



*VoIP SIP/Multicast Speaker
Operations Guide*

Part #011511, 011512

Document Part #932057A
for Firmware Version 22.0

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

VoIP SIP/Multicast Speaker Operations Guide 932057A
Part # 011511, 011512

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.

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

Email: support@cyberdata.net

Fax: (831) 373-4193

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

Revision Information

Revision 932057A, which corresponds to firmware version 22.0, was released on November 19, 2024.

Alert Icons

 <p>GENERAL ALERT</p>	<p>General Alert</p> <p><i>This 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 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 VoIP SIP/Multicast Speaker enclosure is not rated for any AC voltages!

 <p>GENERAL ALERT</p>	<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>
 <p>GENERAL ALERT</p>	<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>
 <p>GENERAL ALERT</p>	<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
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

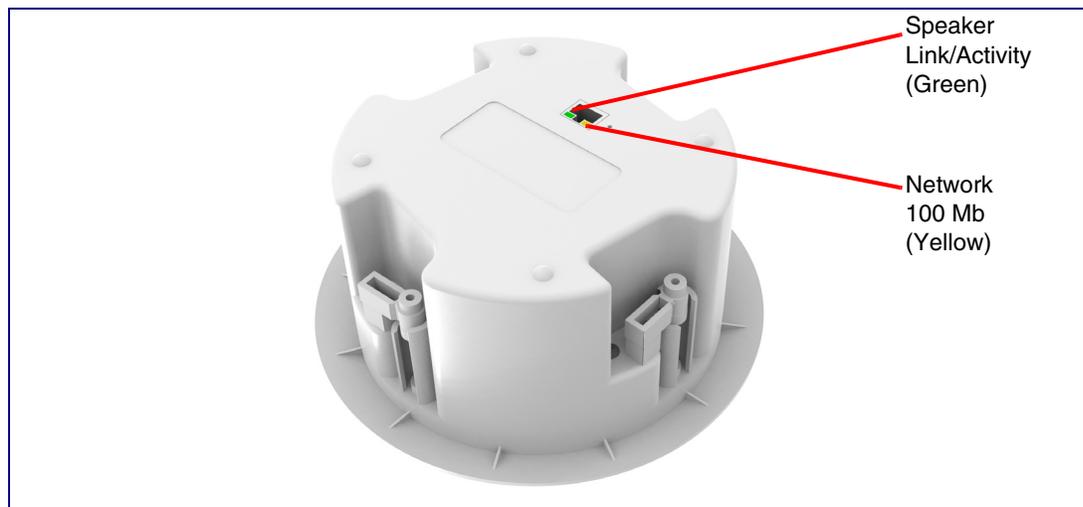
Chapter 1 Ceiling Speaker Device Setup (Part #011511)	1
1.1 Confirm that the Speaker is Operational and Linked to the Network	1
1.2 Link/Activity LED	1
1.2.1 100 Mb LED	1
Chapter 2 Wall Mount Speaker Device Setup (Part #011512)	2
2.1 Confirm that the Speaker is Operational and Linked to the Network	2
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	7
3.4 Audio	8
3.5 Network	9
3.6 SIP (Session Initiation Protocol)	10
3.6.1 Dial Out Extension Strings and DTMF Tones (using rfc2833)	10
3.6.2 Point-to-Point Configuration	11
3.7 SSL	12
3.8 Multicast	14
3.9 Audiofiles	15
3.10 Events	16
3.10.1 Example Packets for Events	17
3.11 Terminus	20
3.12 Autoprovisioning	21
3.13 Firmware	22
3.14 Admin	23
3.15 Command Interface	24
3.15.1 Command Interface Post Commands	24
Appendix A Troubleshooting/Technical Support	26
A.1 Contact Information	26
A.2 Warranty and RMA Information	26
Index	27

1 Ceiling Speaker Device Setup (Part #011511)

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 192.168.1.23). This process will take approximately 80 seconds.

1.2.1 100 Mb LED

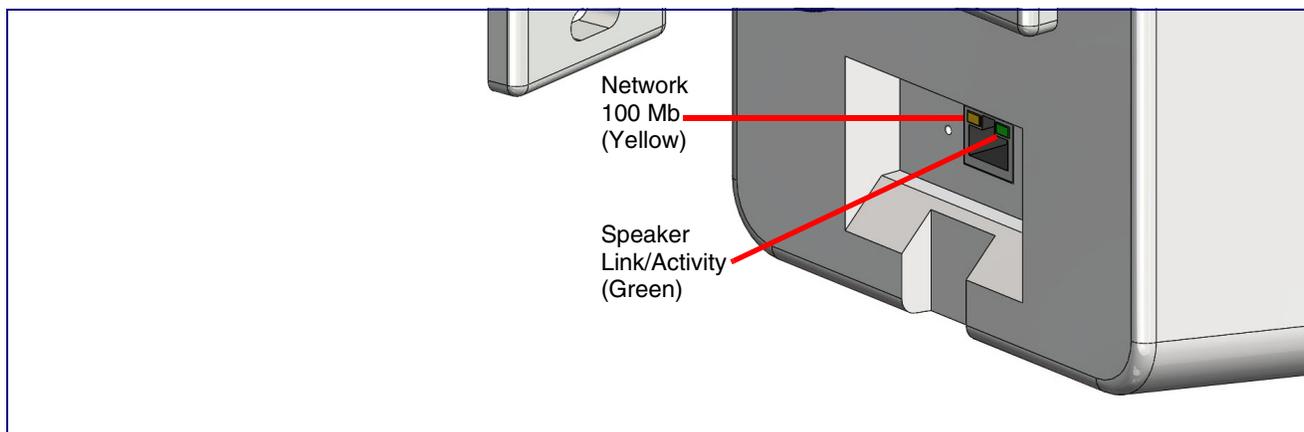
- The yellow **100 Mb** LED is illuminated when the network 100 Mb link to the speaker is established.

2 Wall Mount Speaker Device Setup (Part #011512)

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 192.168.1.23). 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 VoIP SIP/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>

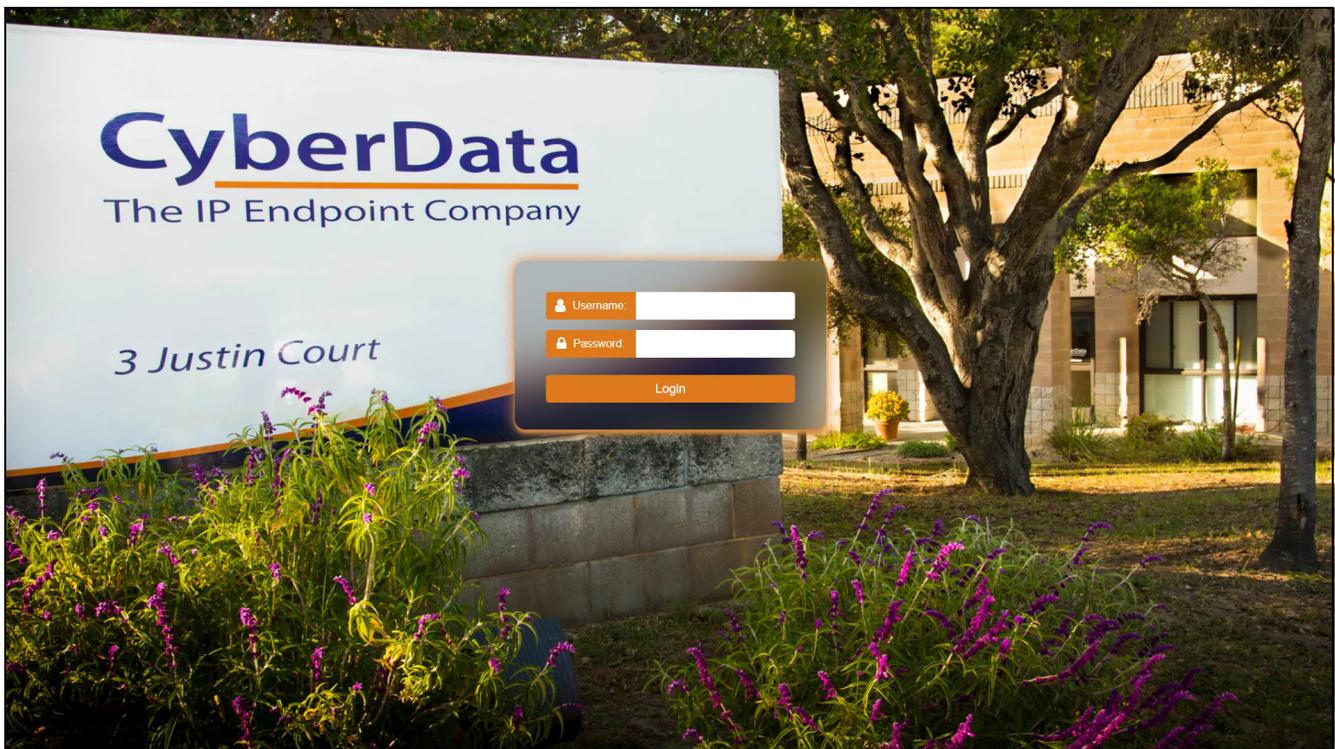
Note The Intercom ships in DHCP mode. To get to the **Home** page, use the discovery utility to scan for the device on the network and open your browser from there.

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

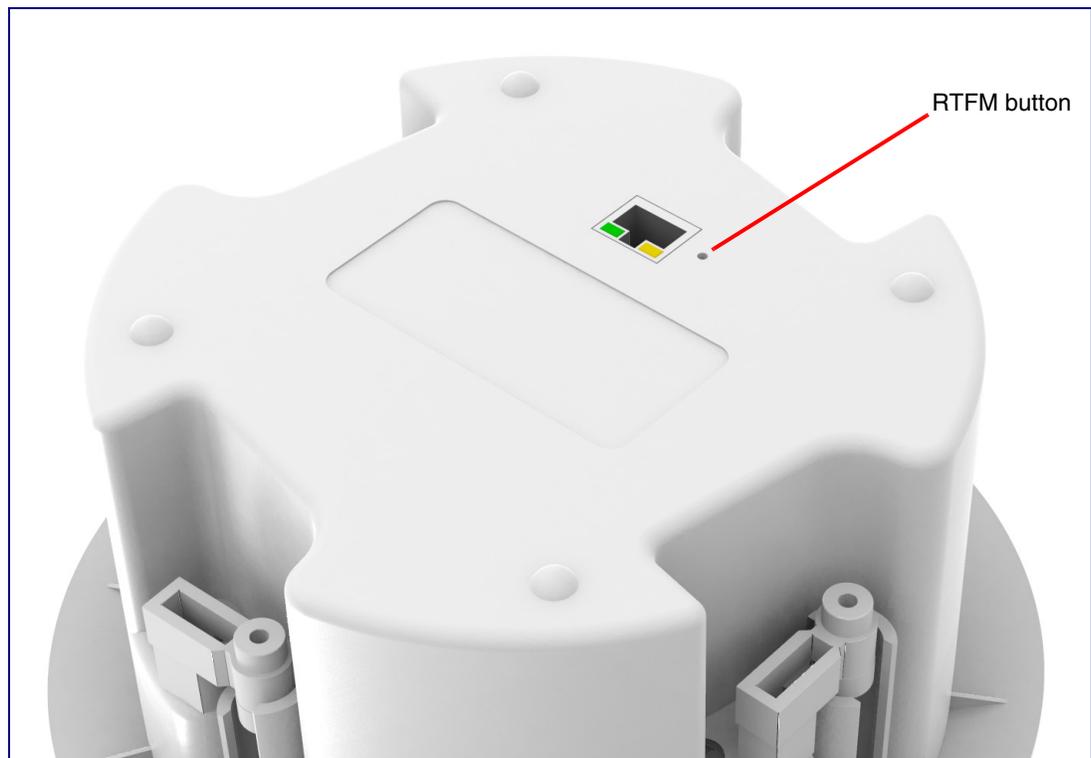
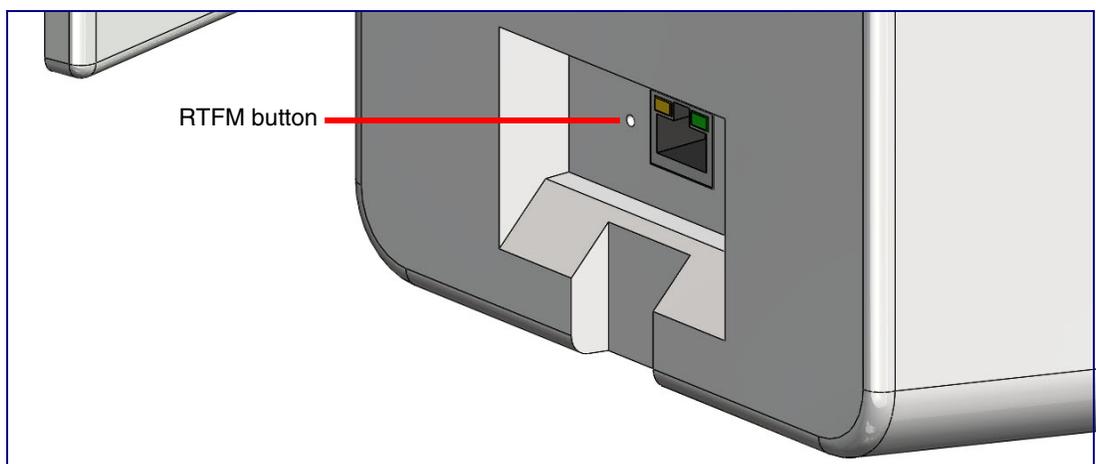


Figure 3-3. RTFM Button



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 (VoIP Speaker, v22.0.3), serial and MAC addresses, available storage (1381MB), and device status (Idle). Action buttons for Test, Save, Cancel, Reboot, and Logout are also present. The main content area is divided into five configuration panels:

- Device Configuration:**

Serial Number	511000002
Mac Address	00:20:f7:04:d6:b4
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	10.10.1.52
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
- Audio Configuration:**

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

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

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

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 3-5. Device Configuration Page

The screenshot displays the CyberData Device Configuration Page. At the top, a purple header bar contains the CyberData logo and the following information: Product: VoIP Speaker, Serial: 511000002, Available Storage: 1381MB, Firmware: v22.0.3, MAC: 00:20:F7:04:d6:b4, and Device Status: Idle. Action buttons for Test, Save, Cancel, Reboot, and Logout are located on the right side of the header.

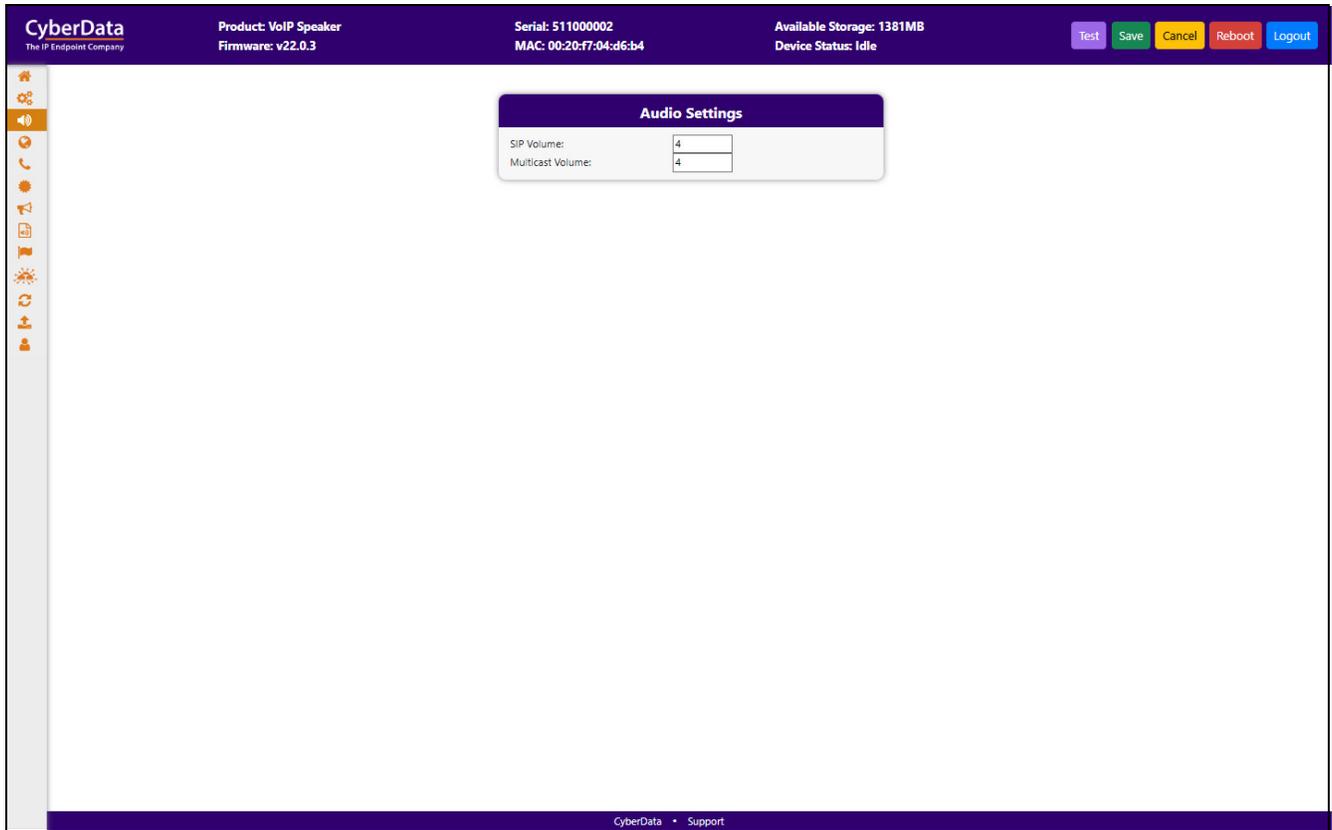
The main content area features two configuration panels:

- Time Settings:**
 - NTP Server:
 - NTP Timezone:
 - Current Time: Tue, 10 Dec 2024 09:06:00
- Misc Settings:**
 - Device Name:

A vertical sidebar on the left contains various system icons. The footer of the page includes the text "CyberData • Support".

3.4 Audio

Figure 3-6. 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 3-7. Network Page

The screenshot displays the Network configuration page for a CyberData device. The interface includes a top header with device details and a sidebar with navigation icons. The main content area is divided into three panels:

- Network Status:** Shows current network parameters:

IP Address Protocol:	DHCP
IP Address:	10.10.1.52
Subnet Mask:	255.0.0.0
Default Gateway:	10.0.0.1
DNS Server 1:	10.0.1.56
DNS Server 2:	
- Network Settings:** Provides fields for configuring network parameters:

Addressing Mode:	DHCP
Hostname:	SipDevice04d6b4
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:** Includes fields for VLAN configuration:

VLAN ID:	0
VLAN Priority:	0

The top header contains the following information: Product: VoIP Speaker, Firmware: v22.0.3, Serial: 511000002, MAC: 00:20:F7:04:d6:b4, Available Storage: 1381MB, and Device Status: Idle. Action buttons for Test, Save, Cancel, Reboot, and Logout are also present.

3.6 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 3-8. SIP Page

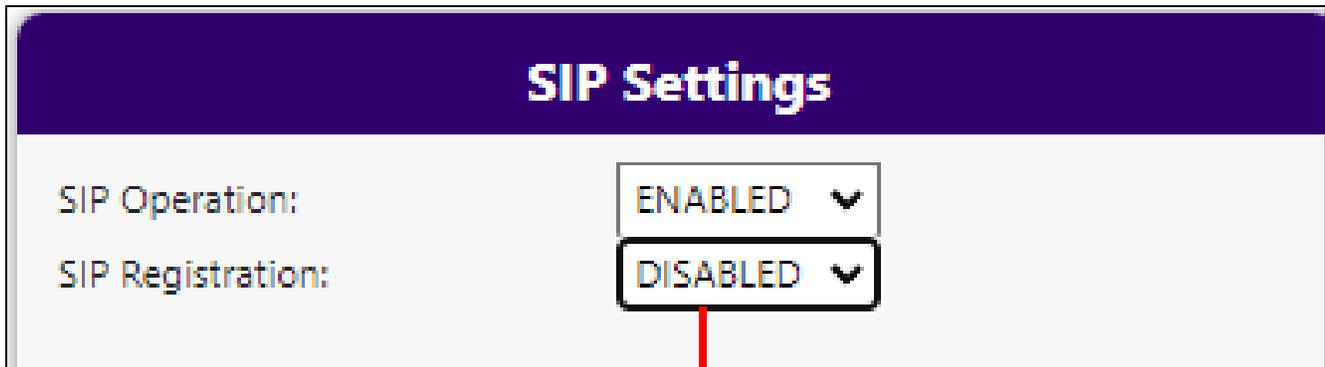
3.6.1 Dial Out Extension Strings and DTMF Tones (using rfc2833)

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

3.6.2 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 3-9](#).

Figure 3-9. SIP Page Set to Point-to-Point Mode



Device is set to NOT register with a SIP server

3.7 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 3-10. SSL Page (1 of 2)

The screenshot displays the CyberData SSL configuration interface. At the top, the device information is shown: Product: VoIP Speaker, Serial: 511000002, Available Storage: 1381MB, Firmware: v22.0.3, MAC: 00-20-f7-04-d6-b4, and Device Status: Idle. The interface is divided into three main sections for certificate management:

- Web Server Certificate:** Shows certificate details (countryName: US, stateOrProvinceName: California, localityName: Monterey, organizationName: Cyberdata, commonName: 0020f704d6b4) and buttons for 'Import Web Certificate' and 'Restore Web Certificate'.
- SIP Client Certificate:** Shows similar certificate details and buttons for 'Import SIP Certificate' and 'Restore SIP Certificate'.
- Autoprovisioning Client Certificate:** Shows similar certificate details and buttons for 'Import Autoprovisioning Certificate' and 'Restore Autoprovisioning Certificate'.

Below these sections is the **List of Trusted CAs** section, which includes an 'Upload CA Certificate' button and a table of existing certificates:

Index	CA 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 shows the CyberData management interface for a VoIP Speaker. The top header includes the CyberData logo, product name (VoIP Speaker), firmware version (v22.0.3), serial number (511100002), MAC address (00:20:f7:04:d6:b4), available storage (1381MB), and device status (Idle). Action buttons for Test, Save, Cancel, Reboot, and Logout are visible in the top right.

The main content area displays a table of installed certificates. Each row contains a certificate name, an 'Info' button, and a 'Remove' button. The certificates listed are:

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 bottom of the page features a footer with the text 'CyberData • Support'.

3.8 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 3-12. Multicast Page

CyberData
The IP Endpoint Company

Product: VoIP Speaker
Firmware: v22.0.3

Serial: 51100002
MAC: 00:20:f7:04:d6:b4

Available Storage: 1381MB
Device Status: Idle

Test Save Cancel Reboot Logout

Multicast Settings

Receive Multicast Audio: **ENABLED** ▼

Polycm Default Channel: 1 ▼

Polycm Priority Channel: 24 ▼

Polycm Emergency Channel: 25 ▼

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

3.9 Audiofiles

The **Audiofiles** page is used to add custom audio to the board. User uploaded audio will take precedence over the audio files shipped with the device.

Figure 3-13. Audiofiles Page

The screenshot shows the CyberData configuration interface for a VoIP Speaker. The header displays the following information:

- CyberData** (The IP Endpoint Company)
- Product:** VoIP Speaker
- Serial:** 511000002
- Available Storage:** 1381MB
- Firmware:** v22.0.3
- MAC:** 00:20:f7:04:d6:b4
- Device Status:** Idle

Navigation buttons include Test, Save, Cancel, Reboot, and Logout.

The main content area is titled **Audio Files** and contains a table with the following rows:

File Name	Current Set To	File Selection	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
Night Ring:	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

The footer of the page contains the text: CyberData • Support

3.10 Events

The **Events** page specifies a remote server that can be used to receive HTTP POST events when actions take place on the device.

Figure 3-14. Events Page

The screenshot displays the CyberData configuration interface for the Events page. At the top, the header includes the CyberData logo, product information (VoIP Speaker, Firmware: v22.0.3), serial and MAC addresses, available storage (1381MB), and device status (Idle). Action buttons for Test, Save, Cancel, Reboot, and Logout are visible in the top right.

The main content area is divided into two panels:

- Event Server:** Contains configuration fields for:
 - Event Generation:
 - Server IP Address:
 - Server Port:
 - Server URL:
- Events:** A list of event types, each with a dropdown menu set to "DISABLED":
 - Application Started Events
 - Heartbeat Events
 - Call Started Events
 - Call Terminated Events
 - Nightring Events
 - Multicast Started Events
 - Multicast Stopped Events

A footer at the bottom of the page contains the text "CyberData • Support".

3.10.1 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>
```

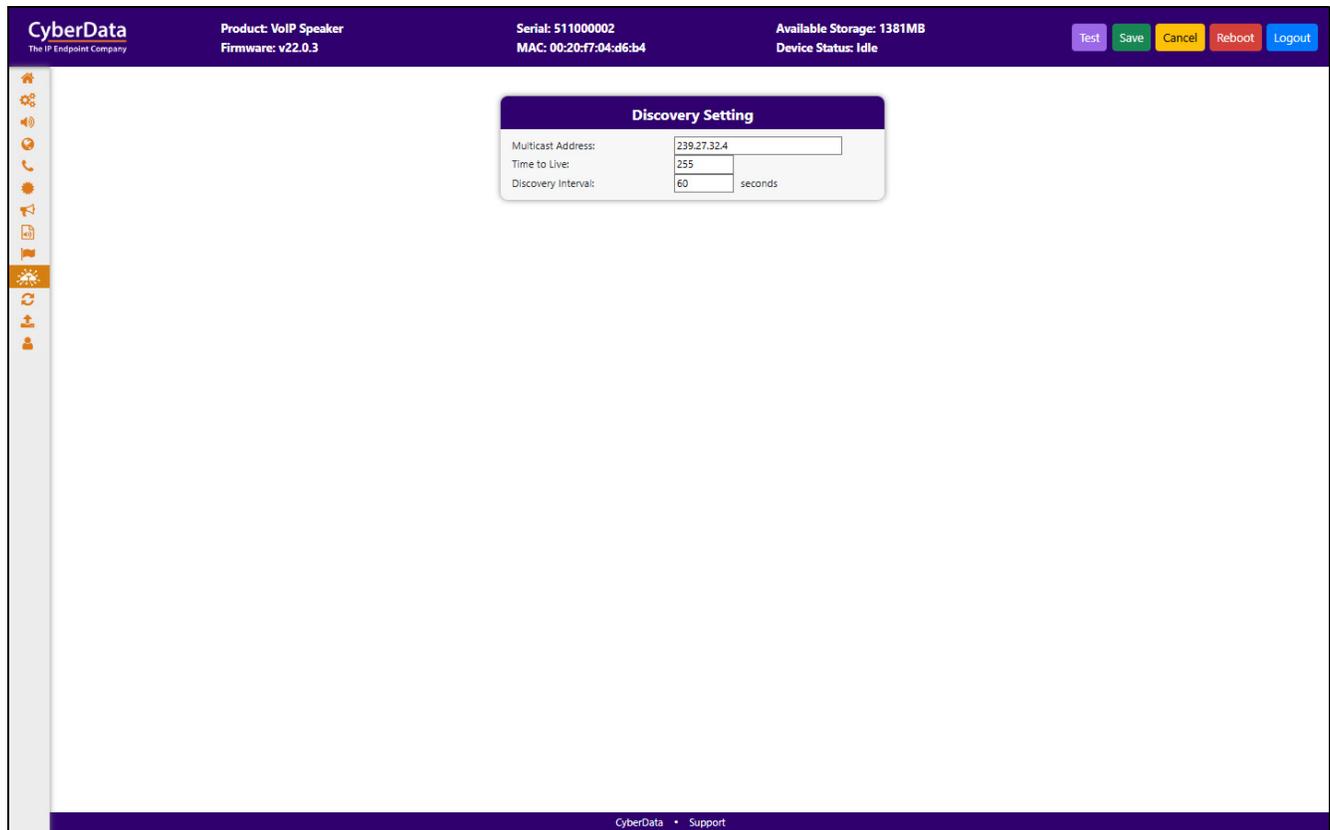
```
POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>NIGHTRINGING</event>
</cyberdata>
```

3.11 Terminus

Terminus Cloud Control™ allows users to configure, monitor, and manage notification functions for CyberData's extensive VoIP product line, all from a single, easy-to-use platform. To learn more about Terminus Cloud Control™, go to <https://www.cyberdata.net/pages/terminus>.

The **Terminus** page allows for configuration of settings related to Terminus Cloud Control™.

Figure 3-15. Terminus Page



3.12 Autoprovisioning

Enabling autoprovisioning allows the device to download provisioning files from a server. It defaults to using DHCP, with options configured in dhcpd.conf on the DHCP server. The file name is <mac address>.xml and if not found, 000000cd.xml.

If a server is named, DHCP is bypassed, and the device will look for a file on the named server..

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

If a server is named, **Use tftp** searches for the file on a tftp server instead of http. If the server is secured (with a password), use **Verify Server Certificate** (username/password) to access it. When using DHCP, these options are configured in dhcpd.conf.

Autoprov autoupdate, **Autoprov at time**, and **Autoprov when idle** options are available with either DHCP or a named server.

The template is an xml file with all options set to default values.

Figure 3-16. Autoprovisioning Page

The screenshot displays the Autoprovisioning configuration page for a CyberData device. At the top, the interface shows the product name 'VoIP Speaker', serial number '511000002', MAC address '00:20:f7:04:d6:b4', and available storage '1381MB'. The device status is 'Idle'. Navigation buttons include 'Test', 'Save', 'Cancel', 'Reboot', and 'Logout'. The main content area is divided into two panels: 'Autoprov Settings' and 'Autoprov Log'. The settings panel includes fields for 'Autoprov' (set to 'ENABLED'), 'Autoprov Server', 'Autoprov Filename', 'Use tftp' (set to 'DISABLED'), 'Verify Server Certificate' (set to 'DISABLED'), 'Username', 'Password', 'Autoprov autoupdate' (0 minutes), 'Autoprov at time' (HHMM), and 'Autoprov when idle' (0 minutes). A 'Download Template' button is located at the bottom of the settings panel. The log panel shows a series of timestamped events: '2024-12-08 11:28:21 Autoprov: no autoprov triggers. Exiting...', '2024-12-08 11:28:26 Autoprovisioning on boot', '2024-12-08 11:28:26 Autoprov found server='http://10.0.0.242' in dhcp option 43', '2024-12-08 11:28:26 Autoprov looking for 0020f704d6b4.xml at http://10.0.0.242', '2024-12-08 11:28:26 Autoprov downloading http://10.0.0.242/0020f704d6b4.xml', '2024-12-08 11:28:26 download_file: download failed', '2024-12-08 11:28:26 Autoprov looking for 000000cd.xml at http://10.0.0.242', '2024-12-08 11:28:26 Autoprov downloading http://10.0.0.242/000000cd.xml', '2024-12-08 11:28:26 download_file: download failed', and '2024-12-08 11:28:26 Autoprov: Failed to fetch autoprov file'. The footer of the page contains 'CyberData • Support'.

3.13 Firmware

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

To upgrade the firmware of your device:

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

<https://www.cyberdata.net/collections/sip>

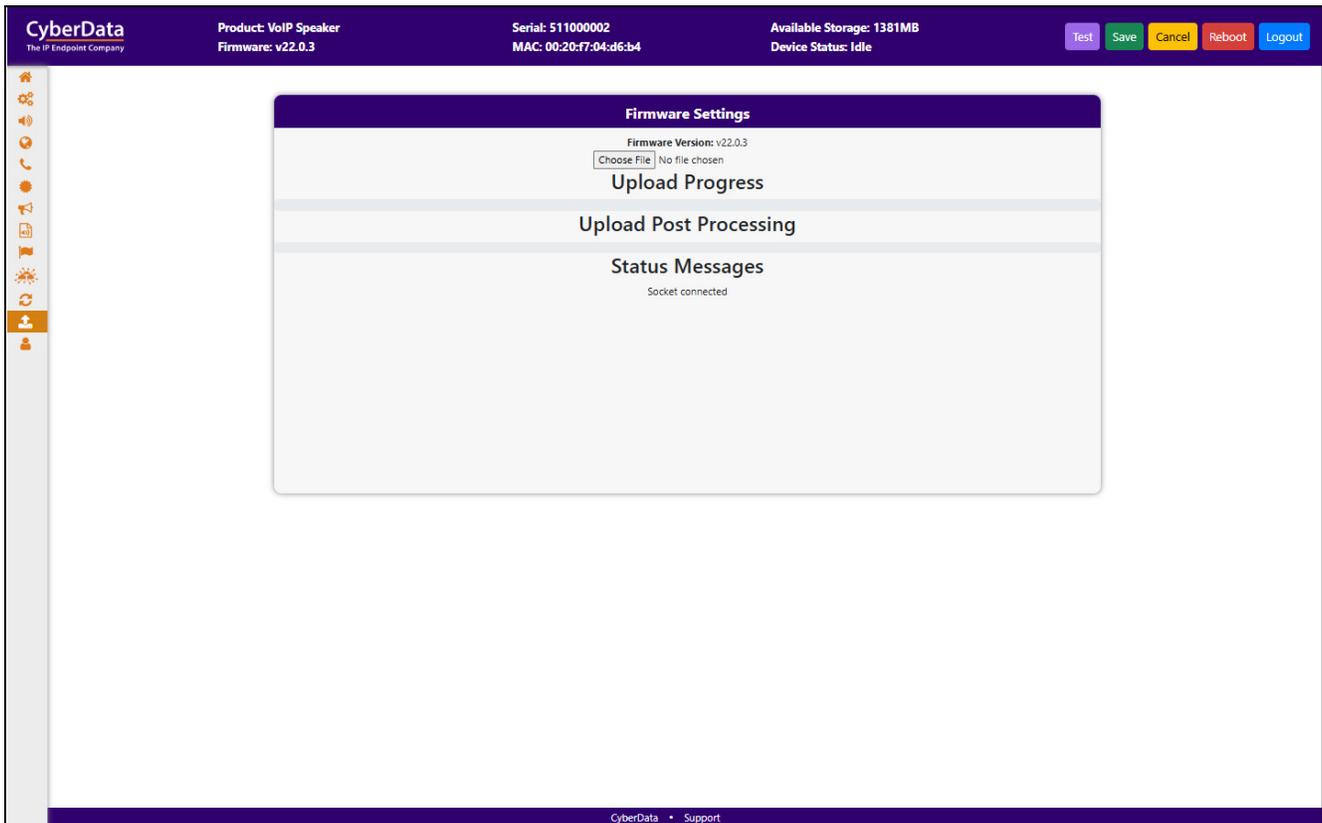
<https://www.cyberdata.net/collections/singlewire> (for InformaCast Enabled devices)

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 3-17. Firmware Page



3.14 Admin

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

Figure 3-18. Admin Page

The screenshot displays the CyberData Admin Page interface. At the top, the header includes the CyberData logo, product information (VoIP Speaker, Firmware: v22.0.3), serial and MAC addresses, available storage (1381MB), and device status (Idle). Action buttons for Test, Save, Cancel, Reboot, and Logout are visible.

The main content area is divided into several sections:

- Admin Settings:** Fields for Username (admin), Password, and Confirm Password.
- Statistics:** Shows Storage (1381MB), Boot Count (2), Reboot Count, and Uptime (up 1 day, 21 hours, 40 minutes).
- Logging Settings:** Includes Debug Level (4) and Log Network Traffic (OFF). Buttons for Get Application Log, Remove Application Log, Get Network Log, Remove Network Log, Get All Logs, and Remove All Logs are present.
- Configuration Settings:** Shows Partition 2 (v22.0.3), Partition 3 (v22.0.3), and Booting Partition (partition 2). Buttons for Restore Default Config, Restore Default Certificates, Import Config, 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. Below these is a table with columns: Username, Home, Device, Audio, Network, SIP, SSL, Multicast, Audiofiles, Events, Terminus, Autopro, Firmware, and Admin.
- Log Viewer:** Includes a Service dropdown (Application), Entries to get (250), Sort dropdown (Oldest), and a View Log button.

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

3.15 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 commands**. However, any program that can send HTTP POST commands to the device should work.

3.15.1 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"
Play the "0" audio file	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"
Play the "1" audio file	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"
Play the "2" audio file	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"
Play the "3" audio file	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"
Play the "4" audio file	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"
Play the "5" audio file	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"
Play the "6" audio file	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"
Play the "7" audio file	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"

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 23
Audio 8
Audiofiles 15
Autoprovisioning 21

C

Command Interface 24
Command Interface Post Commands 24
Contact Information 26

D

Device 7
Dial Out Extension Strings and DTMF Tones 10

F

Firmware 22

H

hazard levels 3
Home Page 6

L

Log In Page 3

M

Multicast 14

P

Point-to-Point Configuration 11

S

SIP (Session Initiation Protocol) 10
SSL 12

T

Terminus 20
Troubleshooting/Technical Support 26

W

Warranty and RMA Information 26