



CyberData Paging Adapters Operations Guide

SIP Compliant
Part #011233, 011280
Document Part #932061A
for Firmware Version 22.0

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

Operations Guide 932061A
SIP Compliant 011233, 011280

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 932061A, which corresponds to firmware version 22.0, was released on November 19, 2024.

Pictorial Alert Icons

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

Hazard Levels

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

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




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

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

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

Important Safety Instructions

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

 <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

Contents

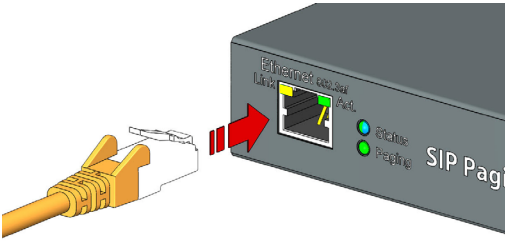
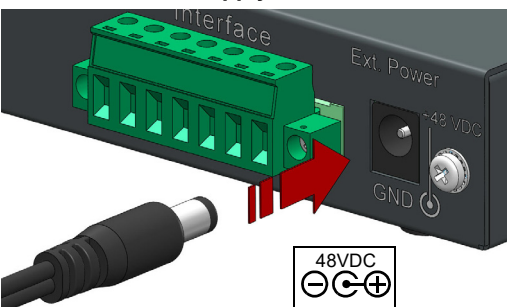
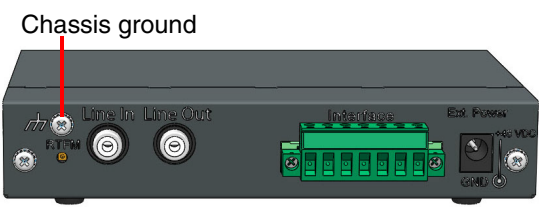
Chapter 1 Setting Up the SIP Paging Adapter	1
1.1 Connect to the Power Source	1
Non-Poe	1
Chassis Ground	1
Poe	1
1.2 Connect to the Network	2
1.3 Confirm that the SIP Paging Adapter is Up and Running	3
Verify Network Activity	3
1.4 Announcing the IP Address	4
1.5 Restore the Factory Default Settings	5
Chapter 2 Configure the Device	6
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
Appendix A Troubleshooting/Technical Support	29
A.1 Contact Information	29
A.2 Warranty and RMA Information	29

1 Setting Up the SIP Paging Adapter

1.1 Connect to the Power Source

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

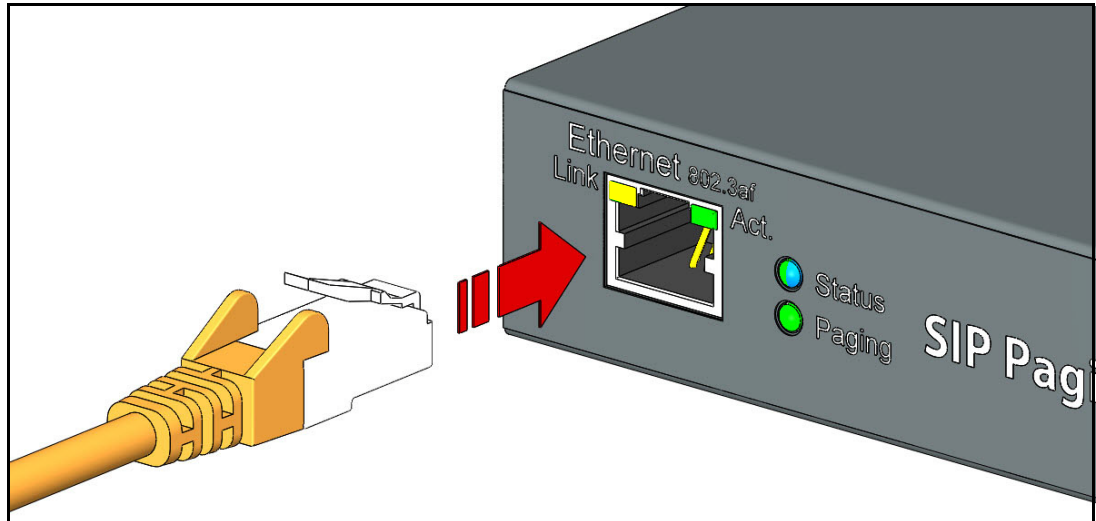
Figure 1-1. Connecting to the Power Source

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

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



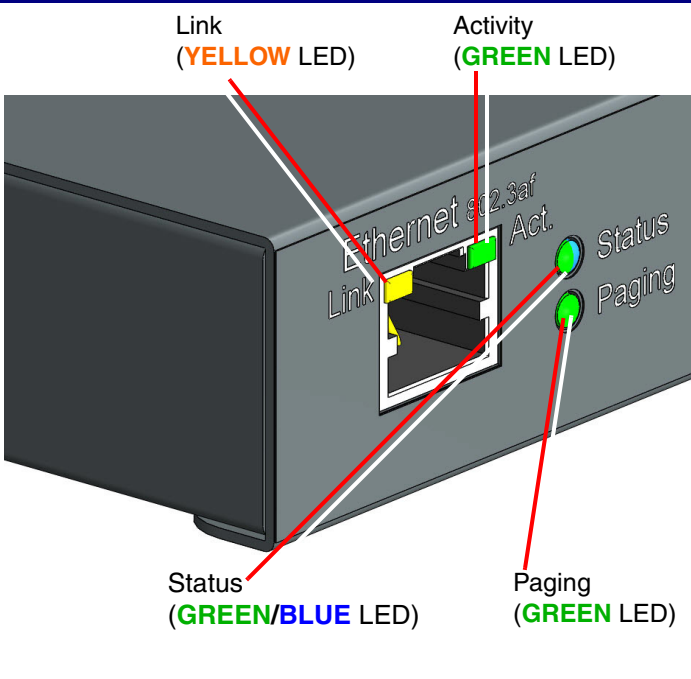
1.3 Confirm that the SIP Paging Adapter is Up and Running

The LEDs on the front of the SIP 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 SIP 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.



The diagram shows the front panel of the SIP Paging Adapter. On the left is an Ethernet port with a yellow LED labeled 'Link' above it. To the right of the port are two green LEDs: a square one labeled 'Status' and a round one labeled 'Paging'. Above the Ethernet port is a green LED labeled 'Activity'. Red lines connect the text labels to the LEDs on the device.

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 SIP 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 SIP 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 ^a	192.168.1.23
Web Access Username	admin
Web Access Password	admin
Subnet Mask ^a	255.255.255.0
Default Gateway ^a	192.168.1.1

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

To restore these parameters to the factory default settings:

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

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

3. The SIP Paging 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>

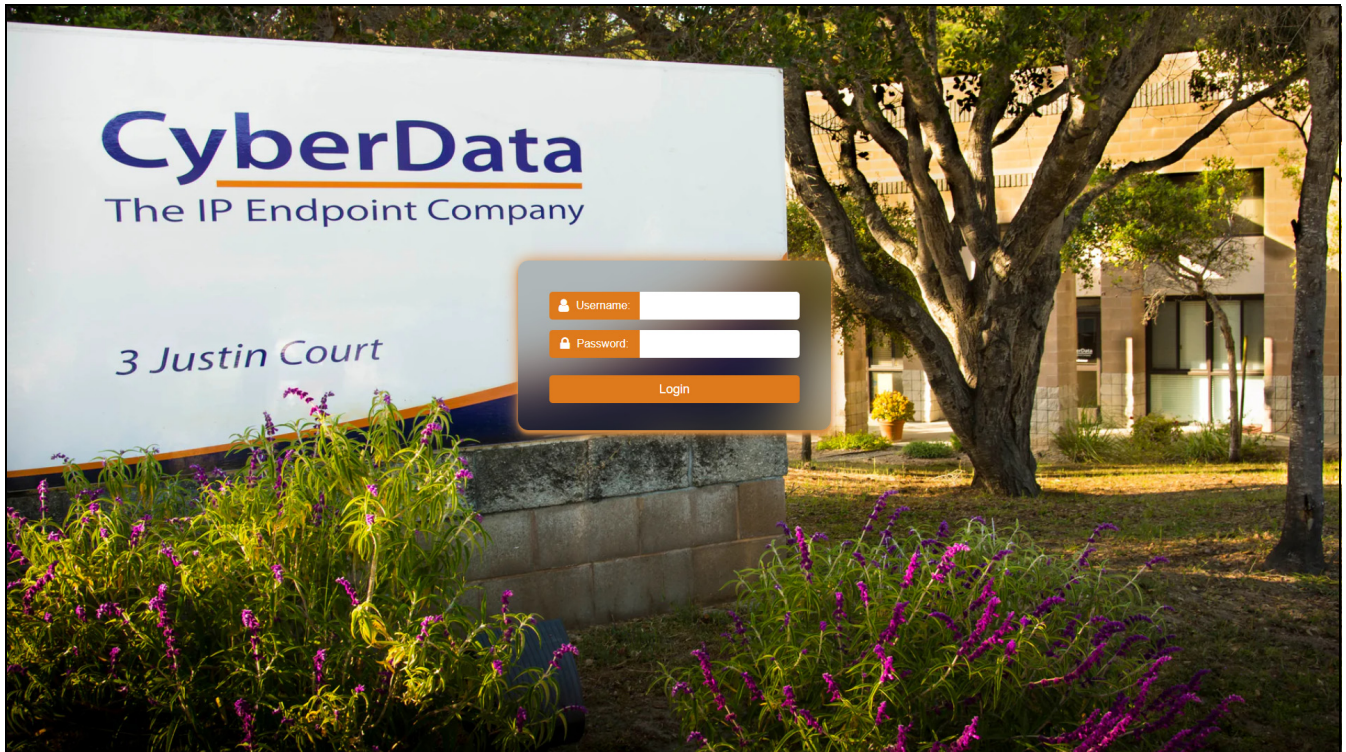
Note The Intercom ships in DHCP mode. To get to the **Home** page, use the discovery utility to scan for the device on the network and open your browser from there.

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

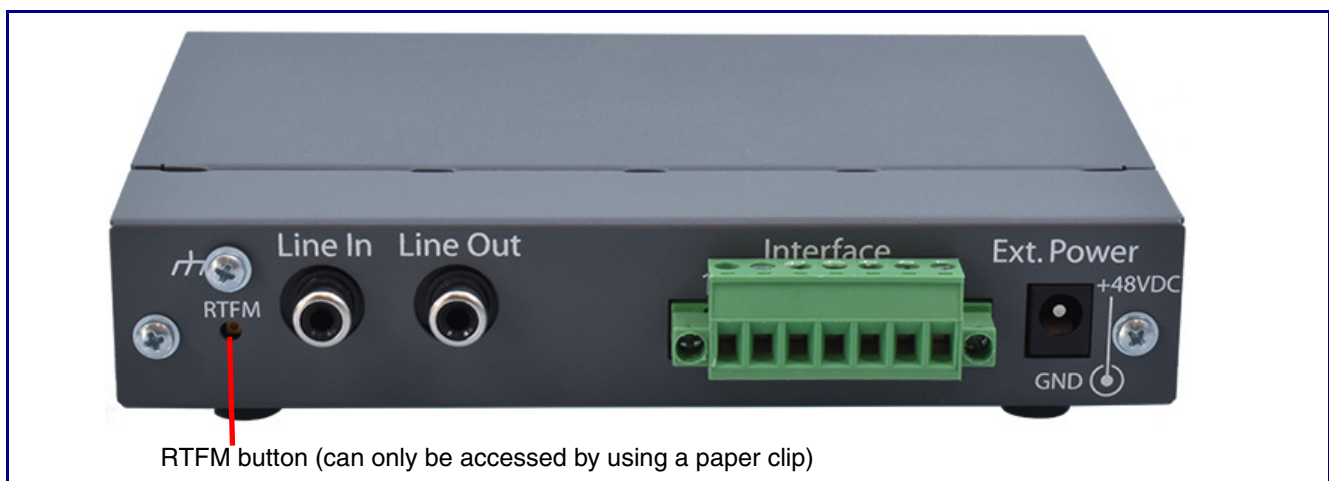


Table 2-2. Factory Default Settings

Parameter	Factory Default Setting
IP Addressing	DHCP
IP Address ^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.

2.7 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

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. The device information includes: Product: Paging Adapter, Firmware: v22.0.1, Serial: 233200002, MAC: 00:20:F7:04:71:ad, Available Storage: 1485MB, and Device Status: Idle. Below this, there are three main sections: Device Configuration, Network Status, and SIP Registration. Each section contains a table of details. On the left side, there is a vertical navigation menu with various icons. At the bottom right, there are buttons for Test, Save, Cancel, Reboot, and Logout. The footer of the page shows 'CyberData - Support'.

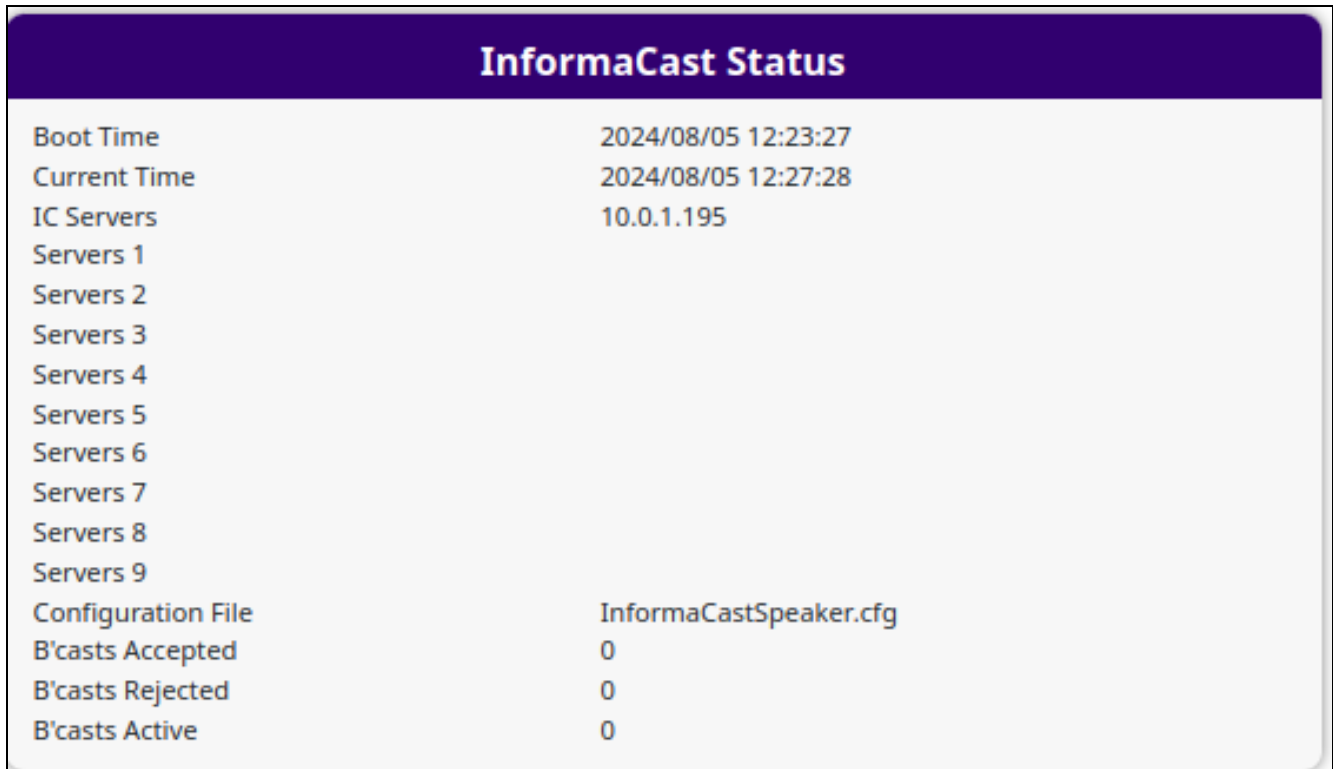
Device Configuration	
Serial Number	233200002
Mac Address	00:20:F7:04:71:ad
Firmware Version	v22.0.1
Partition 2	v22.0.1
Partition 3	v22.0.1
Booting Partition	partition 2

Network Status	
IP Address Protocol	DHCP
IP Address	10.10.0.210
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

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

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

Figure 2-11. InformaCast enabled Device

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

The screenshot displays the Network configuration page for a CyberData Paging Adapter. The interface includes a top navigation bar with device information and a sidebar with navigation icons. The main content area is divided into three panels: Network Status, Network Settings, and VLAN Settings.

Network Status	
IP Address Protocol	DHCP
IP Address	10.10.0.210
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:	SipDevice0471ad
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

At the top right of the page, there are buttons for Test, Save, Cancel, Reboot, and Logout. The footer of the page contains the text "CyberData • Support".

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 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 ▼
-------------------------	-------------------

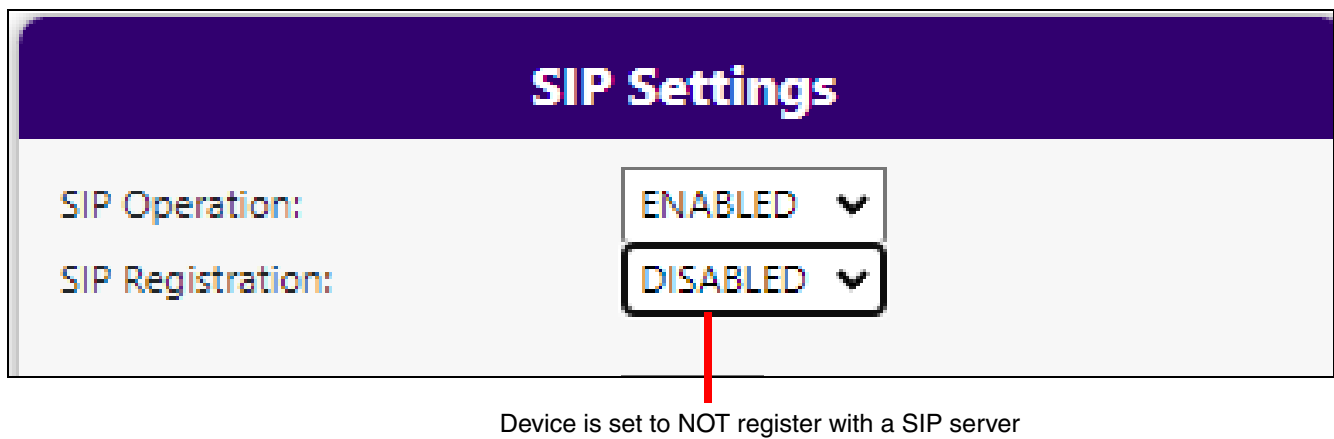
2.10.1 Dial Out Extension Strings and DTMF Tones (using rfc2833)

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)

The screenshot displays the CyberData SSL configuration interface. At the top, the device information is shown: Product: Paging Adapter, Serial: 233200002, Available Storage: 1485MB, Firmware: v22.0.1, MAC: 00:20:77:04:71:ad, and Device Status: Idle. There are buttons for Test, Save, Cancel, Reboot, and Logout.

Three certificate configuration panels are visible:

- Web Server Certificate:** Shows subject details (countryName: US, stateOrProvinceName: California, localityName: Monterey, organizationName: Cyberdata, commonName: 0020F70471ad) and validity dates (notBefore: Jul 31 00:14:39 2020 GMT, notAfter: Jul 29 00:14:39 2030 GMT). It includes 'Choose Files' and 'No file chosen' buttons, and 'Import Web Certificate' and 'Restore Web Certificate' buttons.
- SIP Client Certificate:** Shows identical subject details and validity dates. It includes 'Choose Files' and 'No file chosen' buttons, and 'Import SIP Certificate' and 'Restore SIP Certificate' buttons. A 'Password (optional):' field is present.
- Autoprovisioning Client Certificate:** Shows identical subject details and validity dates. It includes 'Choose Files' and 'No file chosen' buttons, and 'Import Autoprovisioning Certificate' and 'Restore Autoprovisioning Certificate' buttons. A 'Password (optional):' field is present.

Below these panels is the **List of Trusted CAs** section. It features an 'Upload CA Certificate:' field with a 'Choose Files' button and an 'Import CA Certificate' button. Below this are buttons for 'Download CyberData CA', 'Generate Cyberdata CSR', 'Remove All', and 'Restore Defaults'.

ID	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
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

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

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

CyberData
The IP Endpoint Company

 Product: Paging Adapter Serial: 233200002 Available Storage: 1485MB
 Firmware: v22.0.1 MAC: 00-20-f7:04-71:ad 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

Product: Paging Adapter
Serial: 233200002
Available Storage: 1485MB
Firmware: v22.0.1
MAC: 00:20:f7:04:71:a0
Device Status: Idle

Test Save Cancel Reboot Logout

Saved Successfully

Multicast Settings

Recieve Multicast Audio:

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="text" value="DISABLED"/>	<input type="text" value="DISABLED"/>
1	239.168.3.2	3000	MG1	<input type="text" value="DISABLED"/>	<input type="text" value="DISABLED"/>
2	239.168.3.3	4000	MG2	<input type="text" value="DISABLED"/>	<input type="text" value="DISABLED"/>
3	239.168.3.4	5000	MG3	<input type="text" value="DISABLED"/>	<input type="text" value="DISABLED"/>
4	239.168.3.5	6000	MG4	<input type="text" value="DISABLED"/>	<input type="text" value="DISABLED"/>
5	239.168.3.6	7000	MG5	<input type="text" value="DISABLED"/>	<input type="text" value="DISABLED"/>
6	239.168.3.7	8000	MG6	<input type="text" value="DISABLED"/>	<input type="text" value="DISABLED"/>
7	239.168.3.8	9000	MG7	<input type="text" value="DISABLED"/>	<input type="text" value="DISABLED"/>
8	239.168.3.9	10000	MG8	<input type="text" value="DISABLED"/>	<input type="text" value="DISABLED"/>
9	239.168.3.10	11000	Emergency	<input type="text" value="DISABLED"/>	<input type="text" value="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

The screenshot shows the CyberData web interface for a Paging Adapter. The header contains the following information:

- CyberData** (The IP Endpoint Company)
- Product:** Paging Adapter
- Serial:** 233200002
- Available Storage:** 1485MB
- Firmware:** v22.0.1
- MAC:** 00:20:f7:04:71:ad
- Device Status:** Idle

Navigation buttons in the top right include: Test, Save, Cancel, Reboot, and Logout.

The main content area features a sidebar with various icons, including a warning icon. The central focus is the **Fault Detection Settings** form, which contains the following fields:

- Message Playbacks:** 0
- Play Message Locally:** DISABLED
- Call to Extension:** DISABLED
- Dial Out Extension:** 204
- Dial Out ID:** id204

The footer of the interface displays "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)

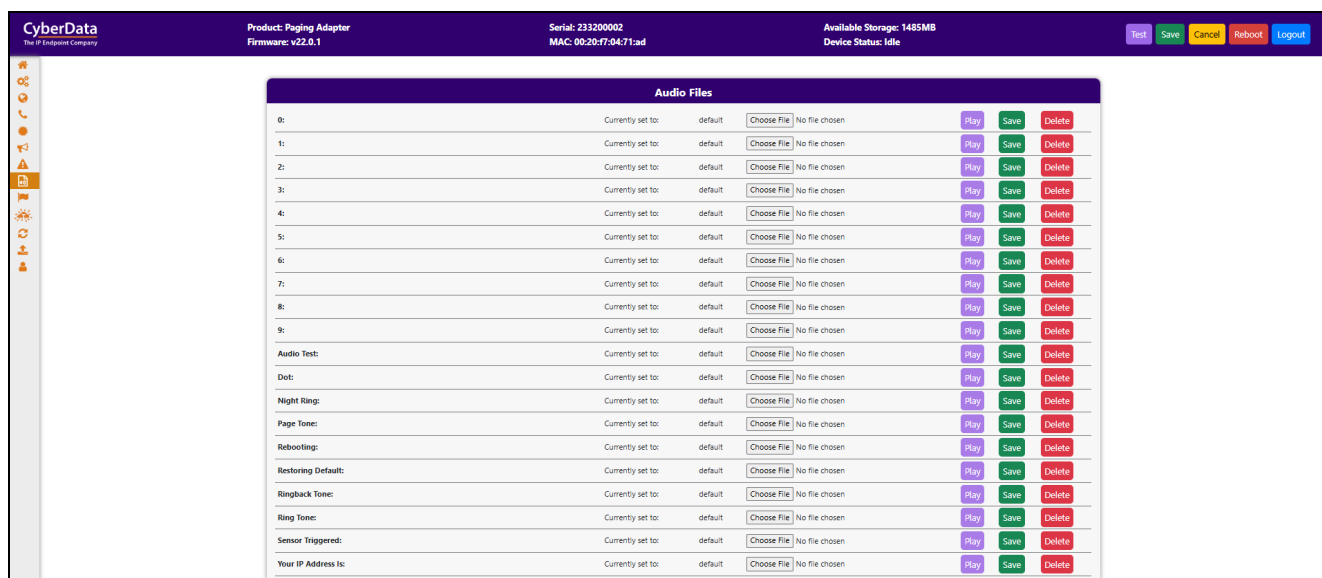


Figure 2-21. Audiofiles Page (2 of 3)

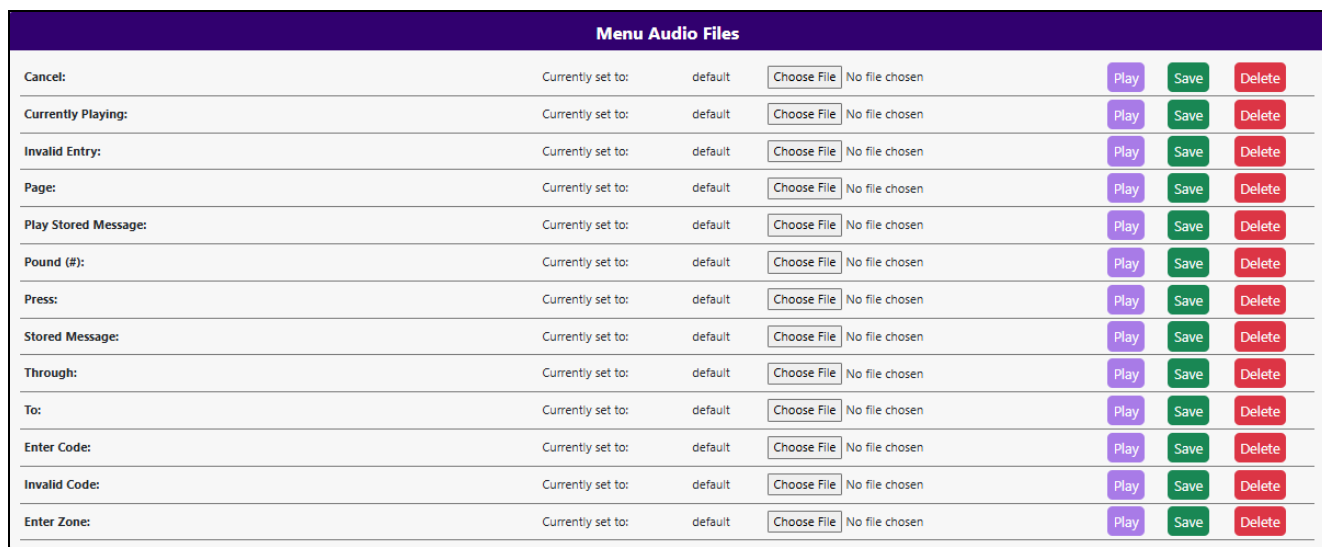


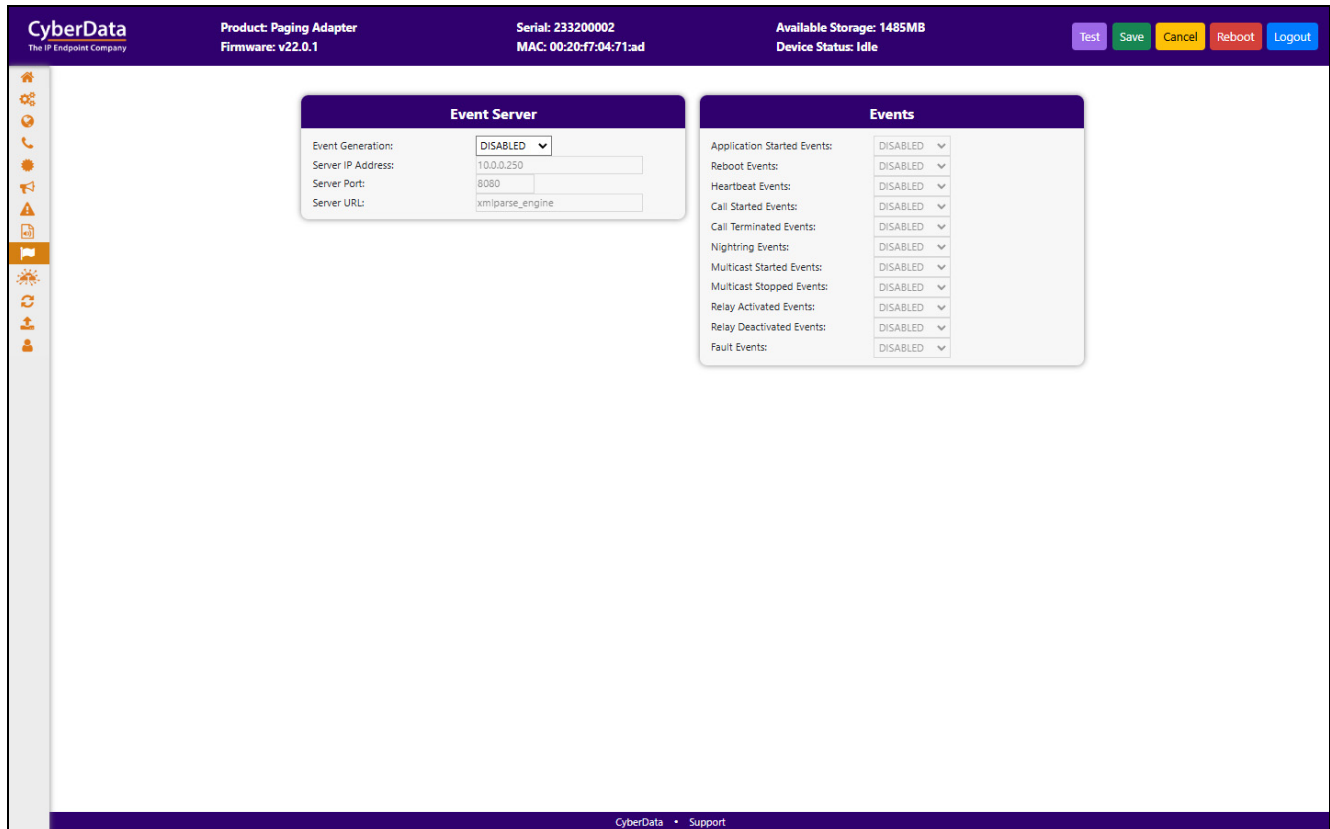
Figure 2-22. Audiofiles Page (3 of 3)

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: <input type="button" value="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: <input type="button" value="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: <input type="button" value="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: <input type="button" value="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: <input type="button" value="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: <input type="button" value="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: <input type="button" value="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: <input type="button" value="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: <input type="button" value="OFF"/>	<input type="button" value="Play"/>	<input type="button" value="Save"/> <input type="button" value="Delete"/>

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



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

Figure 2-24. InformaCast enabled Device



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>
```

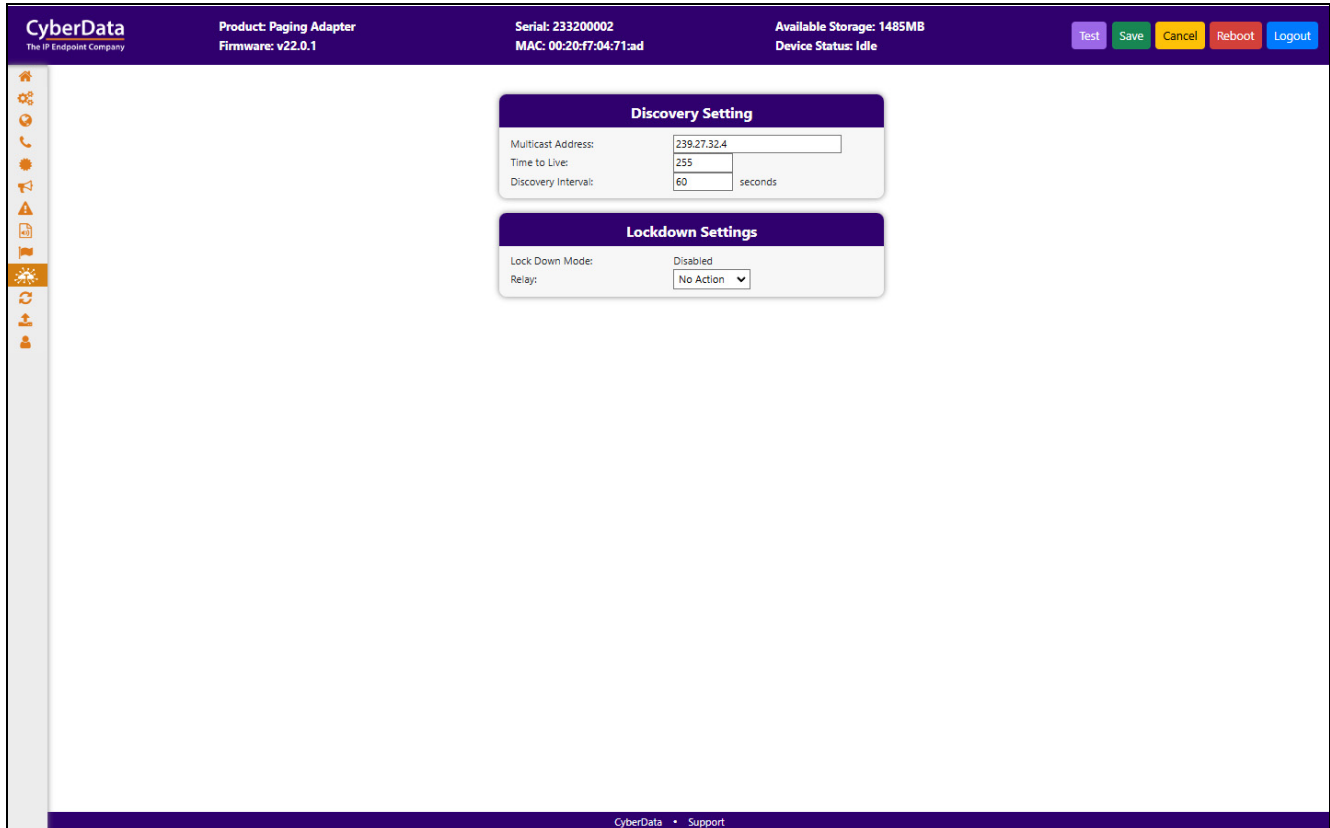
```
POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>NIGHTRINGING</event>
</cyberdata>
```

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



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

Figure 2-26. Autoprovisioning Page

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


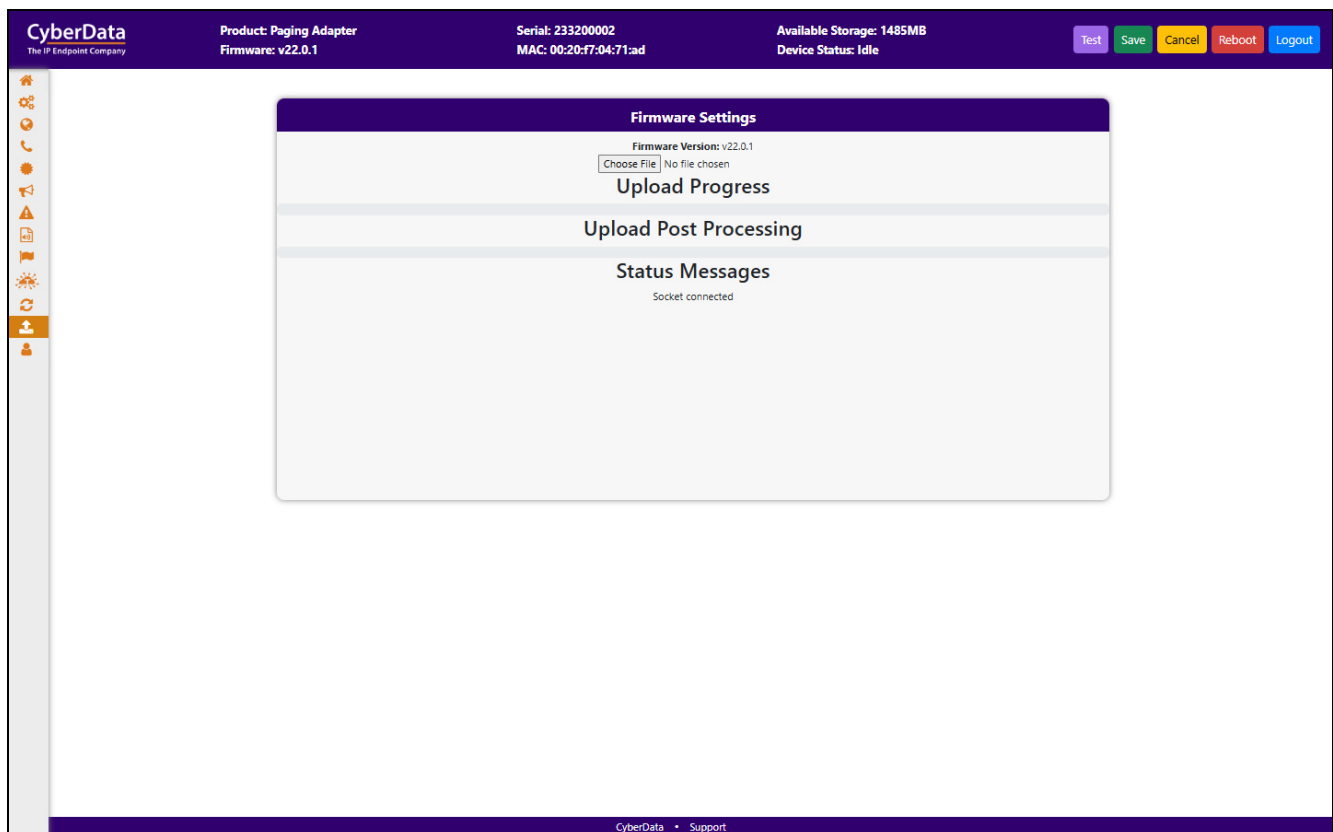
 GENERAL ALERT	<p>Caution</p> <p>Equipment Hazard: Do not reboot the device. It will reboot automatically when the process is complete.</p>
----------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------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

Figure 2-27. Firmware Page



The screenshot displays the CyberData web interface for a Paging Adapter. The top navigation bar includes the CyberData logo and the following information: Product: Paging Adapter, Serial: 233200002, Available Storage: 1485MB, and Device Status: Idle. Action buttons for Test, Save, Cancel, Reboot, and Logout are visible on the right. The main content area is titled 'Firmware Settings' and shows the current Firmware Version as v22.0.1. Below this, there is a 'Choose File' button with the text 'No file chosen'. The page is divided into sections for 'Upload Progress', 'Upload Post Processing', and 'Status Messages', which currently displays 'Socket connected'. A sidebar with various icons is on the left, and the footer contains 'CyberData • Support'.

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

The screenshot displays the CyberData Admin Page interface. At the top, the header includes the CyberData logo, product information (Paging Adapter, Firmware: v22.0.1), serial and MAC addresses, available storage (1485MB), and device status (Idle). Navigation buttons for Test, Save, Cancel, Reboot, and Logout are visible.

The main content area is divided into several sections:

- Admin Settings:** Fields for Username (admin), Password, and Confirm Password.
- Statistics:** System metrics including Storage (1485MB), Boot Count (4), Reboot Count (3), and Uptime (up 5 minutes).
- Logging Settings:** Debug Level (4) and Log Network Traffic (OFF). Buttons for Get Application Log, Remove Application Log, Get Network Log, Remove Network Log, Get All Logs, and Remove All Logs are provided.
- Configuration Settings:** Information about partitions (Partition 2, Partition 3, Booting Partition) and their respective firmware versions. Buttons for Restore Default Config, Restore Default Certificates, Import Config, Export Config, and Boot From Other Partition are present.
- Users List:** A table with columns for Username, Home, Device, Network, SIP, SSL, Multicast, Fault, Audiofiles, Events, Terminus, Autoprov, Firmware, and Admin. Buttons for Add New User, Delete All Users, Import Users, and Export Users are located above the table.
- Log Viewer:** A section for viewing logs, featuring a Service dropdown (Application), Entries to get (250), Sort dropdown (Oldest), and a View Log button.

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

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 ^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 call	<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>
Test Relay	<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_relay"</code>
Activate Relay	<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=activate_relay"</code>
Deactivate Relay	<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=deactivate_relay"</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

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