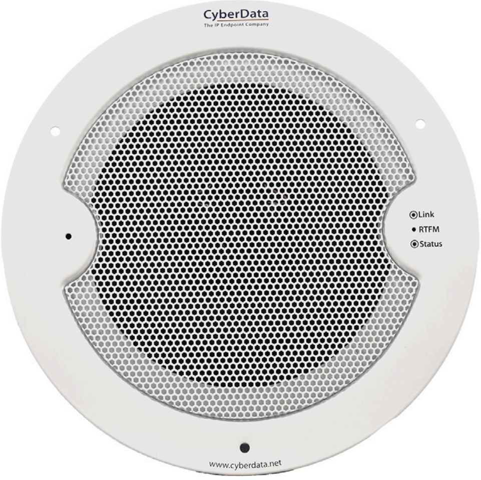
CyberData
The IP Endpoint Company



Speakers with Talk-Back Operations Guide

SIP Compliant
Part #011394, 011396

Document Part #*932055B*
for Firmware Version *23.0*

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

CyberData Speakers with Talk-Back Operations Guide 932055B
Part # 011394, 011396

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 932055B, which corresponds to firmware version 23.0.0, was released on January 25, 2026, and has the following changes:

- Adds Appendix A.3 Electrostatic Discharge (ESD) Sensitivity

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.

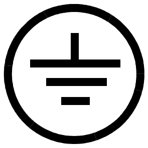
14. **WARNING: The Intercom enclosure is not rated for any AC voltages!**

⚠ 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.

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.

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. Installing the Speaker with Talk-Back

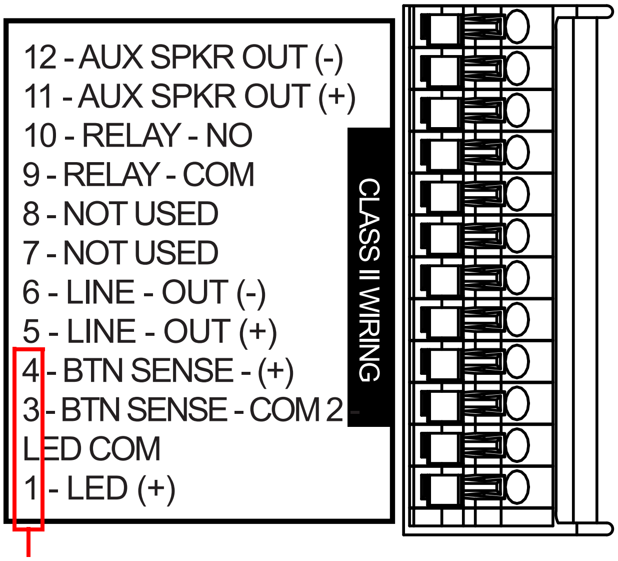
The installation template for the Speaker with Talk-Back is located on the Installation Quick Reference Guide that is included in the packaging with each Speaker.

Additional connections options are shown below.

1.1 Optional Connections

Figure 1. Optional Connections

Function	Connections
Auxiliary 8-Ohm speaker connection (not to be used when the Clock is connected)	**AUX SPEAKER OUT(-)** **AUX SPEAKER OUT(+)**
Relay contacts rated at 30 VDC @ 1A.	**RELAY NO** **RELAY COM**
NOT USED	**LINE IN (+)** **LINE IN (-)**
Audio line - level output to external audio amplifier. 2v P-P into 10k Ohms.	**LINE OUT (-)** **LINE OUT (+)**
Button positive sense connection Button negative sense connection	**SENSE (+)** **SENSE- COM**
LED negative connection LED positive connection	**LED COM** **LED (+)**

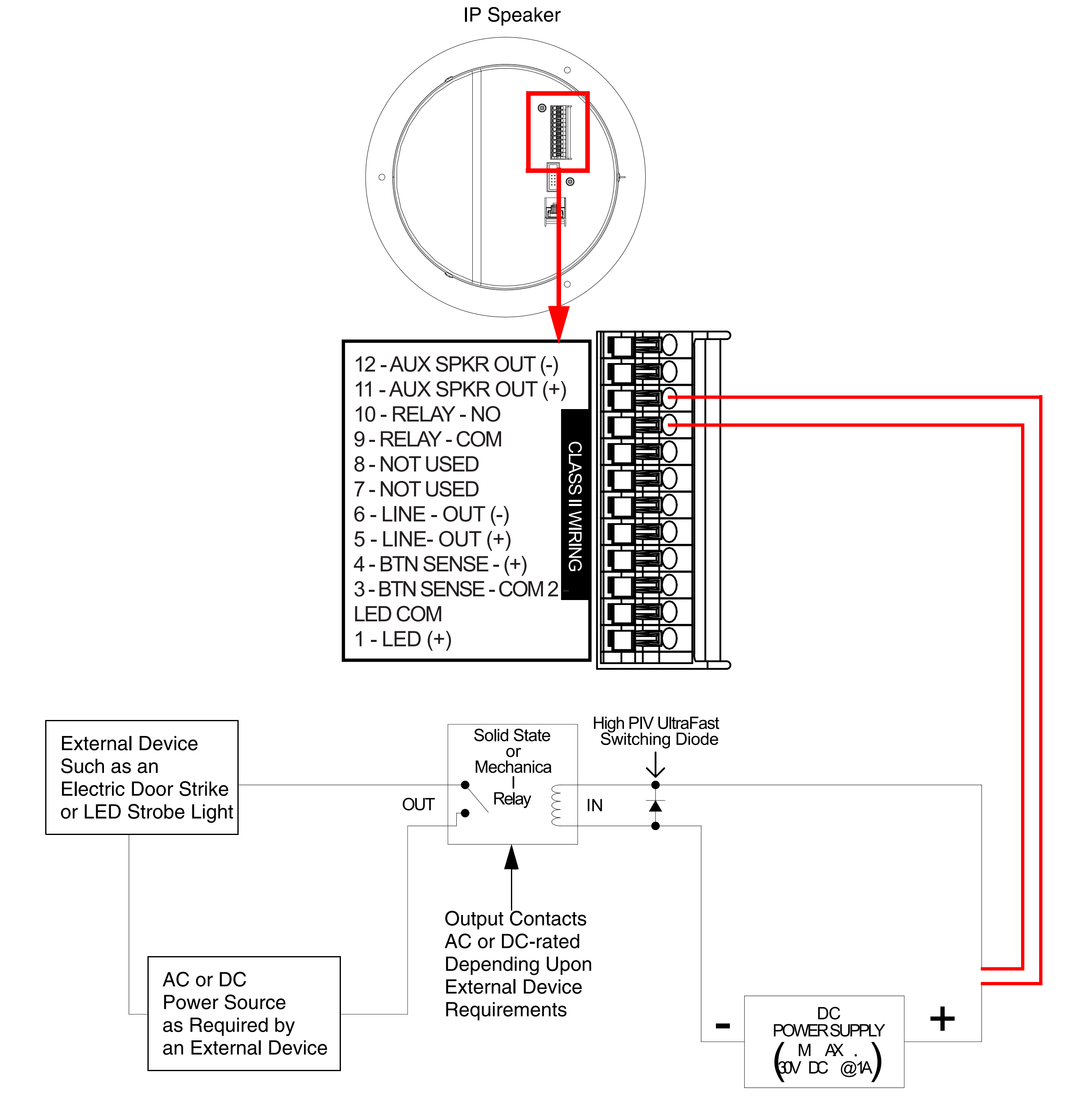


Connections 1 through 4 are intended for use with the **011508 Remote Call Button**

1.2 Speaker with Talk-Back with an External Device

In Figure 2, when the Speaker with Talk-Back is called from a remote phone, the relay on the speaker can be programmed to drive an external device such as an alert strobe. This external device may also be addressed from a separate Unified Communication (UC) server.

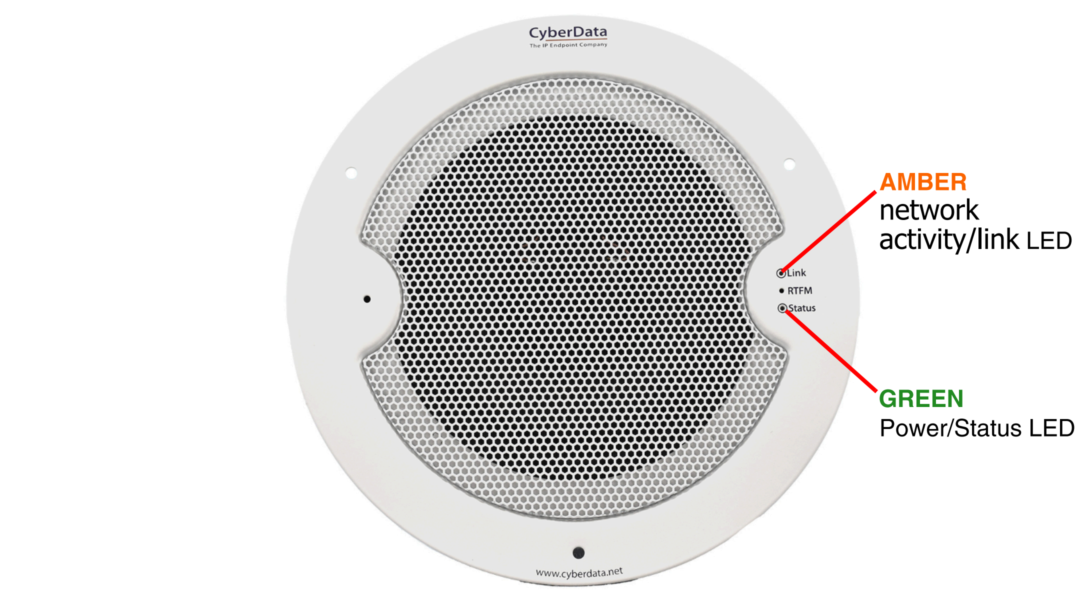
Figure 2. SIP Speaker with Talk-Back with an External Device


IP Speaker
12 - AUX SPKR OUT (-)
11 - AUX SPKR OUT (+)
10 - RELAY - NO
9 - RELAY - COM
8 - NOT USED
7 - NOT USED
6 - LINE - OUT (-)
5 - LINE- OUT (+)
4 - BTN SENSE - (+)
3 - BTN SENSE - COM 2
LED COM
1 - LED (+)
CLASS II WIRING
External Device Such as an Electric Door Strike or LED Strobe Light
Solid State or Mechanica l Relay
OUT
IN
High PIV UltraFast Switching Diode
Output Contacts AC or DC-rated Depending Upon External Device Requirements
AC or DC Power Source as Required by an External Device
-
DC POWER SUPPLY (MAX. 30V DC @1A)
+

1.3 Confirm that the Speaker is Operational and Linked to the Network

After connecting the speaker to the 802.3af compliant Ethernet hub, the LEDs on the speaker face confirm that the speaker is operational and linked to the network.

Figure 3. Status and Activity LEDs



1.3.1 Status LED

After supplying power to the speaker:

1. The green power/status LED and the amber network activity/link LED comes on immediately.
2. After about 23 seconds with a static IP address (or 27 seconds if the board is set to use DHCP), the green LED will blink twice to indicate that the board is fully booted. The speaker will beep at this time if the Beep on Init option is enabled on the Device Page (see Section 2.3, "Device").

Note If the board is set to use DHCP and there is not a DHCP server available on the network, it will try 12 times with a three second delay between tries and eventually fall back to the programmed static IP address (by default 192.168.1.23). This process will take approximately 80 seconds.

Note The front power/status LED will remain solid on during operation.

1.3.2 Link LED

- The Link LED is illuminated when the network link to the speaker is established.
- The Link LED blinks to indicate network traffic.

Chapter 2. Configure the Device

2.1 Log In Page

1. Open your browser to the Intercom 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 Intercom.

   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

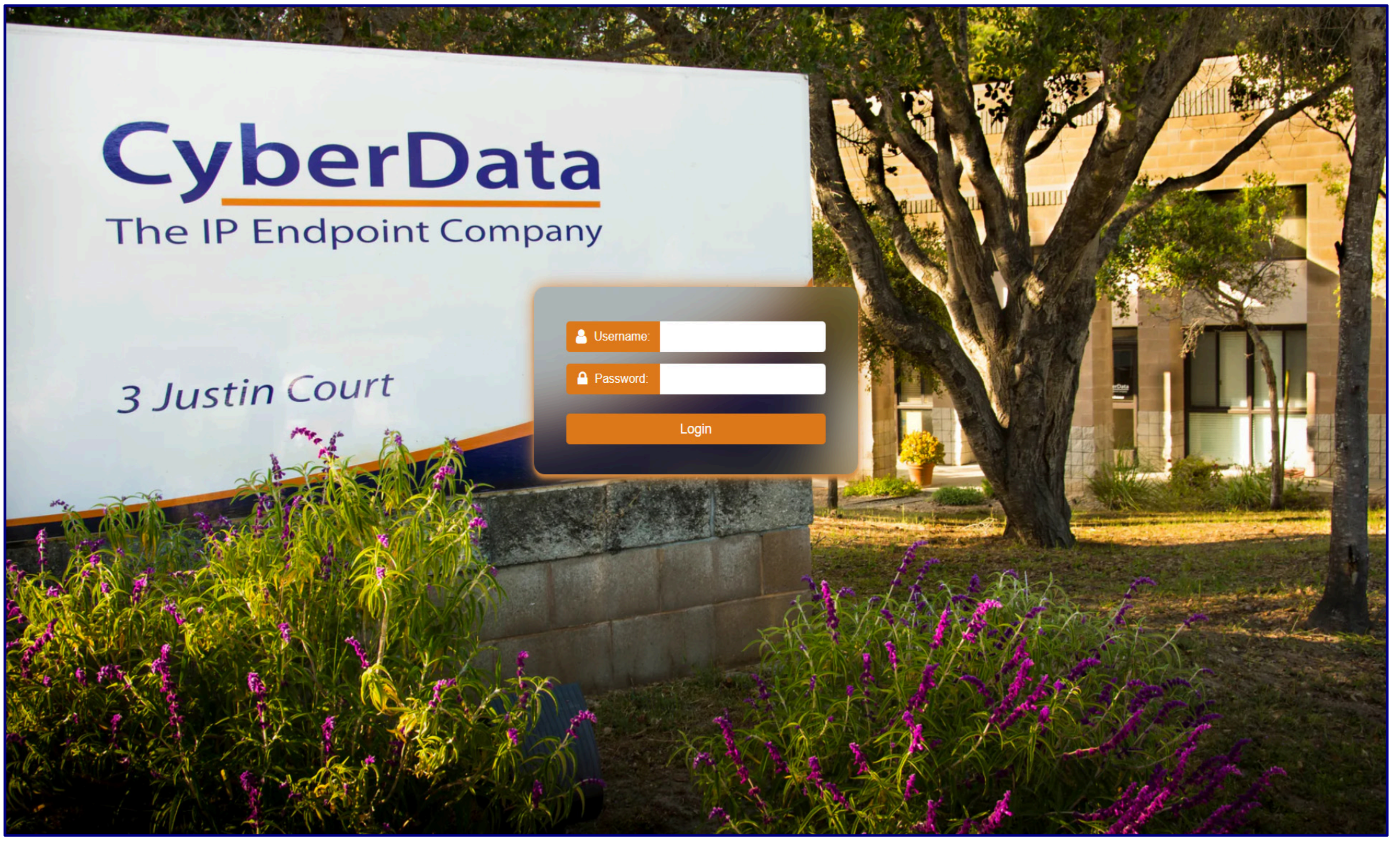
   Note The Intercom ships in DHCP mode. To get to the Home page, use the discovery utility to scan for the device on the network and open your browser from there.

2. On the **Log In** Page (Figure 4), use the following default **Web Access Username** and **Web Access Password** to access the **Home Page** (Figure 6):

   Web Access Username: **admin**

   Web Access Password: **admin**

Figure 4. Log In Page

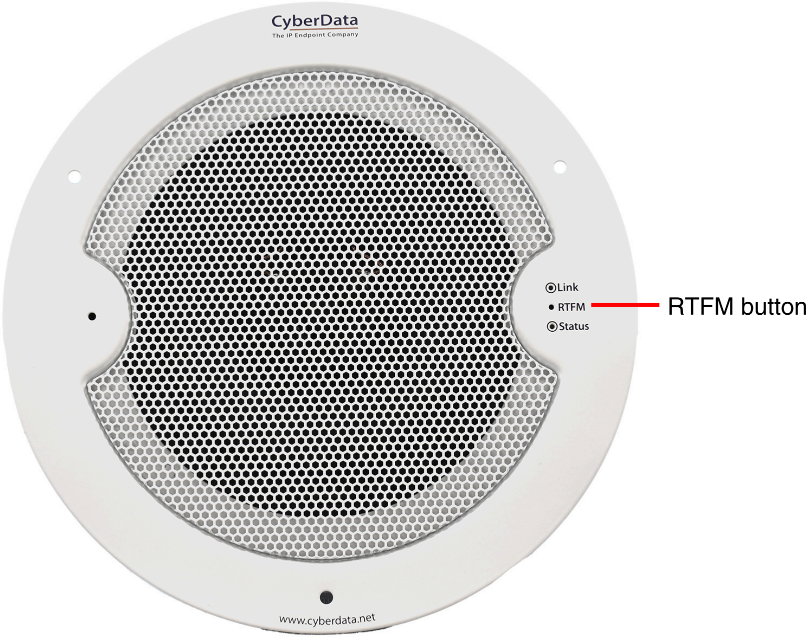


2.1.1 Announcing the IP Address

The RTFM button is located on the front of the each device (Figure 5). Use a paper clip to access the button through the hole.

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

Figure 5. RTFM Button



2.1.2 Restoring Factory Defaults

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

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

Table 1. Factory Default Settings

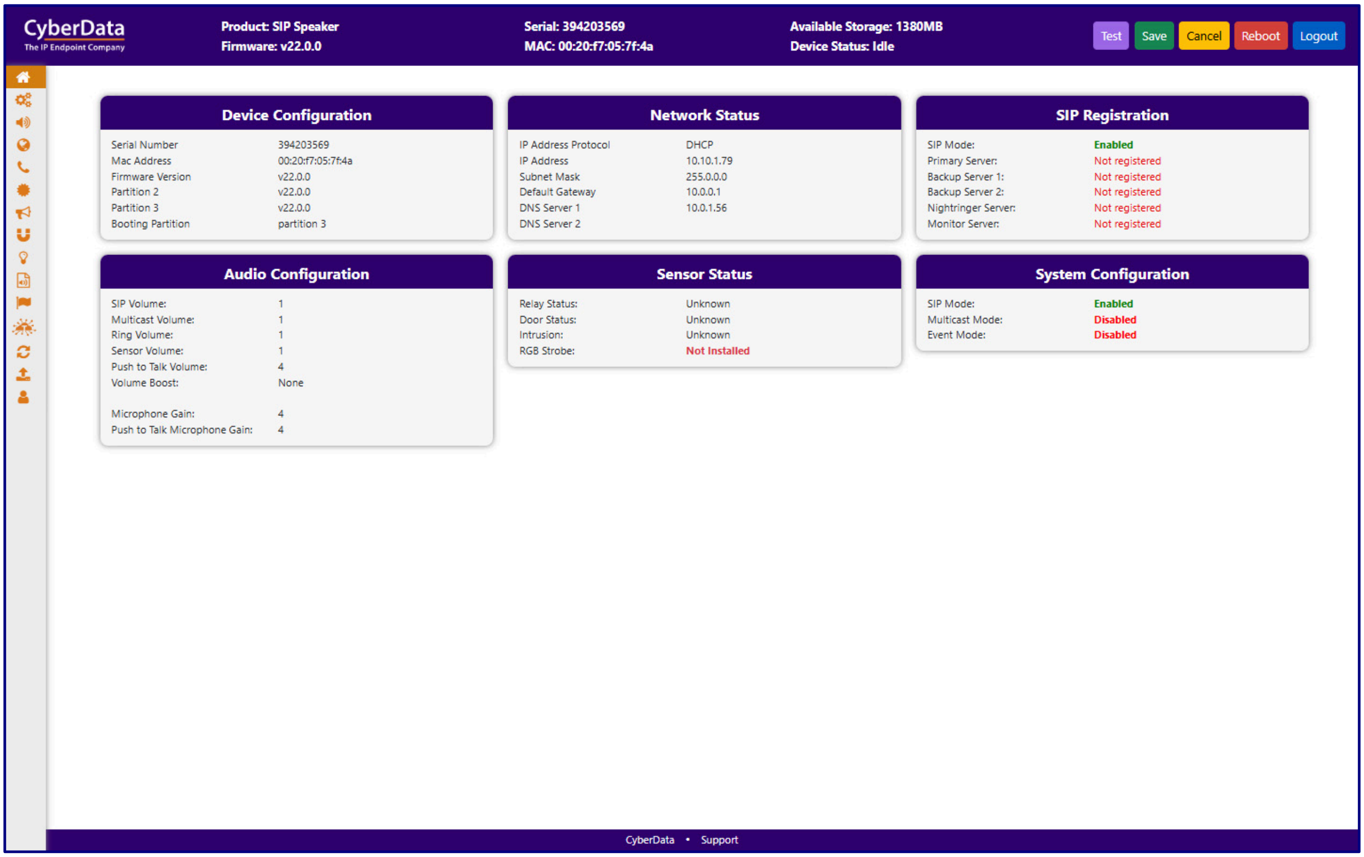
Parameter	Factory Default Setting
IP Addressing	DHCP
IP Address[a]	192.168.1.23
Web Access Username	admin
Web Access Password	admin
Subnet Mask[a]	255.255.255.0
Default Gateway[a]	192.168.1.1

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

2.2 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 6. Home Page



Product: SIP Speaker
Firmware: v22.0.0

Serial: 394203569
MAC: 00:20:f7:05:7f:4a

Available Storage: 1380MB
Device Status: Idle

Device Configuration

Serial Number	394203569
Mac Address	00:20:f7:05:7f:4a
Firmware Version	v22.0.0
Partition 2	v22.0.0
Partition 3	v22.0.0
Booting Partition	partition 3

Network Status

IP Address Protocol	DHCP
IP Address	10.10.1.79
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
Monitor Server:	Not registered

Audio Configuration

SIP Volume:	1
Multicast Volume:	1
Ring Volume:	1
Sensor Volume:	1
Push to Talk Volume:	4
Volume Boost:	None
Microphone Gain:	4
Push to Talk Microphone Gain:	4

Sensor Status

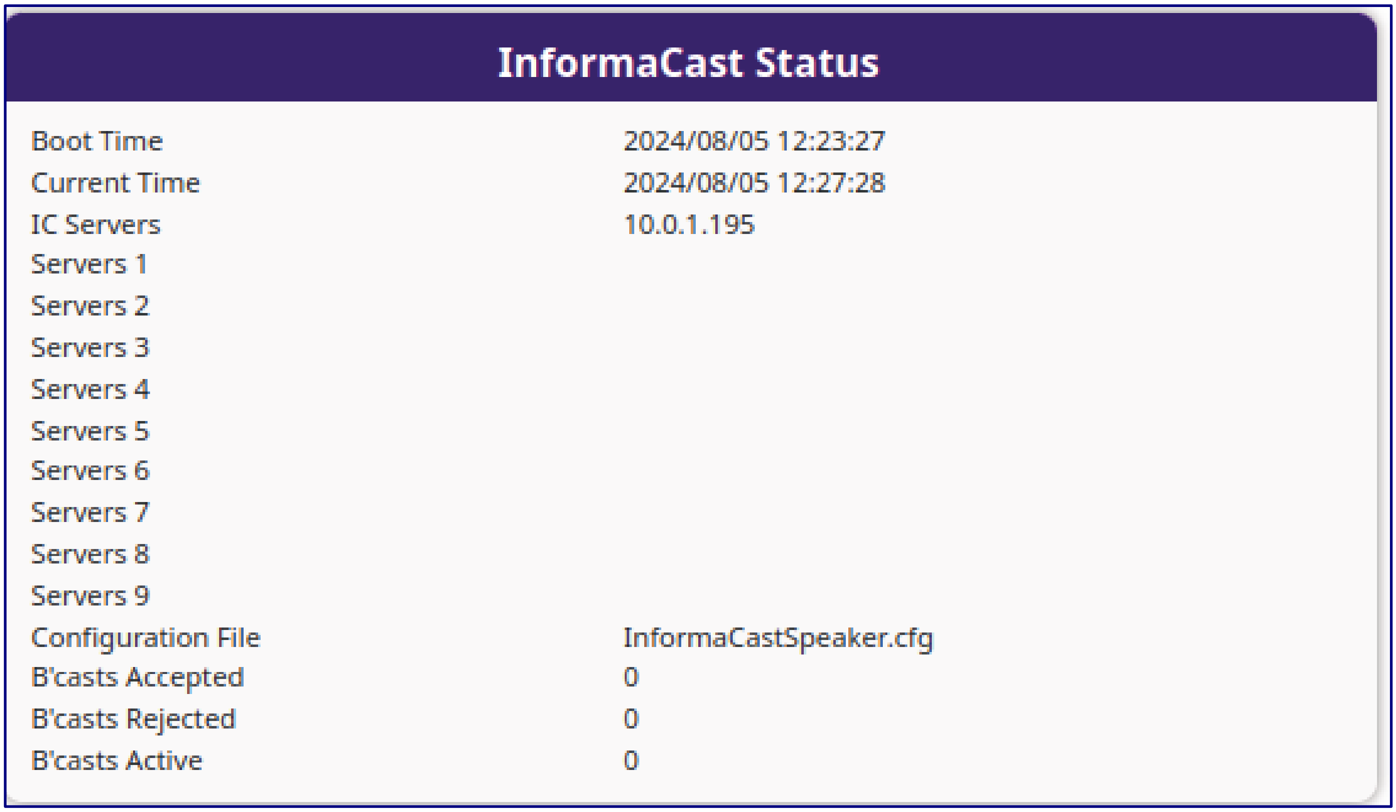
Relay Status:	Unknown
Door Status:	Unknown
Intrusion:	Unknown
RGB Strobe:	Not Installed

System Configuration

SIP Mode:	Enabled
Multicast Mode:	Disabled
Event Mode:	Disabled

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

Figure 7. InformaCast enabled Device



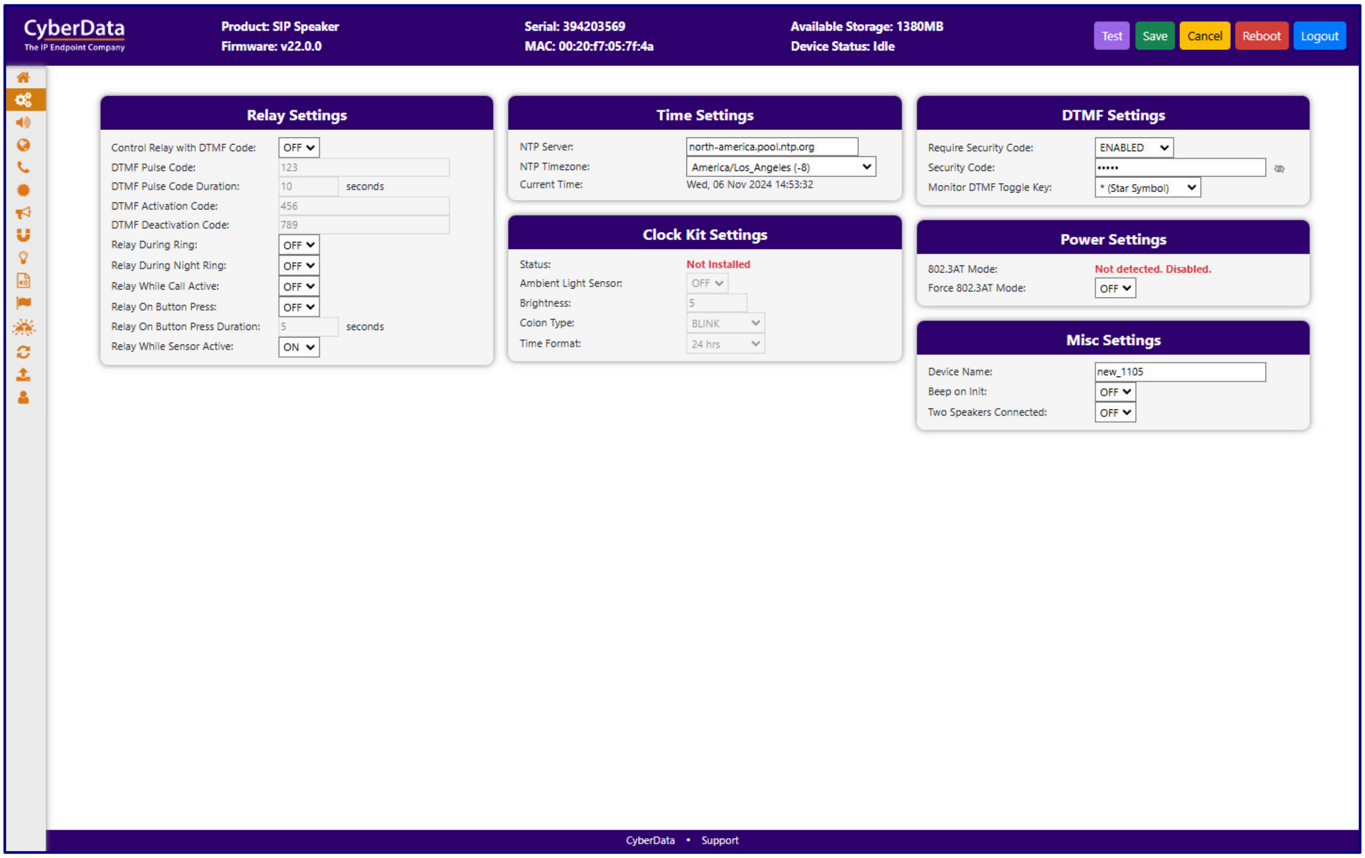
InformaCast Status

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

2.3 Device

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

Figure 8. Device Page



CyberData
The IP Endpoint Company

Product: SIP Speaker
Firmware: v22.0.0

Serial: 394203569
MAC: 00:20:f7:05:7f:4a

Available Storage: 1380MB
Device Status: Idle

Relay Settings

Control Relay with DTMF Code:	OFF
DTMF Pulse Code:	123
DTMF Pulse Code Duration:	10 seconds
DTMF Activation Code:	456
DTMF Deactivation Code:	789
Relay During Ring:	OFF
Relay During Night Ring:	OFF
Relay While Call Active:	OFF
Relay On Button Press:	OFF
Relay On Button Press Duration:	5 seconds
Relay While Sensor Active:	ON

Time Settings

NTP Server:	north-america.pool.ntp.org
NTP Timezone:	America/Los_Angeles (-8)
Current Time:	Wed, 06 Nov 2024 14:53:32

Clock Kit Settings

Status:	Not Installed
Ambient Light Sensor:	OFF
Brightness:	5
Colon Type:	BLINK
Time Format:	24 hrs

DTMF Settings

Require Security Code:	ENABLED
Security Code:	•••••
Monitor DTMF Toggle Key:	* (Star Symbol)

Power Settings

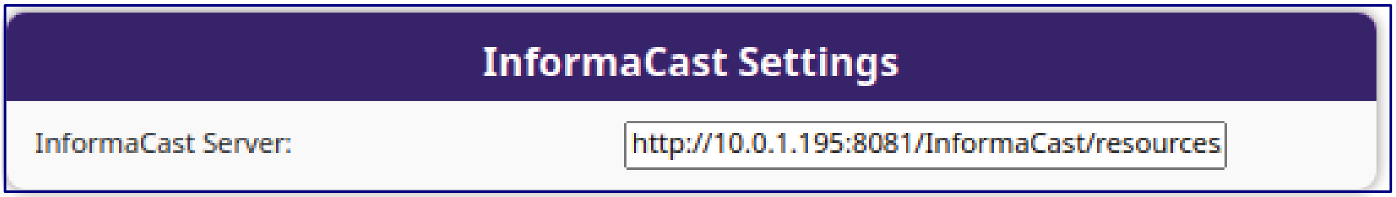
802.3AT Mode:	Not detected. Disabled.
Force 802.3AT Mode:	OFF

Misc Settings

Device Name:	new_1105
Beep on Init:	OFF
Two Speakers Connected:	OFF

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

Figure 9. InformaCast enabled Device

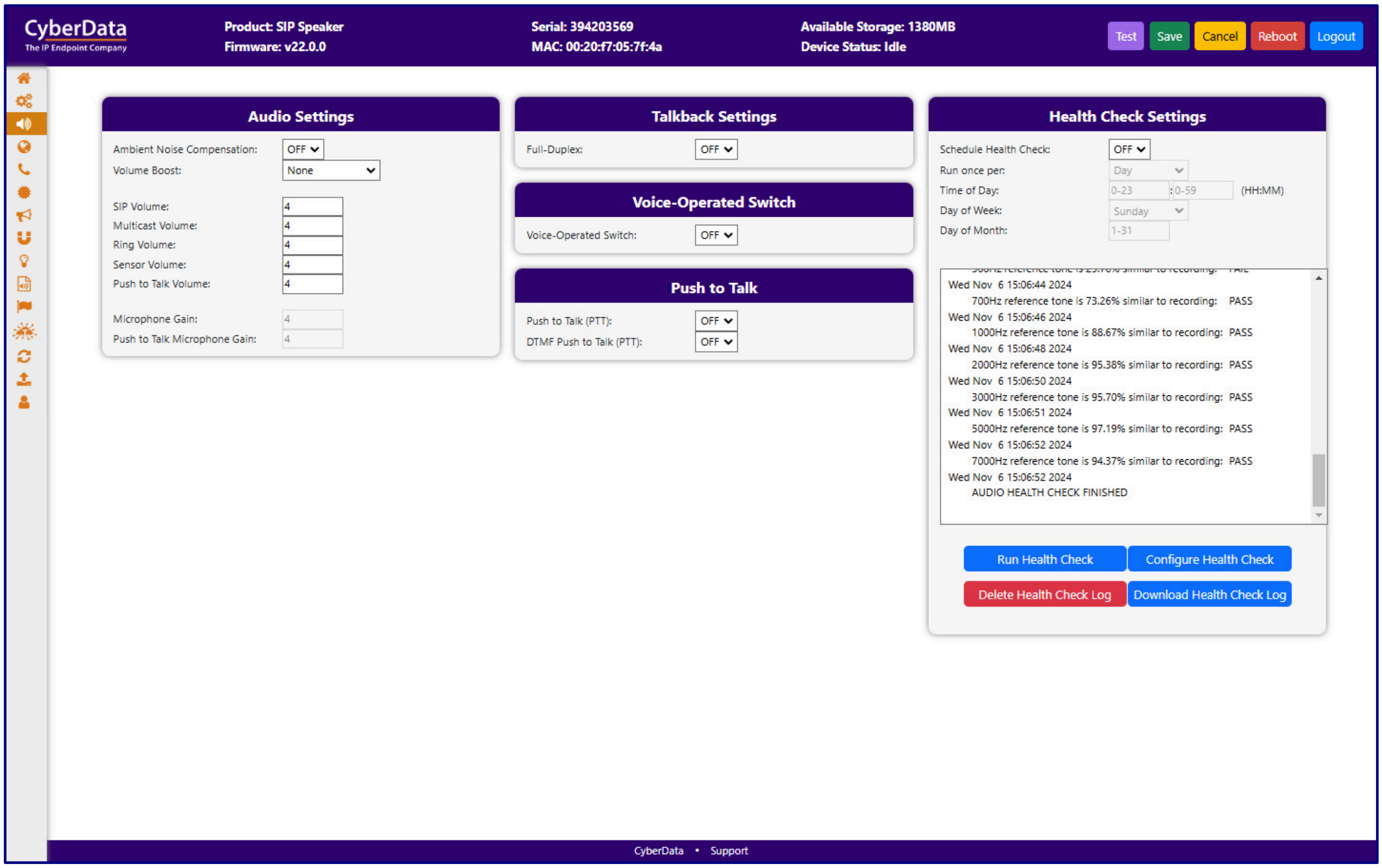


InformaCast Settings

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

2.4 Audio

Figure 10. Audio Page



Product: SIP Speaker
Firmware: v22.0.0
Serial: 394203569
MAC: 00:20:f7:05:7f:4a
Available Storage: 1380MB
Device Status: Idle

Audio Settings

Ambient Noise Compensation: OFF
Volume Boost: None

SIP Volume: 4
Multicast Volume: 4
Ring Volume: 4
Sensor Volume: 4
Push to Talk Volume: 4

Microphone Gain: 4
Push to Talk Microphone Gain: 4

Talkback Settings

Full-Duplex: OFF

Voice-Operated Switch

Voice-Operated Switch: OFF

Push to Talk

Push to Talk (PTT): OFF
DTMF Push to Talk (PTT): OFF

Health Check Settings

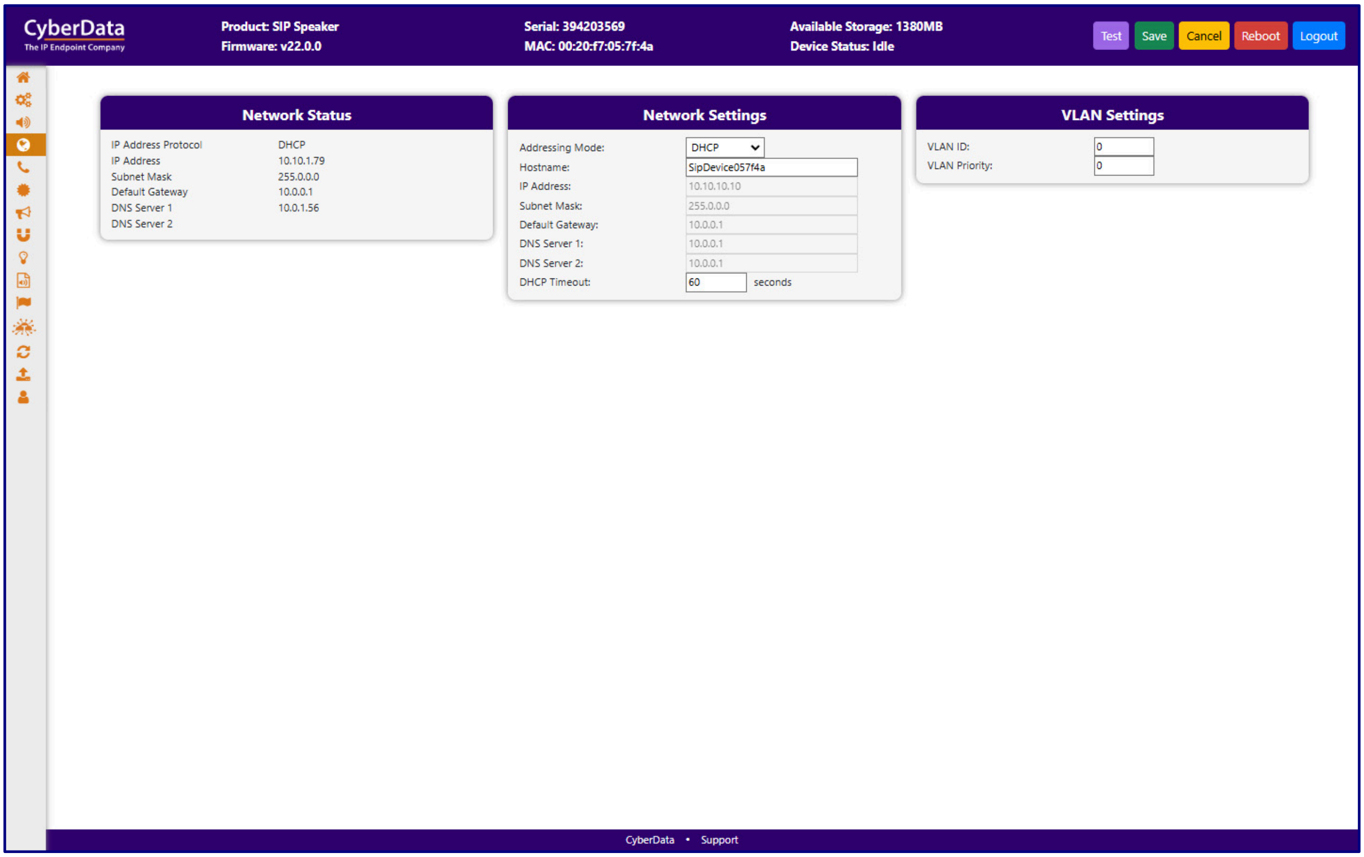
Schedule Health Check: OFF
Run once per: Day
Time of Day: 0-23 : 0-59 (HH:MM)
Day of Week: Sunday
Day of Month: 1-31

```
        500Hz reference tone is 25.70% similar to recording:    FAIL
Wed Nov  6 15:06:44 2024
        700Hz reference tone is 73.26% similar to recording:    PASS
Wed Nov  6 15:06:46 2024
        1000Hz reference tone is 88.67% similar to recording:  PASS
Wed Nov  6 15:06:48 2024
        2000Hz reference tone is 95.38% similar to recording:  PASS
Wed Nov  6 15:06:50 2024
        3000Hz reference tone is 95.70% similar to recording:  PASS
Wed Nov  6 15:06:51 2024
        5000Hz reference tone is 97.19% similar to recording:  PASS
Wed Nov  6 15:06:52 2024
        7000Hz reference tone is 94.37% similar to recording:  PASS
Wed Nov  6 15:06:52 2024
        AUDIO HEALTH CHECK FINISHED
```

2.5 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 11. Network Page



Product: SIP Speaker
Firmware: v22.0.0
Serial: 394203569
MAC: 00:20:f7:05:7f:4a
Available Storage: 1380MB
Device Status: Idle

Network Status

IP Address Protocol	DHCP
IP Address	10.10.1.79
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:	SipDevice057f4a
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

2.6 SIP (Session Initiation Protocol)

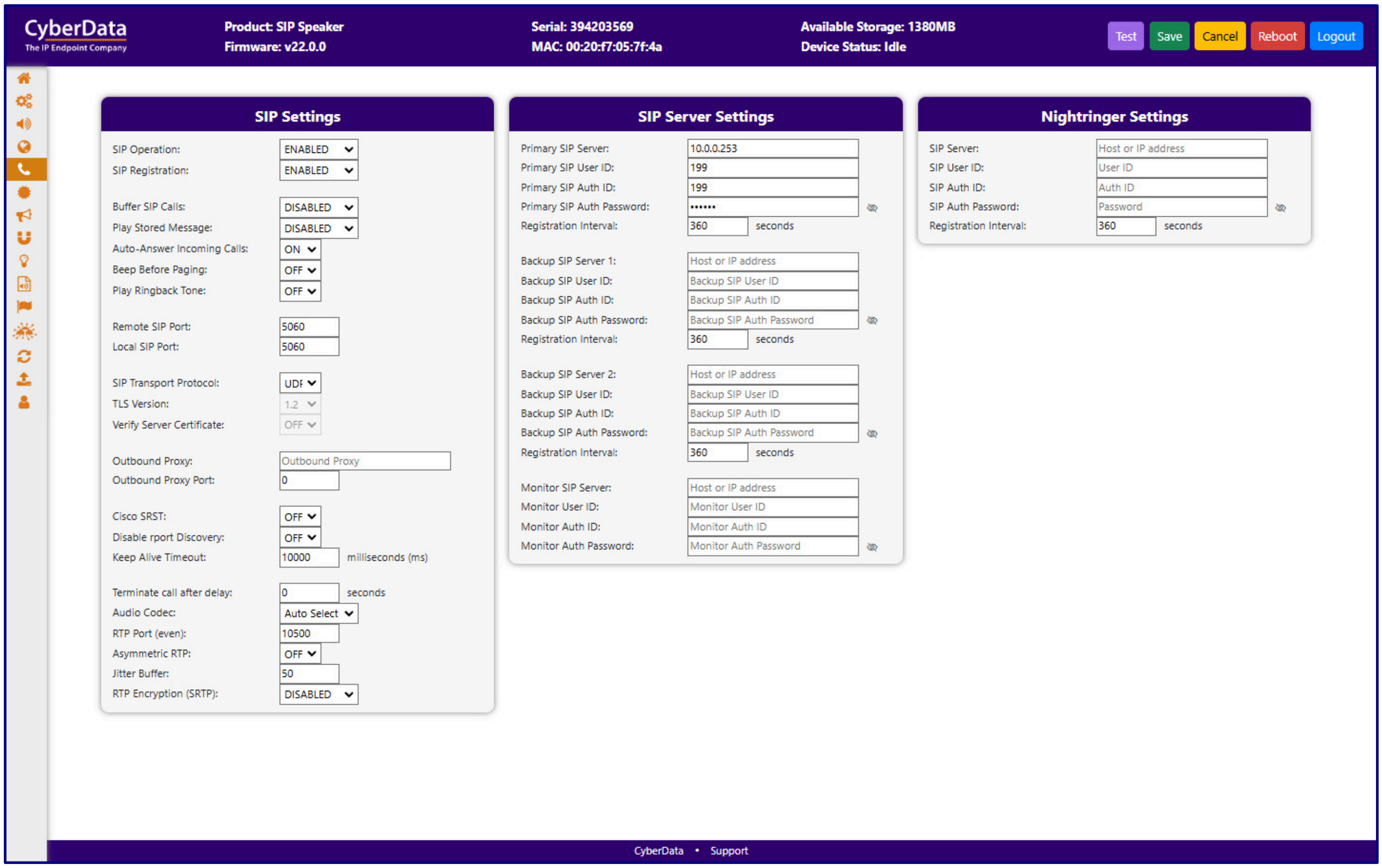
This page sets the options for phone calls. Configure up to 3 servers, with 2 acting as backup, and a server for the nightringer. The nightringer is a second sip extension that only rings, never connects to a call. Many customers use the nightringer in a hunt group.

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 12. SIP Page



Product: SIP Speaker
Firmware: v22.0.0
Serial: 394203569
MAC: 00:20:f7:05:7f:4a
Available Storage: 1380MB
Device Status: Idle

SIP Settings

SIP Operation: ENABLED
SIP Registration: ENABLED

Buffer SIP Calls: DISABLED
Play Stored Message: DISABLED
Auto-Answer Incoming Calls: ON
Beep Before Paging: OFF
Play Ringback Tone: OFF

Remote SIP Port: 5060
Local SIP Port: 5060

SIP Transport Protocol: UDI
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

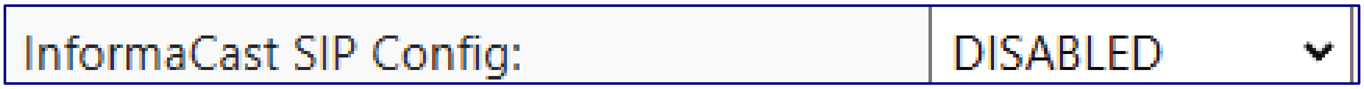
Monitor SIP Server: Host or IP address
Monitor User ID: Monitor User ID
Monitor Auth ID: Monitor Auth ID
Monitor Auth Password: Monitor Auth Password

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 13. InformaCast enabled Device



InformaCast SIP Config: DISABLED

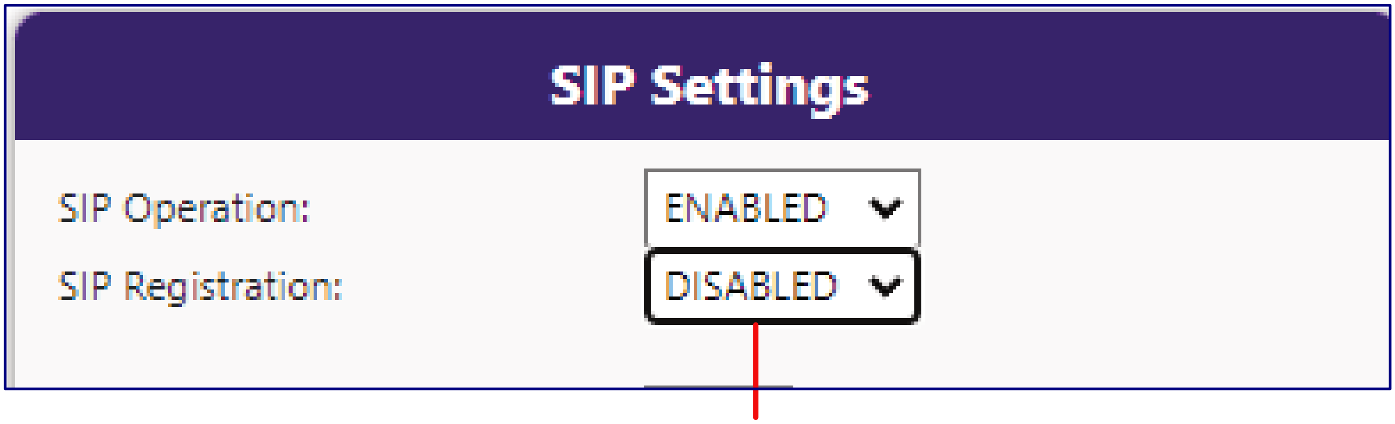
2.6.1 Dial Out Extension Strings and DTMF Tones (using rfc2833)

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

2.6.2 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 14.

Figure 14. SIP Page Set to Point-to-Point Mode



SIP Settings

SIP Operation: ENABLED

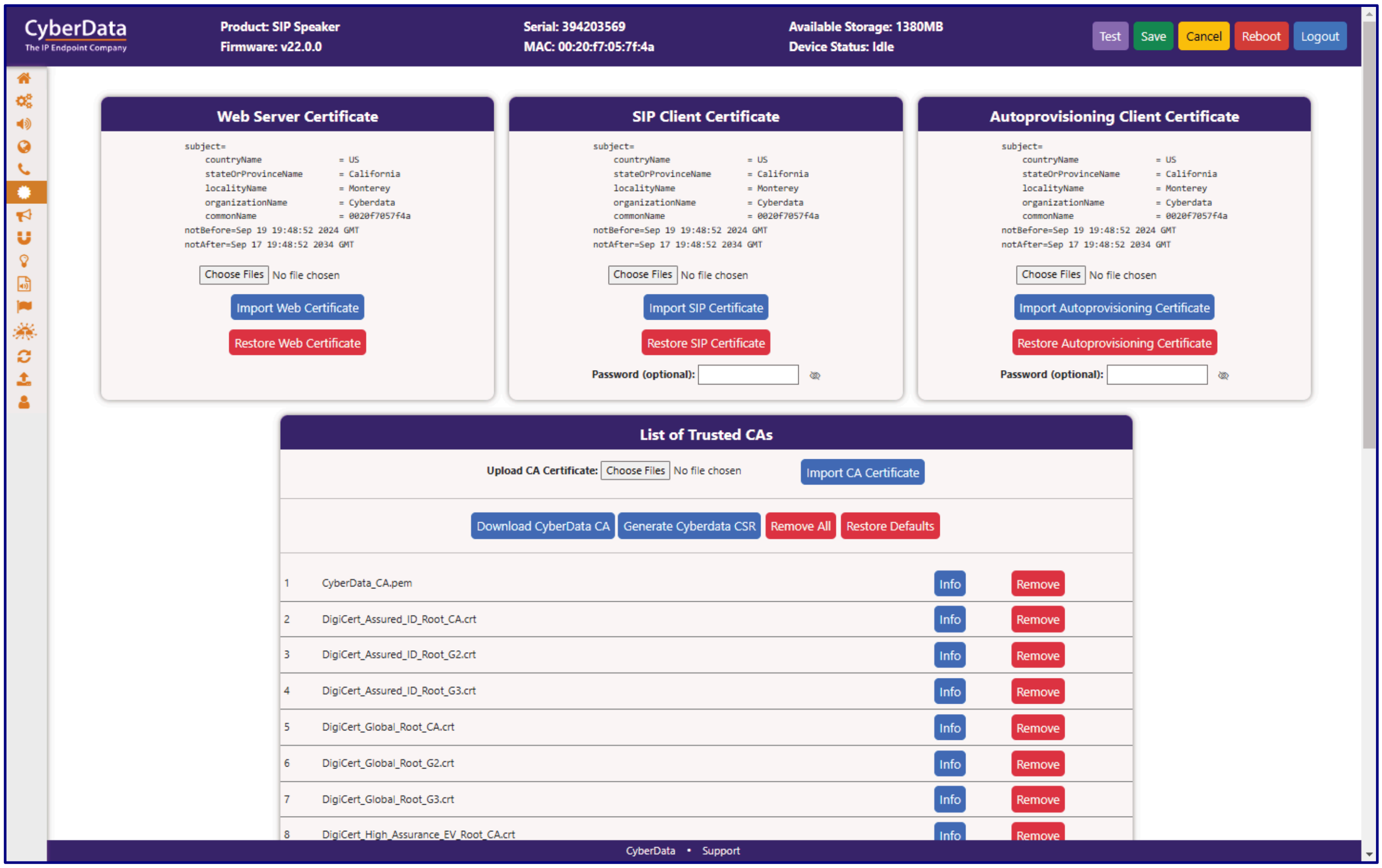
SIP Registration: DISABLED

Device is set to NOT register with a SIP server

2.7 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 15. SSL Page (1 of 2)



Product: SIP Speaker
Firmware: v22.0.0
Serial: 394203569
MAC: 00:20:f7:05:7f:4a
Available Storage: 1380MB
Device Status: Idle

Web Server Certificate

```
subject=
    countryName               = US
    stateOrProvinceName       = California
    localityName              = Monterey
    organizationName          = Cyberdata
    commonName                = 0020f7057f4a
notBefore=Sep 19 19:48:52 2024 GMT
notAfter=Sep 17 19:48:52 2034 GMT
```

SIP Client Certificate

```
subject=
    countryName               = US
    stateOrProvinceName       = California
    localityName              = Monterey
    organizationName          = Cyberdata
    commonName                = 0020f7057f4a
notBefore=Sep 19 19:48:52 2024 GMT
notAfter=Sep 17 19:48:52 2034 GMT
```

Password (optional):

Autoprovisioning Client Certificate

```
subject=
    countryName               = US
    stateOrProvinceName       = California
    localityName              = Monterey
    organizationName          = Cyberdata
    commonName                = 0020f7057f4a
notBefore=Sep 19 19:48:52 2024 GMT
notAfter=Sep 17 19:48:52 2034 GMT
```

Choose Files
No file chosen
Import Autoprovisioning Certificate
Restore Autoprovisioning Certificate

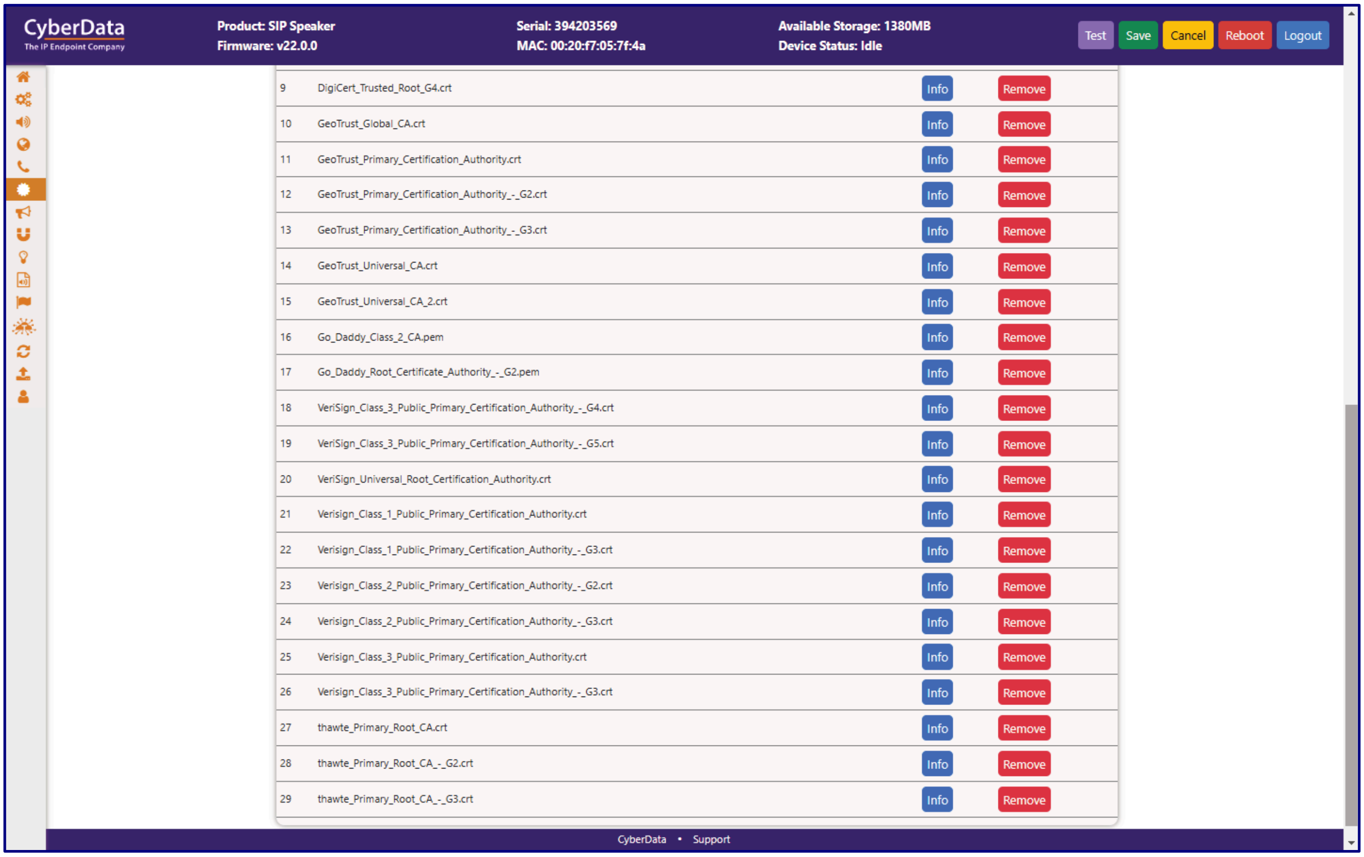
Password (optional):

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 16. SSL Page (2 of 2)



Product: SIP Speaker
Firmware: v22.0.0

Serial: 394203569
MAC: 00:20:f7:05:7f:4a

Available Storage: 1380MB
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

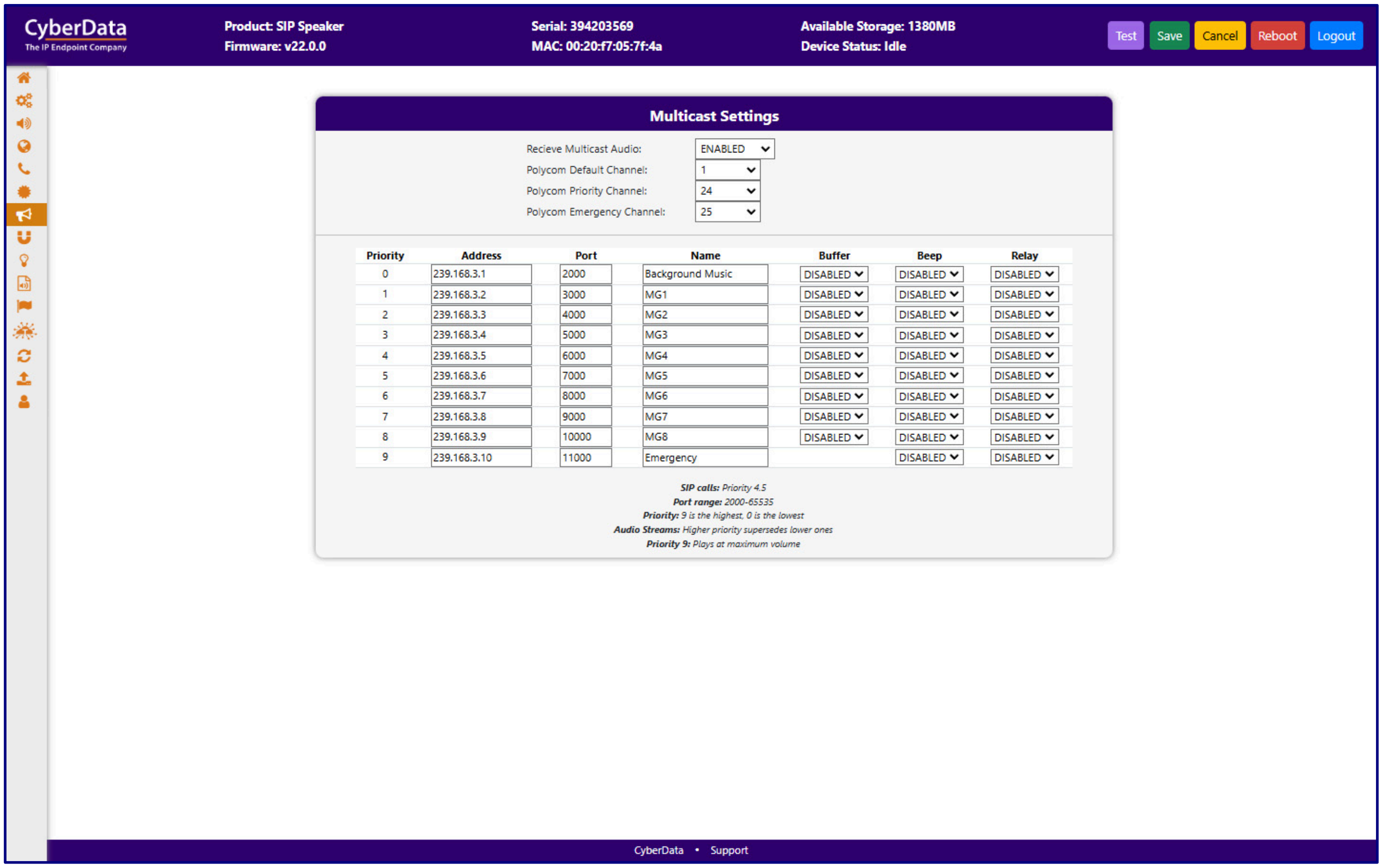
2.8 Multicast

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

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

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

Figure 17. Multicast Page



Product: SIP Speaker
Firmware: v22.0.0
Serial: 394203569
MAC: 00:20:f7:05:7f:4a
Available Storage: 1380MB
Device Status: Idle

Multicast Settings

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

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

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*

2.9 Sensor

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

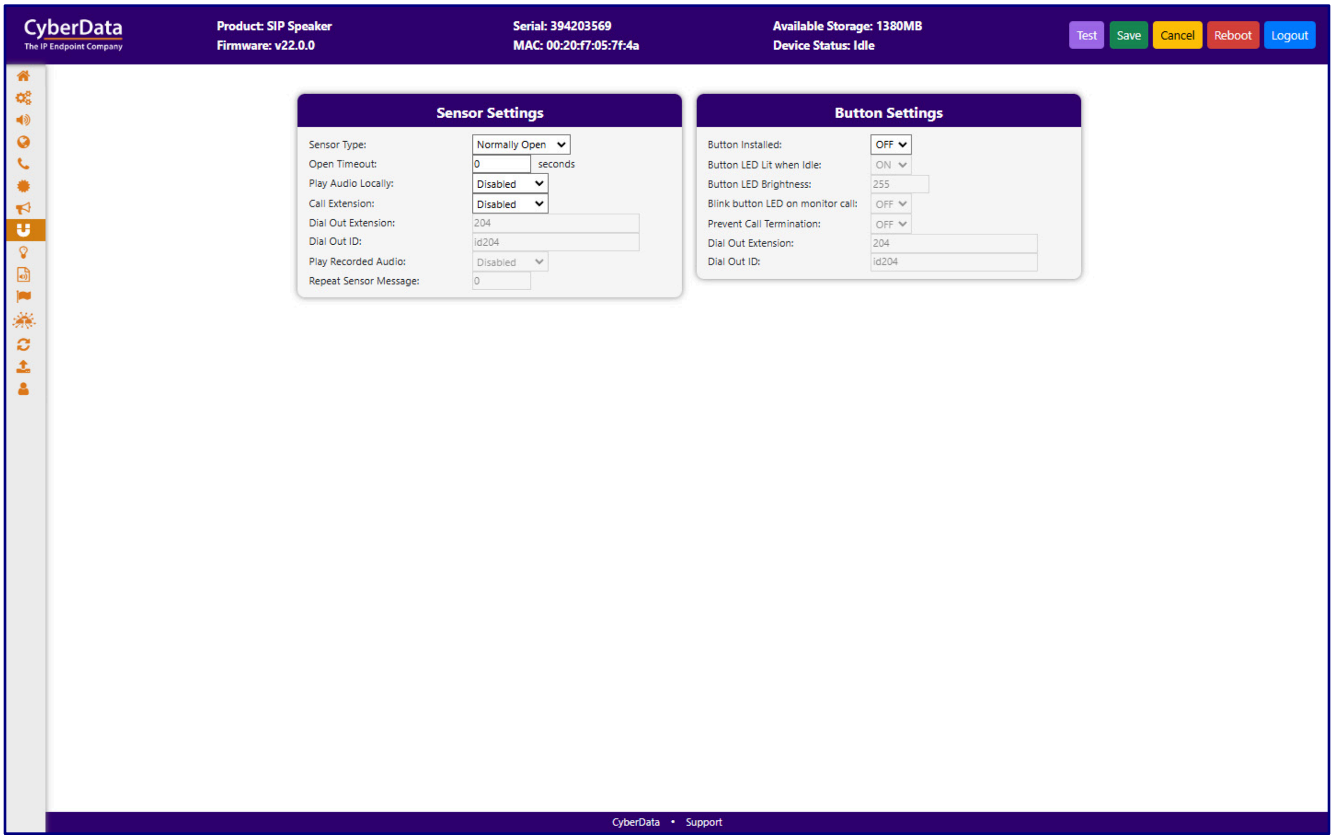
The intrusion sensor is an optical sensor installed on the Intercom board and will be activated when the Intercom is removed from the case.

Each sensor can trigger up to five different actions:

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

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

Figure 18. Sensor Page



Product: SIP Speaker
Firmware: v22.0.0
Serial: 394203569
MAC: 00:20:f7:05:7f:4a
Available Storage: 1380MB
Device Status: Idle

Sensor Settings

Sensor Type:	Normally Open
Open Timeout:	0 seconds
Play Audio Locally:	Disabled
Call Extension:	Disabled
Dial Out Extension:	204
Dial Out ID:	id204
Play Recorded Audio:	Disabled
Repeat Sensor Message:	0

Button Settings

Button Installed:	OFF
Button LED Lit when Idle:	ON
Button LED Brightness:	255
Blink button LED on monitor call:	OFF
Prevent Call Termination:	OFF
Dial Out Extension:	204
Dial Out ID:	id204

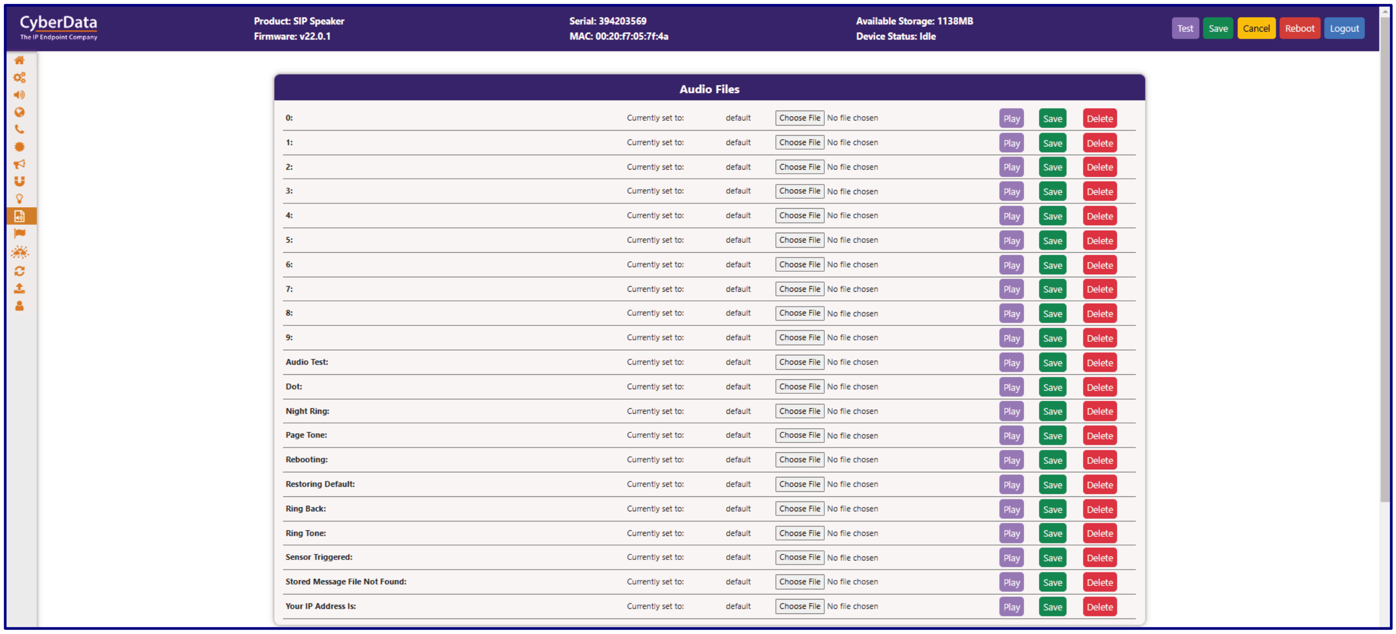
2.10 Audiofiles

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 19. Audiofiles Page (1 of 3)

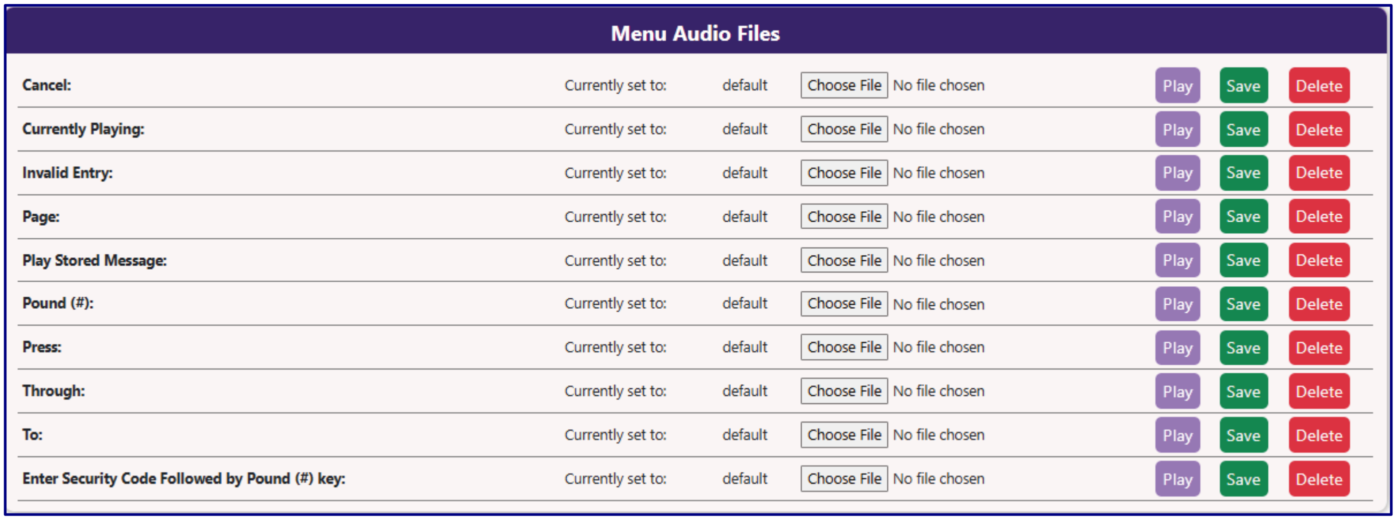


Product: SIP Speaker
Firmware: v22.0.1
Serial: 394203569
MAC: 00:20:f7:05:7f:4a
Available Storage: 1138MB
Device Status: Idle

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
Ring Back:	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
Stored Message File Not Found:	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

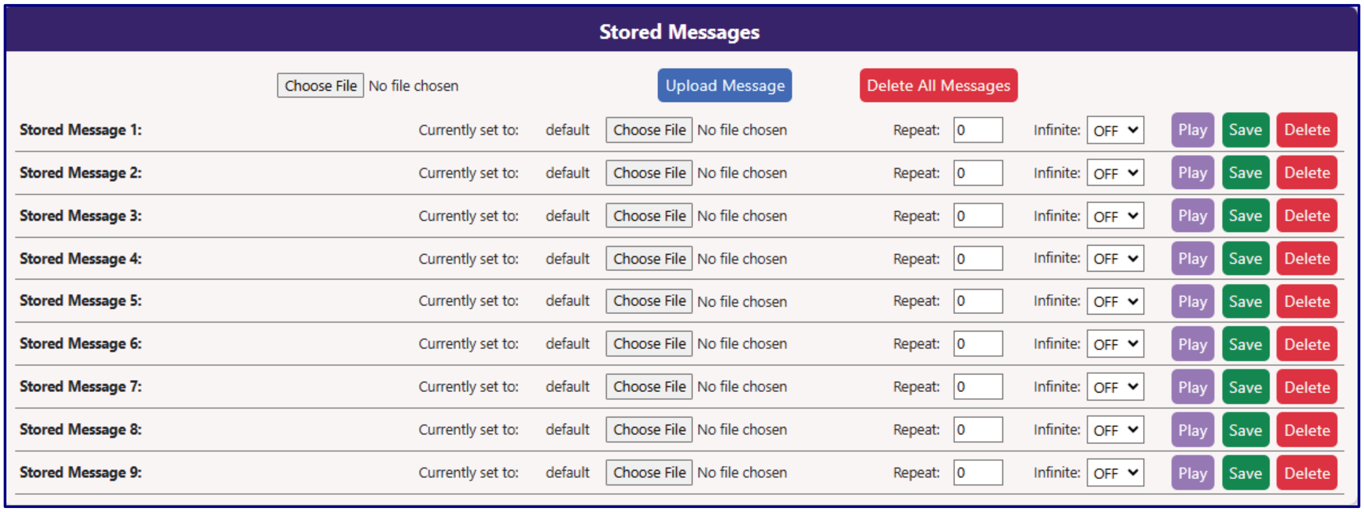
Figure 20. Audiofiles Page (2 of 3)



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
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 Security Code Followed by Pound (#) key:	Currently set to:	default	Choose File No file chosen	Play	Save	Delete

Figure 21. Audiofiles Page (3 of 3)



Stored Messages

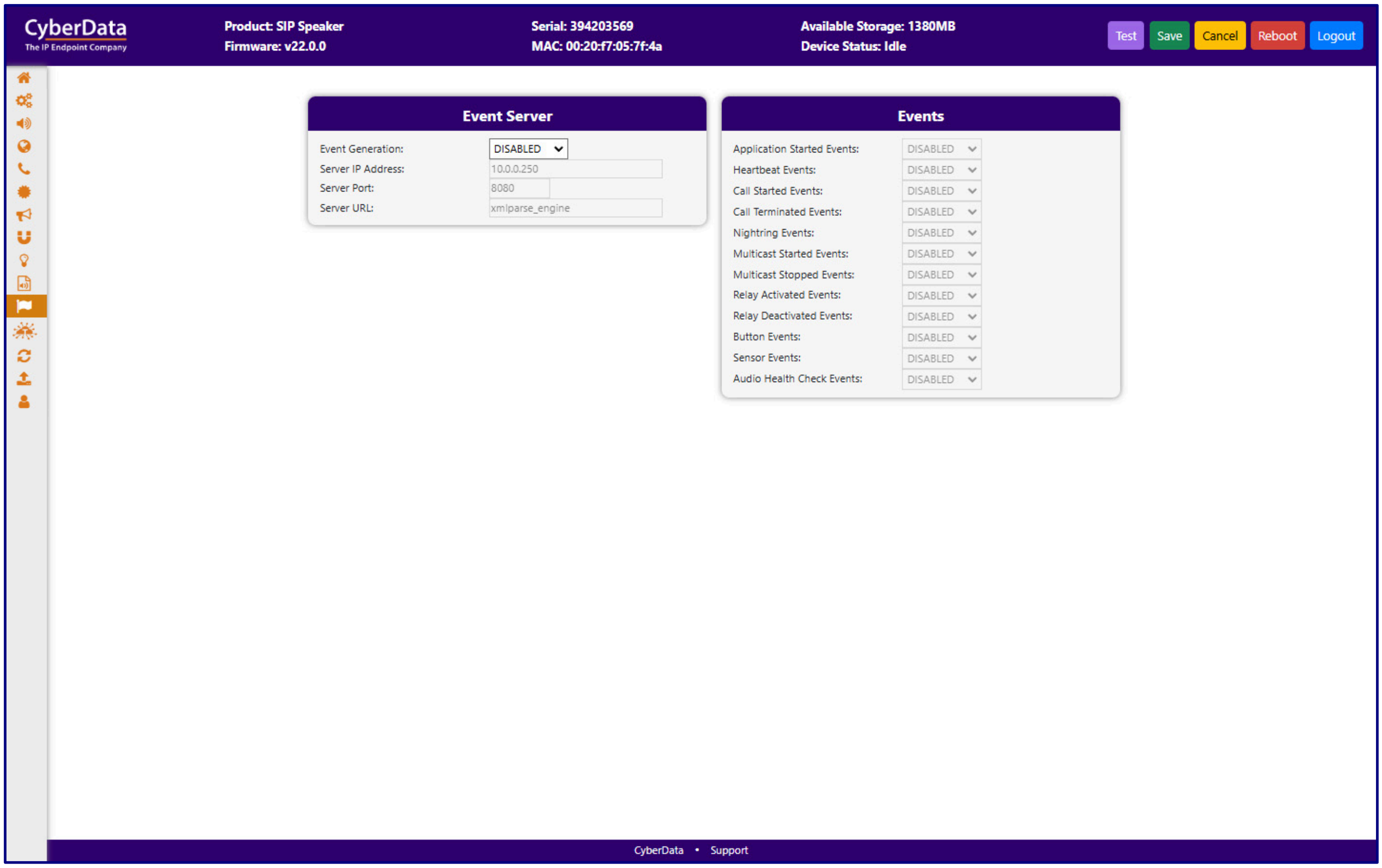
Choose File No file chosen

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

2.11 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 22. Events Page



Product: SIP Speaker
Firmware: v22.0.0
Serial: 394203569
MAC: 00:20:f7:05:7f:4a
Available Storage: 1380MB
Device Status: Idle

Event Server

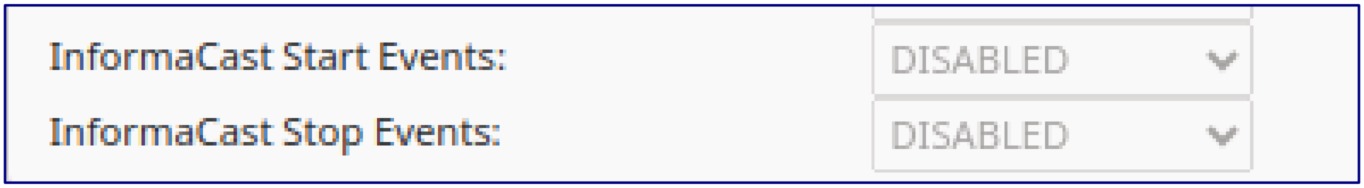
Event Generation: DISABLED
Server IP Address: 10.0.0.250
Server Port: 8080
Server URL: xmlparse_engine

Events

Application Started Events: DISABLED
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
Button Events: DISABLED
Sensor Events: DISABLED
Audio Health Check Events: DISABLED

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

Figure 23. InformaCast enabled Device



InformaCast Start Events: DISABLED
InformaCast Stop Events: DISABLED

2.11.1 Example Packets for Events

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

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

Here are example packets for every event:

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

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

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

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

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

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

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

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

```
POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0 Content-Length: 205
Content-Type: application/x-www-form-urlencoded

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

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

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

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

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

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

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

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

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

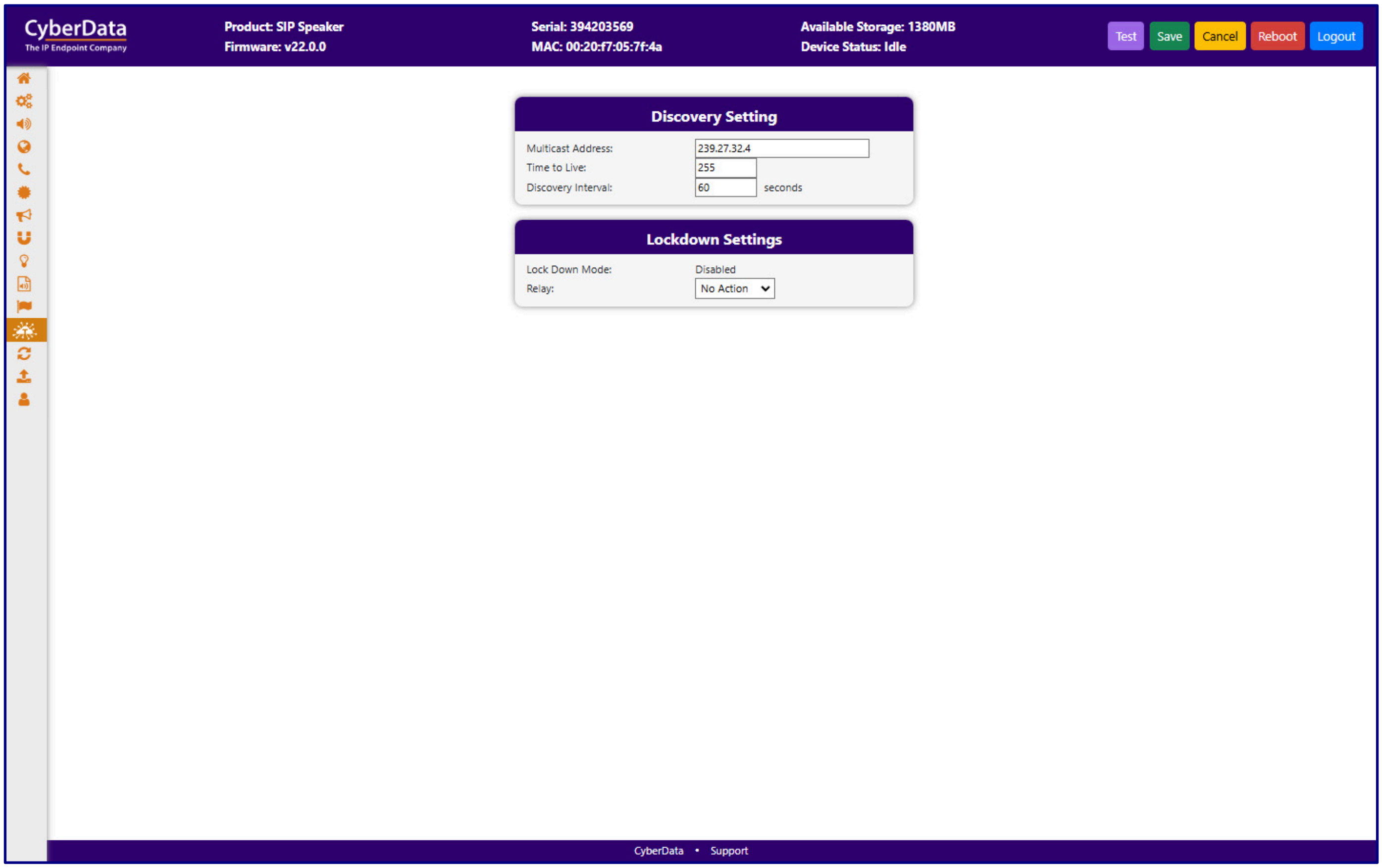
```
POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0 Content-Length: 234
Content-Type: application/x-www-form-urlencoded

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

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

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

2.12 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 24. Terminus Page



Product: SIP Speaker
Firmware: v22.0.0
Serial: 394203569
MAC: 00:20:f7:05:7f:4a
Available Storage: 1380MB
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

2.13 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.

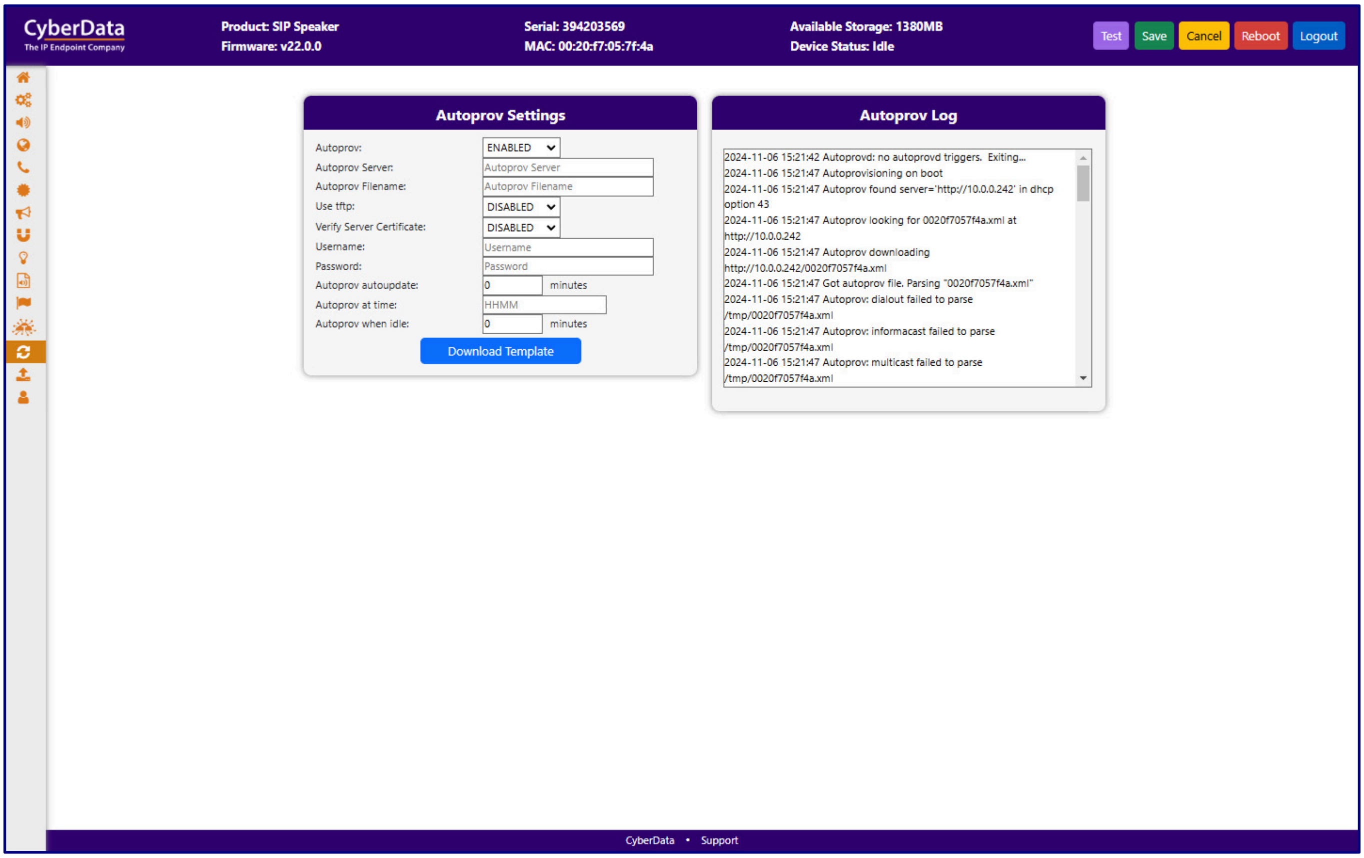
If a file is named, it will be downloaded instead of <mac address>.xml.

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 25. Autoprovisioning Page



Product: SIP Speaker
Firmware: v22.0.0
Serial: 394203569
MAC: 00:20:f7:05:7f:4a
Available Storage: 1380MB
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

Download Template

Autoprov Log

```
2024-11-06 15:21:42 Autoprovd: no autoprovd triggers.  Exiting...
2024-11-06 15:21:47 Autoprovisioning on boot
2024-11-06 15:21:47 Autoprov found server='http://10.0.0.242' in dhcp
option 43
2024-11-06 15:21:47 Autoprov looking for 0020f7057f4a.xml at
http://10.0.0.242
2024-11-06 15:21:47 Autoprov downloading
http://10.0.0.242/0020f7057f4a.xml
2024-11-06 15:21:47 Got autoprov file. Parsing "0020f7057f4a.xml"
2024-11-06 15:21:47 Autoprov: dialout failed to parse
/tmp/0020f7057f4a.xml
2024-11-06 15:21:47 Autoprov: informacast failed to parse
/tmp/0020f7057f4a.xml
2024-11-06 15:21:47 Autoprov: multicast failed to parse
/tmp/0020f7057f4a.xml
```

2.14 Firmware

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

To upgrade the firmware of your device:

1. Download the latest firmware from the following CyberData web site, and locate your device:

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

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

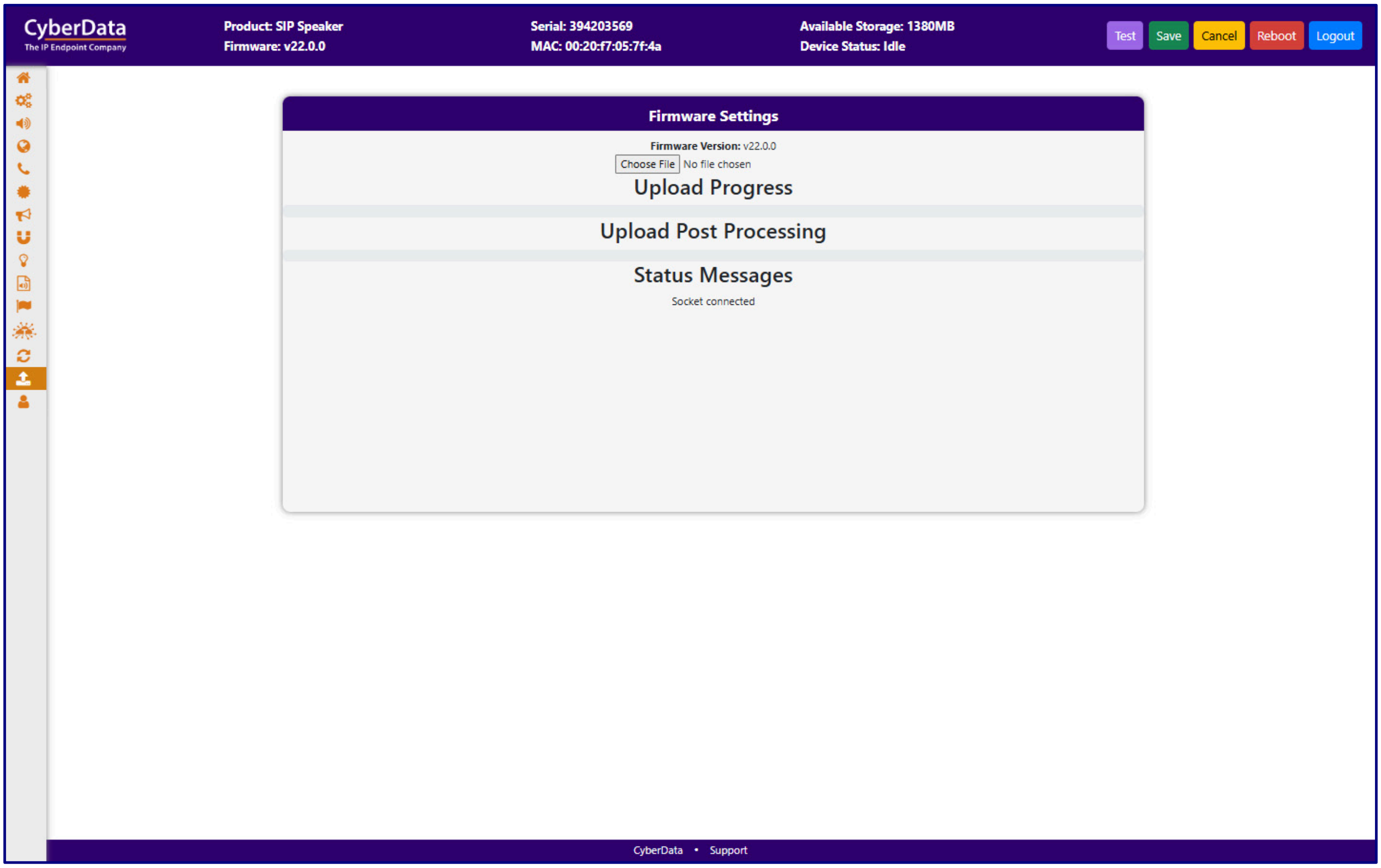
- Firmware file
- Release notes
- Autoprovisioning template

GENERAL ALERT

Caution

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

Figure 26. Firmware Page



Product: SIP Speaker
Firmware: v22.0.0
Serial: 394203569
MAC: 00:20:f7:05:7f:4a
Available Storage: 1380MB
Device Status: Idle

Firmware Settings

Firmware Version: v22.0.0

Choose File No file chosen

Upload Progress

Upload Post Processing

Status Messages

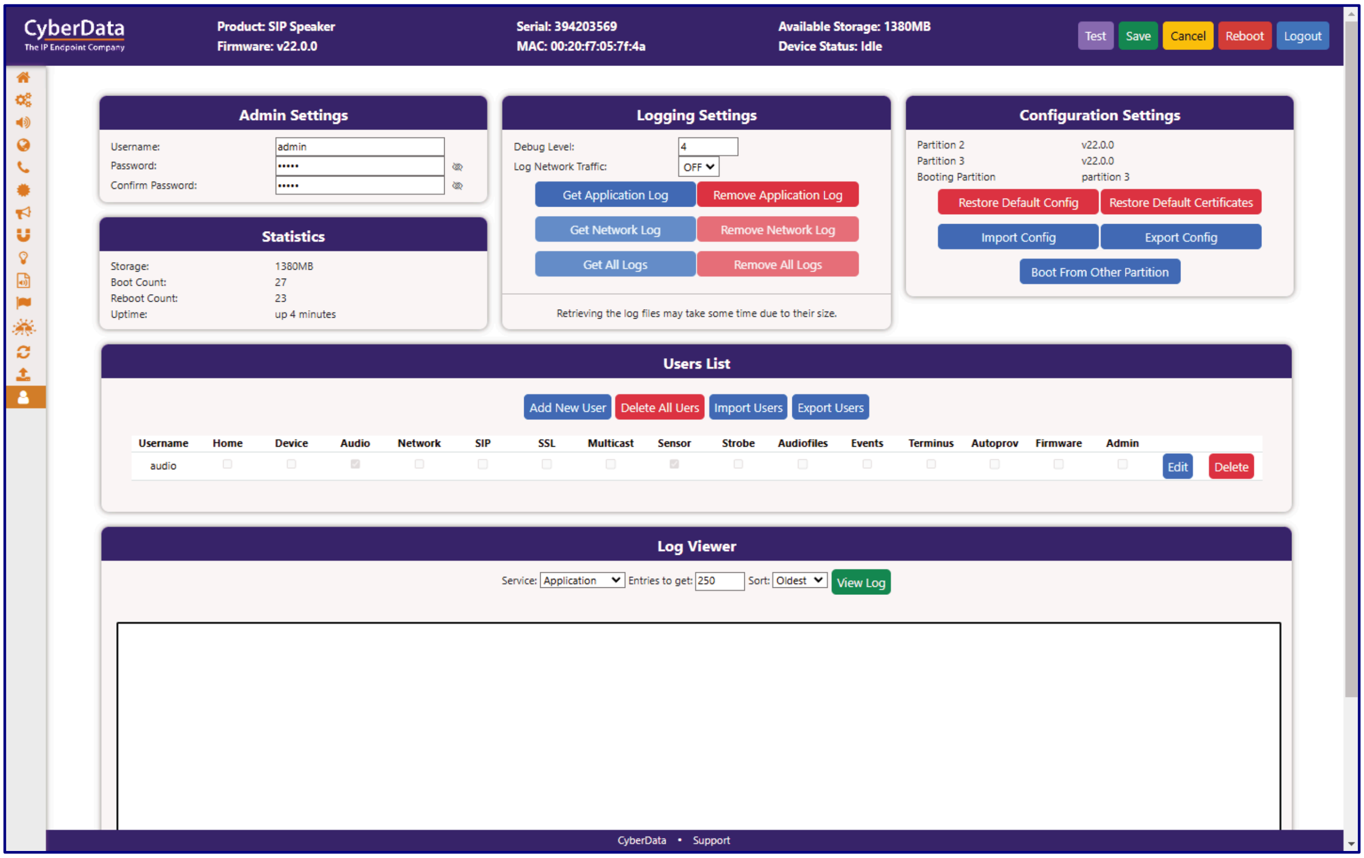
Socket connected

2.15 Admin

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

Note Two factor authentication is enabled here.

Figure 27. Admin Page



Product: SIP Speaker
Firmware: v22.0.0

Serial: 394203569
MAC: 00:20:f7:05:7f:4a

Available Storage: 1380MB
Device Status: Idle

Admin Settings

Username: admin
Password: •••••
Confirm Password: •••••

Statistics

Storage: 1380MB
Boot Count: 27
Reboot Count: 23
Uptime: up 4 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 v22.0.0
Partition 3 v22.0.0
Booting Partition partition 3

Users List

Username	Home	Device	Audio	Network	SIP	SSL	Multicast	Sensor	Strobe	Audiofiles	Events	Terminus	Autoprov	Firmware	Admin		
audio	□	□	☑	□	□	□	□	☑	□	□	□	□	□	□	□	Edit	Delete

Log Viewer

Service: Application Entries to get: 250 Sort: Oldest

2.16 Command Interface

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

2.16.1 Command Interface Post Commands

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

Table 2. Command Interface Post Commands

Device Action	**HTTP Post Command**[1]
Reboot	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.154/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://10.10.1.154/command" --post-data "request=call&extension=600"
Terminate a calli	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"
Speak IP Address	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.154/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://10.10.1.154/command" --post-data "request=test_audio"
Swap boot partitions	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.154/command" --post-data "request=swap_boot_partition"

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

Index

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

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/

A.3 Electrostatic Discharge (ESD) Sensitivity

Notice: Electrostatic Discharge (ESD) Sensitivity

This device conforms to IEC 61000-4-2 Criterion-C standards. While the device is designed for remote installation, direct human contact may occasionally cause an electrostatic discharge that results in the device becoming unresponsive. If the device fails to respond after physical interaction, please perform a hard reboot by cycling the power (turning the device off and back on). Normal operation should resume following reboot.