CyberData
The IP Endpoint Company

CyberData Intercoms Operations Guide

Part #s: *011186, 011209, 011211, 011214, 011305, 011309, 011304, 011530, 011567*

Document Part #*932050A*
for Firmware Version *22.0.1*

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

CyberData Intercoms Operations Guide 932050A
Part # 011186, 011209, 011211, 011214, 011305, 011309, 011304, 011530, 011567

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.

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 932050A, which corresponds to firmware version 22.0.1, 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	Warning *Electrical Hazard:* This product should be installed by a licensed electrician according to all local electrical and building codes.

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

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

Abbreviations and Terms

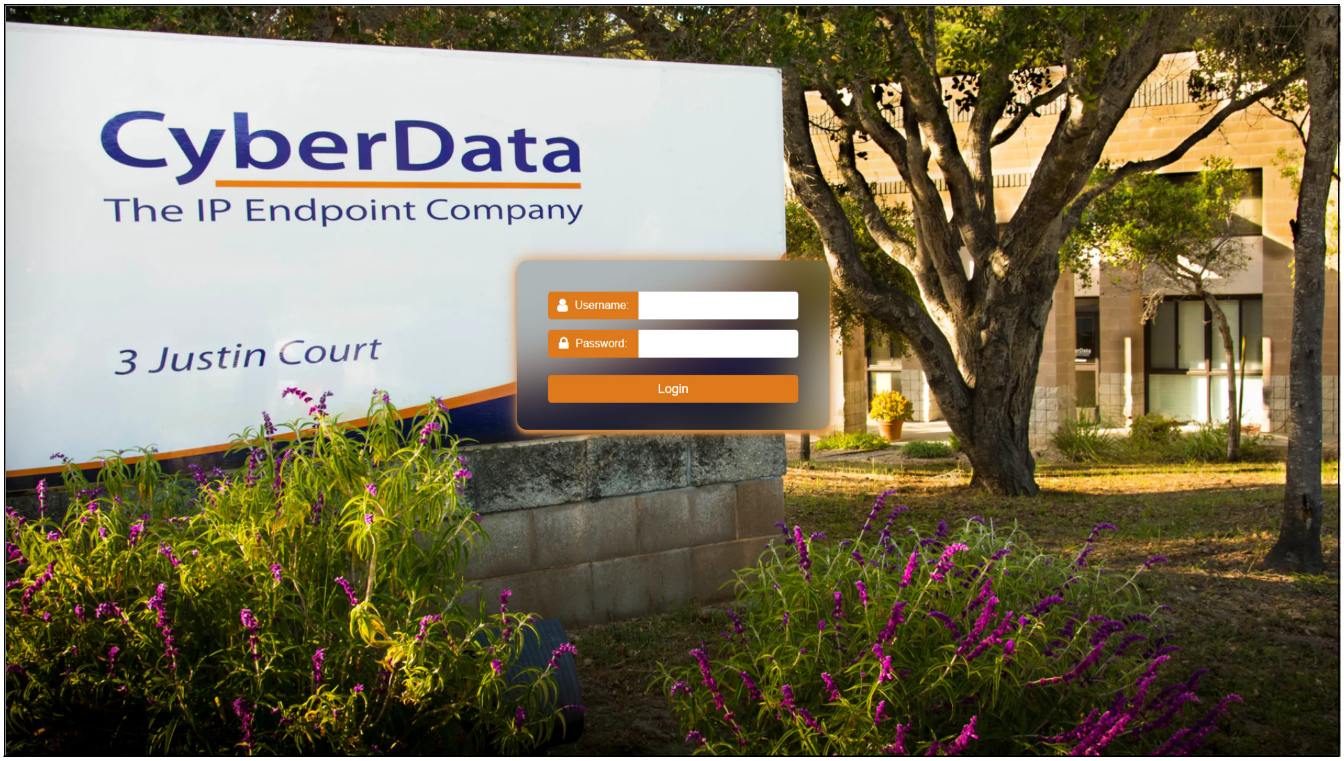
Abbreviation or Term	Definition
A-law	A standard companding algorithm, used in European digital communications systems to optimize, i.e., modify, the dynamic range of an analog signal for digitizing.
AVP	Audio Video Profile
Cat 5	TIA/EIA-568-B Category 5
DHCP	Dynamic Host Configuration Protocol
LAN	Local 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

Contents

1 Configure the Device

1.1 Home Page

Figure 1-1. Log In Page



1. Open your browser to the Intercom 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**

1.1.1 Restoring defaults and announcing the ip address

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

Briefly pressing the RTFM button (Figure 1-2), prompts the device to announce its IP address.

Holding the button for approximately five seconds restores the device to its factory defaults, defaulting to DHCP to obtain an IP address, or using 192.168.1.23 if a DHCP server is not present.

Figure 1-2. RTFM Button (SW1)

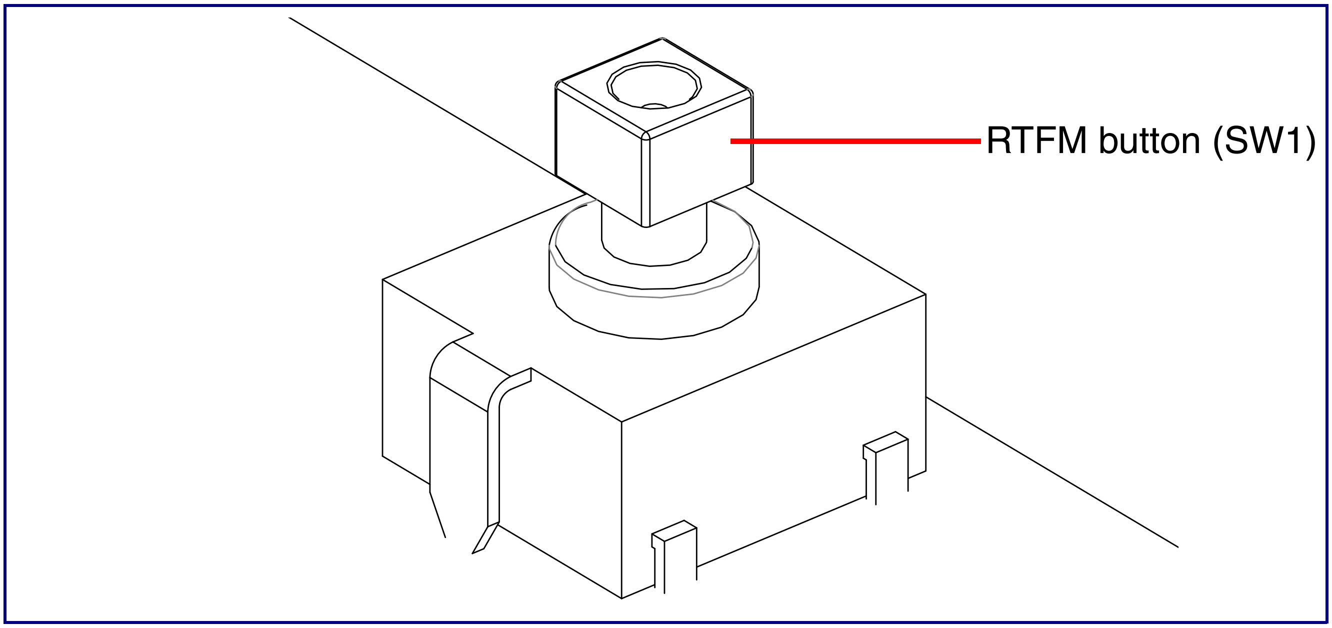
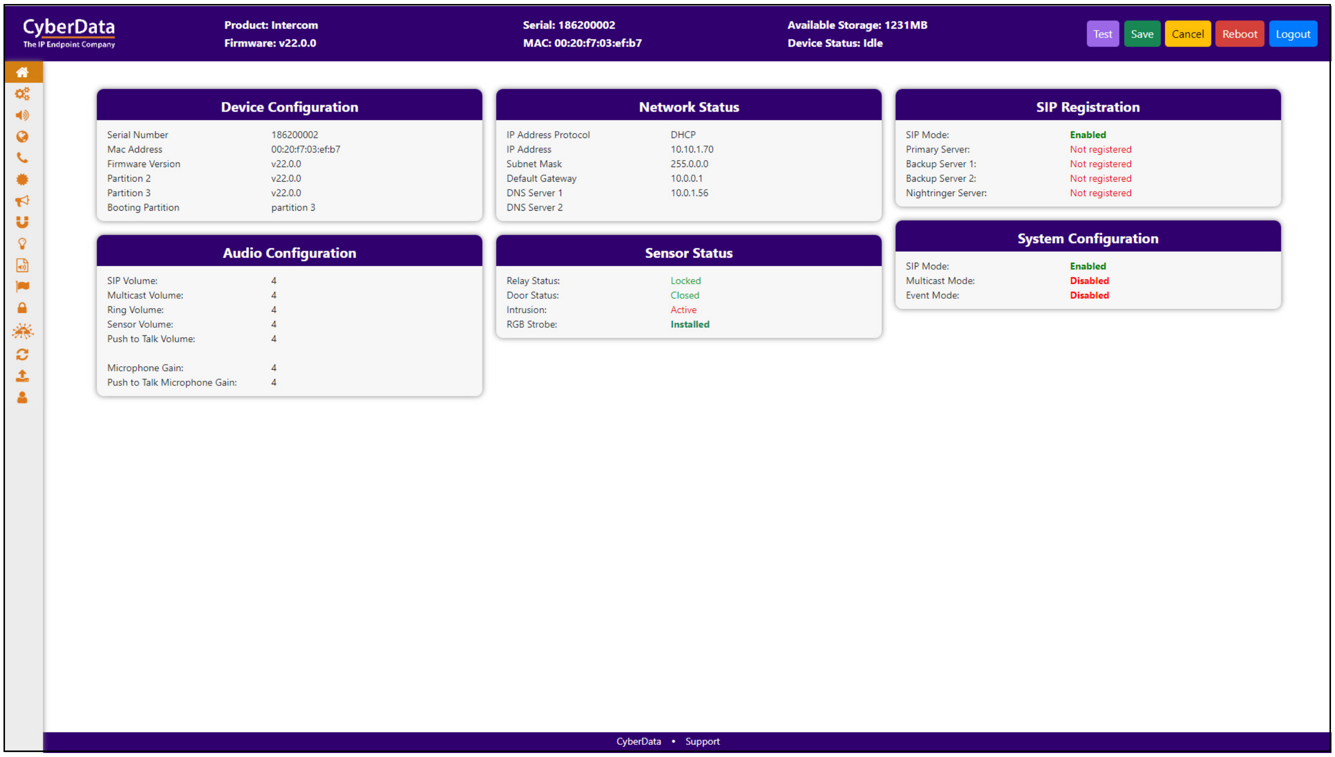


Figure 1-3. Home Page



Product: Intercom
Firmware: v22.0.0

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

Available Storage: 1231MB
Device Status: Idle

Device Configuration

Serial Number	186200002
Mac Address	00:20:f7:03:ef:b7
Firmware Version	v22.0.0
Partition 2	v22.0.0
Partition 3	v22.0.0
Booting Partition	partition 3

Network Status

IP Address Protocol	DHCP
IP Address	10.10.1.70
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
Ring Volume:	4
Sensor Volume:	4
Push to Talk Volume:	4
Microphone Gain:	4
Push to Talk Microphone Gain:	4

Sensor Status

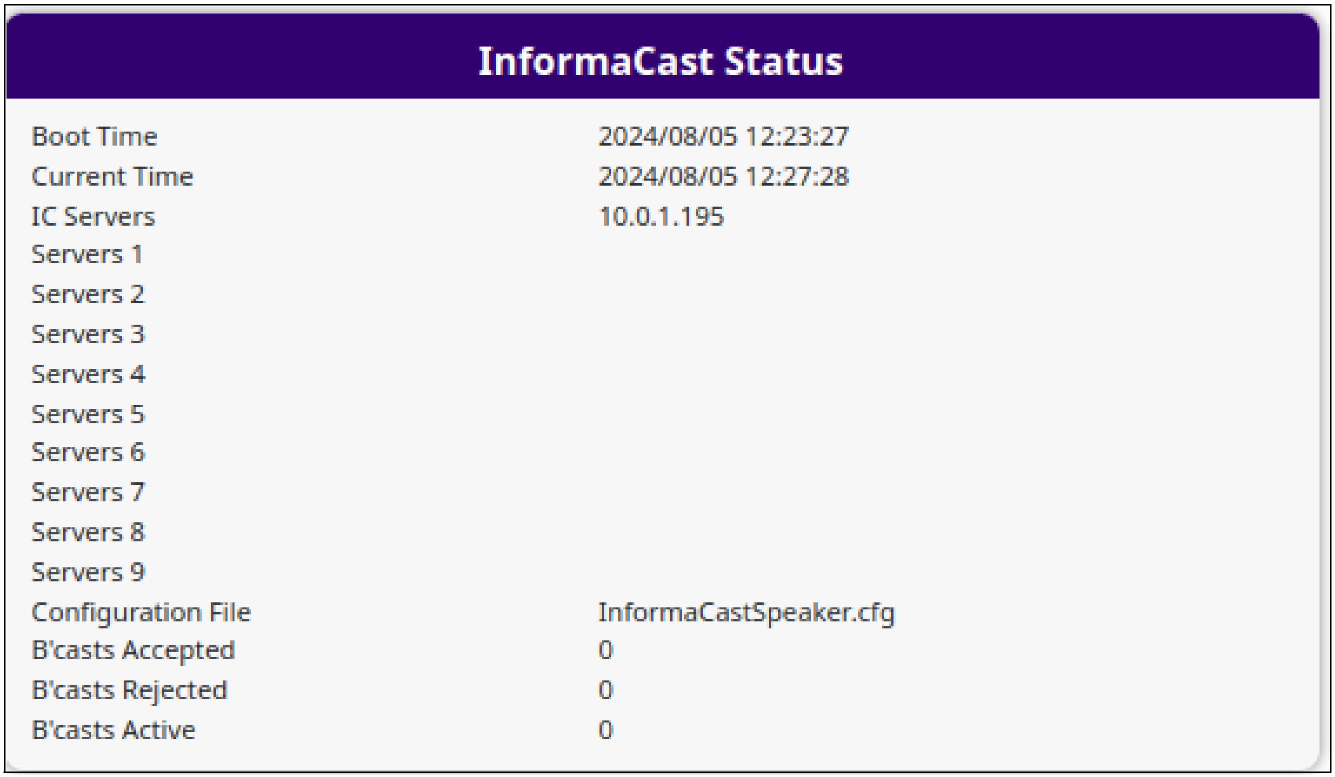
Relay Status:	Locked
Door Status:	Closed
Intrusion:	Active
RGB Strobe:	Installed

System Configuration

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

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

Figure 1-4. InformaCast enabled Device

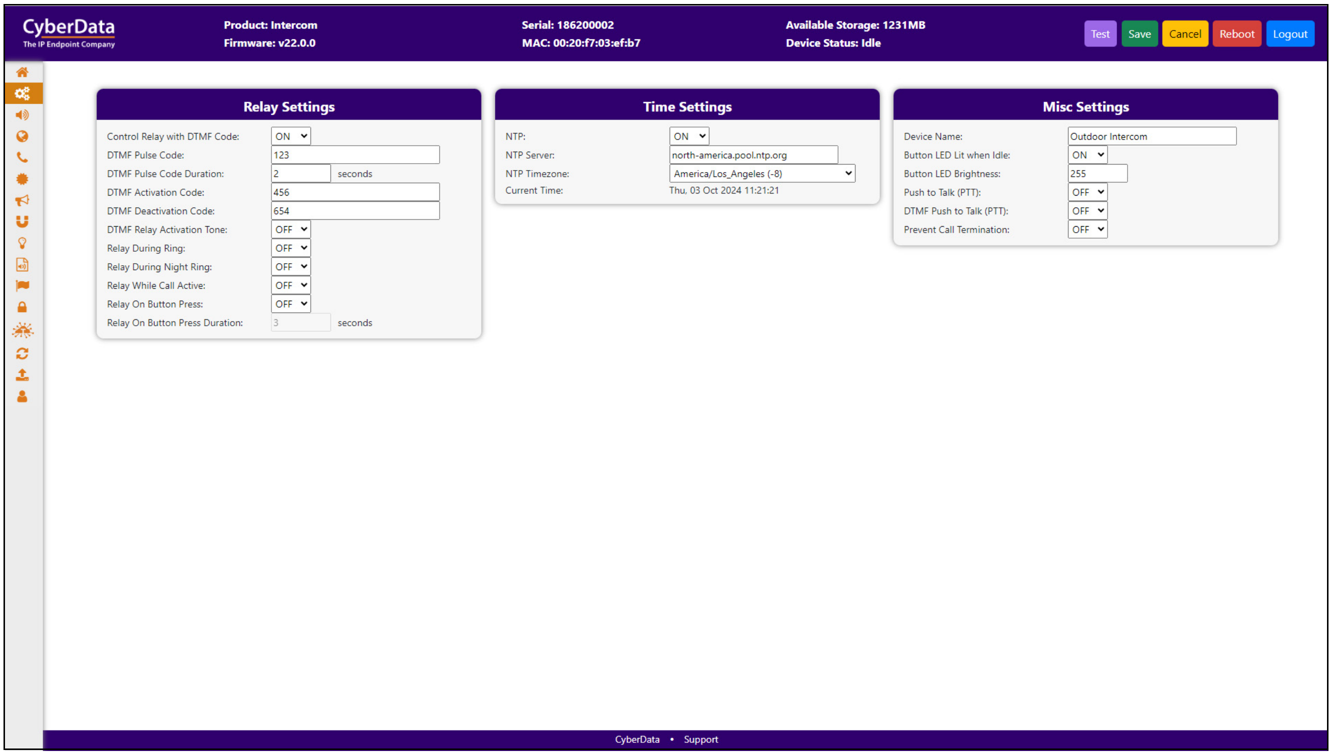


InformaCast Status

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

1.2 Device

Figure 1-5. Device Configuration Page



Product: Intercom
Firmware: v22.0.0
Serial: 186200002
MAC: 00:20:f7:03:ef:b7
Available Storage: 1231MB
Device Status: Idle

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

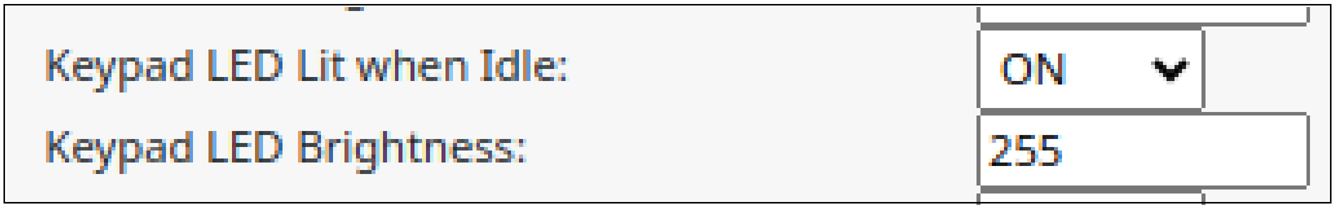
NTP: ON
NTP Server: north-america.pool.ntp.org
NTP Timezone: America/Los_Angeles (-8)
Current Time: Thu, 03 Oct 2024 11:21:21

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

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

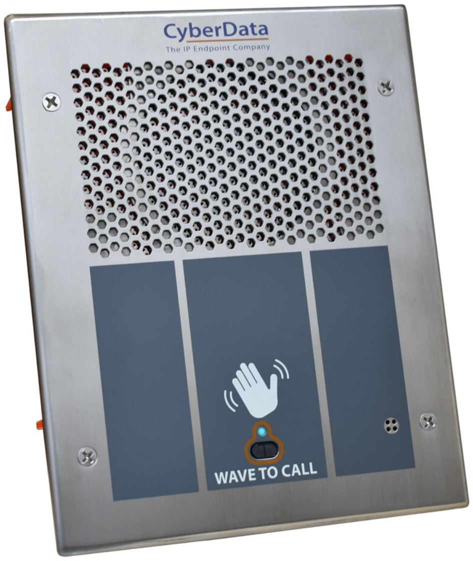
Figure 1-6. Options for the Keypad LED



Keypad LED Lit when Idle: ON
Keypad LED Brightness: 255

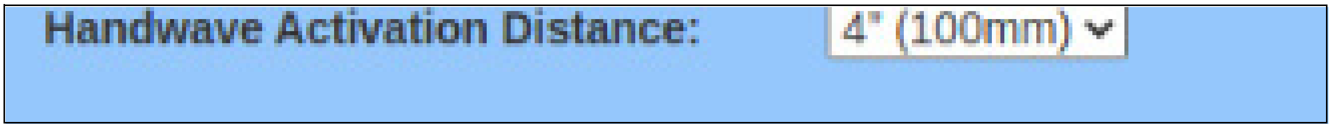
The SIP Hand Wave Indoor Intercom (Figure 1-7) features touchless activation.

Figure 1-7. SIP Hand Wave Indoor Intercom



On the **Device** page, use the Handwave Activation Distance setting (Figure 1-8). Select a distance of 2, 4, or 6 feet.

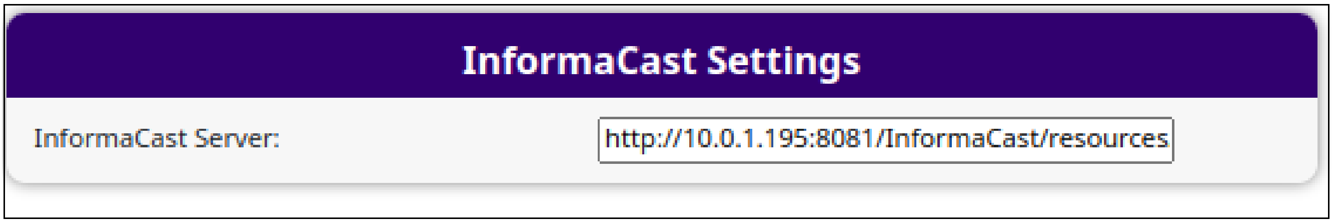
Figure 1-8. Handwave Activation Distance



Handwave Activation Distance: 4" (100mm)

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

Figure 1-9. InformaCast enabled Device

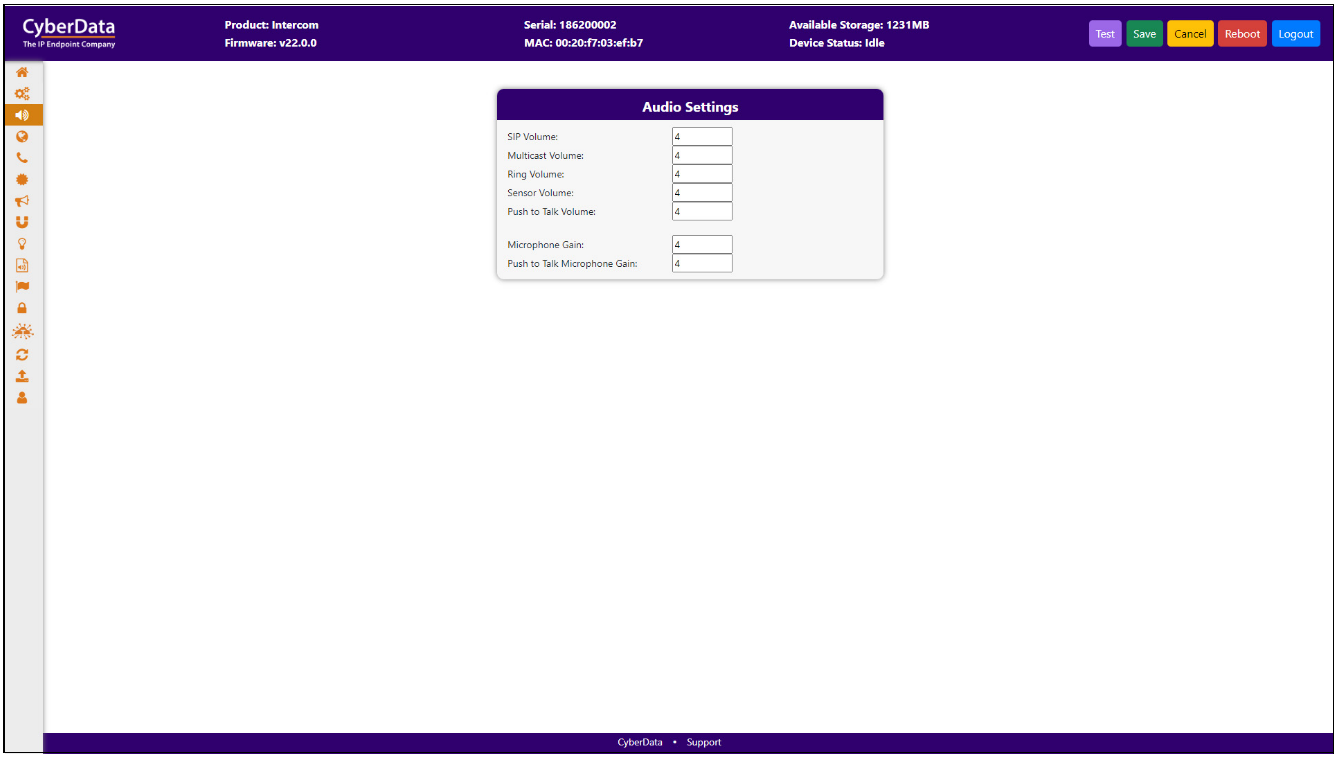


InformaCast Settings

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

1.3 Audio

Figure 1-10. Audio Page



Product: Intercom
Firmware: v22.0.0

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

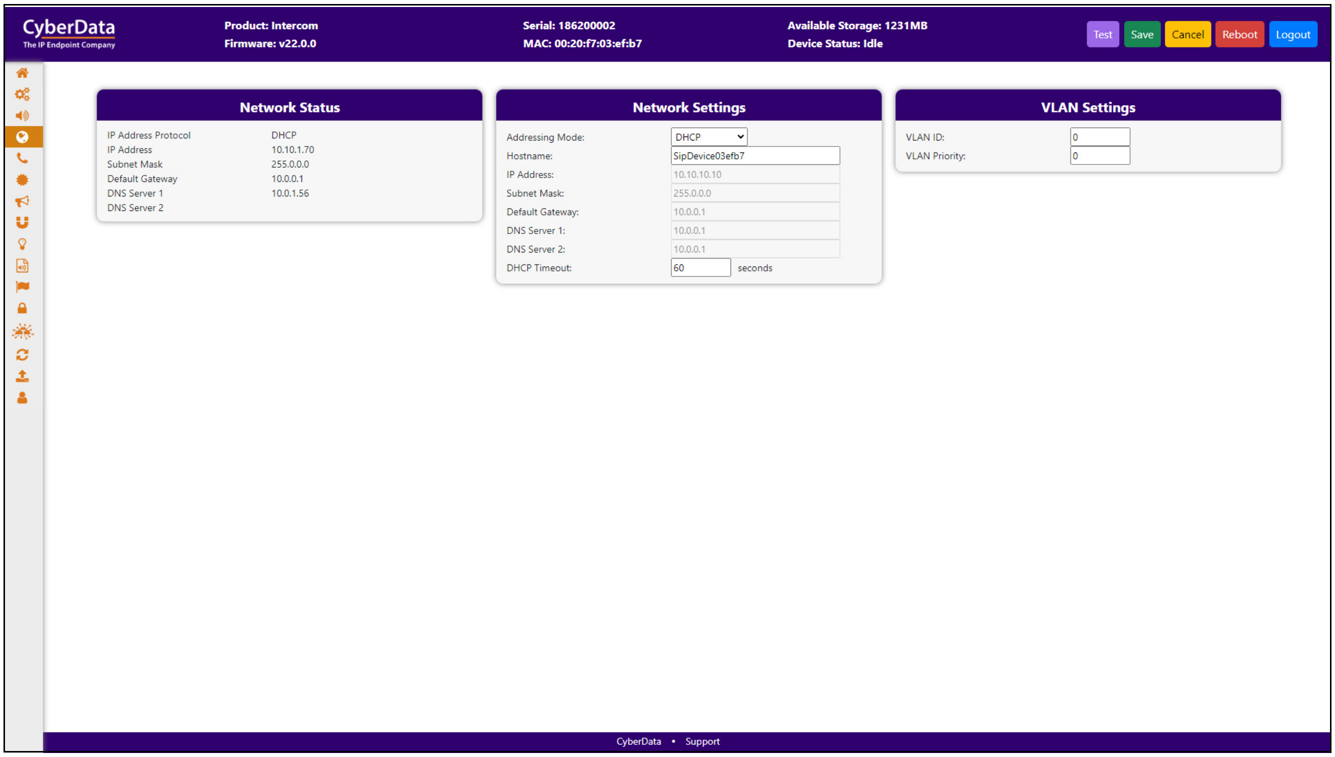
Available Storage: 1231MB
Device Status: Idle

SIP Volume: 4
Multicast Volume: 4
Ring Volume: 4
Sensor Volume: 4
Push to Talk Volume: 4

Microphone Gain: 4
Push to Talk Microphone Gain: 4

1.4 Network

Figure 1-11. Network Page



Product: Intercom
Firmware: v22.0.0
Serial: 186200002
MAC: 00:20:f7:03:ef:b7
Available Storage: 1231MB
Device Status: Idle

Network Status

IP Address Protocol	DHCP
IP Address	10.10.1.70
Subnet Mask	255.0.0.0
Default Gateway	10.0.0.1
DNS Server 1	10.0.1.56
DNS Server 2	

Network Settings

Addressing Mode:	DHCP
Hostname:	SipDevice03efb7
IP Address:	10.10.10.10
Subnet Mask:	255.0.0.0
Default Gateway:	10.0.0.1
DNS Server 1:	10.0.0.1
DNS Server 2:	10.0.0.1
DHCP Timeout:	60 seconds

VLAN Settings

VLAN ID:	0
VLAN Priority:	0

1.5 SIP (Session Initiation Protocol)

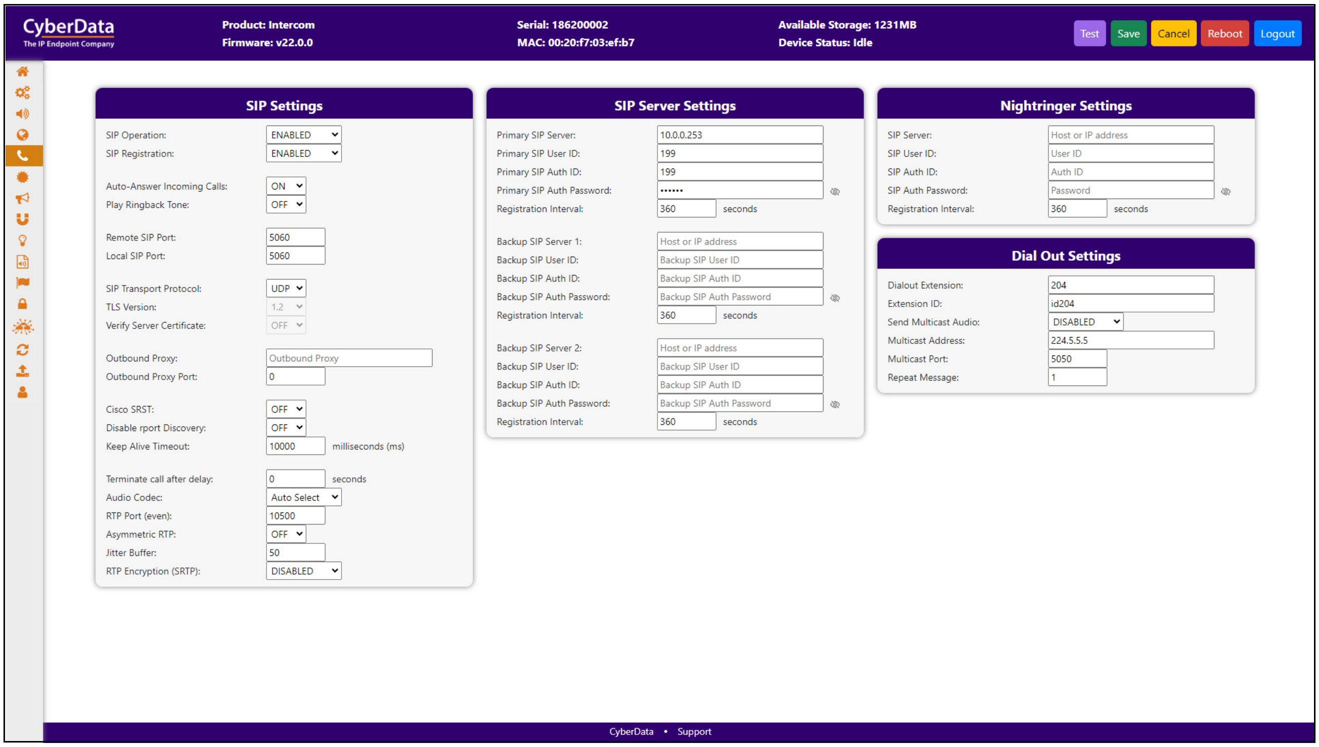
This page sets the options for phone calls. Configure up to 3 servers, with 2 acting as backup, and a server for the nightringer. The nightringer is a second sip extension that only rings, never connects to a call. Many customers use the nightringer in a hunt group.

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 1-12. SIP Page



Product: Intercom
Firmware: v22.0.0
Serial: 186200002
MAC: 00:20:f7:03:ef:b7
Available Storage: 1231MB
Device Status: Idle

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

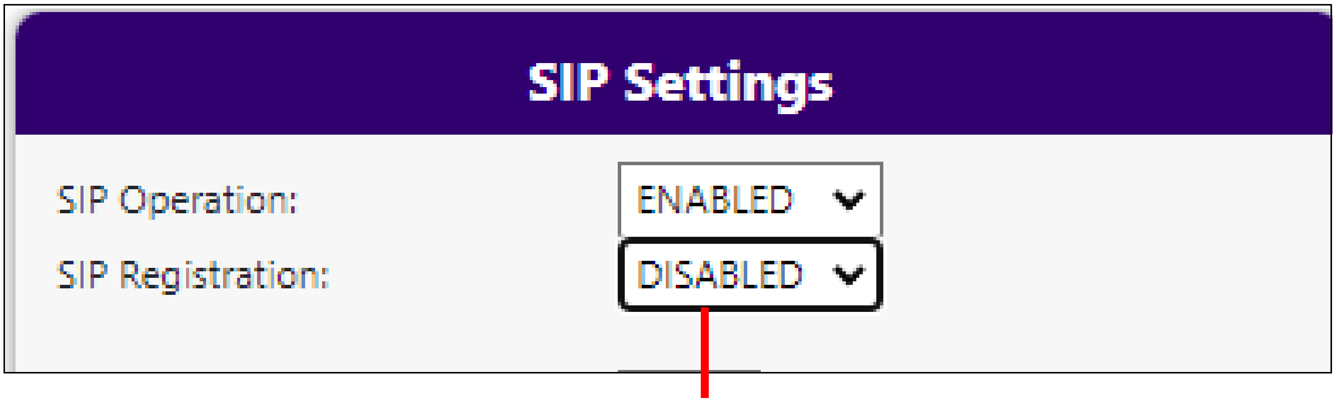
1.5.1 Dial Out Extension Strings and DTMF Tones (using rfc2833)

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

1.5.2 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 1-13.

Figure 1-13. SIP Page Set to Point-to-Point Mode



SIP Settings

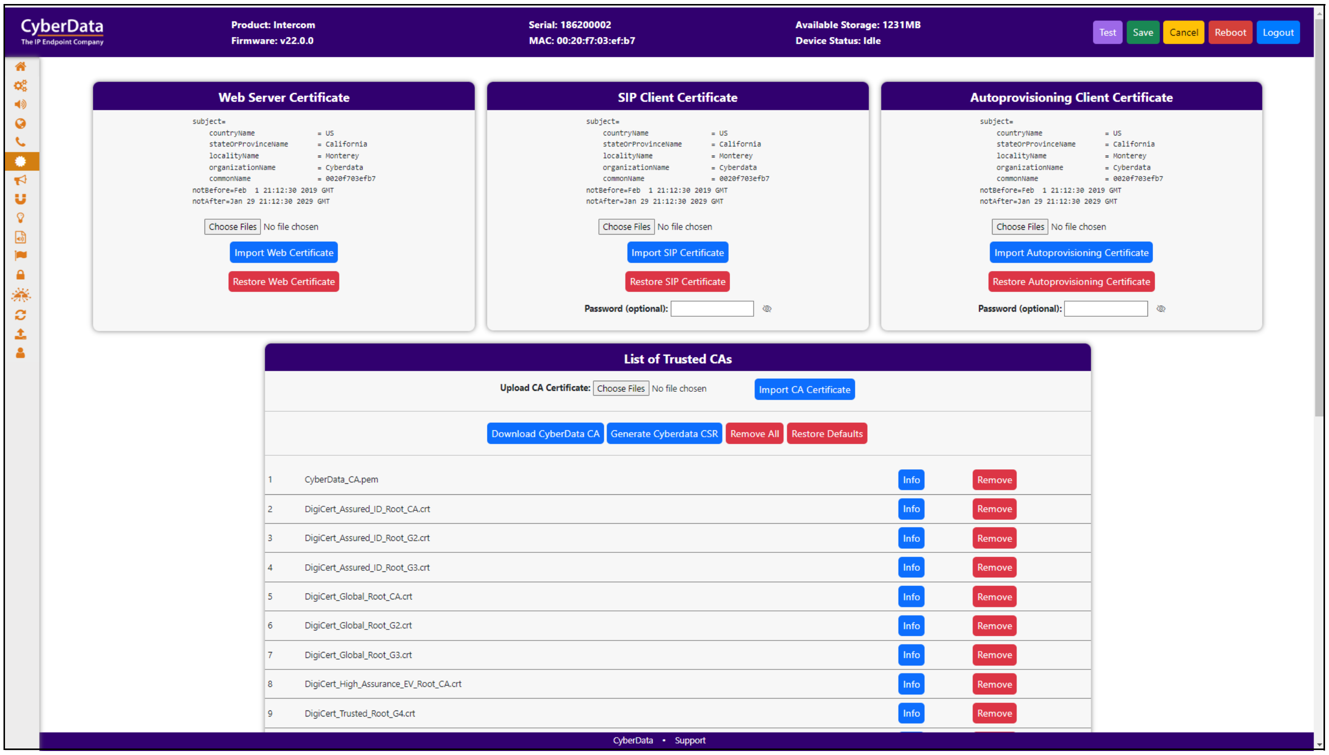
SIP Operation: ENABLED

SIP Registration: DISABLED

Device is set to NOT register with a SIP server

1.6 SSL

Figure 1-14. SSL Page



Product: Intercom
Firmware: v22.0.0
Serial: 186200002
MAC: 00:20:f7:03:ef:b7
Available Storage: 1231MB
Device Status: Idle

Web Server Certificate

```
subject=
    countryName               = US
    stateOrProvinceName       = California
    localityName              = Monterey
    organizationName          = Cyberdata
    commonName                = 0020f703efb7
notBefore=Feb  1 21:12:30 2019 GMT
notAfter=Jan 29 21:12:30 2029 GMT
```

Choose Files No file chosen

Import Web Certificate

Restore Web Certificate

SIP Client Certificate

```
subject=
    countryName               = US
    stateOrProvinceName       = California
    localityName              = Monterey
    organizationName          = Cyberdata
    commonName                = 0020f703efb7
notBefore=Feb  1 21:12:30 2019 GMT
notAfter=Jan 29 21:12:30 2029 GMT
```

Choose Files No file chosen

Import SIP Certificate

Restore SIP Certificate

Password (optional):

Autoprovisioning Client Certificate

```
subject=
    countryName               = US
    stateOrProvinceName       = California
    localityName              = Monterey
    organizationName          = Cyberdata
    commonName                = 0020f703efb7
notBefore=Feb  1 21:12:30 2019 GMT
notAfter=Jan 29 21:12:30 2029 GMT
```

Choose Files No file chosen

Import Autoprovisioning Certificate

Restore Autoprovisioning Certificate

Password (optional):

List of Trusted CAs

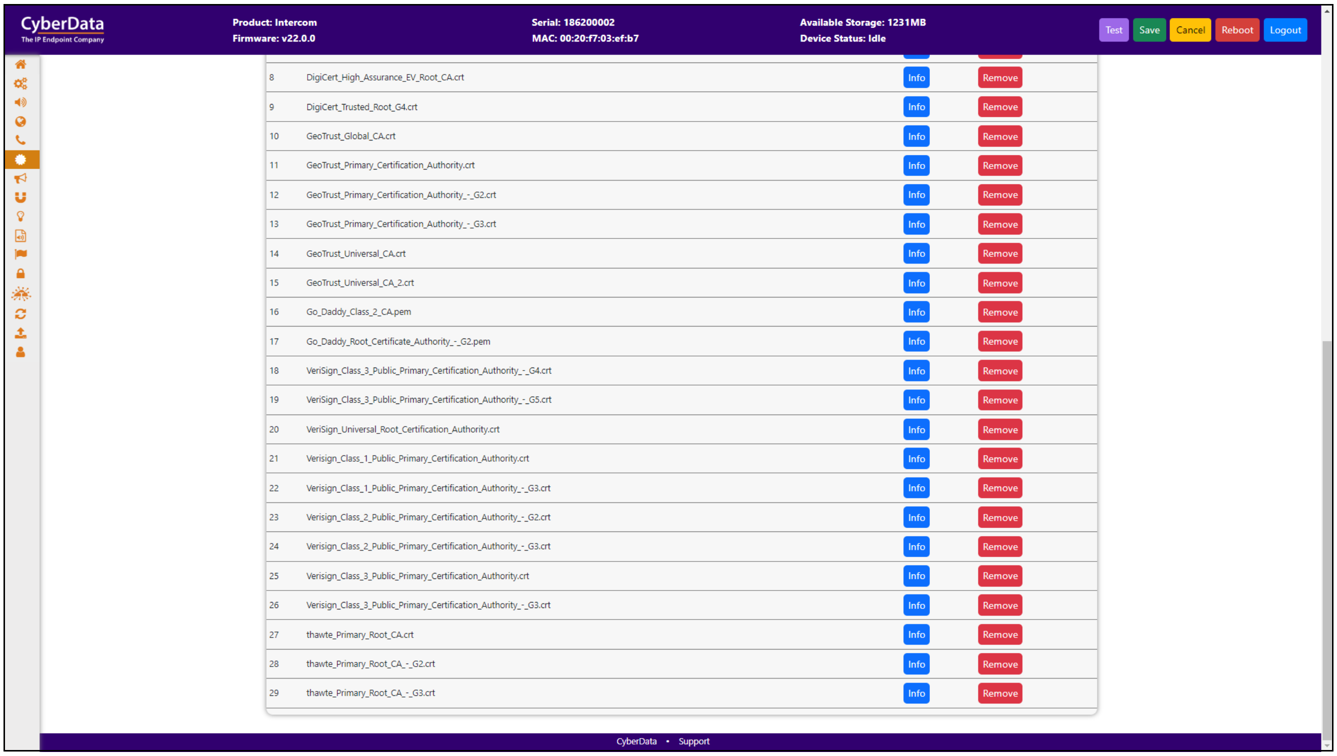
Upload CA Certificate: Choose Files No file chosen Import CA Certificate

Download CyberData CA | Generate Cyberdata CSR | Remove All | Restore Defaults

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

CyberData • Support

Figure 1-15. SSL Page



Product: Intercom
Firmware: v22.0.0
Serial: 186200002
MAC: 00:20:f7:03:ef:b7
Available Storage: 1231MB
Device Status: Idle

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

1.7 Multicast

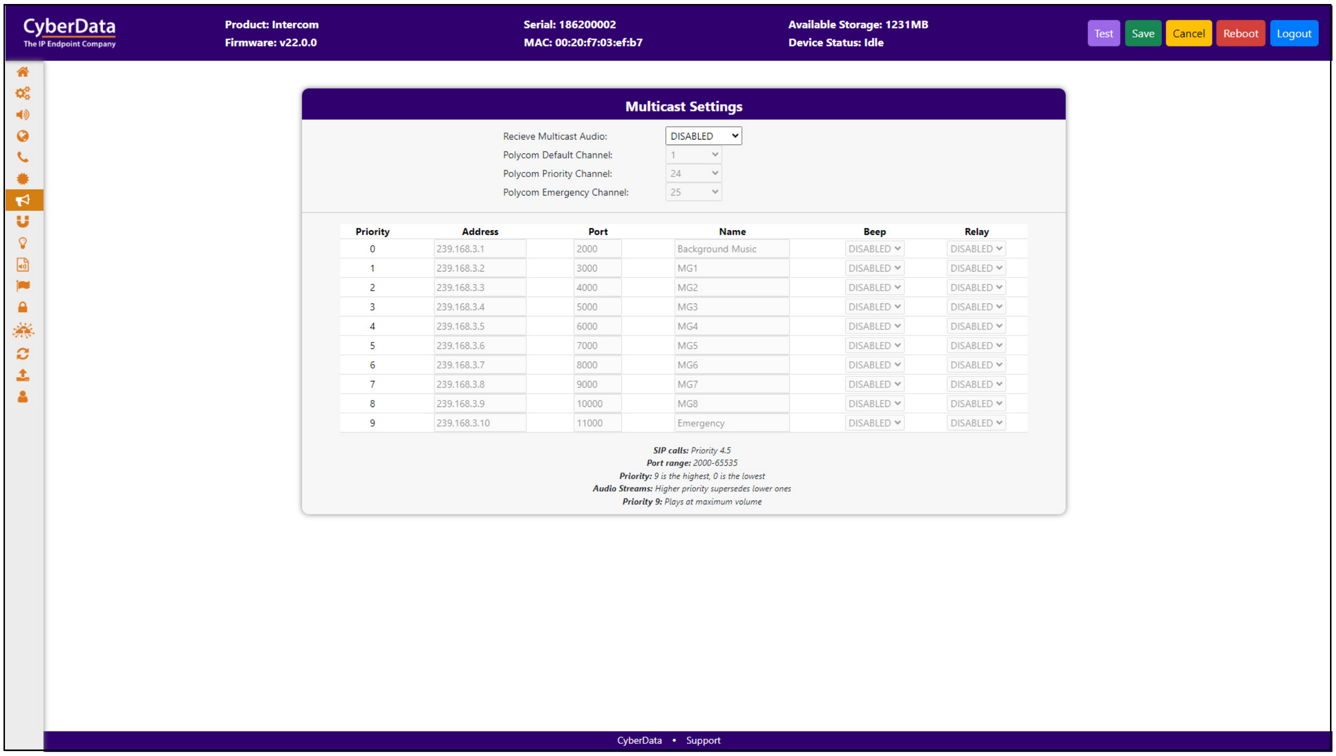
The Multicast Configuration page allows the device to join up to ten paging zones for receiving RTP audio streams. A paging zone can consist of one or many CyberData multicast group-enabled products. There is no limit to how many speakers can participate in a given paging zone. Each multicast group is 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. (I'm waiting to hear from Cameron) The device supports simultaneous SIP and Multicast. The device will prioritize simultaneous audio streams according to their priority in the list. If both SIP and Multicast is enabled, SIP audio streams are considered priority 4.5. SIP audio will interrupt multicast streams with priority 0 through 4 and will be interrupted by multicast streams with priority 5 through 9.

During priority 9 multicast streams, the volume is set to maximum. Ringtones all play at the same priority level. This means that it is possible to have a nightring tone and a normal ringtone playing at the same time.

To use Polycom Group Paging, configure a multicast group with the IP address and port number of the Polycom phone. The default is 224.0.1.116, port 5001, but can be configured through the phone. Polycom defaults to channels 1, 24, and 25, but can also be configured. The payload should be 20 ms and the codec G711mu.

Figure 1-16. Multicast Page



Product: Intercom
Firmware: v22.0.0
Serial: 186200002
MAC: 00:20:f7:03:ef:b7
Available Storage: 1231MB
Device Status: Idle

Multicast Settings

Recieve Multicast Audio: DISABLED
Polycom Default Channel: 1
Polycom Priority Channel: 24
Polycom Emergency Channel: 25

Priority	Address	Port	Name	Beep	Relay
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*

1.8 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.

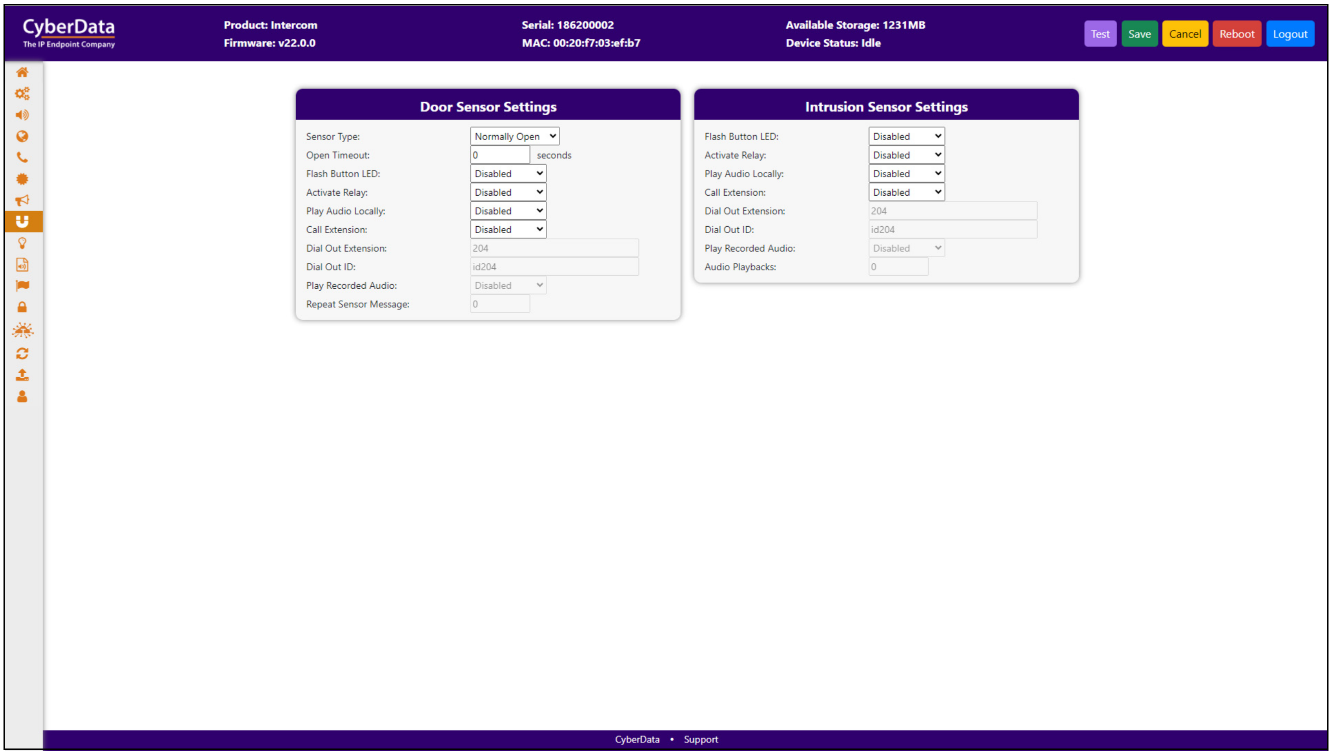
The intrusion sensor is an optical sensor installed on the Intercom board and will be activated when the Intercom is removed from the case.

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 1-17. Sensor Page



Product: Intercom
Firmware: v22.0.0
Serial: 186200002
MAC: 00:20:f7:03:ef:b7
Available Storage: 1231MB
Device Status: Idle

Door Sensor Settings

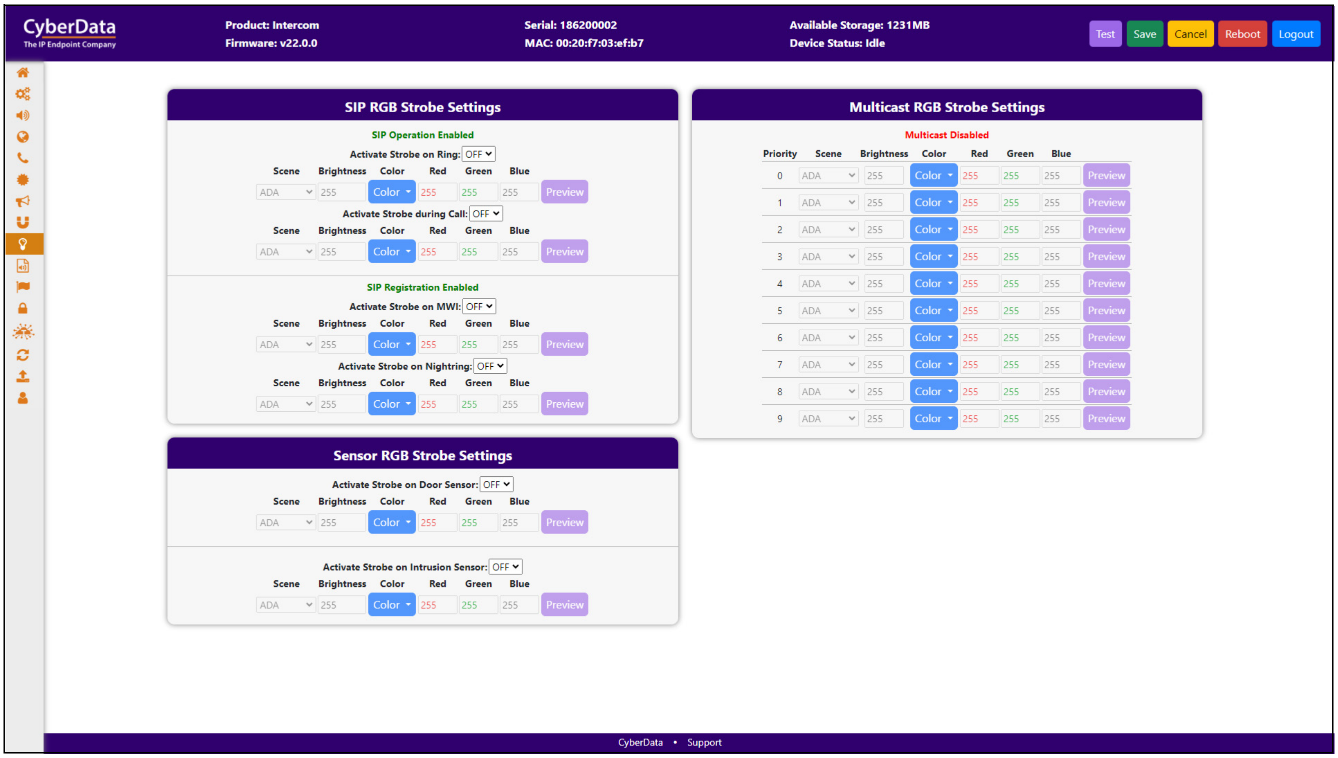
Sensor Type:	Normally Open
Open Timeout:	0 seconds
Flash Button LED:	Disabled
Activate Relay:	Disabled
Play Audio Locally:	Disabled
Call Extension:	Disabled
Dial Out Extension:	204
Dial Out ID:	id204
Play Recorded Audio:	Disabled
Repeat Sensor Message:	0

Intrusion Sensor Settings

Flash Button LED:	Disabled
Activate Relay:	Disabled
Play Audio Locally:	Disabled
Call Extension:	Disabled
Dial Out Extension:	204
Dial Out ID:	id204
Play Recorded Audio:	Disabled
Audio Playbacks:	0

1.9 Strobe

Figure 1-18. Strobe Page



Product: Intercom
Firmware: v22.0.0

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

Available Storage: 1231MB
Device Status: Idle

SIP RGB Strobe Settings

SIP Operation Enabled

Activate Strobe on Ring: OFF

Scene	Brightness	Color	Red	Green	Blue	
ADA	255	Color	255	255	255	Preview

Activate Strobe during Call: OFF

Scene	Brightness	Color	Red	Green	Blue	
ADA	255	Color	255	255	255	Preview

SIP Registration Enabled

Activate Strobe on MWI: OFF

Scene	Brightness	Color	Red	Green	Blue	
ADA	255	Color	255	255	255	Preview

Activate Strobe on Nightring: OFF

Scene	Brightness	Color	Red	Green	Blue	
ADA	255	Color	255	255	255	Preview

Sensor RGB Strobe Settings

Activate Strobe on Door Sensor: OFF

Scene	Brightness	Color	Red	Green	Blue	
ADA	255	Color	255	255	255	Preview

Activate Strobe on Intrusion Sensor: OFF

Scene	Brightness	Color	Red	Green	Blue	
ADA	255	Color	255	255	255	Preview

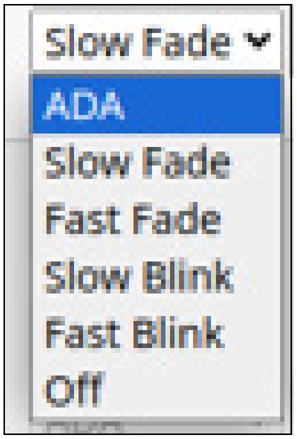
Multicast RGB Strobe Settings

Multicast Disabled

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

For each option, there are 5 scenes available:

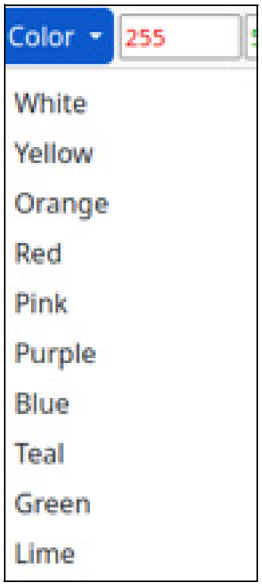
Figure 1-19. 5 Scenes Available



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

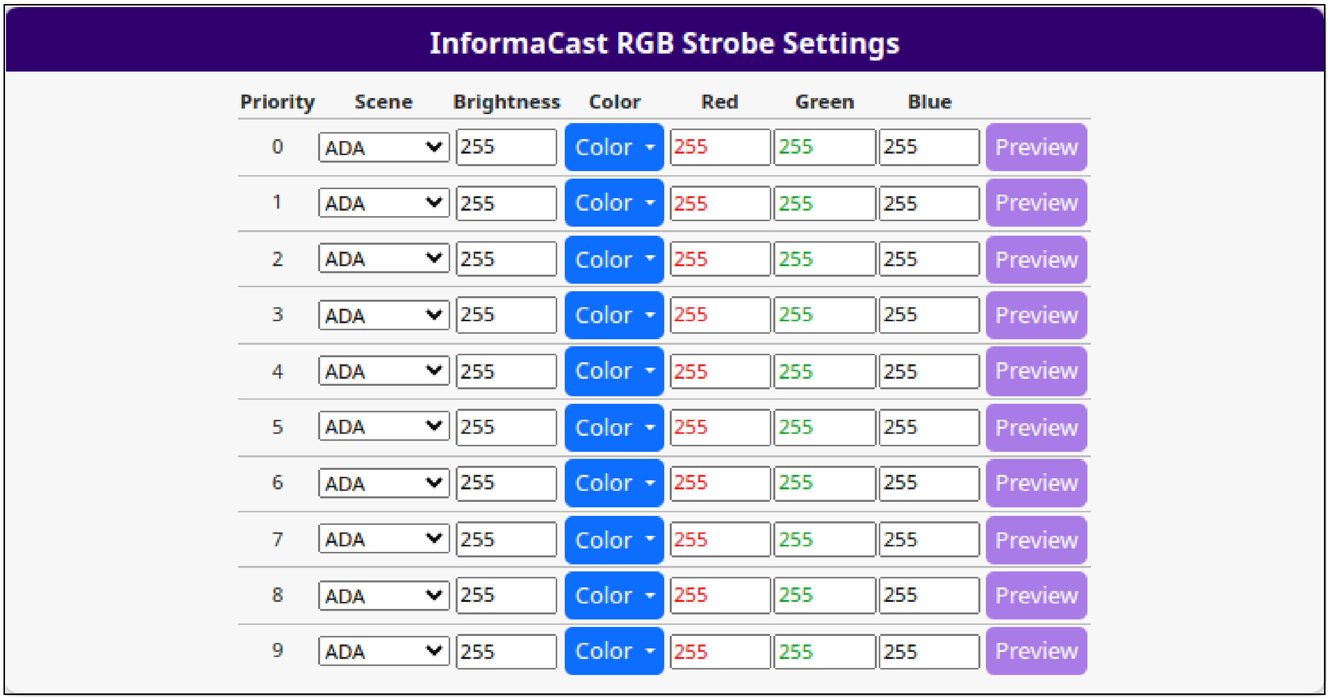
The ADA scene flashes white at maximum brightness (255). Other scenes can adjust the brightness, from 0 to 255.

Figure 1-20. 10 Colors



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

Figure 1-21. InformaCast enabled Device



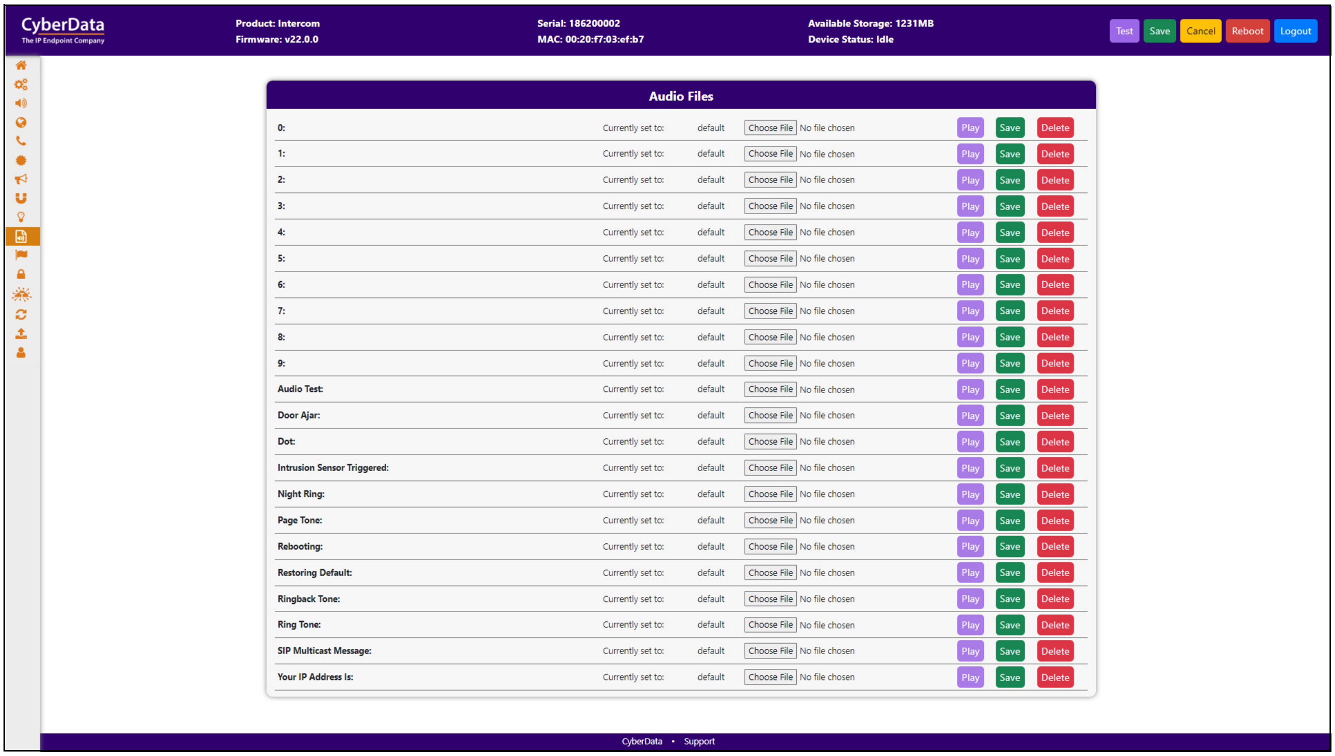
InformaCast RGB Strobe Settings

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

1.10 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 Intercom.

Figure 1-22. Audiofiles Page



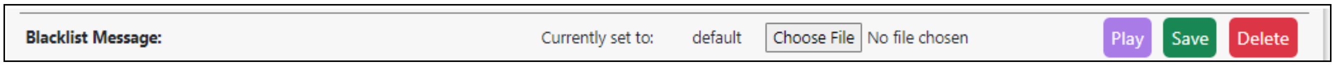
Product: Intercom
Firmware: v22.0.0
Serial: 186200002
MAC: 00:20:f7:03:ef:b7
Available Storage: 1231MB
Device Status: Idle

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
Door Ajar:	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
Intrusion Sensor Triggered:	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
Ringback Tone:	Currently set to:	default	Choose File No file chosen	Play Save Delete
Ring Tone:	Currently set to:	default	Choose File No file chosen	Play Save Delete
SIP Multicast Message:	Currently set to:	default	Choose File No file chosen	Play Save Delete
Your IP Address Is:	Currently set to:	default	Choose File No file chosen	Play Save Delete

Note The keypad also has the audio file “Blacklist message”: Figure 1-23.

Figure 1-23. Keypad audio file “Blacklist message”

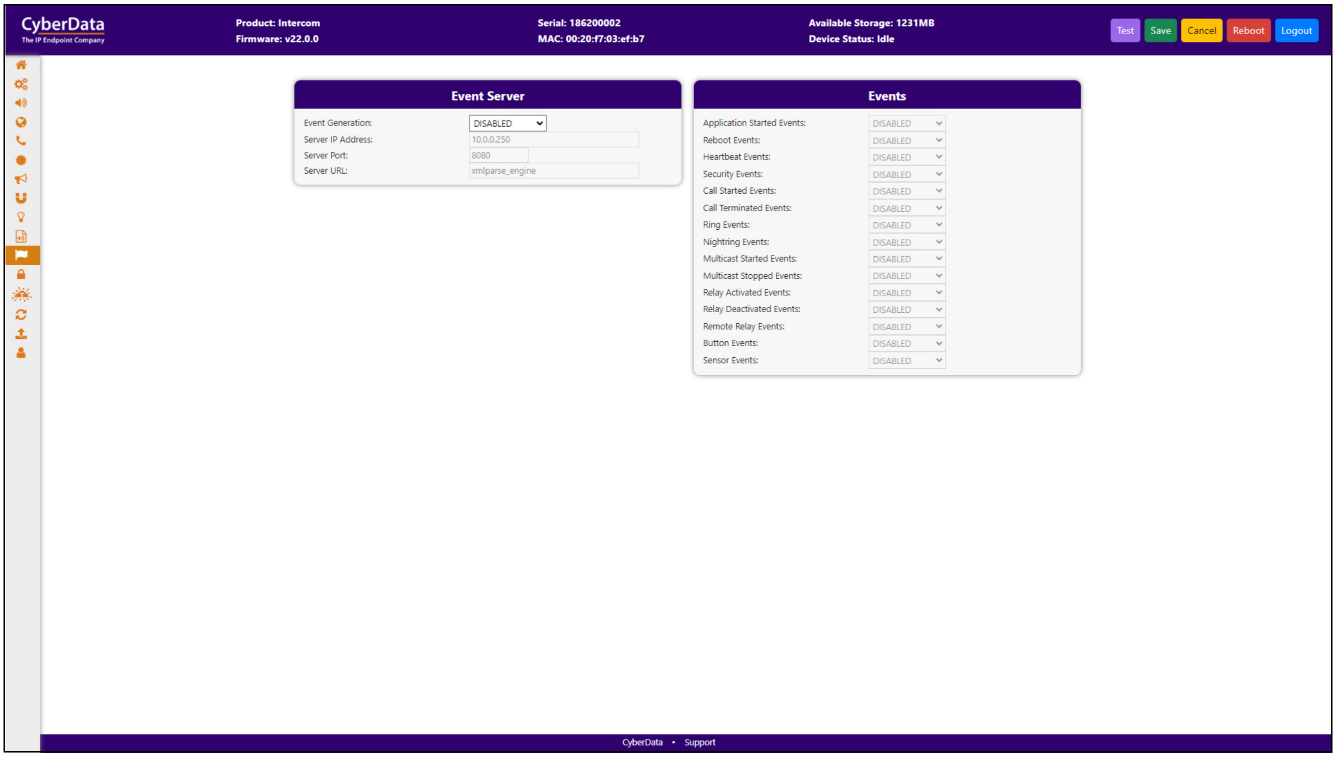


Blacklist Message:	Currently set to:	default	Choose File No file chosen	Play Save Delete

1.11 Events

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

Figure 1-24. Events Page



Product: Intercom
Firmware: v22.0.0

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

Available Storage: 1231MB
Device Status: Idle

Event Server

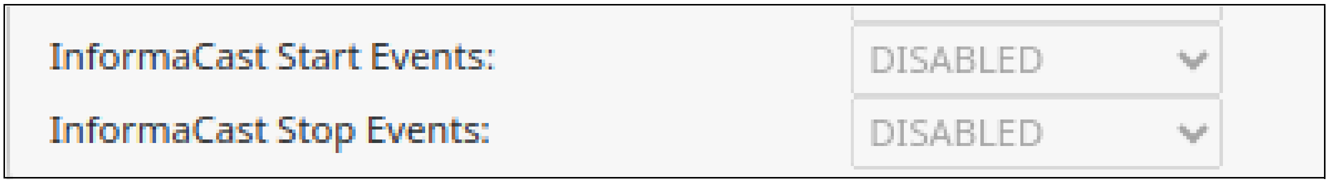
Event Generation:	DISABLED
Server IP Address:	10.0.0.250
Server Port:	8080
Server URL:	xmlparse_engine

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

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

Figure 1-25. InformaCast enabled Device



InformaCast Start Events:	DISABLED
InformaCast Stop Events:	DISABLED

1.11.1 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>
```

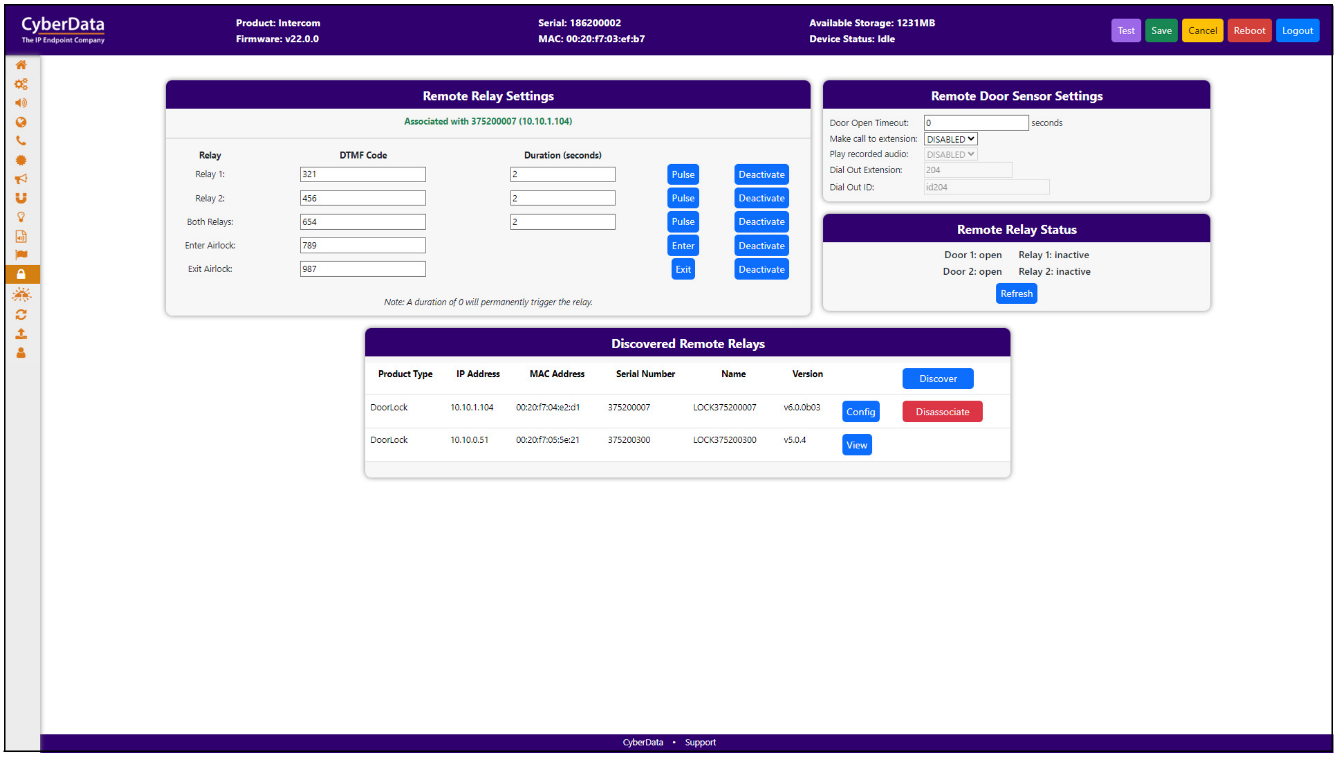
1.12 Door Strike Relay

When a Dual Door Strike Relay (DDSR) is associated with an intercom, the above web page appears. 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 1-26. Door Strike Relay Page (not associated with any DSRs)



Product: Intercom
Firmware: v22.0.0

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

Available Storage: 1231MB
Device Status: Idle

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: id204

Remote Relay Status

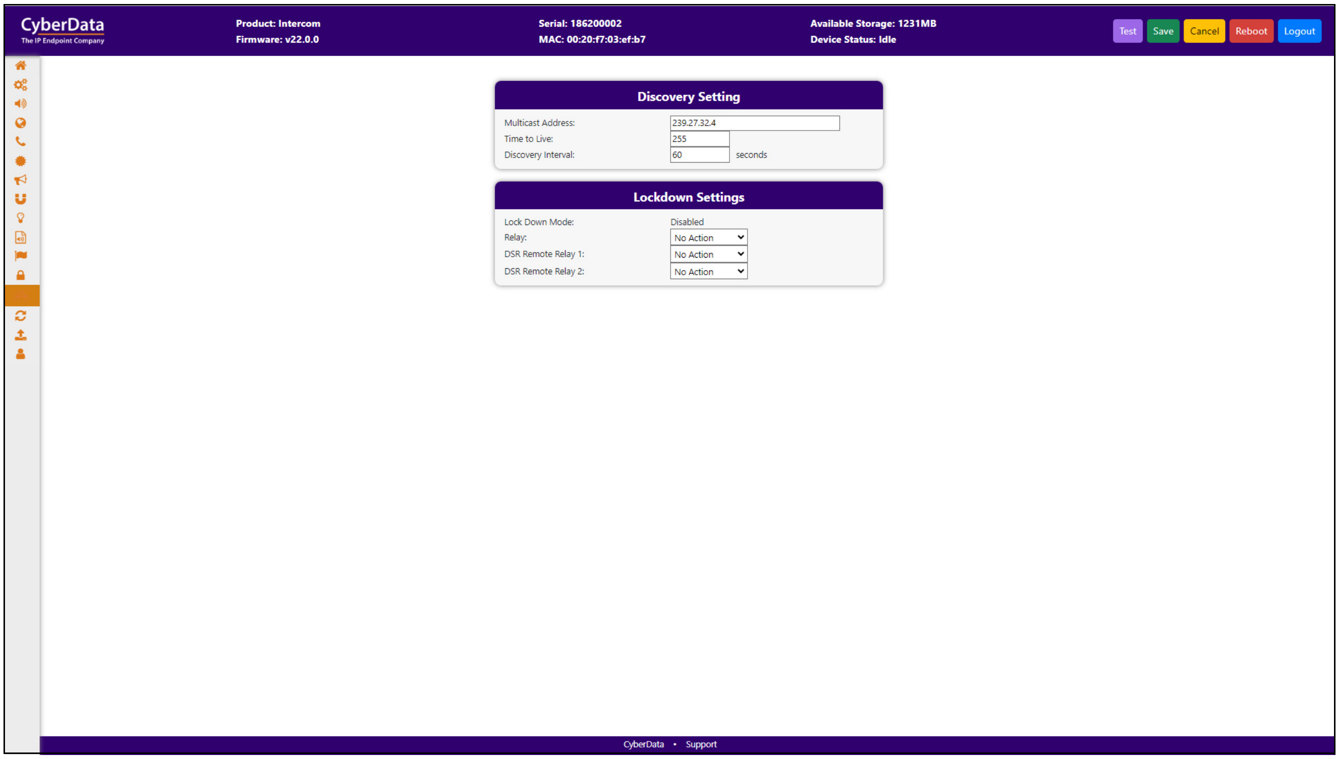
Door 1: open Relay 1: inactive
Door 2: open Relay 2: inactive

Discovered Remote Relays

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

1.13 Terminus

Figure 1-27. Terminus Page



Product: Intercom
Firmware: v22.0.0

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

Available Storage: 1231MB
Device Status: Idle

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

1.14 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..

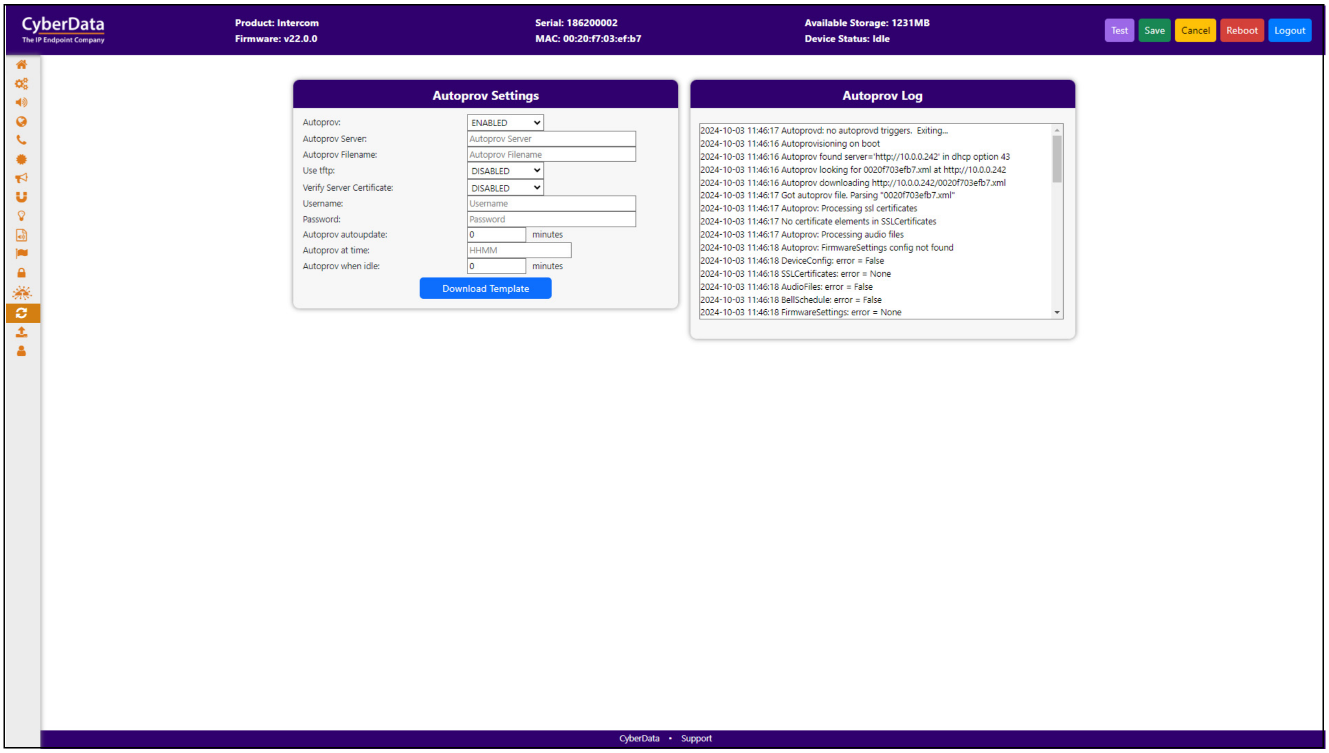
If a file is named, it will be downloaded instead of <mac address>,xml.

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 1-28. Autoprovisioning Page



Product: Intercom
Firmware: v22.0.0

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

Available Storage: 1231MB
Device Status: Idle

Autoprov Settings

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

Download Template

Autoprov Log

```
2024-10-03 11:46:17 Autoprovd: no autoprovd 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
```

1.15 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:

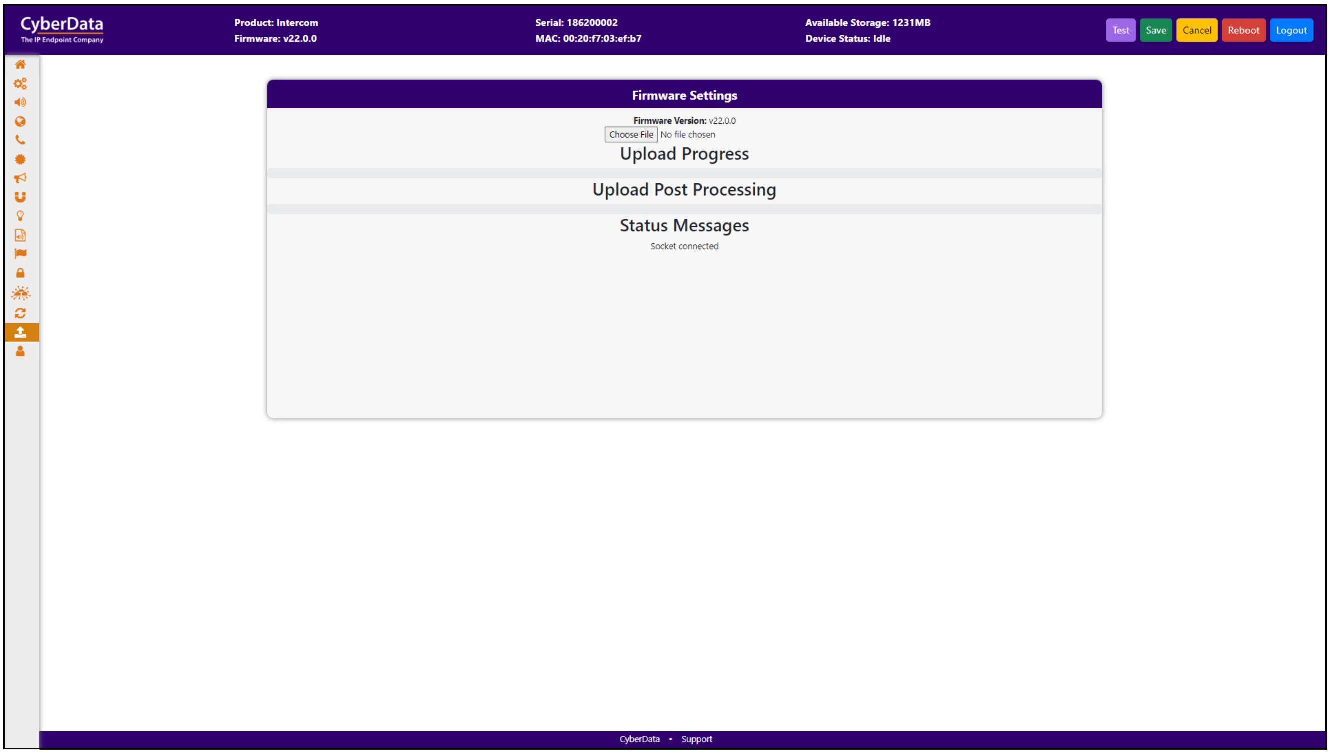
   https://www.cyberdata.net/collections/sip

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 1-29. Firmware Page



Product: Intercom
Firmware: v22.0.0

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

Available Storage: 1231MB
Device Status: Idle

Firmware Settings

Firmware Version: v22.0.0

No file chosen

Upload Progress

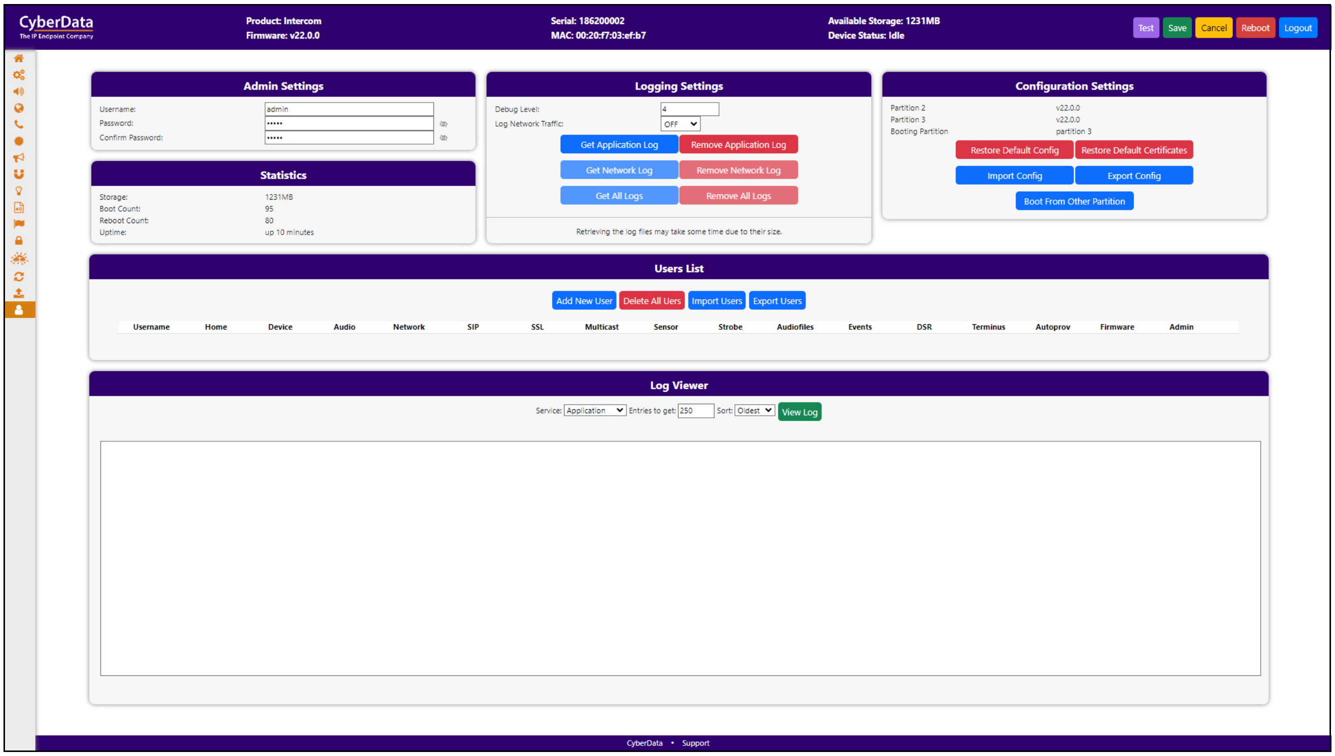
Upload Post Processing

Status Messages

Socket connected

1.16 Admin

Figure 1-30. Admin Page



Product: Intercom
Firmware: v22.0.0

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

Available Storage: 1231MB
Device Status: Idle

Admin Settings

Username:	admin
Password:	•••••
Confirm Password:	•••••

Statistics

Storage:	1231MB
Boot Count:	95
Reboot Count:	80
Uptime:	up 10 minutes

Logging Settings

Debug Level:	4
Log Network Traffic:	OFF

Retrieving the log files may take some time due to their size.

Configuration Settings

Partition 2	v22.0.0
Partition 3	v22.0.0
Booting Partition	partition 3

Users List

Username	Home	Device	Audio	Network	SIP	SSL	Multicast	Sensor	Strobe	Audiofiles	Events	DSR	Terminus	Autoprov	Firmware	Admin

Log Viewer

Service: Application Entries to get: 250 Sort: Oldest

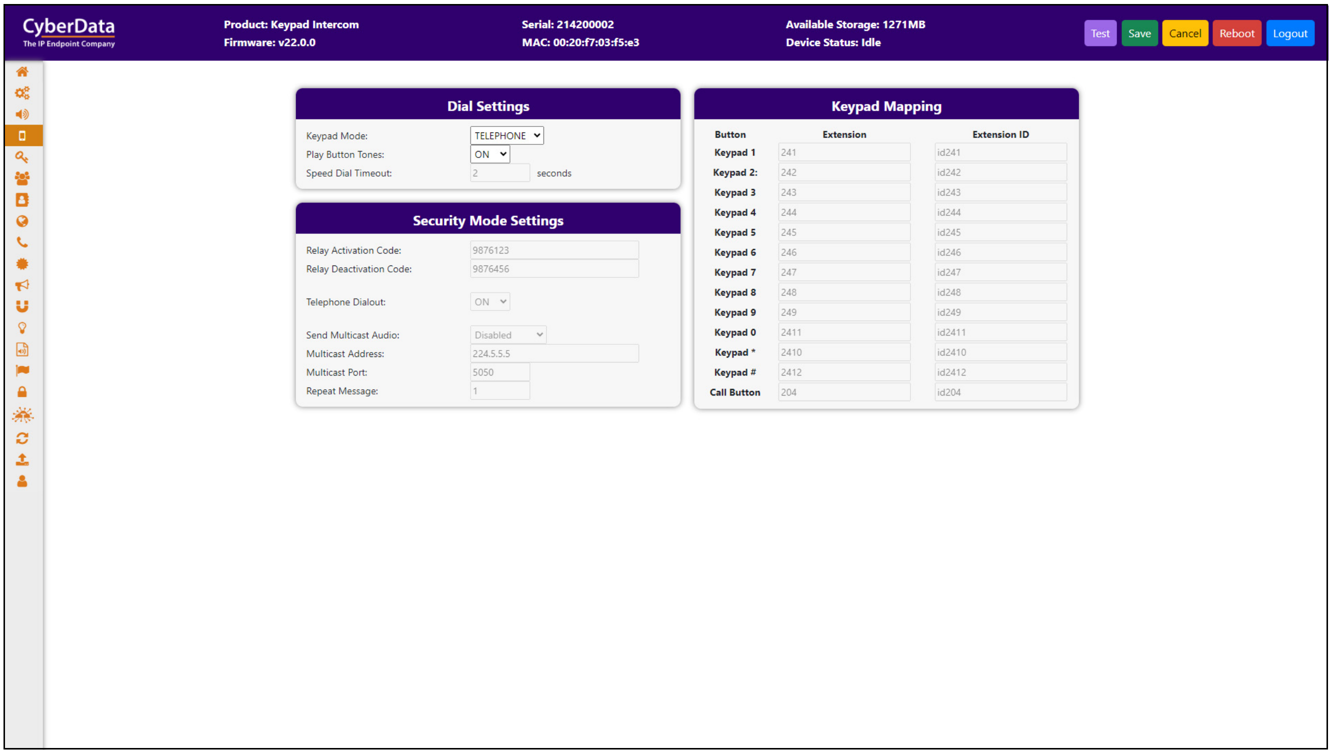
The administrator uses the Users List to create new accounts, assigning user names and passwords, and granting access to specific web pages.

1.17 Keypad Pages

1.17.1 Buttons

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

Figure 1-31. Buttons Page



Product: Keypad Intercom
Firmware: v22.0.0
Serial: 214200002
MAC: 00:20:f7:03:f5:e3
Available Storage: 1271MB
Device Status: Idle

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

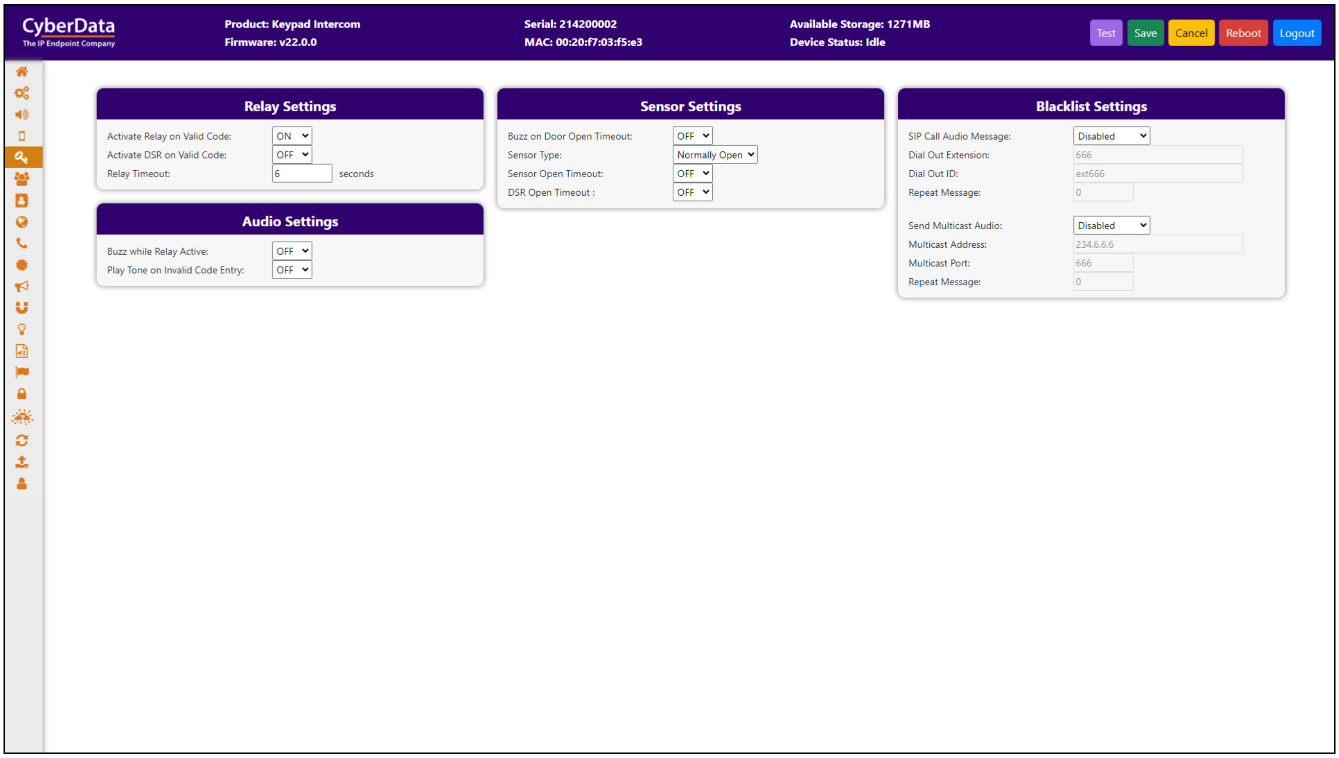
Keypad Mapping

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

1.17.2 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 1-32. Security Page



Product: Keypad Intercom
Firmware: v22.0.0
Serial: 214200002
MAC: 00:20:f7:03:f5:e3
Available Storage: 1271MB
Device Status: Idle

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

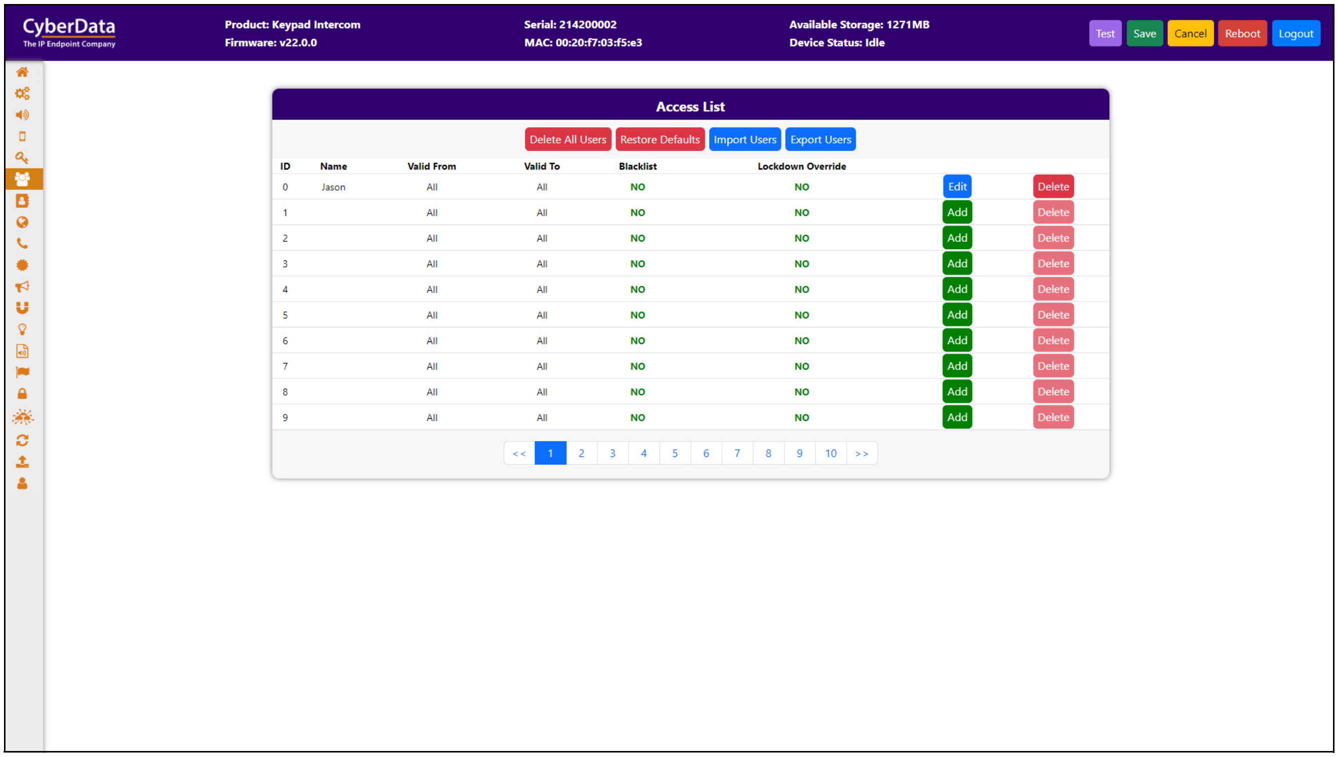
Blacklist Settings

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

1.17.3 Access List

Figure 1-33. Access List Page



Product: Keypad Intercom
Firmware: v22.0.0
Serial: 214200002
MAC: 00:20:f7:03:f5:e3
Available Storage: 1271MB
Device Status: Idle

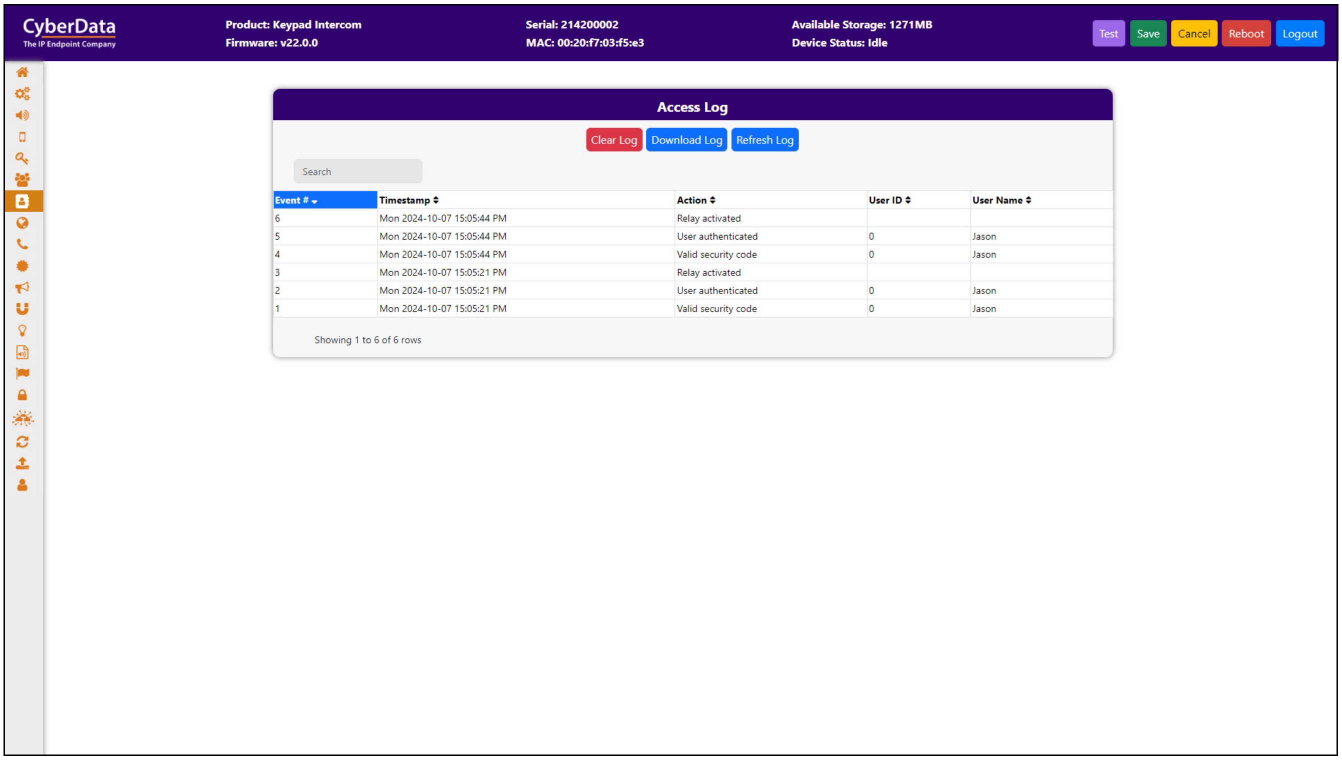
Access List

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

1.17.4 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 1-34. Access Log Page



Product: Keypad Intercom
Firmware: v22.0.0

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

Available Storage: 1271MB
Device Status: Idle

Event # ▾	Timestamp ⇕	Action ⇕	User ID ⇕	User Name ⇕
6	Mon 2024-10-07 15:05:44 PM	Relay activated		
5	Mon 2024-10-07 15:05:44 PM	User authenticated	0	Jason
4	Mon 2024-10-07 15:05:44 PM	Valid security code	0	Jason
3	Mon 2024-10-07 15:05:21 PM	Relay activated		
2	Mon 2024-10-07 15:05:21 PM	User authenticated	0	Jason
1	Mon 2024-10-07 15:05:21 PM	Valid security code	0	Jason

Showing 1 to 6 of 6 rows

1.18 Command Interface

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

1.18.1 Command Interface Post Commands

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

Table 1-1. 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 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