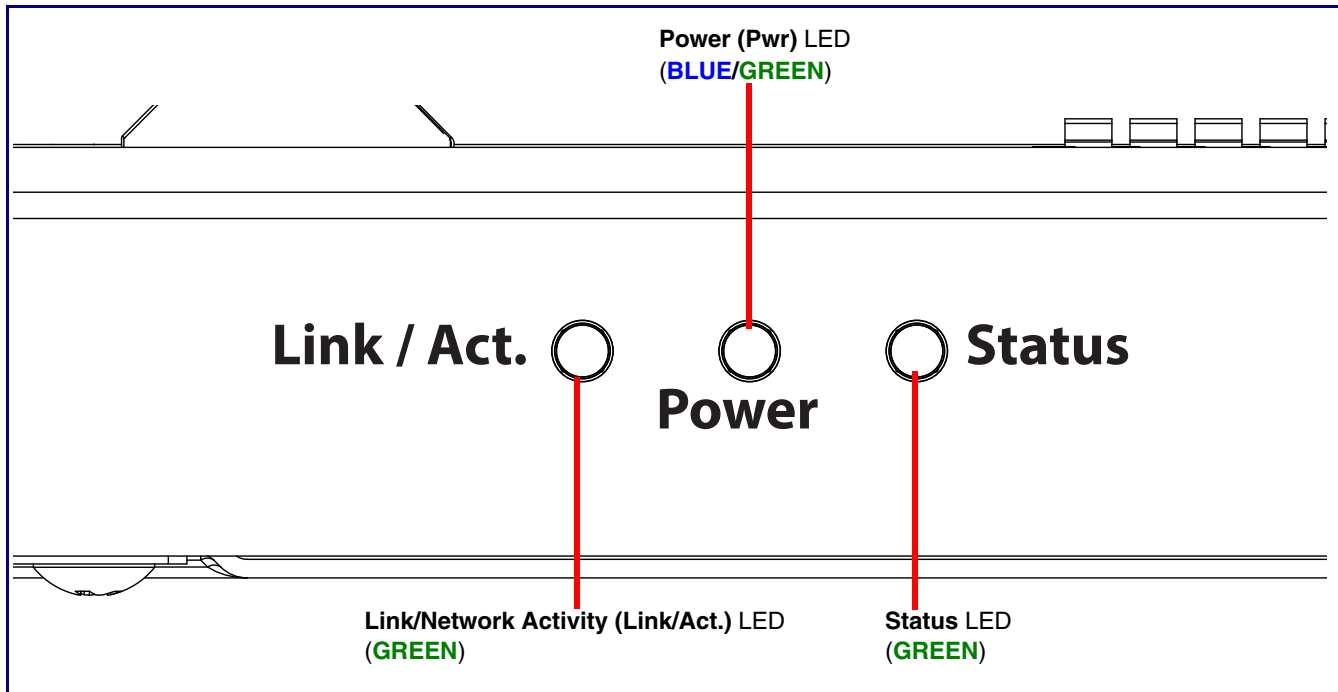
1.1.6 Confirm Operation

After connecting the Paging Amplifier to the 802.3af compliant ethernet hub, use the LEDs on the Paging Amplifier face to confirm that the Paging Amplifier is operational and linked to the network.

Table 1-3. Paging Amplifier LEDs

LED	Color	Function
Power (PWR)	BLUE/GREEN	The power LED is GREEN in low power mode (802.3af) and a BLUE during high power mode (802.3at). The power LED will blink during a boot up or a phone call.
Status	GREEN	After supplying power to the device, a steady GREEN Status LED illuminates. After about 20 seconds the GREEN Status LED will blink twice to indicate that the board is fully booted. The status LED will blink during a page when it is online.
Link/Network Activity (Link/Act.)	GREEN	The Link/Network Activity (Link/Act.) GREEN LED blinks to indicate network traffic.

Figure 1-12. Paging Amplifier LEDs



2 Configure the Device

2.2 Log In Page

1. Open your browser to the device 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 Paging Amplifier.

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

CyberData's VoIP Discovery Utility program is available at the following website address:

<https://www.cyberdata.net/pages/discovery>

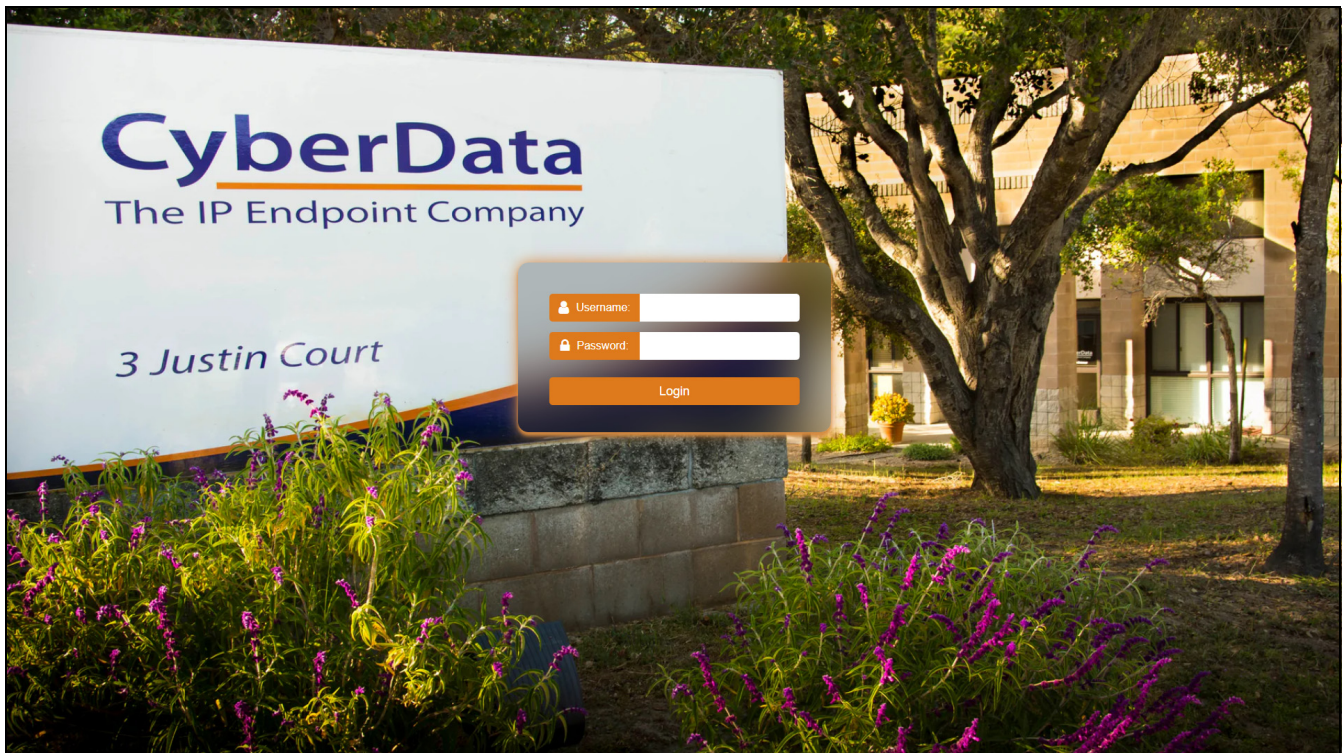
Note The Intercom ships in DHCP mode. To get to the **Home** page, use the discovery utility to scan for the device on the network and open your browser from there.

2. On the Log In Page (Figure 2-13), use the following default **Web Access Username** and **Web Access Password** to access the **Home Page** (Figure 2-2):

Web Access Username: **admin**

Web Access Password: **admin**

Figure 2-13. Log In Page

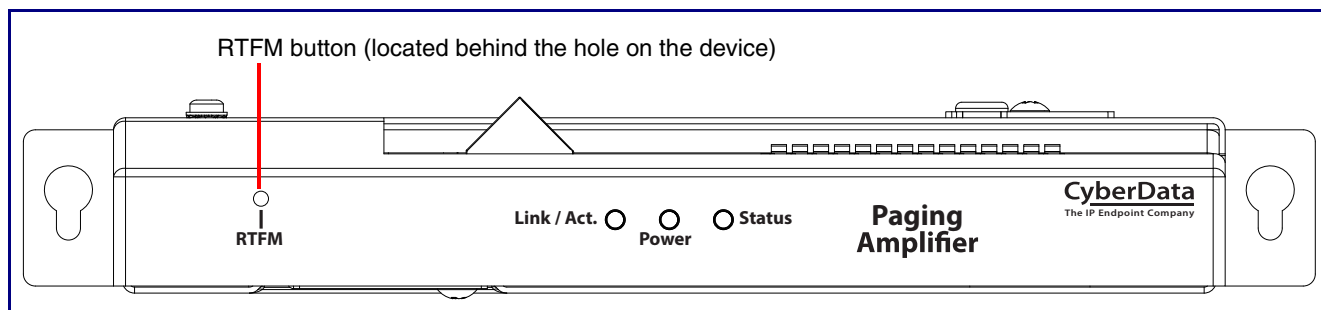


2.2.1 Announcing the IP Address

The RTFM button is located on the front of the each device (Figure 2-1). Use a paper clip to access the button through the hole.

Briefly pressing the RTFM button prompts the device to announce its IP address.

Figure 2-1. RTFM Button



2.2.2 Restoring Factory Defaults

To restore the device to its factory default settings (Table 3-1), hold the RTFM button for approximately seven seconds. After 15 to 20 seconds, "Restoring defaults, rebooting" is announced.

The device will default to DHCP to obtain an IP address, or will use 192.168.1.23 if a DHCP server is not present.

Table 2-1. 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.

2.3 Home Page

The **Home** page provides device specific information such as Serial Number, Mac Address, and Firmware version. This page is designed as an initial landing page to provide general information on the status of the device.

Figure 2-2. Home Page

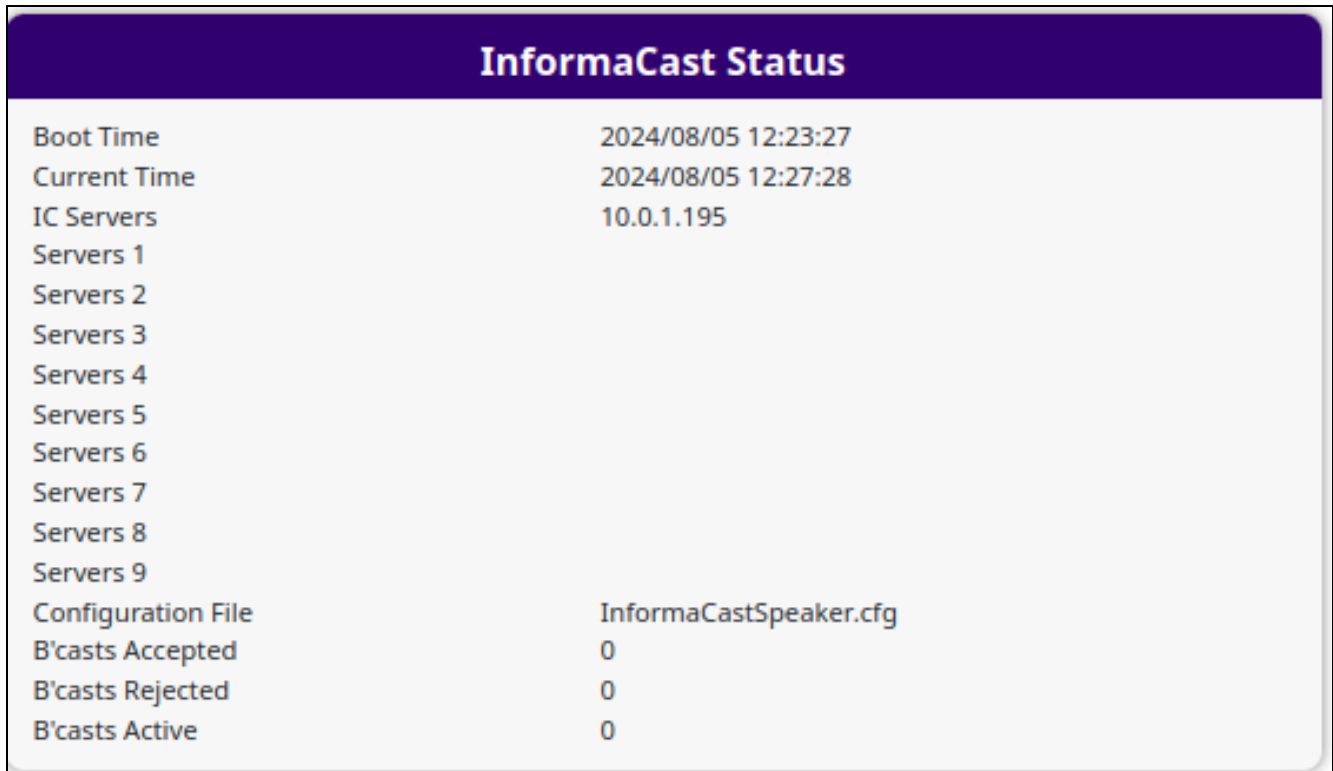
The screenshot displays the CyberData Home Page interface. At the top, the CyberData logo is on the left, and device information is on the right: Product: SIP Paging Amp, Serial: 324200221, Available Storage: 1381MB, Firmware: v22.0.0, MAC: 00:20:f7:05:6a:09, and Device Status: Idle. Action buttons (Test, Save, Cancel, Reboot, Logout) are located to the right of the status. A vertical sidebar on the left contains navigation icons. The main content area is divided into six panels:

- Device Configuration:**
 - Serial Number: 324200221
 - Mac Address: 00:20:f7:05:6a:09
 - Firmware Version: v22.0.0
 - Partition 2: v22.0.0
 - Partition 3: v22.0.0
 - Booting Partition: partition 3
- Network Status:**
 - IP Address Protocol: DHCP
 - IP Address: 10.10.1.103
 - Subnet Mask: 255.0.0.0
 - Default Gateway: 10.0.0.1
 - DNS Server 1: 10.0.1.56
 - DNS Server 2:
- SIP Registration:**
 - SIP Mode: **Enabled**
 - Primary Server: **Not registered**
 - Backup Server 1: **Not registered**
 - Backup Server 2: **Not registered**
 - Nightringer Server: **Not registered**
- Audio Configuration:**
 - SIP Volume: 4
 - Multicast Volume: 4
 - Ring Volume: 4
 - Sensor Volume: 4
 - Volume Boost: None
- Sensor Status:**
 - Relay Status: **Locked**
 - RGB Strobe: **Not Installed**
- System Configuration:**
 - SIP Mode: **Enabled**
 - Multicast Mode: **Disabled**
 - Event Mode: **Disabled**

The footer of the page contains the text "CyberData • Support".

If you are using an InformaCast enabled device, you will see the following:

Figure 2-3. InformaCast enabled Device



InformaCast Status	
Boot Time	2024/08/05 12:23:27
Current Time	2024/08/05 12:27:28
IC Servers	10.0.1.195
Servers 1	
Servers 2	
Servers 3	
Servers 4	
Servers 5	
Servers 6	
Servers 7	
Servers 8	
Servers 9	
Configuration File	InformaCastSpeaker.cfg
B'casts Accepted	0
B'casts Rejected	0
B'casts Active	0

2.4 Device

The **Device** page allows for adjustment of settings that pertain to the physical device such as relay settings and time zone.

Figure 2-4. Device Page

The screenshot displays the CyberData Device Page interface. At the top, the header includes the CyberData logo, product information (SIP Paging Amp, Firmware v22.0.0), serial and MAC addresses, available storage (1381MB), and device status (Idle). Action buttons for Test, Save, Cancel, Reboot, and Logout are visible. The main content area is divided into several settings panels:

- Relay Settings:** Control Relay with DTMF Code (OFF), DTMF Pulse Code (123), DTMF Pulse Code Duration (10 seconds), DTMF Activation Code (456), DTMF Deactivation Code (789), Relay During Ring (OFF), Relay During Night Ring (OFF), and Relay While Call Active (OFF).
- Time Settings:** NTP Server (north-america.pool.ntp.org), NTP Timezone (America/Los_Angeles (-8)), and Current Time (Mon, 11 Nov 2024 13:56:43).
- Power Settings:** 802.3AT Mode (Not detected. Disabled) and Force 802.3AT Mode (OFF).
- DTMF Settings:** Require Security Code (DISABLED) and Security Code (masked).
- Misc Settings:** Device Name (SIP Paging Amp), Beep on Init (OFF), and Two Speakers Connected (OFF).

A vertical sidebar on the left contains navigation icons. The footer shows 'CyberData • Support'.

If you are using an InformaCast enabled device, you will see the following:

Figure 2-5. InformaCast enabled Device

The screenshot shows the InformaCast Settings panel. It features a dark purple header with the text 'InformaCast Settings'. Below the header, the 'InformaCast Server:' label is followed by a text input field containing the URL 'http://10.0.1.195:8081/InformaCast/resources'.

2.5 Audio

Figure 2-6. Audio Page

The screenshot displays the configuration interface for a CyberData SIP Paging Amp. At the top, a purple header bar contains the following information: CyberData logo (The IP Endpoint Company), Product: SIP Paging Amp, Firmware: v22.0.0, Serial: 324200221, MAC: 00:20:f7:05:6a:09, Available Storage: 1381MB, and Device Status: Idle. To the right of this header are five buttons: Test (purple), Save (green), Cancel (yellow), Reboot (red), and Logout (blue). A vertical sidebar on the left contains various system icons. The main content area features a central 'Audio Settings' dialog box with the following configuration options:

Setting	Value
Line-in to Line-out Loopback:	OFF
SIP Volume:	4
Multicast Volume:	4
Ring Volume:	4
Sensor Volume:	4
Volume Boost:	None

At the bottom of the interface, a purple footer bar displays 'CyberData • Support'.

2.6 Network

The **Network** tab provides access to network-related settings. Assigning the device a static IP address or VLAN is done on this page.

Figure 2-7. Network Page

CyberData The IP Endpoint Company
Product: SIP Paging Amp **Firmware:** v22.0.0
Serial: 324200221 **MAC:** 00:20:f7:05:6a:09
Available Storage: 1381MB **Device Status:** Idle

Test **Save** **Cancel** **Reboot** **Logout**

Network Status	
IP Address Protocol	DHCP
IP Address	10.10.1.103
Subnet Mask	255.0.0.0
Default Gateway	10.0.0.1
DNS Server 1	10.0.1.56
DNS Server 2	

Network Settings	
Addressing Mode:	DHCP
Hostname:	SipDevice056a09
IP Address:	10.10.10.10
Subnet Mask:	255.0.0.0
Default Gateway:	10.0.0.1
DNS Server 1:	10.0.0.1
DNS Server 2:	10.0.0.1
DHCP Timeout:	60 seconds

VLAN Settings	
VLAN ID:	0
VLAN Priority:	0

CyberData • Support

2.7 SIP (Session Initiation Protocol)

This page sets the options for phone calls. Configure up to 3 servers, with 2 acting as backup, and a server for the nightringer. The nightringer is a second sip extension that only rings, never connects to a call. Many customers use the nightringer in a hunt group.

Use this page to configure the options for security, transport, codec, and others.

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

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

Figure 2-8. SIP Page

If you are using an InformaCast enabled device, you will see the following:

Figure 2-9. InformaCast enabled Device

InformaCast SIP Config:	DISABLED ▼
-------------------------	---

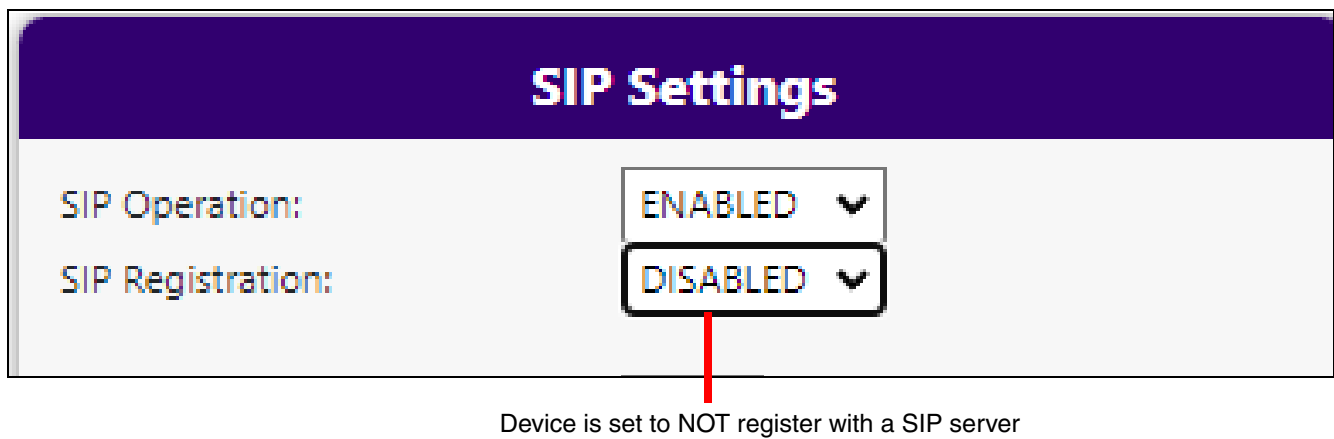
2.7.1 Dial Out Extension Strings and DTMF Tones (using rfc2833)

Outgoing calls support delayed DTMF (rfc2833) with the first comma pausing 2 seconds and subsequent commas pausing 1 second.

2.7.2 Point-to-Point Configuration

Dialing point-to-point allows the device to call and a single endpoint. All CyberData endpoints and many phones can use this option. To do this, enable **SIP Operation**, do not enable **SIP Registration**, and use the endpoint's IP address as the Dial Out extension. Delayed DTMF is supported. See [Figure 2-10](#).

Figure 2-10. SIP Page Set to Point-to-Point Mode



2.8 SSL

The **SSL** tab allows for the adjustment of certificates used by the device. The certificates used for the web server, SIP Client, and Autoprovisioning can be changed here. It is also possible to add additional CA certificates on this page. CA Certificates allow the device to authenticate servers that it contacts.

Figure 2-11. SSL Page (1 of 3)

The screenshot displays the CyberData SSL configuration interface. At the top, the header includes the CyberData logo, product information (SIP Paging Amp, Firmware: v22.0.0), device details (Serial: 324200221, MAC: 00:20:F7:05:6a:09), storage status (1381MB), and device status (Idle). Navigation buttons for Test, Save, Cancel, Reboot, and Logout are present.

The main content area is divided into three sections for certificate management:

- Web Server Certificate:** Shows certificate details (country: US, state: California, locality: Monterey, organization: Cyberdata, commonName: 0020f7056a09) and validity dates (notBefore: May 3 15:35:07 2024 GMT, notAfter: May 1 15:35:07 2034 GMT). It includes a 'Choose Files' button, 'Import Web Certificate', and 'Restore Web Certificate' buttons.
- SIP Client Certificate:** Shows identical certificate details and validity dates. It includes a 'Choose Files' button, 'Import SIP Certificate', and 'Restore SIP Certificate' buttons. A 'Password (optional):' field is also present.
- Autoprovisioning Client Certificate:** Shows identical certificate details and validity dates. It includes a 'Choose Files' button, 'Import Autoprovisioning Certificate', and 'Restore Autoprovisioning Certificate' buttons. A 'Password (optional):' field is also present.

Below these sections is the **List of Trusted CAs** section, which includes an 'Upload CA Certificate' button and a table of existing certificates:

CA Certificate Name	Info	Remove
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

Additional buttons for 'Download CyberData CA', 'Generate Cyberdata CSR', 'Remove All', and 'Restore Defaults' are located above the table. The footer of the page shows 'CyberData • Support'.

Figure 2-12. SSL Page (2 of 3)

The screenshot shows the CyberData SSL configuration page. At the top, there is a header bar with the following information: Product: SIP Paging Amp, Firmware: v22.0.0, Serial: 324200221, MAC: 00:20:f7:05:6a:09, Available Storage: 1381MB, and Device Status: Idle. On the right side of the header, there are buttons for Test, Save, Cancel, Reboot, and Logout. Below the header is a table listing 19 certificates, each with an 'Info' button and a 'Remove' button. The certificates are numbered 6 through 24.

Index	Certificate Name	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
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	Go_Daddy_Class_2_CA.pem	Info	Remove
17	Go_Daddy_Root_Certificate_Authority_-_G2.pem	Info	Remove
18	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G4.crt	Info	Remove
19	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5.crt	Info	Remove
20	VeriSign_Universal_Root_Certification_Authority.crt	Info	Remove
21	Verisign_Class_1_Public_Primary_Certification_Authority.crt	Info	Remove
22	Verisign_Class_1_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
23	Verisign_Class_2_Public_Primary_Certification_Authority_-_G2.crt	Info	Remove
24	Verisign_Class_2_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove

At the bottom of the page, there is a footer with the text "CyberData • Support".

Figure 2-13. SSL Page (3 of 3)

The screenshot shows the CyberData management interface for an SIP Paging Amp. The top header includes the CyberData logo, product name (SIP Paging Amp), firmware version (v22.0.0), serial number (324200221), MAC address (00:20:f7:05:6a:09), available storage (1381MB), and device status (Idle). Action buttons for Test, Save, Cancel, Reboot, and Logout are visible. The main content area is a table of installed certificates, each with an 'Info' button and a 'Remove' button.

ID	Certificate Name	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	Go_Daddy_Class_2_CA.pem	Info	Remove
17	Go_Daddy_Root_Certificate_Authority_-_G2.pem	Info	Remove
18	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G4.crt	Info	Remove
19	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5.crt	Info	Remove
20	VeriSign_Universal_Root_Certification_Authority.crt	Info	Remove
21	Verisign_Class_1_Public_Primary_Certification_Authority.crt	Info	Remove
22	Verisign_Class_1_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
23	Verisign_Class_2_Public_Primary_Certification_Authority_-_G2.crt	Info	Remove
24	Verisign_Class_2_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
25	Verisign_Class_3_Public_Primary_Certification_Authority.crt	Info	Remove
26	Verisign_Class_3_Public_Primary_Certification_Authority_-_G3.crt	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

2.9 Multicast

The Multicast page allows the device to join up to ten paging zones that will activate the strobe when a stream is sent to its address.

A paging zone can consist of one or many CyberData multicast group-enabled products. There is no limit to how many endpoints can be in a given paging zone. Each multicast group is defined by a multicast address and port number.

Each multicast group is assigned a priority, allowing simultaneously arriving pages to be serviced based on importance. Multicast groups are compatible with IGMP through version 3. The device supports simultaneous SIP and Multicast.

Figure 2-14. Multicast Page

CyberData The IP Endpoint Company
Product: SIP Paging Amp
Firmware: v22.0.0
Serial: 324200221
MAC: 00:20:f7:05:6a:09
Available Storage: 1381MB
Device Status: Idle
 Test Save Cancel Reboot Logout

Multicast Settings

Recieve Multicast Audio:

Polycm Default Channel:

Polycm Priority Channel:

Polycm Emergency Channel:

Priority	Address	Port	Name	Buffer	Beep	Relay
0	239.168.3.1	2000	Background Music	DISABLED	DISABLED	DISABLED
1	239.168.3.2	3000	MG1	DISABLED	DISABLED	DISABLED
2	239.168.3.3	4000	MG2	DISABLED	DISABLED	DISABLED
3	239.168.3.4	5000	MG3	DISABLED	DISABLED	DISABLED
4	239.168.3.5	6000	MG4	DISABLED	DISABLED	DISABLED
5	239.168.3.6	7000	MG5	DISABLED	DISABLED	DISABLED
6	239.168.3.7	8000	MG6	DISABLED	DISABLED	DISABLED
7	239.168.3.8	9000	MG7	DISABLED	DISABLED	DISABLED
8	239.168.3.9	10000	MG8	DISABLED	DISABLED	DISABLED
9	239.168.3.10	11000	Emergency	DISABLED	DISABLED	DISABLED

SIP calls: Priority 4.5
Port range: 2000-65535
Priority: 9 is the highest, 0 is the lowest
Audio Streams: Higher priority supersedes lower ones
Priority 9: Plays at maximum volume

CyberData • Support

2.10 Sensor

The door sensor (pins 5 and 6) on the header can be used to monitor a door's open or closed state. There is an option on the **Sensor** page to trigger on an open or short condition on these pins. The door sensor alarm will be activated when the **Door Open Timeout** parameter has been met.

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

Each sensor can trigger up to four different actions:

- Flash the LED until the sensor is deactivated (roughly 10 times/second)
- Activate the relay until the sensor is deactivated
- Loop an audio file out of the Intercom speaker until the sensor is deactivated
- Call an extension and play a pre-recorded audio file

Note Calling a preset extension can be set up as a point-to-point call, but currently can't send delayed DTMF tones.

Figure 2-15. Sensor Page

The screenshot displays the CyberData web interface for a SIP Paging Amp. The top navigation bar includes the CyberData logo, product information (SIP Paging Amp, Firmware: v22.0.0), serial number (324200221), MAC address (00:20:f7:05:6a:09), available storage (1381 MB), and device status (Idle). Action buttons for Test, Save, Cancel, Reboot, and Logout are visible. The main content area features a 'Door Sensor Settings' dialog box with the following fields:

Setting	Value
Sensor Type:	Normally Open
Open Timeout:	5 seconds
Activate Relay:	Disabled
Play Audio Locally:	Disabled
Call Extension:	Disabled
Dial Out Extension:	204
Dial Out ID:	id204
Repeat Sensor Message:	5

The bottom of the interface shows the CyberData logo and a link to Support.

2.11 Audiofiles

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.

This device supports stored messages. When stored messages are enabled, the user will hear "Press 0 to page, press 1 to 9 to play stored message" when calling the device. To configure stored messages, an audio file must be uploaded, using **Choose File** and **Save**. The number of repeats can be specified or set to infinite (where the message plays until cancelled by the # button during a phone call).

Figure 2-16. Audiofiles Page (1 of 2)

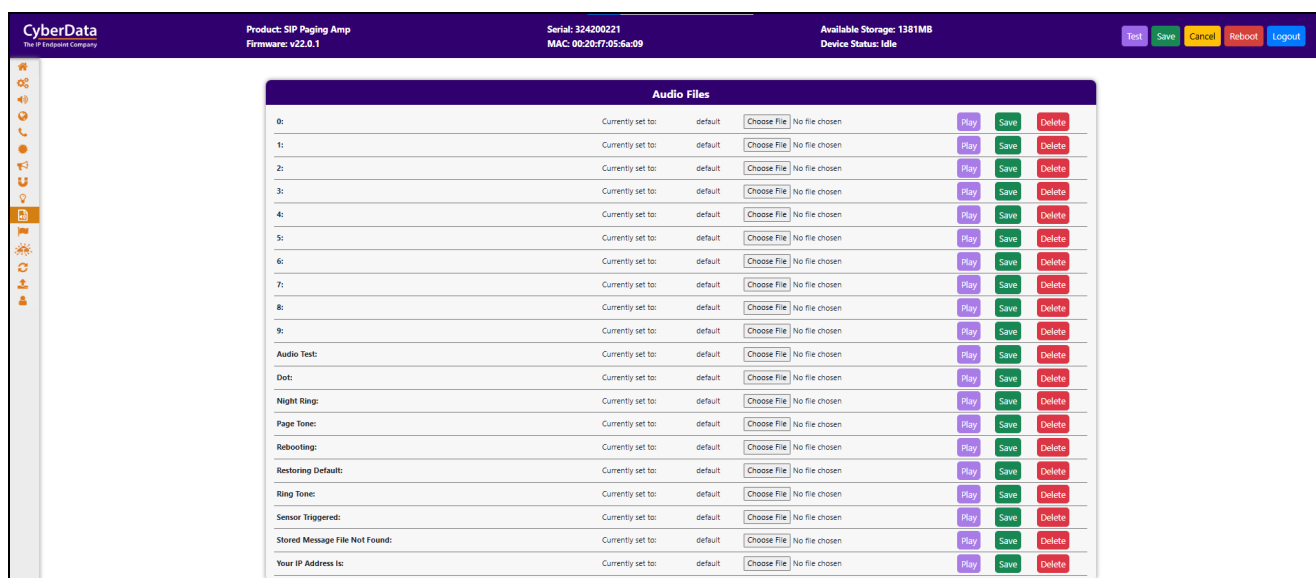


Figure 2-17. Audiofiles Page (2 of 3)

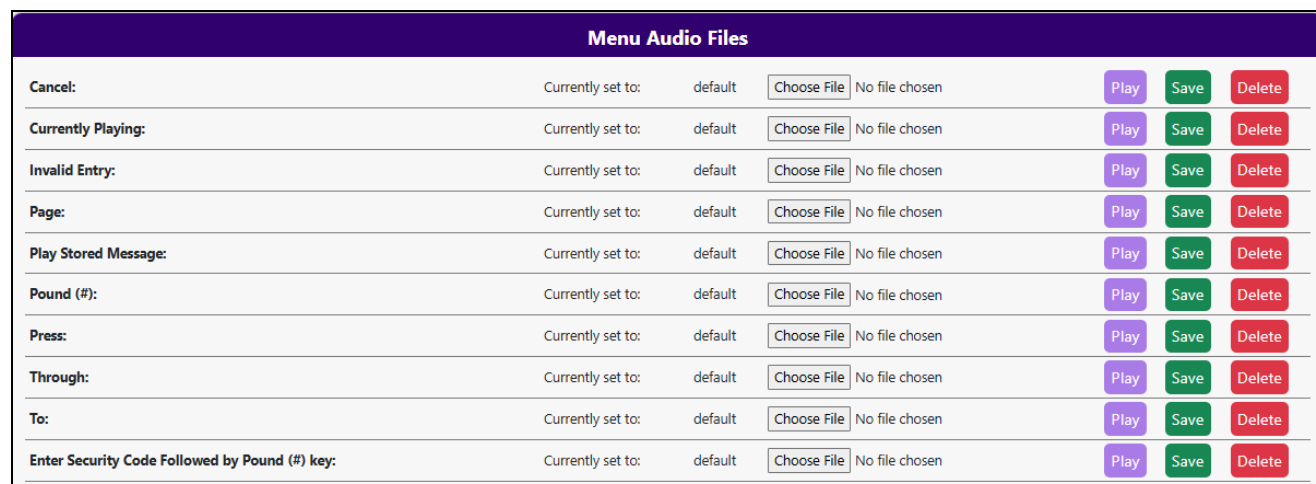


Figure 2-18. Audiofiles Page (3 of 3)

Stored Messages										
		<input type="button" value="Choose File"/> No file chosen			<input type="button" value="Upload Message"/>	<input type="button" value="Delete All Messages"/>				
Stored Message 1:	Currently set to:	default	<input type="button" value="Choose File"/> No file chosen	Repeat:	<input type="text" value="0"/>	Infinite:	OFF	<input type="button" value="Play"/>	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
Stored Message 2:	Currently set to:	default	<input type="button" value="Choose File"/> No file chosen	Repeat:	<input type="text" value="0"/>	Infinite:	OFF	<input type="button" value="Play"/>	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
Stored Message 3:	Currently set to:	default	<input type="button" value="Choose File"/> No file chosen	Repeat:	<input type="text" value="0"/>	Infinite:	OFF	<input type="button" value="Play"/>	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
Stored Message 4:	Currently set to:	default	<input type="button" value="Choose File"/> No file chosen	Repeat:	<input type="text" value="0"/>	Infinite:	OFF	<input type="button" value="Play"/>	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
Stored Message 5:	Currently set to:	default	<input type="button" value="Choose File"/> No file chosen	Repeat:	<input type="text" value="0"/>	Infinite:	OFF	<input type="button" value="Play"/>	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
Stored Message 6:	Currently set to:	default	<input type="button" value="Choose File"/> No file chosen	Repeat:	<input type="text" value="0"/>	Infinite:	OFF	<input type="button" value="Play"/>	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
Stored Message 7:	Currently set to:	default	<input type="button" value="Choose File"/> No file chosen	Repeat:	<input type="text" value="0"/>	Infinite:	OFF	<input type="button" value="Play"/>	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
Stored Message 8:	Currently set to:	default	<input type="button" value="Choose File"/> No file chosen	Repeat:	<input type="text" value="0"/>	Infinite:	OFF	<input type="button" value="Play"/>	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
Stored Message 9:	Currently set to:	default	<input type="button" value="Choose File"/> No file chosen	Repeat:	<input type="text" value="0"/>	Infinite:	OFF	<input type="button" value="Play"/>	<input type="button" value="Save"/>	<input type="button" value="Delete"/>

2.12 Events

The **Events** page specifies a remote server that can be used to receive HTTP POST events when actions take place on the device.

Figure 2-19. Events Page

If you are using an InformaCast enabled device, you will see the following:

Figure 2-20. InformaCast enabled Device

2.12.1 Example Packets for Events

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

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

Here are example packets for every event:

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

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

2.13 Terminus

Terminus Cloud Control™ allows users to configure, monitor, and manage notification functions for CyberData's extensive VoIP product line, all from a single, easy-to-use platform. To learn more about Terminus Cloud Control™, go to <https://www.cyberdata.net/pages/terminus>.

The **Terminus** page allows for configuration of settings related to Terminus Cloud Control™.

Figure 2-21. Terminus Page

The screenshot displays the Terminus configuration page within the CyberData management interface. The header bar is purple and contains the following information:

- CyberData** The IP Endpoint Company
- Product:** SIP Paging Amp
- Serial:** 324200221
- Available Storage:** 1381MB
- Firmware:** v22.0.0
- MAC:** 00:20:f7:05:6a:09
- Device Status:** Idle

Navigation buttons (Test, Save, Cancel, Reboot, Logout) are located in the top right corner. The main content area features two configuration sections:

Discovery Setting

- Multicast Address:
- Time to Live:
- Discovery Interval: seconds

Lockdown Settings

- Lock Down Mode:
- Relay:

The footer of the page contains the text "CyberData • Support".

2.14 Autoprovisioning

Enabling autoprovisioning allows the device to download provisioning files from a server. It defaults to using DHCP, with options configured in dhcpd.conf on the DHCP server. The file name is <mac address>.xml and if not found, 000000cd.xml.

If a server is named, DHCP is bypassed, and the device will look for a file on the named server.

If a file is named, it will be downloaded instead of <mac address>.xml.

If a server is named, **Use tftp** searches for the file on a tftp server instead of http. If the server is secured (with a password), use **Verify Server Certificate** (username/password) to access it. When using DHCP, these options are configured in dhcpd.conf.

Autoprov autoupdate, **Autoprov at time**, and **Autoprov when idle** options are available with either DHCP or a named server.

The template is an xml file with all options set to default values.

Figure 2-22. Autoprovisioning Page

The screenshot displays the Autoprovisioning configuration interface. At the top, the header includes the CyberData logo, product information (SIP Paging Amp, v22.0.0), device serial (324200221), MAC address (00:20:f7:05:6a:09), available storage (1381MB), and device status (Idle). Action buttons for Test, Save, Cancel, Reboot, and Logout are also visible.

The main content area is divided into two panels:

- Autoprov Settings:** Contains various configuration options:
 - Autoprov: ENABLED (dropdown)
 - Autoprov Server: Autoprov Server (text input)
 - Autoprov Filename: Autoprov Filename (text input)
 - Use tftp: DISABLED (dropdown)
 - Verify Server Certificate: DISABLED (dropdown)
 - Username: Username (text input)
 - Password: Password (text input)
 - Autoprov autoupdate: 0 minutes (spinners)
 - Autoprov at time: HHMM (text input)
 - Autoprov when idle: 0 minutes (spinners)
- Autoprov Log:** A scrollable log window showing the following entries:
 - 2024-11-11 14:11:22 Autoprov: no autoprov triggers. Exiting...
 - 2024-11-11 14:11:24 Autoprov found server= 'http://10.0.0.242' in dhcp option 43
 - 2024-11-11 14:11:24 Autoprov looking for 0020f7056a09.xml at http://10.0.0.242
 - 2024-11-11 14:11:24 Autoprov downloading http://10.0.0.242/0020f7056a09.xml
 - 2024-11-11 14:11:24 Got autoprov file. Parsing "0020f7056a09.xml"
 - 2024-11-11 14:11:25 Autoprov: SSLCertificates config not found
 - 2024-11-11 14:11:25 Autoprov: AudioFiles config not found
 - 2024-11-11 14:11:25 Autoprov: FirmwareSettings config not found
 - 2024-11-11 14:11:25 DeviceConfig: error = False
 - 2024-11-11 14:11:25 SSLCertificates: error = None
 - 2024-11-11 14:11:25 AudioFiles: error = None
 - 2024-11-11 14:11:25 BellSchedule: error = False
 - 2024-11-11 14:11:25 FirmwareSettings: error = None
 - 2024-11-11 14:11:25 StoredCalendars: error = None

A 'Download Template' button is located at the bottom of the settings panel. The footer of the page contains 'CyberData • Support'.

2.15 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 from the following CyberData web site, and locate your device:

<https://www.cyberdata.net/collections/sip>

<https://www.cyberdata.net/collections/singlewire> (for InformaCast Enabled devices)

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

- Firmware file
- Release notes
- Autoprovisioning template


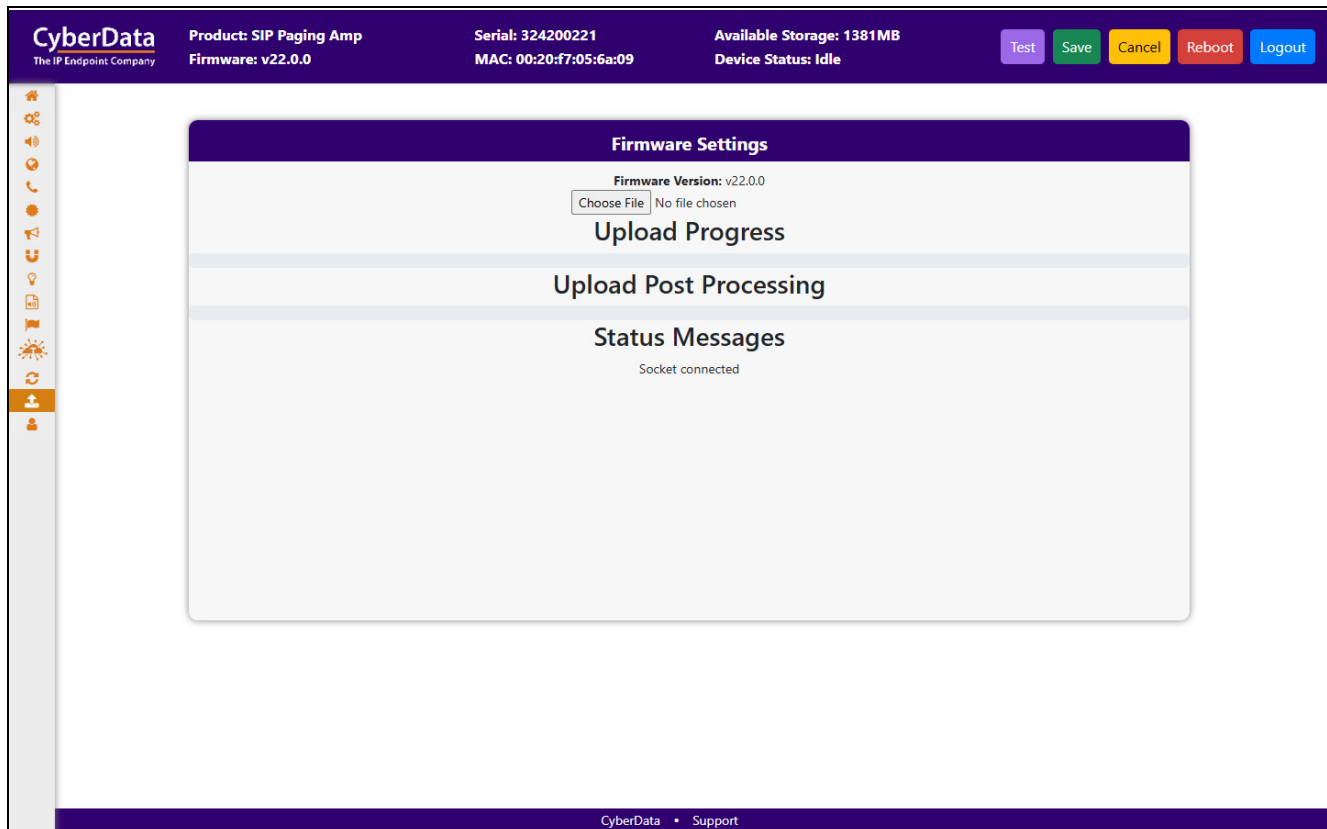
 <small>GENERAL ALERT</small>	<p>Caution</p> <p>Equipment Hazard: Do not reboot the device. It will reboot automatically when the process is complete.</p>
---	--

Figure 2-23. Firmware Page



2.16 Admin

The administrator uses the Users List to create new accounts, assigning user names and passwords, and granting access to specific web pages.

Figure 2-24. Admin Page

The screenshot displays the CyberData Admin interface. At the top, a purple header bar contains the CyberData logo and system information: Product: SIP Paging Amp, Firmware: v22.0.0, Serial: 324200221, MAC: 00:20:f7:05:6a:09, Available Storage: 1381MB, and Device Status: Idle. Action buttons for Test, Save, Cancel, Reboot, and Logout are on the right.

The main content area is divided into several sections:

- Admin Settings:** Includes fields for Username (admin), Password, and Confirm Password.
- Statistics:** Shows Storage (1381MB), Boot Count (21), Reboot Count (15), and Uptime (up 9 minutes).
- Logging Settings:** Features Debug Level (4) and Log Network Traffic (OFF). Buttons include Get Application Log, Remove Application Log, Get Network Log, Remove Network Log, Get All Logs, and Remove All Logs. A note states: "Retrieving the log files may take some time due to their size."
- Configuration Settings:** Lists Partition 2 and 3 (v22.0.0) and Booting Partition (partition 3). Buttons include Restore Default Config, Restore Default Certificates, Import Config, Export Config, and Boot From Other Partition.
- Users List:** Contains buttons for Add New User, Delete All Users, Import Users, and Export Users. Below is a table with columns: Username, Home, Device, Audio, Network, SIP, SSL, Multicast, Sensor, Strobe, Audiofiles, Events, Terminus, Autoprov, Firmware, and Admin.
- Log Viewer:** Includes a Service dropdown (Application), Entries to get (250), and Sort dropdown (Oldest). A View Log button is present.

The footer of the page shows "CyberData • Support".

2.17 Command Interface

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

2.17.1 Command Interface Post Commands

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

Table 2-2. Command Interface Post Commands

Device Action	HTTP Post Command ^a
Reboot	<code>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"</code>
Place call to extension (example: extension 600)	<code>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"</code>
Terminate a calli	<code>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"</code>
Speak IP Address	<code>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"</code>
Test Audio	<code>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"</code>
Swap Boot partitions	<code>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"</code>

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

Appendix A: Troubleshooting/Technical Support

A.1 Contact Information

Contact CyberData Corporation
3 Justin Court
Monterey, CA 93940 USA
www.cyberdata.net
Phone: 831-373-2601
Fax: 831-373-4193

Sales Sales 831-373-2601, Extension 334

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

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

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

Phone: (831) 373-2601, Extension 333

A.2 Warranty and RMA Information

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

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

Index

Numerics

802.3af mode 1, 2, 3
 802.3at compliance switch 1, 2, 3
 802.3at power injector (high power mode) 1, 2, 3

A

Admin 34
 Amplified Outputs 1
 Audio 16
 Audiofiles 25
 Autoprovisioning 32

C

Command Interface 35
 Command Interface Post Commands 35
 Connection Options 4
 Contact Information 36

D

Device 15
 Dial Out Extension Strings and DTMF Tones 19
 Discovery Utility program 11

E

Events 27

F

Firmware 33

H

High Power Mode with One Speaker 2
 High Power Mode with Two Speakers 3
 Home Page 13

L

LEDs 10
 Line-In Connection 4
 Low Power Mode with One Speaker 1

M

Multicast 23

N

Network 17

P

Point-to-Point Configuration 19

R

Relay or LED Strobe Connection 5

S

Sensor 24
 Sensor Connection 5
 SIP (Session Initiation Protocol) 18
 Speaker Connections 1
 SSL 20
 Strobe Connections Behind the Port Cover 6

T

Terminus 31
 Troubleshooting/Technical Support 36

W

Warranty and RMA Information 36