



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


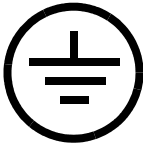
Fax: (831) 373-4193

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

Revision Information

Revision 932056A, which corresponds to firmware version 22.0, was released on January 21, 2025.

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!

 GENERAL ALERT	<p>Warning</p> <p><i>Electrical Hazard:</i> This product should be installed by a licensed electrician according to all local electrical and building codes.</p>
 GENERAL ALERT	<p>Warning</p> <p><i>Electrical Hazard:</i> To prevent injury, this apparatus must be securely attached to the floor/wall in accordance with the installation instructions.</p>
 GENERAL ALERT	<p>Warning</p> <p>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 011505)	 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	 24
A.1 Contact Information	24
A.2 Warranty and RMA Information	24
 Index	 25

1 Multicast Ceiling Speaker Device Setup

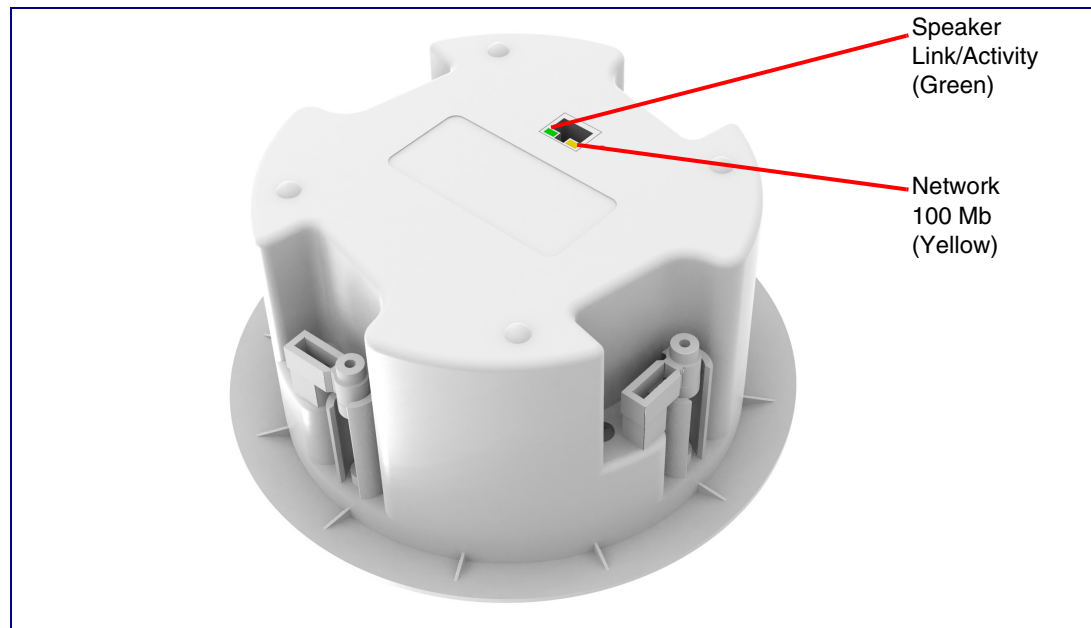
(Part #011458 and 011504)

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.

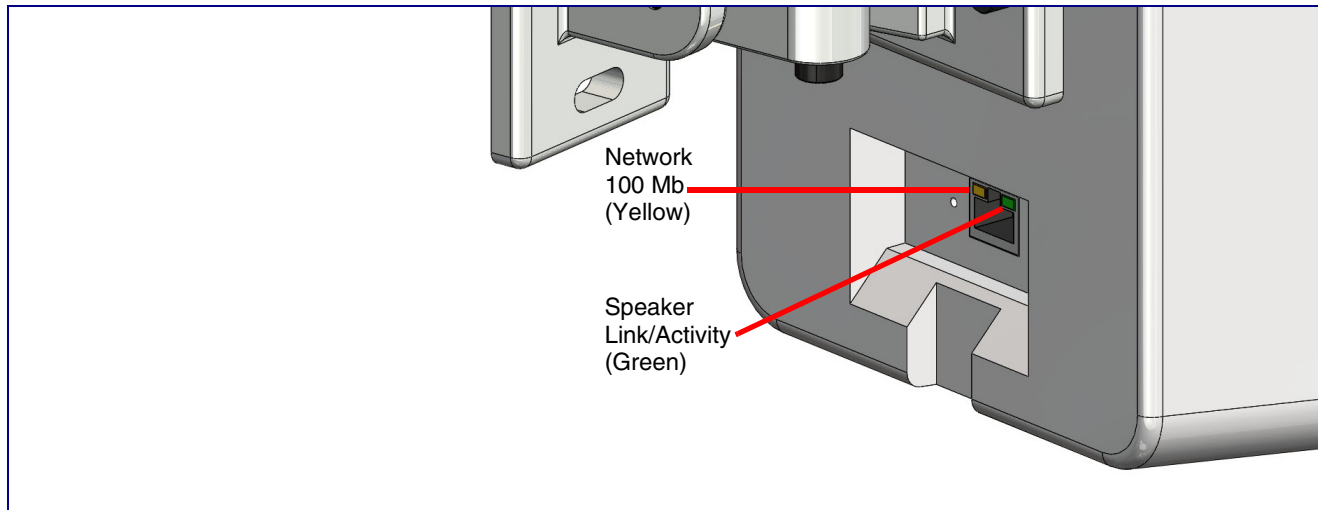
2 Multicast Wall Mount Speaker Device Setup (Part #011487 and 011505)

2

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>

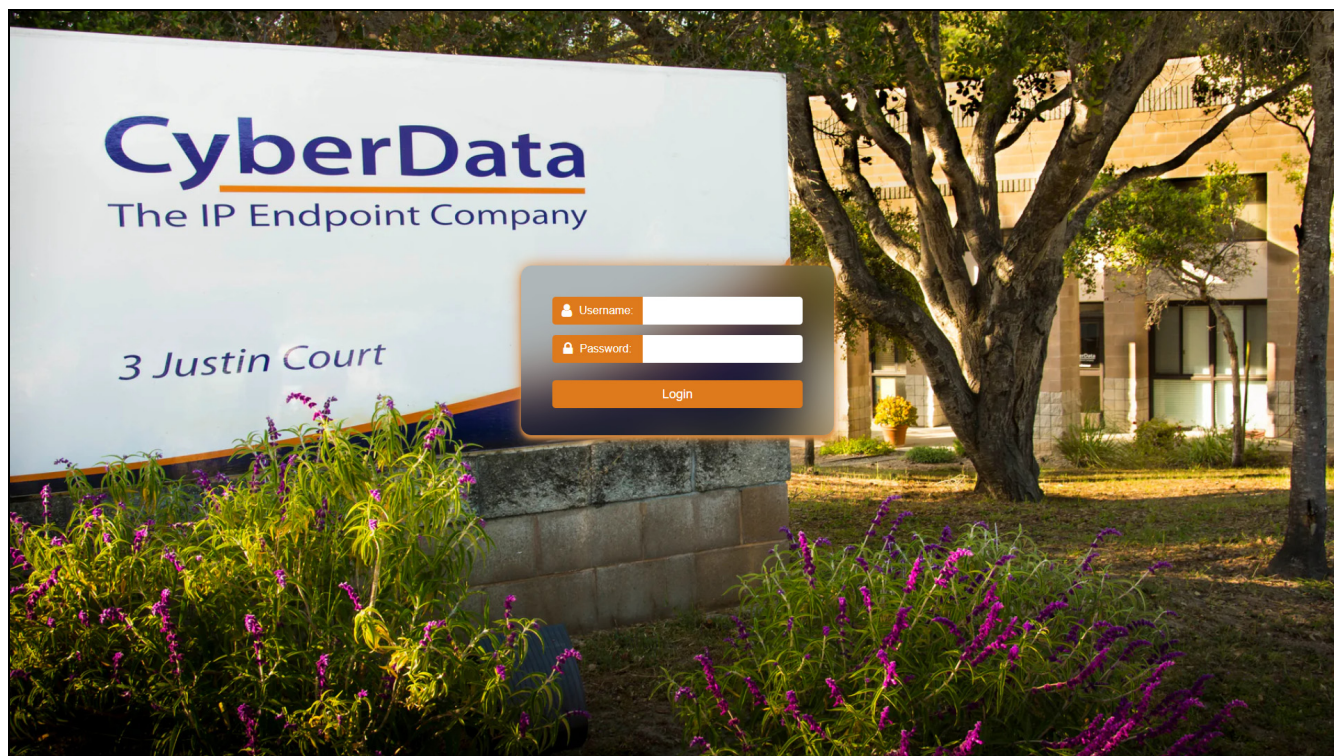
Note The Intercom ships in DHCP mode. To get to the **Home** page, use the discovery utility to scan for the device on the network and open your browser from there.

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)

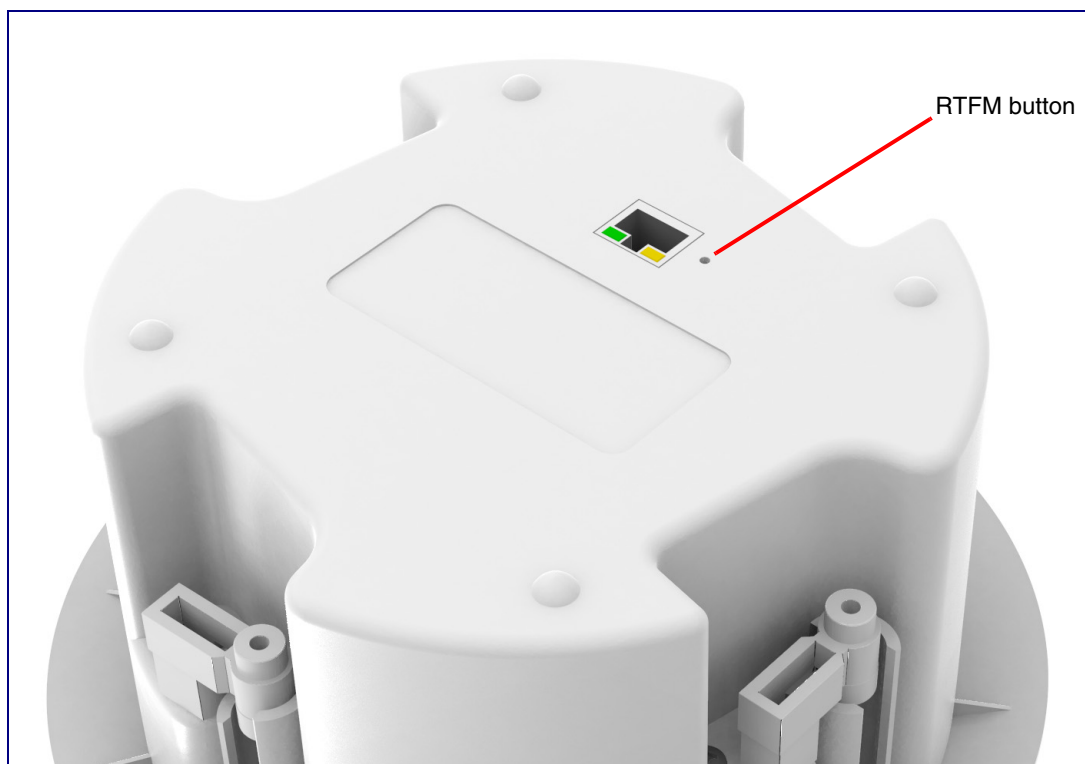
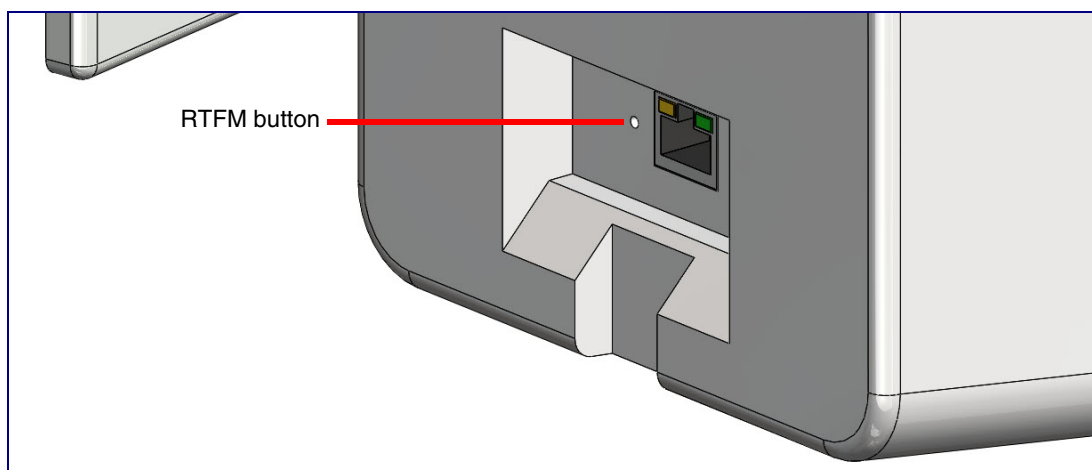


Figure 3-3. RTFM Button (Wall Mount Speakers)



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

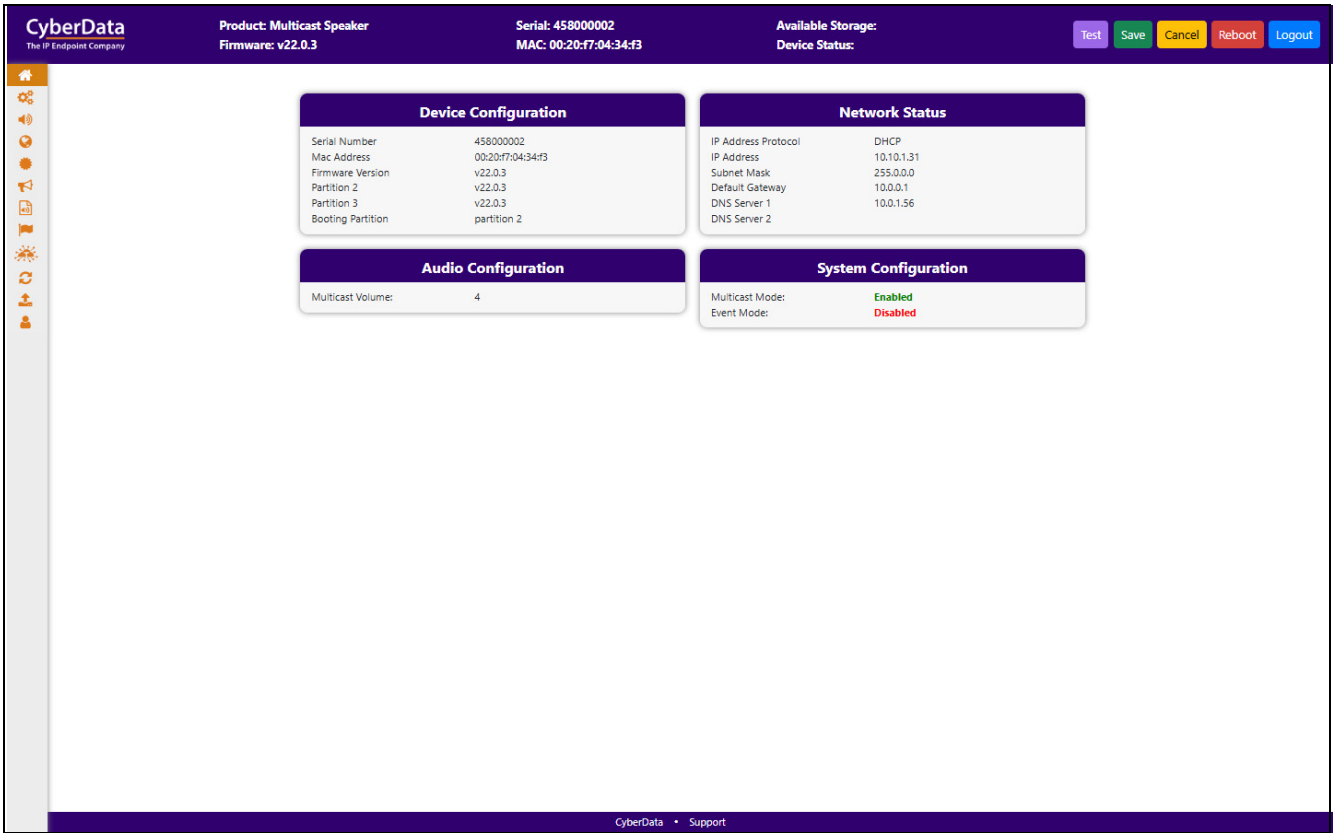
Parameter	Factory Default Setting
IP Addressing	DHCP
IP Address ^a	192.168.1.23
Web Access Username	admin
Web Access Password	admin
Subnet Mask ^a	255.255.255.0
Default Gateway ^a	192.168.1.1

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



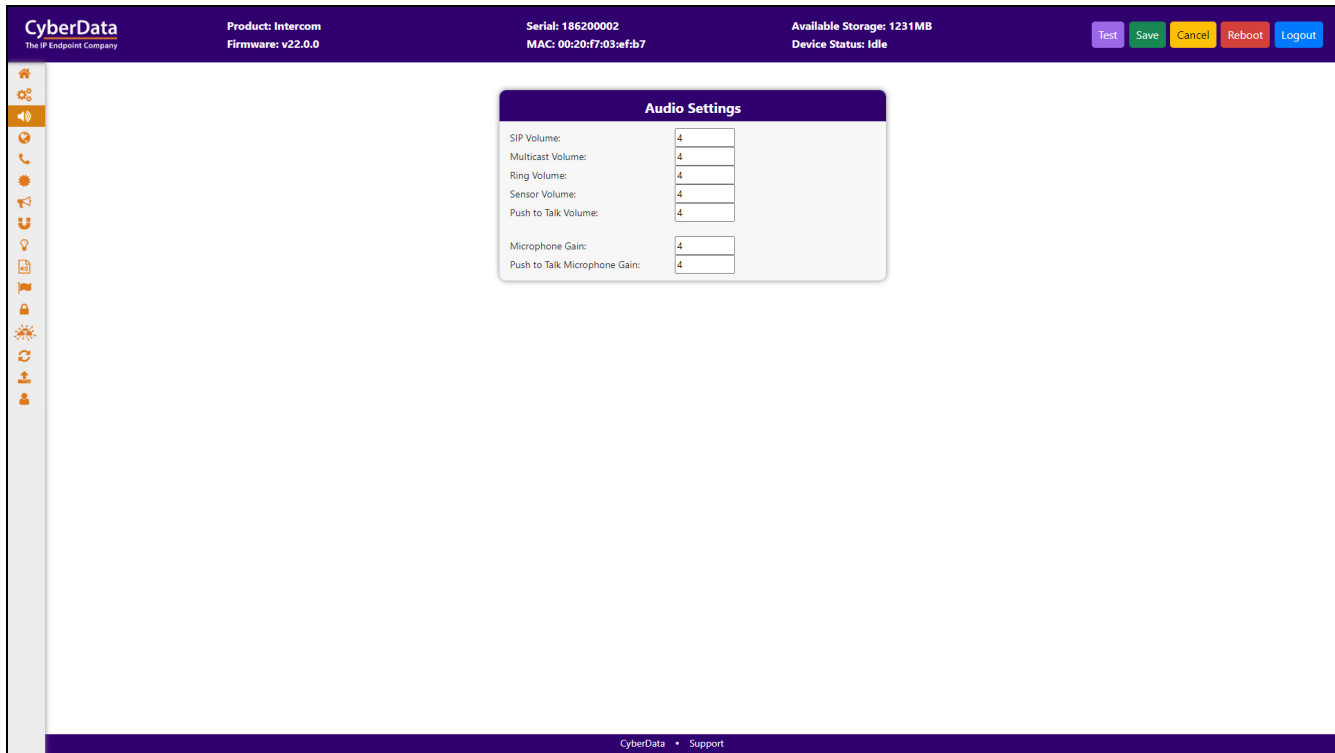
If you are using the InformaCast Enabled Speaker (011504/011505), you will see the following:

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

3.4 Audio

Figure 3-8. Audio Page



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

CyberData
The IP Endpoint Company

Product: Multicast Speaker

Firmware: v22.0.3

Serial: 458000002

MAC: 00:20:f7:04:34:f3

Available Storage: 1485MB

Device Status: Idle

Test

Save

Cancel

Reboot

Logout

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

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, 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)

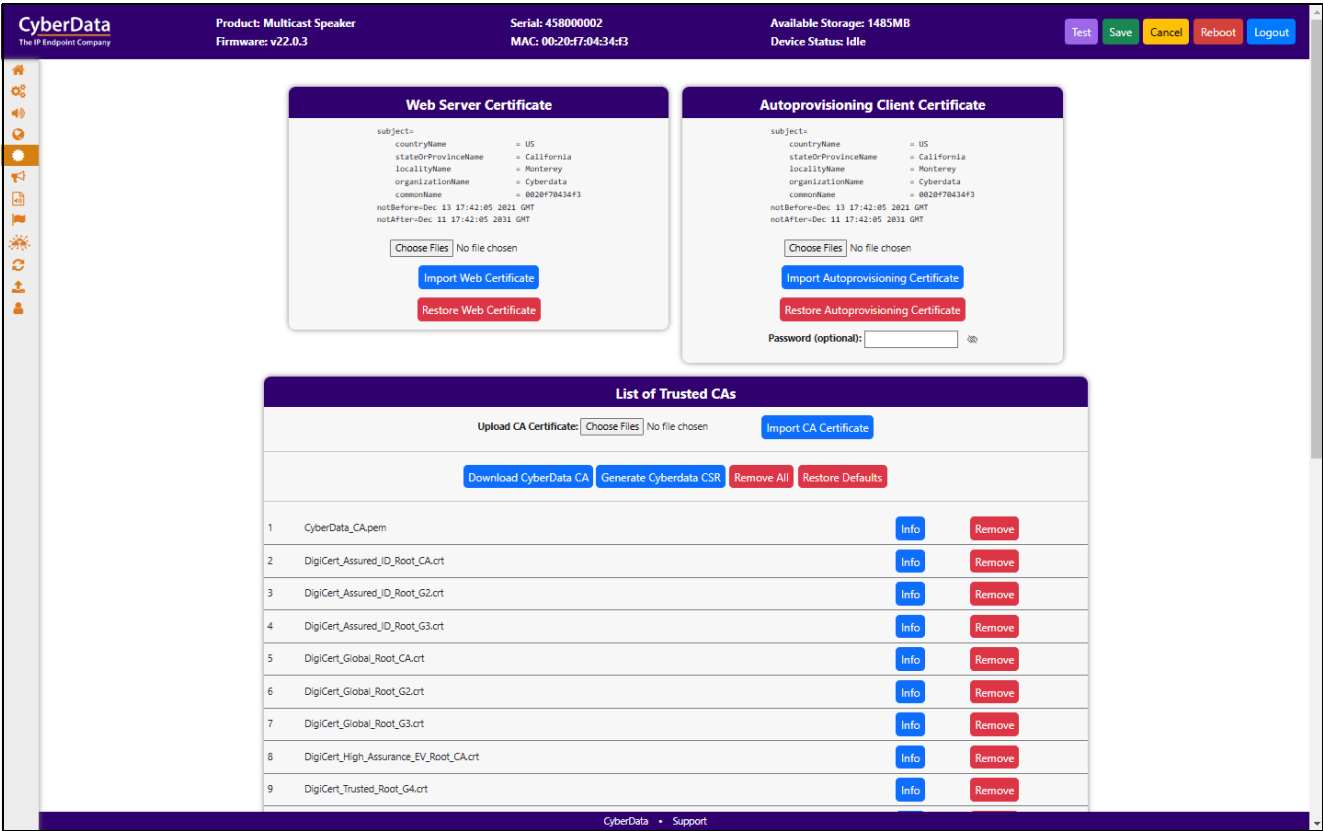


Figure 3-11. SSL Page (2 of 2)

CyberData
The IP Endpoint Company

Product: Multicast Speaker
Firmware: v22.0.3

Serial: 458000002
MAC: 00:20:f7:04:34:f3

Available Storage: 1485MB
Device Status: Idle

[Test](#)
[Save](#)
[Cancel](#)
[Reboot](#)
[Logout](#)

#	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

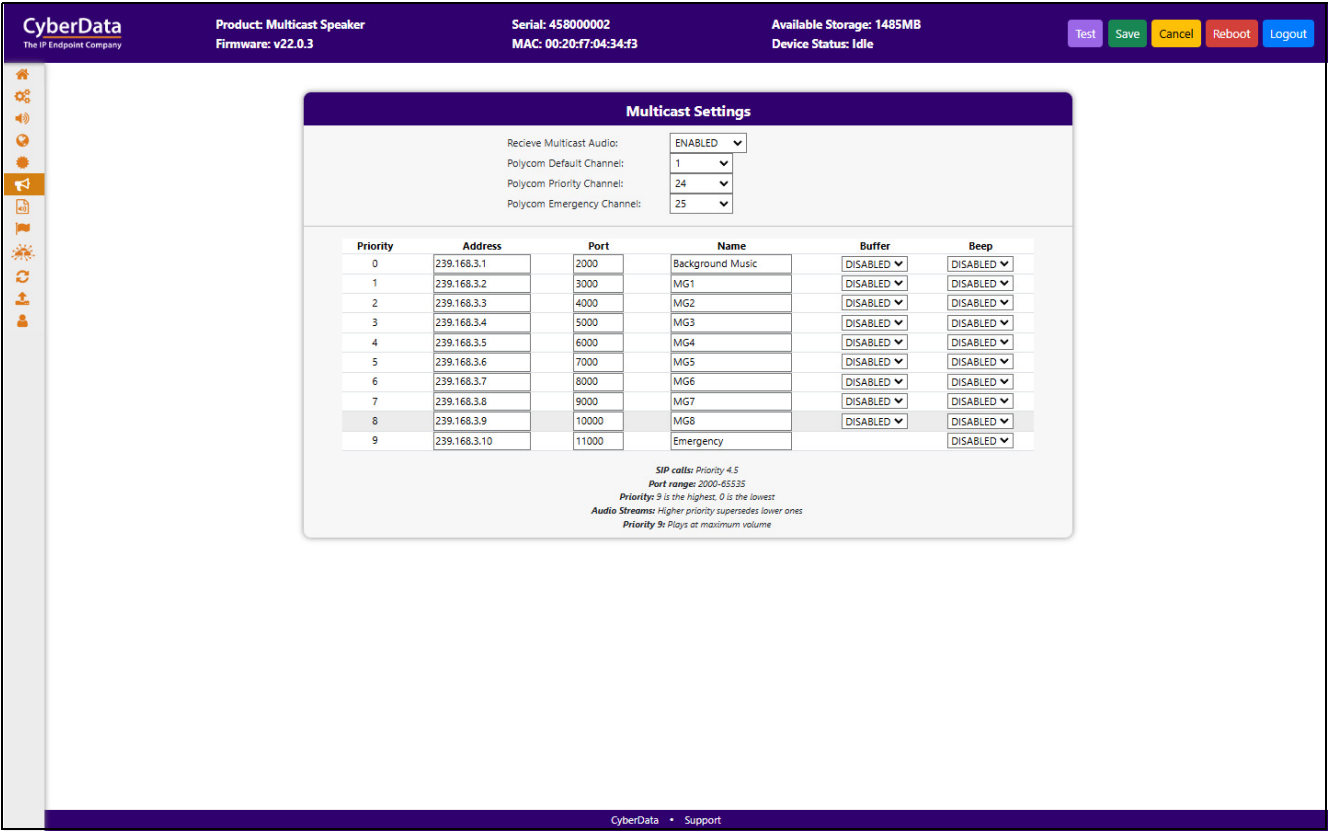
3.7 Multicast

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



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

CyberData
The IP Endpoint Company

Product: Multicast Speaker
Firmware: v22.0.3

Serial: 458000002
MAC: 00:20:d7:04:34:f3

Available Storage: 1485MB
Device Status: Idle

Test Save Cancel Reboot Logout

Audio Files

0:	Currently set to:	default	<input type="button" value="Choose File"/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
1:	Currently set to:	default	<input type="button" value="Choose File"/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
2:	Currently set to:	default	<input type="button" value="Choose File"/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
3:	Currently set to:	default	<input type="button" value="Choose File"/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
4:	Currently set to:	default	<input type="button" value="Choose File"/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
5:	Currently set to:	default	<input type="button" value="Choose File"/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
6:	Currently set to:	default	<input type="button" value="Choose File"/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
7:	Currently set to:	default	<input type="button" value="Choose File"/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
8:	Currently set to:	default	<input type="button" value="Choose File"/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
9:	Currently set to:	default	<input type="button" value="Choose File"/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
Audio Test:	Currently set to:	default	<input type="button" value="Choose File"/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
Dot:	Currently set to:	default	<input type="button" value="Choose File"/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
Page Tone:	Currently set to:	default	<input type="button" value="Choose File"/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
Rebooting:	Currently set to:	default	<input type="button" value="Choose File"/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
Restoring Default:	Currently set to:	default	<input type="button" value="Choose File"/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
Your IP Address Is:	Currently set to:	default	<input type="button" value="Choose File"/>	No file chosen	<input type="button" value="Play"/>	<input type="button" value="Save"/>	<input type="button" value="Delete"/>

CyberData • Support

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

CyberData
The IP Endpoint Company

Product: Multicast Speaker
Firmware: v22.0.3

Serial: 458000002
MAC: 00:20:f7:04:34:f3

Available Storage: 1485MB
Device Status: Idle

TestSaveCancelRebootLogout

Event Server

Event Generation:
Server IP Address:
Server Port:
Server URL:

DISABLED
10.0.0.250
8080
xmiparse_engine

Events

Application Started Events:
Heartbeat Events:
Multicast Started Events:
Multicast Stopped Events:

DISABLED
DISABLED
DISABLED
DISABLED

CyberData • Support

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

Figure 3-15. InformaCast enabled Device

InformaCast Start Events:

DISABLED

InformaCast Stop Events:

DISABLED

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>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>
```


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 displays the Terminus configuration page within the CyberData web interface. The top header bar is purple and contains the following information: CyberData logo, Product: Multicast Speaker, Firmware: v22.0.3, Serial: 45800002, MAC: 00:20:f7:04:34:f3, Available Storage: 1485MB, and Device Status: Idle. On the right side of the header are buttons for Test, Save, Cancel, Reboot, and Logout. A vertical sidebar on the left contains various icons, with the 'Discovery' icon highlighted. The main content area features a 'Discovery Setting' dialog box with the following fields: Multicast Address (239.27.32.4), Time to Live (255), and Discovery Interval (60 seconds). The footer of the page shows '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 for a CyberData device. The top header 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 (Test, Save, Cancel, Reboot, Logout) are located in the top right.

The main content area is divided into two panels:

- Autoprov Settings:** Contains configuration options for Autoprov (ENABLED), Autoprov Server, Autoprov Filename, Use tftp (DISABLED), Verify Server Certificate (DISABLED), Username, Password, Autoprov autoupdate (0 minutes), Autoprov at time (HHMM), and Autoprov when idle (0 minutes). A 'Download Template' button is at the bottom.
- Autoprov Log:** A scrollable log showing the following sequence of events:
 - 2024-12-08 11:16:52 Autoprov: no autoprov triggers. Exiting...
 - 2024-12-08 11:16:57 Autoprov: provisioning 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 002070434f3.xml at http://10.0.0.242
 - 2024-12-08 11:16:57 Autoprov downloading http://10.0.0.242/002070434f3.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 002070434f3.xml at 10.0.1.118
 - 2024-12-08 11:16:57 Autoprov downloading 10.0.1.118/002070434f3.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


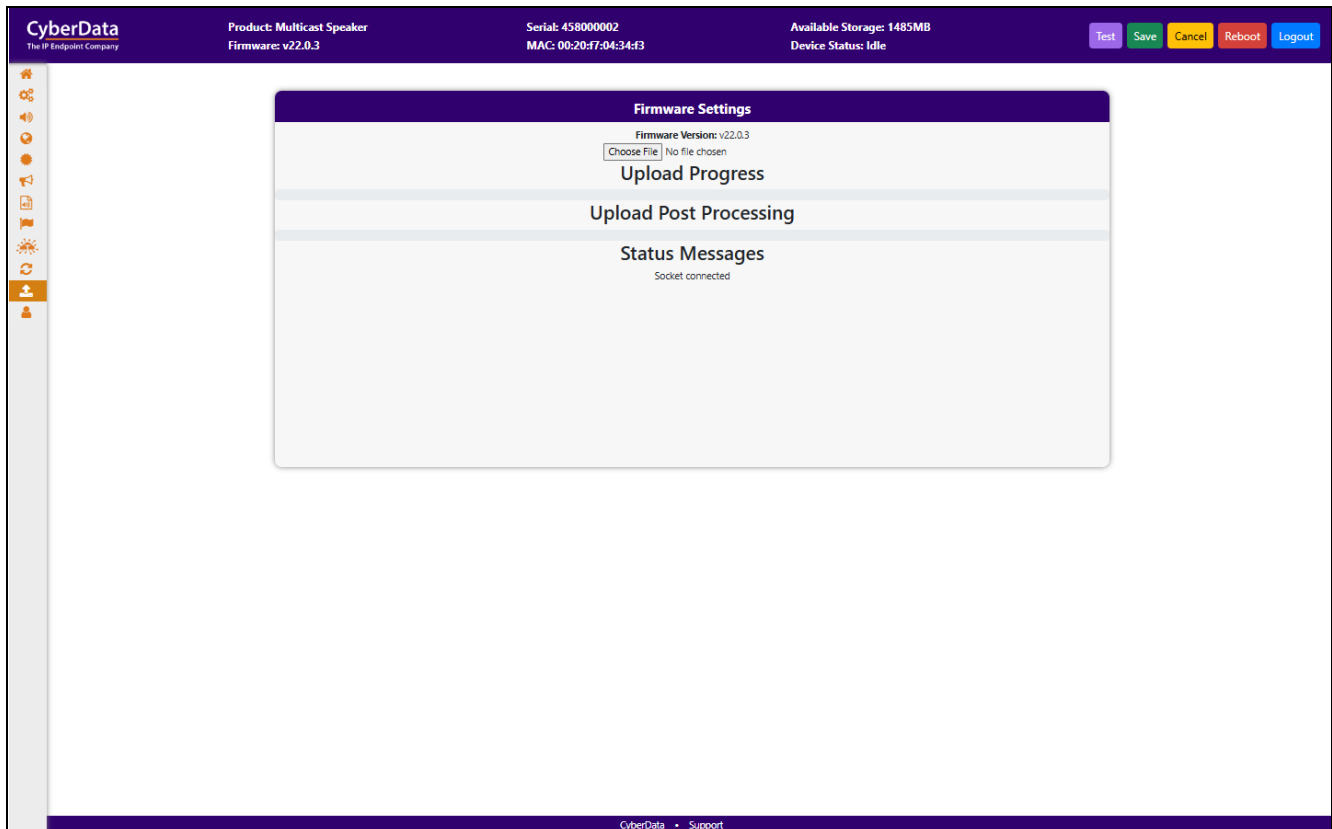
 GENERAL ALERT	Caution Equipment Hazard: Do not reboot the device. It will reboot automatically when the process is complete.
--	---

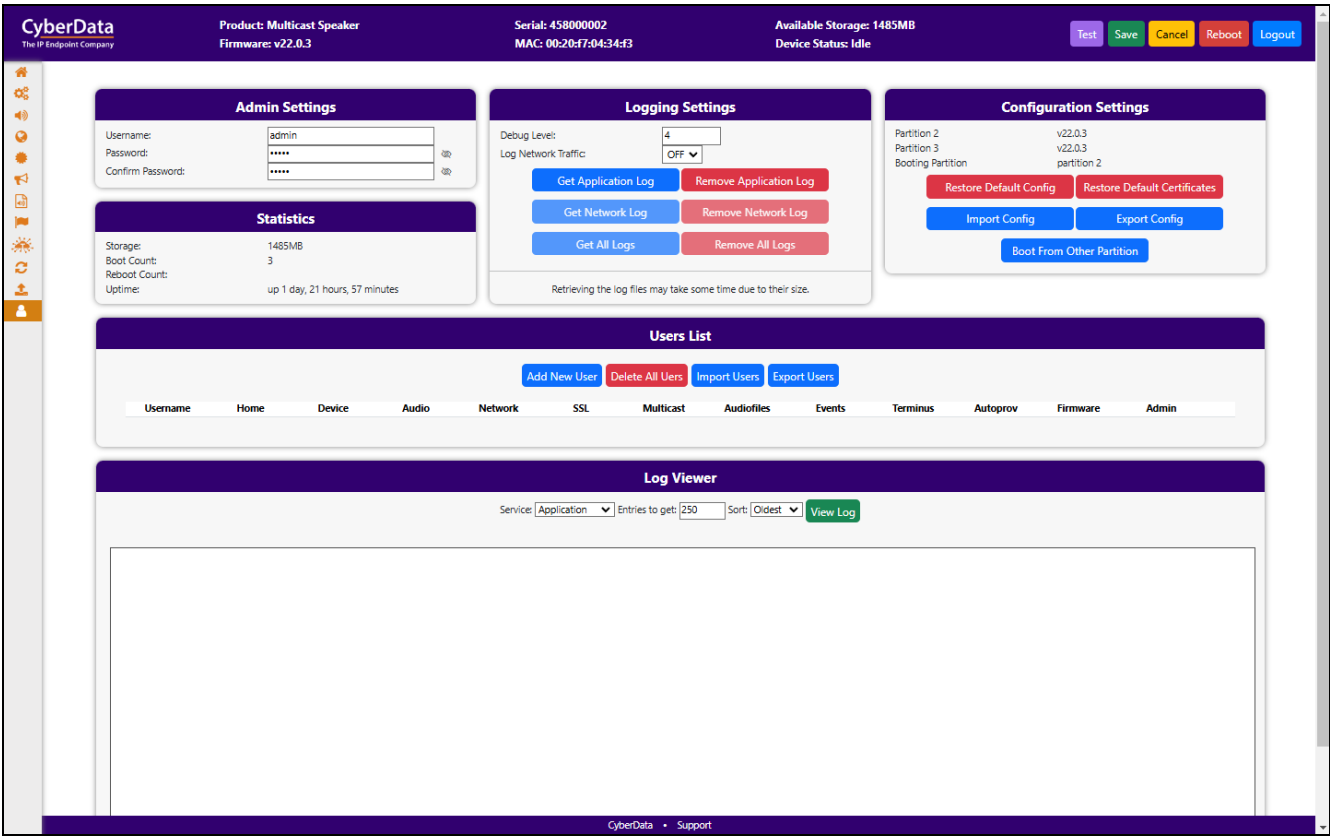
Figure 3-18. Firmware Page



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



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	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"
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"
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"
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"

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 The fastest way to get technical support for your VoIP product is to submit a VoIP Technical
Support 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 24