CyberData
The IP Endpoint Company

SIP Call/Panic Button Operations Guide

SIP Compliant
Part #011049, 011491

Document Part #*932062B*
for Firmware Version *22.0*

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

CyberData SIP Call/Panic Button Operations Guide 932062B
Part # 011049, 011491

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
Fax: (831) 373-4193
Company and product information is at **www.cyberdata.net**.

Revision Information

Revision 932062B, which corresponds to firmware version 22.0, was released on March 20, 2026, and has the following changes:

- Updates the product name to **SIP Call/Panic Button** throughout the document.

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!**

Warning

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

Warning

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

Warning

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

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.

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

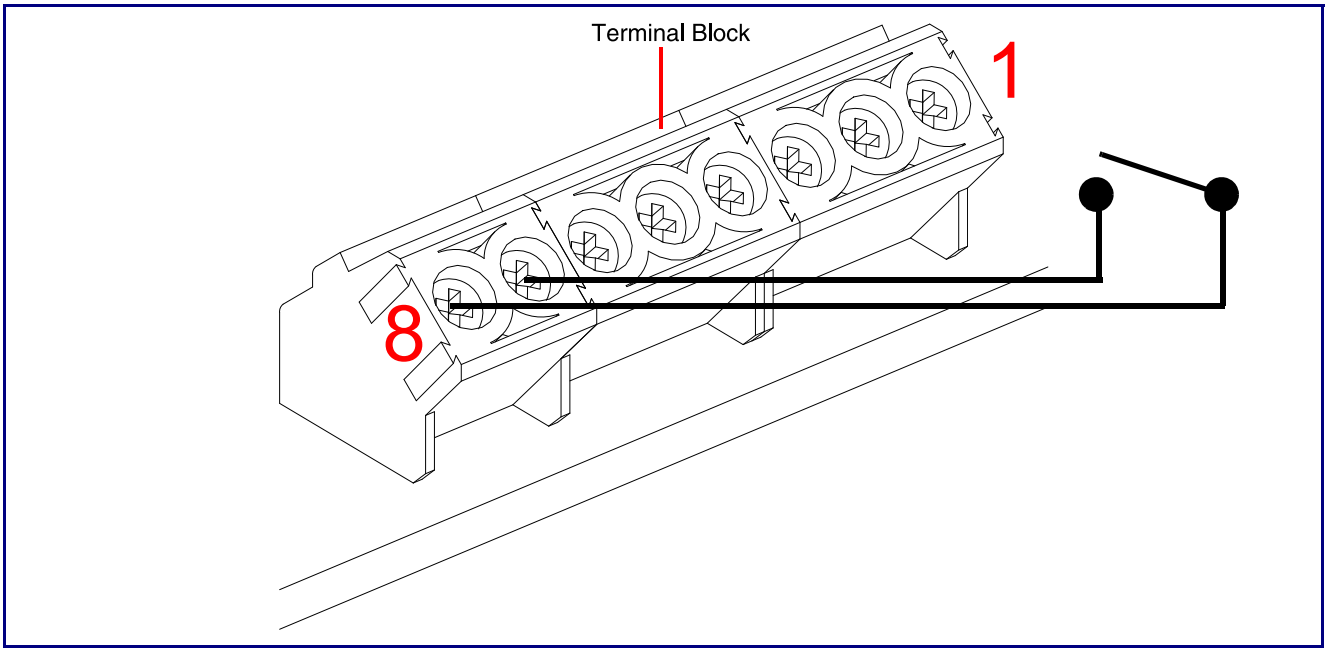
Contents

1 Installing the SIP Call/Panic 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)

Figure 1. Remote Switch Connection



1.1.1 Using the On-Board Relay

Warning

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

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.

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.

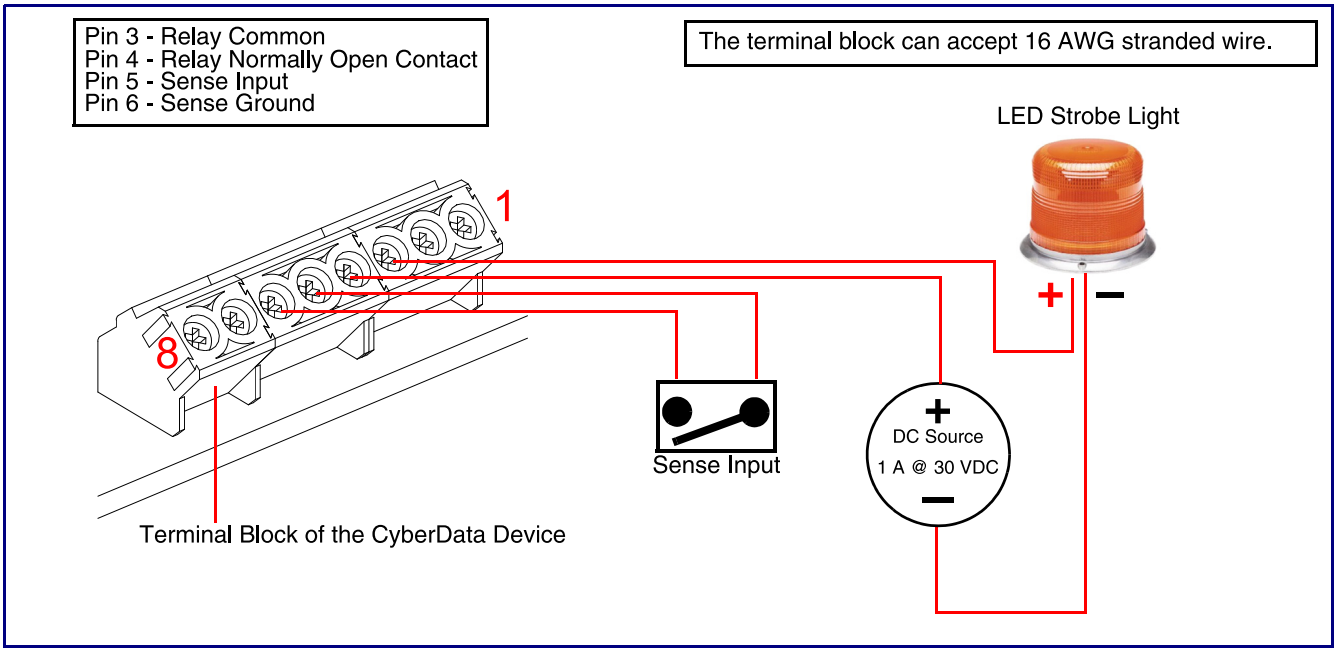
1.2 Wiring the Circuit

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 2. Devices Less than 1A at 30 VDC



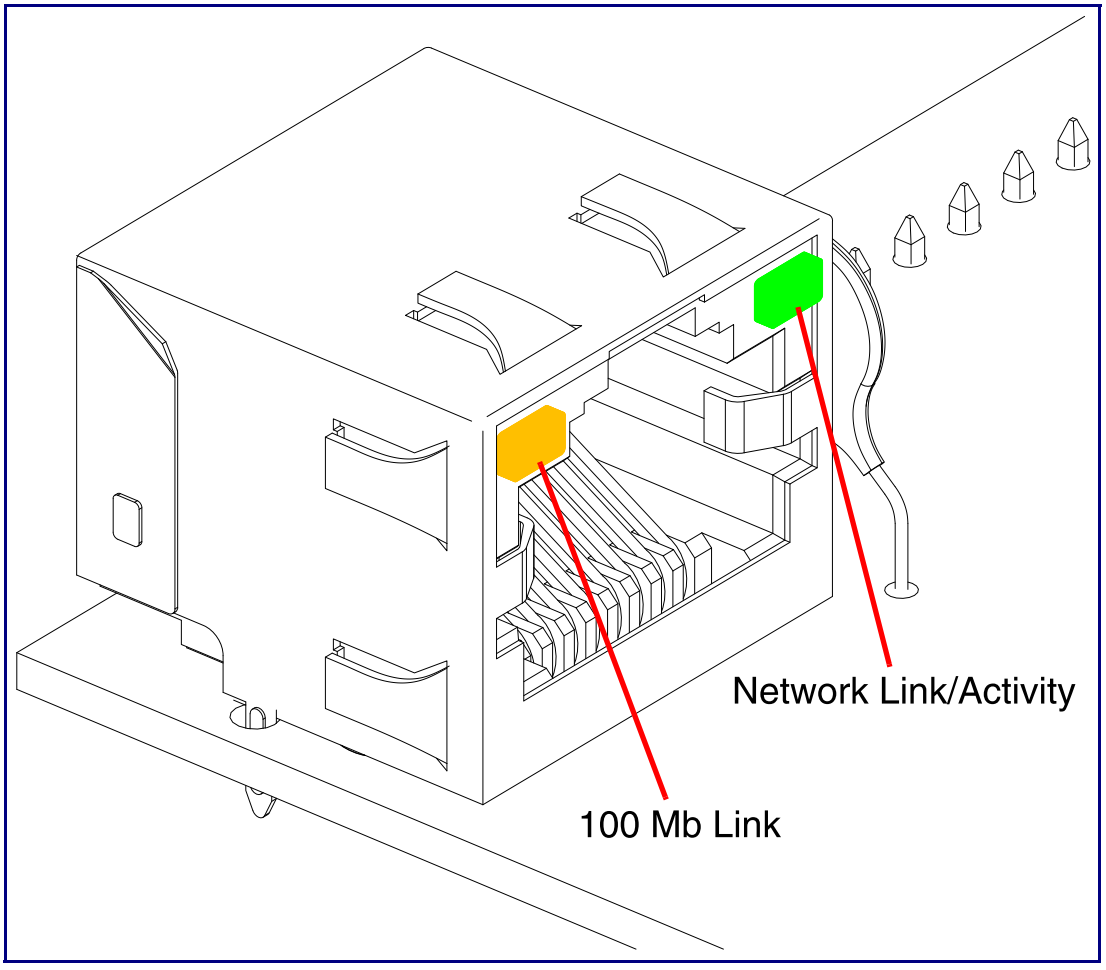
1.3 Activity and Link LEDs

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 3).
- The square, **AMBER** 100 Mb **Link** LED above the Ethernet port indicates that the network 100 Mb connection has been established (see Figure 3).

Figure 3. Activity and Link LED



1.4 Call Button and the Call Button LED

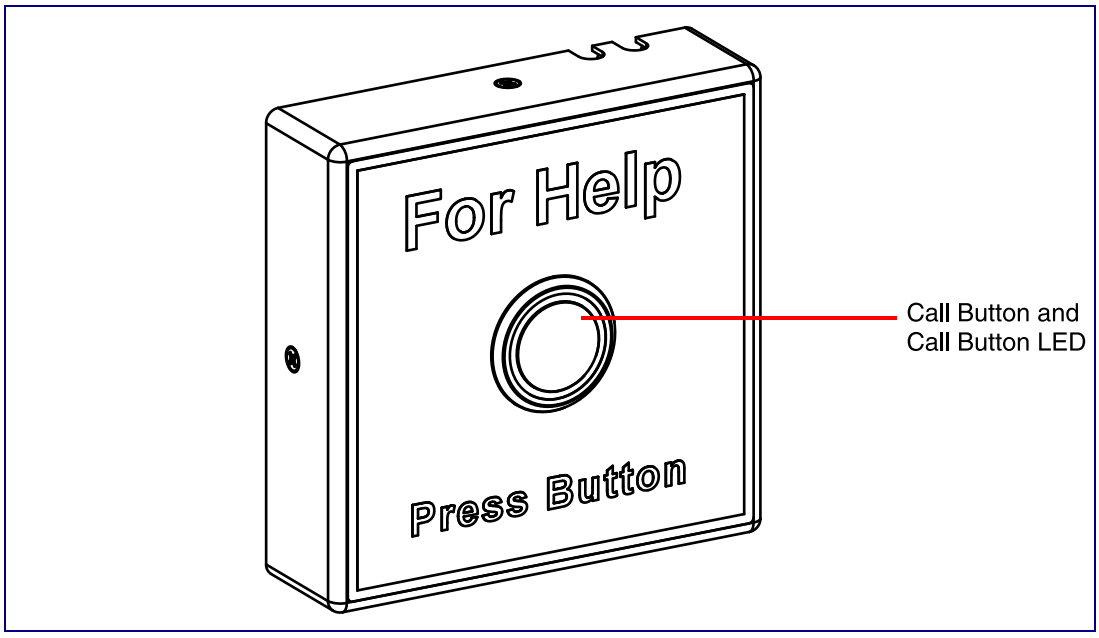
1.4.1 Calling with the The Call Button

- 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 4. Call Button and Call Button LED



1.5 Restore the Factory Default Settings

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

To restore the device to its factory default settings (Table 2), hold the RTFM button (Figure 5) for approximately seven seconds.

The device will default to DHCP to obtain an IP address, or will use 192.168.1.23 if a DHCP server is not present.

Figure 5. RTFM Button

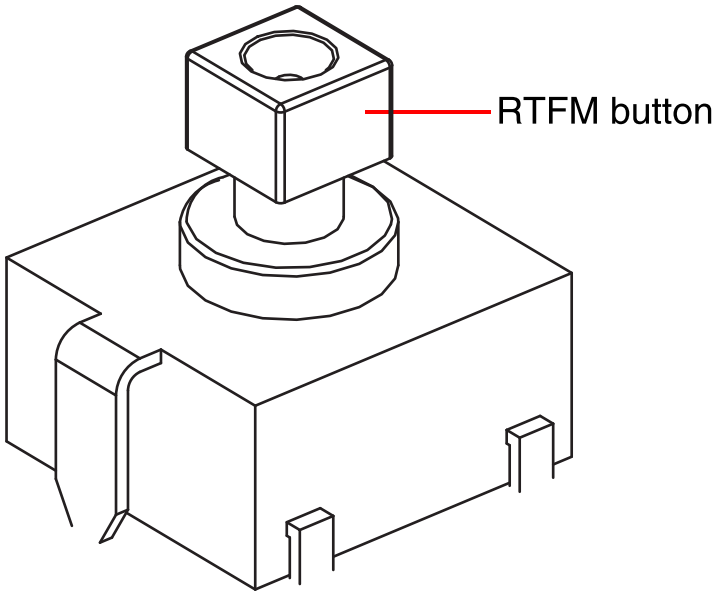


Table 1. Factory Default Settings

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.

2 Configure the Device

2.1 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

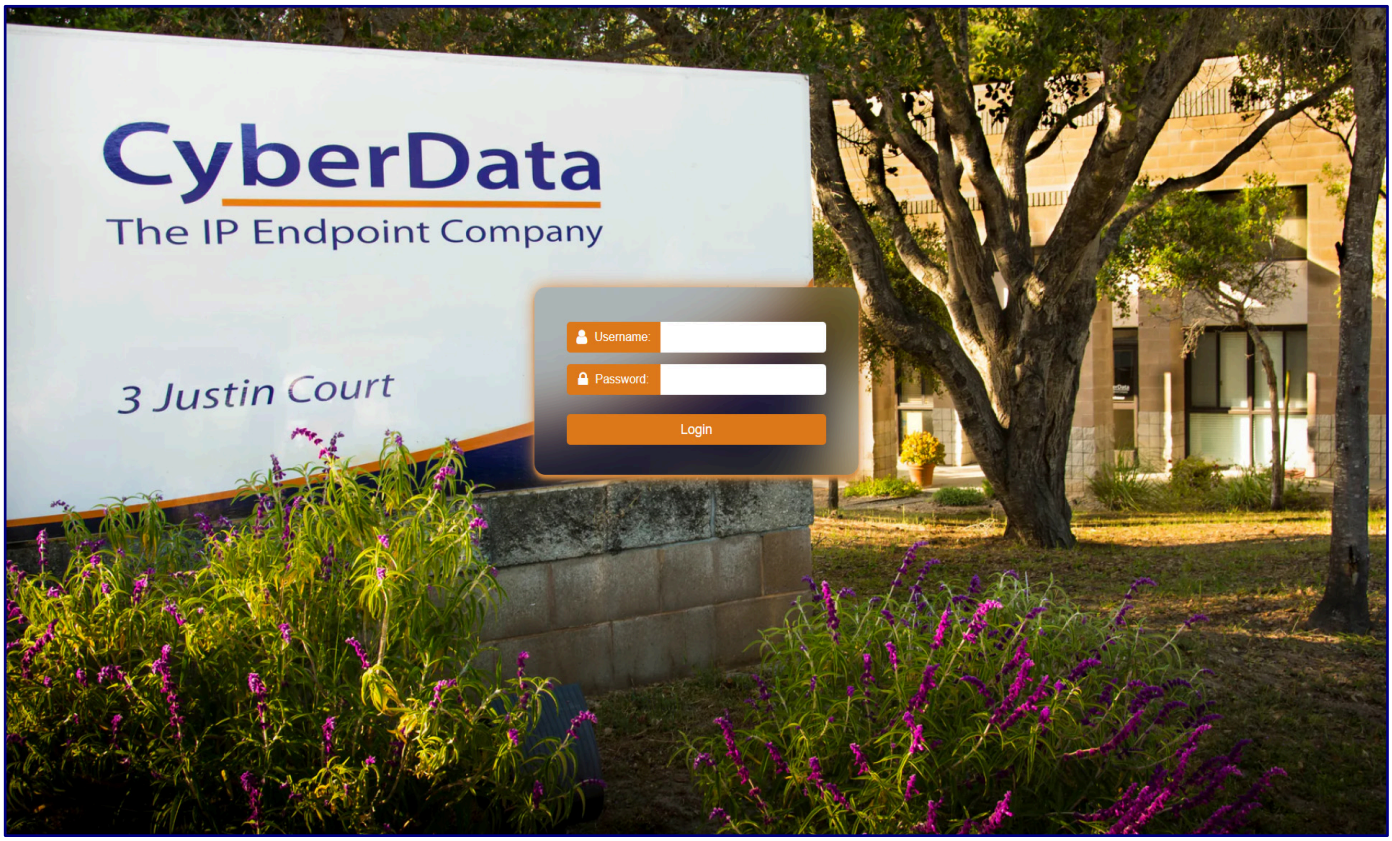
   Note The Intercom ships in DHCP mode. To get to the Home page, use the discovery utility to scan for the device on the network and open your browser from there.

2. On the **Log In** Page (Figure 6), use the following default **Web Access Username** and **Web Access Password** to access the **Home Page** (Figure 7):

   Web Access Username: **admin**

   Web Access Password: **admin**

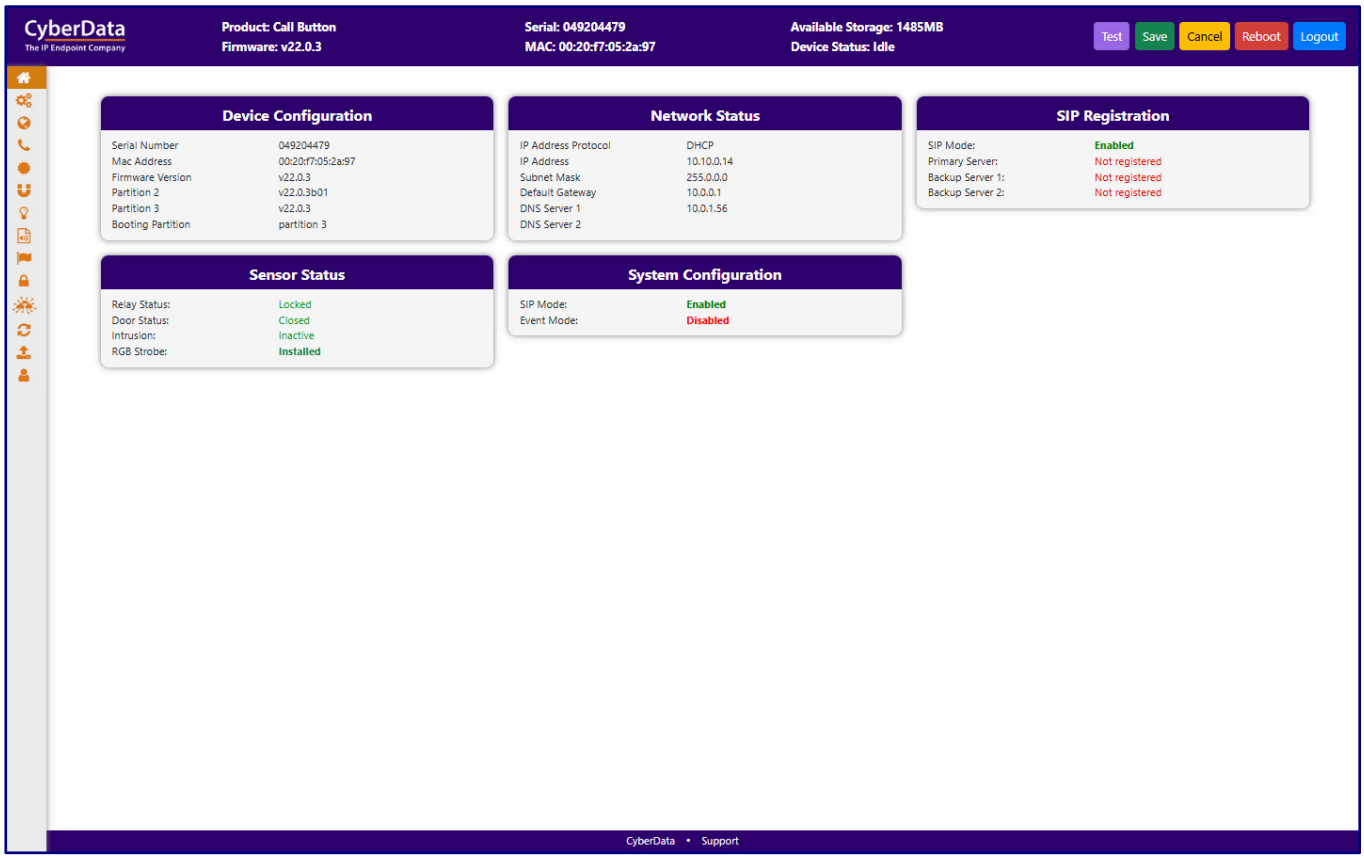
Figure 6. Log In Page



2.2 Home Page

The **Home** page provides device specific information such as Serial Number, Mac Address, and Firmware version. This page is designed as an initial landing page to provide general information on the status of the device.

Figure 7. Home Page

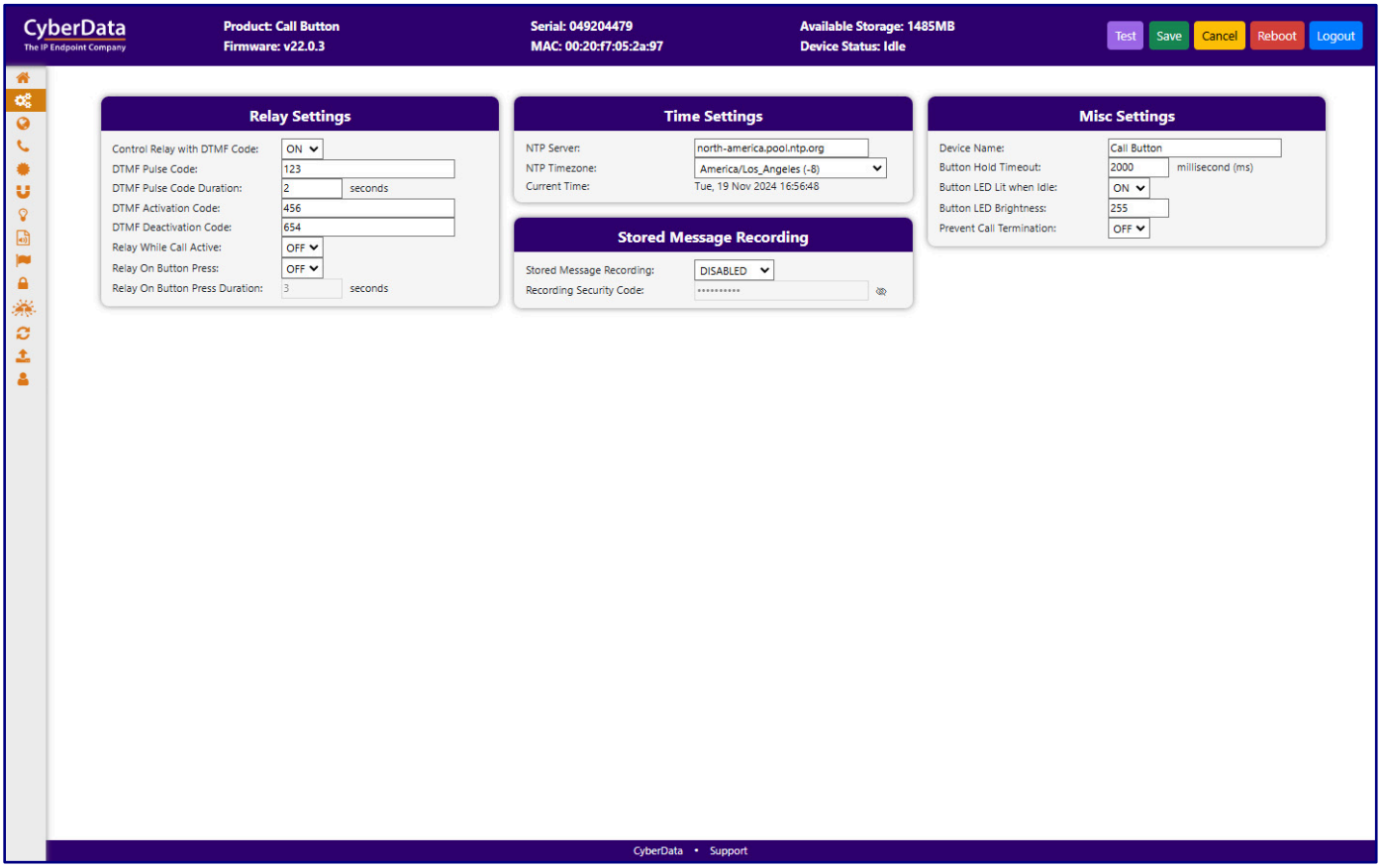


2.3 Device

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

Note Enabling DDSR mode sets the device to end of life 011375 Network Dual Door Strike Relay (DDSR) mode. 3 DDSR Mode provides screen captures for this mode.

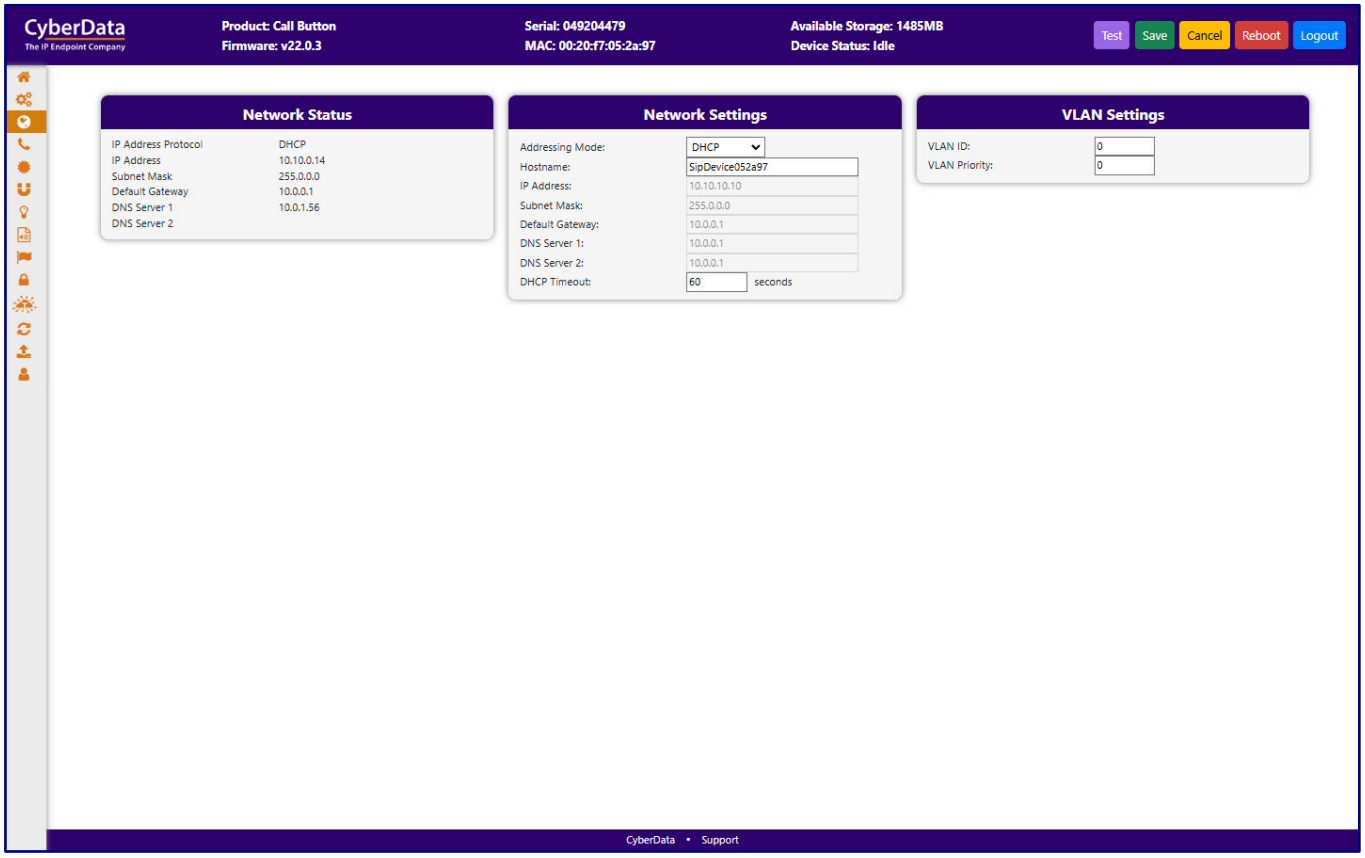
Figure 8. Device Page



2.4 Network

The **Network** tab provides access to network-related settings. Assigning the device a static IP address or VLAN is done on this page.

Figure 9. Network Page



2.5 SIP (Session Initiation Protocol)

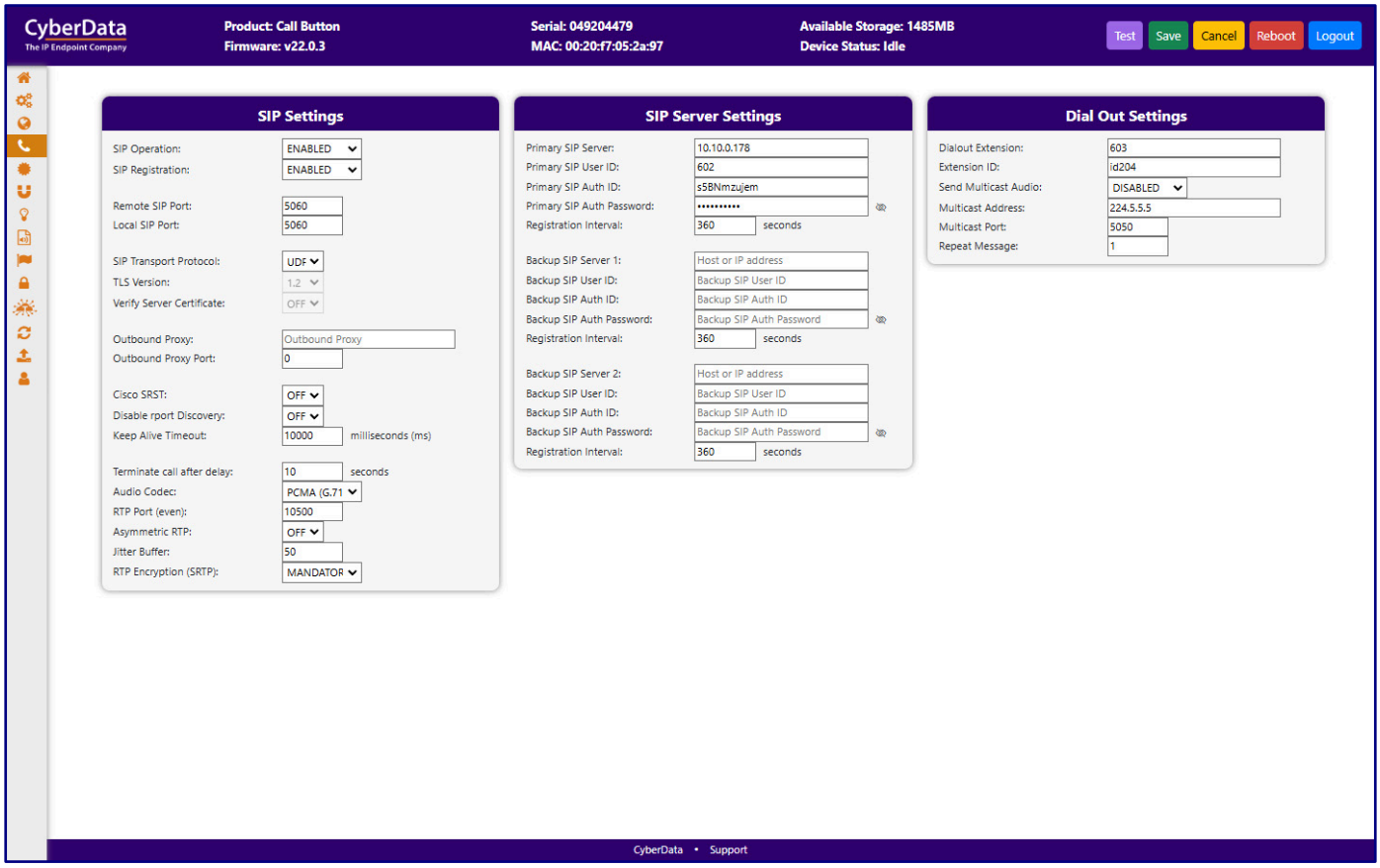
This page sets the options for phone calls. Configure up to 3 servers, with 2 acting as backup, and a server for the nightringer. The nightringer is a second sip extension that only rings, never connects to a call. Many customers use the nightringer in a hunt group.

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 10. SIP Page



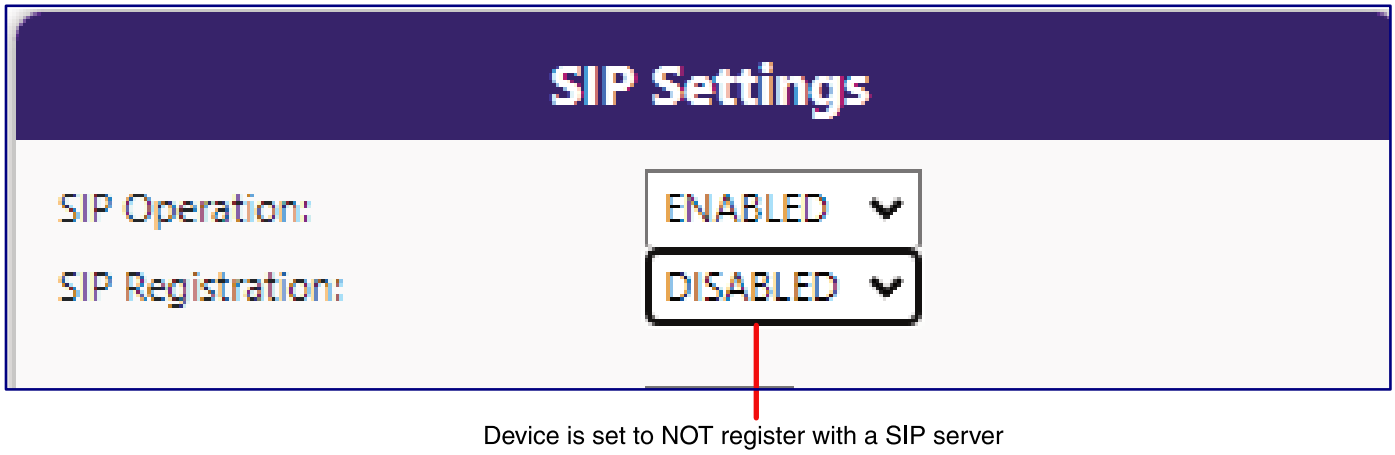
2.5.1 Dial Out Extension Strings and DTMF Tones (using rfc2833)

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 11.

Figure 11. SIP Page Set to Point-to-Point Mode



2.6 SSL

The **SSL** tab allows for the adjustment of certificates used by the device. The certificates used for the web server, SIP Client, and Autoprovisioning can be changed here. It is also possible to add additional CA certificates on this page. CA Certificates allow the device to authenticate servers that it contacts.

Figure 12. SSL Page (1 of 2)

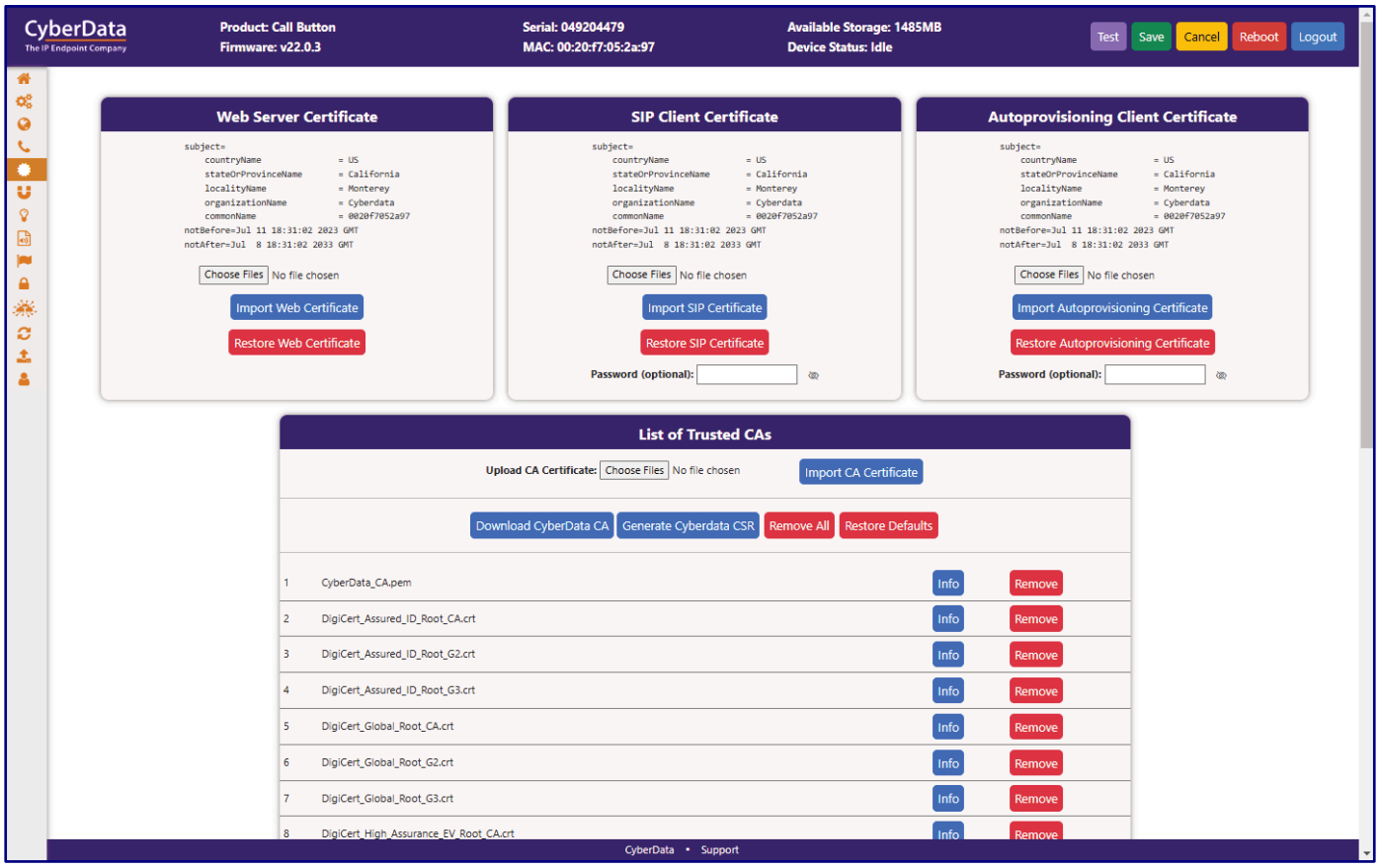
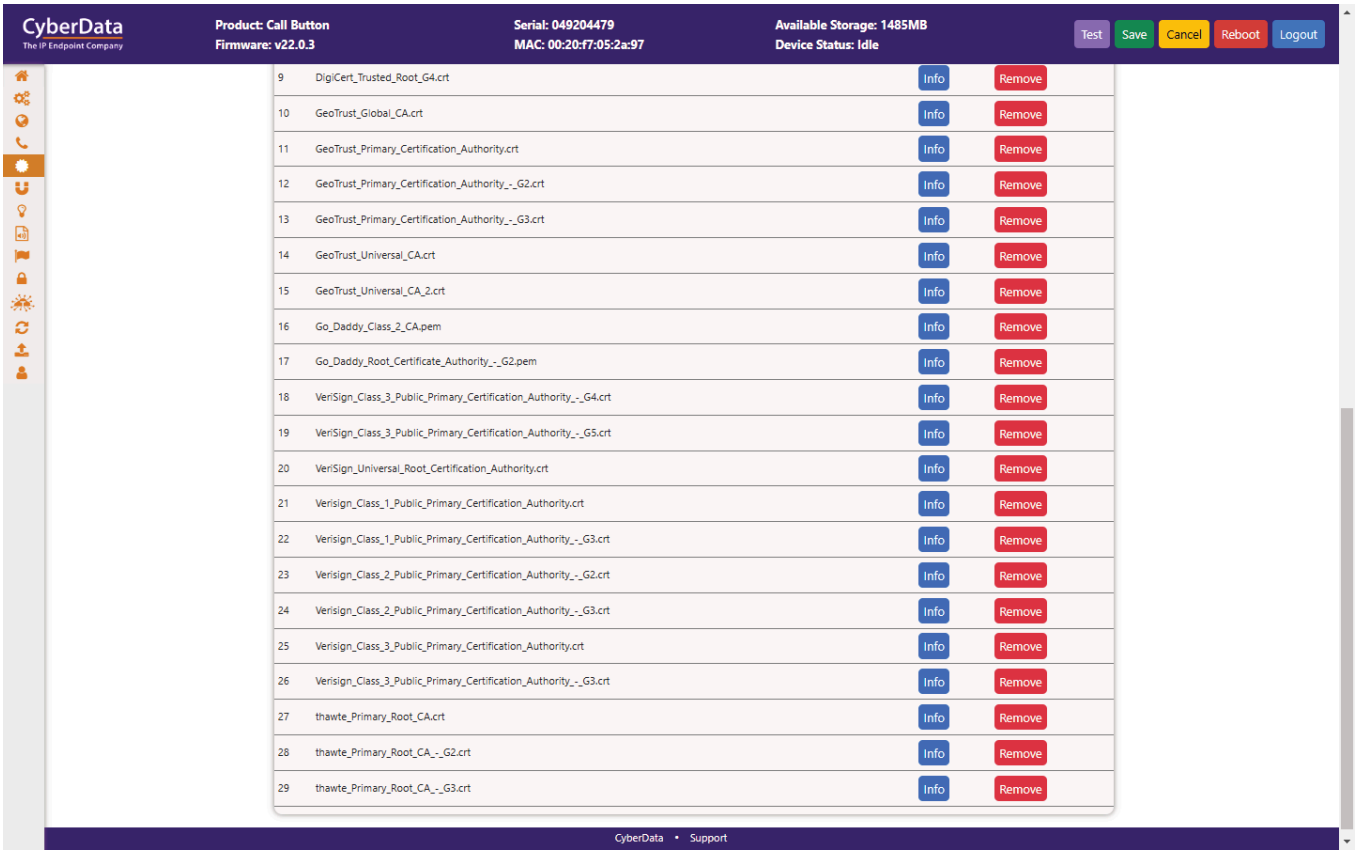


Figure 13. SSL Page (2 of 2)



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.

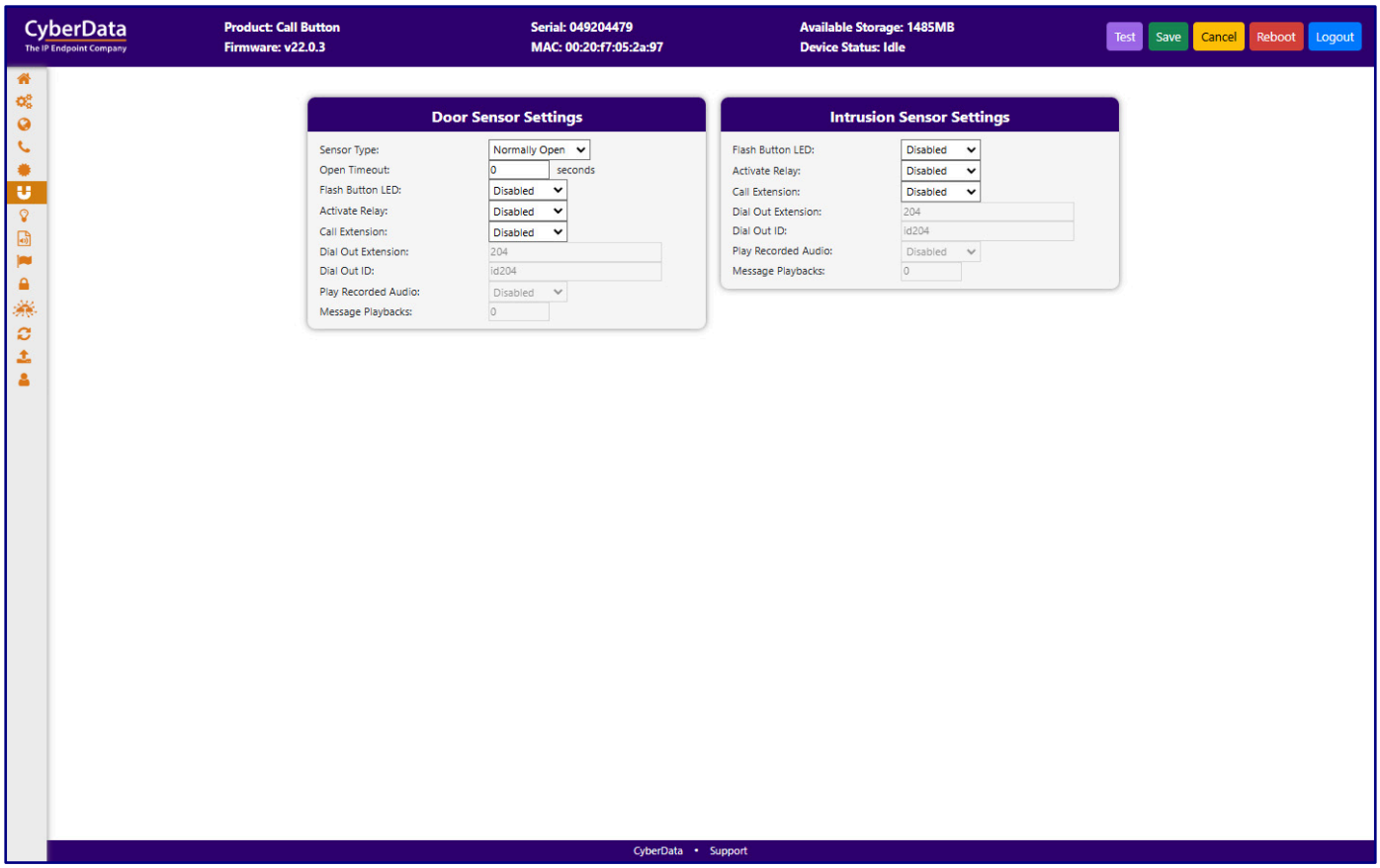
The intrusion sensor is an optical sensor installed on the device board and will be activated when the device is removed from the case.

Each sensor can trigger up to three different actions:

- Flash the LED until the sensor is deactivated (roughly 10 times/second)
- Activate the relay until the sensor is deactivated
- Call an extension and play a pre-recorded audio file

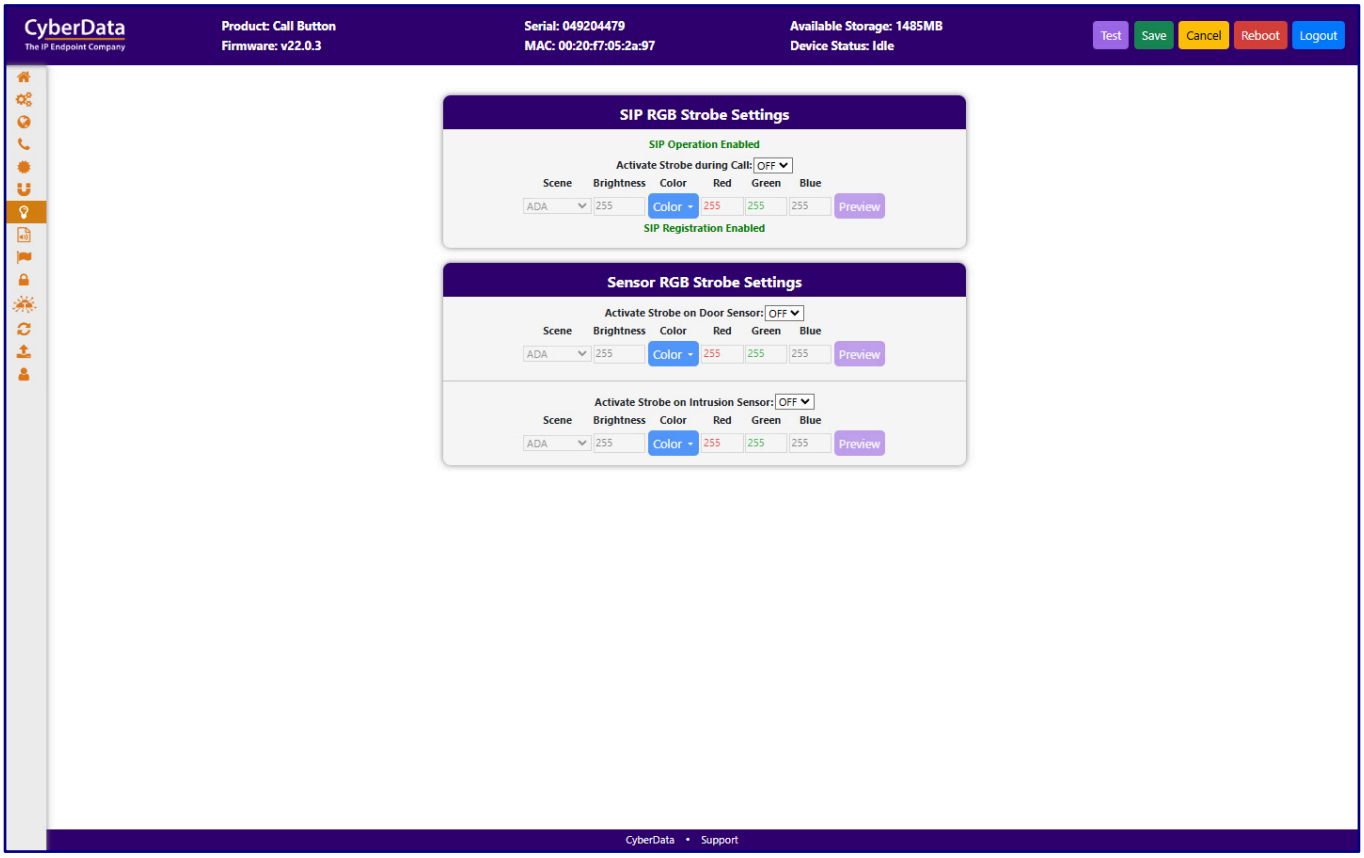
Note Calling a preset extension can be set up as a point-to-point call, but currently can't send delayed DTMF tones.

Figure 14. Sensor Page



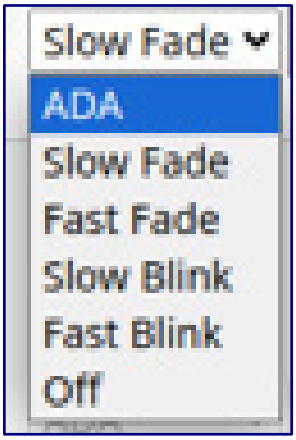
2.8 Strobe

Figure 15. Strobe Page



For each option, there are 5 scenes available:

Figure 16. 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 17. 10 Colors

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 device.

Figure 18. Audiofiles Page (1 of 2)

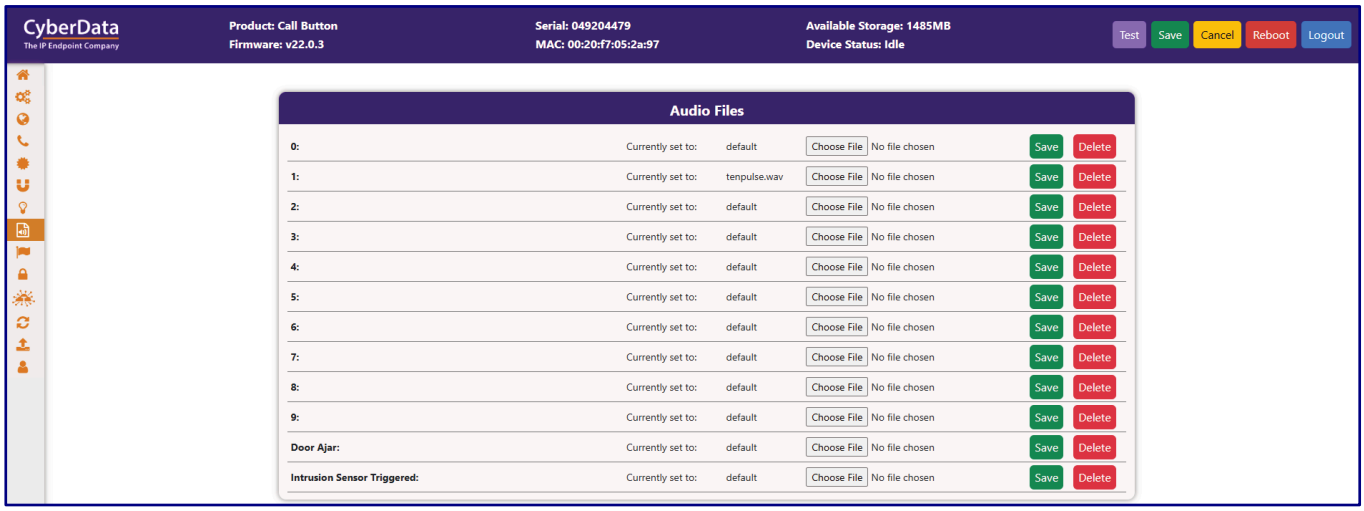
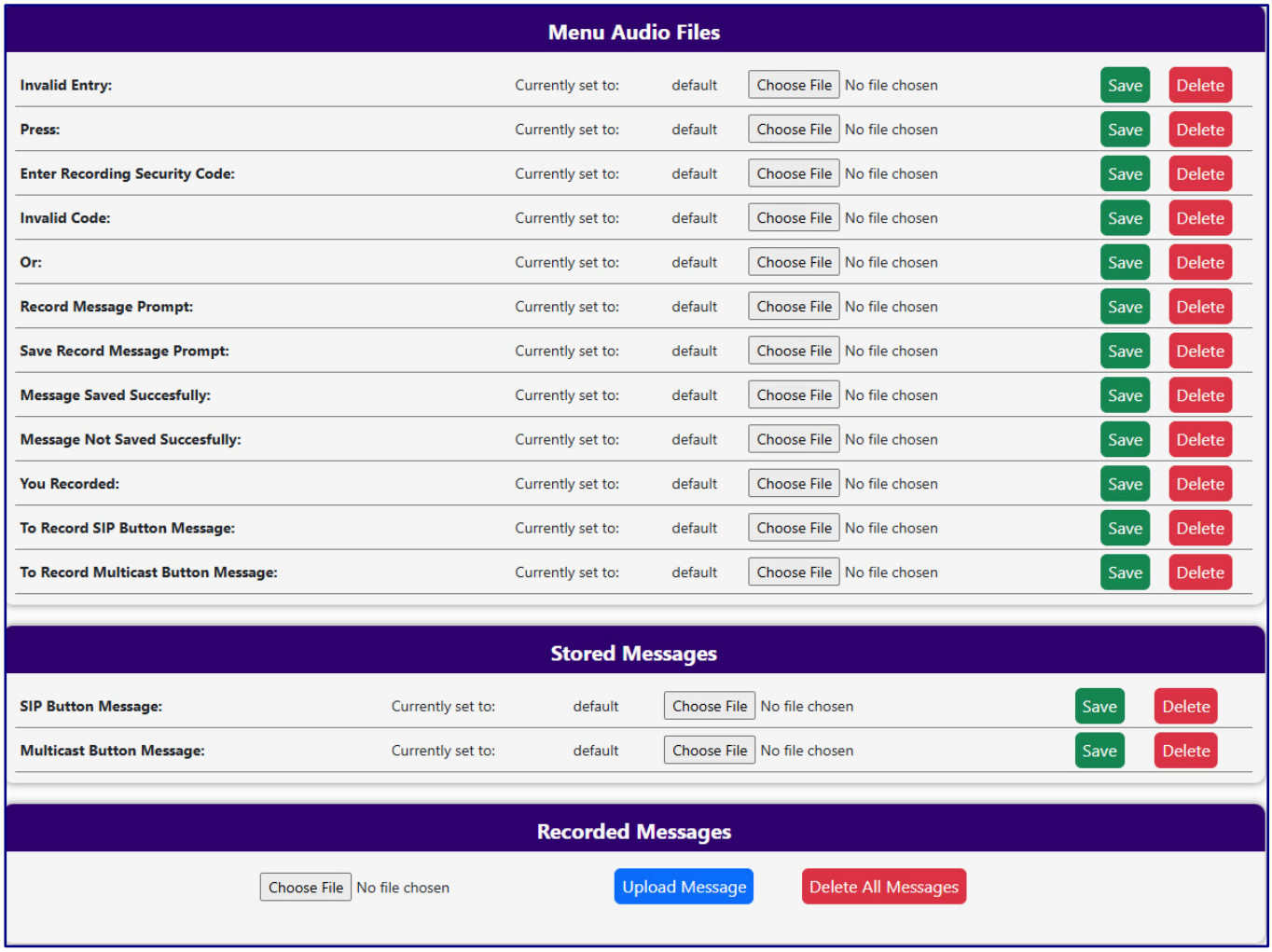


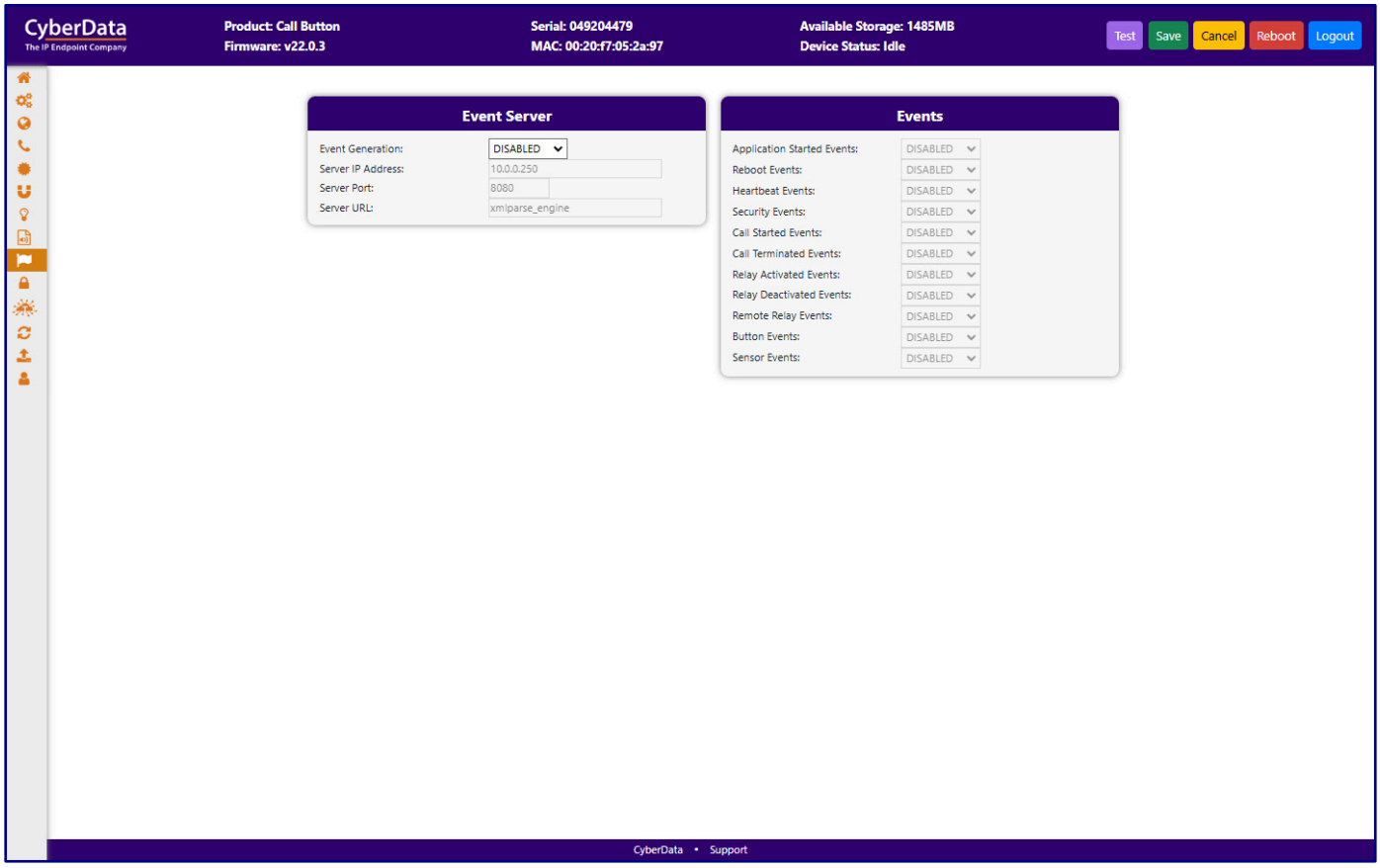
Figure 19. Audiofiles Page (2 of 2)



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 device.

Figure 20. Events Page



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.

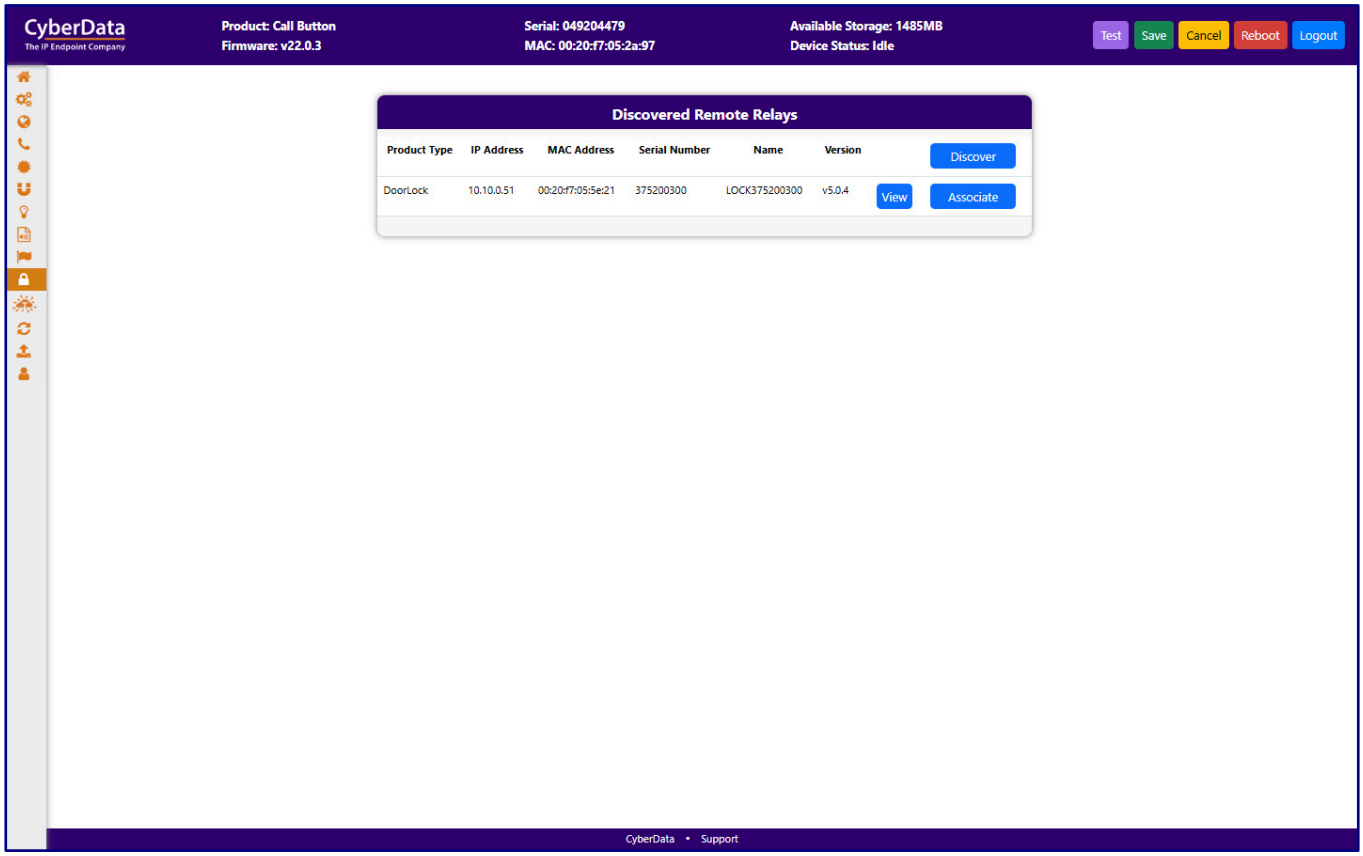
Here are example packets for every event:

```
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>APPLICATION_STARTED</event>
</cyberdata>


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

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


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

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

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

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

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

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

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

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

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

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

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

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

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

2.11 Remote Relay

Figure 21. Remote Relay Page

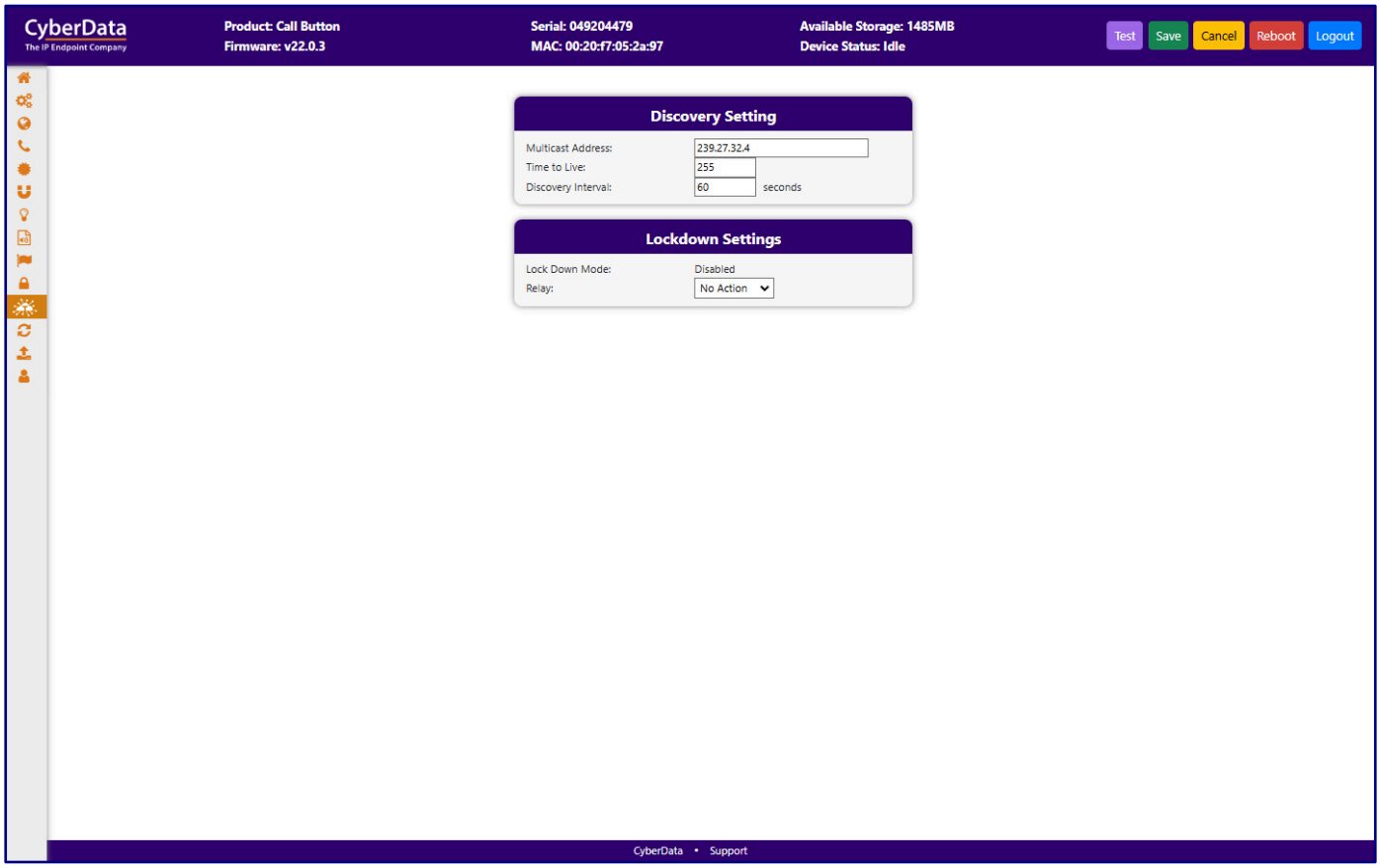


2.12 Terminus

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

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

Figure 22. Terminus Page



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.

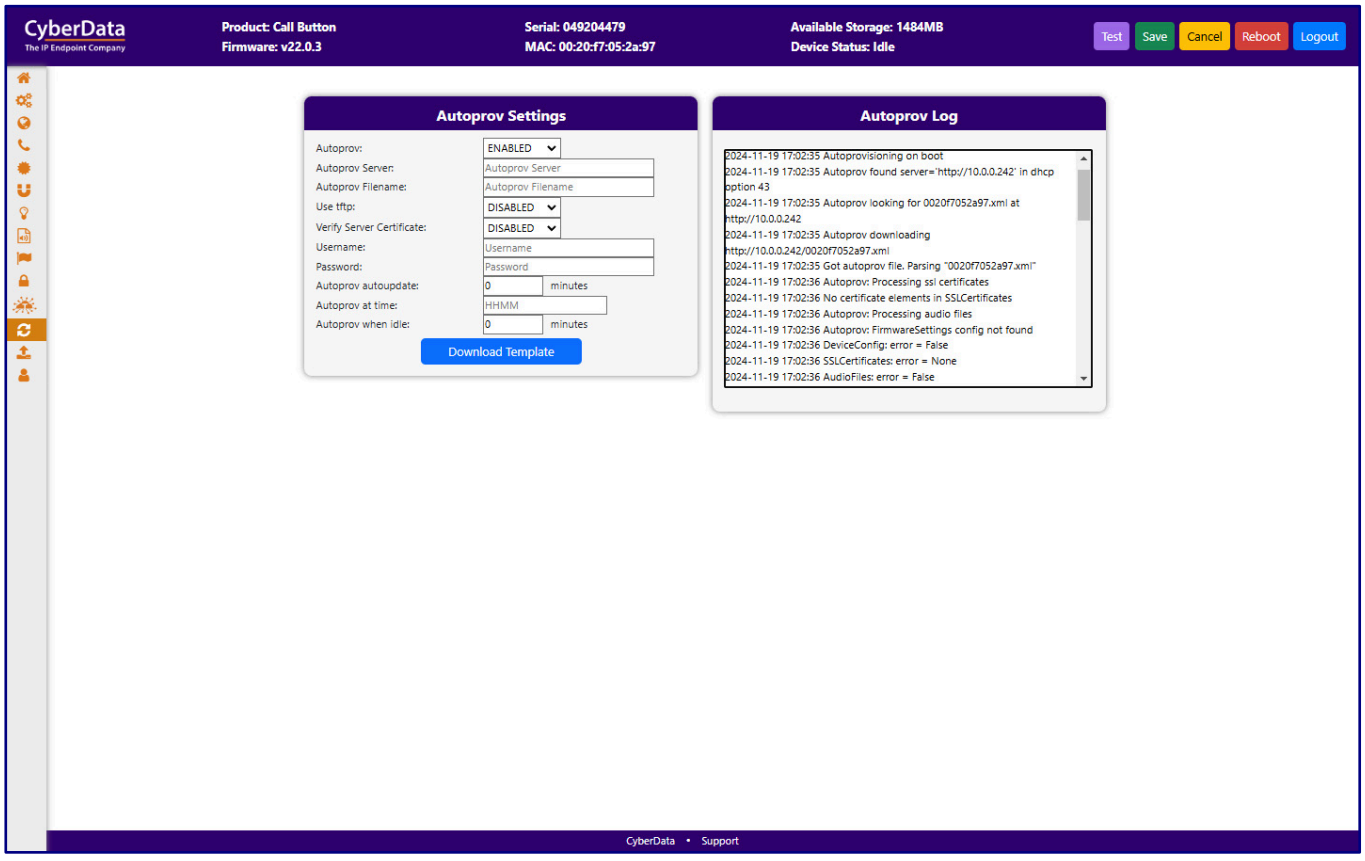
If a file is named, it will be downloaded instead of <mac address>.xml.

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 23. Autoprovisioning Page



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

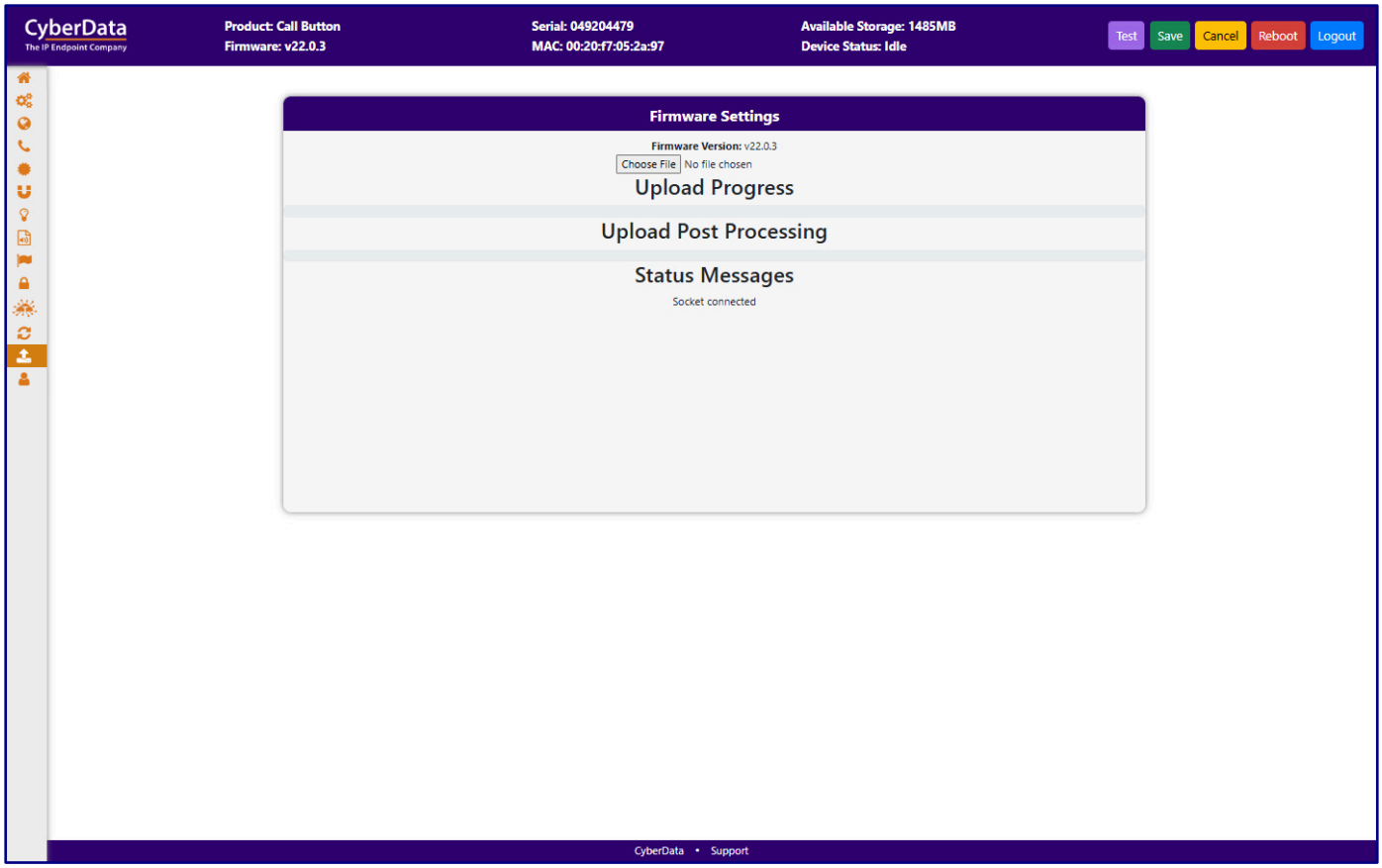
2. Unzip the firmware version file. This file may contain the following:

- Firmware file
- Release notes
- Autoprovisioning template

Caution

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

Figure 24. Firmware Page

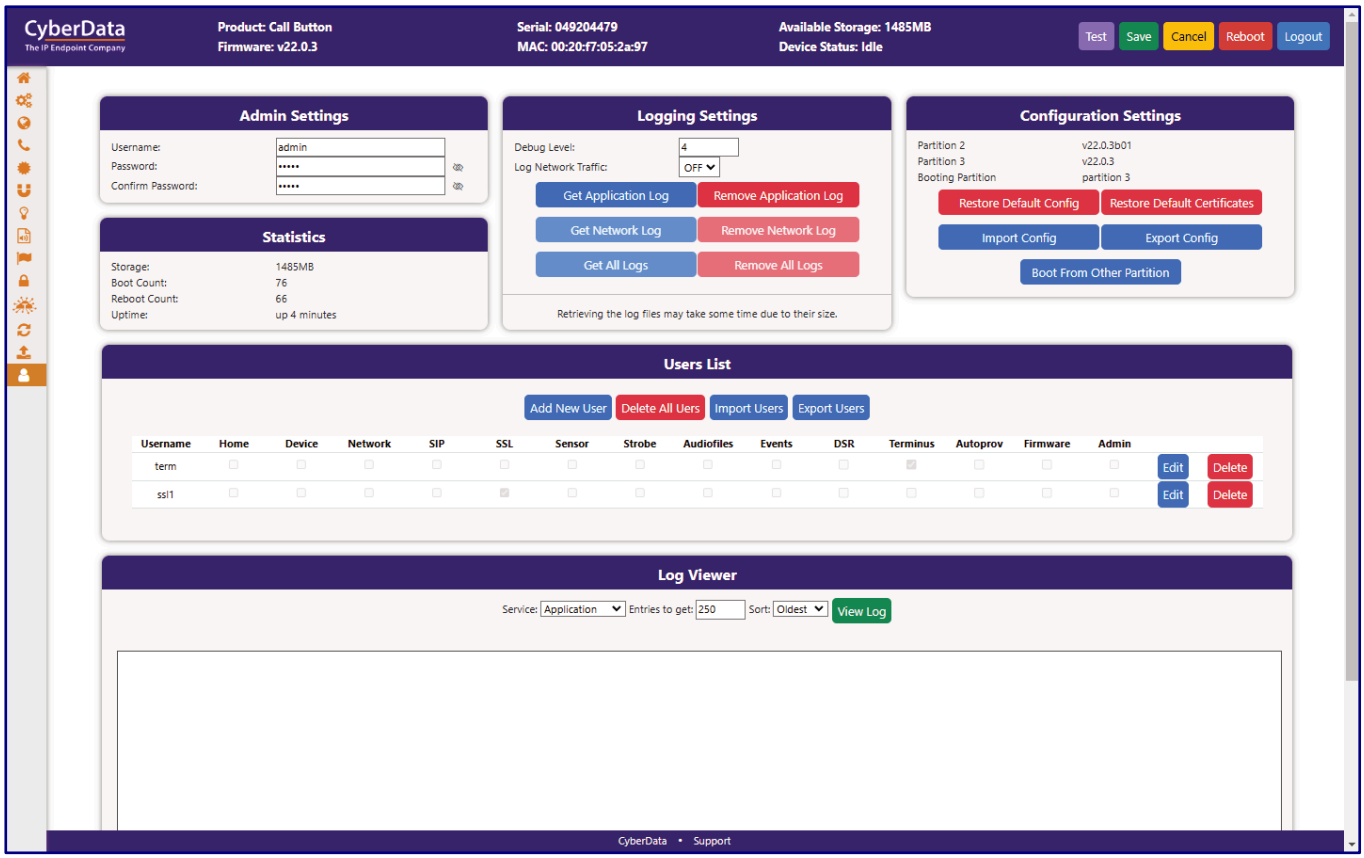


2.15 Admin

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

Note Two factor authentication is enabled here.

Figure 25. Admin Page



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 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

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

Table 2. Command Interface Post Commands

Device Action	HTTP Post Command[1]
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"
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"

[1]Type and enter all of each http POST command on one line.

Index

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/