



Intercom Operations Guide

Part #s: 011186, 011209, 011211, 011214, 011216,
011304, 011305, 011309, 011567

Document Part #932050A
for Firmware Version 22.0

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

Intercom Operations Guide 932050A
Part # 011186, 011209, 011211, 011214, 011216, 011305, 011309, 011304, 011567

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 932050A, which corresponds to firmware version 22.0, was released on November 19, 2024.

Pictorial Alert Icons

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

Hazard Levels

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

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

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




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

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

Important Safety Instructions

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

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

 GENERAL ALERT	<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
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 Configure the Device	1
1.1 Log In Page	1
1.1.1 Restoring Defaults and Announcing the IP Address	2
1.2 Home Page	3
1.3 Device	5
1.4 Audio	6
1.5 Network	7
1.6 SIP (Session Initiation Protocol)	8
1.6.1 Dial Out Extension Strings and DTMF Tones (using rfc2833)	9
1.6.2 Point-to-Point Configuration	9
1.7 SSL	10
1.8 Multicast	12
1.9 Sensor	13
1.10 Strobe	14
1.11 Audiofiles	16
1.12 Events	17
1.12.1 Example Packets for Events	18
1.13 Door Strike Relay	21
1.14 Terminus	22
1.15 Autoprovisioning	23
1.16 Firmware	24
1.17 Admin	25
1.18 Keypad Pages	26
1.18.1 Buttons	26
1.18.2 Security	27
1.18.3 Access List	28
1.18.4 Access Log	29
1.19 Command Interface	30
1.19.1 Command Interface Post Commands	30
 Appendix A Troubleshooting/Technical Support	 31
A.1 Contact Information	31
A.2 Warranty and RMA Information	31
 Index	 32

1 Configure the Device

1.1 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 Intercom.

Note You may also download CyberData's VoIP Discovery Utility program which allows you to easily find and configure the default web address of the CyberData VoIP products.

CyberData's VoIP Discovery Utility program is available at the following website address:

<https://www.cyberdata.net/pages/discovery>

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

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

Web Access Username: **admin**

Web Access Password: **admin**

Figure 1-1. Log In Page



1.1.1 Restoring Defaults and Announcing the IP Address

The RTFM button is located on the back of the device.

To restore the device to its factory default settings (Table 1-1), hold the RTFM button for approximately seven seconds.

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.

Figure 1-2. RTFM Button

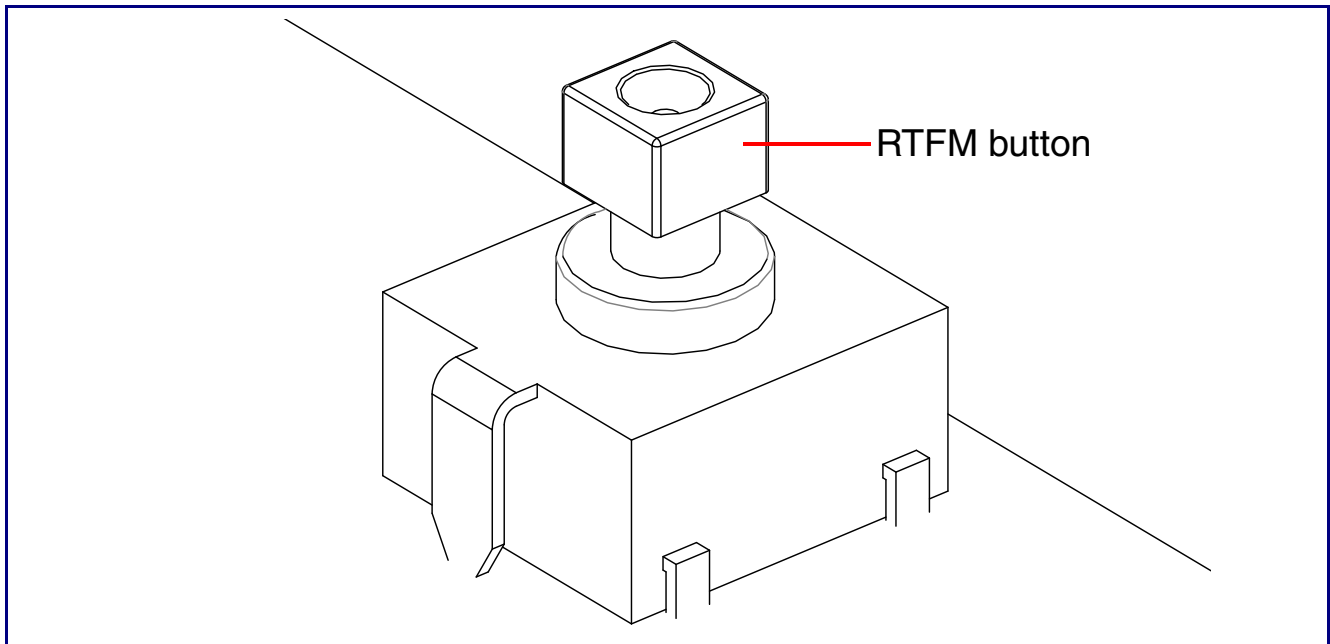


Table 1-1. Factory Default Settings

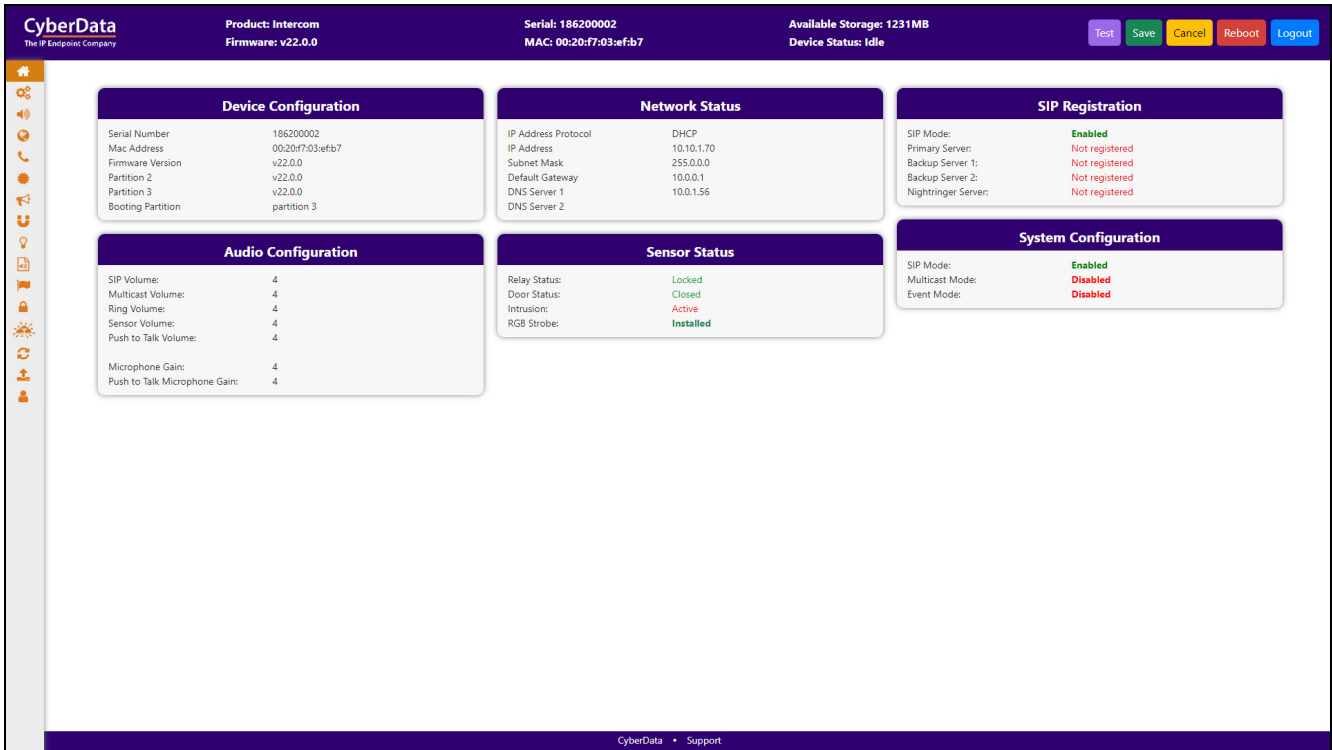
Parameter	Factory Default Setting
IP Addressing	DHCP
IP Address ^a	192.168.1.23
Web Access Username	admin
Web Access Password	admin
Subnet Mask ^a	255.255.255.0
Default Gateway ^a	192.168.1.1

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

1.2 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 1-3. Home Page



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

Figure 1-4. 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

1.3 Device

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

Figure 1-5. Device Configuration Page

CyberData
The IP Endpoint Company

Product: Intercom
Firmware: v22.0.0

Serial: 186200002
MAC: 00:20:f7:03:ef:b7

Available Storage: 1231MB
Device Status: Idle

TestSaveCancelRebootLogout

Relay Settings

Control Relay with DTMF Code: ON
DTMF Pulse Code: 123
DTMF Pulse Code Duration: 2 seconds
DTMF Activation Code: 456
DTMF Deactivation Code: 654
DTMF Relay Activation Tone: OFF
Relay During Ring: OFF
Relay During Night Ring: OFF
Relay While Call Active: OFF
Relay On Button Press: OFF
Relay On Button Press Duration: 3 seconds

Time Settings

NTP: ON
NTP Server: north-america.pool.ntp.org
NTP Timezone: America/Los_Angeles (-8)
Current Time: Thu, 03 Oct 2024 11:21:21

Misc Settings

Device Name: Outdoor Intercom
Button LED Lit when Idle: ON
Button LED Brightness: 255
Push to Talk (PTT): OFF
DTMF Push to Talk (PTT): OFF
Prevent Call Termination: OFF

CyberData • Support

Note Devices with a keypad also have the following options for the keypad LED (brightness is from 0 to 255). See [Figure 1-6](#).

Figure 1-6. Options for the Keypad LED

Keypad LED Lit when Idle:

ON

Keypad LED Brightness:

255

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

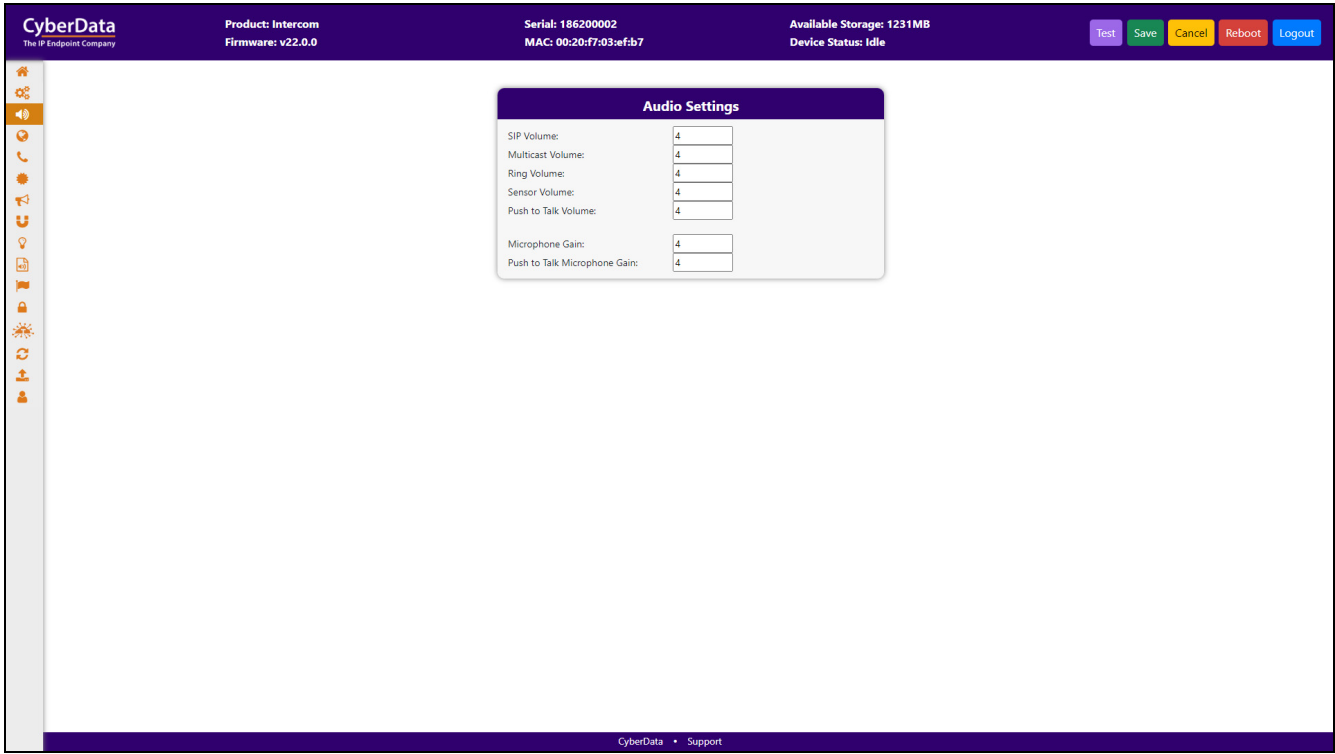
Figure 1-7. InformaCast enabled Device

InformaCast Settings

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

1.4 Audio

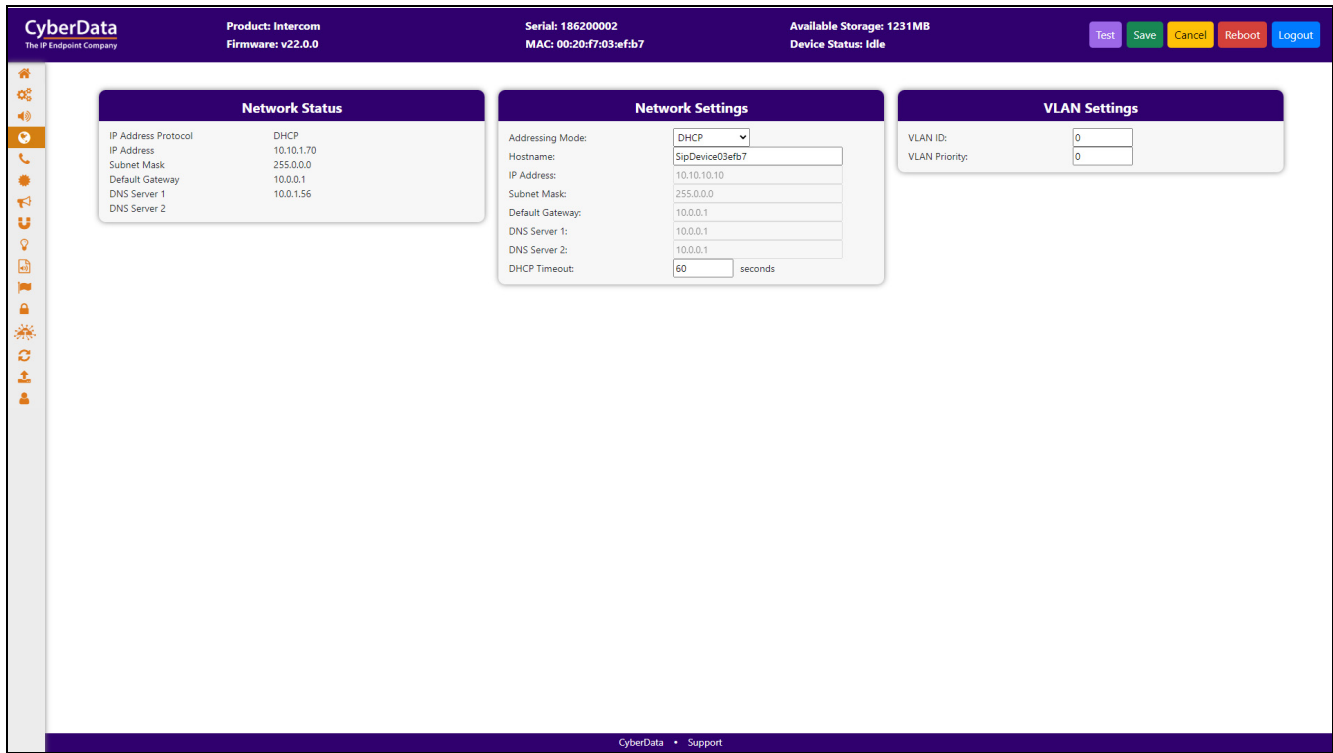
Figure 1-8. Audio Page



1.5 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 1-9. Network Page



1.6 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/Ring 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 1-10. SIP Page

CyberData
The IP Endpoint Company

Product: Intercom
Firmware: v22.0.0

Serial: 186200002
MAC: 00:20:f7:03:ef:b7

Available Storage: 1231MB
Device Status: Idle

TestSaveCancelRebootLogout

SIP Settings

SIP Operation:

ENABLED

▼

SIP Registration:

ENABLED

▼

Auto-Answer Incoming Calls:

ON

▼

Play Ringback Tone:

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

Dial Out Settings

Dialout Extension:

204

Extension ID:

id204

Send Multicast Audio:

DISABLED

▼

Multicast Address:

224.5.5.5

Multicast Port:

5050

Repeat Message:

1

CyberData • Support

Note The Office Ringer is generally used with **Auto Answer** disabled, and produces a loud ring when called. With **Auto Answer** enabled, it will establish a half duplex call, where the Office Ringer receives audio.

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

Figure 1-11. InformaCast enabled Device

InformaCast SIP Config:

DISABLED

Operations Guide 932050A CyberData Corporation

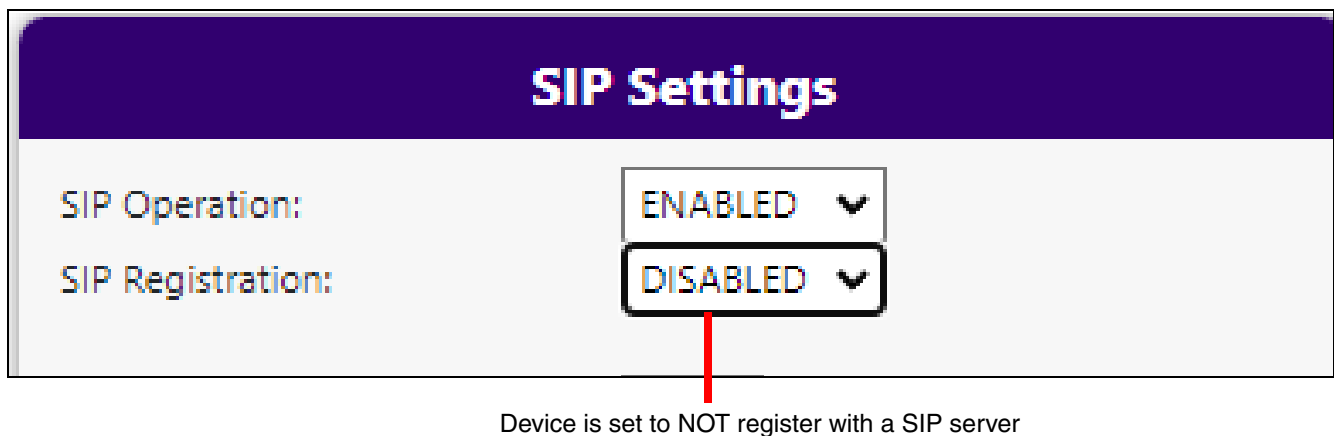
1.6.1 Dial Out Extension Strings and DTMF Tones (using rfc2833)

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

1.6.2 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 1-12](#).

Figure 1-12. SIP Page Set to Point-to-Point Mode



1.7 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 1-13. SSL Page (1 of 2)

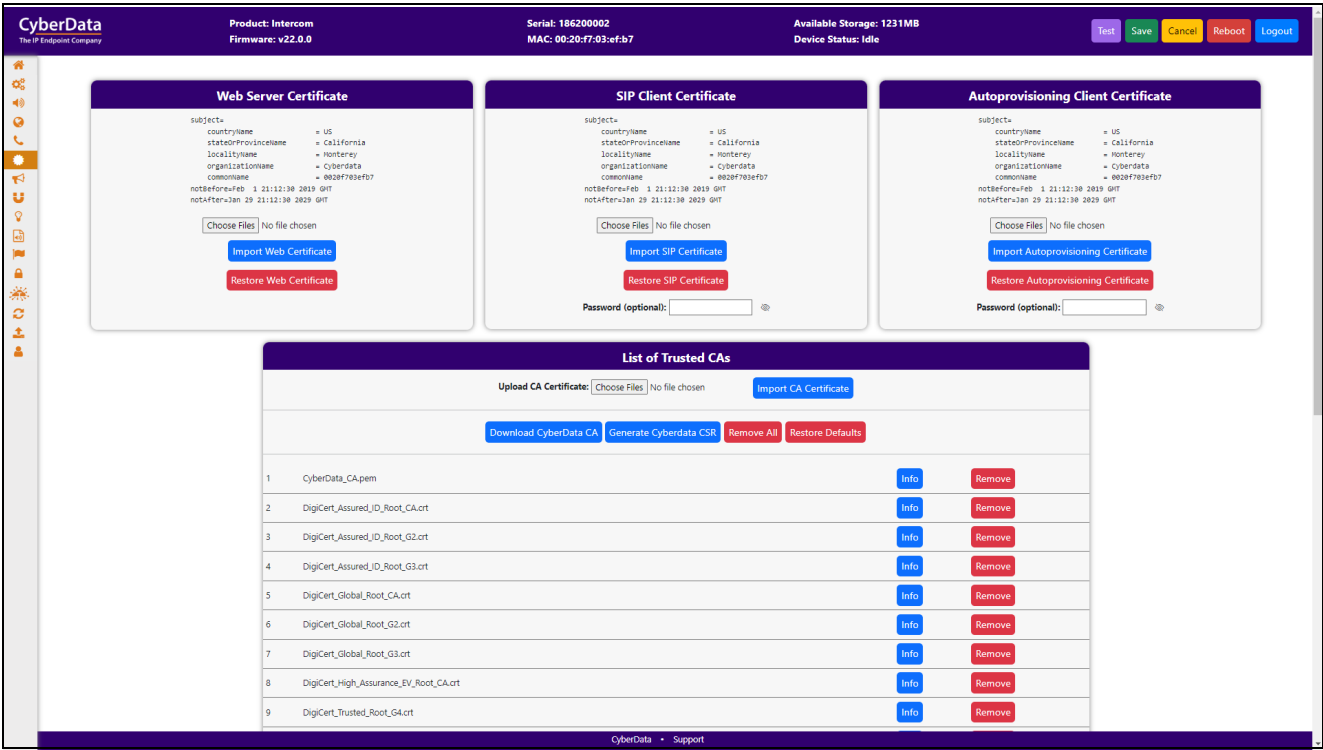


Figure 1-14. SSL Page (2 of 2)

CyberData
The IP Endpoint Company

Product: Intercom
Firmware: v22.0.0

Serial: 186200002
MAC: 00:20:f7:03:ef:b7

Available Storage: 1231MB
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_-_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

CyberData • Support

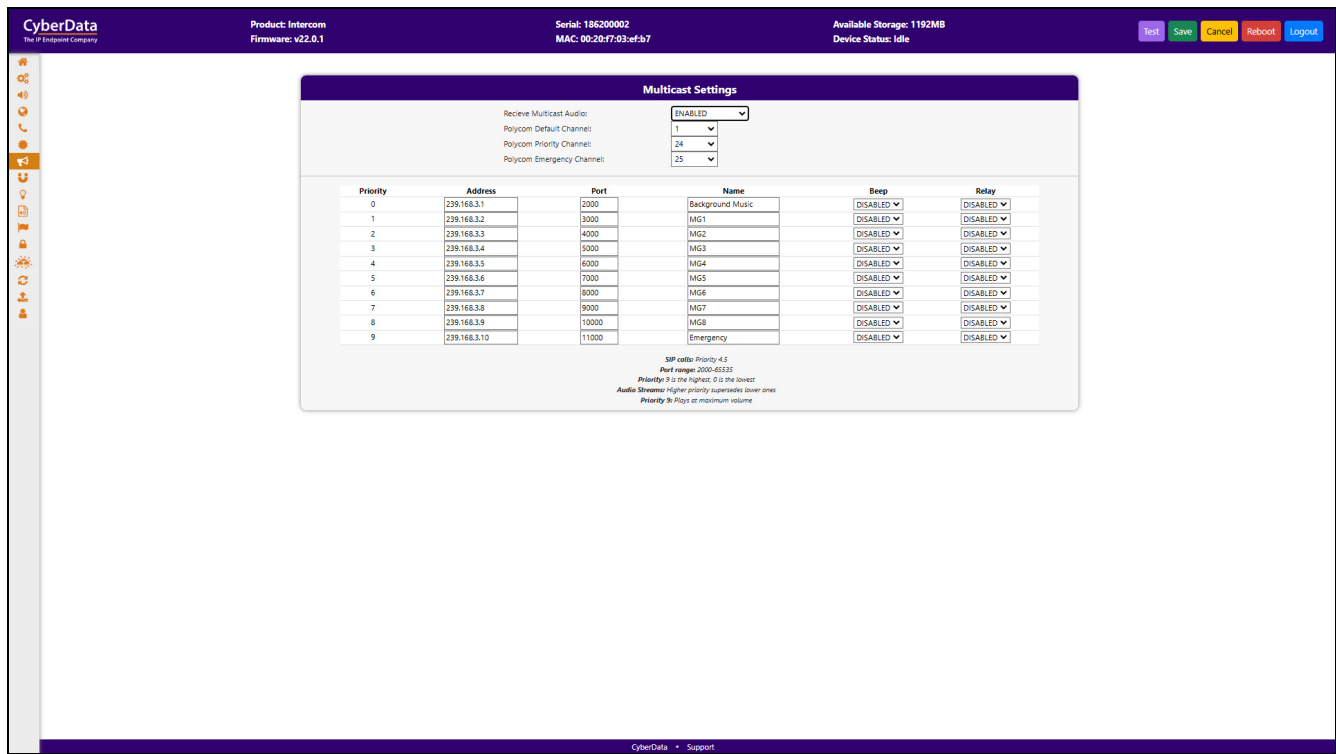
1.8 Multicast

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 1-15. Multicast Page



1.9 Sensor

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

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

Each sensor can trigger up to five different actions:

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

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

Figure 1-16. Sensor Page

The screenshot displays the CyberData web interface for configuring sensors. The top header bar is purple and contains the CyberData logo, product information (Intercom, v22.0.0), serial and MAC addresses, available storage (1231MB), and device status (Idle). On the right of the header are buttons for Test, Save, Cancel, Reboot, and Logout. A vertical sidebar on the left contains various system icons. The main content area is divided into two panels: 'Door Sensor Settings' and 'Intrusion Sensor Settings'.

Door Sensor Settings:

- Sensor Type: Normally Open (dropdown)
- Open Timeout: 0 seconds (input field)
- Flash Button LED: Disabled (dropdown)
- Activate Relay: Disabled (dropdown)
- Play Audio Locally: Disabled (dropdown)
- Call Extension: Disabled (dropdown)
- Dial Out Extension: 204 (input field)
- Dial Out ID: id204 (input field)
- Play Recorded Audio: Disabled (dropdown)
- Repeat Sensor Message: 0 (input field)

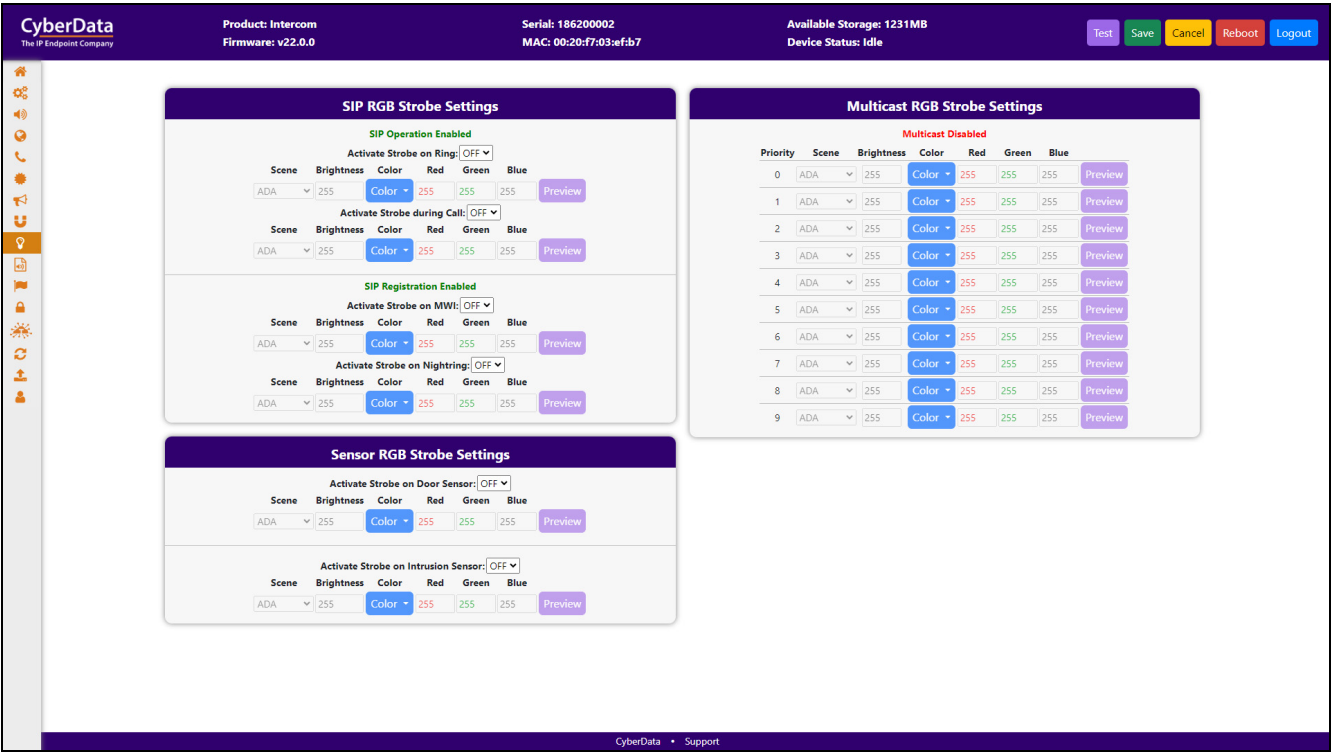
Intrusion Sensor Settings:

- Flash Button LED: Disabled (dropdown)
- Activate Relay: Disabled (dropdown)
- Play Audio Locally: Disabled (dropdown)
- Call Extension: Disabled (dropdown)
- Dial Out Extension: 204 (input field)
- Dial Out ID: id204 (input field)
- Play Recorded Audio: Disabled (dropdown)
- Audio Playbacks: 0 (input field)

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

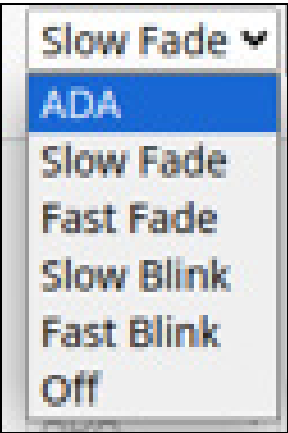
1.10 Strobe

Figure 1-17. Strobe Page



For each option, there are 5 scenes available:

Figure 1-18. 5 Scenes Available



Use the red, green, and blue values to create custom colors.

The ADA scene flashes white at maximum brightness (255). Other scenes can adjust the brightness, from 0 to 255.

Figure 1-19. 10 Colors

Color ▾ 255

- White
- Yellow
- Orange
- Red
- Pink
- Purple
- Blue
- Teal
- Green
- Lime

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

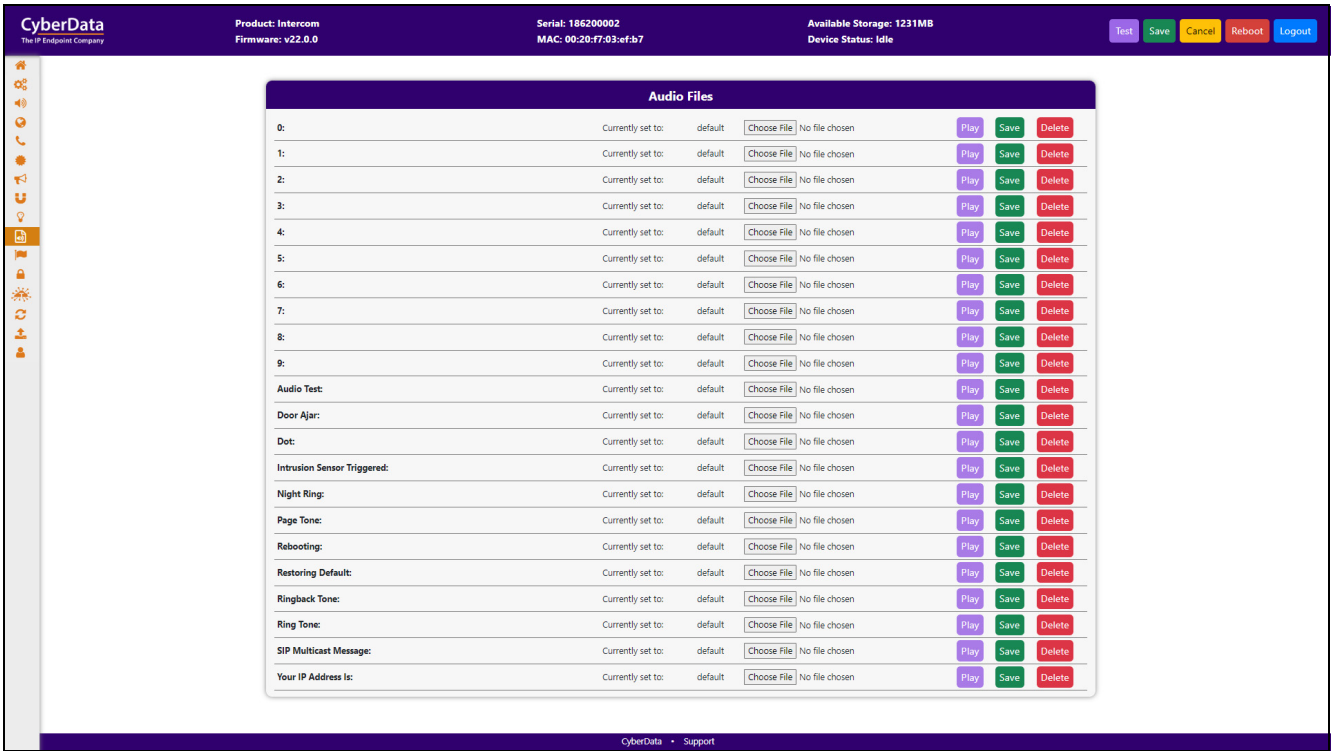
Figure 1-20. InformaCast enabled Device

InformaCast RGB Strobe Settings							
Priority	Scene	Brightness	Color	Red	Green	Blue	
0	ADA ▾	255	Color ▾	255	255	255	Preview
1	ADA ▾	255	Color ▾	255	255	255	Preview
2	ADA ▾	255	Color ▾	255	255	255	Preview
3	ADA ▾	255	Color ▾	255	255	255	Preview
4	ADA ▾	255	Color ▾	255	255	255	Preview
5	ADA ▾	255	Color ▾	255	255	255	Preview
6	ADA ▾	255	Color ▾	255	255	255	Preview
7	ADA ▾	255	Color ▾	255	255	255	Preview
8	ADA ▾	255	Color ▾	255	255	255	Preview
9	ADA ▾	255	Color ▾	255	255	255	Preview

1.11 Audiofiles

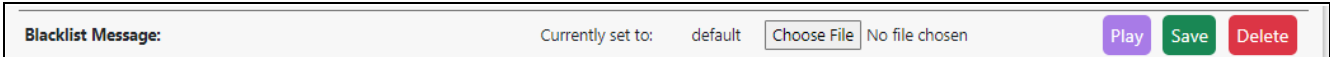
The **Audiofiles** page is used to add custom audio to the board. User uploaded audio will take precedence over the audio files shipped with the device.

Figure 1-21. Audiofiles Page



Note The keypad also has the audio file “Blacklist message”: [Figure 1-22](#).

Figure 1-22. Keypad audio file “Blacklist message”



1.12 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 1-23. Events Page

CyberData
The IP Endpoint Company

Product: Intercom
Firmware: v22.0.0

Serial: 186200002
MAC: 00-20-f7-03-ef-b7

Available Storage: 1231MB
Device Status: Idle

TestSaveCancelRebootLogout

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

Security Events:

DISABLED

Call Started Events:

DISABLED

Call Terminated Events:

DISABLED

Ring Events:

DISABLED

Nightring Events:

DISABLED

Multicast Started Events:

DISABLED

Multicast Stopped Events:

DISABLED

Relay Activated Events:

DISABLED

Relay Deactivated Events:

DISABLED

Remote Relay Events:

DISABLED

Button Events:

DISABLED

Sensor Events:

DISABLED

CyberDataSupport

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

Figure 1-24. InformaCast enabled Device

InformaCast Start Events:

DISABLED

InformaCast Stop Events:

DISABLED

1.12.1 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>
```

1.13 Door Strike Relay

When a Dual Door Strike Relay (DDSR) is associated with a device, the **Door Strike Relay** page appears (Figure 1-25). The DTMF codes entered during a phone call will activate the relays for the specified times, with **0** activating/deactivating indefinitely, until deactivated from the web page, or the DTMF code is entered.

Entering airlock activates the outer relay (relay 2 until the door (door 2) is opened and closed or until it reaches the **Energize Time** configured in the **Configure DSR** dialog box. When door 2 closes, the inner relay (relay1) is activated until door 1 closes. Exit airlock activates the inner relay (relay 1).

If either door is opened longer than the time specified in **Remote Door Sensor Settings**, the device can make a call to a specified extension.

Figure 1-25. Door Strike Relay Page

CyberData
The IP Endpoint Company

Product: Intercom
Firmware: v22.0.0

Serial: 186200002
MAC: 00:20:f7:03:ef:b7

Available Storage: 1231MB
Device Status: Idle

TestSaveCancelRebootLogout

Remote Relay Settings

Associated with 375200007 (10.10.1.104)

Relay	DTMF Code	Duration (seconds)		
Relay 1:	321	2	Pulse	Deactivate
Relay 2:	456	2	Pulse	Deactivate
Both Relays:	654	2	Pulse	Deactivate
Enter Airlock:	789		Enter	Deactivate
Exit Airlock:	987		Exit	Deactivate

Note: A duration of 0 will permanently trigger the relay.

Remote Door Sensor Settings

Door Open Timeout: 0 seconds

Make call to extension: DISABLED

Play recorded audio: DISABLED

Dial Out Extension: 204

Dial Out ID: 0204

Remote Relay Status

Door 1: open Relay 1: inactive

Door 2: open Relay 2: inactive

Refresh

Discovered Remote Relays

Product Type	IP Address	MAC Address	Serial Number	Name	Version	
DoorLock	10.10.1.104	00:20:f7:04:e2:d1	375200007	LOCK375200007	v6.0.0b03	DiscoverConfigDisassociate
DoorLock	10.10.0.51	00:20:f7:05:5e:21	375200300	LOCK375200300	v5.0.4	View

CyberDataSupport

1.14 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 1-26. Terminus Page

The screenshot displays the Terminus configuration page within the CyberData web interface. The top navigation bar is purple and contains the CyberData logo, product information (Intercom, v22.0.0), device details (Serial: 186200002, MAC: 00:20:f7:03:ef:b7), available storage (1231MB), 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 for navigation. The main content area features two configuration panels: 'Discovery Setting' and 'Lockdown Settings'. The 'Discovery Setting' panel includes fields for Multicast Address (239.27.32.4), Time to Live (255), and Discovery Interval (60 seconds). The 'Lockdown Settings' panel includes a Lock Down Mode dropdown (set to Disabled) and three relay settings (Relay, DSR Remote Relay 1, and DSR Remote Relay 2), all set to 'No Action'. The footer of the interface shows 'CyberData • Support'.

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
DSR Remote Relay 1:	No Action
DSR Remote Relay 2:	No Action

1.15 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 1-27. Autoprovisioning Page

The screenshot displays the CyberData Autoprovisioning configuration interface. At the top, a status bar shows 'Product: Intercom', 'Serial: 186200002', 'Available Storage: 1231MB', and 'Device Status: Idle'. Below this, the 'Autoprov Settings' panel contains the following fields:

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

A 'Download Template' button is located at the bottom of the settings panel. To the right, the 'Autoprov Log' panel displays a list of events:

- 2024-10-03 11:46:17 Autoprov: no autoprov triggers. Exiting...
- 2024-10-03 11:46:16 Autoprovisioning on boot
- 2024-10-03 11:46:16 Autoprov found server="http://10.0.0.242" in dhcp option 43
- 2024-10-03 11:46:16 Autoprov looking for 0020f703efb7.xml at http://10.0.0.242
- 2024-10-03 11:46:16 Autoprov downloading http://10.0.0.242/0020f703efb7.xml
- 2024-10-03 11:46:17 Got autoprov file. Parsing "0020f703efb7.xml"
- 2024-10-03 11:46:17 Autoprov: Processing ssl certificates
- 2024-10-03 11:46:17 No certificate elements in SSLCertificates
- 2024-10-03 11:46:17 Autoprov: Processing audio files
- 2024-10-03 11:46:18 Autoprov: FirmwareSettings config not found
- 2024-10-03 11:46:18 DeviceConfig: error = False
- 2024-10-03 11:46:18 SSLCertificates: error = None
- 2024-10-03 11:46:18 AudioFiles: error = False
- 2024-10-03 11:46:18 BellSchedule: error = False
- 2024-10-03 11:46:18 FirmwareSettings: error = None

1.16 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


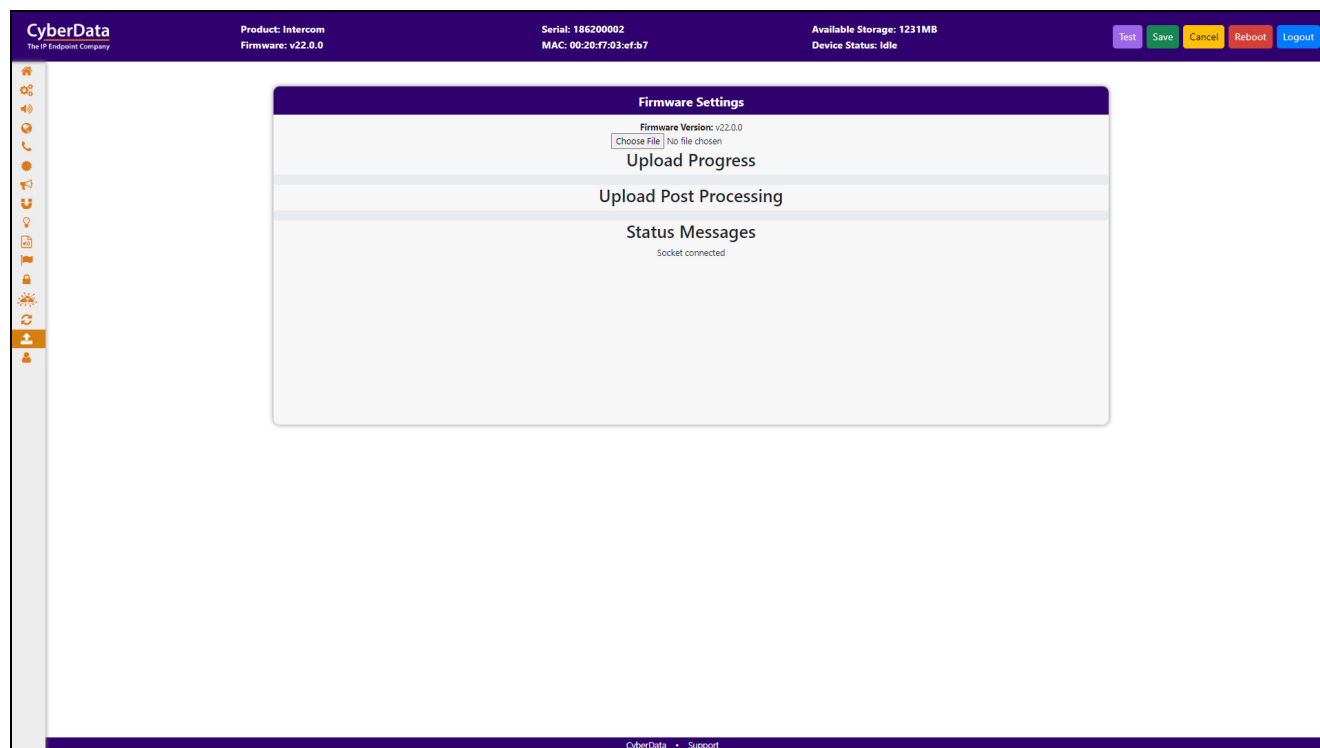
 GENERAL ALERT	Caution Equipment Hazard: Do not reboot the device. It will reboot automatically when the process is complete.
--	---

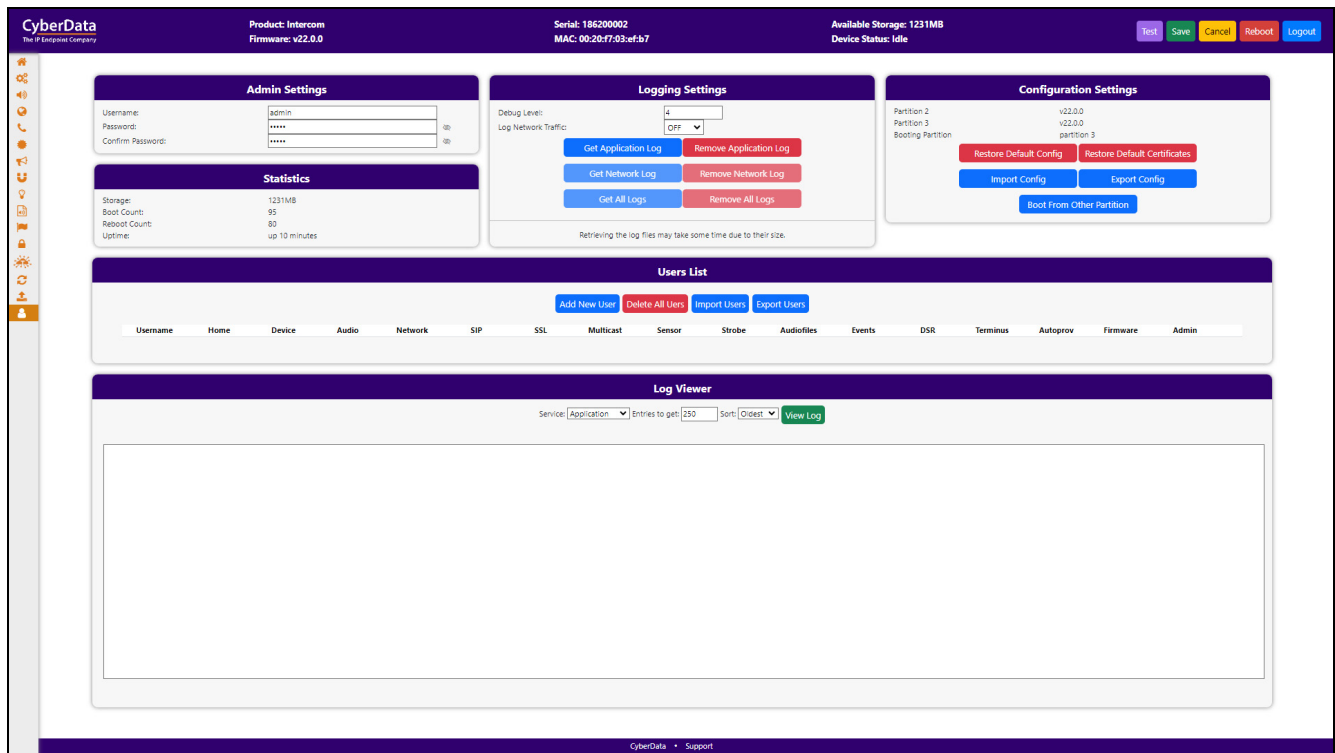
Figure 1-28. Firmware Page



1.17 Admin

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

Figure 1-29. Admin Page



1.18 Keypad Pages

1.18.1 Buttons

Note **SECURITY** must be selected as the dial mode to use security settings and to send multicast.

Figure 1-30. Buttons Page

CyberData
The IP Endpoint Company

Product: Keypad Intercom
Firmware: v22.0.0

Serial: 214200002
MAC: 00:20:f7:03:f5:e3

Available Storage: 1271MB
Device Status: Idle

TestSaveCancelRebootLogout

Dial Settings

Keypad Mode: TELEPHONE
Play Button Tones: ON
Speed Dial Timeout: 2 seconds

Security Mode Settings

Relay Activation Code: 9876123
Relay Deactivation Code: 9876456
Telephone Dialout: ON
Send Multicast Audio: Disabled
Multicast Address: 224.5.5.5
Multicast Port: 5050
Repeat Message: 1

Keypad Mapping

Button	Extension	Extension ID
Keypad 1	241	id241
Keypad 2	242	id242
Keypad 3	243	id243
Keypad 4	244	id244
Keypad 5	245	id245
Keypad 6	246	id246
Keypad 7	247	id247
Keypad 8	248	id248
Keypad 9	249	id249
Keypad 0	2411	id2411
Keypad *	2410	id2410
Keypad #	2412	id2412
Call Button	204	id204

1.18.2 Security

Note When a user from the access list enters their access code, the actions that follow are configured on this page. **SECURITY** mode must be enabled on the **Buttons** page.

Figure 1-31. Security Page

CyberData
The IP Endpoint Company

Product: Keypad Intercom
Firmware: v22.0.0

Serial: 214200002
MAC: 00:20:f7:03:f5:a3

Available Storage: 1271MB
Device Status: Idle

TestSaveCancelRebootLogout

Relay Settings

Activate Relay on Valid Code: ON
Activate DSR on Valid Code: OFF
Relay Timeout: 6 seconds

Audio Settings

Buzz while Relay Active: OFF
Play Tone on Invalid Code Entry: OFF

Sensor Settings

Buzz on Door Open Timeout: OFF
Sensor Type: Normally Open
Sensor Open Timeout: OFF
DSR Open Timeout: OFF

Blacklist Settings

SIP Call Audio Message: Disabled
Dial Out Extension: 666
Dial Out ID: ext666
Repeat Message: 0
Send Multicast Audio: Disabled
Multicast Address: 234.6.6.6
Multicast Port: 666
Repeat Message: 0

1.18.3 Access List

Figure 1-32. Access List Page

CyberData
The IP Endpoint Company

Product: Keypad Intercom
Firmware: v22.0.0

Serial: 214200002
MAC: 00:20:f7:03:f5:e3

Available Storage: 1271MB
Device Status: Idle

TestSaveCancelRebootLogout

Access List

Delete All UsersRestore DefaultsImport UsersExport Users

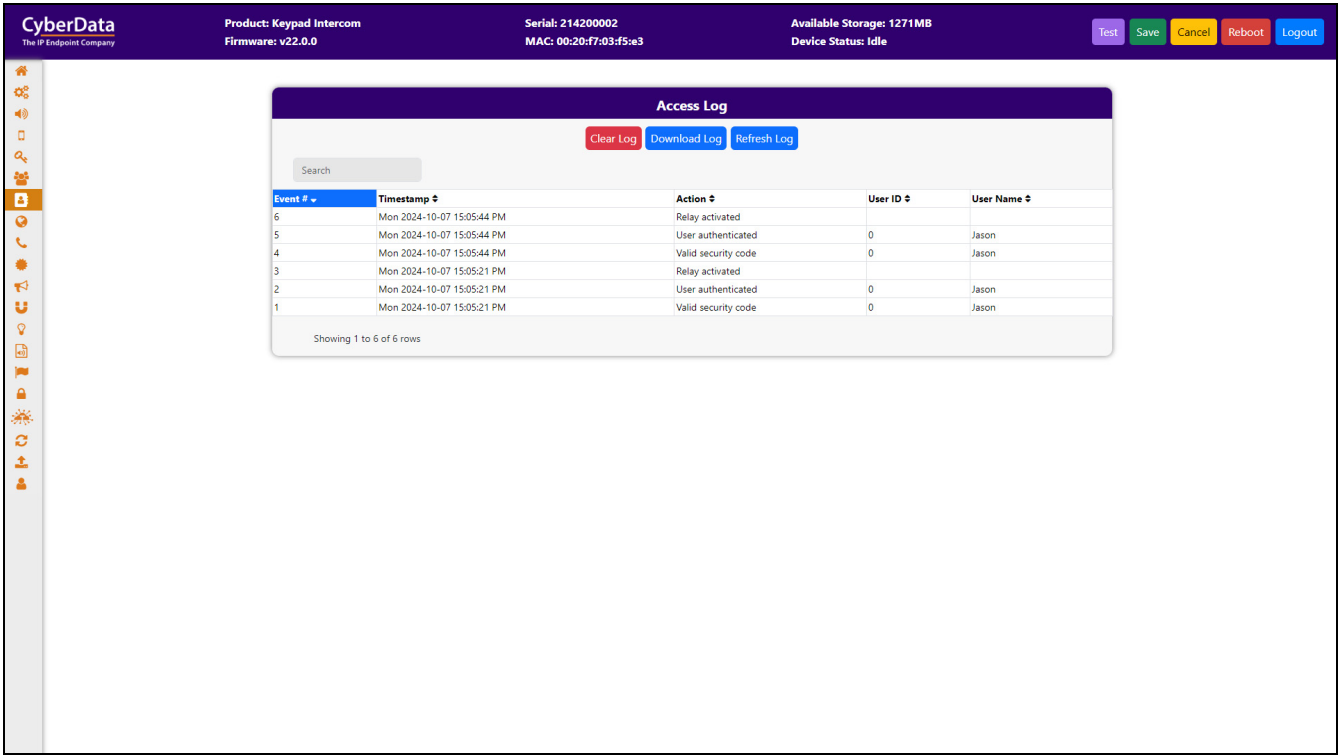
ID	Name	Valid From	Valid To	Blacklist	Lockdown Override		
0	Jason	All	All	NO	NO	Edit	Delete
1		All	All	NO	NO	Add	Delete
2		All	All	NO	NO	Add	Delete
3		All	All	NO	NO	Add	Delete
4		All	All	NO	NO	Add	Delete
5		All	All	NO	NO	Add	Delete
6		All	All	NO	NO	Add	Delete
7		All	All	NO	NO	Add	Delete
8		All	All	NO	NO	Add	Delete
9		All	All	NO	NO	Add	Delete

<<12345678910>>

1.18.4 Access Log

Note The Access log is exported in CSV format, and is compatible with many spreadsheet programs, including MS Excel and Google Sheets.

Figure 1-33. Access Log Page



1.19 Command Interface

Some functions on the device can be activated using simple POST commands to the web interface. The examples in [Table 1-2](#) use the free unix utility, **wget** commands. However, any program that can send HTTP POST commands to the device should work.

1.19.1 Command Interface Post Commands

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

Table 1-2. 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"
Place call to extension (example: extension 600)	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.154/command" --post-data "request=call&extension=600"
Test Relay	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_relay"
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"
Test Mic	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_mic"
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

Access List 28
Access Log 29
Admin 25
Audio 6
Audiofiles 16
Autoprovisioning 23

B

Buttons 26

C

Command Interface 30
Command Interface Post Commands 30
Contact Information 31

D

Device 5
Dial Out Extension Strings and DTMF Tones 9, 10
Discovery Utility program 1
Door Strike Relay 21

E

Events 17

F

Firmware 24

H

Home Page 3

K

Keypad Pages 26

L

Log In Page 1

M

Multicast 12

N

Network 7

P

Point-to-Point Configuration 9

S

Security 27
Sensor 13
SIP (Session Initiation Protocol) 8
SSL 10
Stroke 14

T

Terminus 22
Troubleshooting/Technical Support 31

W

Warranty and RMA Information 31