CyberData
The IP Endpoint Company

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

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.

CyberData
The IP Endpoint Company

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

⚠ GENERAL ALERT	General Alert 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.
⏚	Ground This pictorial alert indicates the Earth grounding connection point.

Hazard Levels

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

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

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

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

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

Important Safety Instructions

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

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

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

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

Abbreviations and Terms

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

Contents

Chapter 1 Configure the Device 1

Appendix A Troubleshooting/Technical Support 24

1 Configure the Device

1.1 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

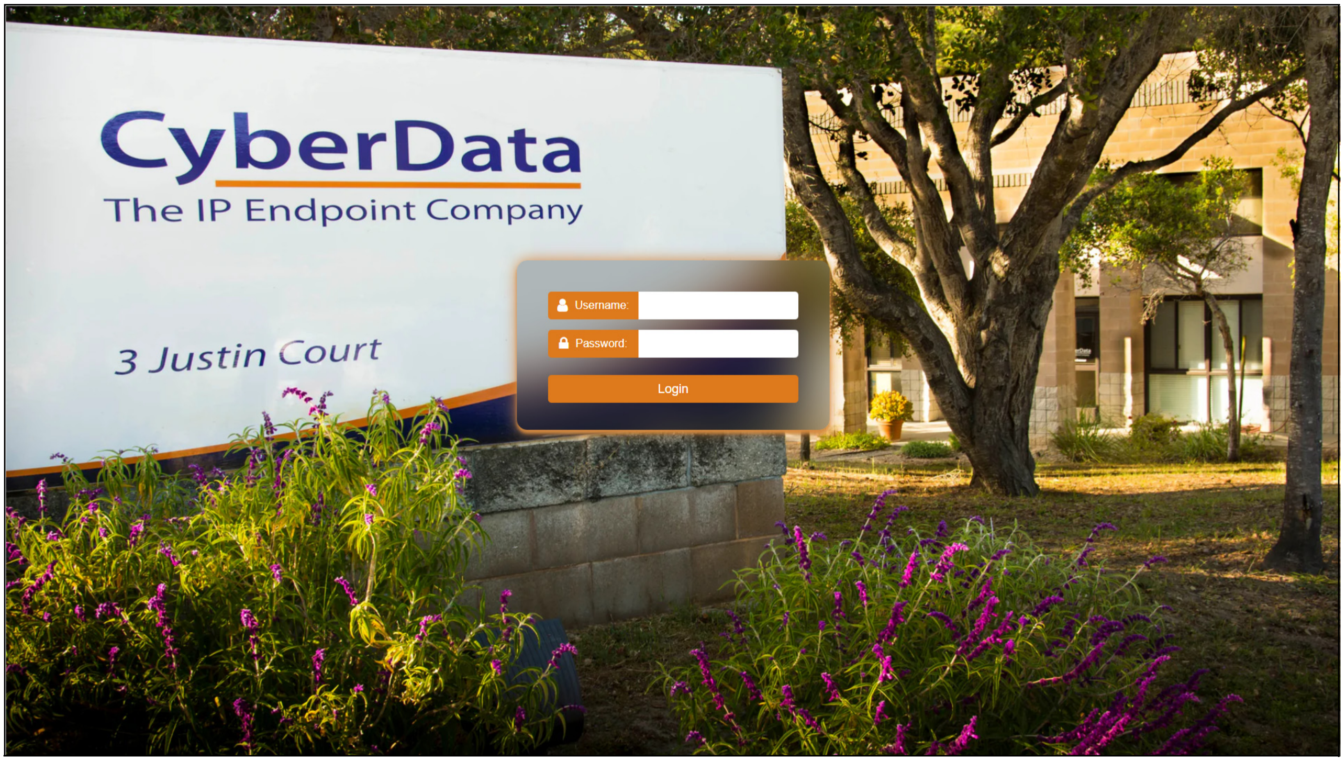
Note The Intercom ships in DHCP mode. To get to the **Home** page, use the discovery utility to scan for the device on the network and open your browser from there.

2. On the Log In Page (Figure 1-1), use the following default **Web Access Username** and **Web Access Password** to access the **Home Page** (Figure 1-3):

   Web Access Username: **admin**

   Web Access Password: **admin**

Figure 1-1. Log In Page



1.1.1 Restoring Defaults and Announcing the IP Address

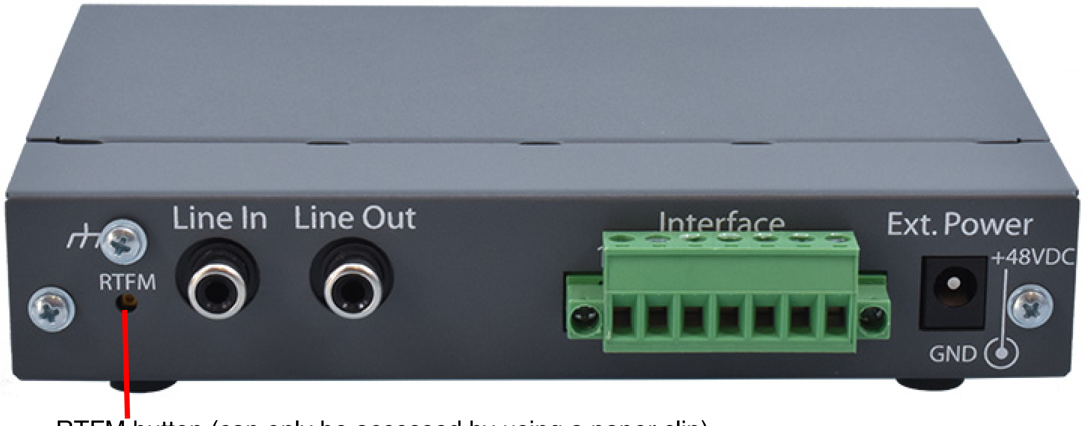
The RTFM button is located on the back of the device.

Briefly pressing the RTFM button (Figure 1-2), 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 1-1), 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 1-2. RTFM Button



RTFM button (can only be accessed by using a paper clip)

Table 1-1. Factory Default Settings

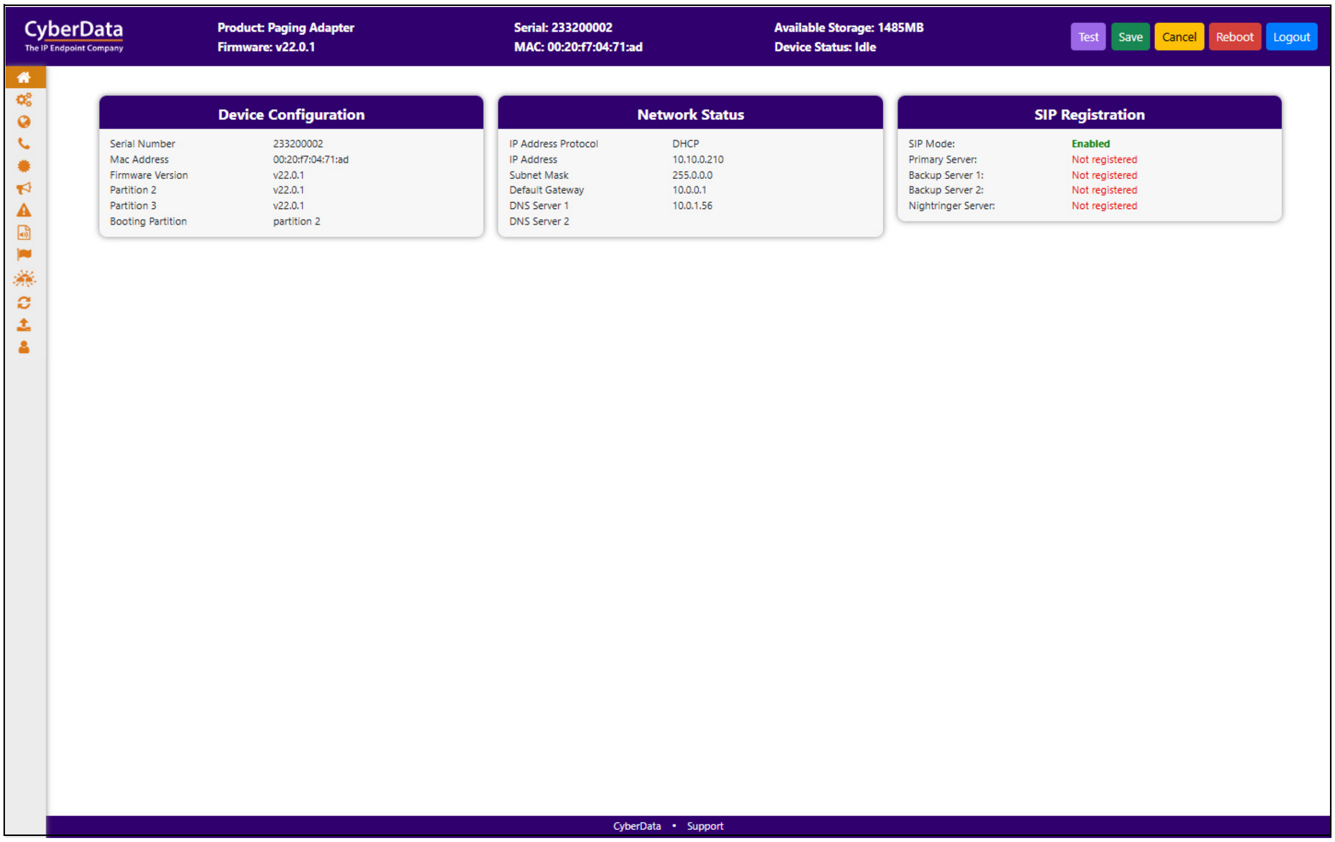
Parameter	Factory Default Setting
IP Addressing	DHCP
IP Address[a]	192.168.1.23
Web Access Username	admin
Web Access Password	admin
Subnet Mask[a]	255.255.255.0
Default Gateway[a]	192.168.1.1

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

1.2 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 1-3. Home Page



Product: Paging Adapter
Firmware: v22.0.1

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

Available Storage: 1485MB
Device Status: Idle

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

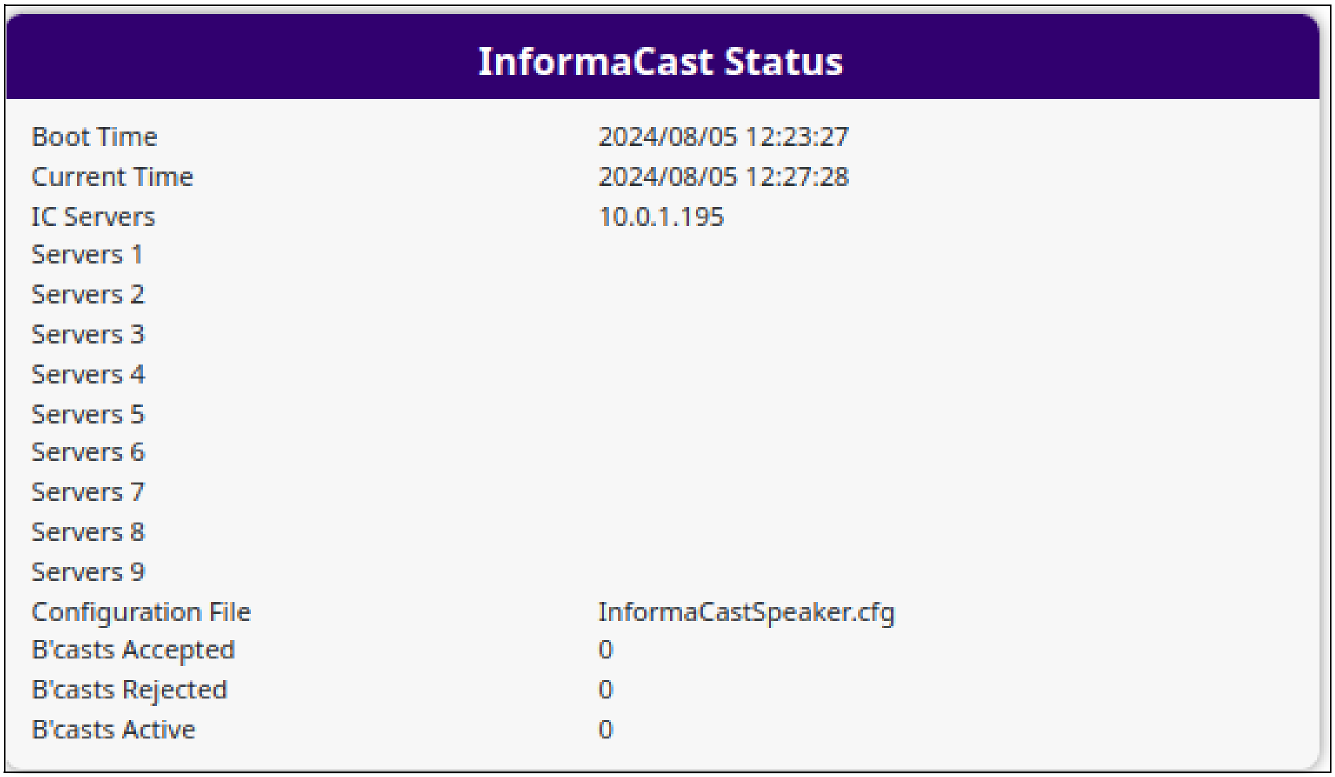
IP Address Protocol	DHCP
IP Address	10.10.0.210
Subnet Mask	255.0.0.0
Default Gateway	10.0.0.1
DNS Server 1	10.0.1.56
DNS Server 2	

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 1-4. InformaCast enabled Device



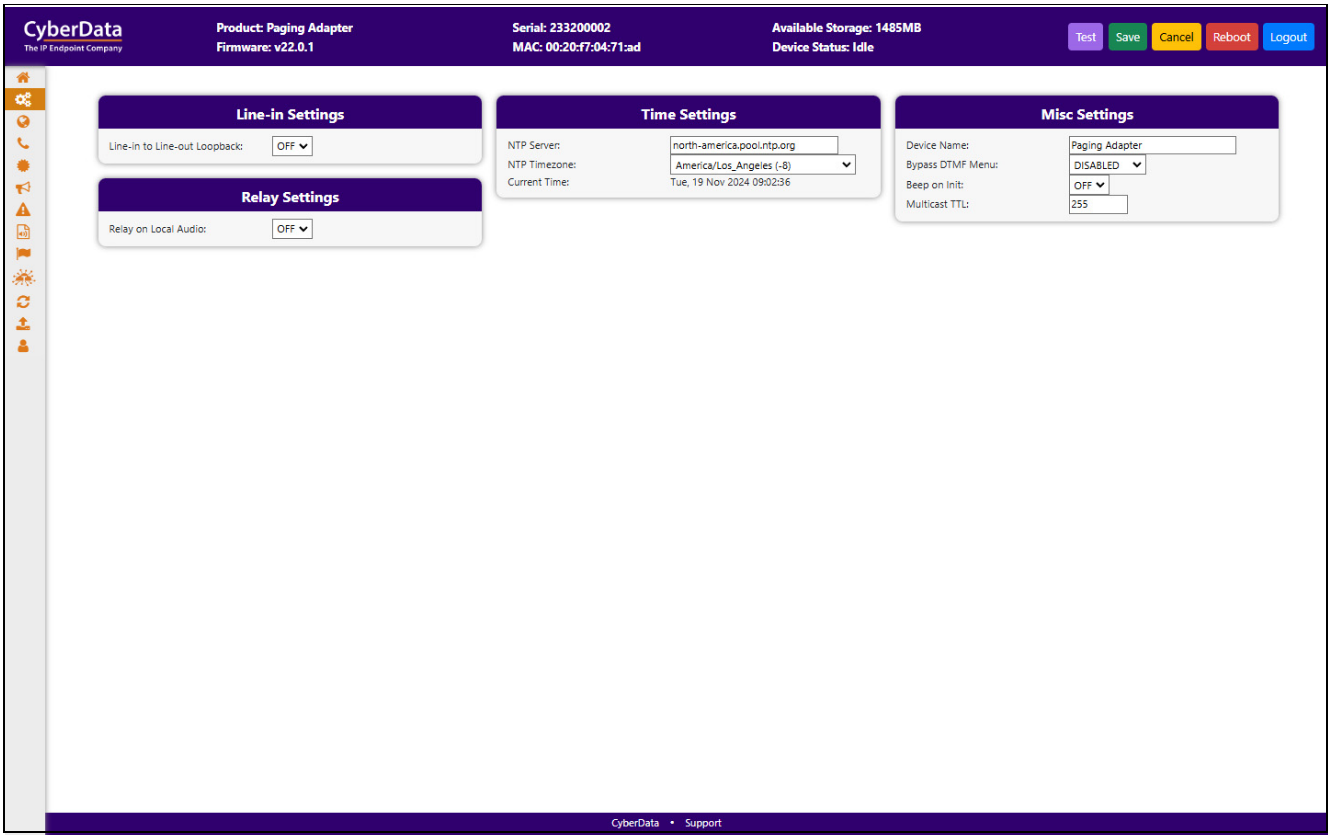
InformaCast Status

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

1.3 Device

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

Figure 1-5. Device Configuration Page



Product: Paging Adapter
Firmware: v22.0.1

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

Available Storage: 1485MB
Device Status: Idle

Line-in Settings

Line-in to Line-out Loopback: OFF

Relay Settings

Relay on Local Audio: OFF

Time Settings

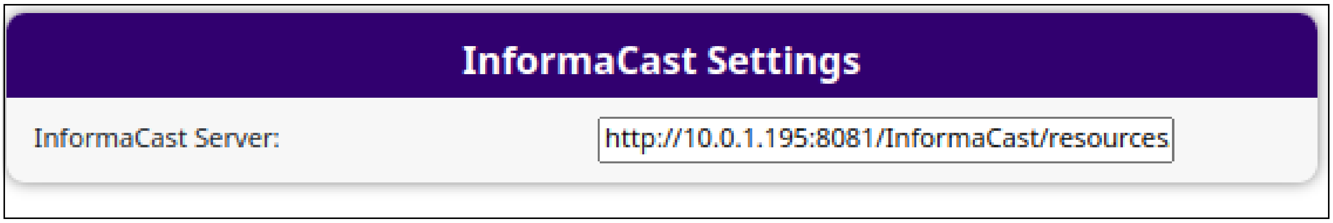
NTP Server: north-america.pool.ntp.org
NTP Timezone: America/Los_Angeles (-8)
Current Time: Tue, 19 Nov 2024 09:02:36

Misc Settings

Device Name: Paging Adapter
Bypass DTMF Menu: DISABLED
Beep on Init: OFF
Multicast TTL: 255

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

Figure 1-6. InformaCast enabled Device



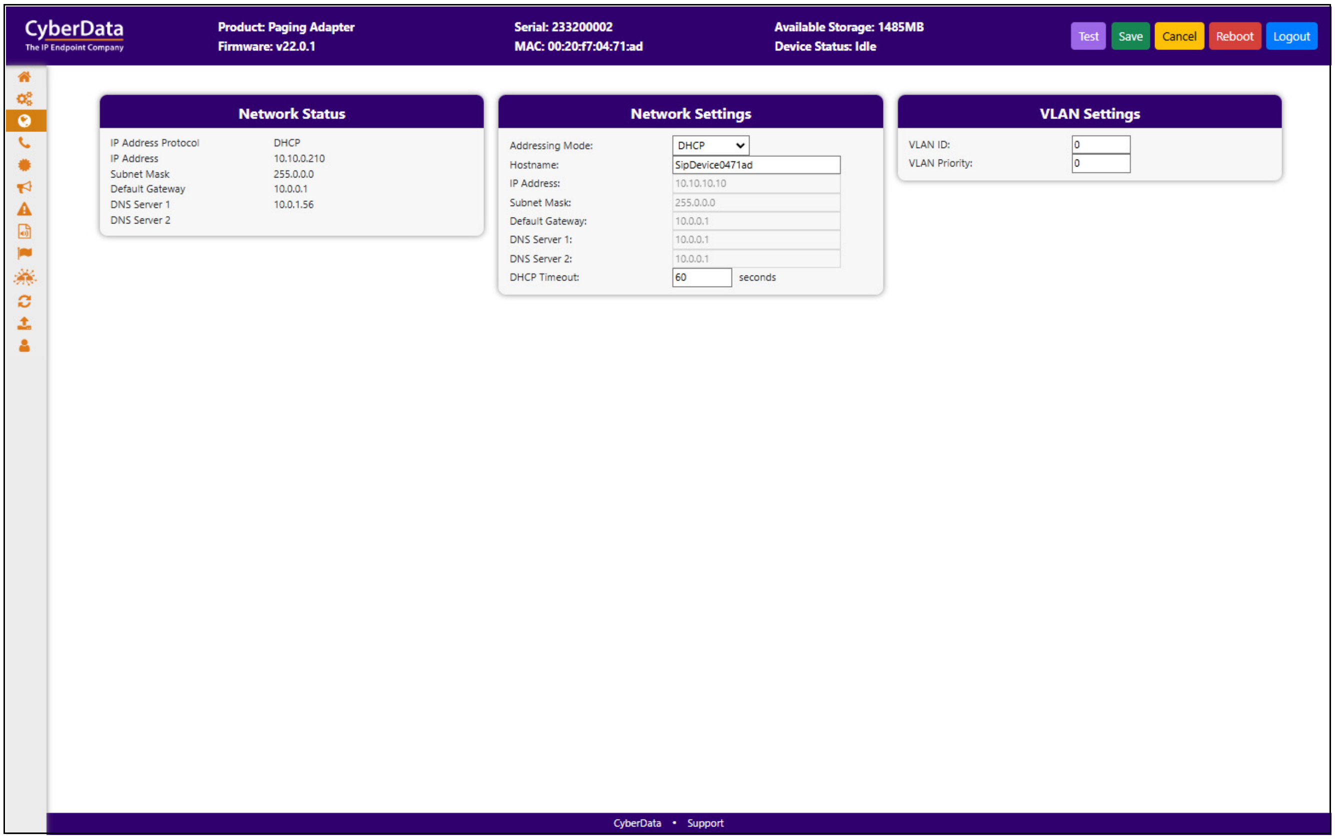
InformaCast Settings

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

1.4 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 1-7. Network Page



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

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

1.5 SIP (Session Initiation Protocol)

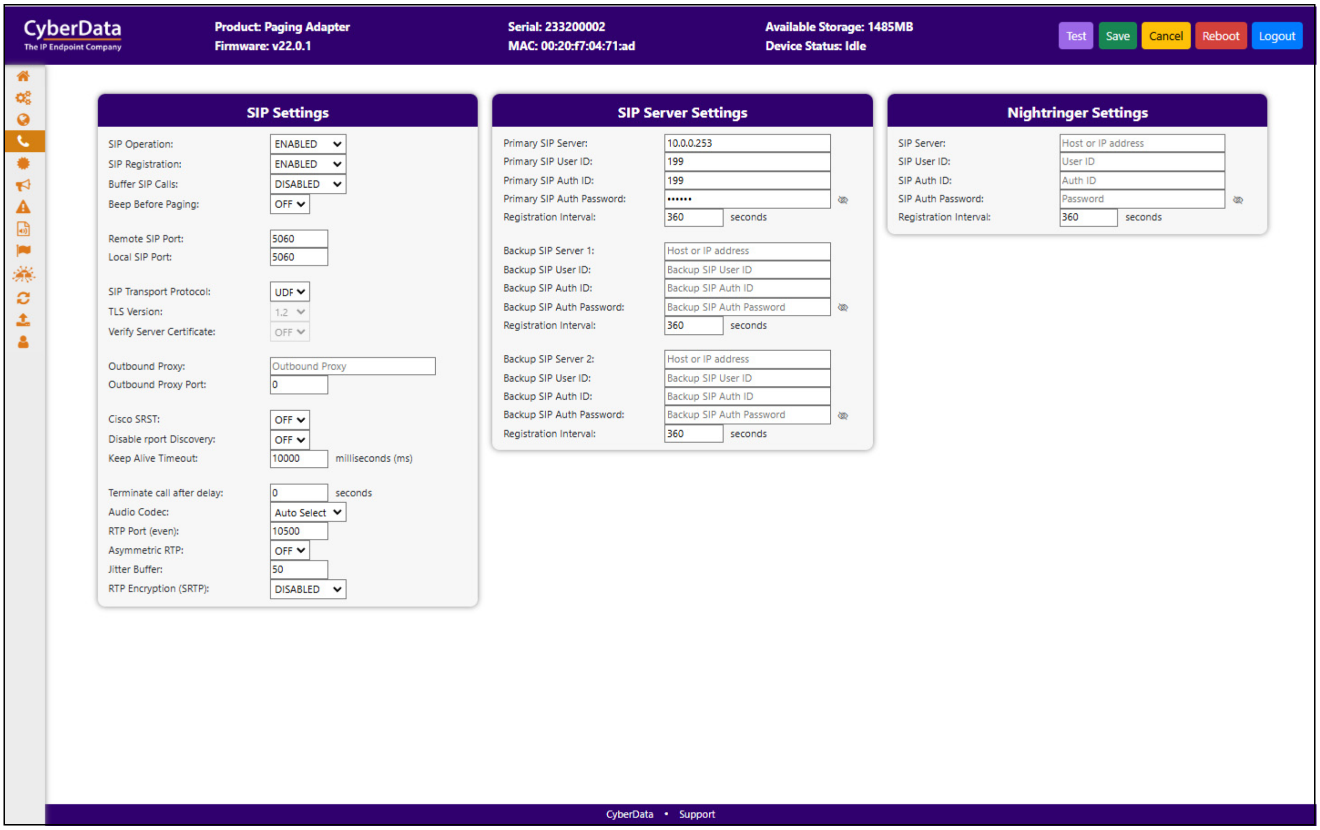
This page sets the options for phone calls. Configure up to 3 servers, with 2 acting as backup, and a server for the nightringer. The nightringer is a second sip extension that only rings, never connects to a call. Many customers use the nightringer in a hunt group.

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 1-8. SIP Page



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

SIP Settings

SIP Operation:	ENABLED	
SIP Registration:	ENABLED	
Buffer SIP Calls:	DISABLED	
Beep Before Paging:	OFF	
Remote SIP Port:	5060	
Local SIP Port:	5060	
SIP Transport Protocol:	UDP	
TLS Version:	1.2	
Verify Server Certificate:	OFF	
Outbound Proxy:	Outbound Proxy	
Outbound Proxy Port:	0	
Cisco SRST:	OFF	
Disable rport Discovery:	OFF	
Keep Alive Timeout:	10000	milliseconds (ms)
Terminate call after delay:	0	seconds
Audio Codec:	Auto Select	
RTP Port (even):	10500	
Asymmetric RTP:	OFF	
Jitter Buffer:	50	
RTP Encryption (SRTP):	DISABLED	

SIP Server Settings

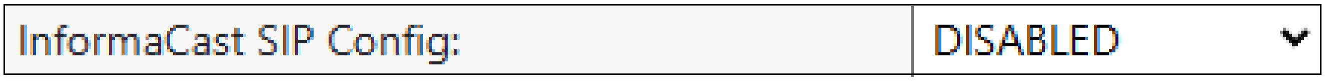
Primary SIP Server:	10.0.0.253	
Primary SIP User ID:	199	
Primary SIP Auth ID:	199	
Primary SIP Auth Password:	••••••	
Registration Interval:	360	seconds
Backup SIP Server 1:	Host or IP address	
Backup SIP User ID:	Backup SIP User ID	
Backup SIP Auth ID:	Backup SIP Auth ID	
Backup SIP Auth Password:	Backup SIP Auth Password	
Registration Interval:	360	seconds
Backup SIP Server 2:	Host or IP address	
Backup SIP User ID:	Backup SIP User ID	
Backup SIP Auth ID:	Backup SIP Auth ID	
Backup SIP Auth Password:	Backup SIP Auth Password	
Registration Interval:	360	seconds

Nightringer Settings

SIP Server:	Host or IP address	
SIP User ID:	User ID	
SIP Auth ID:	Auth ID	
SIP Auth Password:	Password	
Registration Interval:	360	seconds

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

Figure 1-9. InformaCast enabled Device



InformaCast SIP Config:	DISABLED

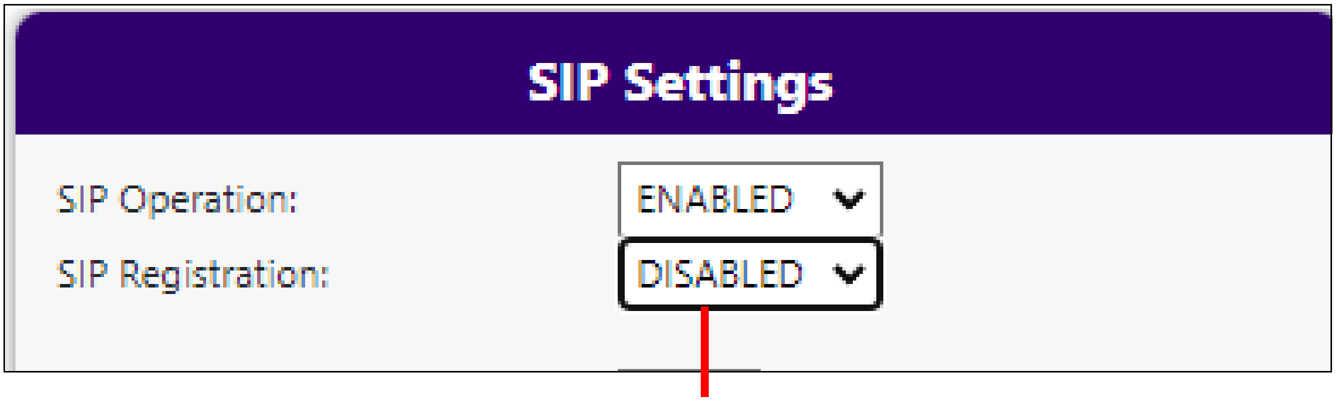
1.5.1 Dial Out Extension Strings and DTMF Tones (using rfc2833)

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

1.5.2 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 1-10.

Figure 1-10. SIP Page Set to Point-to-Point Mode



SIP Settings

SIP Operation: ENABLED

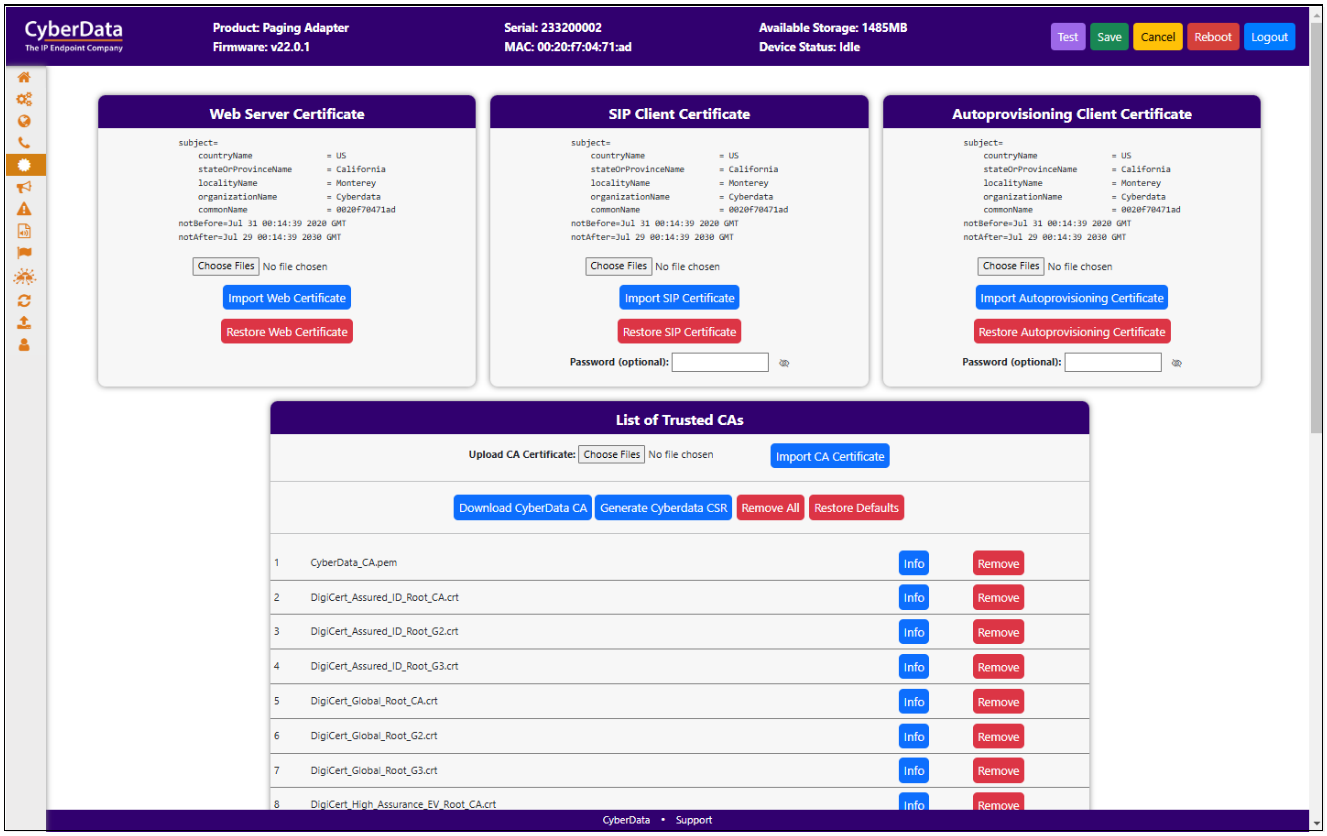
SIP Registration: DISABLED

Device is set to NOT register with a SIP server

1.6 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 1-11. SSL Page (1 of 2)



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

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
```

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
```

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

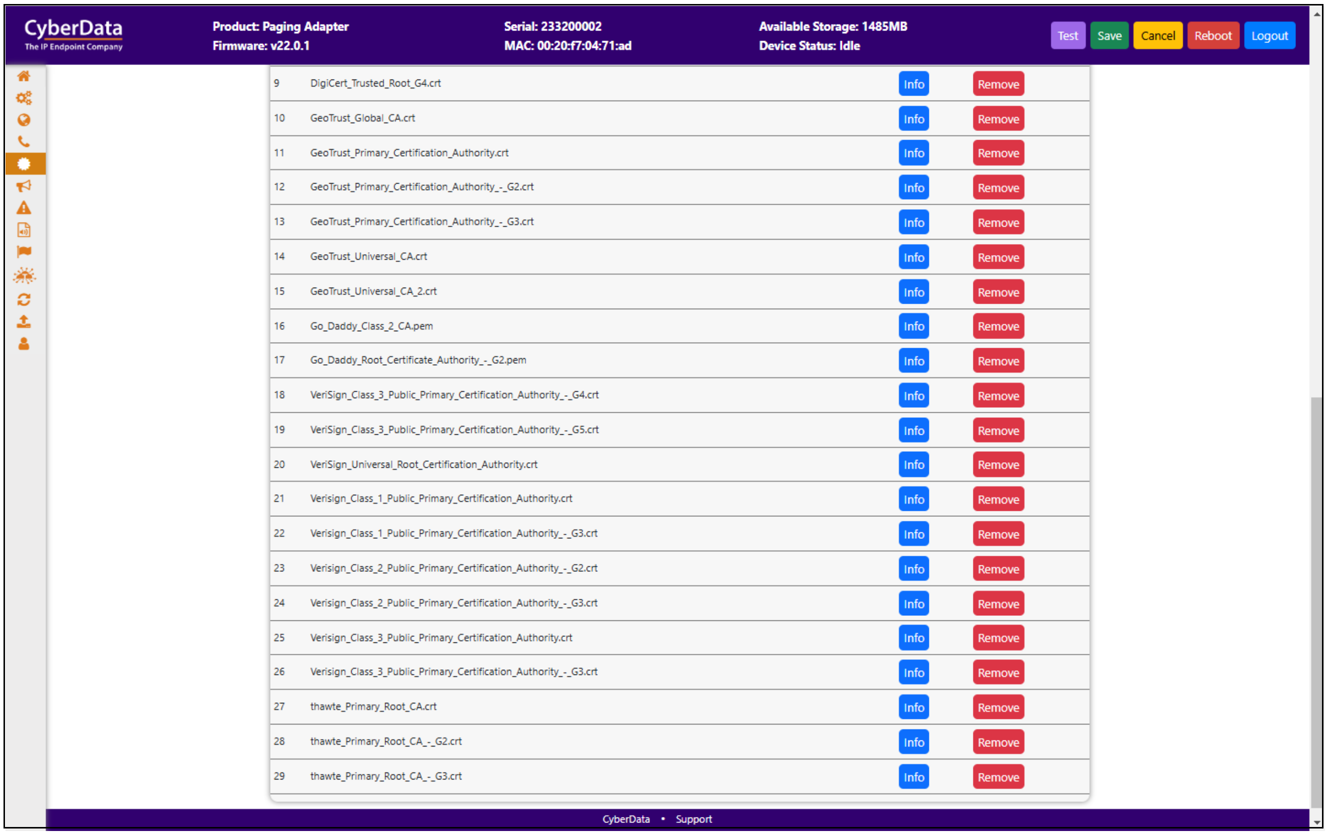
Password (optional):

List of Trusted CAs

Upload CA Certificate:

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

Figure 1-12. SSL Page (2 of 2)



Product: Paging Adapter
Firmware: v22.0.1

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

Available Storage: 1485MB
Device Status: Idle

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

1.7 Multicast

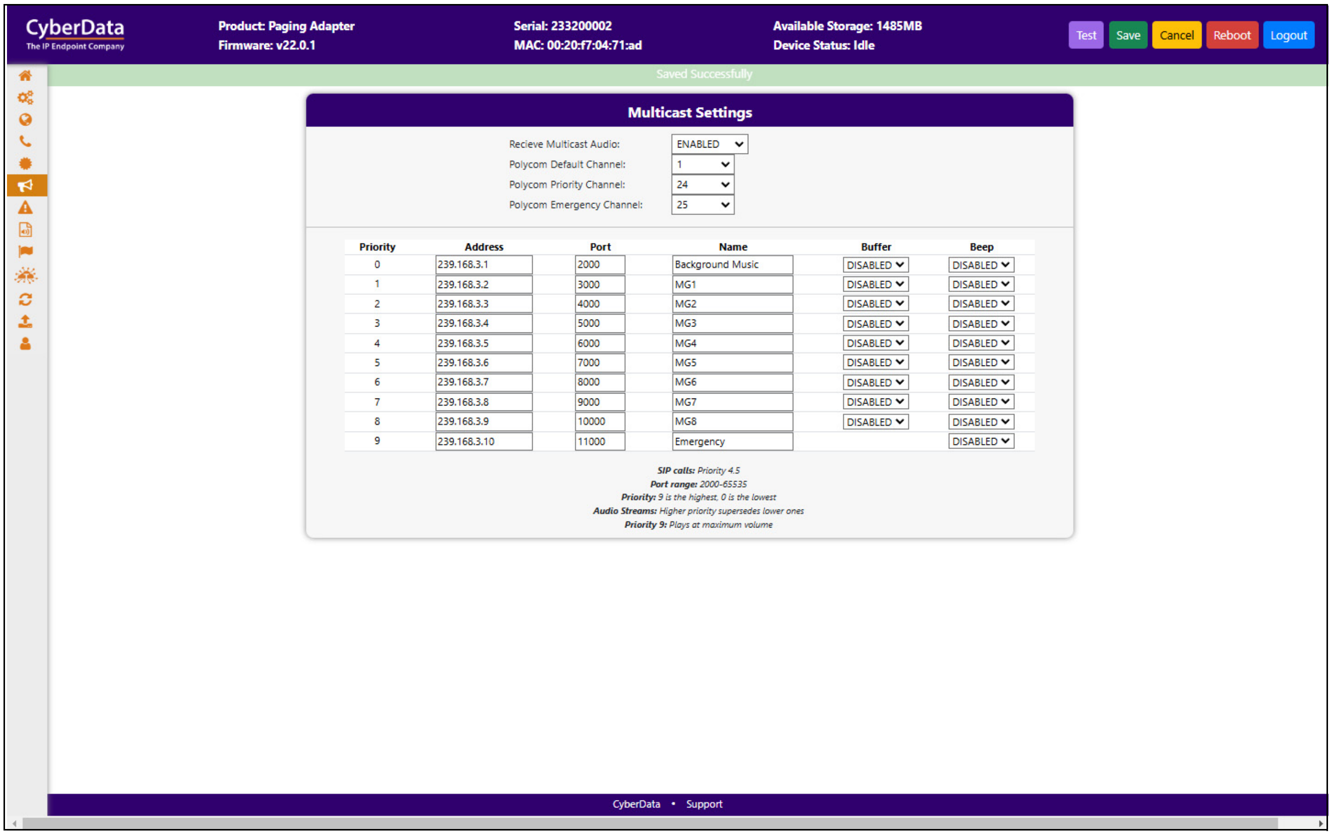
The Multicast Configuration page allows the device to join up to ten paging zones for receiving RTP audio streams. A paging zone can consist of one or many CyberData multicast group-enabled products. There is no limit to how many speakers can participate in a given paging zone. Each multicast group is 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 1-13. Multicast Page



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

Saved Successfully

Multicast Settings

Recieve Multicast Audio: ENABLED
Polycom Default Channel: 1
Polycom Priority Channel: 24
Polycom Emergency Channel: 25

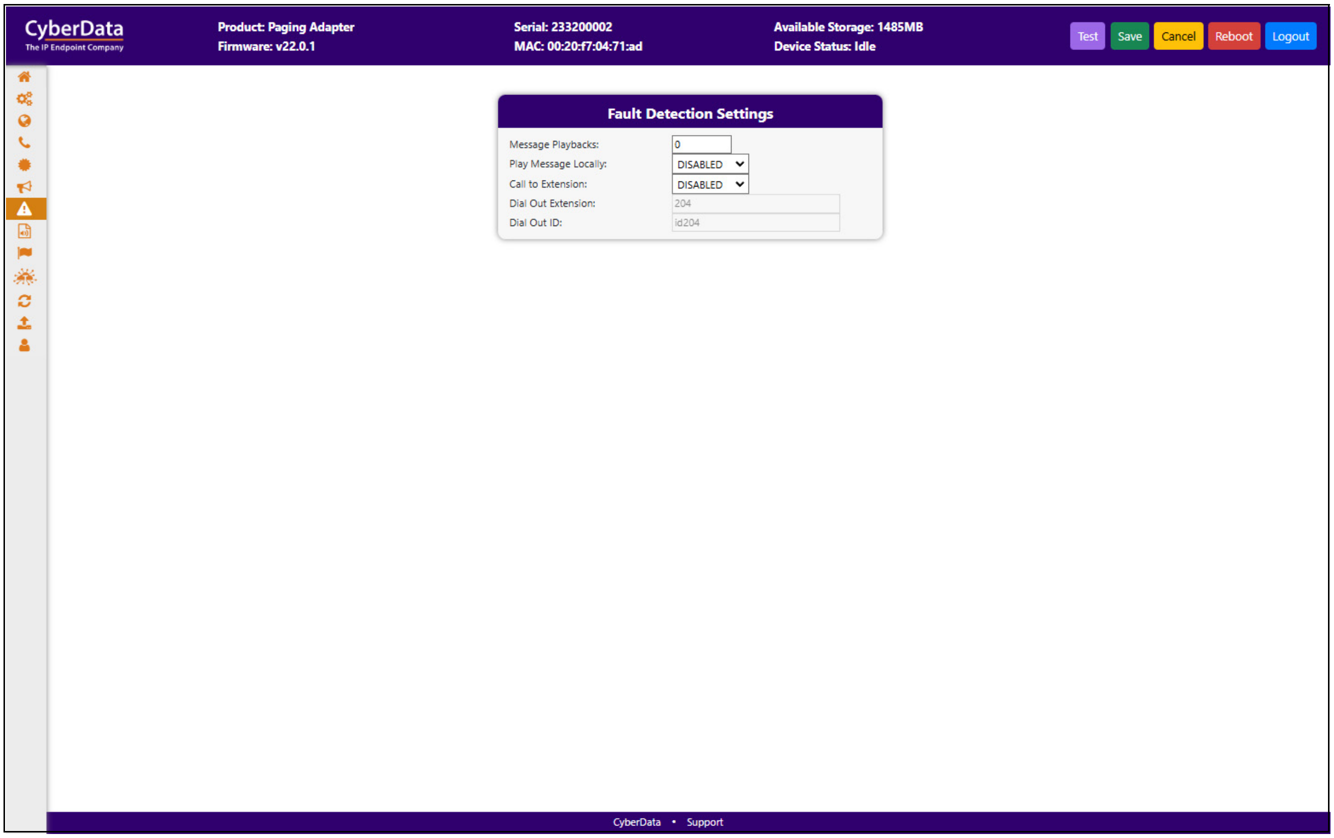
Priority	Address	Port	Name	Buffer	Beep
0	239.168.3.1	2000	Background Music	DISABLED	DISABLED
1	239.168.3.2	3000	MG1	DISABLED	DISABLED
2	239.168.3.3	4000	MG2	DISABLED	DISABLED
3	239.168.3.4	5000	MG3	DISABLED	DISABLED
4	239.168.3.5	6000	MG4	DISABLED	DISABLED
5	239.168.3.6	7000	MG5	DISABLED	DISABLED
6	239.168.3.7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

1.8 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 1-14. Fault Page



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

Fault Detection Settings

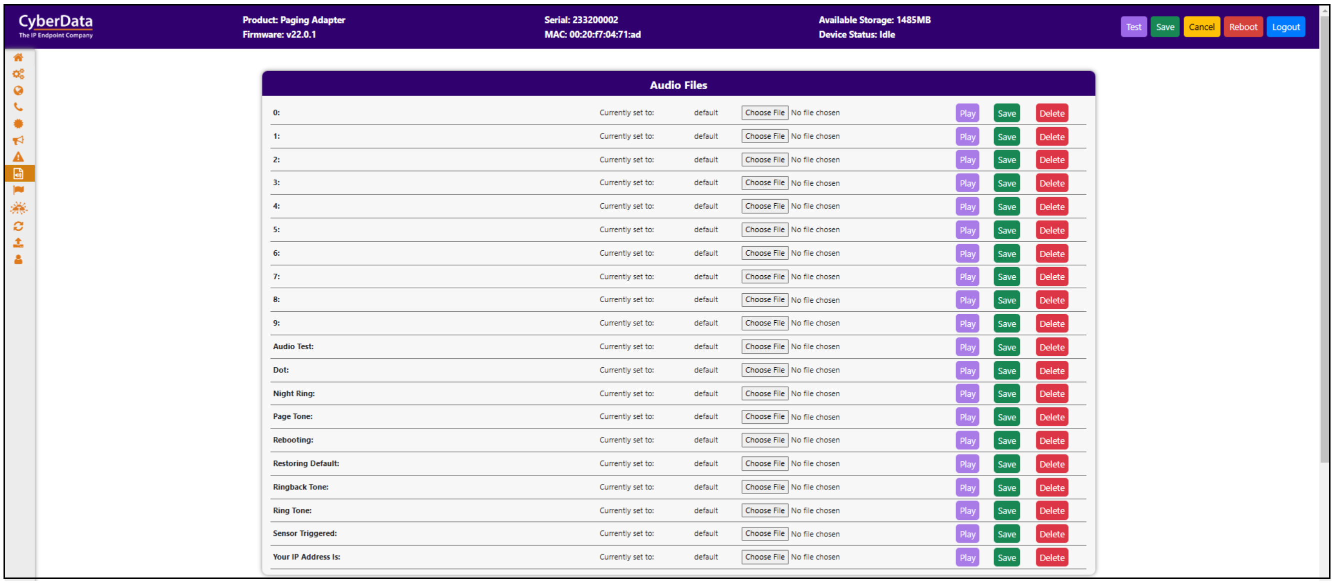
Message Playbacks:	0
Play Message Locally:	DISABLED
Call to Extension:	DISABLED
Dial Out Extension:	204
Dial Out ID:	id204

1.9 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 1-15. Audiofiles Page (1 of 3)



CyberData
The IP Endpoint Company

Product: Paging Adapter
Firmware: v22.0.1

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

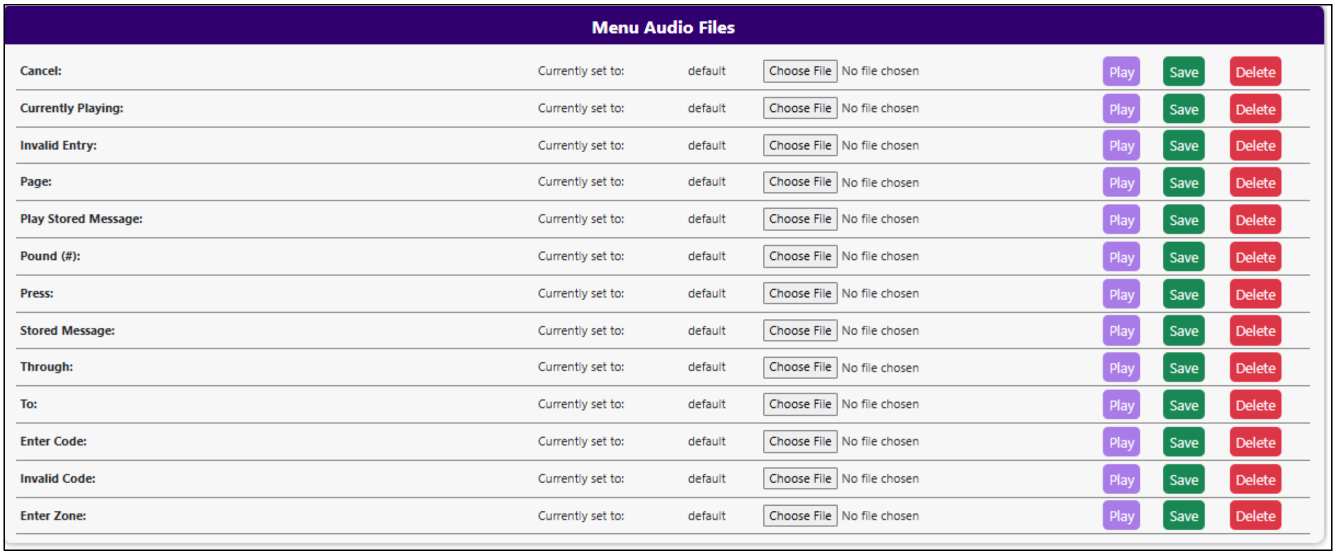
Available Storage: 1485MB
Device Status: Idle

Test Save Cancel Reboot Logout

Audio Files

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

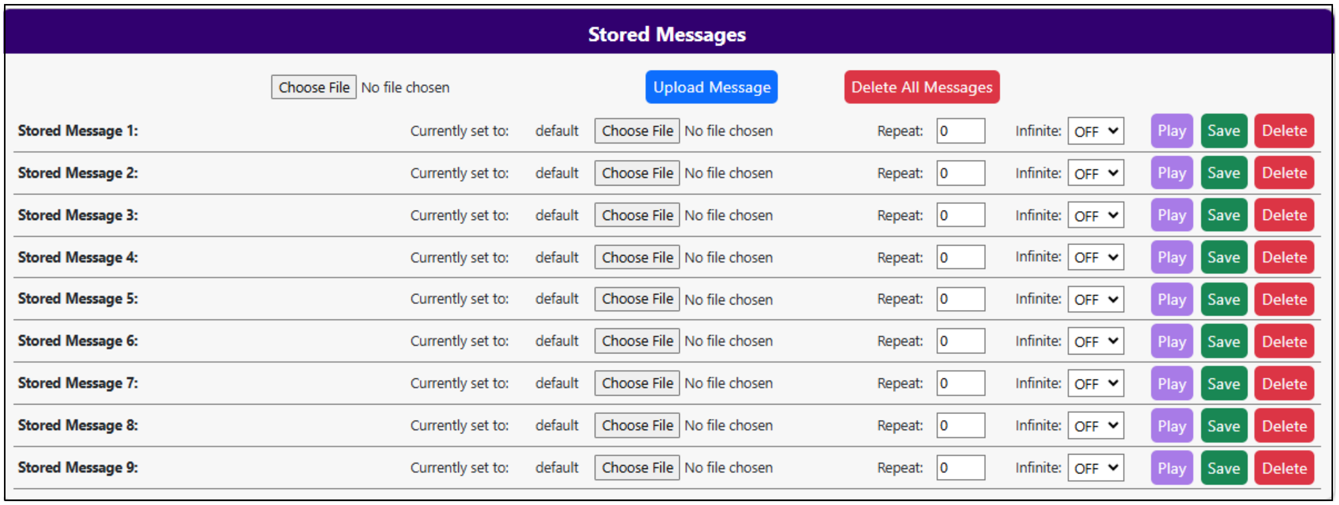
Figure 1-16. Audiofiles Page (2 of 3)



Menu Audio Files

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

Figure 1-17. Audiofiles Page (3 of 3)



Stored Messages

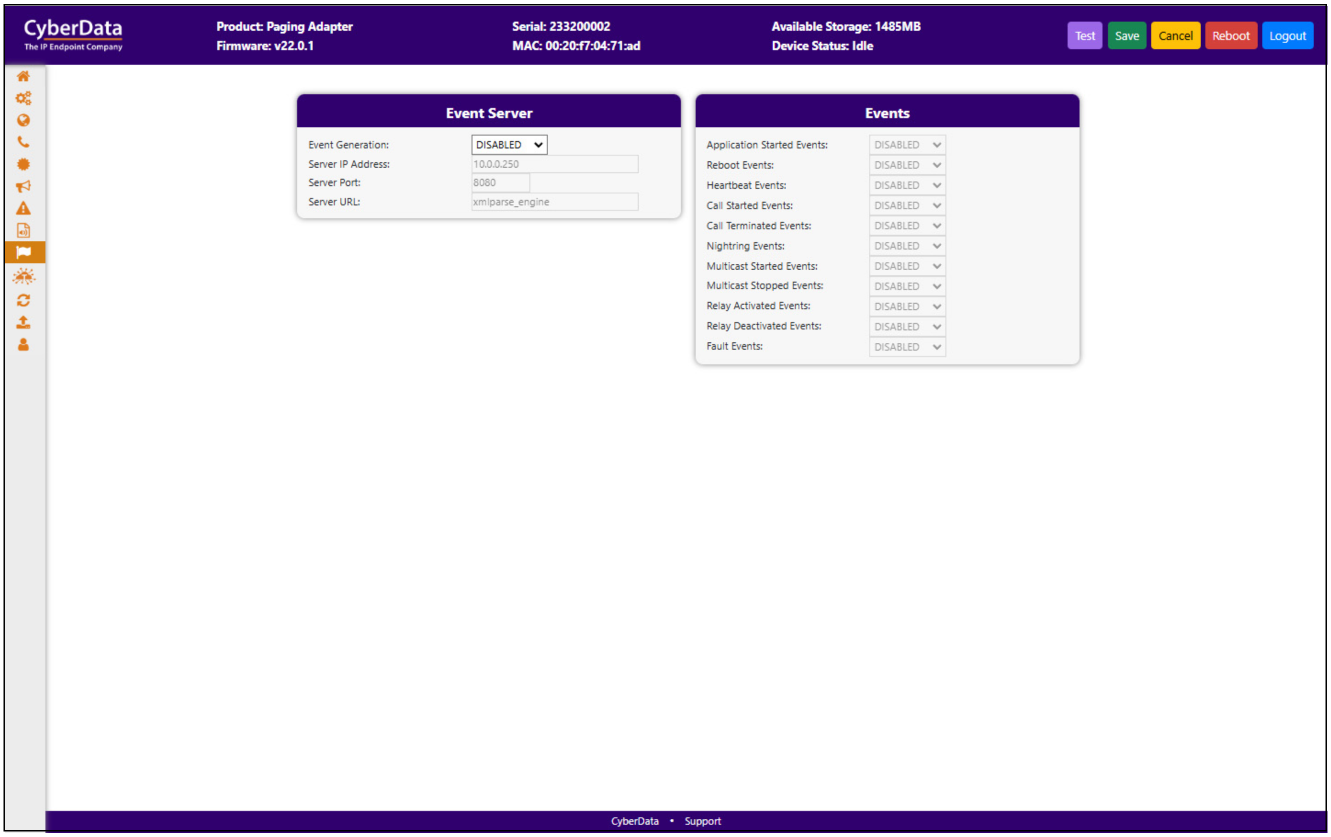
Choose File No file chosen Upload Message Delete All Messages

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

1.10 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 1-18. Events Page



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

Event Server

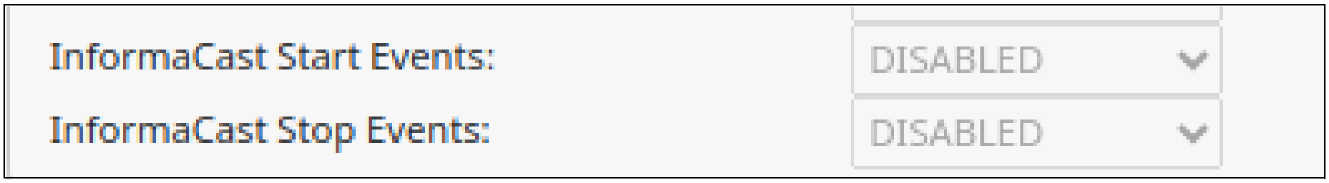
Event Generation: DISABLED
Server IP Address: 10.0.0.250
Server Port: 8080
Server URL: xmlparse_engine

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

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

Figure 1-19. InformaCast enabled Device



InformaCast Start Events: DISABLED
InformaCast Stop Events: DISABLED

1.10.0.1 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
```

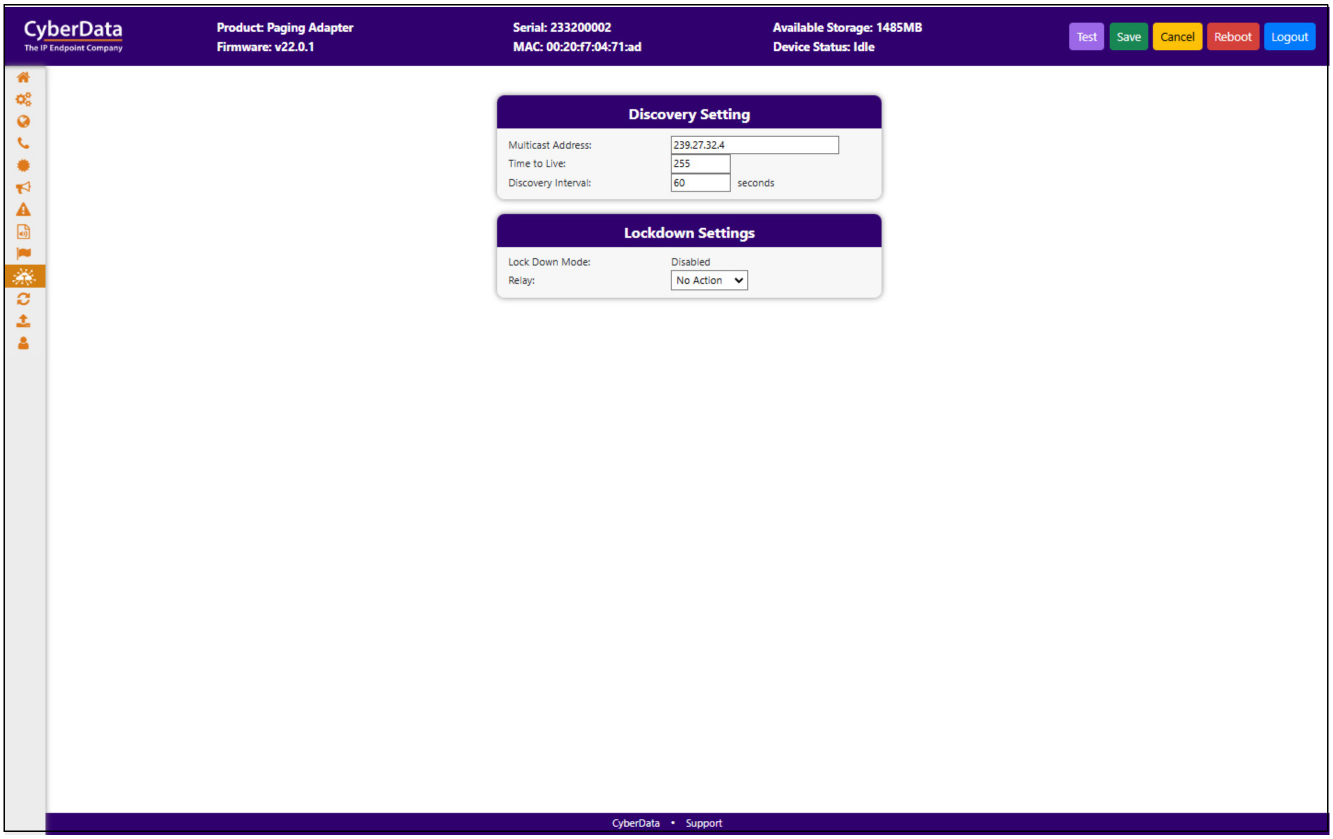
```
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>RELAY_DEACTIVATED</event>
</cyberdata>

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>
```

1.11 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 1-20. Terminus Page



Product: Paging Adapter
Firmware: v22.0.1

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

Available Storage: 1485MB
Device Status: Idle

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

1.12 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.

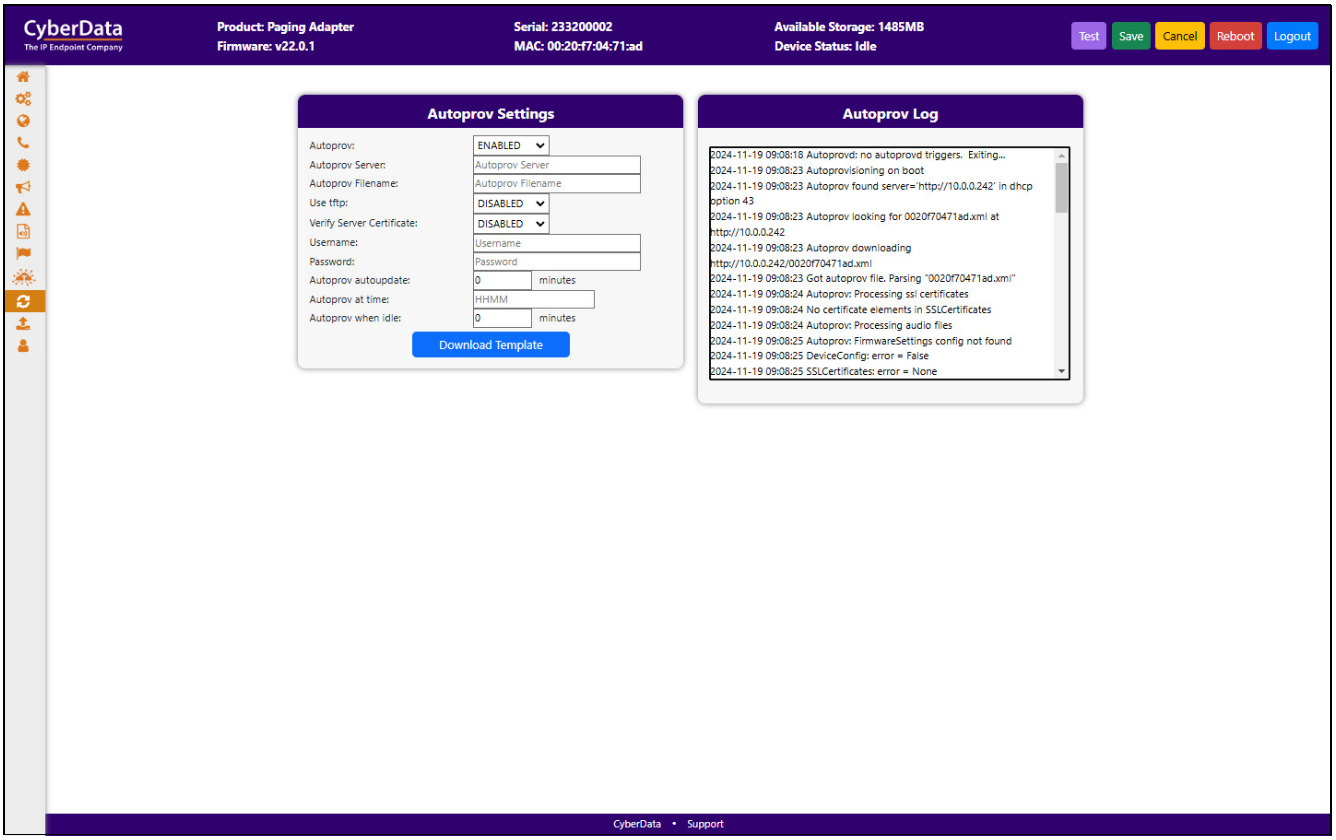
If a file is named, it will be downloaded instead of <mac address>.xml.

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 1-21. Autoprovisioning Page



Product: Paging Adapter
Firmware: v22.0.1

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

Available Storage: 1485MB
Device Status: Idle

Autoprov Settings

Autoprov:	ENABLED
Autoprov Server:	Autoprov Server
Autoprov Filename:	Autoprov Filename
Use tftp:	DISABLED
Verify Server Certificate:	DISABLED
Username:	Username
Password:	Password
Autoprov autoupdate:	0 minutes
Autoprov at time:	HHMM
Autoprov when idle:	0 minutes

Autoprov Log

```
2024-11-19 09:08:18 Autoprovd: no autoprovd triggers.  Exiting...
2024-11-19 09:08:23 Autoprovisioning 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
```

1.13 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:

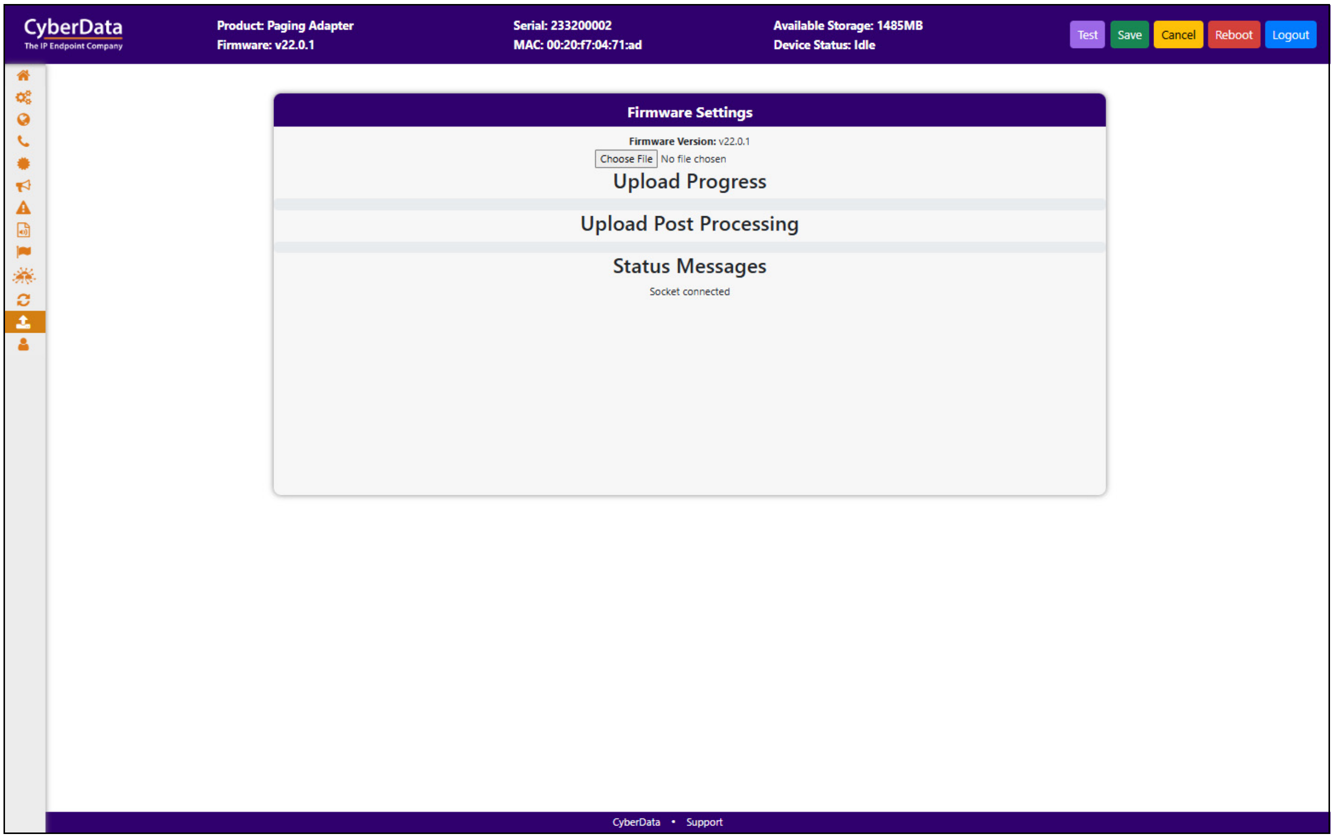
- Firmware file
- Release notes
- Autoprovisioning template

GENERAL ALERT

Caution

Equipment Hazard: Do not reboot the device. It will reboot automatically when the process is complete.

Figure 1-22. Firmware Page



Product: Paging Adapter
Firmware: v22.0.1

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

Available Storage: 1485MB
Device Status: Idle

Firmware Settings

Firmware Version: v22.0.1

Choose File No file chosen

Upload Progress

Upload Post Processing

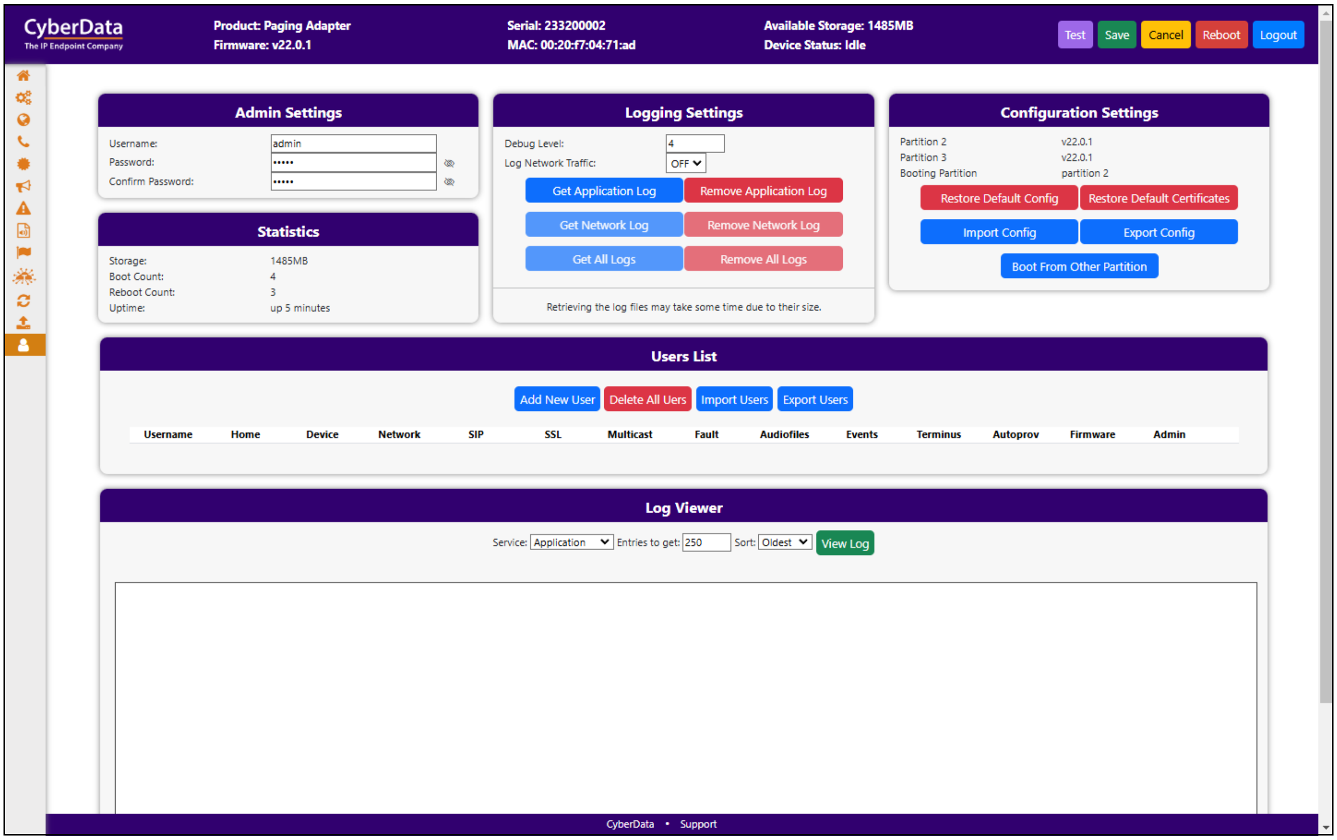
Status Messages

Socket connected

1.14 Admin

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

Figure 1-23. Admin Page



Product: Paging Adapter
Firmware: v22.0.1

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

Available Storage: 1485MB
Device Status: Idle

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

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

Users List

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

Log Viewer

Service: Application Entries to get: 250 Sort: Oldest

1.15 Command Interface

Some functions on the device can be activated using simple POST commands to the web interface. The examples in Table 1-2 use the free unix utility, **wget commands**. However, any program that can send HTTP POST commands to the device should work.

1.15.1 Command Interface Post Commands

The commands in Table 1-2 require an authenticated session (a valid username and password to work).

Table 1-2. Command Interface Post Commands

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

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

Appendix A: Troubleshooting/Technical Support

A.1 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