



Multicast Speaker Operations Guide

Part #011458, 011487, 011504, 011505

Document Part #932056A
for Firmware Version 22.0

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

Multicast Speaker Operations Guide 932056A
Part # 011458, 011487, 011504, 011505

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

Email: support@cyberdata.net



Fax: (831) 373-4193

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

Revision Information

Revision 932056A, which corresponds to firmware version 22.0, was released on December 11, 2024.

Pictorial Alert Icons

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

Hazard Levels

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

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

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




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

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

Important Safety Instructions

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

14. WARNING: The Multicast Speaker enclosure is not rated for any AC voltages!

 <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
u-law	A companding algorithm, primarily used in the digital telecommunication
UC	Unified Communications
VoIP	Voice over Internet Protocol

Contents

Chapter 1 Multicast Ceiling Speaker Device Setup (Part #011458 and 011504)	1
1.1 Confirm that the Speaker is Operational and Linked to the Network	1
1.2 Link/Activity LED	1
1.2.1 100 Mb LED	1
Chapter 2 Multicast Wall Mount Speaker Device Setup (Part #011487 and 011504)	2
2.1 Confirm that the Speaker is Operational and Linked to the Network	2
2.2 Link/Activity LED	2
2.2.1 100 Mb LED	2
Chapter 3 Configure the Device	3
3.1 Log In Page	3
3.1.1 Announcing the IP Address	4
3.1.2 Restoring Factory Defaults	5
3.2 Home Page	6
3.3 Device	8
3.4 Audio	9
3.5 Network	10
3.6 SSL	11
3.7 Multicast	13
3.8 Audiofiles	14
3.9 Events	15
3.9.1 Example Packets for Events	16
3.10 Terminus	19
3.11 Autoprovisioning	20
3.12 Firmware	21
3.13 Admin	22
3.14 Command Interface	23
3.14.1 Command Interface Post Commands	23
Appendix A Troubleshooting/Technical Support	25
A.1 Contact Information	25
A.2 Warranty and RMA Information	25
Index	26

1 Multicast Ceiling Speaker Device Setup

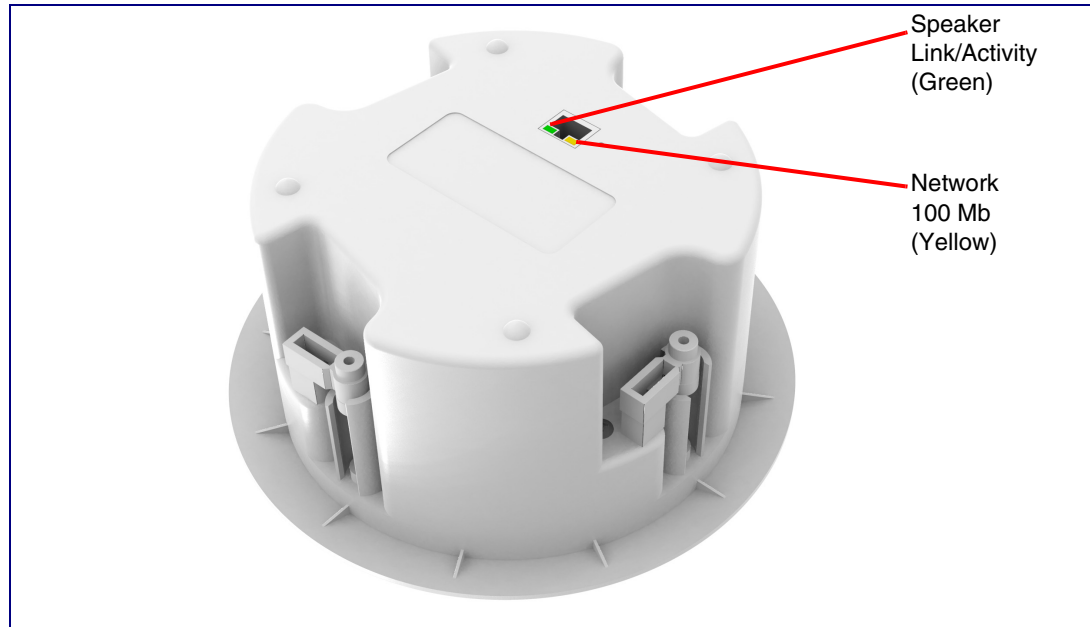
(Part #011458 and 011504)

1

1.1 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 rear of the speaker housing confirm that the speaker is operational and linked to the network.

Figure 1-1. Status and Activity LEDs



1.2 Link/Activity LED

After supplying power to the speaker:

1. The green Link/Activity LED comes on immediately to show that there is a good network connection, and then blinks to show network activity.
2. After about 23 seconds with a static IP address (or 27 seconds if the board is set to use DHCP), the speaker should be ready.

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 10.10.10.10). This process will take approximately 80 seconds.

1.2.1 100 Mb LED

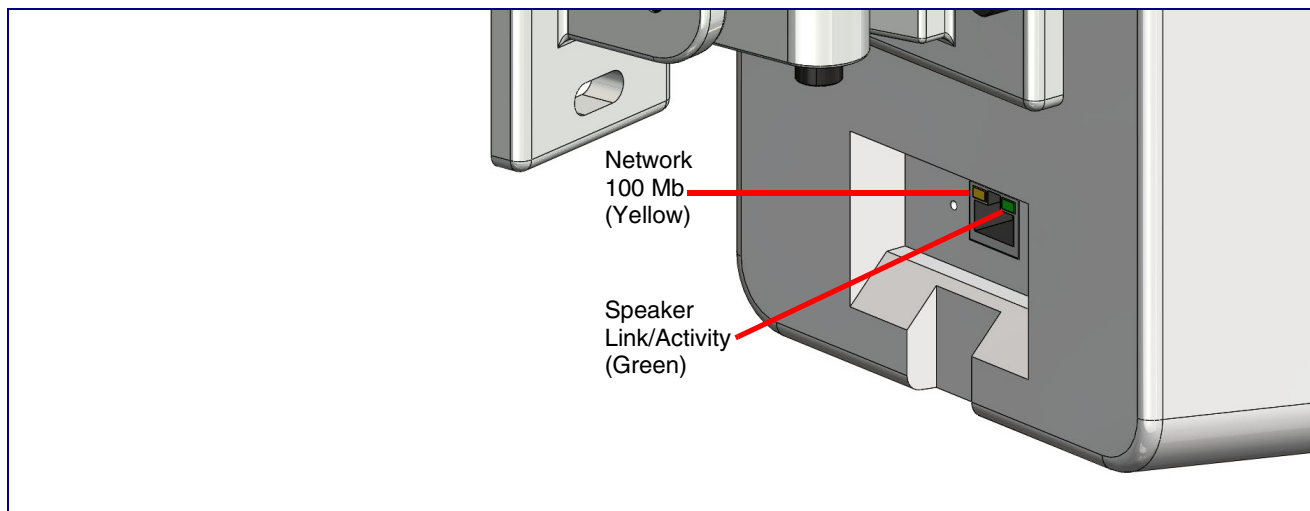
- The yellow **100 Mb** LED is illuminated when the network 100 Mb link to the speaker is established.

2 Multicast Wall Mount Speaker Device Setup (Part #011487 and 011504)

2.1 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 rear of the speaker housing confirm that the speaker is operational and linked to the network.

Figure 2-1. Status and Activity LEDs



2.2 Link/Activity LED

After supplying power to the speaker:

1. The green Link/Activity LED comes on immediately to show that there is a good network connection, and then blinks to show network activity.
2. After about 23 seconds with a static IP address (or 27 seconds if the board is set to use DHCP), the speaker should be ready.

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 10.10.10.10). This process will take approximately 80 seconds.

2.2.1 100 Mb LED

- The yellow **100 Mb** LED is illuminated when the network 100 Mb link to the speaker is established.

3 Configure the Device

3.1 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 Multicast Speaker.

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>

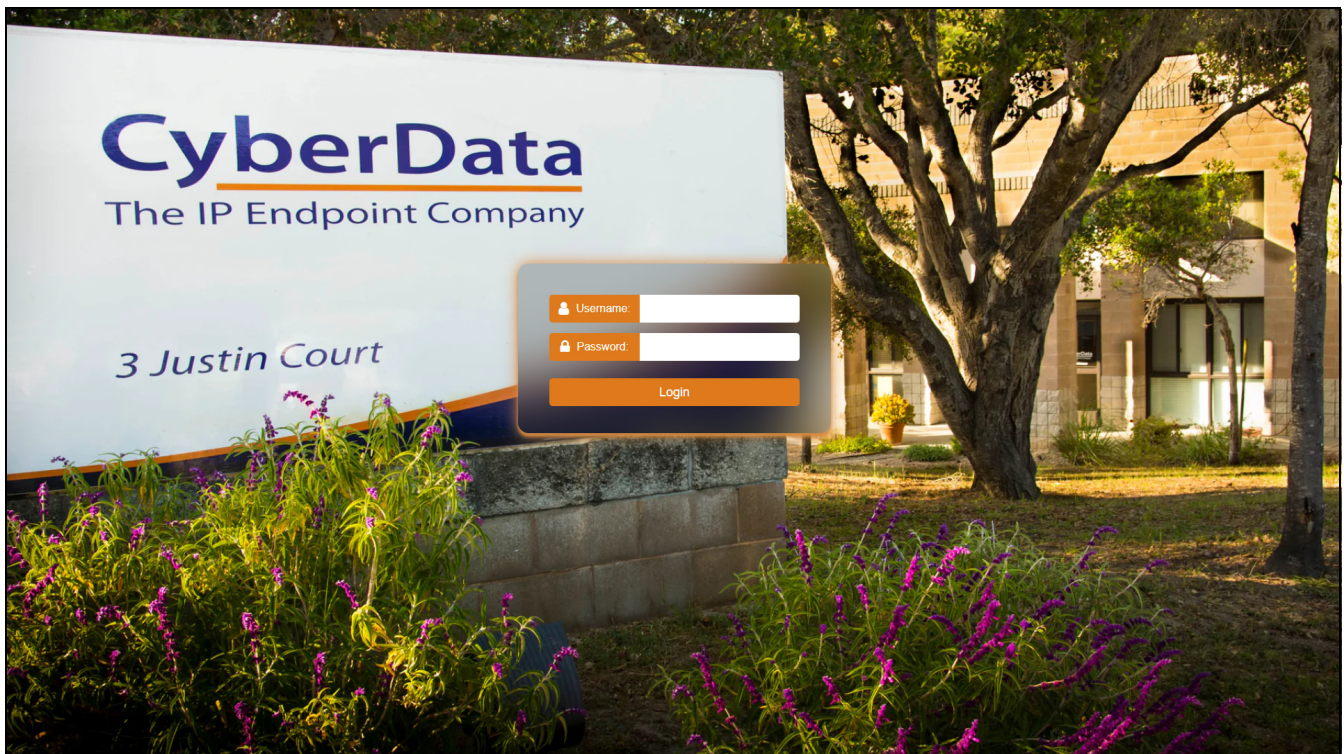
Note The Intercom ships in DHCP mode. To get to the **Home** page, use the discovery utility to scan for the device on the network and open your browser from there.

2. On the Log In Page (Figure 3-1), use the following default **Web Access Username** and **Web Access Password** to access the **Home Page** (Figure 3-4):

Web Access Username: **admin**

Web Access Password: **admin**

Figure 3-1. Log In Page



3.1.1 Announcing the IP Address

The RTFM button is located on the back of the each device (Figure 3-2 and Figure 3-3). 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 3-2. RTFM Button (Ceiling Speakers)

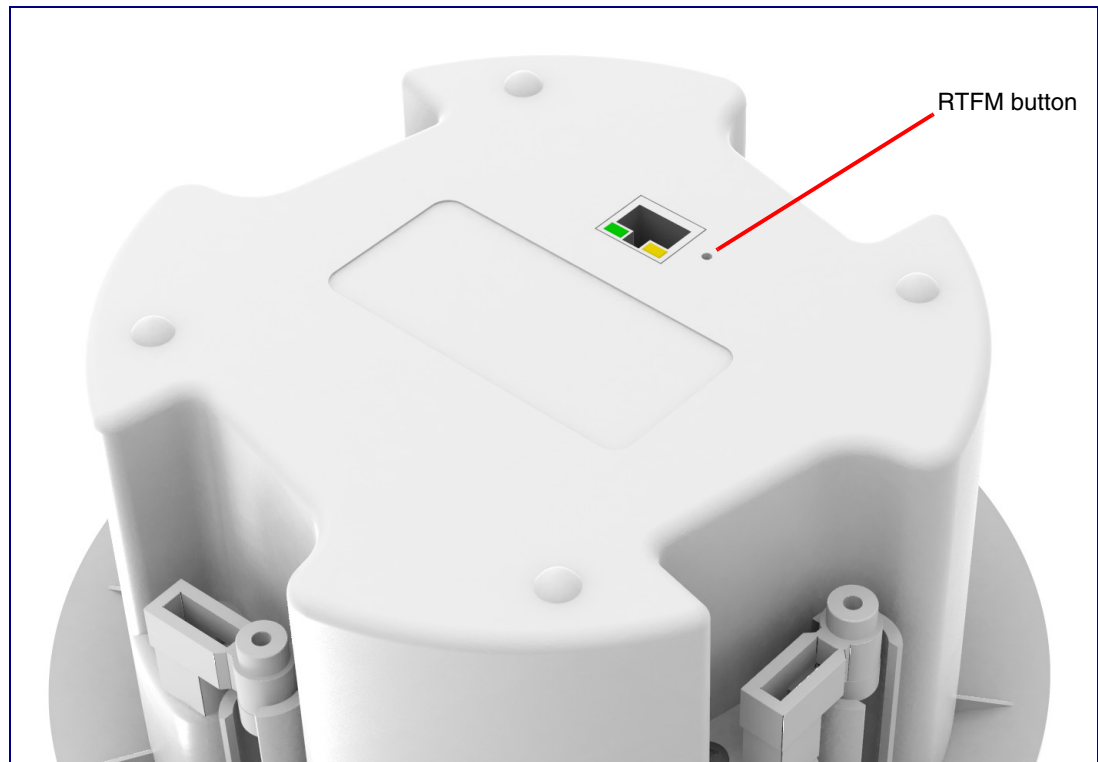
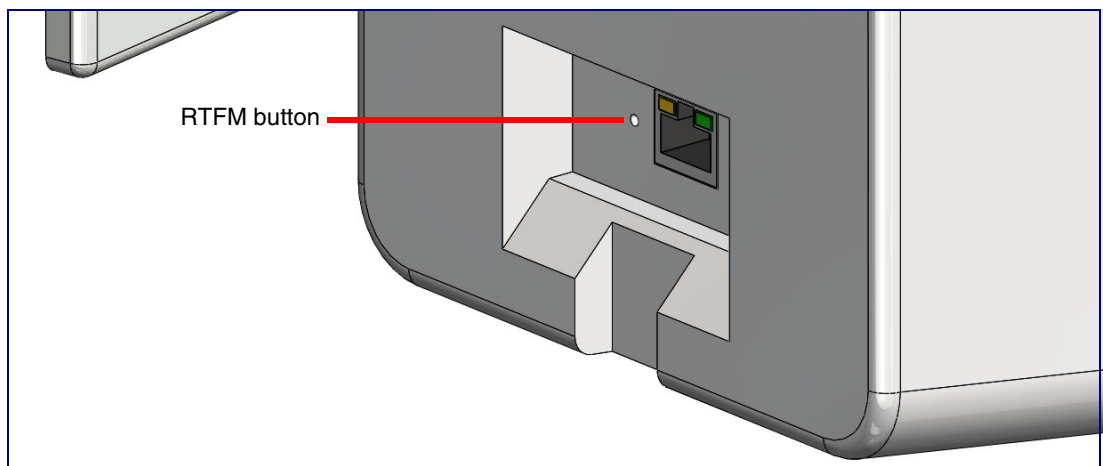


Figure 3-3. RTFM Button (Wall Mount Speakers)



3.1.2 Restoring Factory Defaults

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

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

Table 3-1. 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.

3.2 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 3-4. Home Page

The screenshot displays the CyberData Home Page interface. At the top, the header includes the CyberData logo, product information (Multicast Speaker, Firmware: v22.0.3), serial and MAC addresses (458000002, 00:20:f7:04:34:f3), available storage, and device status. A navigation sidebar is on the left, and a top toolbar contains buttons for Test, Save, Cancel, Reboot, and Logout.

The main content area is divided into four configuration panels:

- Device Configuration:**

Serial Number	458000002
Mac Address	00:20:f7:04:34:f3
Firmware Version	v22.0.3
Partition 2	v22.0.3
Partition 3	v22.0.3
Booting Partition	partition 2
- Network Status:**

IP Address Protocol	DHCP
IP Address	10.10.1.31
Subnet Mask	255.0.0.0
Default Gateway	10.0.0.1
DNS Server 1	10.0.1.56
DNS Server 2	
- Audio Configuration:**

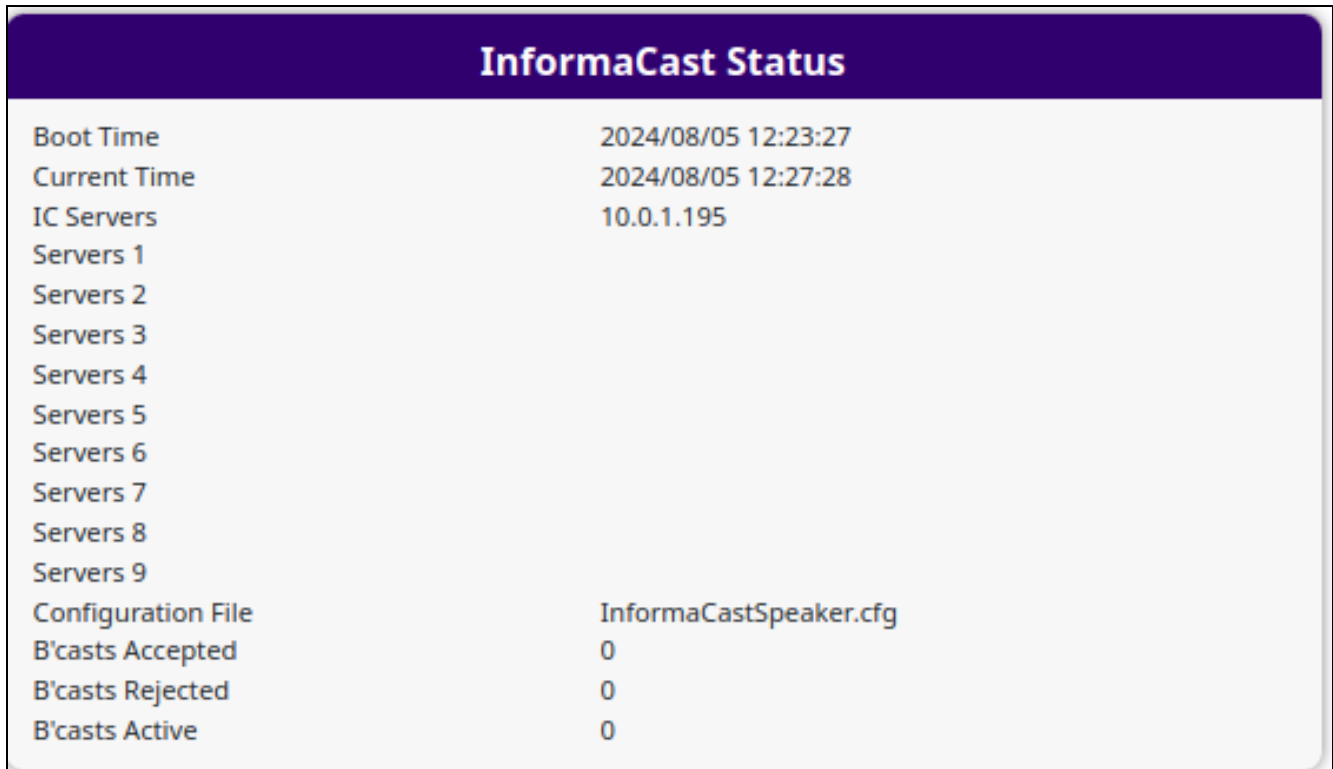
Multicast Volume:	4
-------------------	---
- System Configuration:**

Multicast Mode:	Enabled
Event Mode:	Disabled

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

If you are using the InformaCast Enabled Speaker (011504/011505), you will see the following:

Figure 3-5. InformaCast enabled Device

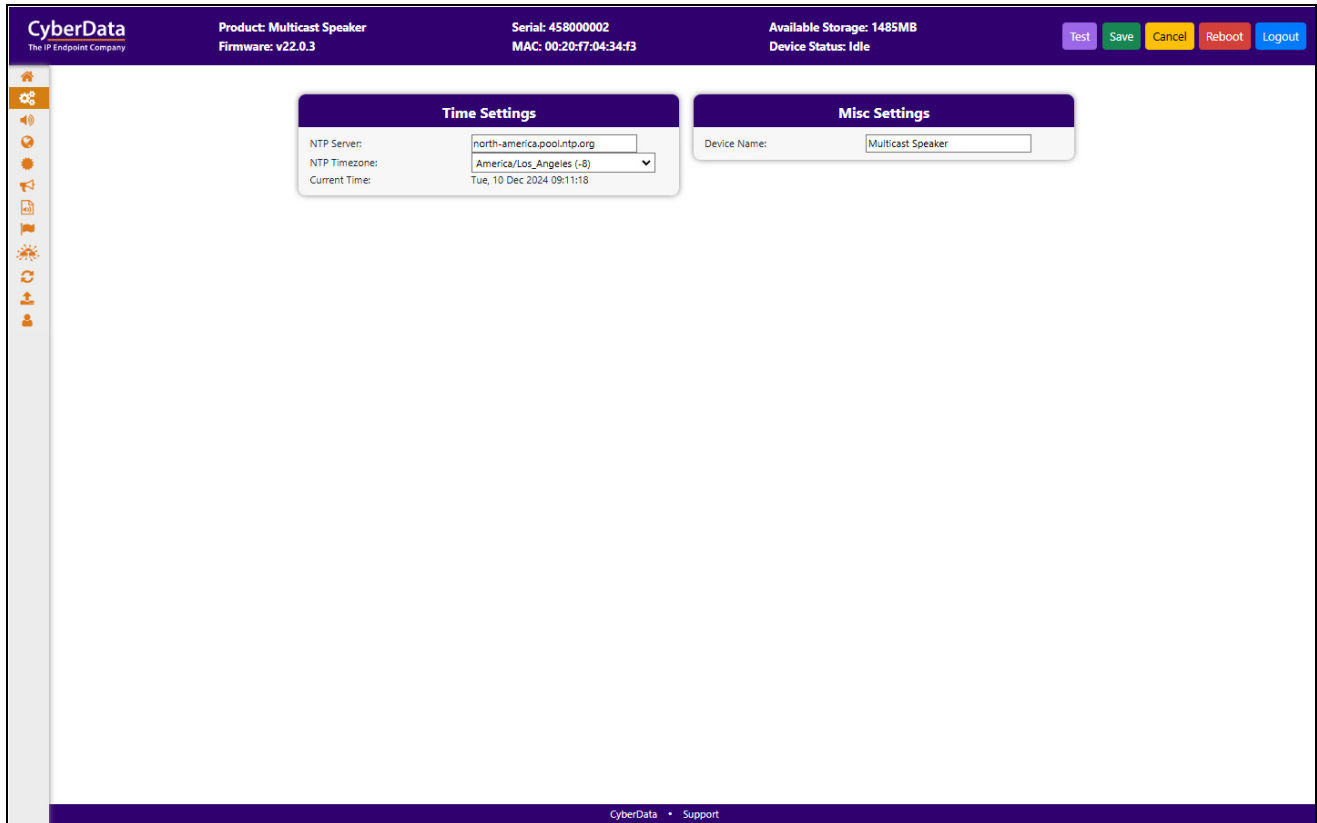


InformaCast Status	
Boot Time	2024/08/05 12:23:27
Current Time	2024/08/05 12:27:28
IC Servers	10.0.1.195
Servers 1	
Servers 2	
Servers 3	
Servers 4	
Servers 5	
Servers 6	
Servers 7	
Servers 8	
Servers 9	
Configuration File	InformaCastSpeaker.cfg
B'casts Accepted	0
B'casts Rejected	0
B'casts Active	0

3.3 Device

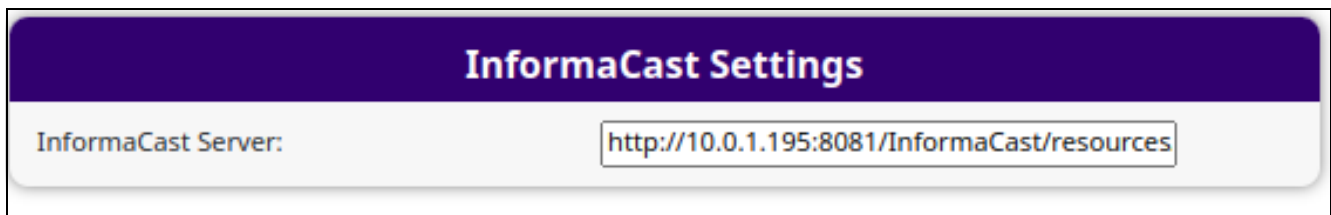
The **Device** page allows for adjustment of settings that pertain to the physical device such as relay settings and time zone.

Figure 3-6. Device Configuration Page



If you are using the InformaCast Enabled Speaker (011504/011505), you will see the following:

Figure 3-7. InformaCast enabled Device



3.4 Audio

Figure 3-8. Audio Page

The screenshot displays the CyberData web interface for configuring audio settings. The top navigation bar includes the CyberData logo, product and firmware information, device serial and MAC addresses, available storage, and device status. Action buttons for Test, Save, Cancel, Reboot, and Logout are located in the top right. The central 'Audio Settings' panel contains the following configuration options:

Setting	Value
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

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

3.5 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 3-9. Network Page

The screenshot displays the Network configuration page for a CyberData device. The header includes the CyberData logo, product information (Multicast Speaker, Firmware v22.0.3), serial and MAC addresses (45800002, 00:20:f7:04:34:f3), available storage (1485MB), and device status (Idle). Action buttons for Test, Save, Cancel, Reboot, and Logout are present.

The main content area is divided into three panels:

- Network Status:**

IP Address Protocol	DHCP
IP Address	10.10.1.31
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:	SipDevice0434f3
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

The footer contains the text "CyberData • Support".

3.6 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 3-10. SSL Page (1 of 2)

The screenshot displays the SSL configuration interface for a CyberData device. At the top, the device's product (Multicast Speaker), serial number (45800002), MAC address (00:20:f7:04:34:e3), and available storage (1485MB) are shown. The page is divided into three main sections:

- Web Server Certificate:** Contains fields for subject details (country, state, locality, organization, common name) and validity dates. It includes buttons for 'Choose Files', 'Import Web Certificate', and 'Restore Web Certificate'.
- Autoprovisioning Client Certificate:** Similar to the web server certificate section, with buttons for 'Import Autoprovisioning Certificate' and 'Restore Autoprovisioning Certificate'. It also features a 'Password (optional):' field.
- List of Trusted CAs:** A table listing installed certificates with 'Info' and 'Remove' actions for each.

Index	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
9	DigiCert_Trusted_Root_G4.crt	Info	Remove

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

The screenshot displays the SSL configuration page for a CyberData device. The header includes the CyberData logo, product information (Multicast Speaker, Firmware: v22.0.3), serial number (45800002), MAC address (00:20:f7:04:34:f3), available storage (1485MB), and device status (Idle). A navigation bar contains buttons for Test, Save, Cancel, Reboot, and Logout. The main content area is a table listing 22 certificates, each with an 'Info' button and a 'Remove' button.

ID	Certificate Name	Info	Remove
8	DigiCert_High_Assurance_EV_Root_CA.crt	Info	Remove
9	DigiCert_Trusted_Root_G4.crt	Info	Remove
10	GeoTrust_Global_CA.crt	Info	Remove
11	GeoTrust_Primary_Certification_Authority.crt	Info	Remove
12	GeoTrust_Primary_Certification_Authority_-_G2.crt	Info	Remove
13	GeoTrust_Primary_Certification_Authority_-_G3.crt	Info	Remove
14	GeoTrust_Universal_CA.crt	Info	Remove
15	GeoTrust_Universal_CA_2.crt	Info	Remove
16	Go_Daddy_Class_2_CA.pem	Info	Remove
17	Go_Daddy_Root_Certificate_Authority_-_G2.pem	Info	Remove
18	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G4.crt	Info	Remove
19	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5.crt	Info	Remove
20	VeriSign_Universal_Root_Certification_Authority.crt	Info	Remove
21	VeriSign_Class_1_Public_Primary_Certification_Authority.crt	Info	Remove
22	VeriSign_Class_1_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
23	VeriSign_Class_2_Public_Primary_Certification_Authority_-_G2.crt	Info	Remove
24	VeriSign_Class_2_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
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

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

3.7 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 3-12. Multicast Page

CyberData
The IP Endpoint Company

Product: Multicast Speaker
Firmware: v22.0.3

Serial: 45800002
MAC: 00:20:F7:04:34:F3

Available Storage: 1485MB
Device Status: Idle

Test Save Cancel Reboot Logout

Multicast Settings

Receive Multicast Audio:

Polycorn Default Channel:

Polycorn Priority Channel:

Polycorn 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

3.8 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.

Figure 3-13. Audiofiles Page

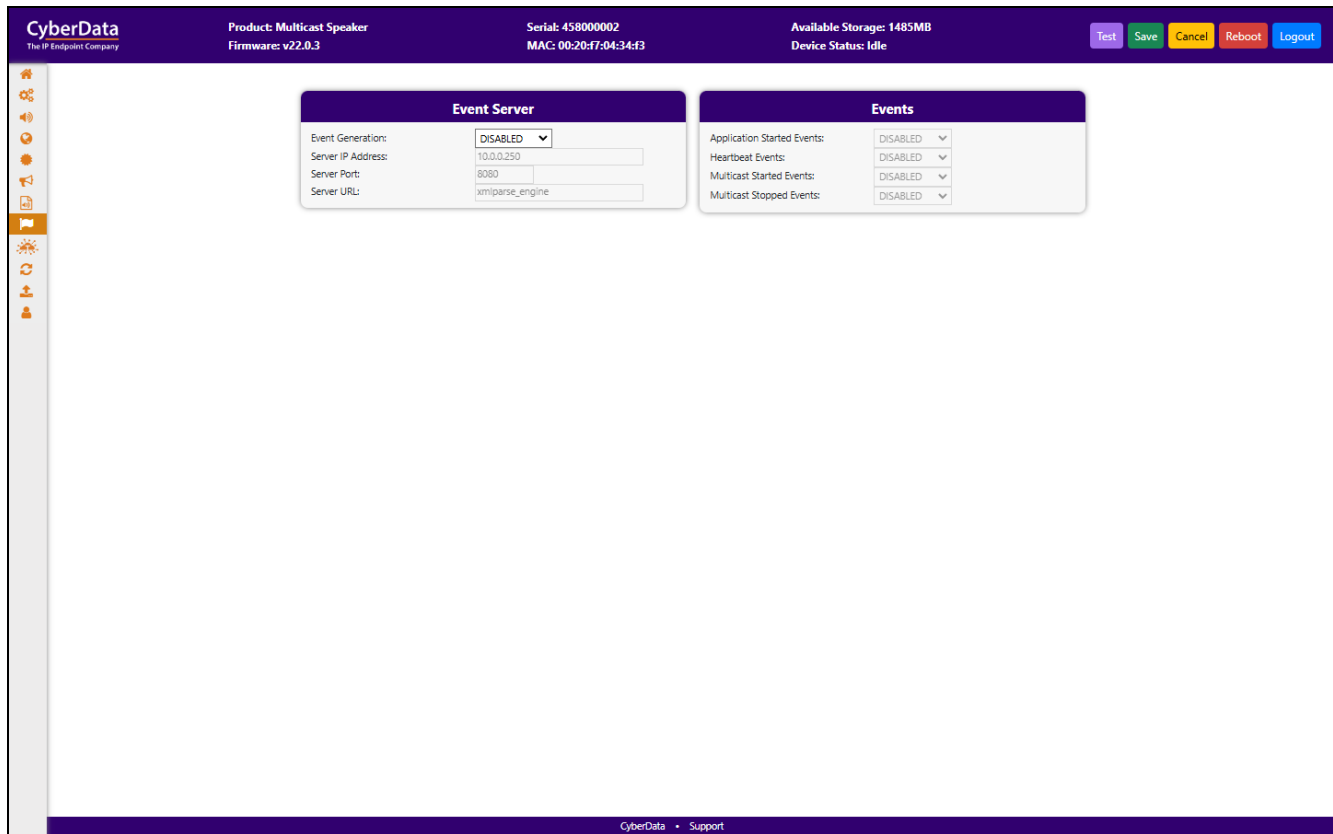
The screenshot displays the 'Audio Files' configuration page in the CyberData web interface. The page header includes the CyberData logo, product information (Multicast Speaker, Firmware: v22.0.3), device details (Serial: 45800002, MAC: 00:20:f7:04:34:f3), and storage status (Available Storage: 1485MB, Device Status: Idle). A navigation bar at the top right contains buttons for Test, Save, Cancel, Reboot, and Logout. The main content area features a table with 13 rows, each representing a different audio file. Each row includes a 'Currently set to:' field (all set to 'default'), a 'Choose File' button, a 'No file chosen' status, and three action buttons: 'Play', 'Save', and 'Delete'. The rows are labeled 0 through 9, followed by 'Audio Test:', 'Dot:', 'Page Tone:', 'Rebooting:', 'Restoring Default:', and 'Your IP Address Is:'.

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

3.9 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 3-14. Events Page



If you are using the InformaCast Enabled Speaker (011504/011505), you will see the following:

Figure 3-15. InformaCast enabled Device



3.9.1 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>
```


3.10 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 3-16. Terminus Page

The screenshot shows the Terminus configuration page within the CyberData web interface. The page has a purple header bar with the following information:

- CyberData** The IP Endpoint Company
- Product: Multicast Speaker
- Firmware: v22.0.3
- Serial: 45800002
- MAC: 00:20:f7:04:34:f3
- Available Storage: 1485MB
- Device Status: Idle

On the right side of the header bar, there are five buttons: Test (purple), Save (green), Cancel (yellow), Reboot (red), and Logout (blue).

The main content area features a central "Discovery Setting" dialog box with the following fields:

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

A vertical sidebar on the left contains several icons, with the "Discovery" icon (a sun-like symbol) highlighted in orange. At the bottom of the page, there is a footer with the text "CyberData • Support".

3.11 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 3-17. Autoprovisioning Page

The screenshot displays the Autoprovisioning configuration interface. At the top, the device information includes: Product: Multicast Speaker, Firmware: v22.0.3, Serial: 45800002, MAC: 00:20:f7:04:34:f3, Available Storage: 1485MB, and Device Status: Idle. Action buttons for Test, Save, Cancel, Reboot, and Logout are present.

The **Autoprov Settings** panel contains the following fields:

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

A **Download Template** button is located below the settings.

The **Autoprov Log** panel shows the following log entries:

```

2024-12-08 11:16:52 Autoprov: no autoprov triggers. Exiting...
2024-12-08 11:16:57 Autoprovisioning on boot
2024-12-08 11:16:57 Autoprov found server='http://10.0.0.242' in dhcp option 43
2024-12-08 11:16:57 Autoprov looking for 0020f70434f3.xml at http://10.0.0.242
2024-12-08 11:16:57 Autoprov downloading http://10.0.0.242/0020f70434f3.xml
2024-12-08 11:16:57 download_file: download failed
2024-12-08 11:16:57 Autoprov looking for 000000cd.xml at http://10.0.0.242
2024-12-08 11:16:57 Autoprov downloading http://10.0.0.242/000000cd.xml
2024-12-08 11:16:57 download_file: download failed
2024-12-08 11:16:57 Autoprov: Failed to fetch autoprov file
2024-12-08 11:16:57 Autoprov found server='10.0.1.118' in dhcp option 72
2024-12-08 11:16:57 Autoprov looking for 0020f70434f3.xml at 10.0.1.118
2024-12-08 11:16:57 Autoprov downloading 10.0.1.118/0020f70434f3.xml
2024-12-08 11:17:01 download_file: download failed
  
```

The footer of the page includes the CyberData logo and a link to Support.

3.12 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


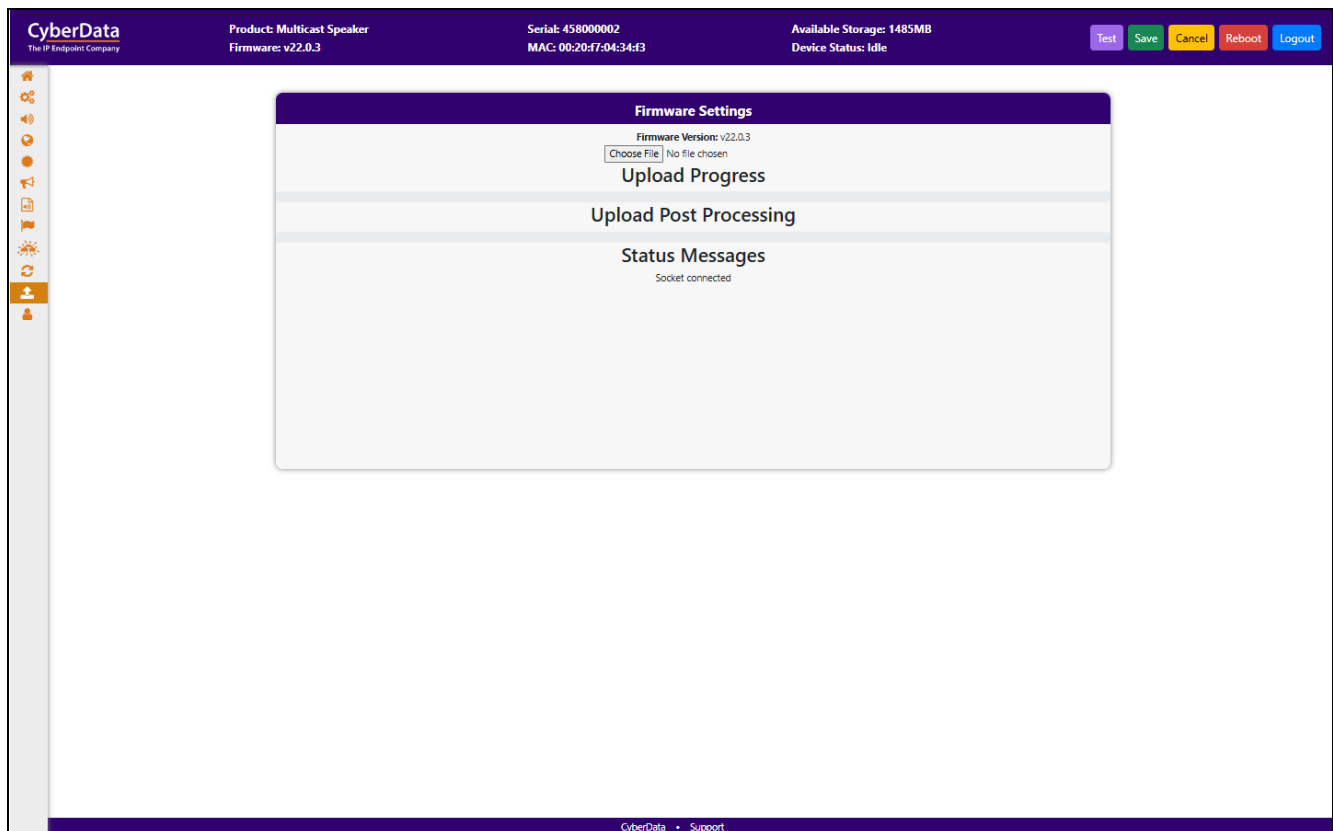
 GENERAL ALERT	<p>Caution</p> <p>Equipment Hazard: Do not reboot the device. It will reboot automatically when the process is complete.</p>
--	--

Figure 3-18. Firmware Page



3.13 Admin

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

Figure 3-19. Admin Page

The screenshot displays the CyberData Admin Page for a Multicast Speaker device. The top navigation bar includes the CyberData logo, product information (Multicast Speaker, Firmware: v22.0.3), serial and MAC addresses, available storage (1485MB), and device status (Idle). Action buttons for Test, Save, Cancel, Reboot, and Logout are present.

The main content area is divided into several sections:

- Admin Settings:** Fields for Username (admin), Password, and Confirm Password.
- Statistics:** Shows Storage (1485MB), Boot Count (3), Reboot Count, and Uptime (up 1 day, 21 hours, 57 minutes).
- Logging Settings:** Includes Debug Level (4) and Log Network Traffic (OFF). Buttons for Get/Remove Application, Network, and All Logs are provided.
- Configuration Settings:** Lists Partition 2 (v22.0.3), Partition 3 (v22.0.3), and Booting Partition (partition 2). Buttons for Restore Default Config, Restore Default Certificates, Import/Export Config, and Boot From Other Partition are available.
- Users List:** Features buttons for Add New User, Delete All Users, Import Users, and Export Users. A table header lists columns: Username, Home, Device, Audio, Network, SSL, Multicast, Audiofiles, Events, Terminus, Autopro, Firmware, and Admin.
- Log Viewer:** Includes a Service dropdown (Application), Entries to get (250), Sort (Oldest), and a View Log button.

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

3.14 Command Interface

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

3.14.1 Command Interface Post Commands

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

Table 3-2. Command Interface Post Commands

Device Action	HTTP Post Command ^a
Reboot	<code>wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.154/command" --post-data "request=reboot"</code>
Test Audio	<code>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"</code>
Speak IP Address	<code>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"</code>
Play the "0" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "0=Play"</code>
Play the "1" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "1=Play"</code>
Play the "2" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "2=Play"</code>
Play the "3" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "3=Play"</code>
Play the "4" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "4=Play"</code>
Play the "5" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "5=Play"</code>
Play the "6" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "6=Play"</code>
Play the "7" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "7=Play"</code>

Table 3-2. Command Interface Post Commands (continued)

Device Action	HTTP Post Command^a
Play the "8" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "8=Play"</code>
Play the "9" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "9=Play"</code>
Play the "Dot" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "d=Play"</code>
Play the Audio Test	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "audiotest=Play"</code>
Play the "Page Tone" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "pagetone=Play"</code>
Play the "Your IP Address Is" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "youripaddressis=Play"</code>
Play the "Rebooting" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "rebooting=Play"</code>
Play the "Restoring Default" audio file	<code>wget --user admin --password admin --auth-no-challenge --no-check-certificate "https://10.10.1.138/audiofiles/" --quiet -O /dev/null --post-data "restoringdefault=Play"</code>
Swap boot partitions	<code>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"</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

A

Admin 22
Audio 9
Audiofiles 14

C

Command Interface 23
Command Interface Post Commands 23

D

Device 8

E

Events 15

F

Firmware 21

H

Home Page 6

M

Multicast 13

N

Network 10

S

SSL 11

T

Terminus 19

W

Warranty and RMA Information 25