



# *CyberData Paging Adapters Operations Guide*

*SIP Compliant*  
Part #011233, 011280

Document Part #932061B  
for Firmware Version 22.0

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

---

**Operations Guide 932061B**  
**SIP Compliant 011233, 011280**

**COPYRIGHT NOTICE:**

© 2025, 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](http://www.cyberdata.net).

---


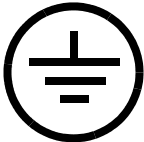
# Revision Information

Revision 932061B, which corresponds to firmware version 22.0, was released on July 10, 2025, and has the following changes:

- Updates [Figure 2-10, "Device Configuration Page"](#)

---

## Pictorial Alert Icons

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

---

## Hazard Levels

**Danger:** Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury. This is limited to the most extreme situations.

**Warning:** Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.

**Caution:** Indicates a potentially hazardous situation which, if not avoided, could result in minor or moderate injury. It may also alert users against unsafe practices.

**Notice:** Indicates a statement of company policy (that is, a safety policy or protection of property).

The safety guidelines for the equipment in this manual do not purport to address all the safety issues of the equipment. It is the responsibility of the user to establish appropriate safety, ergonomic, and health practices and determine the applicability of regulatory limitations prior to use. Potential safety hazards are identified in this manual through the use of words Danger, Warning, and Caution, the specific hazard type, and pictorial alert icons.

---

# Important Safety Instructions

1. Read these instructions.
2. Keep these instructions.
3. Heed all warnings.
4. Follow all instructions.
5. Do not use this apparatus near water.
6. Clean only with dry cloth.
7. Do not block any ventilation openings. Install in accordance with the manufacturer's instructions.
8. Do not install near any heat sources such as radiators, heat registers, stoves, or other apparatus (including amplifiers) that produce heat.
9. Do not defeat the safety purpose of the polarized or grounding-type plug. A polarized plug has two blades with one wider than the other. A grounding type plug has two blades and a third grounding prong. The wide blade or the third prong are provided for your safety. If the provided plug does not fit into your outlet, consult an electrician for replacement of the obsolete outlet.
10. Protect the power cord from being walked on or pinched particularly at plugs, convenience receptacles, and the point where they exit from the apparatus.
11. Only use attachments/accessories specified by the manufacturer.
12. Refer all servicing to qualified service personnel. Servicing is required when the apparatus has been damaged in any way, such as power-supply cord or plug is damaged, liquid has been spilled or objects have fallen into the apparatus, the apparatus has been exposed to rain or moisture, does not operate normally, or has been dropped.
13. Prior to installation, consult local building and electrical code requirements.



## Warning

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



## Warning

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



## Warning

The PoE connector is intended for intra-building connections only and does not route to the outside plant.

---

## Abbreviations and Terms

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

# Contents

---

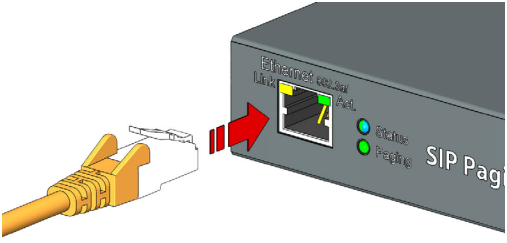
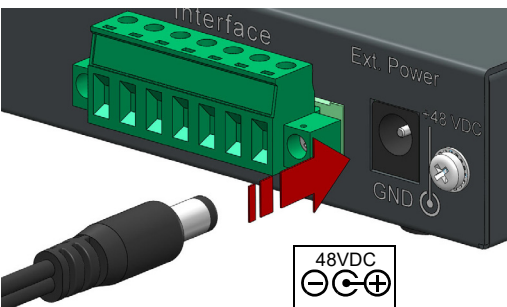

<b>Chapter 1 Setting Up the Paging Adapter</b>	<b>1</b>
1.1 Connect to the Power Source .....	1
Non-Poe .....	1
Chassis Ground .....	1
Poe .....	1
1.2 Connect to the Network .....	2
1.3 Confirm that the Paging Adapter is Up and Running .....	3
Verify Network Activity .....	3
1.4 Announcing the IP Address .....	4
1.5 Restore the Factory Default Settings .....	5
 <b>Chapter 2 Configure the Device</b>	 <b>6</b>
2.6 Log In Page .....	6
2.6.1 Restoring Defaults and Announcing the IP Address .....	7
2.7 Home Page .....	8
2.8 Device .....	10
2.9 Network .....	11
2.10 SIP (Session Initiation Protocol) .....	12
2.10.1 Dial Out Extension Strings and DTMF Tones (using rfc2833) .....	13
2.10.2 Point-to-Point Configuration .....	13
2.11 SSL .....	14
2.12 Multicast .....	16
2.13 Fault .....	17
2.14 Audiofiles .....	18
2.15 Events .....	20
Example Packets for Events .....	21
2.16 Terminus .....	24
2.17 Autoprovisioning .....	25
2.18 Firmware .....	26
2.19 Admin .....	27
2.20 Command Interface .....	28
2.20.1 Command Interface Post Commands .....	28
 <b>Appendix A Troubleshooting/Technical Support</b>	 <b>29</b>
A.1 Contact Information .....	29
A.2 Warranty and RMA Information .....	29

# 1 Setting Up the Paging Adapter

## 1.1 Connect to the Power Source

To use PoE, plug a Cat 5 Ethernet cable from the Paging Adapter **Ethernet** port to your network. As an alternative to PoE, you can plug one end of a +48V DC power supply into the SIP Paging Adapter, 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 1-1](#).

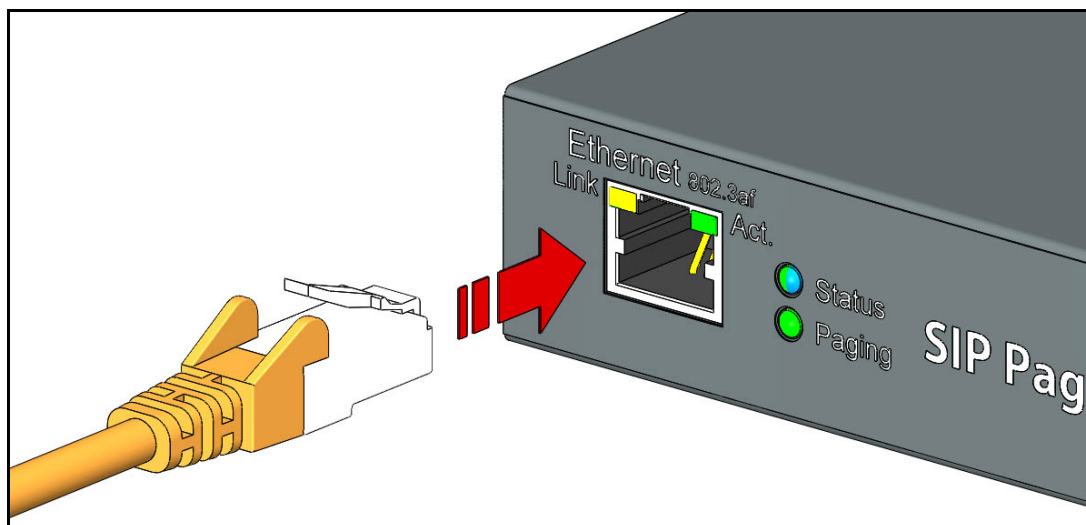
**Figure 1-1. Connecting to the Power Source**

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

## 1.2 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 1-2. Connecting to the Network**





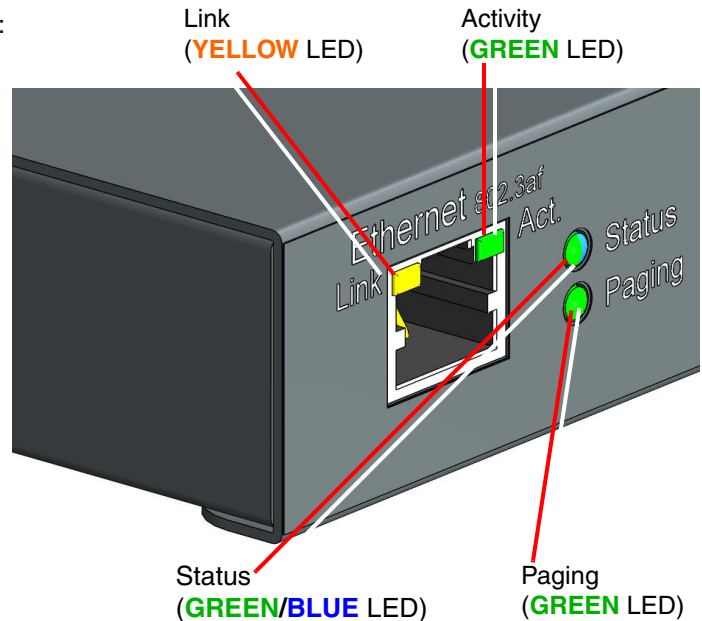
## 1.3 Confirm that the Paging Adapter is Up and Running

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

**Figure 1-3. 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 Paging Adapter 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.



### 1.3.0.1 Verify Network Activity

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

## 1.4 Announcing the IP Address

To announce the IP address for the Paging Adapter, briefly press and then quickly release the **RTFM** switch. See [Figure 1-4](#).

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

**Figure 1-4. RTFM Switch**



## 1.5 Restore the Factory Default Settings

The Paging Adapter is delivered with factory set default values for the parameters in [Table 1-1](#). Use the **RTFM** switch (see [Figure 1-5](#)) on the back of the unit to restore these parameters to the factory default settings.

**Figure 1-5. RTFM Switch**



**Note** When you perform this procedure, the factory default settings are restored. The default parameters for access are shown in [Table 1-1](#).

**Table 1-1. Factory Default Settings**

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

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

To restore these parameters to the factory default settings:

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

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

3. The Paging Adapter settings are restored to the factory defaults.

# 2 Configure the Device

## 2.6 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 Adapter.

**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>

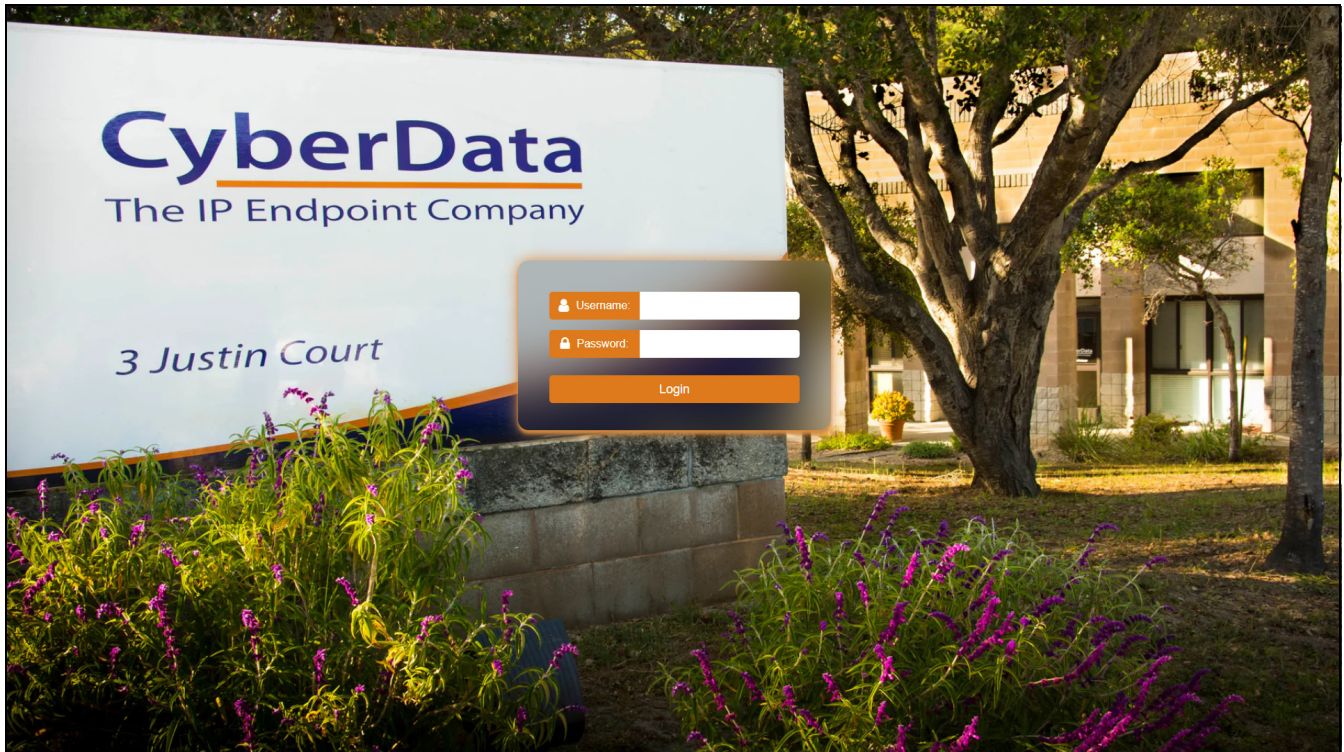
**Note** The Intercom ships in DHCP mode. To get to the **Home** page, use the discovery utility to scan for the device on the network and open your browser from there.

2. On the Log In Page (Figure 2-6), use the following default **Web Access Username** and **Web Access Password** to access the **Home Page** (Figure 2-8):

Web Access Username: **admin**

Web Access Password: **admin**

Figure 2-6. Log In Page



## 2.6.1 Restoring Defaults and Announcing the IP Address

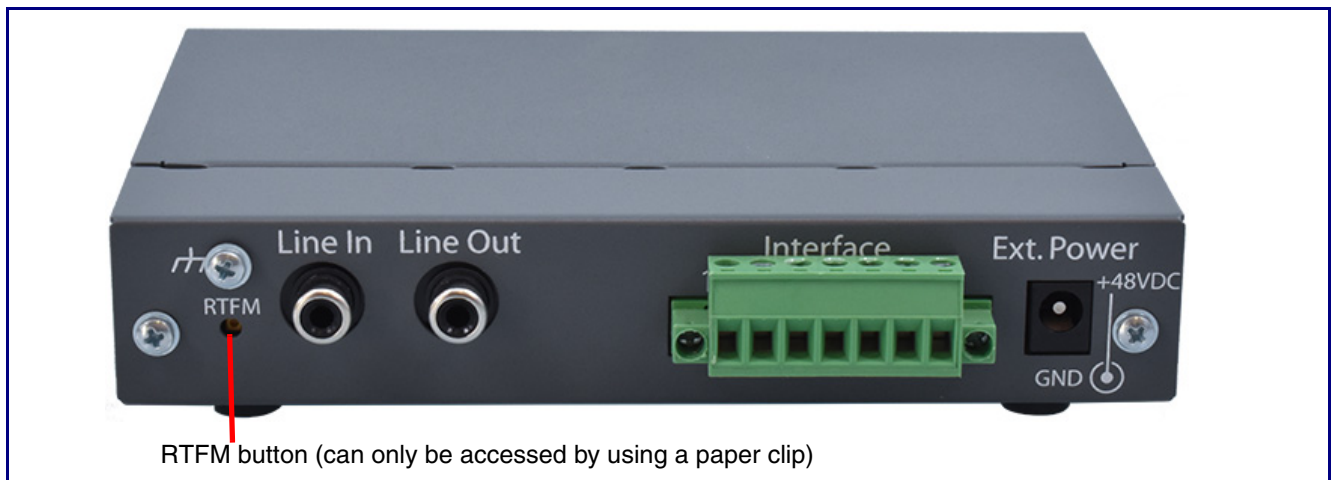
The RTFM button is located on the back of the device.

Briefly pressing the RTFM button (Figure 2-7), prompts the device to announce its IP address (a speaker or amplified speaker must be connected).

To restore the device to its factory default settings (Table 2-2), hold the RTFM button for approximately seven seconds. After 15-20 seconds, "Restoring defaults, rebooting" is announced (a speaker or amplified speaker must be connected).

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.

**Figure 2-7. RTFM Button**



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

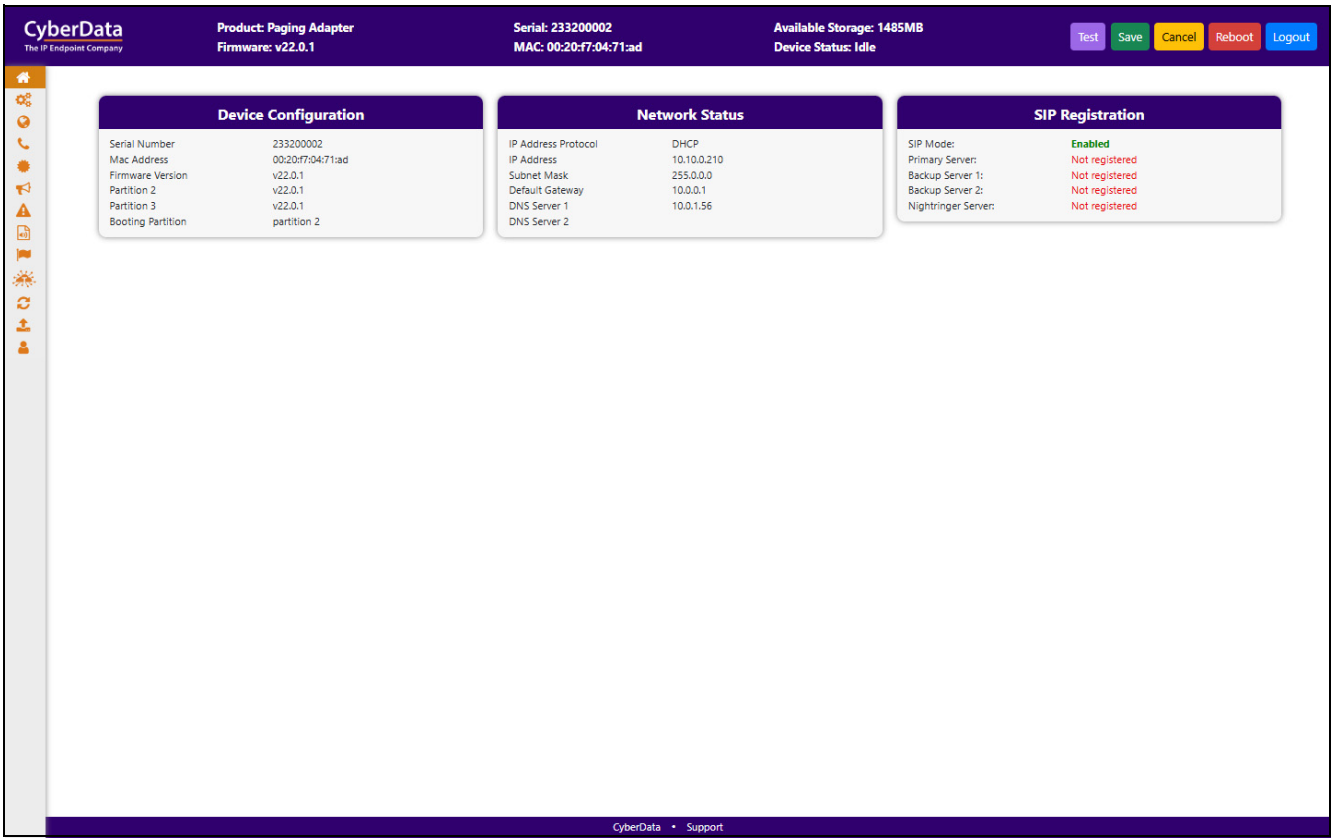
Parameter	Factory Default Setting
IP Addressing	DHCP
IP Address <sup>a</sup>	192.168.1.23
Web Access Username	admin
Web Access Password	admin
Subnet Mask <sup>a</sup>	255.255.255.0
Default Gateway <sup>a</sup>	192.168.1.1

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

## 2.7 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 2-8. Home Page



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

Figure 2-9. 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



## 2.8 Device

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

Figure 2-10. Device Configuration Page

CyberData

The IP Endpoint Company

Product: Paging Adapter

Firmware: v22.0.4

Serial: 233200002

MAC: 00:20:F7:04:71:AD

Available Storage: 1381MB

Device Status: Idle

Test

Save

Cancel

Reboot

Logout

Line-in Settings

Line-in to Line-out Loopback: OFF

Line-in Gain: 127

Line-in Playback Volume: 8

Time Settings

NTP Server(s): 216.239.35.4, 216.239.35.0, 216.239.

NTP Timezone: America/Los\_Angeles (-8)

Current Time: Thu, 10 Jul 2025 11:20:32

Misc Settings

Device Name: Paging Adapter

Beep on Init: OFF

Multicast TTL: 255

Relay Settings

Relay Status: Locked

Relay on Local Audio: OFF

DTMF Settings

DTMF Duration: 500

Bypass DTMF Menu: DISABLED

Pre-configured DTMF for Analog Zone: DISABLED

Analog Zone:

Manual DTMF Entry for Analog Zone: DISABLED

Require Security Code: DISABLED

Security Code: \*\*\*\*\*

CyberData

Support

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

Figure 2-11. InformaCast enabled Device

InformaCast Settings

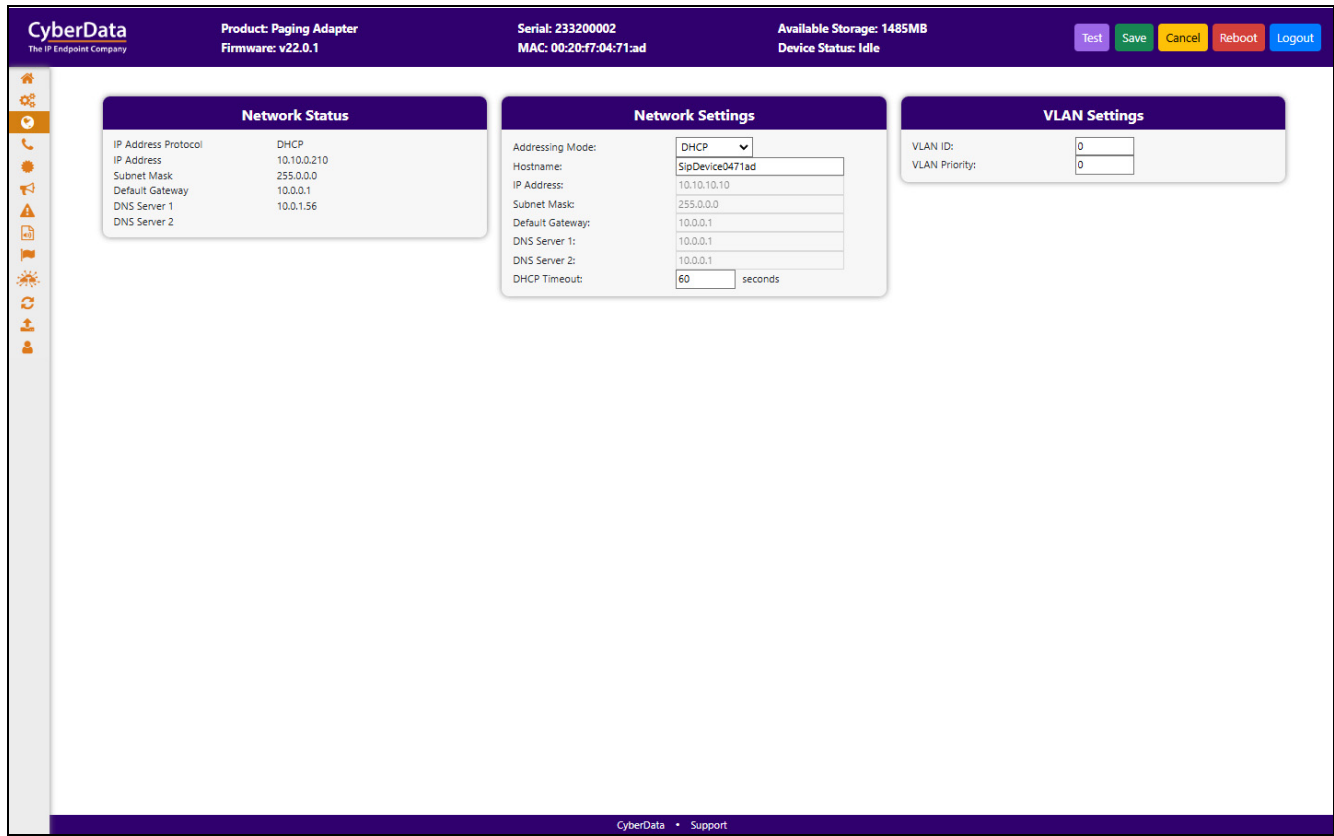
InformaCast Server: http://10.0.1.195:8081/InformaCast/resources



## 2.9 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 2-12. Network Page



## 2.10 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/Ring 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 2-13. SIP Page

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

Figure 2-14. InformaCast enabled Device

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

---

## 2.10.1 Dial Out Extension Strings and DTMF Tones (using rfc2833)

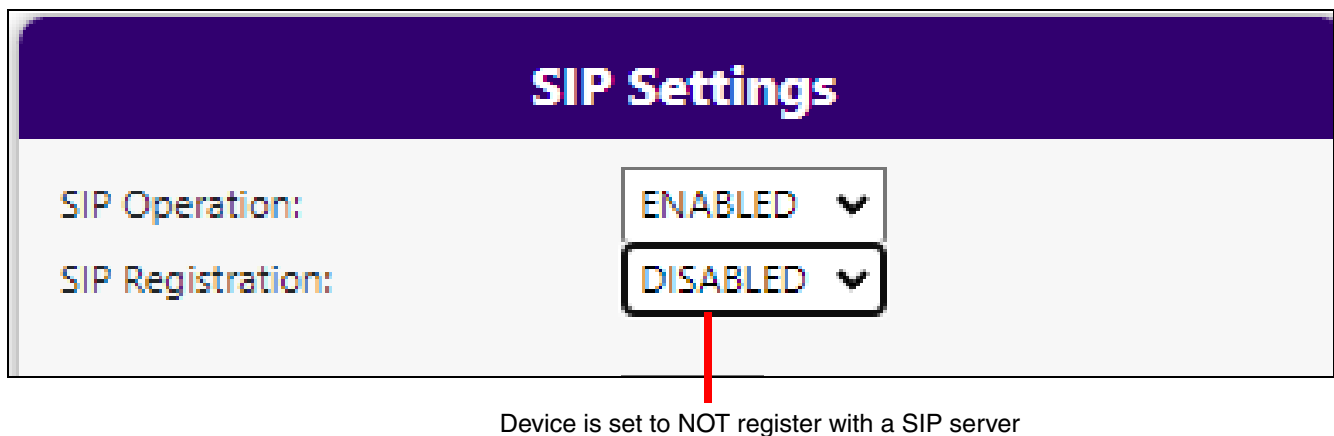
Outgoing calls support delayed DTMF (rfc2833) with the first comma pausing 2 seconds and subsequent commas pausing 1 second.

---

## 2.10.2 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 2-15](#).

**Figure 2-15. SIP Page Set to Point-to-Point Mode**



## 2.11 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 2-16. SSL Page (1 of 2)

CyberData  
The IP Endpoint Company

Product: Paging Adapter  
Firmware: v22.0.1

Serial: 233200002  
MAC: 00:20:f7:04:71:ad

Available Storage: 1485MB  
Device Status: Idle

TestSaveCancelRebootLogout

Web Server Certificate

subject= countryName = US stateOrProvinceName = California localityName = Monterey organizationName = Cyberdata commonName = 0020f70471ad notBefore=Jul 31 00:14:39 2020 GMT notAfter=Jul 29 00:14:39 2030 GMT

Choose Files No file chosen

Import Web Certificate

Restore Web Certificate

SIP Client Certificate

subject= countryName = US stateOrProvinceName = California localityName = Monterey organizationName = Cyberdata commonName = 0020f70471ad notBefore=Jul 31 00:14:39 2020 GMT notAfter=Jul 29 00:14:39 2030 GMT

Choose Files No file chosen

Import SIP Certificate

Restore SIP Certificate

Password (optional):

Autoprovisioning Client Certificate

subject= countryName = US stateOrProvinceName = California localityName = Monterey organizationName = Cyberdata commonName = 0020f70471ad notBefore=Jul 31 00:14:39 2020 GMT notAfter=Jul 29 00:14:39 2030 GMT

Choose Files No file chosen

Import Autoprovisioning Certificate

Restore Autoprovisioning Certificate

Password (optional):

List of Trusted CAs

Upload CA Certificate: Choose Files No file chosen Import CA Certificate

Download CyberData CA Generate Cyberdata CSR 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

CyberData • Support

Figure 2-17. SSL Page (2 of 2)

**CyberData**  
The IP Endpoint Company

**Product:** Paging Adapter  
**Firmware:** v22.0.1

**Serial:** 233200002  
**MAC:** 00:20:f7:04:71:ad

**Available Storage:** 1485MB  
**Device Status:** Idle

Test Save Cancel Reboot Logout

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
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

CyberData • Support

## 2.12 Multicast

The Multicast Configuration page allows the device to join up to ten paging zones for receiving RTP audio streams. A paging zone can consist of one or many CyberData multicast group-enabled products. There is no limit to how many speakers can participate 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. The device will prioritize simultaneous audio streams according to their priority in the list. If both SIP and Multicast is enabled, SIP audio streams are considered priority 4.5. SIP audio will interrupt multicast streams with priority 0 through 4 and will be interrupted by multicast streams with priority 5 through 9.

Ringtones all play at the same priority level. This means that it is possible to have a nightring tone and a normal ringtone playing at the same time.

To use Polycom Group Paging, configure a multicast group with the IP address and port number of the Polycom phone. The default is 224.0.1.116, port 5001, but can be configured through the phone. Polycom defaults to channels 1, 24, and 25, but can also be configured. The payload should be 20 ms and the codec G711mu.

Figure 2-18. Multicast Page

**CyberData**  
The IP Endpoint Company

Product: Paging Adapter  
Firmware: v22.0.1

Serial: 233200002  
MAC: 00:20:f7:04:71:ad

Available Storage: 1485MB  
Device Status: Idle

Test Save Cancel Reboot Logout

Saved Successfully

### Multicast Settings

Recieve Multicast Audio: ☐ ENABLED

Polycom Default Channel:

Polycom Priority Channel:

Polycom Emergency Channel:

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

## 2.13 Fault

The **Fault** page controls configuration of all Fault or sensor-related capabilities of the unit. This can include the fault sensor that is used to have the device take action based on a physical input to the device.

**Figure 2-19. Fault Page**

CyberData  
The IP Endpoint Company

Product: Paging Adapter  
Firmware: v22.0.1

Serial: 233200002  
MAC: 00:20:f7:04:71:a6

Available Storage: 1485MB  
Device Status: Idle

TestSaveCancelRebootLogout

Fault Detection Settings

Message Playbacks:

0

Play Message Locally:

DISABLED

Call to Extension:

DISABLED

Dial Out Extension:

204

Dial Out ID:

ID204

CyberData • Support

## 2.14 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 2-20. Audiofiles Page (1 of 3)

File Name	Currently set to:	default	Choose File	No file chosen	Play	Save	Delete
0:		default	Choose File	No file chosen	Play	Save	Delete
1:		default	Choose File	No file chosen	Play	Save	Delete
2:		default	Choose File	No file chosen	Play	Save	Delete
3:		default	Choose File	No file chosen	Play	Save	Delete
4:		default	Choose File	No file chosen	Play	Save	Delete
5:		default	Choose File	No file chosen	Play	Save	Delete
6:		default	Choose File	No file chosen	Play	Save	Delete
7:		default	Choose File	No file chosen	Play	Save	Delete
8:		default	Choose File	No file chosen	Play	Save	Delete
9:		default	Choose File	No file chosen	Play	Save	Delete
Audio Test:		default	Choose File	No file chosen	Play	Save	Delete
Dot:		default	Choose File	No file chosen	Play	Save	Delete
Night Ring:		default	Choose File	No file chosen	Play	Save	Delete
Page Tone:		default	Choose File	No file chosen	Play	Save	Delete
Rebooting:		default	Choose File	No file chosen	Play	Save	Delete
Restoring Default:		default	Choose File	No file chosen	Play	Save	Delete
Ringback Tone:		default	Choose File	No file chosen	Play	Save	Delete
Ring Tone:		default	Choose File	No file chosen	Play	Save	Delete
Sensor Triggered:		default	Choose File	No file chosen	Play	Save	Delete
Your IP Address Is:		default	Choose File	No file chosen	Play	Save	Delete

Figure 2-21. Audiofiles Page (2 of 3)

File Name	Currently set to:	default	Choose File	No file chosen	Play	Save	Delete
Cancel:		default	Choose File	No file chosen	Play	Save	Delete
Currently Playing:		default	Choose File	No file chosen	Play	Save	Delete
Invalid Entry:		default	Choose File	No file chosen	Play	Save	Delete
Page:		default	Choose File	No file chosen	Play	Save	Delete
Play Stored Message:		default	Choose File	No file chosen	Play	Save	Delete
Pound (#):		default	Choose File	No file chosen	Play	Save	Delete
Press:		default	Choose File	No file chosen	Play	Save	Delete
Stored Message:		default	Choose File	No file chosen	Play	Save	Delete
Through:		default	Choose File	No file chosen	Play	Save	Delete
To:		default	Choose File	No file chosen	Play	Save	Delete
Enter Code:		default	Choose File	No file chosen	Play	Save	Delete
Invalid Code:		default	Choose File	No file chosen	Play	Save	Delete
Enter Zone:		default	Choose File	No file chosen	Play	Save	Delete



Figure 2-22. Audiofiles Page (3 of 3)

Stored Messages

Choose File

No file chosen

Upload Message

Delete All Messages

Stored Message 1:	Currently set to:	default	<div>Choose File</div>	No file chosen	Repeat:	<div>0</div>	Infinite:	<div>OFF</div>	<div>Play</div>	<div>Save</div>	<div>Delete</div>
Stored Message 2:	Currently set to:	default	<div>Choose File</div>	No file chosen	Repeat:	<div>0</div>	Infinite:	<div>OFF</div>	<div>Play</div>	<div>Save</div>	<div>Delete</div>
Stored Message 3:	Currently set to:	default	<div>Choose File</div>	No file chosen	Repeat:	<div>0</div>	Infinite:	<div>OFF</div>	<div>Play</div>	<div>Save</div>	<div>Delete</div>
Stored Message 4:	Currently set to:	default	<div>Choose File</div>	No file chosen	Repeat:	<div>0</div>	Infinite:	<div>OFF</div>	<div>Play</div>	<div>Save</div>	<div>Delete</div>
Stored Message 5:	Currently set to:	default	<div>Choose File</div>	No file chosen	Repeat:	<div>0</div>	Infinite:	<div>OFF</div>	<div>Play</div>	<div>Save</div>	<div>Delete</div>
Stored Message 6:	Currently set to:	default	<div>Choose File</div>	No file chosen	Repeat:	<div>0</div>	Infinite:	<div>OFF</div>	<div>Play</div>	<div>Save</div>	<div>Delete</div>
Stored Message 7:	Currently set to:	default	<div>Choose File</div>	No file chosen	Repeat:	<div>0</div>	Infinite:	<div>OFF</div>	<div>Play</div>	<div>Save</div>	<div>Delete</div>
Stored Message 8:	Currently set to:	default	<div>Choose File</div>	No file chosen	Repeat:	<div>0</div>	Infinite:	<div>OFF</div>	<div>Play</div>	<div>Save</div>	<div>Delete</div>
Stored Message 9:	Currently set to:	default	<div>Choose File</div>	No file chosen	Repeat:	<div>0</div>	Infinite:	<div>OFF</div>	<div>Play</div>	<div>Save</div>	<div>Delete</div>

## 2.15 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 2-23. Events Page

CyberData  
The IP Endpoint Company

Product: Paging Adapter  
Firmware: v22.0.1

Serial: 233200002  
MAC: 00:20:f7:04:71:ad

Available Storage: 1485MB  
Device Status: Idle

TestSaveCancelRebootLogout

Event Server

Event Generation: 

DISABLED

Server IP Address: 

10.0.0.250

Server Port: 

8080

Server URL: 

xmlparse\_engine

Events

Application Started Events: 

DISABLED

Reboot Events: 

DISABLED

Heartbeat Events: 

DISABLED

Call Started Events: 

DISABLED

Call Terminated Events: 

DISABLED

Nightring Events: 

DISABLED

Multicast Started Events: 

DISABLED

Multicast Stopped Events: 

DISABLED

Relay Activated Events: 

DISABLED

Relay Deactivated Events: 

DISABLED

Fault Events: 

DISABLED

CyberData • Support

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

Figure 2-24. InformaCast enabled Device

InformaCast Start Events: 

DISABLED

InformaCast Stop Events: 

DISABLED

### 2.15.0.1 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>
```

## 2.16 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 2-25. Terminus Page**

**CyberData**  
The IP Endpoint Company

Product: Paging Adapter  
Firmware: v22.0.1

Serial: 233200002  
MAC: 00:20:f7:04:71:ad

Available Storage: 1485MB  
Device Status: Idle

Test Save Cancel Reboot Logout

**Discovery Setting**

Multicast Address: 239.27.32.4

Time to Live: 255

Discovery Interval: 60 seconds

**Lockdown Settings**

Lock Down Mode: Disabled

Relay: No Action

CyberData • Support

## 2.17 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 2-26. Autoprovisioning Page**

The screenshot displays the Autoprovisioning configuration interface. At the top, a header bar contains the CyberData logo, product information (Paging Adapter, v22.0.1), serial and MAC addresses, available storage (1485MB), and device status (Idle). Action buttons (Test, Save, Cancel, Reboot, Logout) are on the right. A left sidebar shows navigation icons. The main area is divided into two panels: 'Autoprov Settings' and 'Autoprov Log'.

**Autoprov Settings:**

- Autoprov: **ENABLED** (dropdown)
- Autoprov Server:
- Autoprov Filename:
- Use tftp: **DISABLED** (dropdown)
- Verify Server Certificate: **DISABLED** (dropdown)
- Username:
- Password:
- Autoprov autoupdate:  minutes
- Autoprov at time:
- Autoprov when idle:  minutes
- Download Template** (button)

**Autoprov Log:**

```

2024-11-19 09:08:18 Autoprov: no autoprov triggers. Exiting...
2024-11-19 09:08:23 Autoprov: provisioning on boot
2024-11-19 09:08:23 Autoprov found server='http://10.0.0.242' in dhcp
option 43
2024-11-19 09:08:23 Autoprov looking for 0020f70471ad.xml at
http://10.0.0.242
2024-11-19 09:08:23 Autoprov downloading
http://10.0.0.242/0020f70471ad.xml
2024-11-19 09:08:23 Got autoprov file. Parsing "0020f70471ad.xml"
2024-11-19 09:08:24 Autoprov: Processing ssl certificates
2024-11-19 09:08:24 No certificate elements in SSLCertificates
2024-11-19 09:08:24 Autoprov: Processing audio files
2024-11-19 09:08:25 Autoprov: FirmwareSettings config not found
2024-11-19 09:08:25 DeviceConfig: error = False
2024-11-19 09:08:25 SSLCertificates: error = None
  
```

The footer of the interface includes 'CyberData • Support'.

## 2.18 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>

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

- Firmware file
- Release notes
- Autoprovisioning template


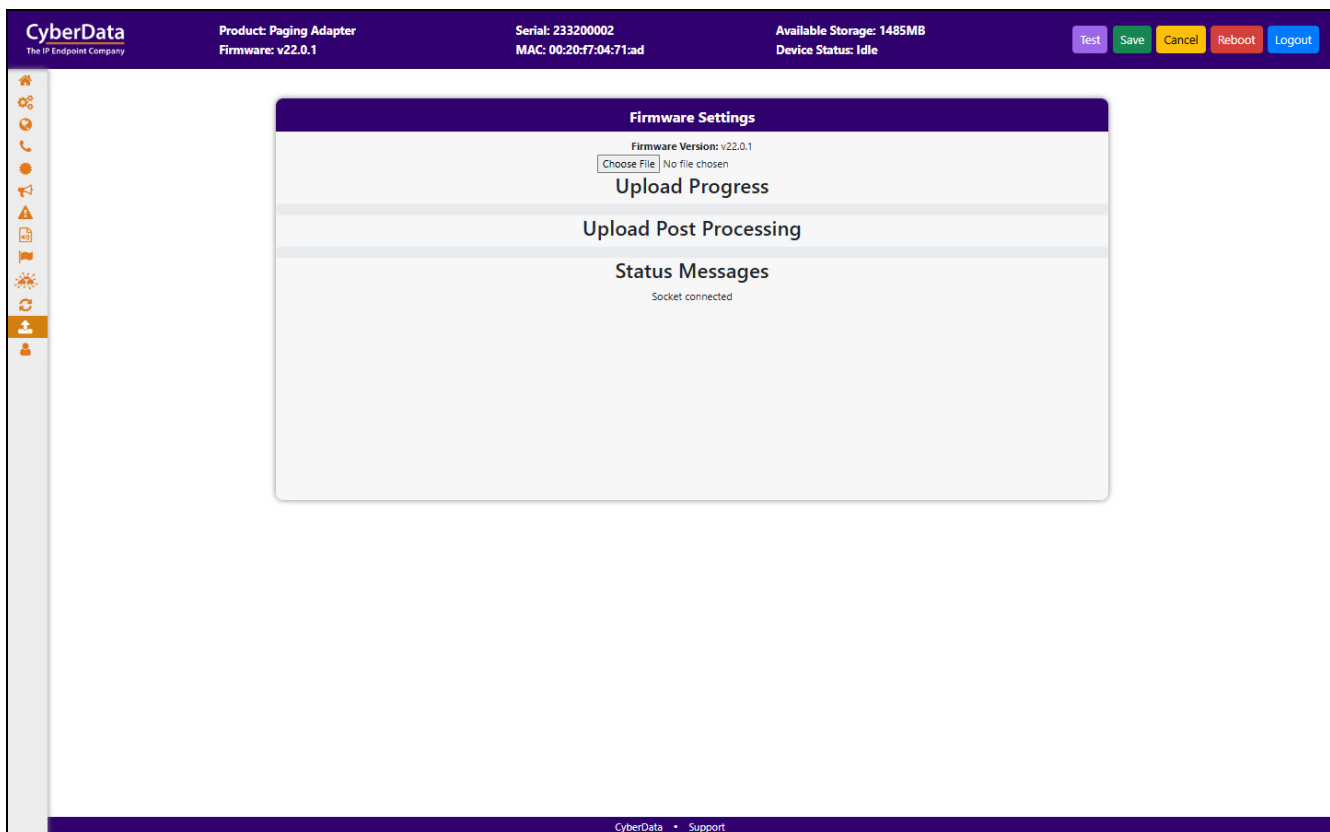
 GENERAL ALERT	<p><b>Caution</b></p> <p><b>Equipment Hazard:</b> Do not reboot the device. It will reboot automatically when the process is complete.</p>
--	--

Figure 2-27. Firmware Page





## 2.19 Admin

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

Figure 2-28. Admin Page

CyberData  
The IP Endpoint Company

Product: Paging Adapter  
Firmware: v22.0.1

Serial: 233200002  
MAC: 00:20:f7:04:71:ad

Available Storage: 1485MB  
Device Status: Idle

TestSaveCancelRebootLogout

Admin Settings

Username: admin  
Password: \*\*\*\*\*  
Confirm Password: \*\*\*\*\*

Statistics

Storage: 1485MB  
Boot Count: 4  
Reboot Count: 3  
Uptime: up 5 minutes

Logging Settings

Debug Level: 4  
Log Network Traffic: OFF

Get Application LogRemove Application Log  
Get Network LogRemove Network Log  
Get All LogsRemove All Logs

Retrieving the log files may take some time due to their size.

Configuration Settings

Partition 2 v22.0.1  
Partition 3 v22.0.1  
Booting Partition partition 2

Restore Default ConfigRestore Default Certificates  
Import ConfigExport Config  
Boot From Other Partition

Users List

Add New UserDelete All UsersImport UsersExport Users

Username	Home	Device	Network	SIP	SSL	Multicast	Fault	Audiofiles	Events	Terminus	Autopro	Firmware	Admin
----------	------	--------	---------	-----	-----	-----------	-------	------------	--------	----------	---------	----------	-------

Log Viewer

Service: ApplicationEntries to get: 250Sort: OldestView Log

CyberDataSupport

## 2.20 Command Interface

Some functions on the device can be activated using simple POST commands to the web interface. The examples in [Table 2-3](#) use the free unix utility, **wget** commands. However, any program that can send HTTP POST commands to the device should work.

### 2.20.1 Command Interface Post Commands

The commands in [Table 2-3](#) require an authenticated session (a valid username and password to work).

**Table 2-3. Command Interface Post Commands**

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

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

# Appendix A: Troubleshooting/Technical Support

---

## A.1 Contact Information

Contact	<p>CyberData Corporation 3 Justin Court Monterey, CA 93940 USA <a href="http://www.cyberdata.net">www.cyberdata.net</a> Phone: 831-373-2601 Fax: 831-373-4193</p>
Sales	<p>Sales 831-373-2601, Extension 334</p>
Technical Support	<p>The fastest way to get technical support for your VoIP product is to submit a VoIP Technical Support form at the following website:</p> <p><a href="https://support.cyberdata.net/">https://support.cyberdata.net/</a></p> <p>The Support Form initiates a ticket which CyberData uses for tracking customer requests. Most importantly, the Support Form tells us which PBX system and software version that you are using, the make and model of the switch, and other important information. This information is essential for troubleshooting. Please also include as much detail as possible in the <b>Comments</b> section of the Support Form.</p> <p>Phone: (831) 373-2601, Extension 333</p>

---

## A.2 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 1

## A

activity light 3  
Admin 27  
Audiofiles 18  
Autoprovisioning 25

## C

cat 5 ethernet cable 1  
Command Interface 28  
Command Interface Post Commands 28  
Contact Information 29

## D

default  
    gateway 5  
    IP address 5  
    subnet mask 5  
    username and password 5  
default gateway 5  
default settings, restoring 5  
Device 10  
Dial Out Extension Strings and DTMF Tones 13  
Discovery Utility program 6

## E

ethernet port 1  
Events 20

## F

Fault 17  
Firmware 26

## G

green link light 3

## H

Home Page 8

## I

IP address 5  
IP addressing  
    default  
        IP addressing setting 5

## L

link light 3  
Log In Page 6

## M

Multicast 16

## N

Network 11  
network activity, verifying 3  
network, connecting to 2

## P

password  
    restoring the default 5  
Point-to-Point Configuration 13  
port  
    ethernet 1  
power  
    connecting to 1

## R

restoring factory default settings 5

## S

SIP (Session Initiation Protocol) 12

SSL 14

status light 3

subnet mask 5

## T

Terminus 24

Troubleshooting/Technical Support 29

## U

username

restoring the default 5

## V

verifying

network activity 3

## W

Warranty and RMA Information 29

web access password 5

web access username 5