



IP66 Indoor/Outdoor Horns Operations Guide

Part #011457, 011472

Document Part #932058A
for Firmware Version 22.0

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

IP66 Indoor/Outdoor Horn Operations Guide 932058A
Part # 011457, 011472

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 932058A, which corresponds to firmware version 22.0, was released on November 19, 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.



Warning

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



Warning

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



Warning

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

Abbreviations and Terms

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

Chapter 1 Device Setup	1
1.1 Setup and Factory Default settings	1
1.2 Power Test and Status LED	2
1.3 RTFM Switch	3
1.3.1 RTFM Access	3
1.3.2 Announcing the IP Address	5
1.3.3 Restoring the Factory Default Settings	5
 Chapter 2 Configure the Device	 6
2.4 Log In Page	6
2.5 Home Page	7
2.6 Device	9
2.7 Audio	10
2.8 Network	11
2.9 SIP (Session Initiation Protocol)	12
2.9.1 Dial Out Extension Strings and DTMF Tones (using rfc2833)	12
2.9.2 Point-to-Point Configuration	13
2.10 SSL	14
2.11 Multicast	16
2.12 Audiofiles	17
2.13 Events	20
2.13.1 Example Packets for Events	21
2.14 Terminus	24
2.15 Autoprovisioning	25
2.16 Firmware	26
2.17 Admin	27
2.18 Command Interface	28
2.18.1 Command Interface Post Commands	28
 Appendix A Troubleshooting/Technical Support	 29
A.1 Contact Information	29
A.2 Warranty and RMA Information	29
 Index	 30

1 Device Setup

1.1 Setup and Factory Default settings

Configure each IP66 Indoor/Outdoor Horn and verify its operation before you mount it.

Use a standard web browser to configure the Horn online.

When configuring more than one IP66 Indoor/Outdoor Horn, attach the IHorns to the network and configure one at a time to avoid IP address conflicts.

When you are ready to mount the Horns, refer to the Quick Reference Placemat for instructions. The placemat is available in the **Documentation** tab of the CyberData product webpage for your device.

CyberData delivers each IP66 Indoor/Outdoor Horn with the factory default values indicated in [Table 1-1](#).

Table 1-1. Factory Default Settings

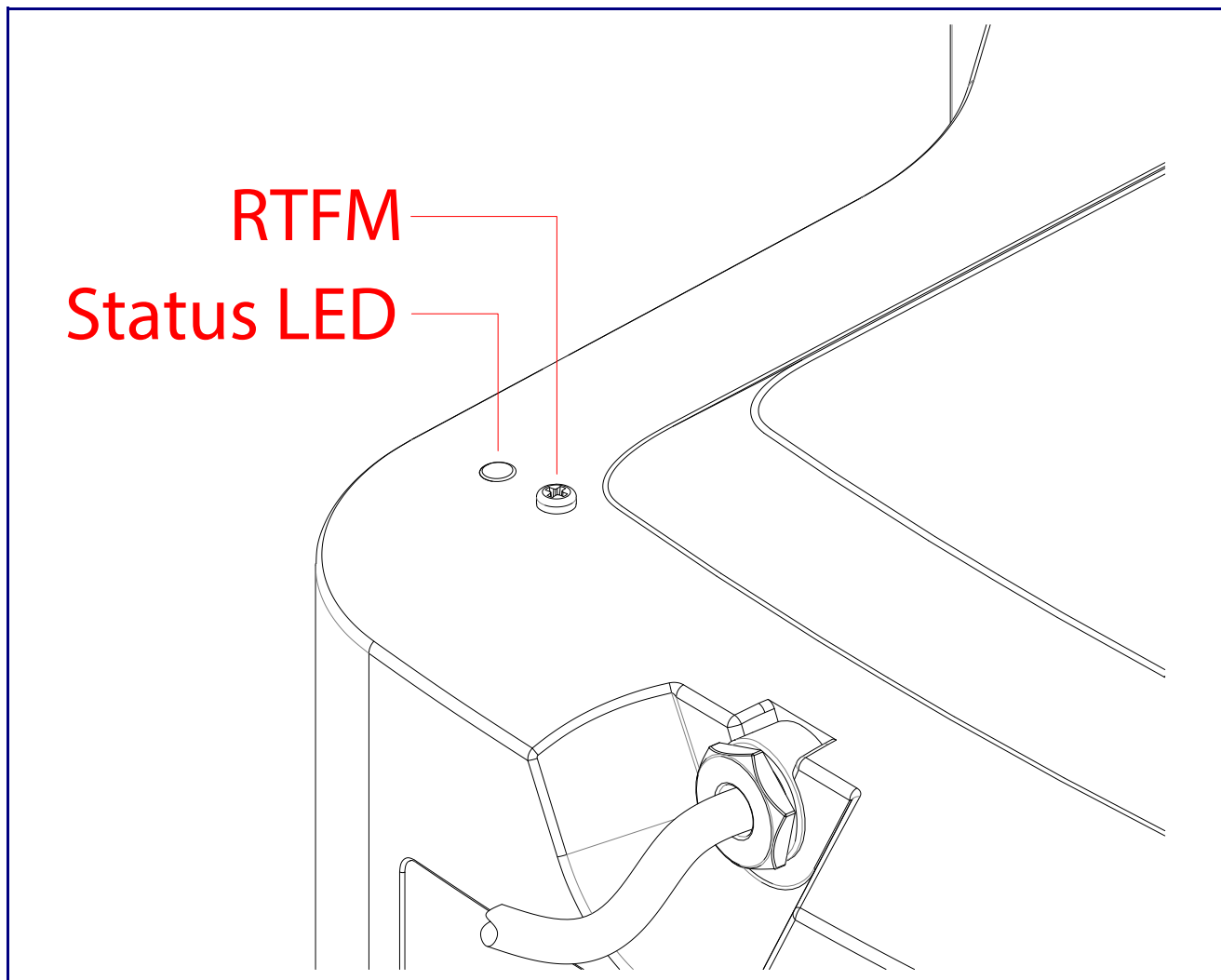
Parameter	Factory Default Setting
IP Addressing	DHCP
IP Address ^a	192.168.1.23
Web Access Username	admin
Web Access Password	admin
Subnet Mask ^a	255.255.255.0
Default Gateway ^a	192.168.1.1

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

1.2 Power Test and Status LED

1. Plug in the CyberData device and monitor the Status LED activity on the bottom side of the horn during the initialization process. See [Figure 1-1](#).

Figure 1-1. Status LED



2. After about 20 seconds, the **GREEN Status** LED will blink fast to indicate that the device is acquiring an IP address and attempting to autoprovision. It will turn off thereafter until the device has finished booting. When the device has fully booted, the **GREEN Status** LED will turn on solid.

If there is no DHCP server available on the network, it will try 12 times for 60 seconds and eventually fall back to the programmed static IP address (by default 192.168.1.23) or the previously used DHCP address if a prior lease was established. This process will take approximately 80 seconds.

3. When the device has completed the initialization process, pressing and holding the RTFM switch for a couple of seconds will announce the IP address. See [Section 1.3, "RTFM Switch"](#)

This concludes the power test.

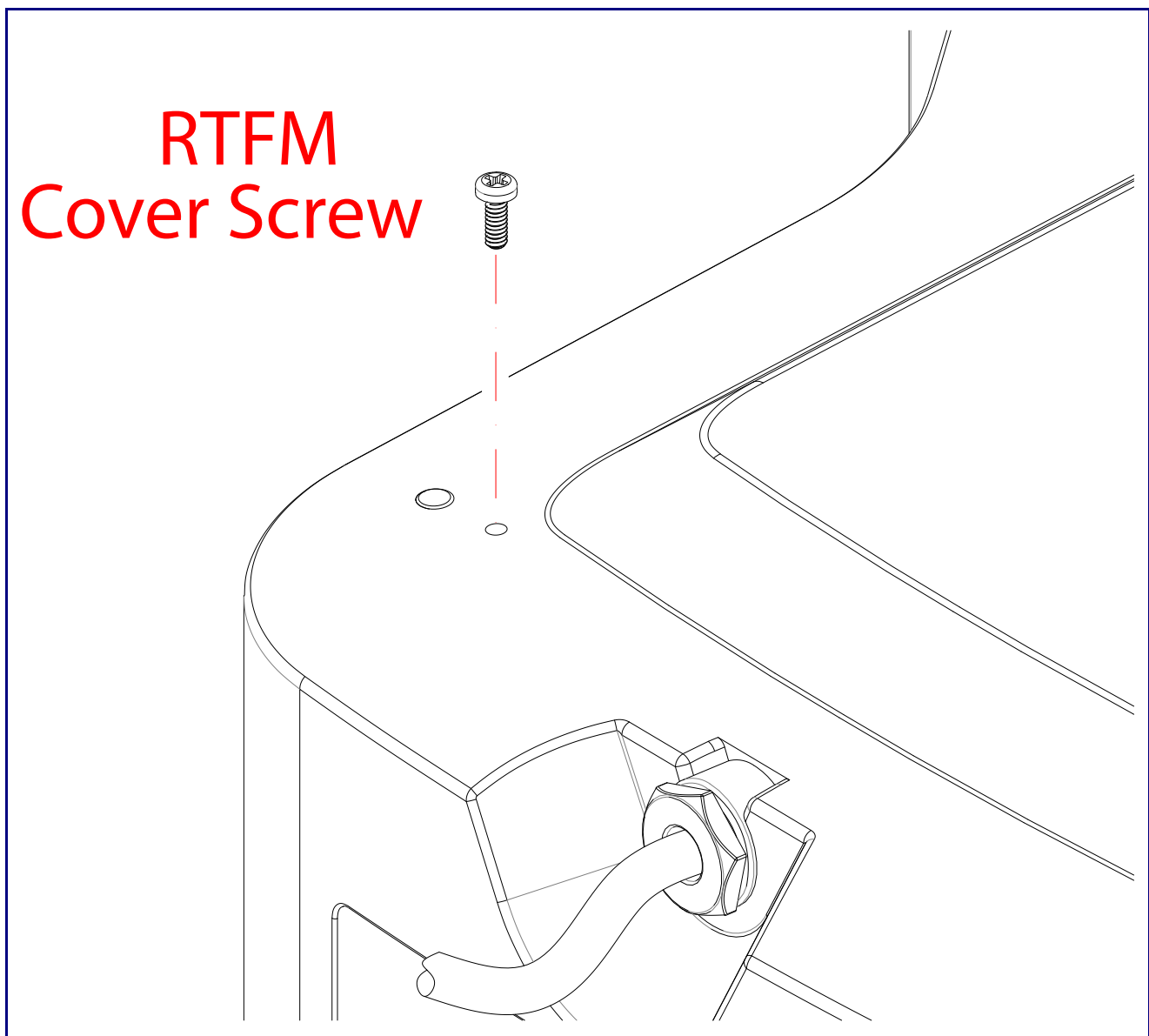
1.3 RTFM Switch

When the IP66 Indoor/Outdoor Horn is operational and linked to the network, use the Reset Test Function Management (**RTFM**) switch (Figure 1-3) (located behind the hole on the device) to announce and confirm the device's IP Address and test the audio to verify that it is working.

1.3.1 RTFM Access

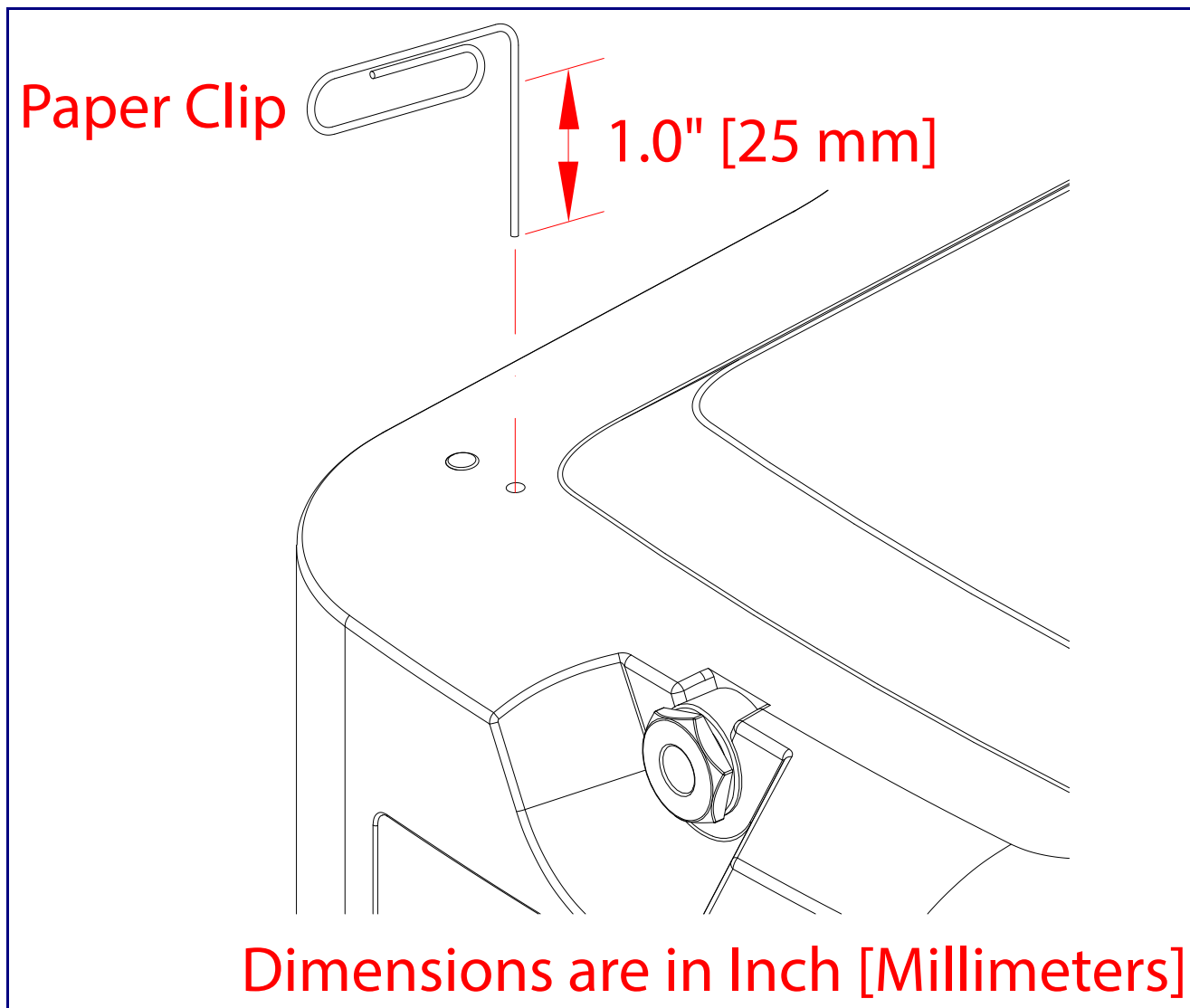
The RTFM switch access will be on the bottom side of the horn hidden under a screw (Figure 1-2) that will be used to keep the unit IP66 sealed with the gasket washer. Remove the screw to gain access to the RTFM switch (Figure 1-3).

Figure 1-2. Remove the screw to gain access to the RTFM switch



4. Use a paper clip to feed through the hole to press the RTFM switch. See [Figure 1-3](#).

Figure 1-3. RTFM Switch



1.3.2 Announcing the IP Address

To announce a device's current IP address:

- Use a bent paperclip or a similar object to press and hold the RTFM switch for a couple of seconds and then release it.



Caution

Equipment Caution: Pressing and holding the RTFM switch for more than five seconds will restore the device to the factory default settings. See the [“Restoring the Factory Default Settings”](#) section.

1.3.3 Restoring the Factory Default Settings

To restore the factory default settings, complete the following steps:

1. Use a bent paperclip or a similar object to press and hold the RTFM switch until you hear the device announce the words, “restoring defaults” and “rebooting”.
2. Release the RTFM switch. The device will be restored to the factory default settings.

2 Configure the Device

2.4 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 IP66 Indoor/Outdoor Horn.

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>

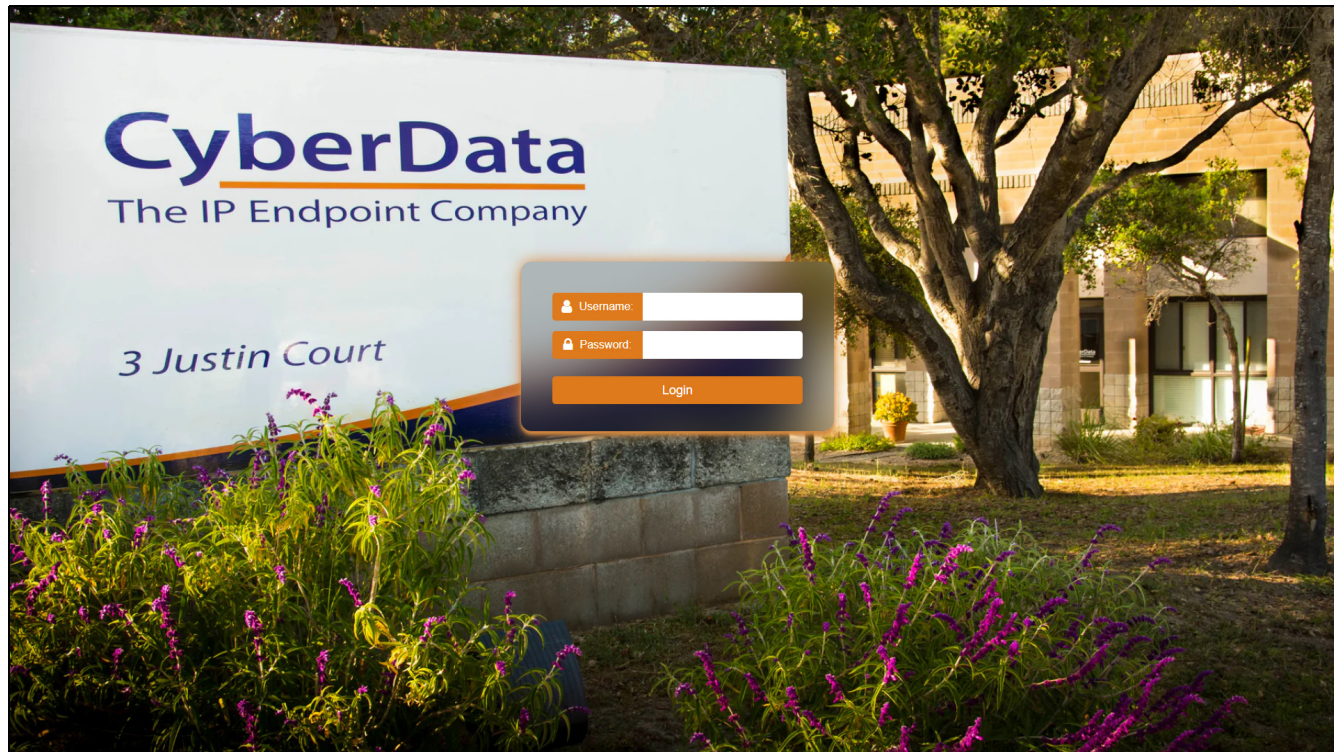
Note The Intercom ships in DHCP mode. To get to the **Home** page, use the discovery utility to scan for the device on the network and open your browser from there.

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

Web Access Username: **admin**

Web Access Password: **admin**

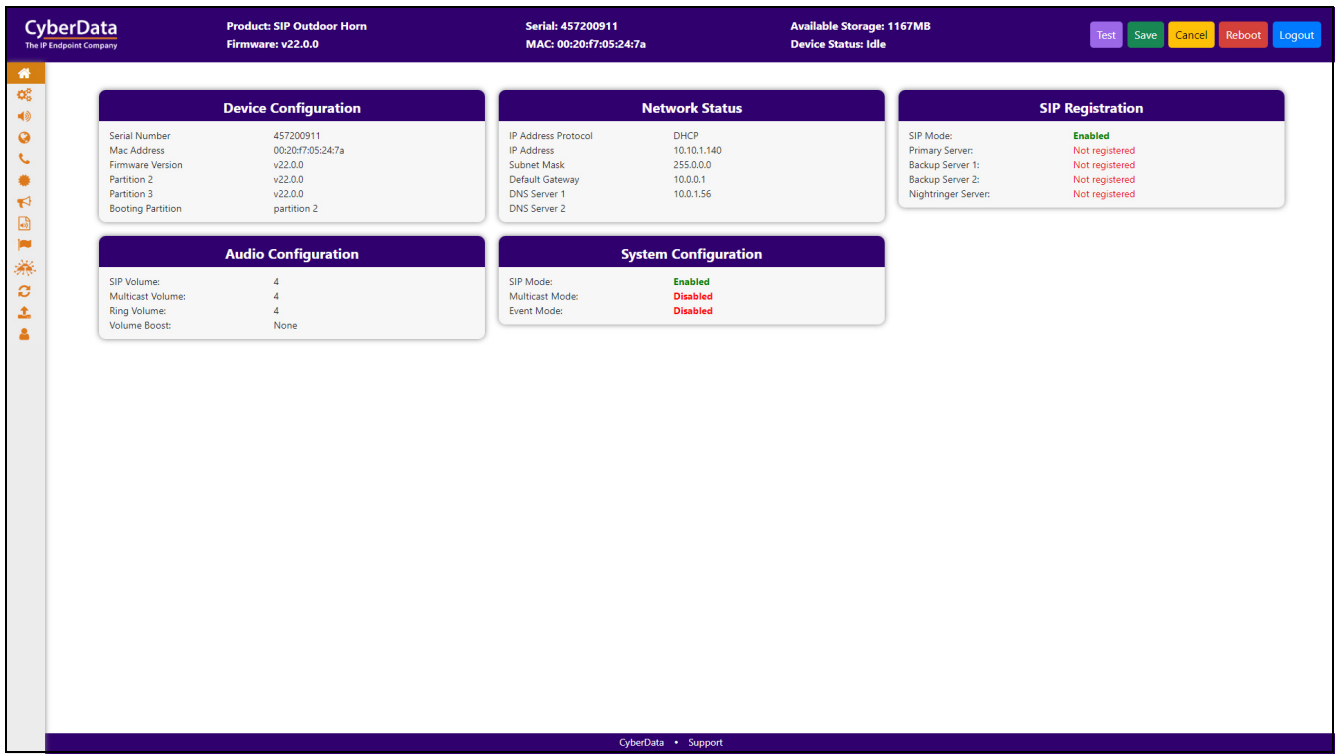
Figure 2-1. Log In Page



2.5 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 2-2. Home Page



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

Figure 2-3. InformaCast enabled Device

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

2.6 Device

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

Figure 2-4. Device Configuration Page

CyberData
The IP Endpoint Company

Product: SIP Outdoor Horn
Firmware: v22.0.0

Serial: 457200911
MAC: 00:20:f7:05:24:7a

Available Storage: 1249MB
Device Status: Idle

TestSaveCancelRebootLogout

Time Settings

NTP Server:
north-america.pool.ntp.org

NTP Timezone:
America/Los_Angeles (-8)

Current Time:
Wed, 06 Nov 2024 13:45:10

DTMF Settings

Require Security Code:
DISABLED

Security Code:

Power Settings

802.3AT Mode:
Not detected. Disabled.

Force 802.3AT Mode:
OFF

Misc Settings

Device Name:
SIP Outdoor Horn

Beep on Init:
OFF

CyberData • Support

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

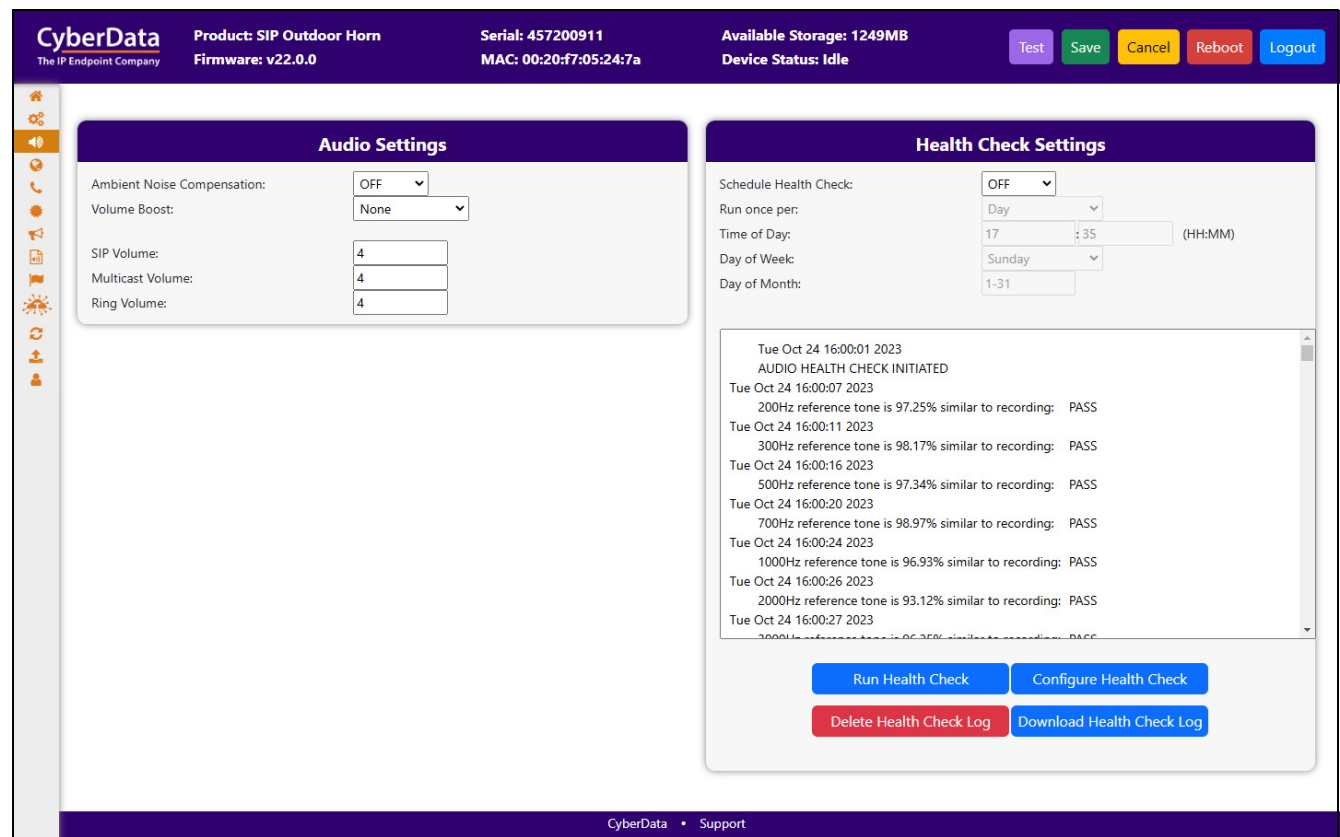
Figure 2-5. InformaCast enabled Device

InformaCast Settings

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

2.7 Audio

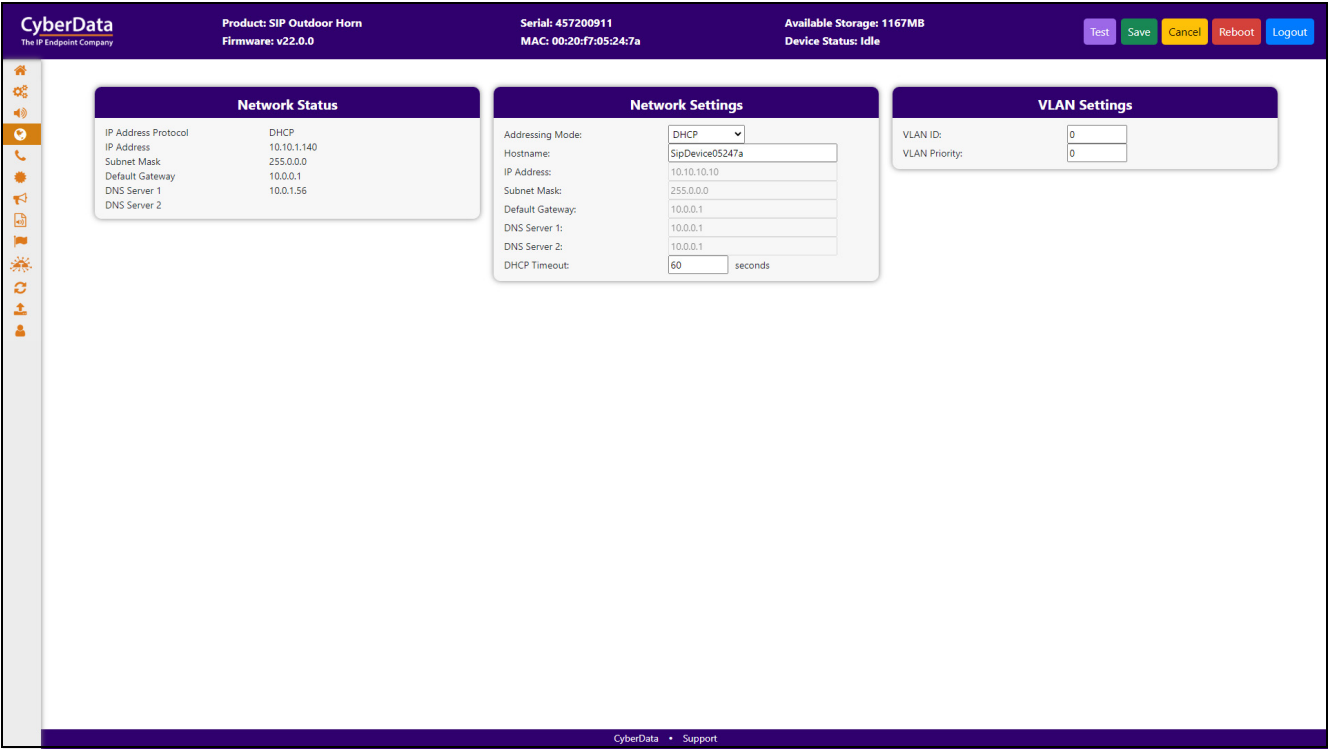
Figure 2-6. Audio Page



2.8 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 2-7. Network Page



2.9 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 2-8. SIP Page

CyberData
The IP Endpoint Company

Product: SIP Outdoor Horn
Firmware: v22.0.0

Serial: 457200911
MAC: 00:20:f7:05:24:7a

Available Storage: 1167MB
Device Status: Idle

TestSaveCancelRebootLogout

SIP Settings

SIP Operation:

ENABLED

▼

SIP Registration:

ENABLED

▼

Buffer SIP Calls:

DISABLED

▼

Beep Before Paging:

OFF

▼

Remote SIP Port:

5060

Local SIP Port:

5060

SIP Transport Protocol:

UDP

▼

TLS Version:

1.2

▼

Verify Server Certificate:

OFF

▼

Outbound Proxy:

Outbound Proxy

Outbound Proxy Port:

0

Cisco SRST:

OFF

▼

Disable rport Discovery:

OFF

▼

Keep Alive Timeout:

10000

 milliseconds (ms)

Terminate call after delay:

0

 seconds

Audio Codec:

Auto Select

▼

RTP Port (even):

10500

Asymmetric RTP:

OFF

▼

Jitter Buffer:

50

RTP Encryption (SRTP):

DISABLED

▼

SIP Server Settings

Primary SIP Server:

10.0.0.253

Primary SIP User ID:

199

Primary SIP Auth ID:

199

Primary SIP Auth Password:

Ⓢ

Registration Interval:

360

 seconds

Backup SIP Server 1:

Host or IP address

Backup SIP User ID:

Backup SIP User ID

Backup SIP Auth ID:

Backup SIP Auth ID

Backup SIP Auth Password:

Backup SIP Auth Password

Ⓢ

Registration Interval:

360

 seconds

Backup SIP Server 2:

Host or IP address

Backup SIP User ID:

Backup SIP User ID

Backup SIP Auth ID:

Backup SIP Auth ID

Backup SIP Auth Password:

Backup SIP Auth Password

Ⓢ

Registration Interval:

360

 seconds

Nightringer Settings

SIP Server:

Host or IP address

SIP User ID:

User ID

SIP Auth ID:

Auth ID

SIP Auth Password:

Password

Ⓢ

Registration Interval:

360

 seconds

CyberData • Support

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

Figure 2-9. InformaCast enabled Device

InformaCast SIP Config:

DISABLED

▼

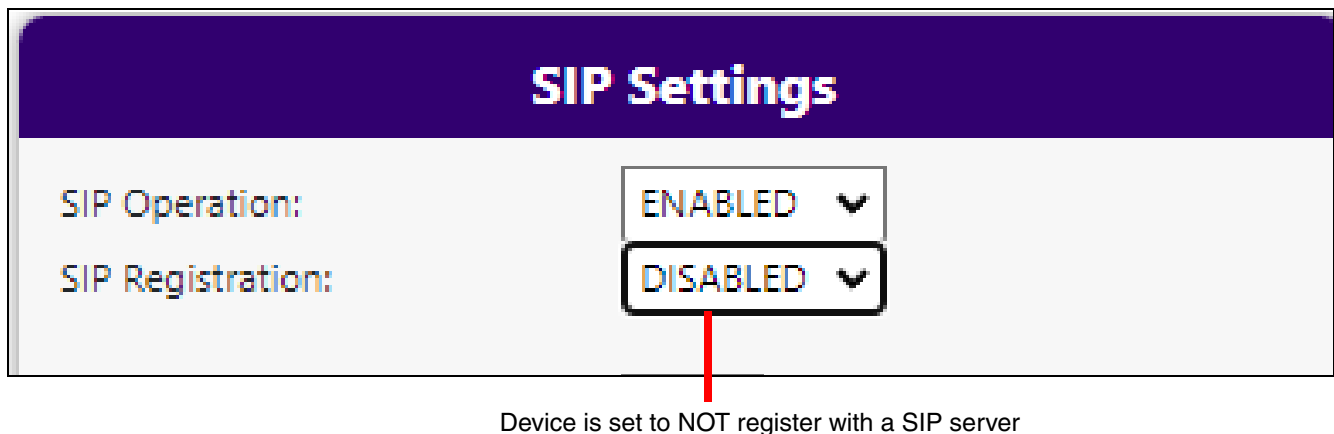
2.9.1 Dial Out Extension Strings and DTMF Tones (using rfc2833)

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

2.9.2 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 2-10](#).

Figure 2-10. SIP Page Set to Point-to-Point Mode



2.10 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 2-11. SSL Page (1 of 2)

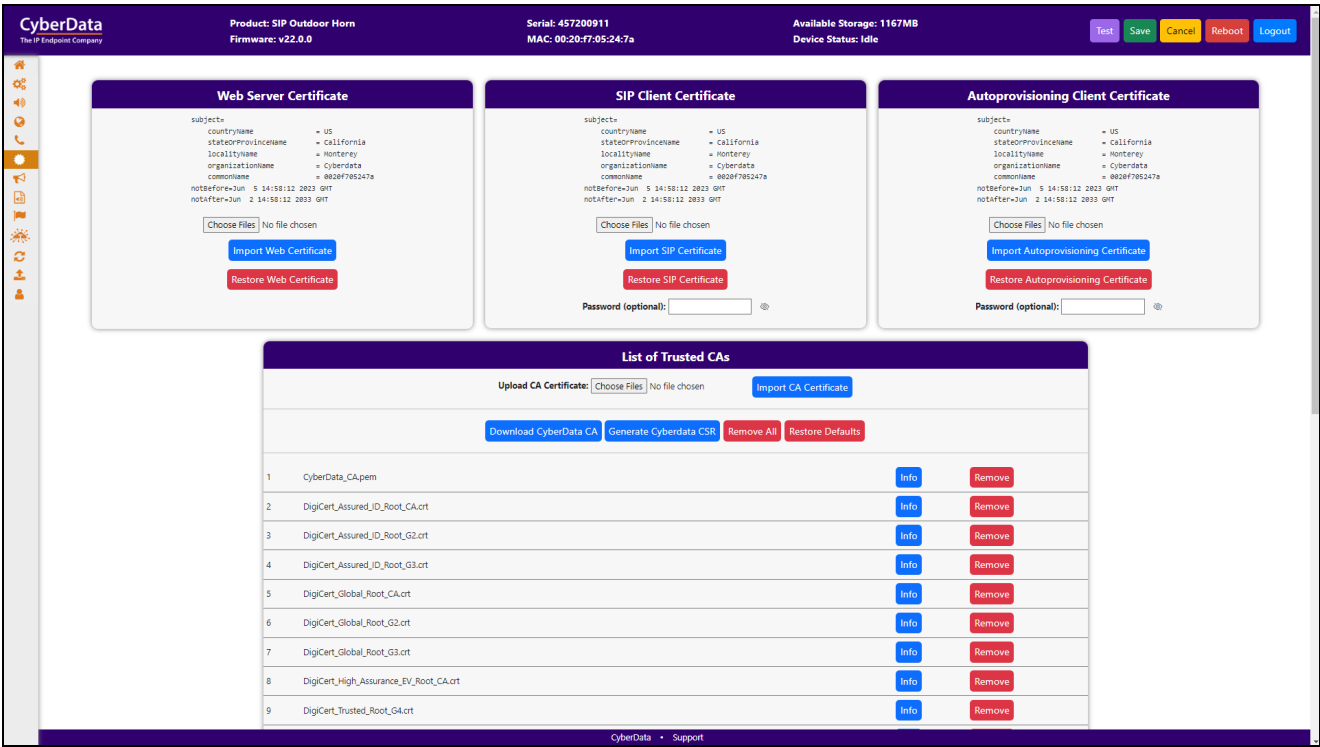


Figure 2-12. SSL Page (2 of 2)

CyberData

The IP Endpoint Company

Product: SIP Outdoor Horn

Firmware: v22.0.0

Serial: 457200911

MAC: 00:20:f7:05:24:7a

Available Storage: 1167MB

Device Status: Idle

Test

Save

Cancel

Reboot

Logout

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_-_G3.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

CyberData • Support

2.11 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 2-13. Multicast Page

CyberData

The IP Endpoint Company

Product: SIP Outdoor Horn
Firmware: v22.0.0

Serial: 457200911
MAC: 00:20:f7:05:24:7a

Available Storage: 1167MB
Device Status: Idle

TestSaveCancelRebootLogout

Multicast Settings

Recieve Multicast Audio:

DISABLED

Polycom Default Channel:

1

Polycom Priority Channel:

24

Polycom Emergency Channel:

25

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

SIP calls: Priority 4,5
Port range: 2000-65535
Priority: 9 is the highest, 0 is the lowest
Audio Streams: Higher priority supersedes lower ones
Priority 9: Plays at maximum volume

CyberData • Support

2.12 Audiofiles

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

This device supports stored messages. When stored messages are enabled, the user will hear "Press 0 to page, press 1 to 9 to play stored message" when calling the device.

To configure stored messages, an audio file must be uploaded, using **Choose File** and **Save**. The number of repeats can be specified or set to infinite (where the message plays until cancelled by the # button during a phone call).

Figure 2-14. Audiofiles Page (1 of 3)

CyberData The IP Endpoint Company

Product: SIP Outdoor Horn
Firmware: v22.0.0

Serial: 457200911
MAC: 00:20:f7:05:24:7a

Available Storage: 1249MB
Device Status: Idle

Test Save Cancel Reboot Logout

Audio Files							
0:	Currently set to:	default	Choose File	No file chosen	Play	Save	Delete
1:	Currently set to:	default	Choose File	No file chosen	Play	Save	Delete
2:	Currently set to:	default	Choose File	No file chosen	Play	Save	Delete
3:	Currently set to:	default	Choose File	No file chosen	Play	Save	Delete
4:	Currently set to:	default	Choose File	No file chosen	Play	Save	Delete
5:	Currently set to:	default	Choose File	No file chosen	Play	Save	Delete
6:	Currently set to:	default	Choose File	No file chosen	Play	Save	Delete
7:	Currently set to:	default	Choose File	No file chosen	Play	Save	Delete
8:	Currently set to:	default	Choose File	No file chosen	Play	Save	Delete
9:	Currently set to:	default	Choose File	No file chosen	Play	Save	Delete
Audio Test:	Currently set to:	default	Choose File	No file chosen	Play	Save	Delete
Dot:	Currently set to:	default	Choose File	No file chosen	Play	Save	Delete
Night Ring:	Currently set to:	default	Choose File	No file chosen	Play	Save	Delete
Page Tone:	Currently set to:	default	Choose File	No file chosen	Play	Save	Delete
Rebooting:	Currently set to:	default	Choose File	No file chosen	Play	Save	Delete
Restoring Default:	Currently set to:	default	Choose File	No file chosen	Play	Save	Delete
Stored Message File Not Found:	Currently set to:	default	Choose File	No file chosen	Play	Save	Delete

CyberData • Support

Figure 2-15. Audiofiles Page (2 of 3)

CyberData
The IP Endpoint Company

Product: SIP Outdoor Horn
Firmware: v22.0.0

Serial: 457200911
MAC: 00:20:f7:05:24:7a

Available Storage: 1249MB
Device Status: Idle

TestSaveCancelRebootLogout

Your IP Address Is:Currently set to: defaultChoose FileNo file chosenPlaySaveDelete

Menu Audio Files

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

Stored Messages

Stored Message 1:	Currently set to: default	Choose File	No file chosen	Repeat: 0	Infinite: OFF	Play	Save	Delete
Stored Message 2:	Currently set to: default	Choose File	No file chosen	Repeat: 0	Infinite: OFF	Play	Save	Delete
Stored Message 3:	Currently set to: default	Choose File	No file chosen	Repeat: 0	Infinite: OFF	Play	Save	Delete

CyberData • Support

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

CyberData
The IP Endpoint Company

Product: SIP Outdoor Horn
Firmware: v22.0.0

Serial: 457200911
MAC: 00:20:f7:05:24:7a

Available Storage: 1249MB
Device Status: Idle

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

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

Stored Messages

Stored Message 1:	Currently set to:	default	Choose File	No file chosen	Repeat: <input type="text" value="0"/>	Infinite: <input type="text" value="OFF"/>	Play	Save	Delete
Stored Message 2:	Currently set to:	default	Choose File	No file chosen	Repeat: <input type="text" value="0"/>	Infinite: <input type="text" value="OFF"/>	Play	Save	Delete
Stored Message 3:	Currently set to:	default	Choose File	No file chosen	Repeat: <input type="text" value="0"/>	Infinite: <input type="text" value="OFF"/>	Play	Save	Delete
Stored Message 4:	Currently set to:	default	Choose File	No file chosen	Repeat: <input type="text" value="0"/>	Infinite: <input type="text" value="OFF"/>	Play	Save	Delete
Stored Message 5:	Currently set to:	default	Choose File	No file chosen	Repeat: <input type="text" value="0"/>	Infinite: <input type="text" value="OFF"/>	Play	Save	Delete
Stored Message 6:	Currently set to:	default	Choose File	No file chosen	Repeat: <input type="text" value="0"/>	Infinite: <input type="text" value="OFF"/>	Play	Save	Delete
Stored Message 7:	Currently set to:	default	Choose File	No file chosen	Repeat: <input type="text" value="0"/>	Infinite: <input type="text" value="OFF"/>	Play	Save	Delete
Stored Message 8:	Currently set to:	default	Choose File	No file chosen	Repeat: <input type="text" value="0"/>	Infinite: <input type="text" value="OFF"/>	Play	Save	Delete
Stored Message 9:	Currently set to:	default	Choose File	No file chosen	Repeat: <input type="text" value="0"/>	Infinite: <input type="text" value="OFF"/>	Play	Save	Delete

CyberData • Support

2.13 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 2-17. Events Page

CyberData

The IP Endpoint Company

Product: SIP Outdoor Horn

Firmware: v22.0.0

Serial: 457200911

MAC: 00:20:f7:05:24:7a

Available Storage: 1167MB

Device Status: Idle

Test

Save

Cancel

Reboot

Logout

Event Server

Event Generation:

DISABLED

Server IP Address:

10.0.0.250

Server Port:

8080

Server URL:

xmlparse_engine

Events

Application Started Events:

DISABLED

Reboot Events:

DISABLED

Heartbeat Events:

DISABLED

Call Started Events:

DISABLED

Call Terminated Events:

DISABLED

Nightring Events:

DISABLED

Multicast Started Events:

DISABLED

Multicast Stopped Events:

DISABLED

Audio Health Check Events:

DISABLED

CyberData

Support

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

Figure 2-18. InformaCast enabled Device

InformaCast Start Events:

DISABLED

InformaCast Stop Events:

DISABLED

2.13.1 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>
```

2.14 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 2-19. Terminus Page

The screenshot shows the Terminus configuration page for a CyberData device. The header bar is purple and contains the following information:

- CyberData** The IP Endpoint Company
- Product: SIP Outdoor Horn
- Firmware: v22.0.0
- Serial: 457200911
- MAC: 00:20:f7:05:24:7a
- Available Storage: 1167MB
- Device Status: Idle
- Buttons: Test, Save, Cancel, Reboot, Logout

The main content area is white. On the left is a vertical sidebar with various icons. The central area contains two configuration panels:

Discovery Setting

- Multicast Address: 239.27.32.4
- Time to Live: 255
- Discovery Interval: 60 seconds

Lockdown Settings

- Lock Down Mode: Disabled
- Relay: No Action

The footer of the page is purple and contains the text: CyberData • Support

2.15 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 2-20. Autoprovisioning Page

CyberData The IP Endpoint Company

Product: SIP Outdoor Horn
Firmware: v22.0.0

Serial: 457200911
MAC: 00:20:f7:05:24:7a

Available Storage: 1249MB
Device Status: Idle

Test Save Cancel Reboot Logout

Autoprov Settings

Autoprov:

Autoprov Server:

Autoprov Filename:

Use tftp:

Verify Server Certificate:

Username:

Password:

Autoprov autoupdate: minutes

Autoprov at time:

Autoprov when idle: minutes

[Download Template](#)

Autoprov Log

```

2024-11-06 13:38:53 Autoprov: no autoprov triggers. Exiting...
2024-11-06 13:38:56 Autoprov found server='http://10.0.0.242' in dhcp option 43
2024-11-06 13:38:56 Autoprov looking for 0020f705247a.xml at http://10.0.0.242
2024-11-06 13:38:56 Autoprov downloading http://10.0.0.242/0020f705247a.xml
2024-11-06 13:38:56 Got autoprov file. Parsing "0020f705247a.xml"
2024-11-06 13:38:57 Autoprov: Processing ssl certificates
2024-11-06 13:38:57 No certificate elements in SSLCertificates
2024-11-06 13:38:57 Autoprov: Processing audio files
2024-11-06 13:38:58 Autoprov: FirmwareSettings config not found
2024-11-06 13:38:58 DeviceConfig: error = False
2024-11-06 13:38:58 SSLCertificates: error = None
2024-11-06 13:38:58 AudioFiles: error = False
2024-11-06 13:38:58 BellSchedule: error = False
2024-11-06 13:38:58 FirmwareSettings: error = None
  
```

CyberData • Support

2.16 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


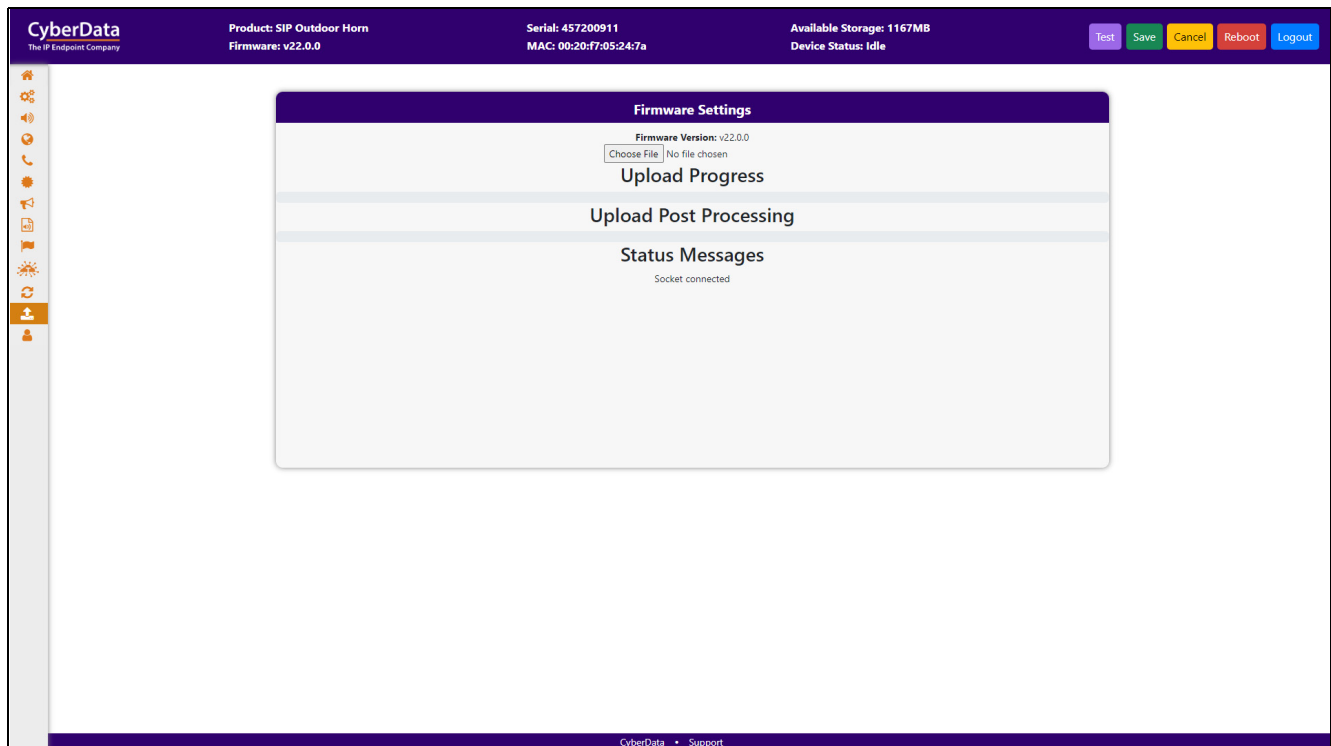
 GENERAL ALERT	<p>Caution</p> <p>Equipment Hazard: Do not reboot the device. It will reboot automatically when the process is complete.</p>
--	--

Figure 2-21. Firmware Page



2.17 Admin

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

Figure 2-22. Admin Page

The screenshot displays the CyberData Admin Page for a SIP Outdoor Horn device. The interface includes a top navigation bar with device information and a sidebar with icons for various functions. The main content area is divided into several sections:

- Admin Settings:** Fields for Username (admin), Password, and Confirm Password.
- Statistics:** Displays Storage (1167MB), Boot Count (68), Reboot Count (51), and Uptime (up 12 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 (v22.0.0), Partition 3 (v22.0.0), and Booting Partition (partition 2). Buttons for Restore Default Config, Restore Default Certificates, Import Config, Export Config, and Root From Other Partition are available.
- Users List:** A table with columns for Username, Home, Device, Audio, Network, SIP, SSL, Multicast, Audiofiles, Events, Terminus, Autopro, Firmware, and Admin. Buttons for Add New User, Delete All Users, Import Users, and Export Users are located above the table.
- Log Viewer:** A section for viewing logs, with a dropdown for Service (Application), a text input for Entries to get (250), a dropdown for Sort (Oldest), and a View Log button.

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

2.18 Command Interface

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

2.18.1 Command Interface Post Commands

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

Table 2-2. Command Interface Post Commands

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

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

Appendix A: Troubleshooting/Technical Support

A.1 Contact Information

Contact CyberData Corporation
 3 Justin Court
 Monterey, CA 93940 USA
 www.cyberdata.net
 Phone: 831-373-2601
 Fax: 831-373-4193

Sales Sales 831-373-2601, Extension 334

Technical 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 27
Announcing the IP Address 5
Audiofiles 17
Autoprovisioning 25

C

Command Interface 28
Command Interface Post Commands 28
Contact Information 29

D

Device 9
Dial Out Extension Strings and DTMF Tones 12
Discovery Utility program 6

E

Events 20

F

Firmware 26

H

hazard levels 3
Home Page 7

L

Log In Page 6

M

Multicast 16

N

Network 11

P

Point-to-Point Configuration 13

R

Restoring the Factory Default Settings 5
RTFM Switch 3

S

SIP (Session Initiation Protocol) 12
SSL 14

T

Terminus 24
Troubleshooting/Technical Support 29

W

Warranty and RMA Information 29