CyberData
The IP Endpoint Company

SIP Call Button
Operations Guide

Part #*011049, 011491*

Document Part #*932062A*
for Firmware Version *22.0.0*

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

SIP Call Button Operations Guide 932062A
Part # 011049, 011491

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 932062A, which corresponds to firmware version 22.0.0, 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 SIP Call Button 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

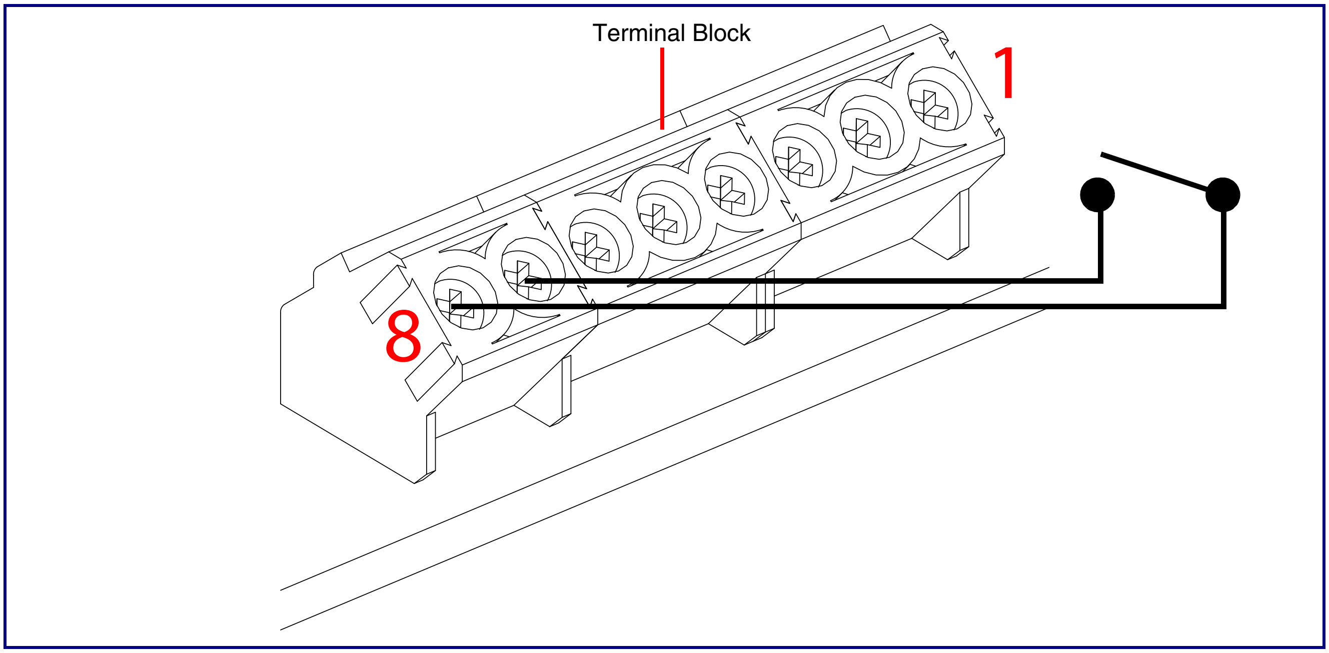
Contents

1 Installing the SIP Call Button

1.1 Remote Switch Connection

Wiring pins 7 and 8 of the terminal block to a switch will initiate a SIP call when the switch is closed. The call will go to the extension specified as the dial out extension on the **SIP** page.

Figure 1-1. Remote Switch Connection



1.1.1 Using the On-Board Relay

⚠ 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:* The relay contacts are dry and provided for a normally open and momentarily closed configuration. Neither the alternate power input nor PoE power can be used to drive a door strike.

⚠ GENERAL ALERT	**Warning** *Electrical Hazard:* The relay does not support AC powered door strikes. Any use of this relay beyond its normal operating range can cause damage to the product and is not covered under our warranty policy.

The device has a built-in relay that can be activated by a web configurable DTMF string that can be received from a VoIP phone supporting out of band (RFC2833) DTMF as well as a number of other triggering events. See the **Device Page** on the web interface for relay settings.

This relay can be used to trigger low current devices like LED strobes and security camera input signals as long as the load is not an inductive type and the relay is limited to a maximum of 1 Amp @ 30 VDC. Inductive loads can cause excessive “hum” and can interfere with or damage the unit’s electronics.

We highly recommend that inductive load and high current devices use our Network Dual Door Strike Relay (CD# 011375) (see Section 1.2.2, "Network Dual Door Strike Relay Wiring Diagram with External Power Source").

This relay interface also has a general purpose input port that can be used to monitor an external switch and generate an event.

For more information on the sensor options, see the **Sensor Page** on the web interface.

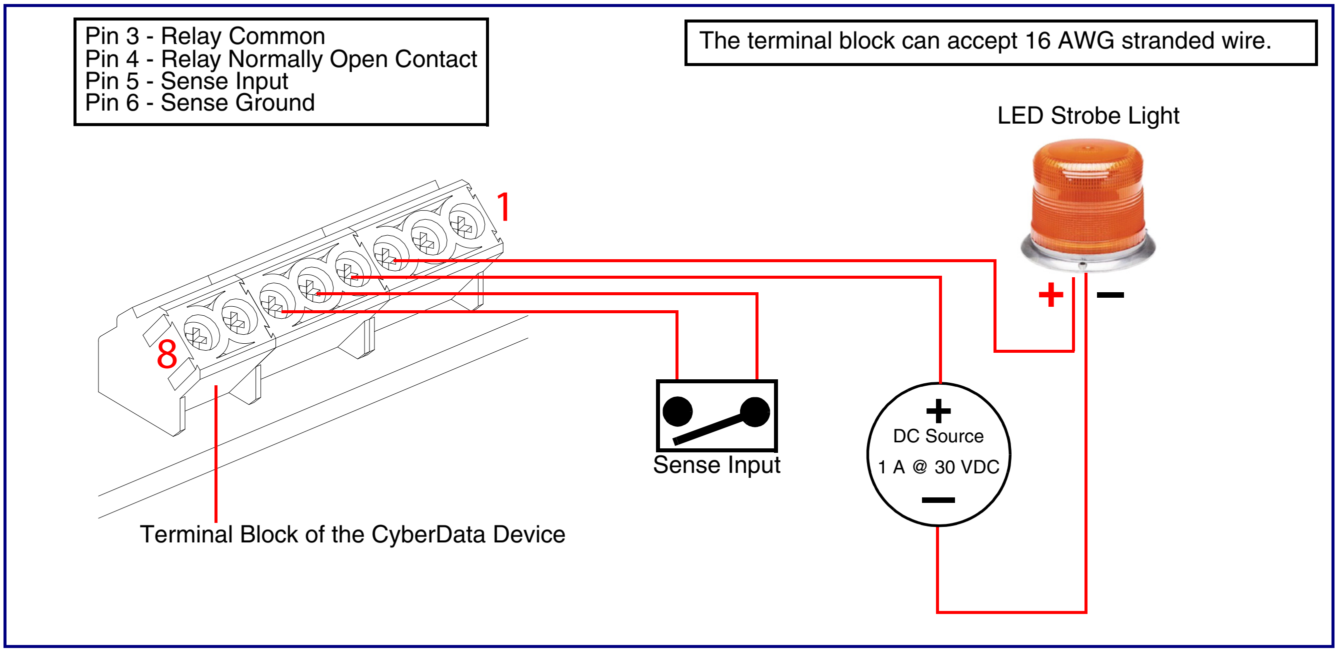
1.2 Wiring the Circuit

1.2.1 Devices Less than 1A at 30 VDC

If the power for the device is less than 1A at 30 VDC and is not an inductive load, then see Figure 1-2 for the wiring diagram.

When configuring with an inductive load, please use an intermediary relay with a High PIV Ultrafast Switching Diode. We recommend using the Network Dual Door Strike Relay (CD# 011375) (see Section 1.2.2, "Network Dual Door Strike Relay Wiring Diagram with External Power Source").

Figure 1-2. Devices Less than 1A at 30 VDC


Pin 3 - Relay Common
Pin 4 - Relay Normally Open Contact
Pin 5 - Sense Input
Pin 6 - Sense Ground
The terminal block can accept 16 AWG stranded wire.
LED Strobe Light
1
8
+
−
Sense Input
+
DC Source
1 A @ 30 VDC
−
Terminal Block of the CyberData Device

1.2.2 Network Dual Door Strike Relay Wiring Diagram with External Power Source

For wiring an electronic door strike to work over a network, we recommend the use of our external Network Dual Door Strike Relay (CD# 011375).

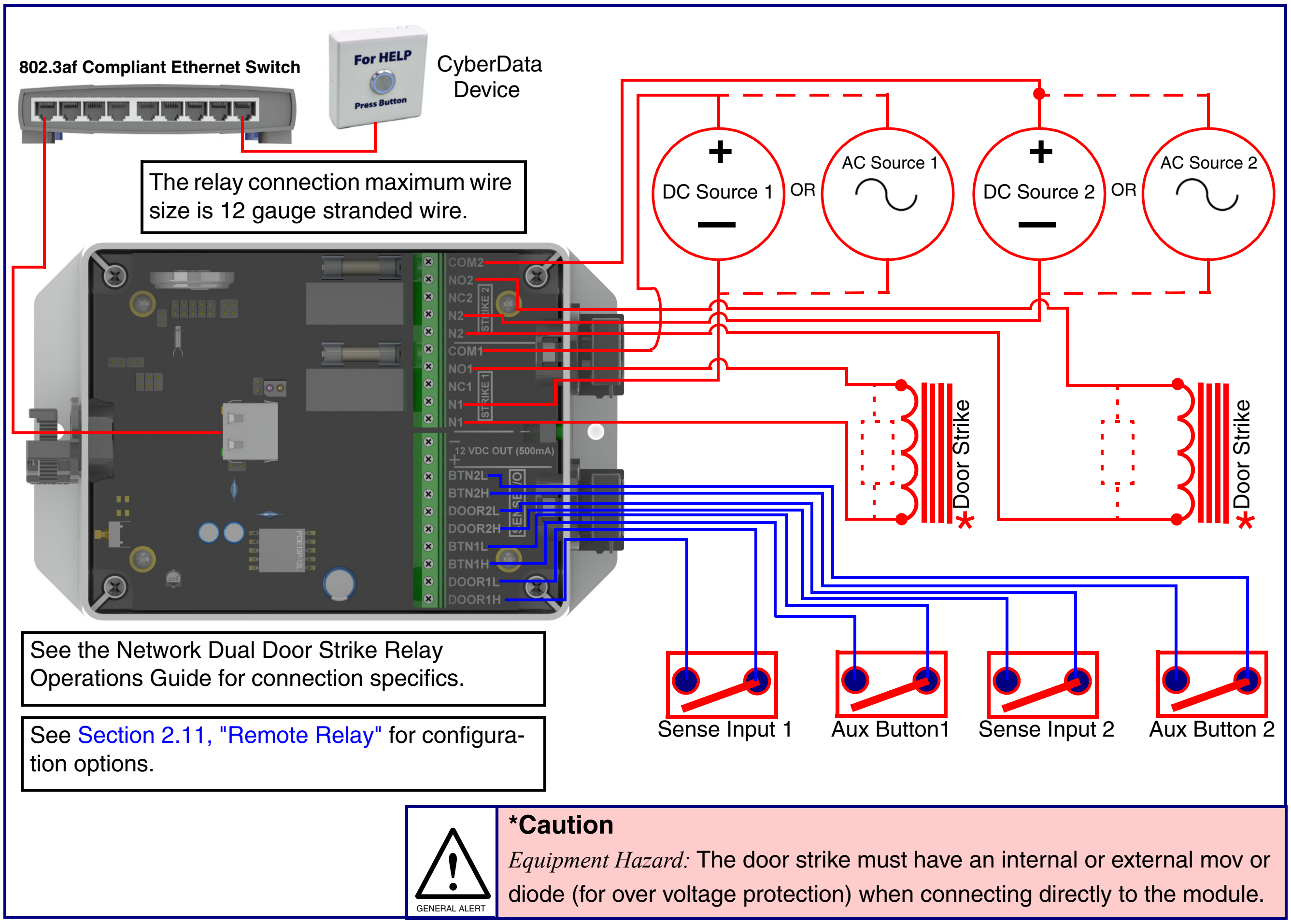
This product provides an easier method of connecting standard door strikes as well as AC and higher voltage devices. See Figure 1-3 and Figure 1-4 for the wiring diagrams.

GENERAL ALERT

Warning

Electrical Hazard: Hazardous voltages may be present. No user serviceable part inside. Refer to qualified service personnel for connecting or servicing.

Figure 1-3. Network Dual Door Strike Relay Wiring Diagram with External Power Source



The relay connection maximum wire size is 12 gauge stranded wire.

See the Network Dual Door Strike Relay Operations Guide for connection specifics.

See Section 2.11, "Remote Relay" for configuration options.

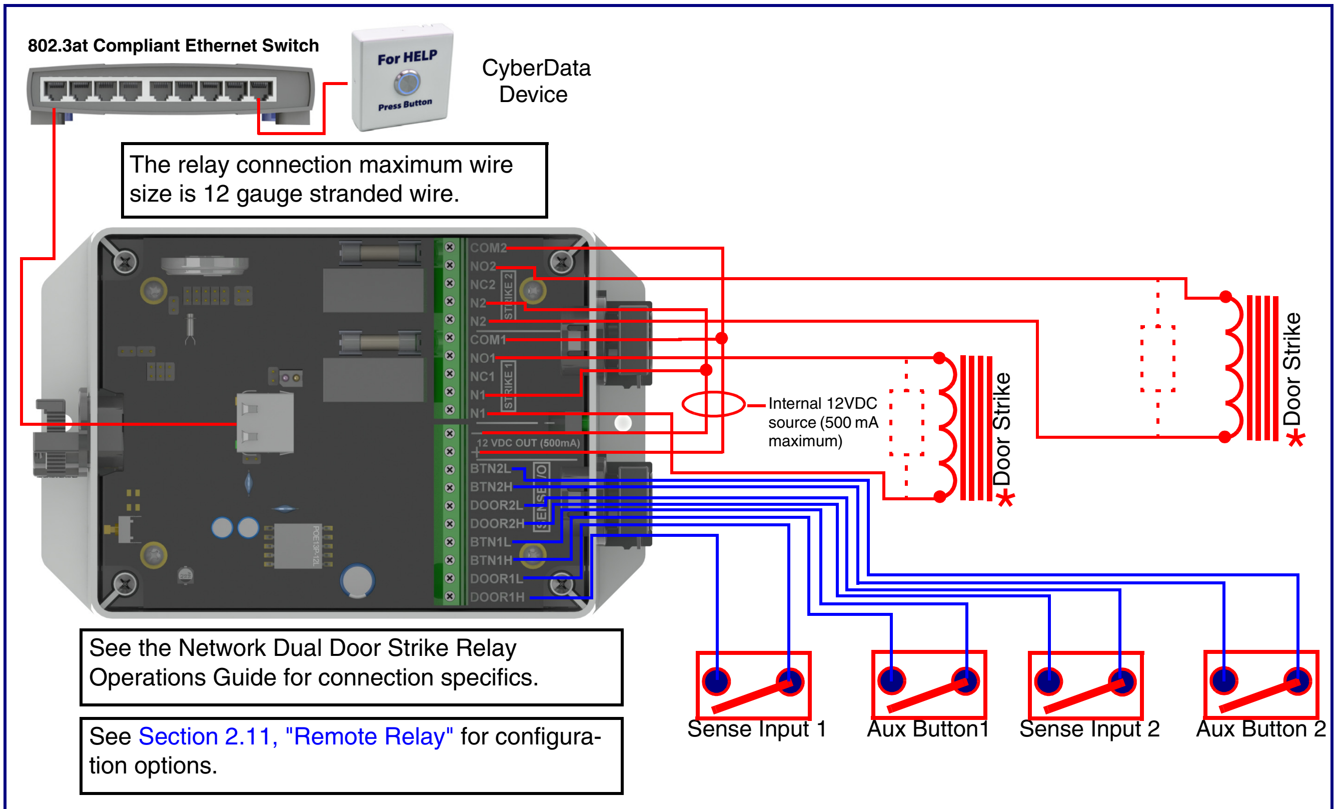
GENERAL ALERT

***Caution**

Equipment Hazard: The door strike must have an internal or external mov or diode (for over voltage protection) when connecting directly to the module.

1.2.3 Network Dual Door Strike Relay Wiring Diagram Using PoE+

Figure 1-4. Network Dual Door Strike Relay Wiring Diagram Using PoE+



The relay connection maximum wire size is 12 gauge stranded wire.

See the Network Dual Door Strike Relay Operations Guide for connection specifics.

See Section 2.11, "Remote Relay" for configuration options.

GENERAL ALERT

***Caution**

Equipment Hazard: The door strike must have an internal or external mov or diode (for over voltage protection) when connecting directly to the module.

If you have questions about connecting door strikes or setting up the web configurable options, please contact our support department at the following website:

https://support.cyberdata.net/

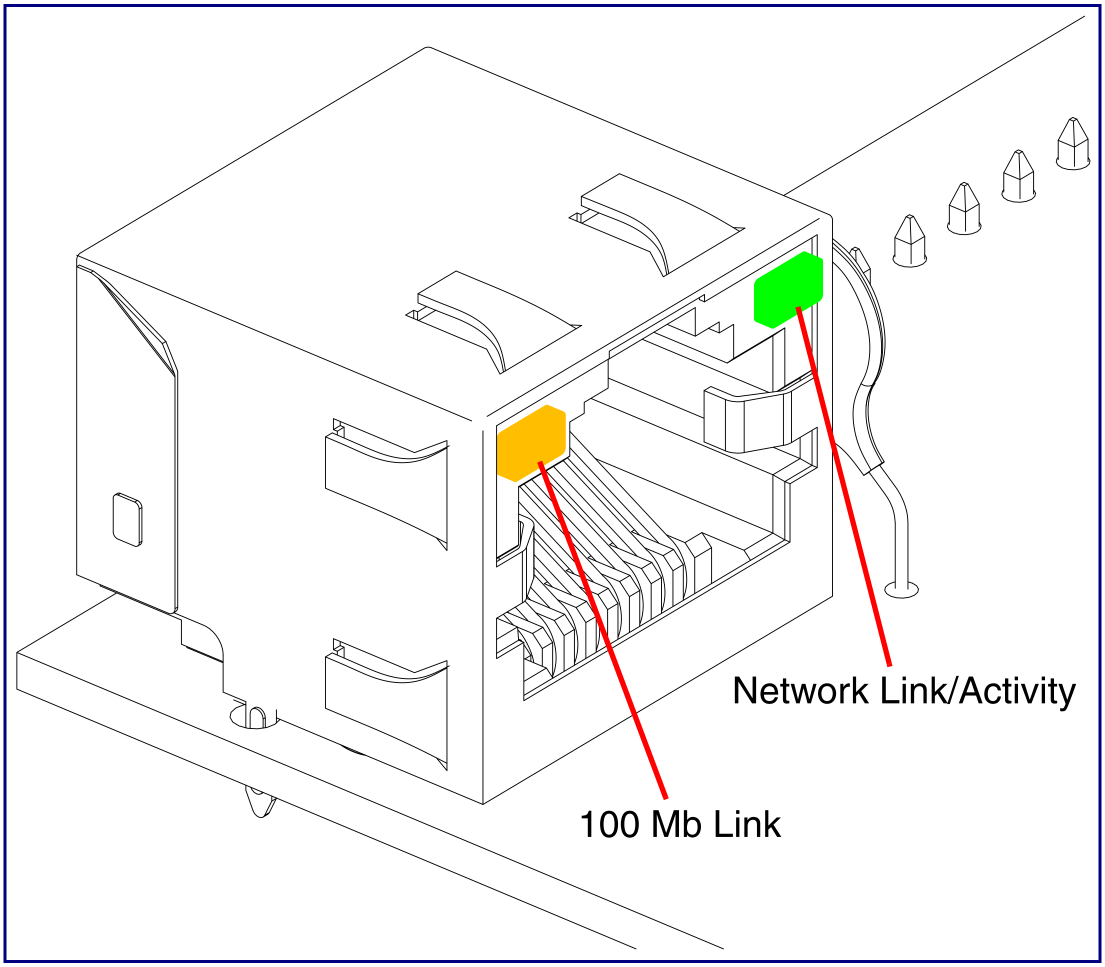
1.3 Activity and Link LEDs

1.3.1 Verifying the Network Connectivity and Data Rate

When you plug in the Ethernet cable or power supply to the Intercom, the following occurs:

- The square, **GREEN Network Link/Activity** LED blinks when there is network activity (see Figure 1-5).
- The square, **AMBER 100 Mb Link** LED above the Ethernet port indicates that the network 100 Mb connection has been established (see Figure 1-5).

Figure 1-5. Activity and Link LED



1.4 Call Button and the Call Button LED

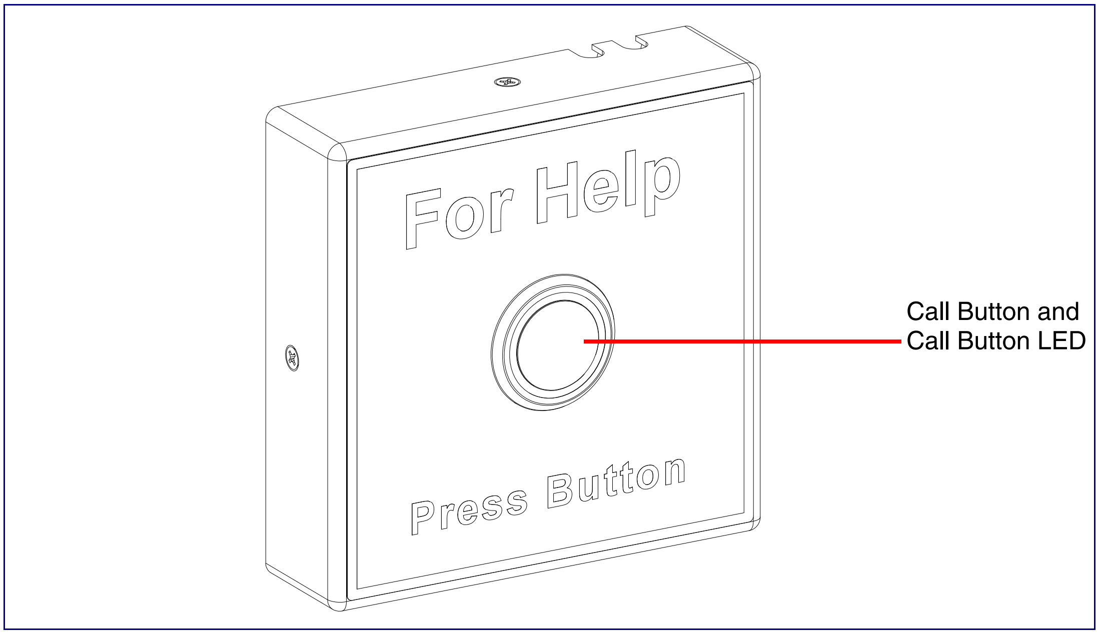
1.4.1 Calling with the The Call Button

- You may initiate a call by pressing the Call Button.
- An active call is indicated by the Call Button LED blinking at one second intervals.
- The device automatically answers an incoming call.
- You can press the Call Button to terminate an active call.

1.4.2 Call Button LED Function

- Upon initial power or reset, the Call Button LED will illuminate.
- On boot, the Call Button LED will flash ten times a second while setting up the network and downloading autoprovisioning files.
- The device “autoprovisions” by default, and the initial process may take several minutes as the device searches for and downloads updates. The Call Button LED will blink during this process. During the initial provisioning, or after the factory defaults have been reset, the device may download firmware twice. The device will blink, remain solid for 10 to 20 seconds, and then resume blinking. This process will take longer if there are many audio files downloading.
- When the software has finished initialization, the Call Button LED will blink twice.
- When a call is established (not just ringing), the Call Button LED will blink.
- On the **Device Page** (see Section 2.3, "Device"), there is an option called **Button Lit When Idle**. This option sets the normal state for the indicator LED. The Call Button LED will still blink during initialization and calls.
- The Call Button LED flashes briefly at the beginning of RTFM mode.

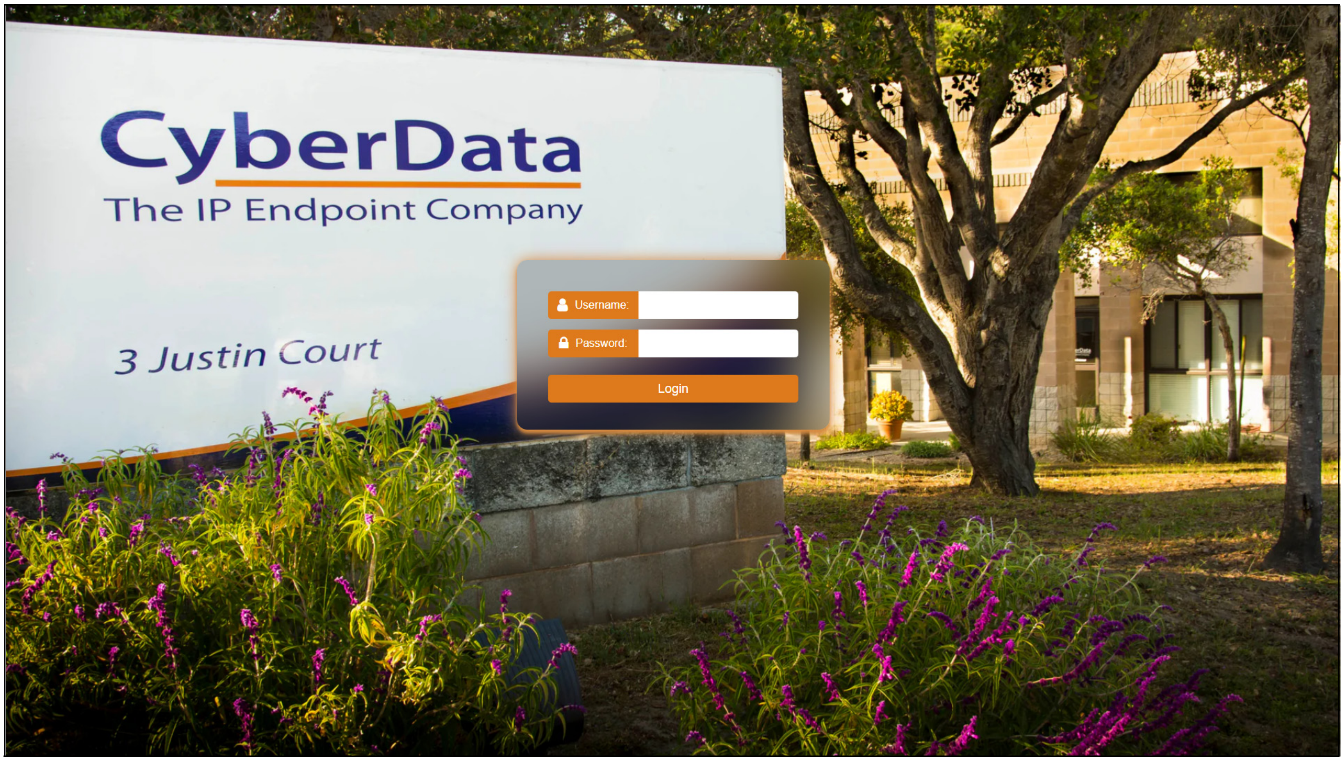
Figure 1-6. Call Button and Call Button LED



2 Configure the Device

2.1 Home Page

Figure 2-1. Log In Page



1. Open your browser to the SIP Call Button 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 SIP Call Button.

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

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

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

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

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

   Web Access Username: **admin**

   Web Access Password: **admin**

2.2 Restoring Defaults

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

Holding the RTFM button (Figure 2-2), for approximately five seconds restores the device to its factory defaults (Table 2-1), defaulting to DHCP to obtain an IP address, or using 192.168.1.23 if a DHCP server is not present.

Figure 2-2. RTFM Button (SW1)

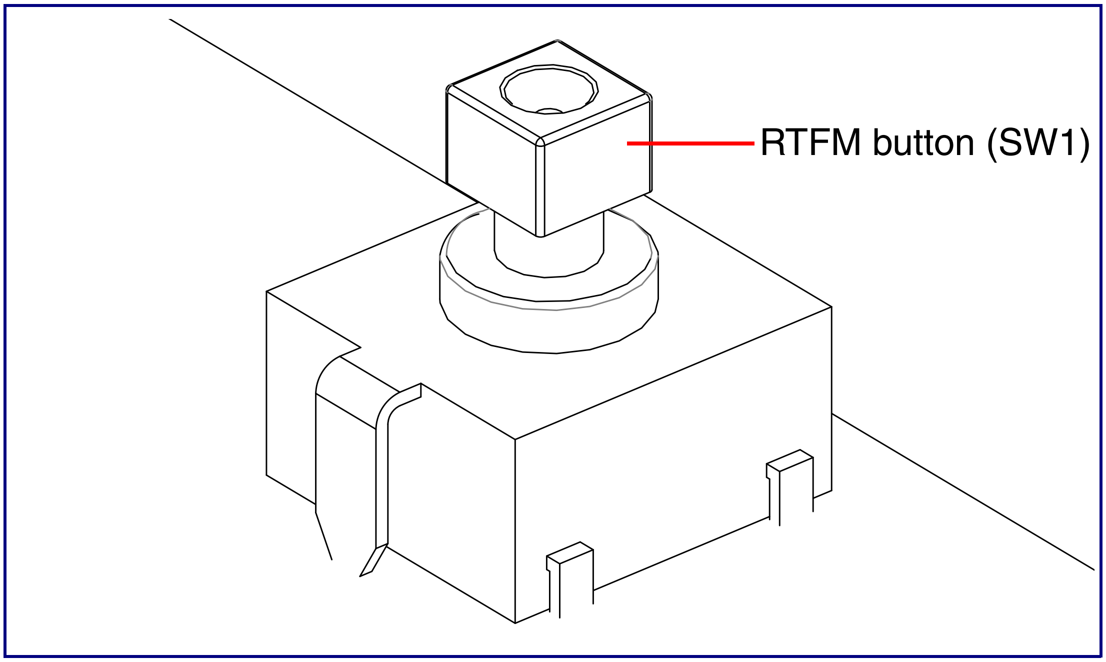
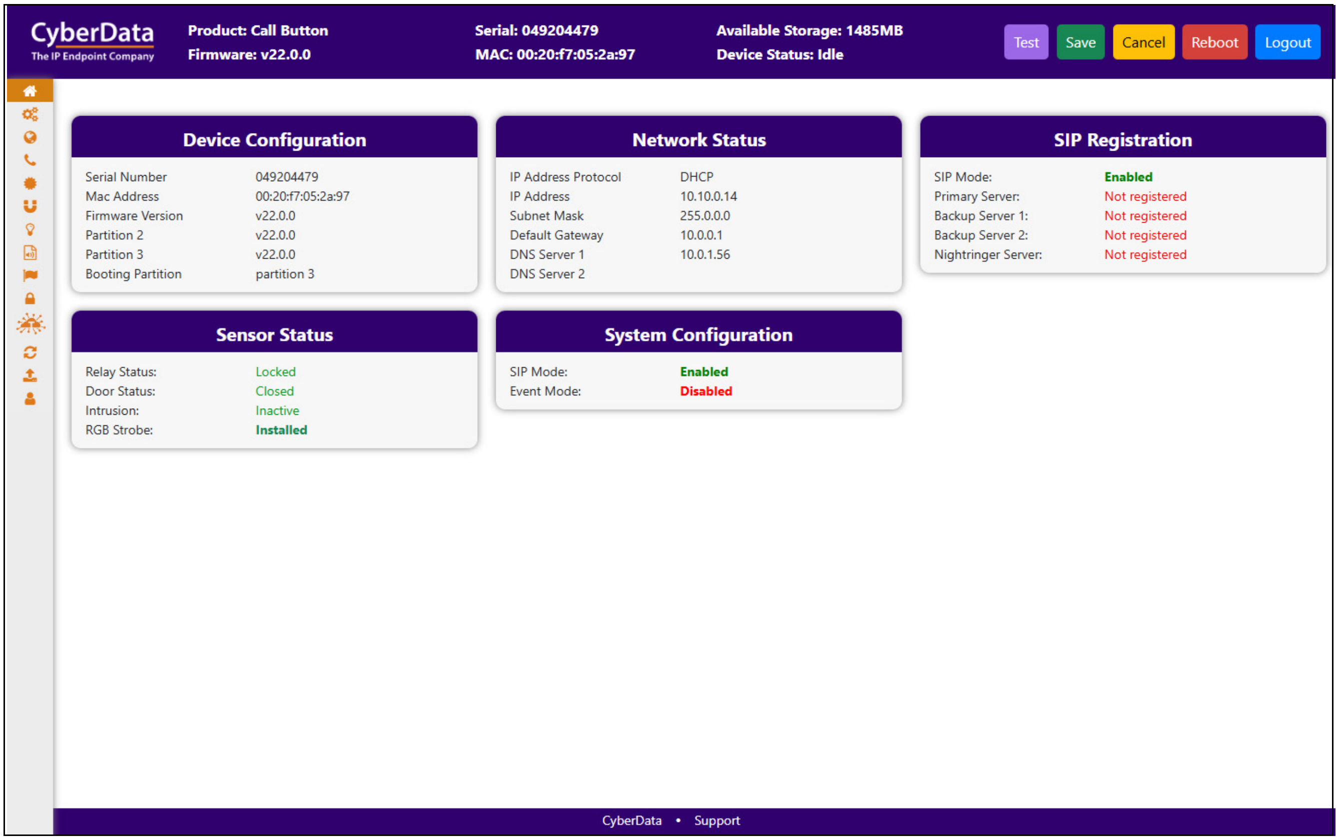


Table 2-1. Factory Default Settings

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.

Figure 2-3. Home Page



Product: Call Button
Firmware: v22.0.0

Serial: 049204479
MAC: 00:20:f7:05:2a:97

Available Storage: 1485MB
Device Status: Idle

Device Configuration

Serial Number	049204479
Mac Address	00:20:f7:05:2a:97
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	10.10.0.14
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

Sensor Status

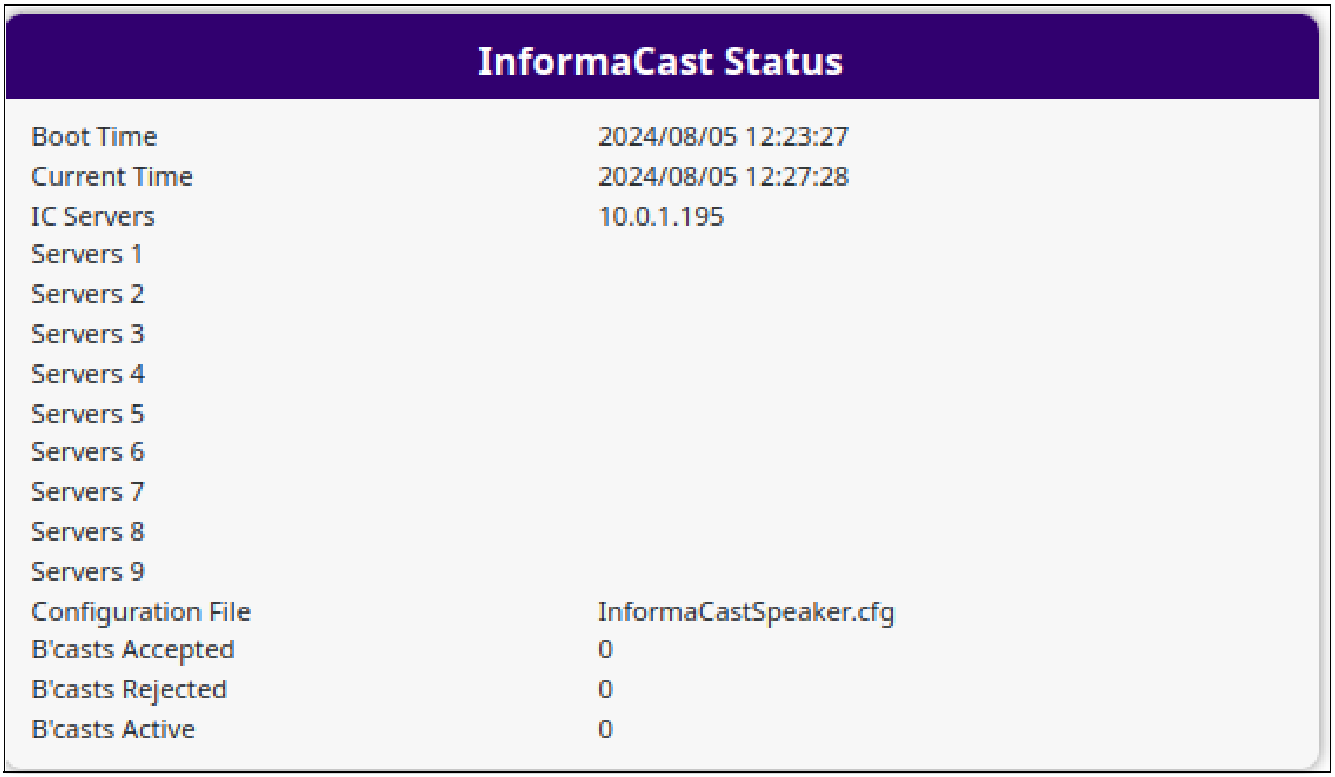
Relay Status:	Locked
Door Status:	Closed
Intrusion:	Inactive
RGB Strobe:	Installed

System Configuration

SIP Mode:	Enabled
Event Mode:	Disabled

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

Figure 2-4. InformaCast enabled Device

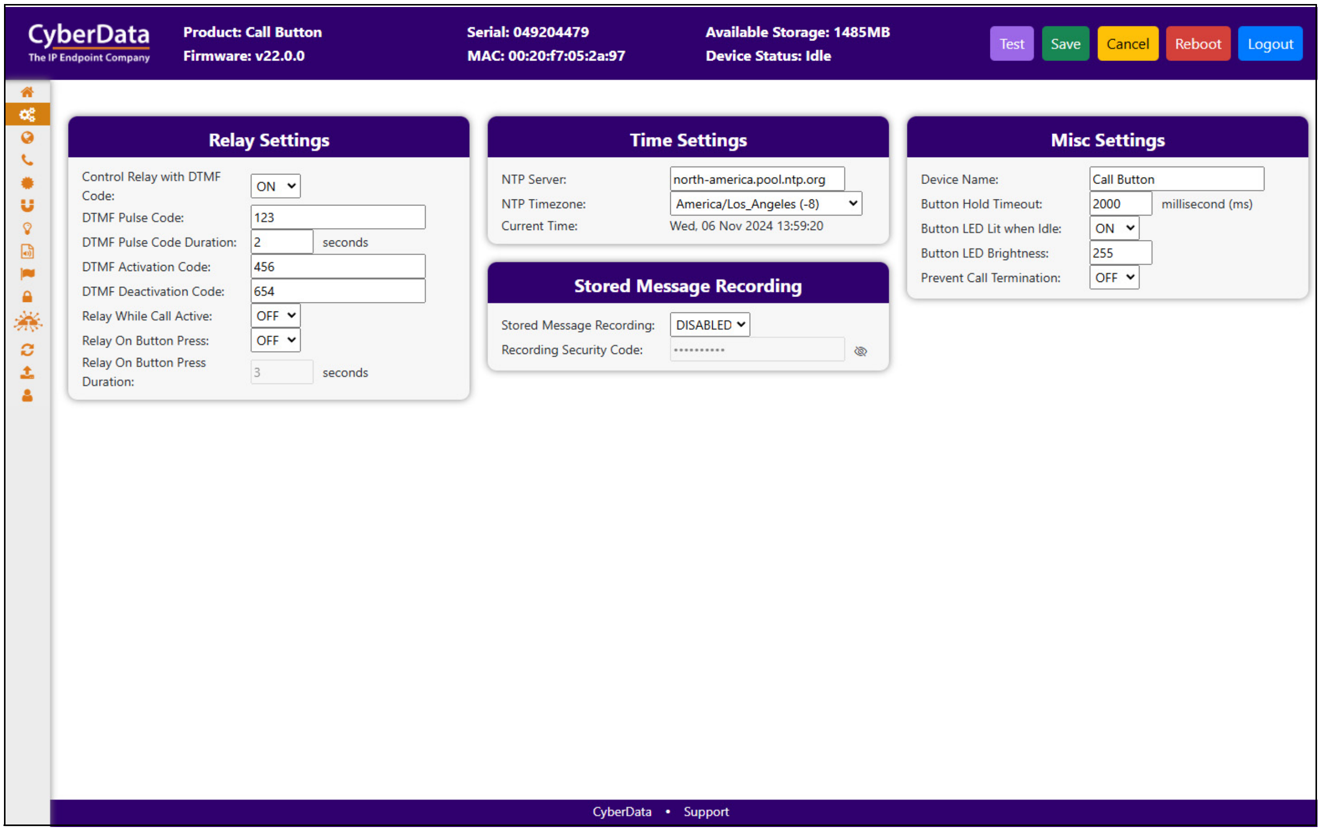


InformaCast Status

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

2.3 Device

Figure 2-5. Device Page



Product: Call Button
Firmware: v22.0.0
Serial: 049204479
MAC: 00:20:f7:05:2a:97
Available Storage: 1485MB
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
Relay While Call Active: OFF
Relay On Button Press: OFF
Relay On Button Press Duration: 3 seconds

Time Settings

NTP Server: north-america.pool.ntp.org
NTP Timezone: America/Los_Angeles (-8)
Current Time: Wed, 06 Nov 2024 13:59:20

Stored Message Recording

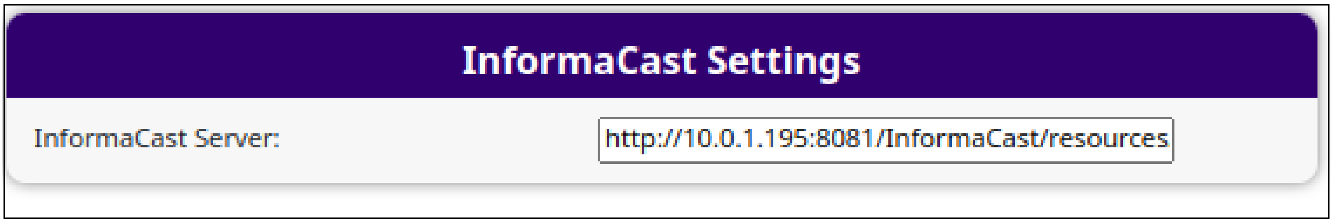
Stored Message Recording: DISABLED
Recording Security Code: ••••••••••

Misc Settings

Device Name: Call Button
Button Hold Timeout: 2000 millisecond (ms)
Button LED Lit when Idle: ON
Button LED Brightness: 255
Prevent Call Termination: OFF

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

Figure 2-6. InformaCast enabled Device

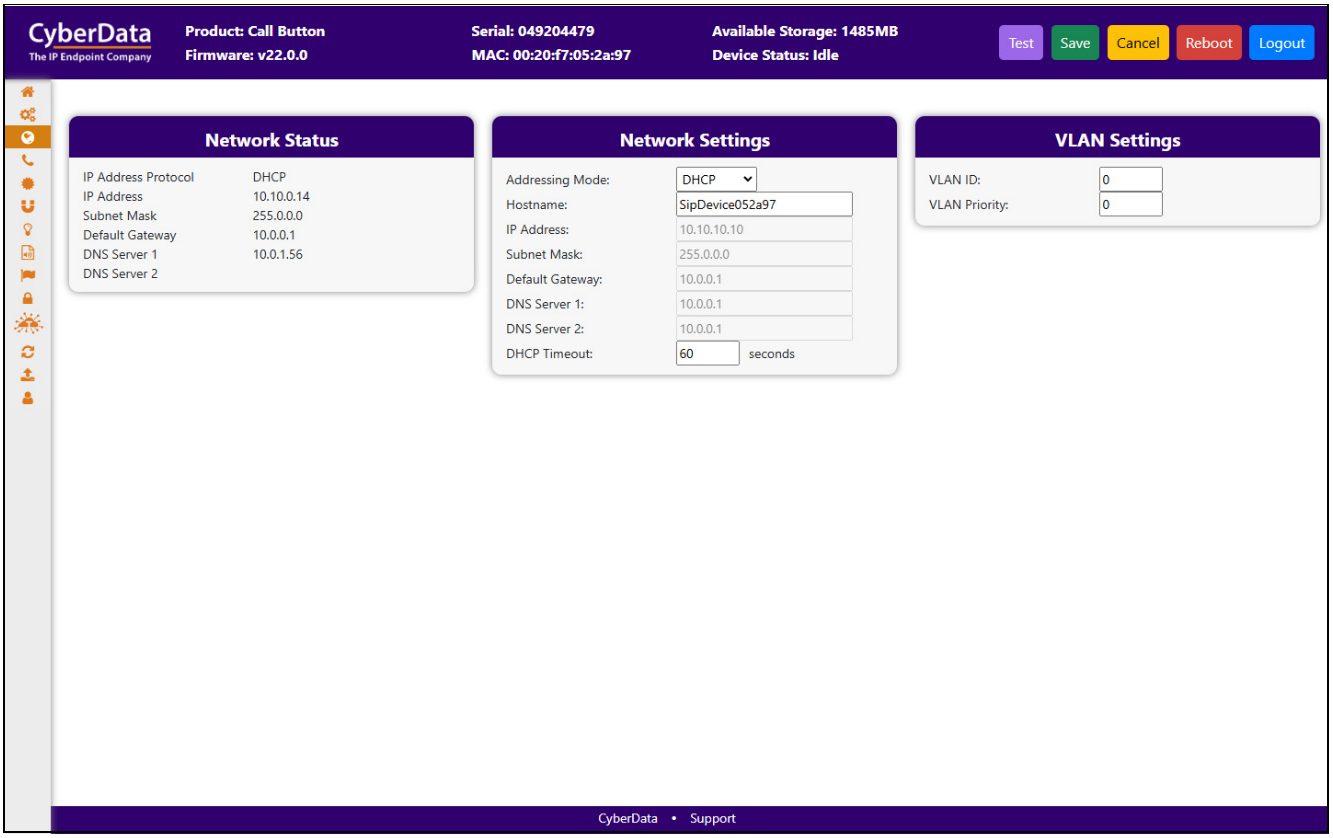


InformaCast Settings

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

2.4 Network

Figure 2-7. Network Page



Product: Call Button
Firmware: v22.0.0
Serial: 049204479
MAC: 00:20:f7:05:2a:97
Available Storage: 1485MB
Device Status: Idle

Network Status

IP Address Protocol	DHCP
IP Address	10.10.0.14
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:	SipDevice052a97
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

2.5 SIP (Session Initiation Protocol)

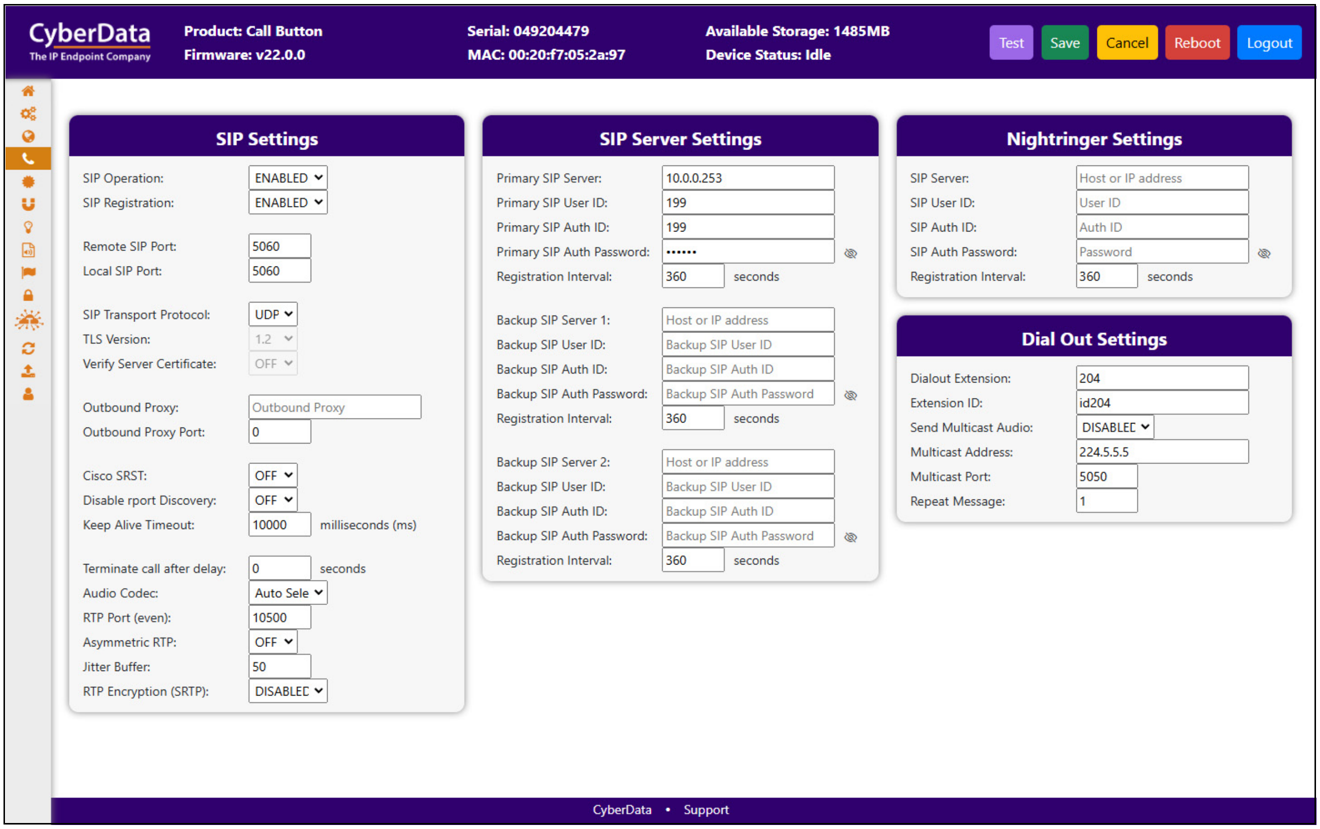
This page sets the options for phone calls. Configure up to 3 servers, with 2 acting as backup.

Use this page to configure the options for security, transport, codec, and others.

Note For specific server configurations, go to the following website address:

https://www.cyberdata.net/pages/connecting-to-ip-pbx-servers

Figure 2-8. SIP Page



Product: Call Button
Firmware: v22.0.0
Serial: 049204479
MAC: 00:20:f7:05:2a:97
Available Storage: 1485MB
Device Status: Idle

SIP Settings

SIP Operation:	ENABLED
SIP Registration:	ENABLED
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 Sele
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

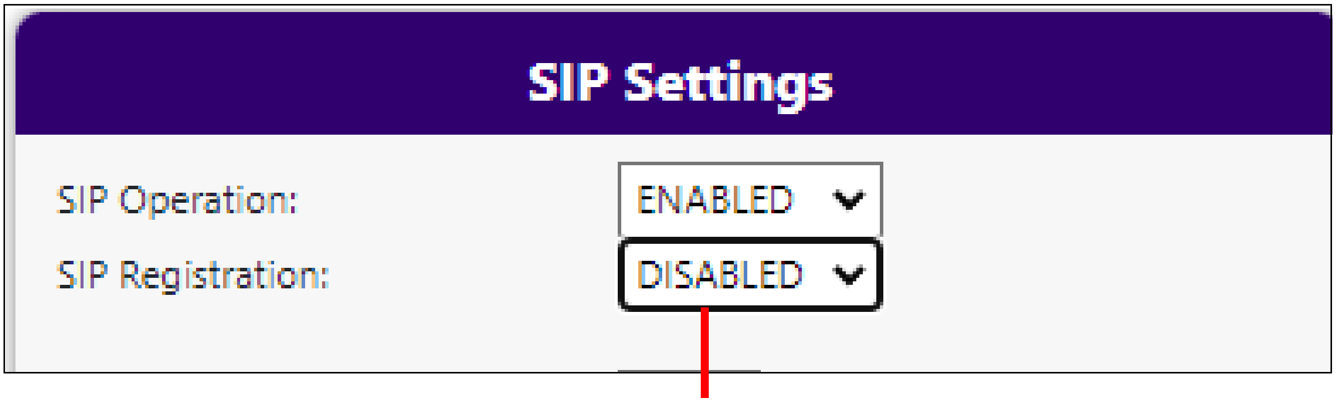
2.5.1 Dial Out Extension Strings and DTMF Tones (using rfc2833)

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

2.5.2 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 2-9.

Figure 2-9. SIP Page Set to Point-to-Point Mode



SIP Settings

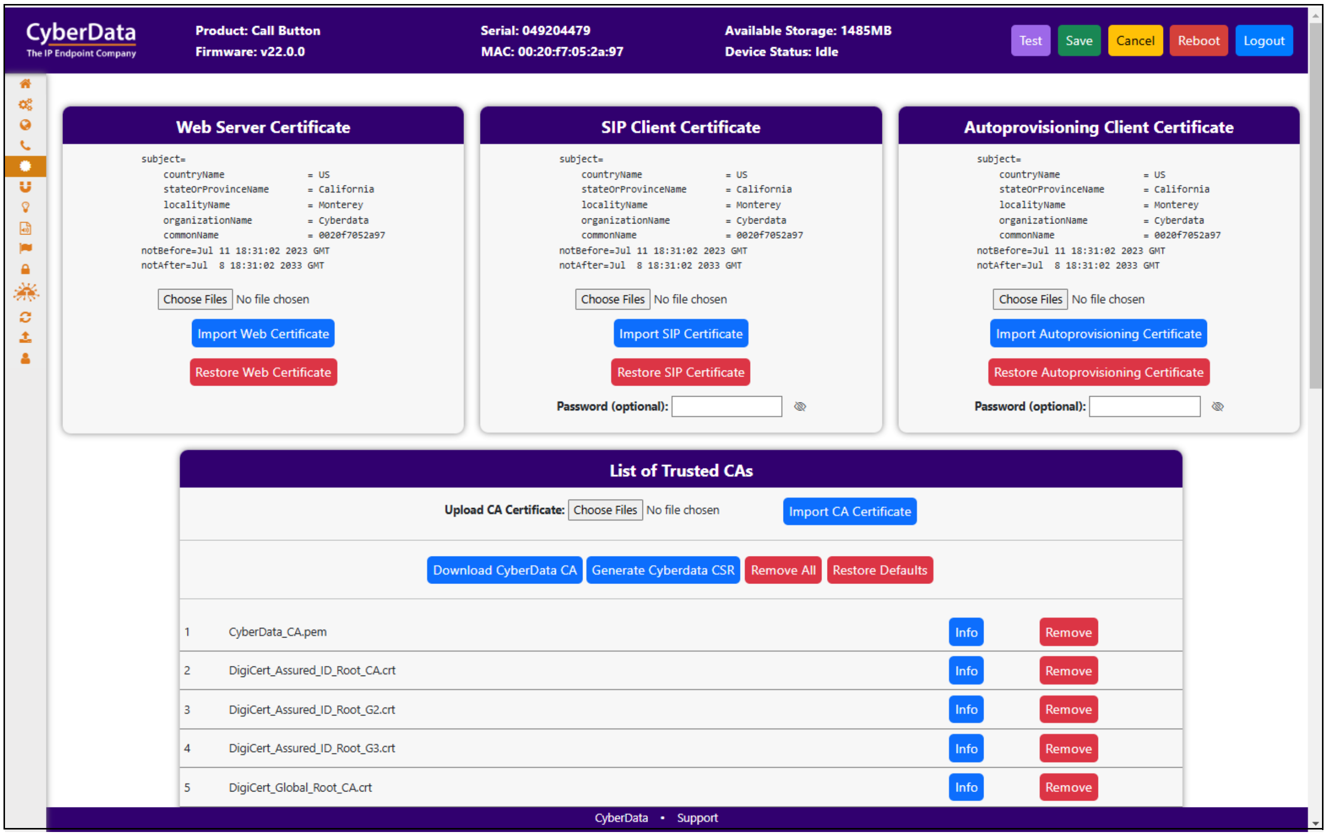
SIP Operation: ENABLED

SIP Registration: DISABLED

Device is set to NOT register with a SIP server

2.6 SSL

Figure 2-10. SSL Page



Product: Call Button
Firmware: v22.0.0
Serial: 049204479
MAC: 00:20:f7:05:2a:97
Available Storage: 1485MB
Device Status: Idle

Web Server Certificate

```
subject=
    countryName               = US
    stateOrProvinceName       = California
    localityName              = Monterey
    organizationName          = Cyberdata
    commonName                = 0020f7052a97
notBefore=Jul 11 18:31:02 2023 GMT
notAfter=Jul  8 18:31:02 2033 GMT
```

SIP Client Certificate

```
subject=
    countryName               = US
    stateOrProvinceName       = California
    localityName              = Monterey
    organizationName          = Cyberdata
    commonName                = 0020f7052a97
notBefore=Jul 11 18:31:02 2023 GMT
notAfter=Jul  8 18:31:02 2033 GMT
```

Password (optional):

Autoprovisioning Client Certificate

```
subject=
    countryName               = US
    stateOrProvinceName       = California
    localityName              = Monterey
    organizationName          = Cyberdata
    commonName                = 0020f7052a97
notBefore=Jul 11 18:31:02 2023 GMT
notAfter=Jul  8 18:31:02 2033 GMT
```

Choose Files
No file chosen
Import Autoprovisioning Certificate
Restore Autoprovisioning Certificate

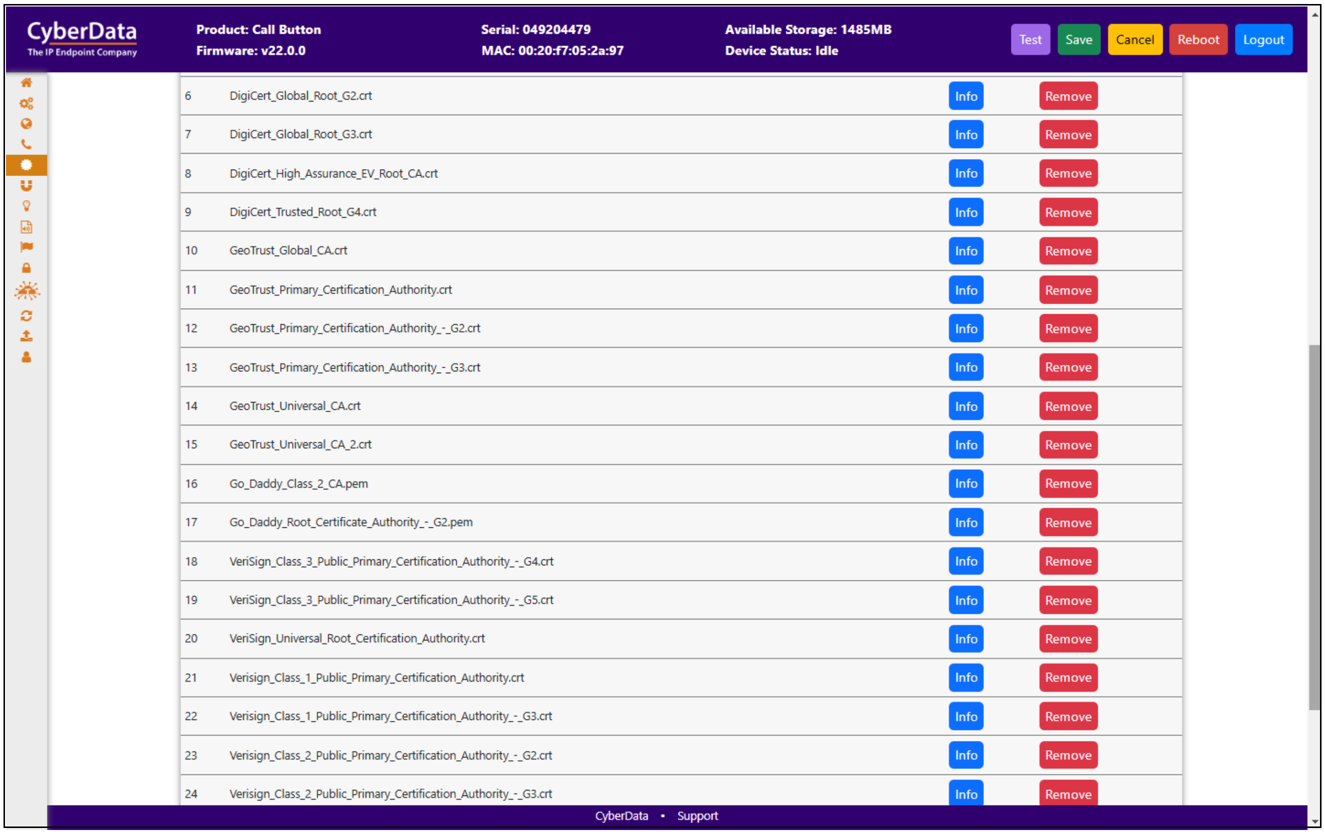
Password (optional):

List of Trusted CAs

Upload CA Certificate:

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

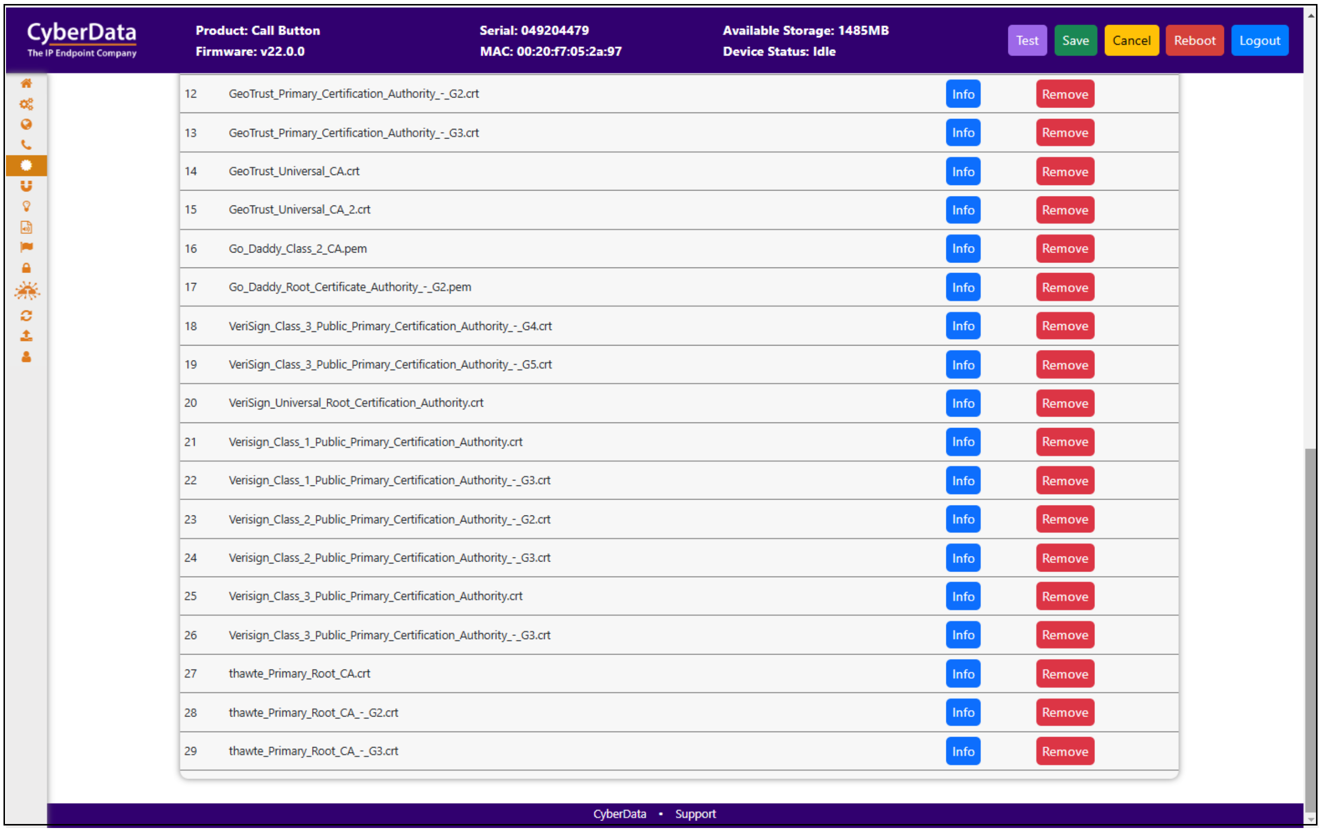
Figure 2-11. SSL Page



Product: Call Button
Firmware: v22.0.0
Serial: 049204479
MAC: 00:20:f7:05:2a:97
Available Storage: 1485MB
Device Status: Idle

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
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

Figure 2-12. SSL Page



Product: Call Button
Firmware: v22.0.0
Serial: 049204479
MAC: 00:20:f7:05:2a:97
Available Storage: 1485MB
Device Status: Idle

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

2.7 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.

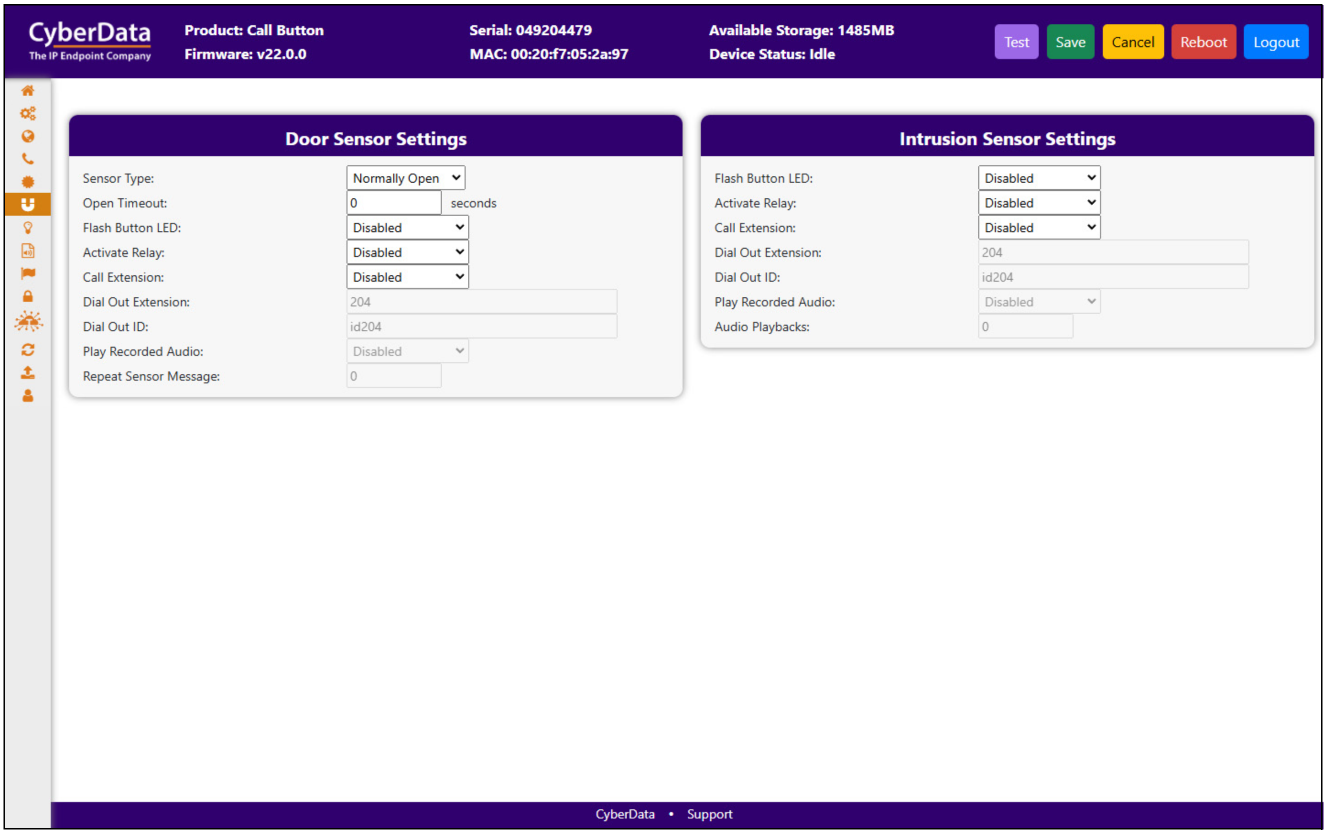
The intrusion sensor is an optical sensor installed on the Intercom board and will be activated when the Intercom is removed from the case.

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 2-13. Sensor Page



Product: Call Button
Firmware: v22.0.0
Serial: 049204479
MAC: 00:20:f7:05:2a:97
Available Storage: 1485MB
Device Status: Idle

Door Sensor Settings

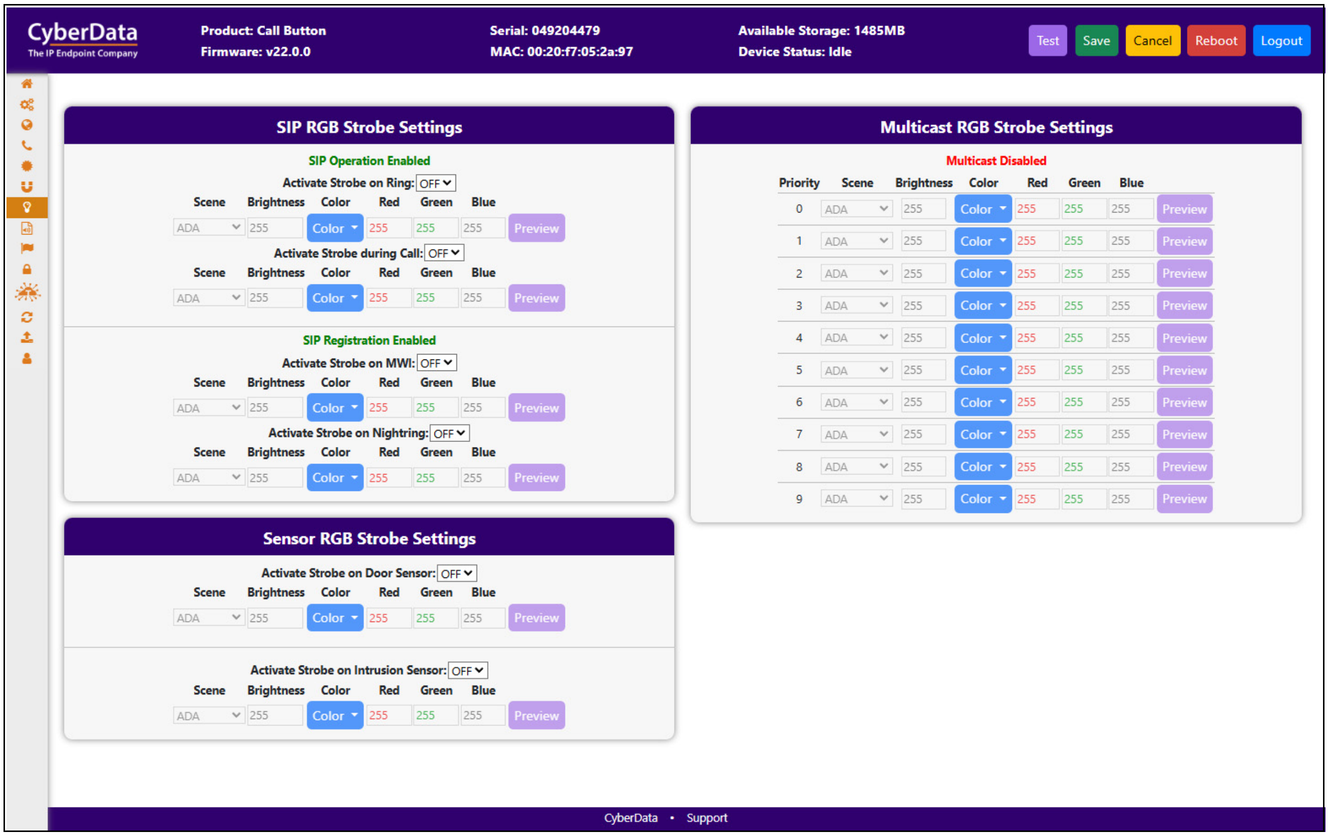
Sensor Type:	Normally Open
Open Timeout:	0 seconds
Flash Button LED:	Disabled
Activate Relay:	Disabled
Call Extension:	Disabled
Dial Out Extension:	204
Dial Out ID:	id204
Play Recorded Audio:	Disabled
Repeat Sensor Message:	0

Intrusion Sensor Settings

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

2.8 Strobe

Figure 2-14. Strobe Page



Product: Call Button
Firmware: v22.0.0

Serial: 049204479
MAC: 00:20:f7:05:2a:97

Available Storage: 1485MB
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

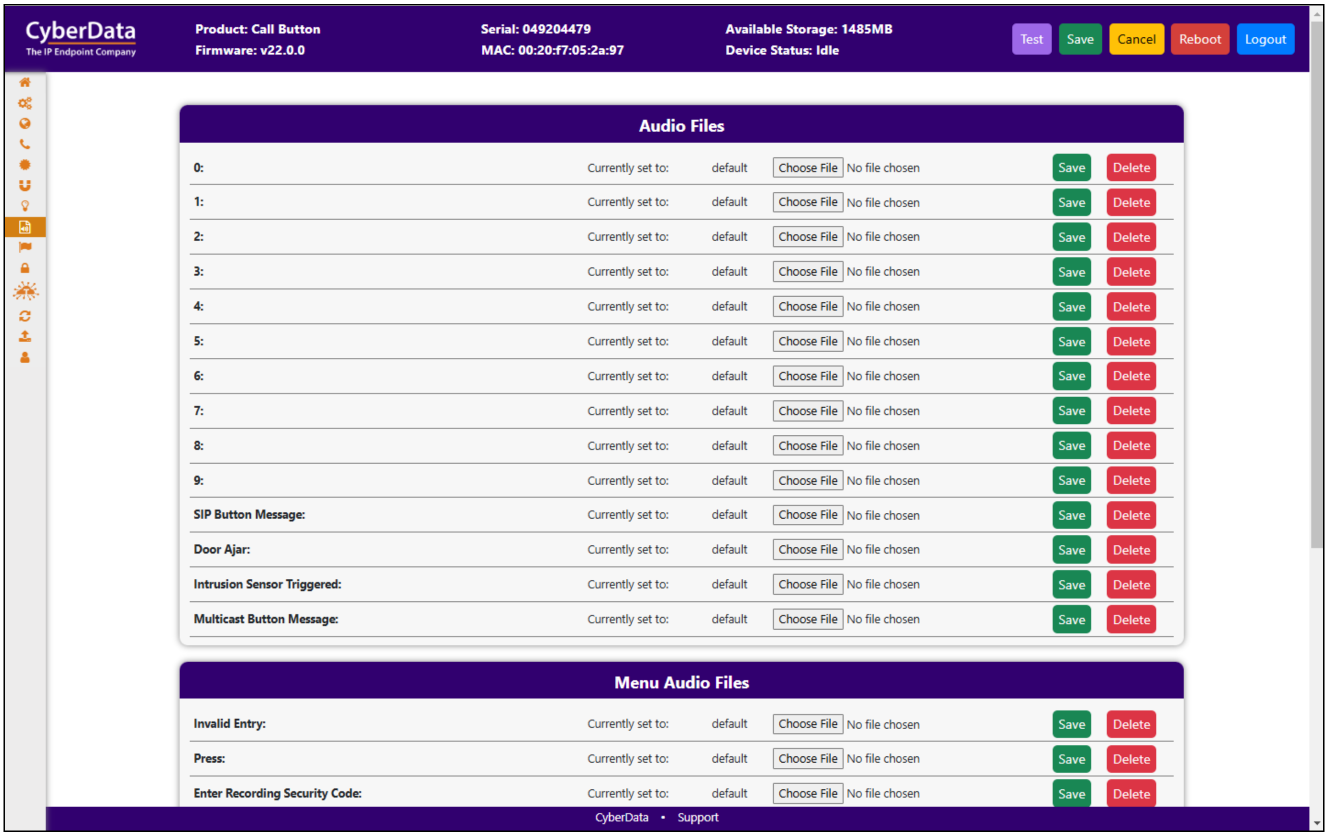
Priority	Scene	Brightness	Color	Red	Green	Blue	
0	ADA	255	Color	255	255	255	Preview
1	ADA	255	Color	255	255	255	Preview
2	ADA	255	Color	255	255	255	Preview
3	ADA	255	Color	255	255	255	Preview
4	ADA	255	Color	255	255	255	Preview
5	ADA	255	Color	255	255	255	Preview
6	ADA	255	Color	255	255	255	Preview
7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

CyberData • Support

2.9 Audiofiles

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

Figure 2-15. Audiofiles Page



Product: Call Button
Firmware: v22.0.0
Serial: 049204479
MAC: 00:20:f7:05:2a:97
Available Storage: 1485MB
Device Status: Idle

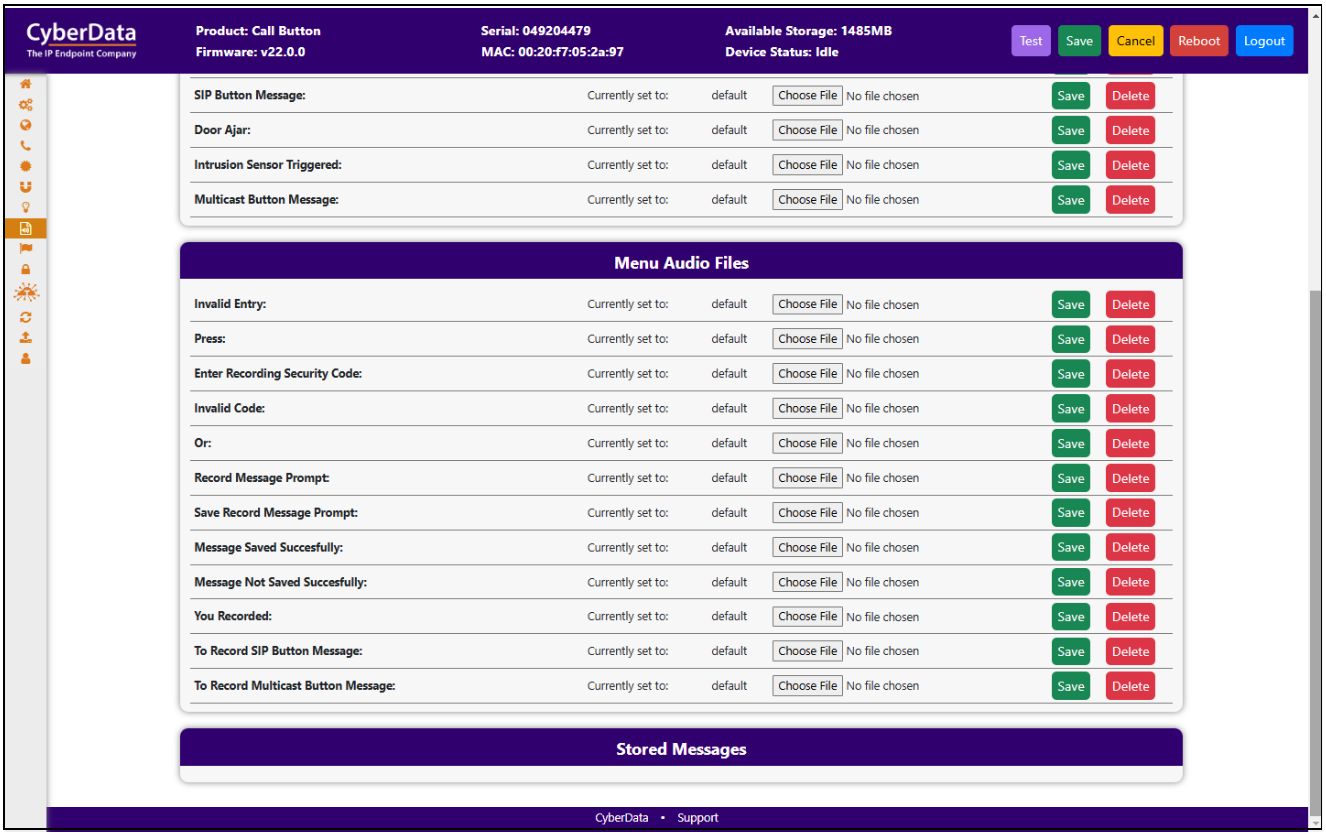
Audio Files

0:	Currently set to:	default	Choose File No file chosen	Save	Delete
1:	Currently set to:	default	Choose File No file chosen	Save	Delete
2:	Currently set to:	default	Choose File No file chosen	Save	Delete
3:	Currently set to:	default	Choose File No file chosen	Save	Delete
4:	Currently set to:	default	Choose File No file chosen	Save	Delete
5:	Currently set to:	default	Choose File No file chosen	Save	Delete
6:	Currently set to:	default	Choose File No file chosen	Save	Delete
7:	Currently set to:	default	Choose File No file chosen	Save	Delete
8:	Currently set to:	default	Choose File No file chosen	Save	Delete
9:	Currently set to:	default	Choose File No file chosen	Save	Delete
SIP Button Message:	Currently set to:	default	Choose File No file chosen	Save	Delete
Door Ajar:	Currently set to:	default	Choose File No file chosen	Save	Delete
Intrusion Sensor Triggered:	Currently set to:	default	Choose File No file chosen	Save	Delete
Multicast Button Message:	Currently set to:	default	Choose File No file chosen	Save	Delete

Menu Audio Files

Invalid Entry:	Currently set to:	default	Choose File No file chosen	Save	Delete
Press:	Currently set to:	default	Choose File No file chosen	Save	Delete
Enter Recording Security Code:	Currently set to:	default	Choose File No file chosen	Save	Delete

Figure 2-16. Audiofiles Page



Product: Call Button
Firmware: v22.0.0
Serial: 049204479
MAC: 00:20:f7:05:2a:97
Available Storage: 1485MB
Device Status: Idle

SIP Button Message:	Currently set to:	default	Choose File	No file chosen	Save	Delete
Door Ajar:	Currently set to:	default	Choose File	No file chosen	Save	Delete
Intrusion Sensor Triggered:	Currently set to:	default	Choose File	No file chosen	Save	Delete
Multicast Button Message:	Currently set to:	default	Choose File	No file chosen	Save	Delete

Menu Audio Files

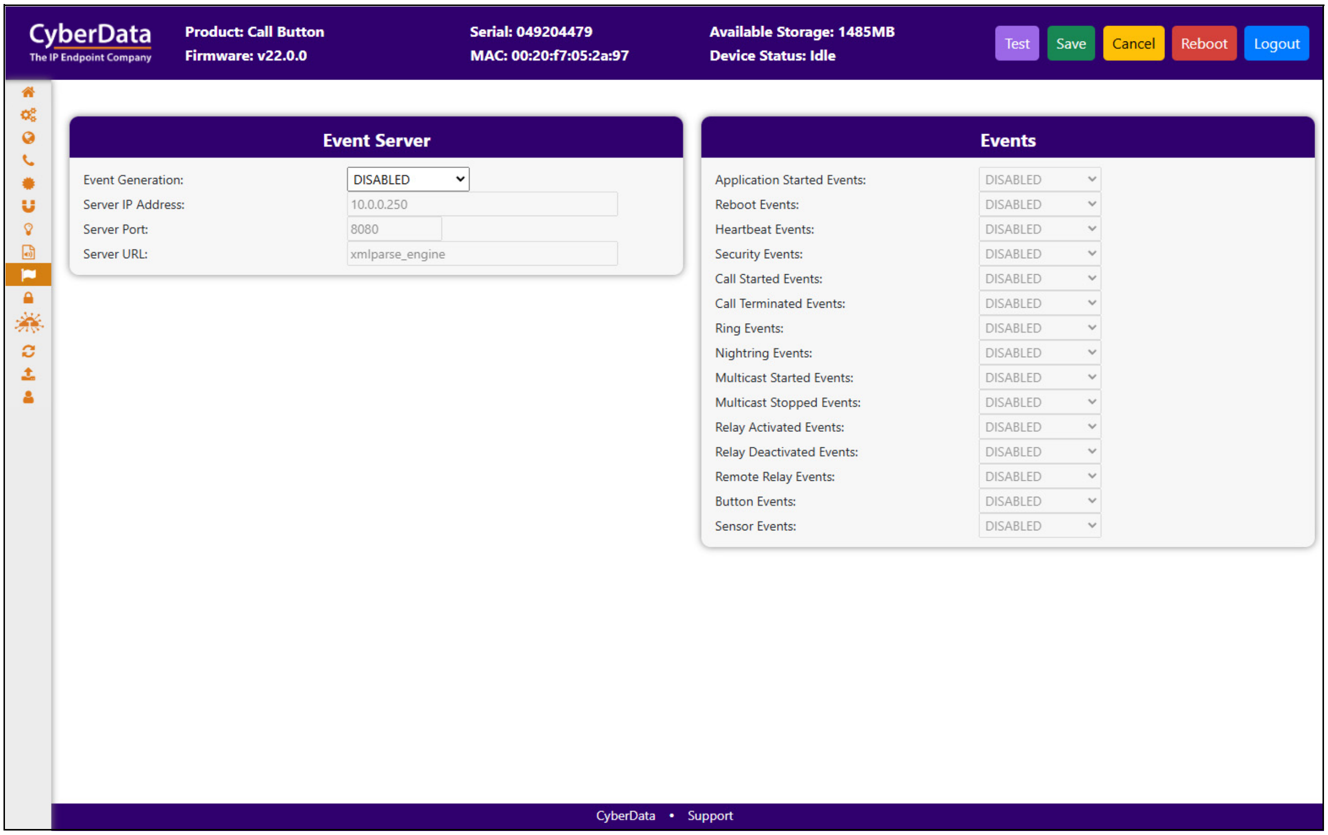
Invalid Entry:	Currently set to:	default	Choose File	No file chosen	Save	Delete
Press:	Currently set to:	default	Choose File	No file chosen	Save	Delete
Enter Recording Security Code:	Currently set to:	default	Choose File	No file chosen	Save	Delete
Invalid Code:	Currently set to:	default	Choose File	No file chosen	Save	Delete
Or:	Currently set to:	default	Choose File	No file chosen	Save	Delete
Record Message Prompt:	Currently set to:	default	Choose File	No file chosen	Save	Delete
Save Record Message Prompt:	Currently set to:	default	Choose File	No file chosen	Save	Delete
Message Saved Succesfully:	Currently set to:	default	Choose File	No file chosen	Save	Delete
Message Not Saved Succesfully:	Currently set to:	default	Choose File	No file chosen	Save	Delete
You Recorded:	Currently set to:	default	Choose File	No file chosen	Save	Delete
To Record SIP Button Message:	Currently set to:	default	Choose File	No file chosen	Save	Delete
To Record Multicast Button Message:	Currently set to:	default	Choose File	No file chosen	Save	Delete

Stored Messages

2.10 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 2-17. Events Page



Product: Call Button
Firmware: v22.0.0
Serial: 049204479
MAC: 00:20:f7:05:2a:97
Available Storage: 1485MB
Device Status: Idle

Event Server

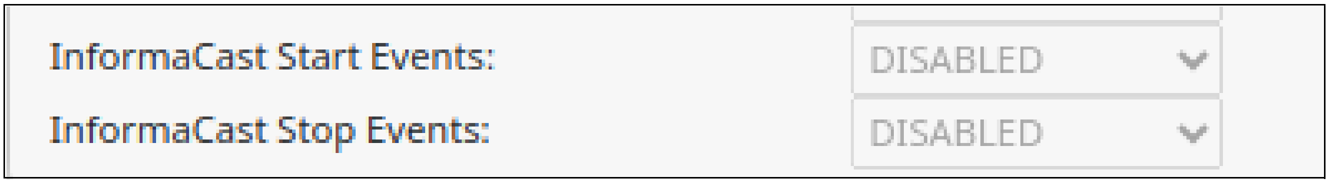
Event Generation:	DISABLED
Server IP Address:	10.0.0.250
Server Port:	8080
Server URL:	xmlparse_engine

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 2-18. InformaCast enabled Device



InformaCast Start Events:	DISABLED
InformaCast Stop Events:	DISABLED

2.10.1 Example Packets for Events

The server and port are used to point to the listening server and the 'Remote Event Server URL' is the destination URL (typically the script running on the remote server that's used to parse and process the POST events).

Note The XML is URL-encoded before transmission so the following examples are not completely accurate.

Here are example packets for every event:

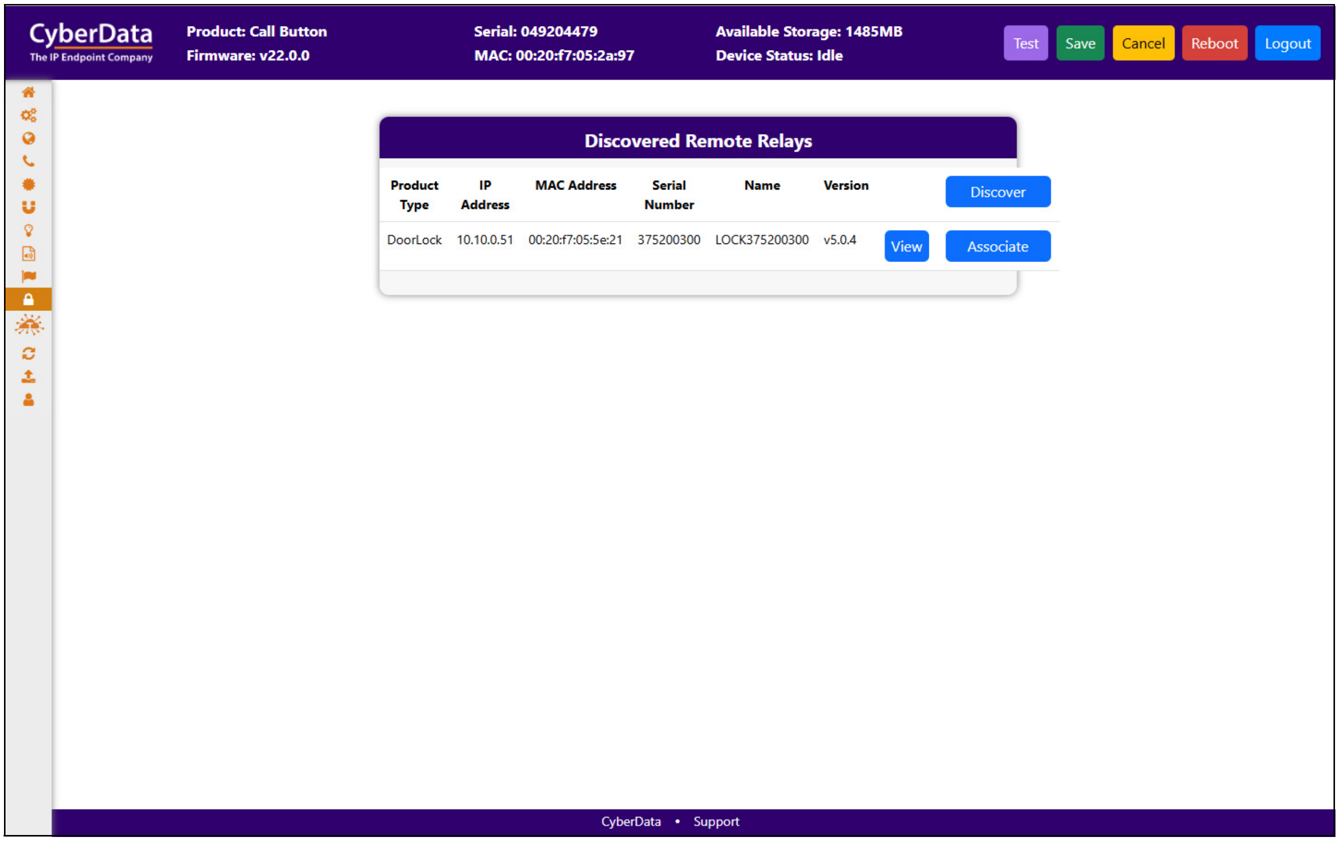
```
POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 197
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>POWERON</event>
</cyberdata>


POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 199
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>HEARTBEAT</event>
</cyberdata>


POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 196
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>BUTTON</event>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 201
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>CALL_ACTIVE</event>
</cyberdata>
```

```
POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 205
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>CALL_TERMINATED</event>
</cyberdata>


POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 197
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>RINGING</event>
</cyberdata>


POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>MULTICAST_START</event>
<index>8</index>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 233
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>MULTICAST_STOP</event>
<index>8</index>
</cyberdata>

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

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

2.11 Remote Relay

Figure 2-19. Remote Relay Page



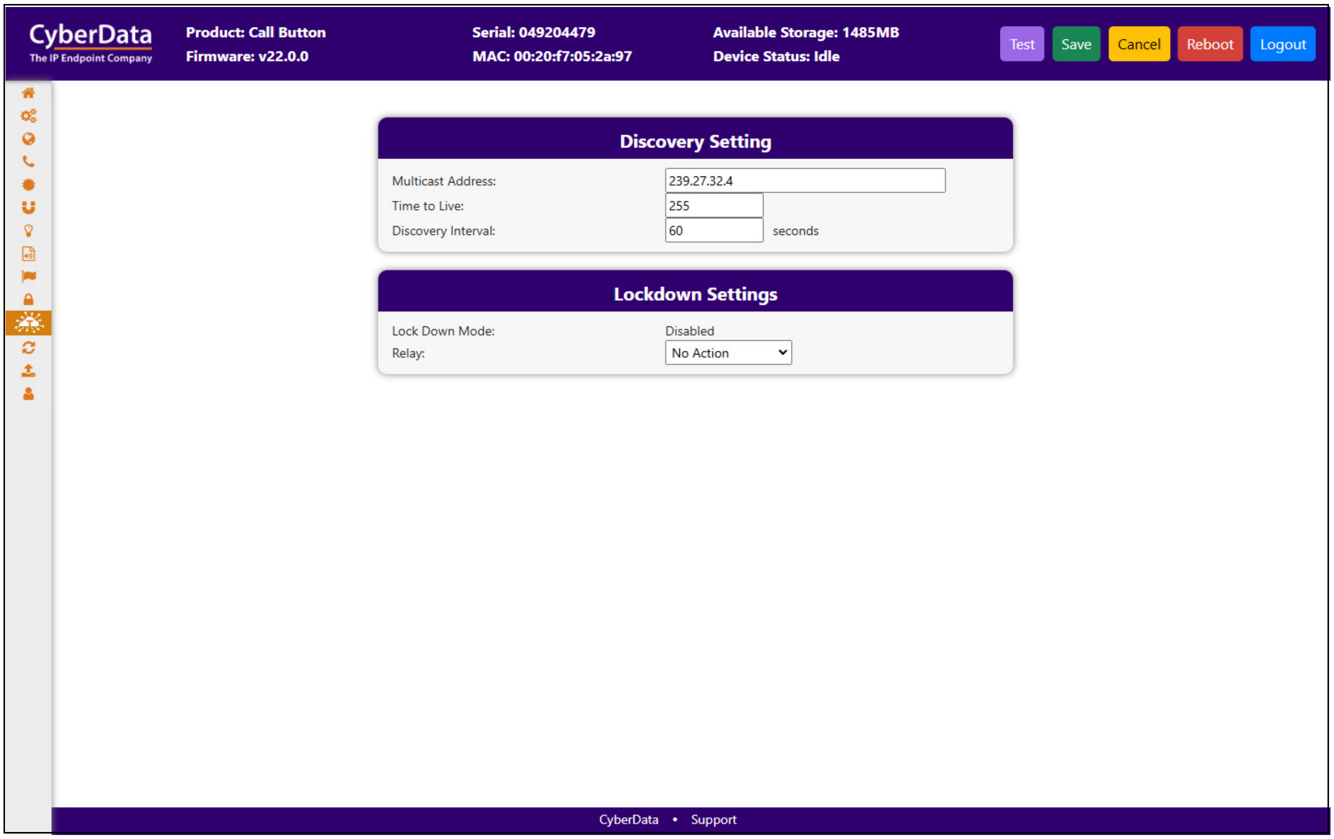
Product: Call Button
Firmware: v22.0.0
Serial: 049204479
MAC: 00:20:f7:05:2a:97
Available Storage: 1485MB
Device Status: Idle

Discovered Remote Relays

Product Type	IP Address	MAC Address	Serial Number	Name	Version
DoorLock	10.10.0.51	00:20:f7:05:5e:21	375200300	LOCK375200300	v5.0.4

2.12 Terminus

Figure 2-20. Terminus Page



Product: Call Button
Firmware: v22.0.0
Serial: 049204479
MAC: 00:20:f7:05:2a:97
Available Storage: 1485MB
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

2.13 Autoprovisioning

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

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

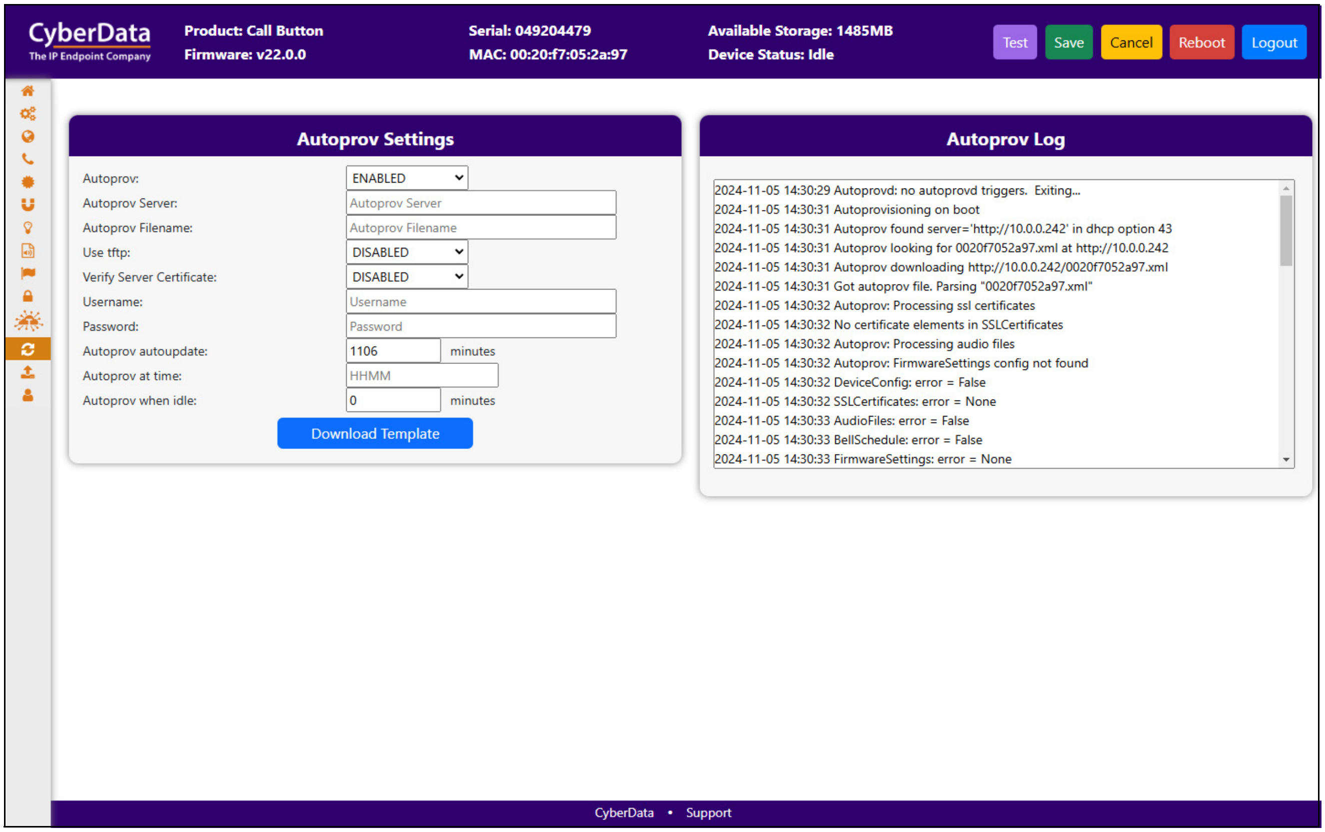
If a file is named, it will be downloaded instead of <mac address>,xml.

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

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

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

Figure 2-21. Autoprovisioning Page



Product: Call Button
Firmware: v22.0.0
Serial: 049204479
MAC: 00:20:f7:05:2a:97
Available Storage: 1485MB
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: 1106 minutes
Autoprov at time: HHMM
Autoprov when idle: 0 minutes

Download Template

Autoprov Log

```
2024-11-05 14:30:29 Autoprovd: no autoprovd triggers.  Exiting...
2024-11-05 14:30:31 Autoprovisioning on boot
2024-11-05 14:30:31 Autoprov found server='http://10.0.0.242' in dhcp option 43
2024-11-05 14:30:31 Autoprov looking for 0020f7052a97.xml at http://10.0.0.242
2024-11-05 14:30:31 Autoprov downloading http://10.0.0.242/0020f7052a97.xml
2024-11-05 14:30:31 Got autoprov file. Parsing "0020f7052a97.xml"
2024-11-05 14:30:32 Autoprov: Processing ssl certificates
2024-11-05 14:30:32 No certificate elements in SSLCertificates
2024-11-05 14:30:32 Autoprov: Processing audio files
2024-11-05 14:30:32 Autoprov: FirmwareSettings config not found
2024-11-05 14:30:32 DeviceConfig: error = False
2024-11-05 14:30:32 SSLCertificates: error = None
2024-11-05 14:30:33 AudioFiles: error = False
2024-11-05 14:30:33 BellSchedule: error = False
2024-11-05 14:30:33 FirmwareSettings: error = None
```

2.14 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:

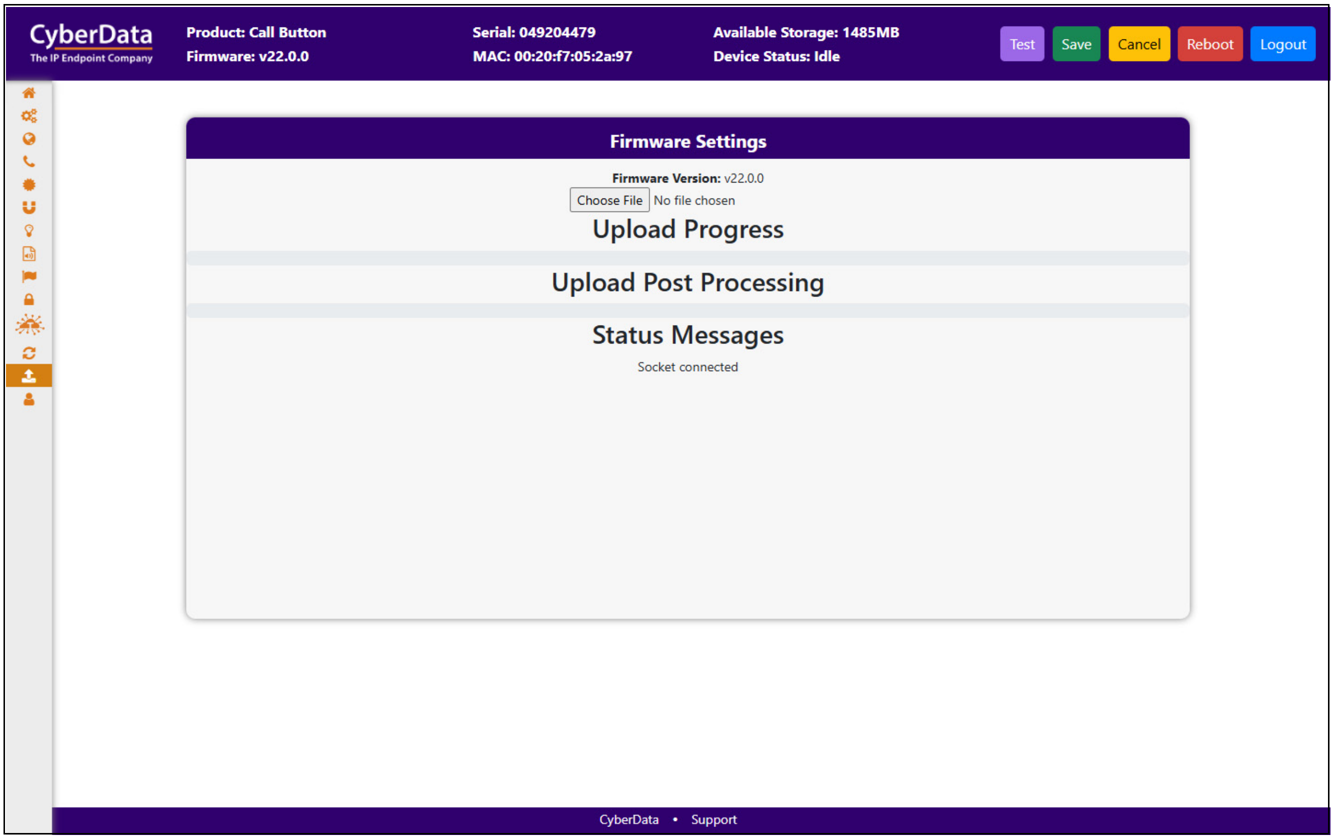
- Firmware file
- Release notes
- Autoprovisioning template

GENERAL ALERT

Caution

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

Figure 2-22. Firmware Page



Product: Call Button
Firmware: v22.0.0
Serial: 049204479
MAC: 00:20:f7:05:2a:97
Available Storage: 1485MB
Device Status: Idle

Firmware Settings

Firmware Version: v22.0.0

Choose File No file chosen

Upload Progress

Upload Post Processing

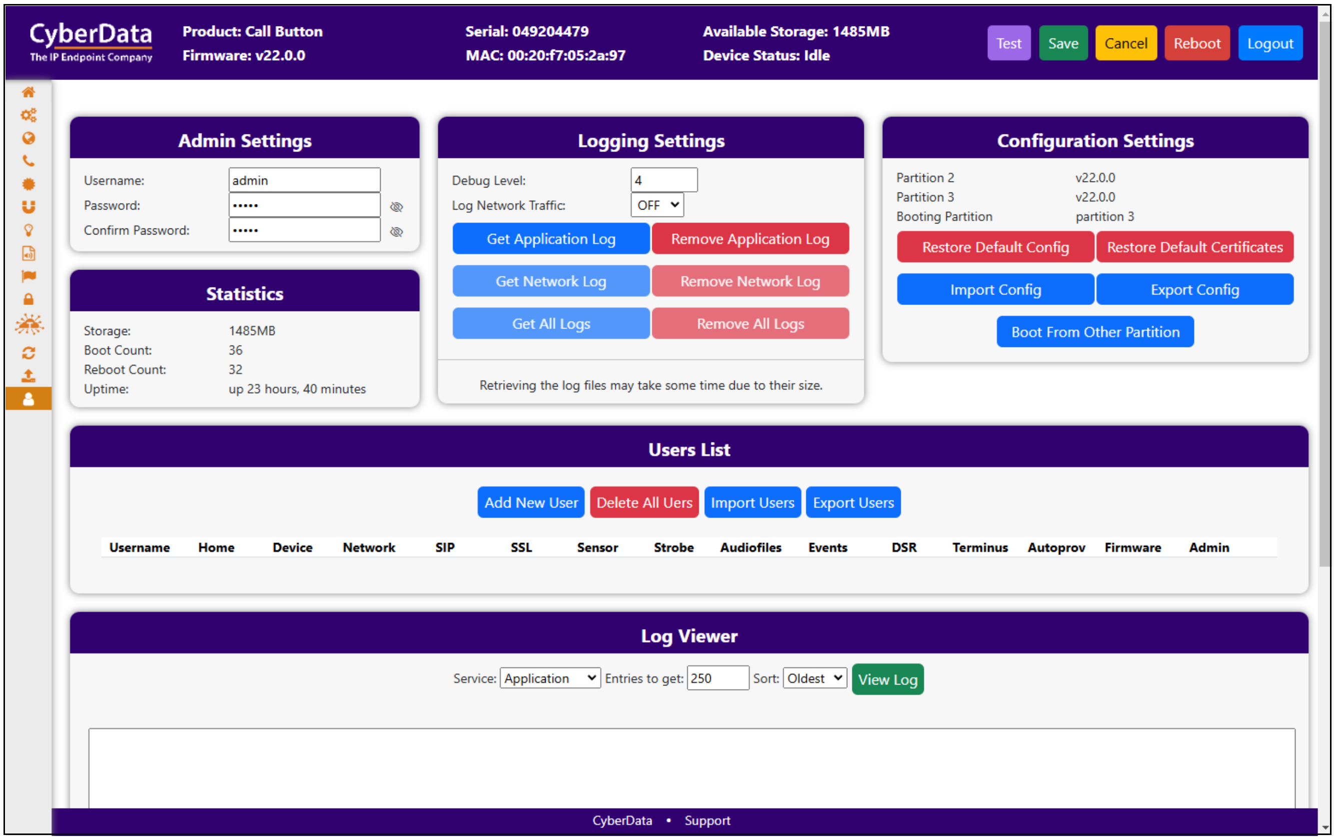
Status Messages

Socket connected

CyberData • Support

2.15 Admin

Figure 2-23. Admin Page



Product: Call Button
Firmware: v22.0.0
Serial: 049204479
MAC: 00:20:f7:05:2a:97
Available Storage: 1485MB
Device Status: Idle

Admin Settings

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

Statistics

Storage:	1485MB
Boot Count:	36
Reboot Count:	32
Uptime:	up 23 hours, 40 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	Network	SIP	SSL	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.

2.16 Command Interface

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

2.16.1 Command Interface Post Commands

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

Table 2-2. Command Interface Post Commands

Device Action	HTTP Post Command[a]
Trigger relay (for configured delay)	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/command.cgi" --post-data "test_relay=yes"
Place call to extension (example: extension 130)	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/command.cgi" --post-data "call=130"
Terminate active call	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/command.cgi" --post-data "terminate=yes"
Force reboot	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/command.cgi" --post-data "reboot=yes"
Trigger the Door Sensor Test (Sensor Config page)	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/sensor.cgi" --post-data "doortest=yes"
Trigger the Intrusion Sensor Test (Sensor Config page)	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/sensor.cgi" --post-data "intrusiontest=yes"

[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