CyberData
The IP Endpoint Company

SIP Dual Relay Controller Operations Guide

Part #*011484*

Document Part #*931778D*
for Firmware Version *22.0.1*

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

SIP Dual Relay Controller Operations Guide 931778D
Part # 011484

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 931778D, which corresponds to firmware version 22.0.1, was released on June 2, 2025, and has the following changes:

- Updates Chapter 2, “Configure the Device for the new Terminus firmware.

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 device 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

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 Product Overview and Setup

1.1 Typical System Installation

The following figures illustrate how the SIP Dual Relay Controller can be installed as part of a VoIP phone system.

Warning

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

Figure 1-1. Single Door Typical Use Case

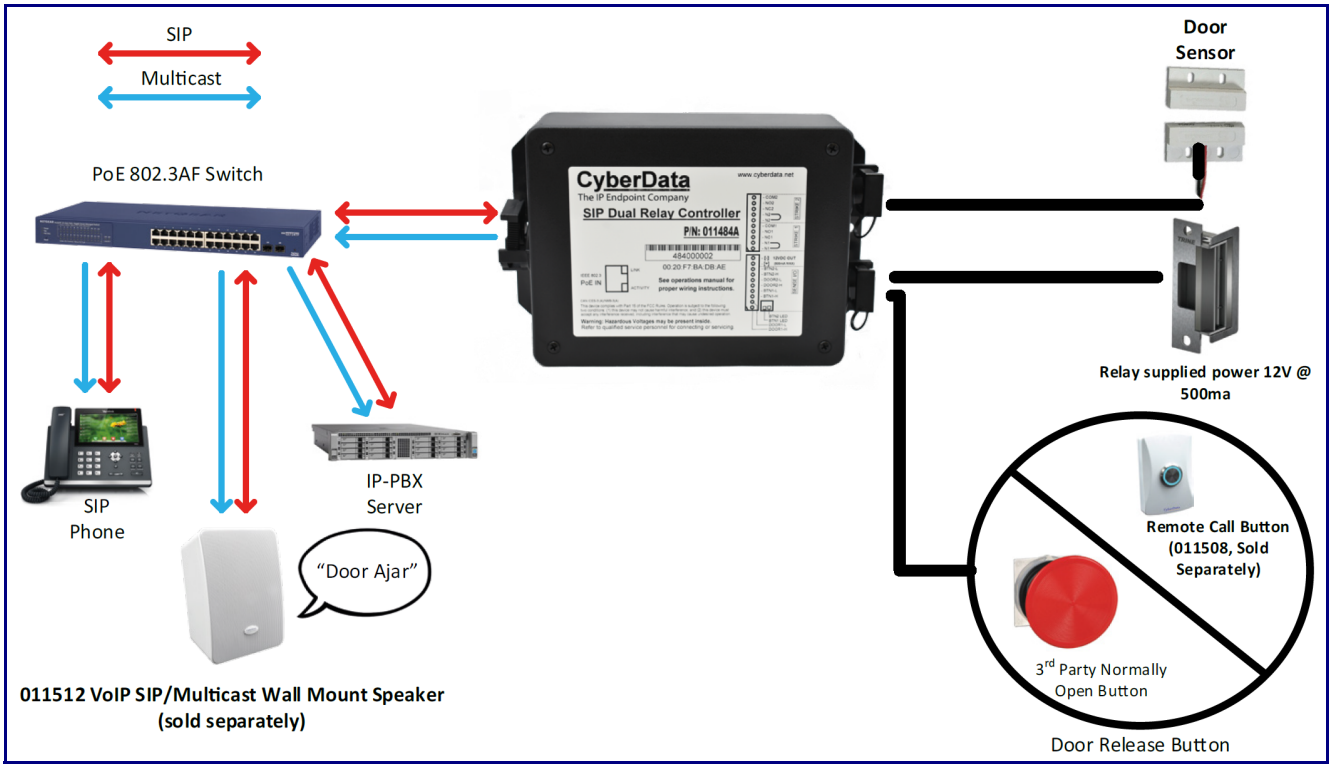


Figure 1-2. Typical Air Lock Use Case

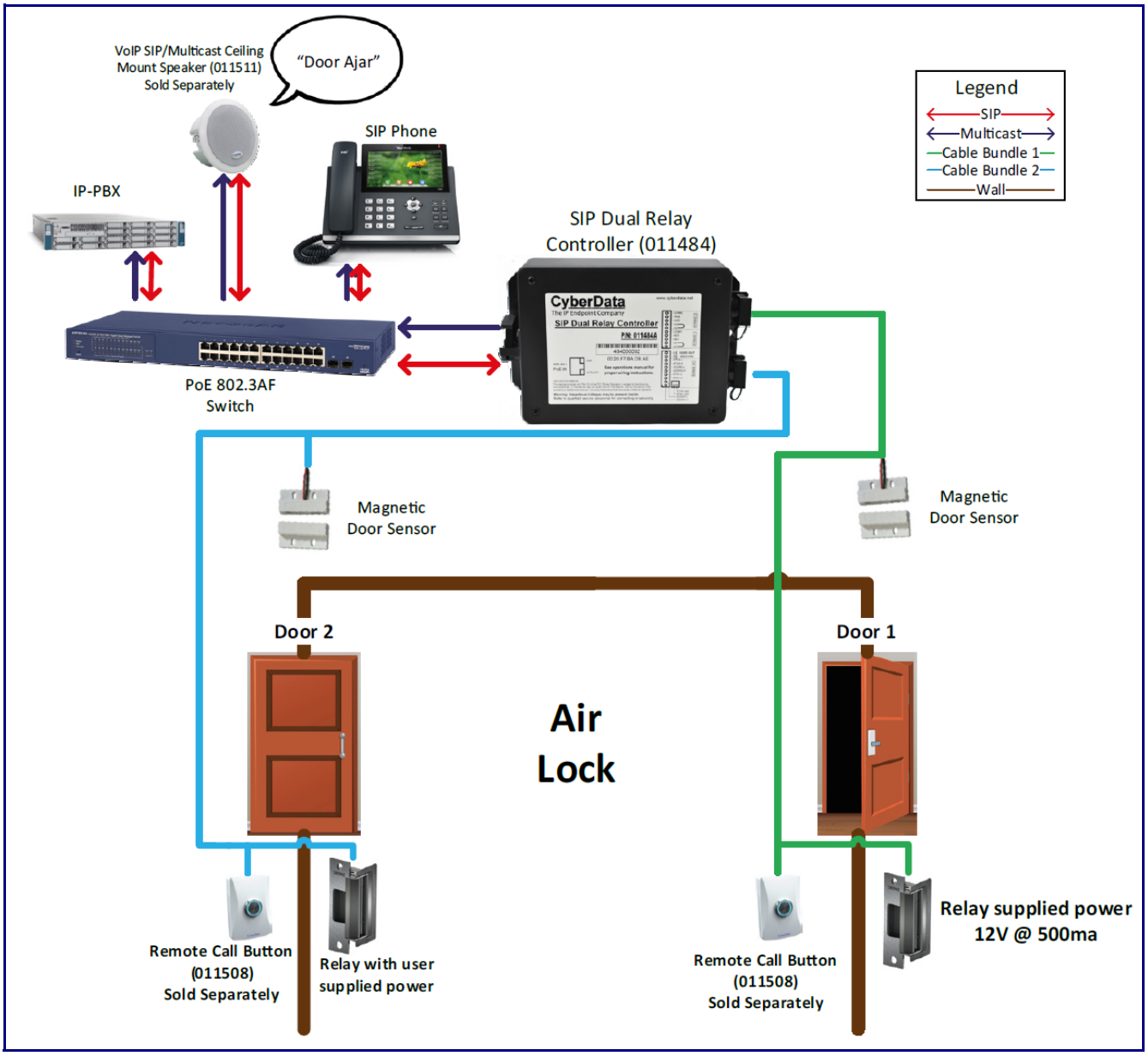


Figure 1-3. Wiring

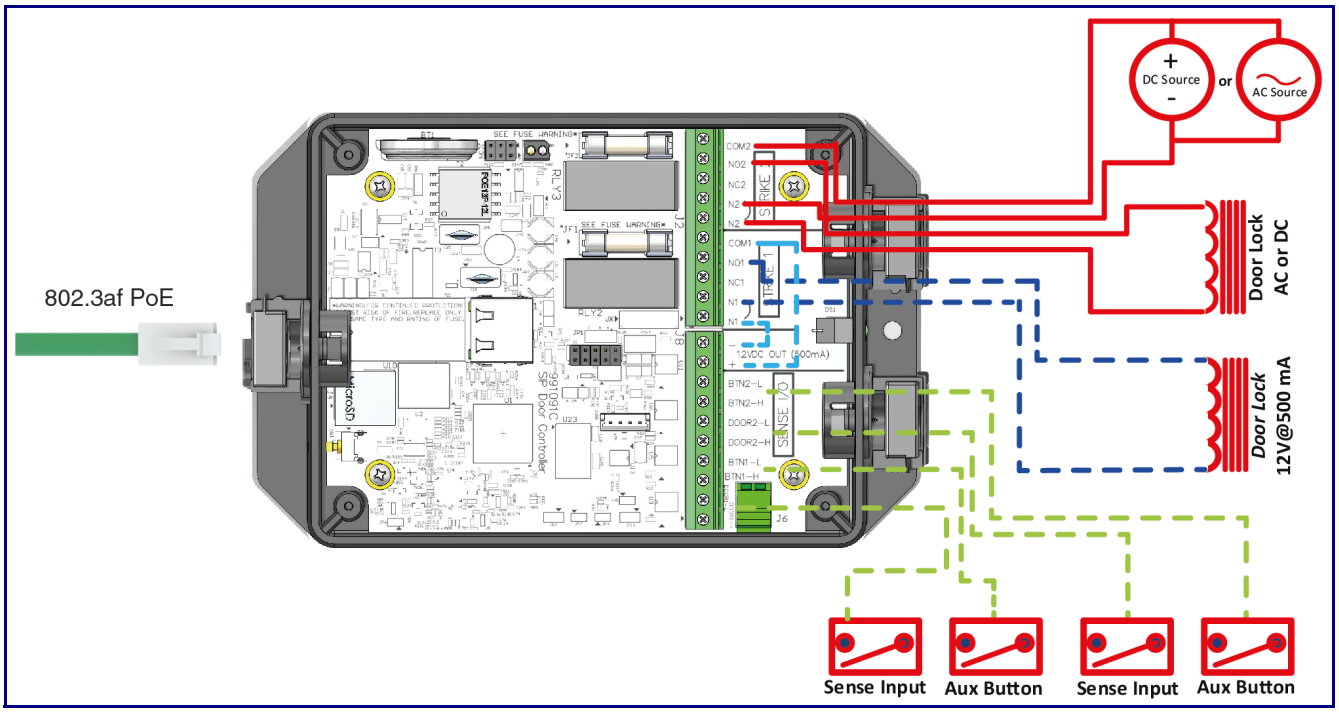


Figure 1-4. Wiring Example with a HES 1500 Electric Strike Using Internal Power Supply

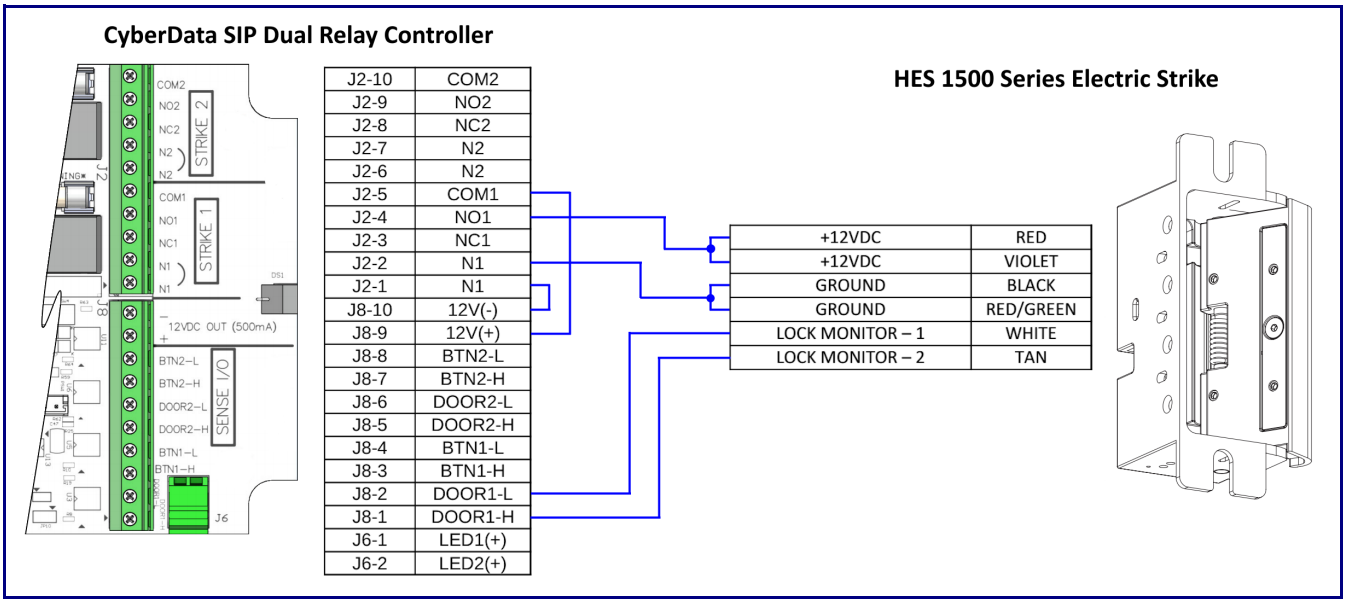
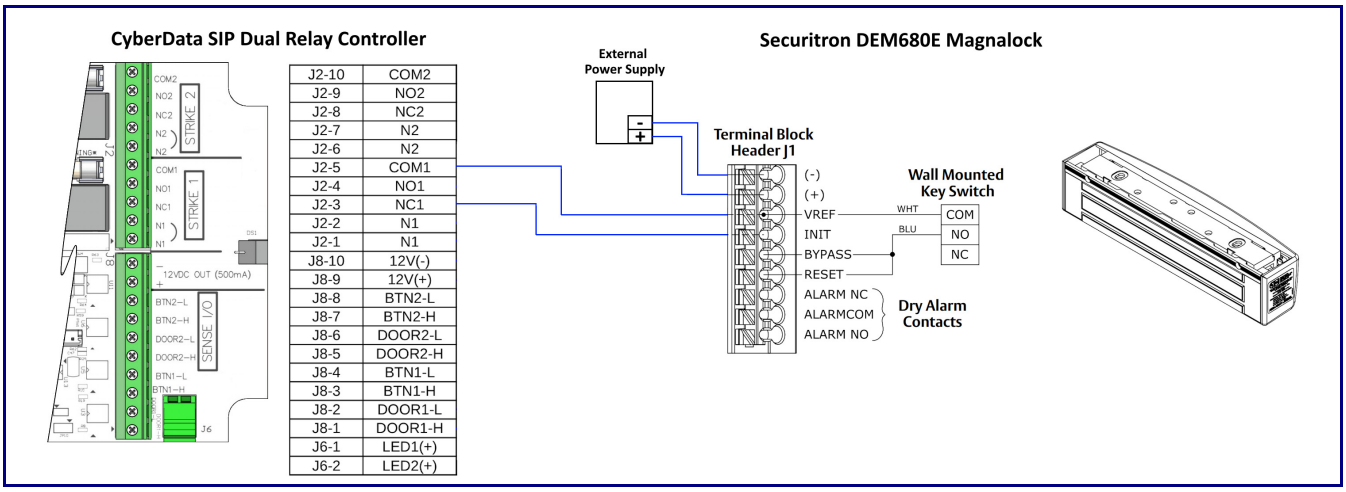
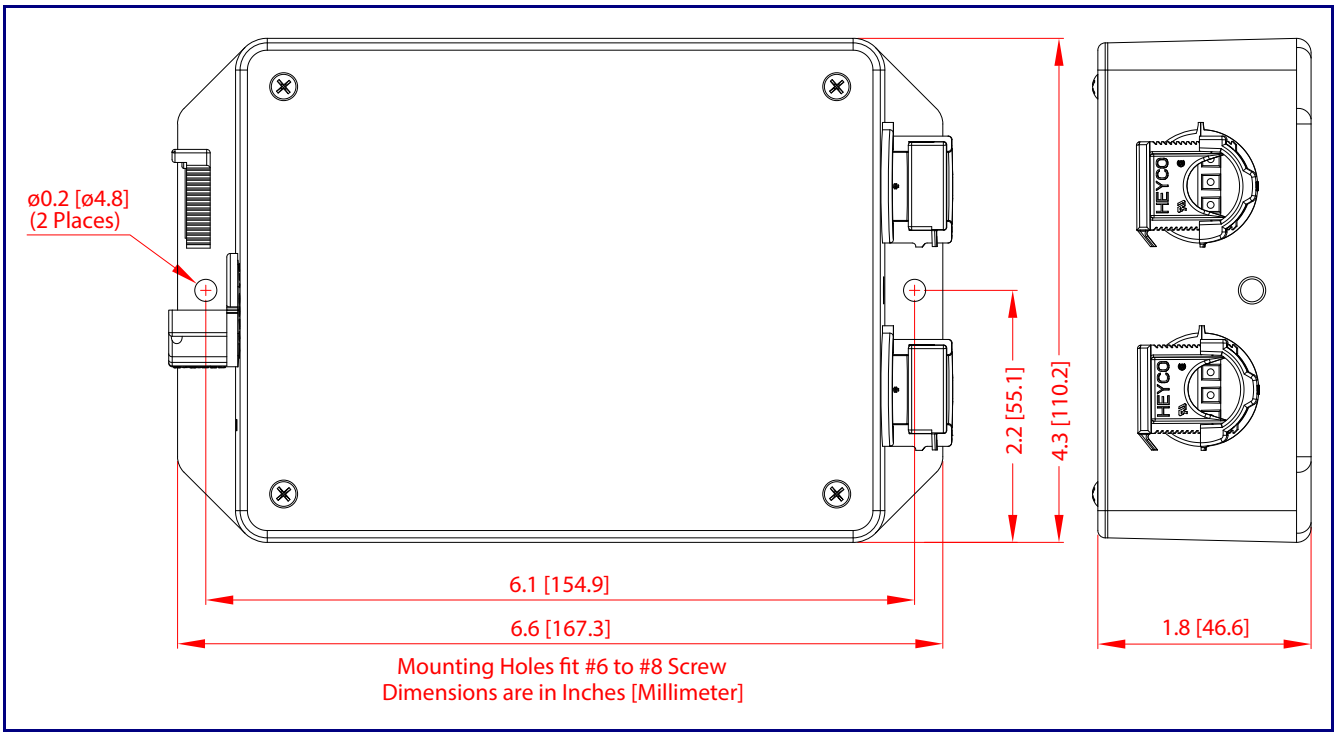


Figure 1-5. Wiring Example with a Securitron DEM680E Magnalock Using External Power Supply



1.2 Dimensions

Figure 1-6. Dimensions



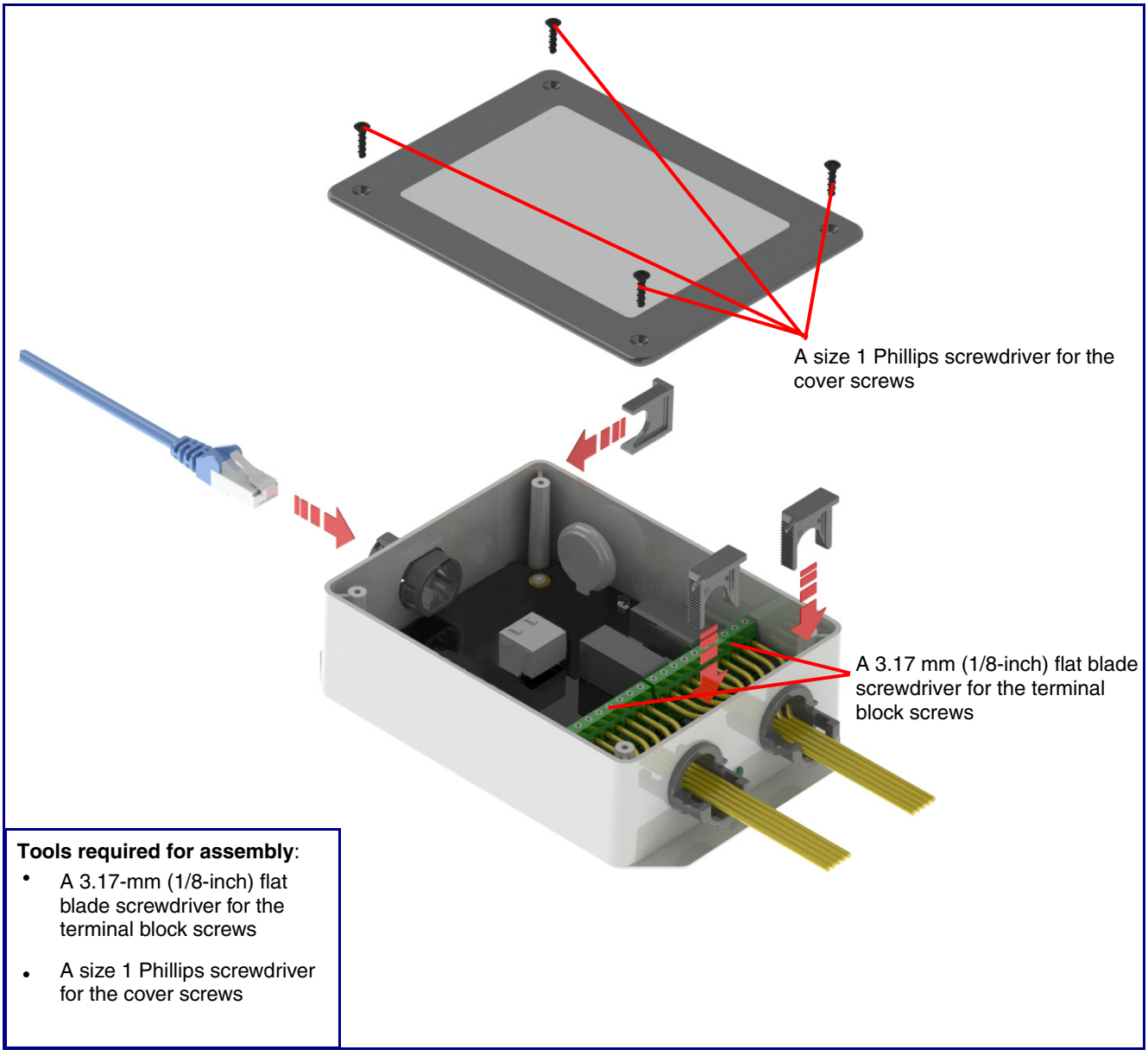
1.3 SIP Dual Relay Controller Components

Figure 1-7 shows the components of the SIP Dual Relay Controller.

Figure 1-7. SIP Dual Relay Controller Components

1.4 Assembly

Figure 1-8. Assembly



Tools required for assembly:

- A 3.17-mm (1/8-inch) flat blade screwdriver for the terminal block screws
- A size 1 Phillips screwdriver for the cover screws

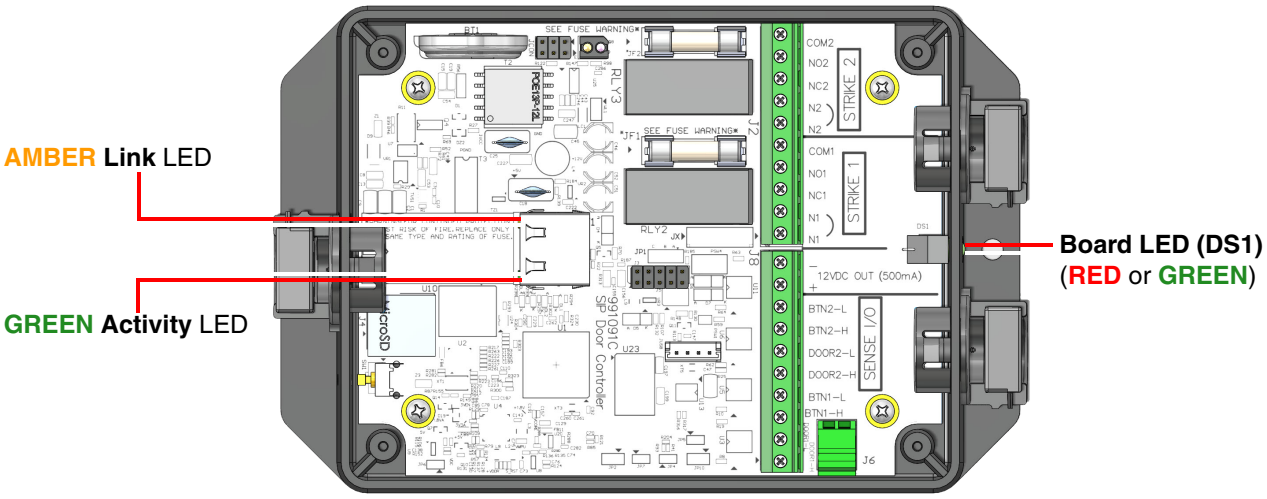
1.5 LED Behavior

See Table 1-1 and Figure 1-9 for the meaning of the device's LED behavior.

Table 1-1. LED Behavior

Status and Link LEDs (at J1):	
LED Behavior	**Means**
The **AMBER Status** LED is on and the **GREEN Link** LED is on and blinking.	No fault detected. The device is on the network and the device is not active.
Note: On boot, within approximately three seconds, the **AMBER Status** LED and the **GREEN Link** LED come on with the **GREEN Link** LED beginning to blink almost immediately.	
Board LED (DS1):	
LED Behavior	**Means**
On and solid **GREEN**	Neither relays nor sensors are active
Slow blinking **GREEN**	Either the relay or the sensor is active for Door/Device 2
Fast blinking **GREEN**	Either the relay or the sensor is active for Door/Device 1
On and solid **RED**	Either both relays, or a relay and a sensor are active**:** • Relay 1 and Relay 2 • Relay 1 and Sensor 2 • Sensor 1 and Relay 2 • Sensor 1 and Sensor 2

Figure 1-9. LEDs



1.6 Wiring the SIP Dual Relay Controller

1.6.1 SIP Dual Relay Controller Wiring Diagram with External Power Source

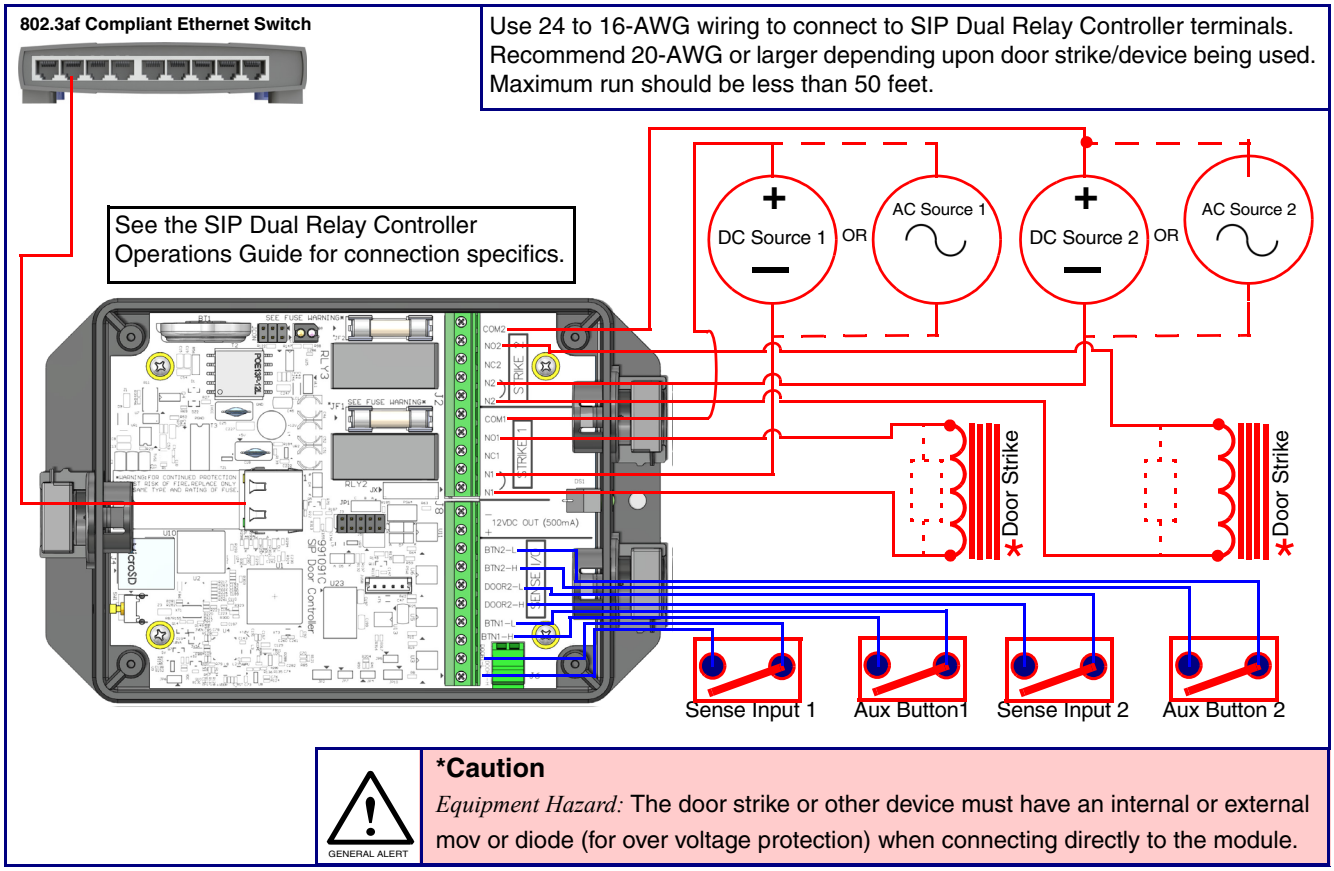
This product provides an easier method of connecting standard door strikes as well as AC and higher voltage devices. See Figure 1-10 and Figure 1-11 for the wiring diagrams.

GENERAL ALERT

Warning

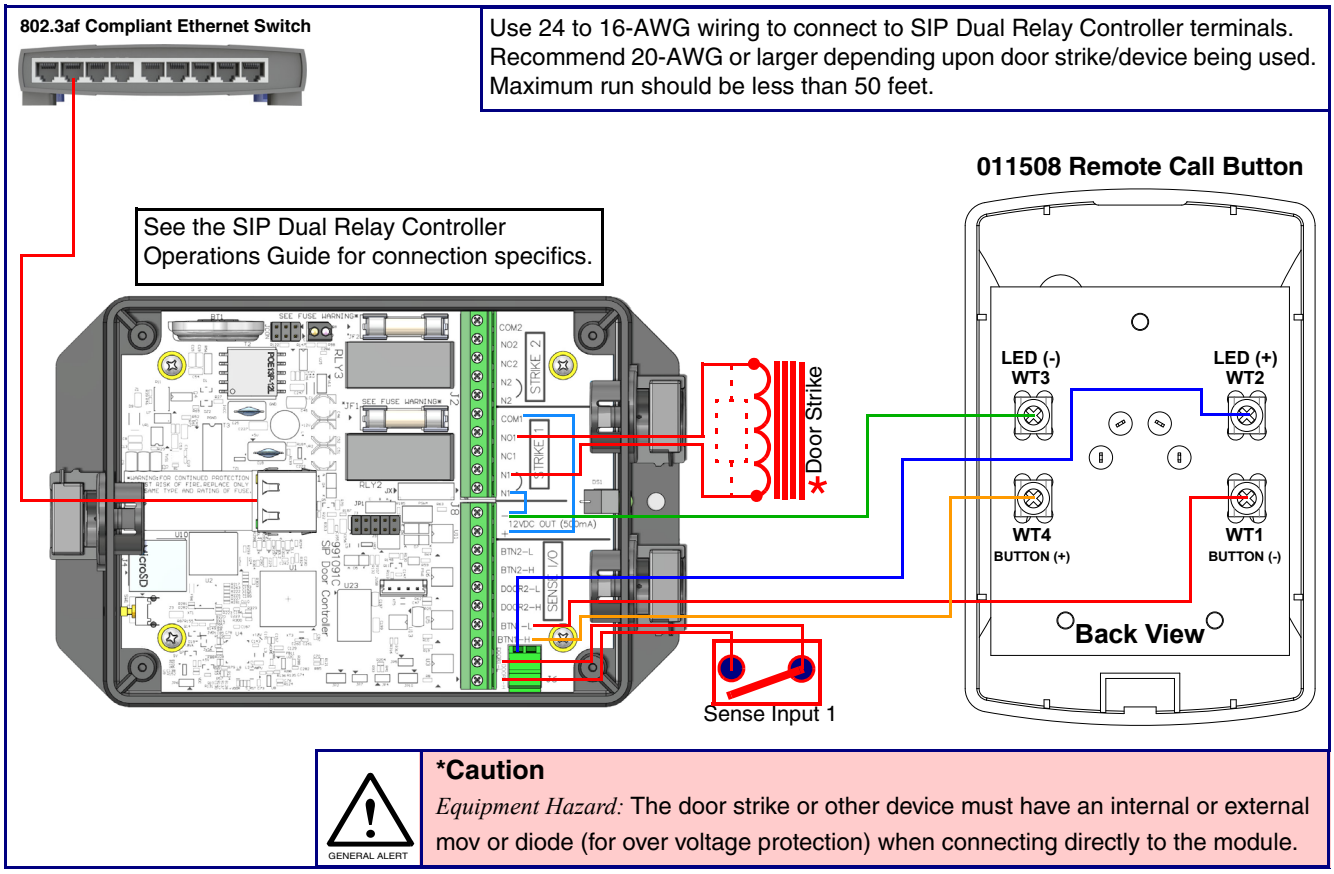
Electrical Hazard: Hazardous voltages may be present. No user serviceable part inside. Refer to qualified service personnel for connecting or servicing.

Figure 1-10. SIP Dual Relay Controller Wiring Diagram with External Power Source



1.6.2 Example Diagram Using PoE Power and One SIP Dual Relay Controller with the 011508 Remote Call Button

Figure 1-11. Diagram Using PoE Power and One SIP Dual Relay Controller with the 011508 Remote Call Button[1]



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.This Diagram shows one button and one device control example. This controller supports a second set (button/device control). If a second button/device control is needed, use Button-2 and Strike-2 connections.

1.7 Terminal Block Wiring Connections

See Figure 1-12 and Table 1-2 for the terminal block wiring connections.

Figure 1-12. Terminal Block Wiring Connections

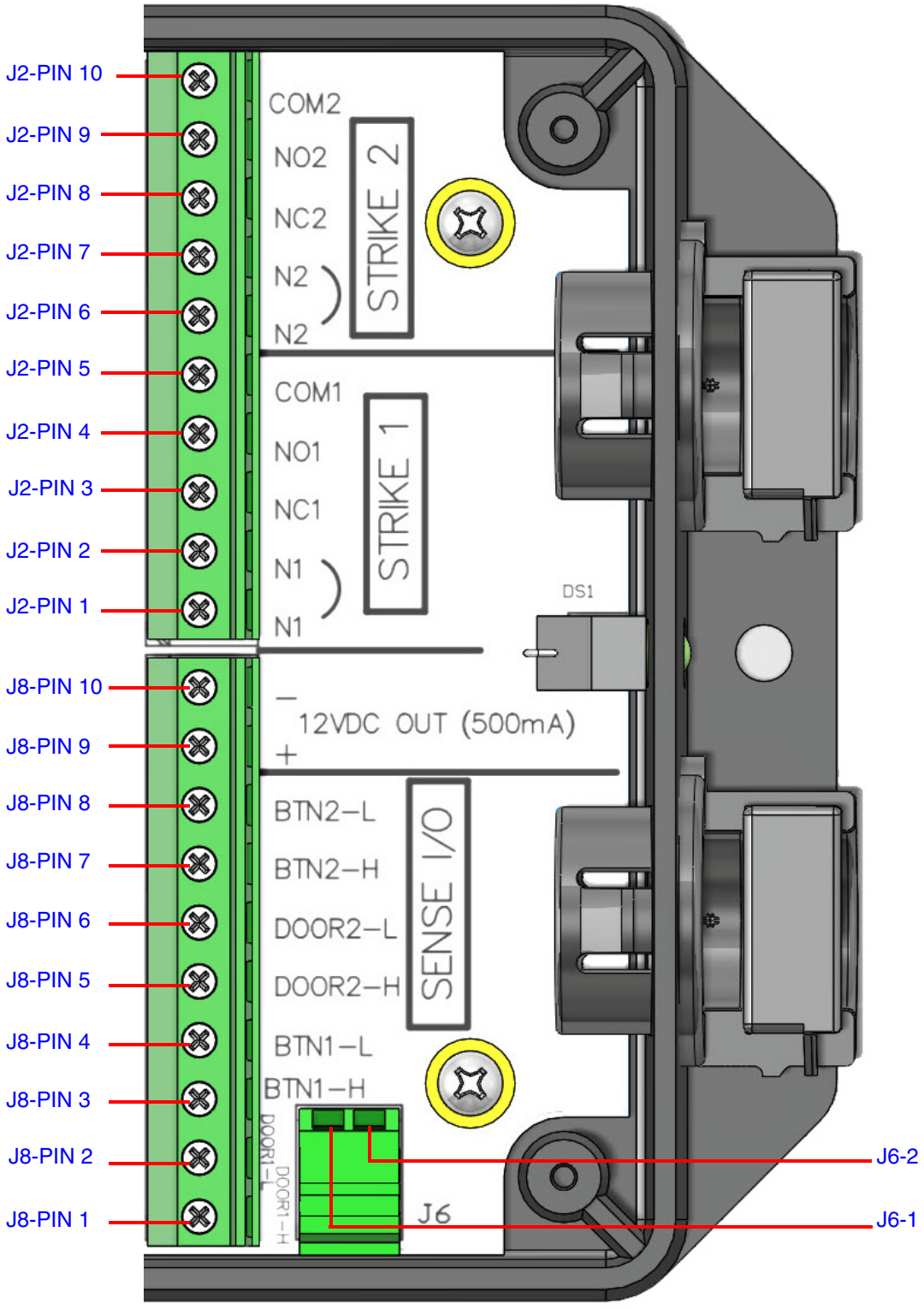


Table 1-2. Terminal Block Wiring Connections

Connections	Silkscreen Label	Description
J2-PIN 1	N1	Door Strike 1: Neutral or common tie point. Allows the user to tie the power source and door strike commons together internally to the box.
J2-PIN 2	N1	
J2-PIN 3	NC1	Door Strike 1: Normally closed relay contact
J2-PIN 4	NO1	Door Strike 1: Normally opened relay contact
J2-PIN 5	COM1	Door Strike 1: Relay common connection
J2-PIN 6	N2	Door Strike 2: Neutral or common tie point. Allows the user to tie the power source and door strike commons together internally to the box.
J2-PIN 7	N2	
J2-PIN 8	NC2	Door Strike 2: Normally closed relay contact
J2-PIN 9	NO2	Door Strike 2: Normally opened relay contact
J2-PIN 10	COM2	Door Strike 2: Relay common connection
J8-PIN 1	DOOR1-H	Door 1 sense high side connection
J8-PIN 2	DOOR1-L	Door 1 sense low side connection/Ground LED Return
J8-PIN 3	BTN1-H	Button 1 sense high side connection
J8-PIN 4	BTN1-L	Button 1 sense low side connection/Ground LED Return
J8-PIN 5	DOOR2-H	Door 2 sense high side connection
J8-PIN 6	DOOR2-L	Door 2 sense low side connection/Ground LED Return
J8-PIN 7	BTN2-H	Button 2 sense high side connection
J8-PIN 8	BTN2-L	Button 2 sense low side connection/Ground LED Return
J8-PIN 9	12V(+)	+12 V out at 500 mA
J8-PIN 10	12V(-)	Common connection for 12V output/Ground LED Return
J6-1	LED1(+)	Remote Button LED1(+)
J6-2	LED2(+)	Remote Button LED2(+)

1.8 Jumper Definitions

See Table 1-2 for the jumper definitions.

Table 1-3. Jumper Definitions

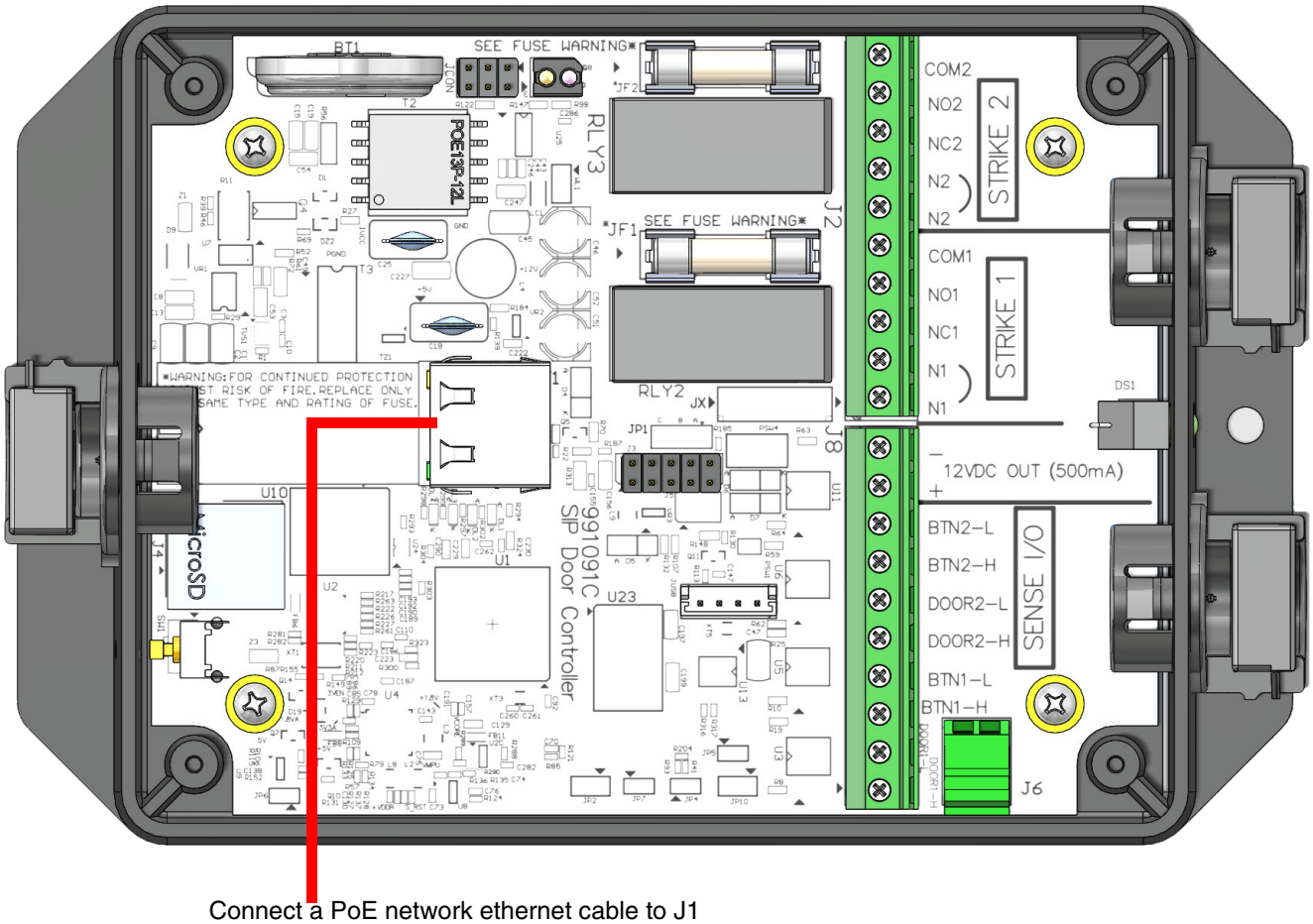
Jumper	Description
JP5	Missing Installed—Held in reset
JP10	Missing—Intrusion sensor enabled Installed—Intrusion sensor disabled

1.9 Reset to Factory Defaults

To reset the device to the original factory default settings, complete the following steps:

1. Apply power to the device by connecting a PoE network ethernet cable to J1.

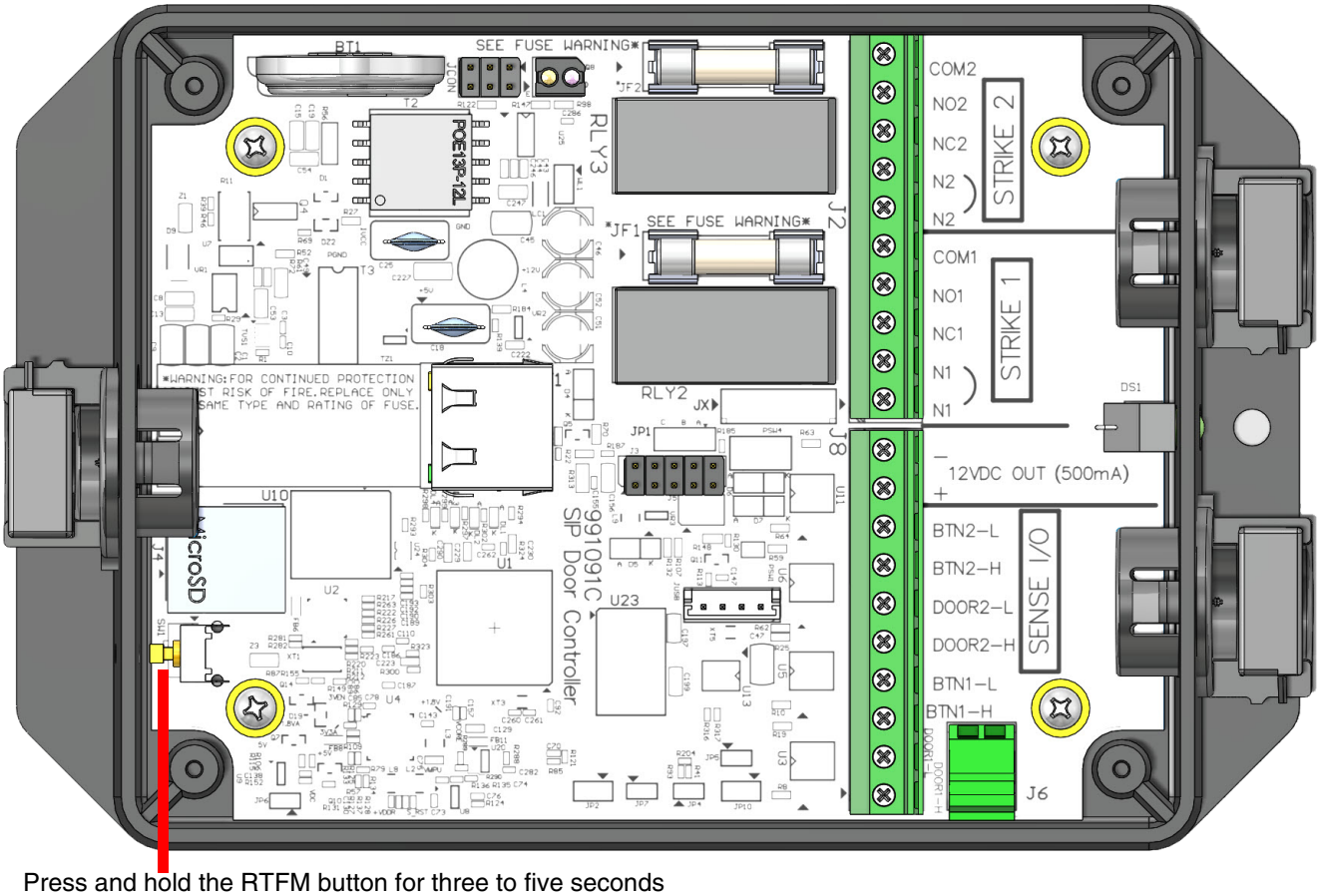
Figure 1-13. Connect a PoE network ethernet cable to J1



Connect a PoE network ethernet cable to J1

2. While the device is powered, press and hold the RTFM button for three to five seconds.

Figure 1-14. Press and hold the RTFM button for three to five seconds



Press and hold the RTFM button for three to five 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.

Table 1-4. 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 device IP address.

Note If the network does not have access to a DHCP server, the device will default to an IP address of 192.168.1.23.

Note Make sure that the PC is on the same IP network as the SIP Dual Relay Controller.

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

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

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

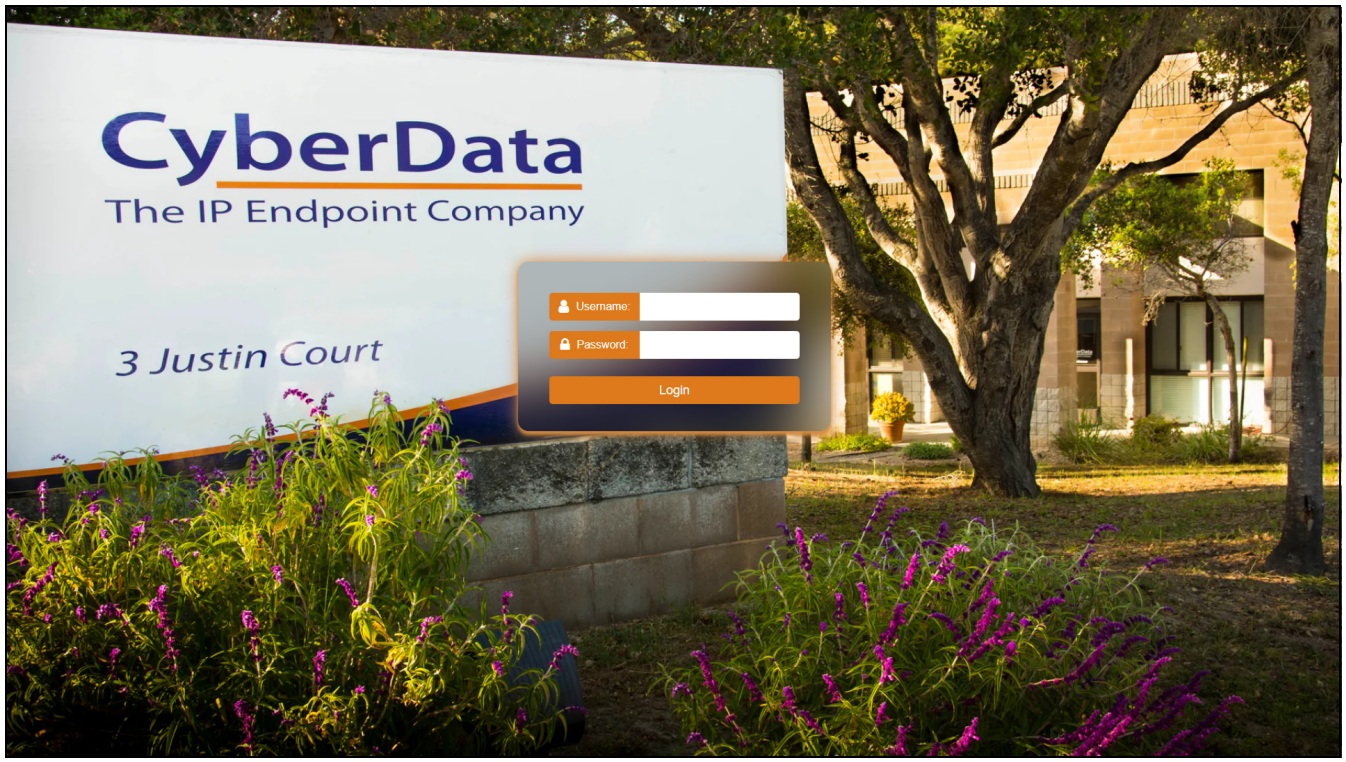
Note The Intercom ships in DHCP mode. To get to the **Home** page, use the discovery utility to scan for the device on the network and open your browser from there.

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

   Web Access Username: **admin**

   Web Access Password: **admin**

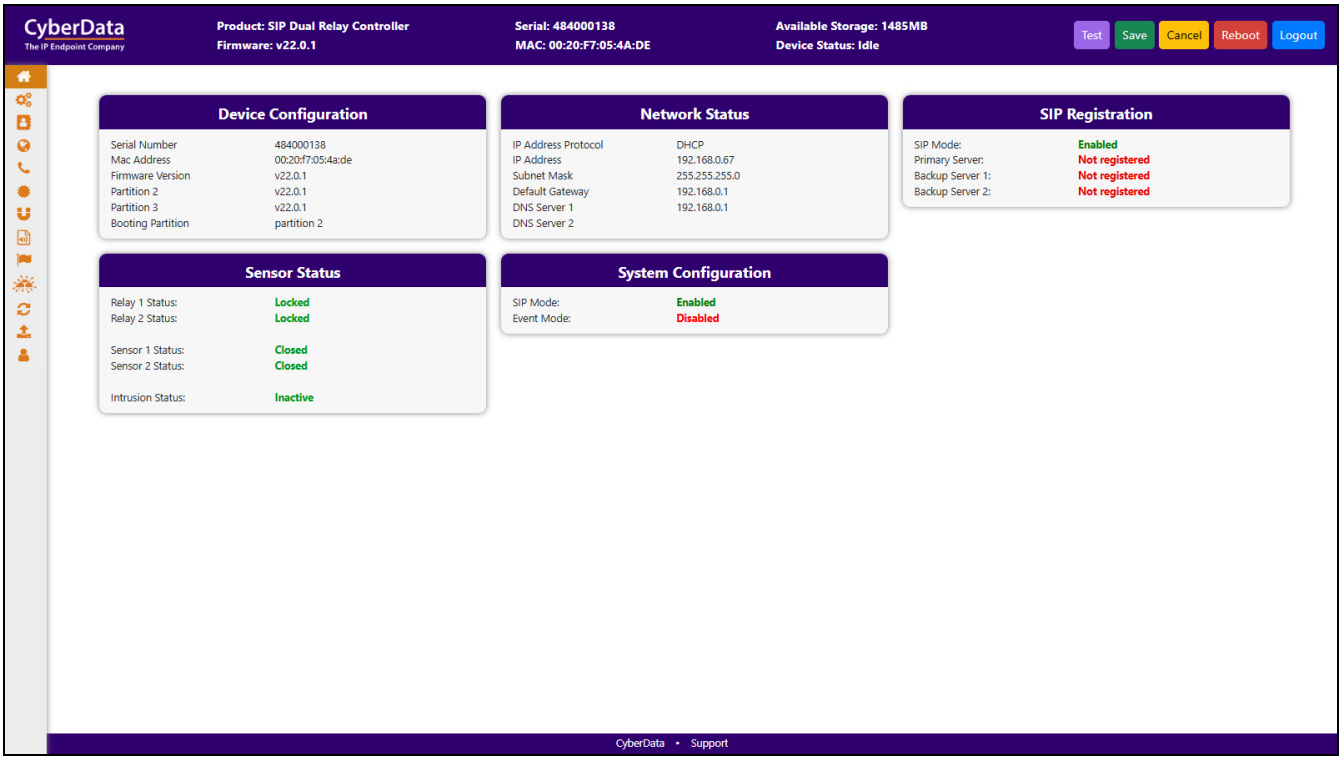
Figure 2-1. Log In Page



2.2 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 2-2. 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.

Figure 2-3. Device Configuration Page

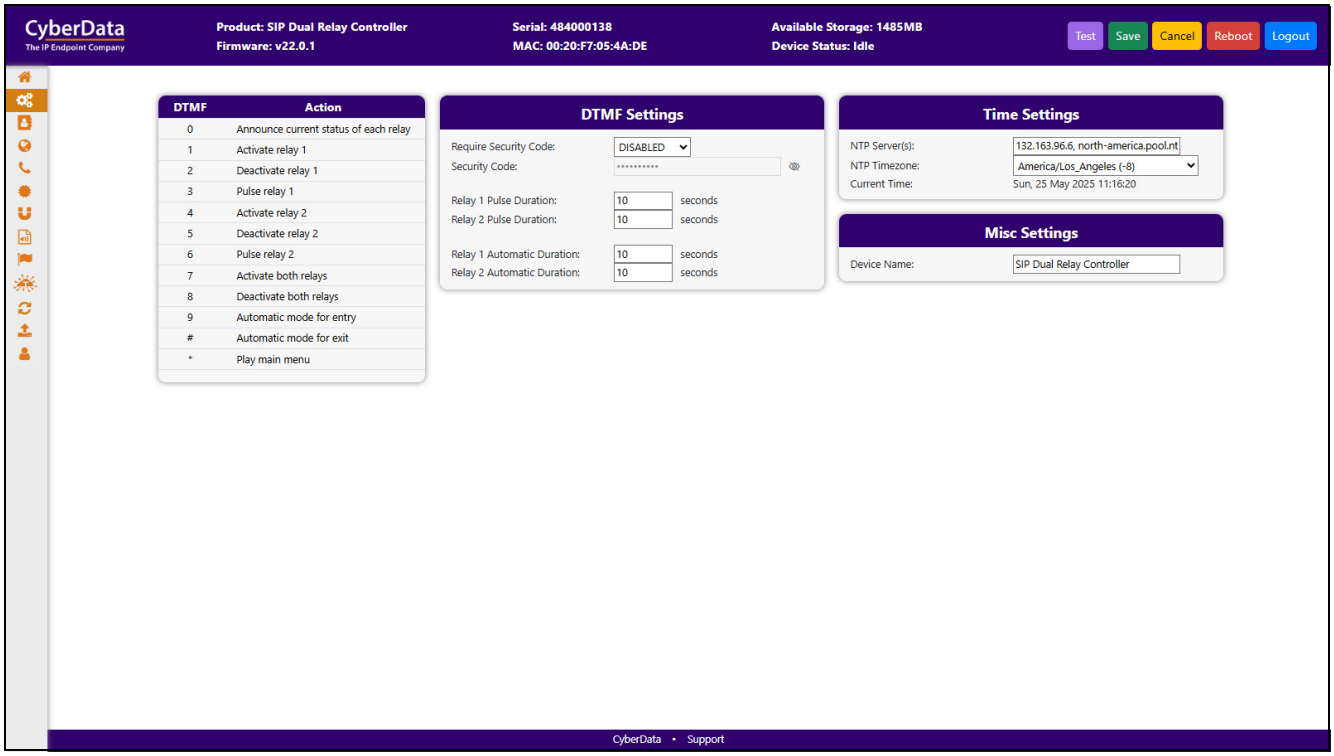


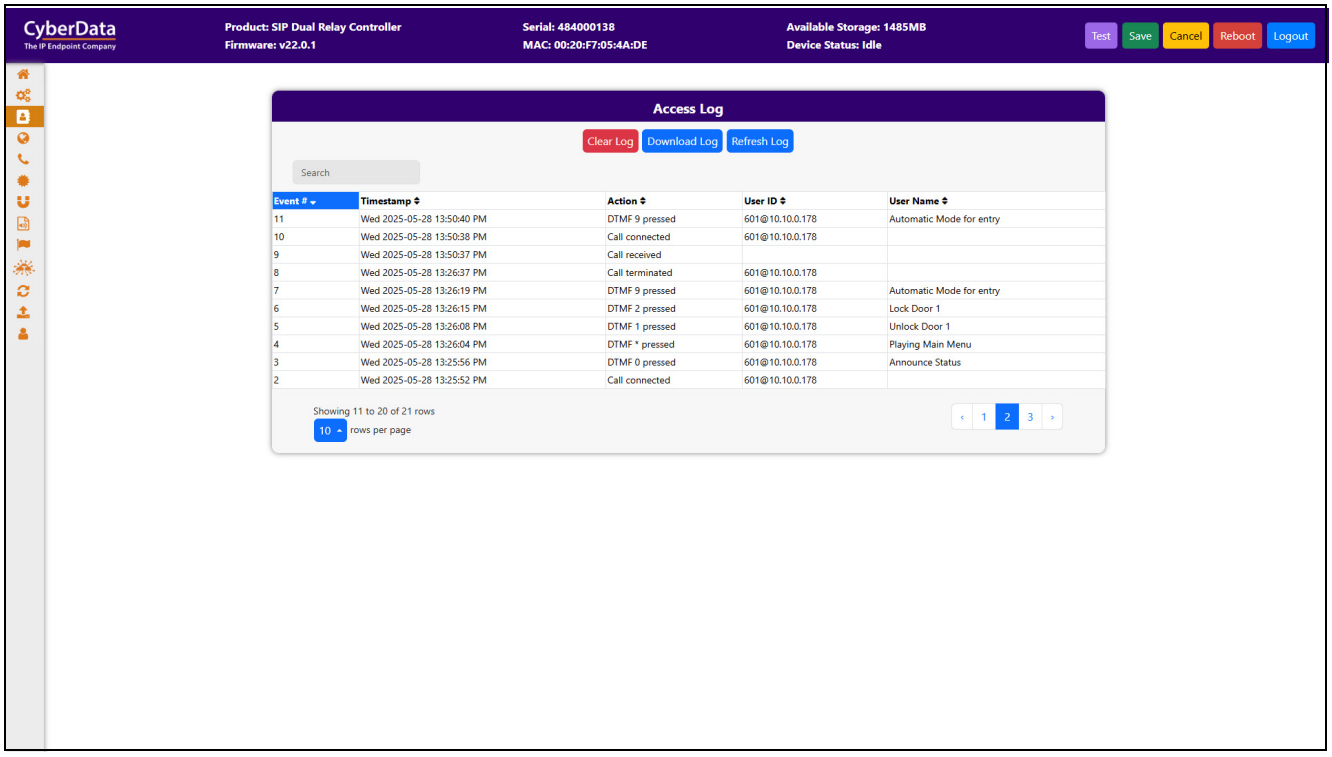
Table 2-1. Automatic mode for entry and exit

Setting	Description
Automatic mode for entry	Automatic mode (also known as an airlock) activates relay 1 until outdoor 1 is opened and closed, at which point relay 2 activates. If door 1 is not open within the time configured on the **Sensor** page, automatic mode is cancelled.
Automatic mode for exit	Automatic mode for exit initially activates relay 2.

2.4 Access Log

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

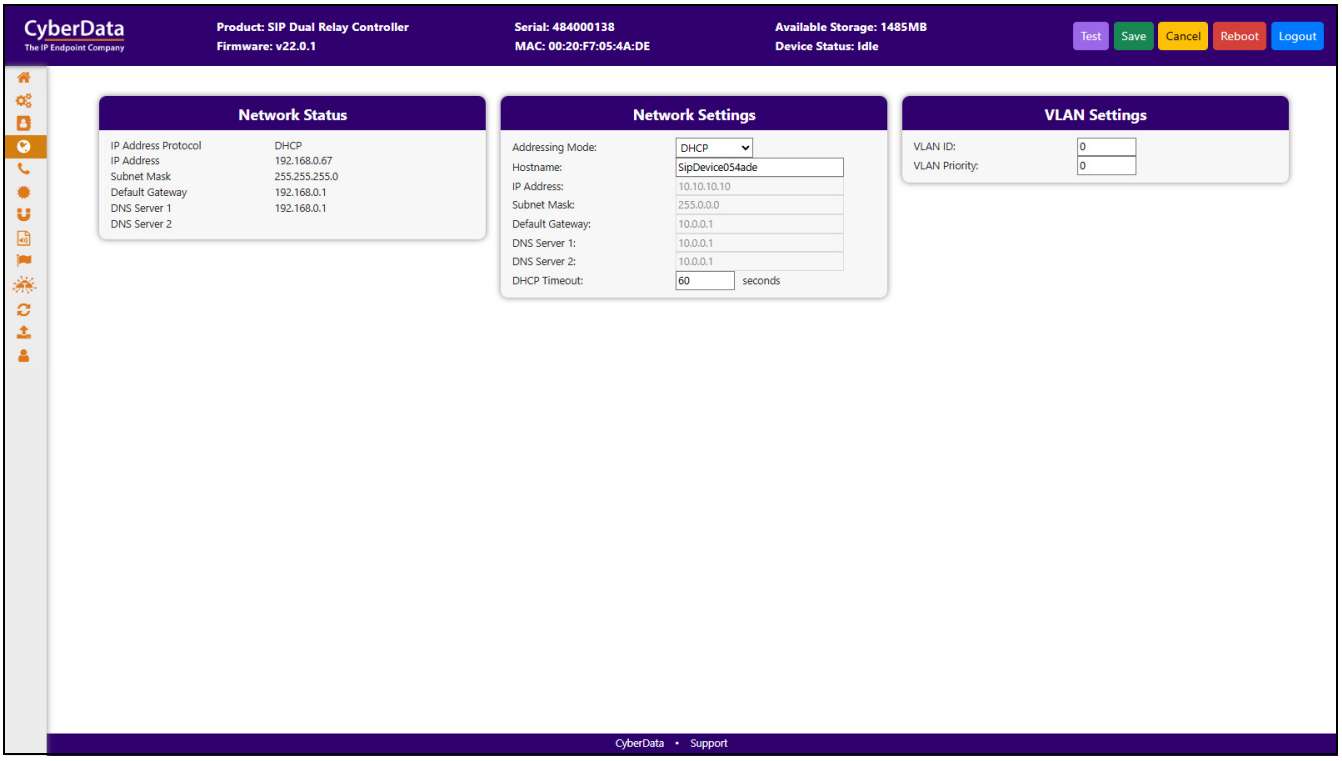
Figure 2-4. Access Log Page



2.5 Network

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

Figure 2-5. Network Page



2.6 SIP (Session Initiation Protocol)

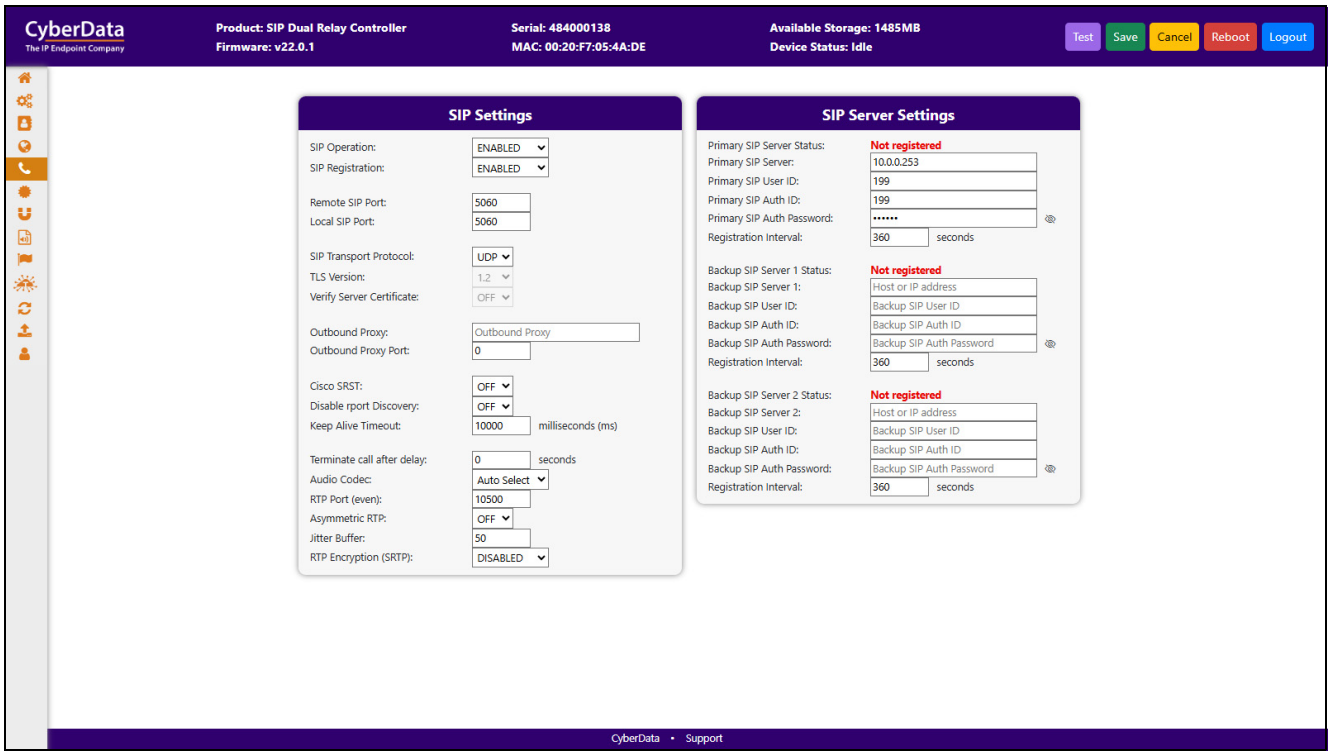
This page sets the options for phone calls. Configure up to 3 servers, with 2 acting as backup, and a server for the nightringer. The nightringer is a second sip extension that only rings, never connects to a call. Many customers use the nightringer in a Hunt/Ring Group.

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

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

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

Figure 2-6. SIP Page



2.7 SSL

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

Figure 2-7. SSL Page (1 of 2)

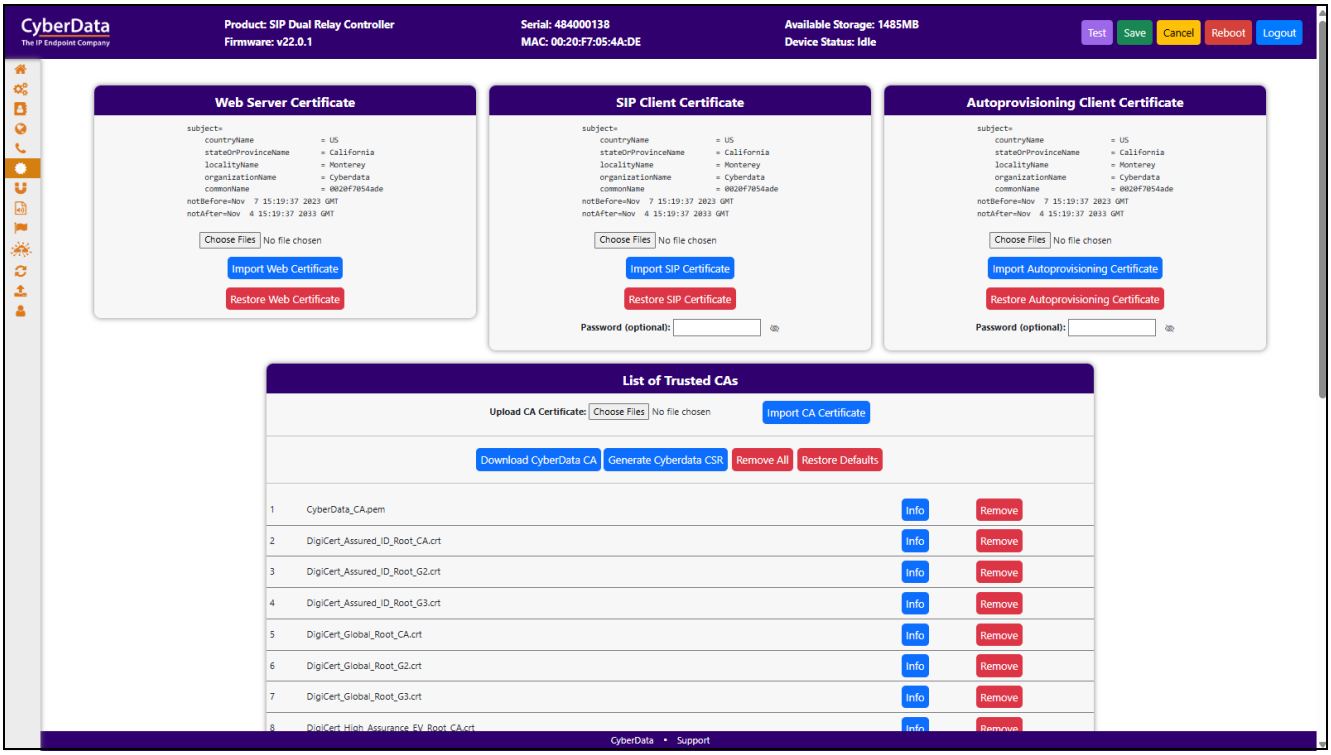
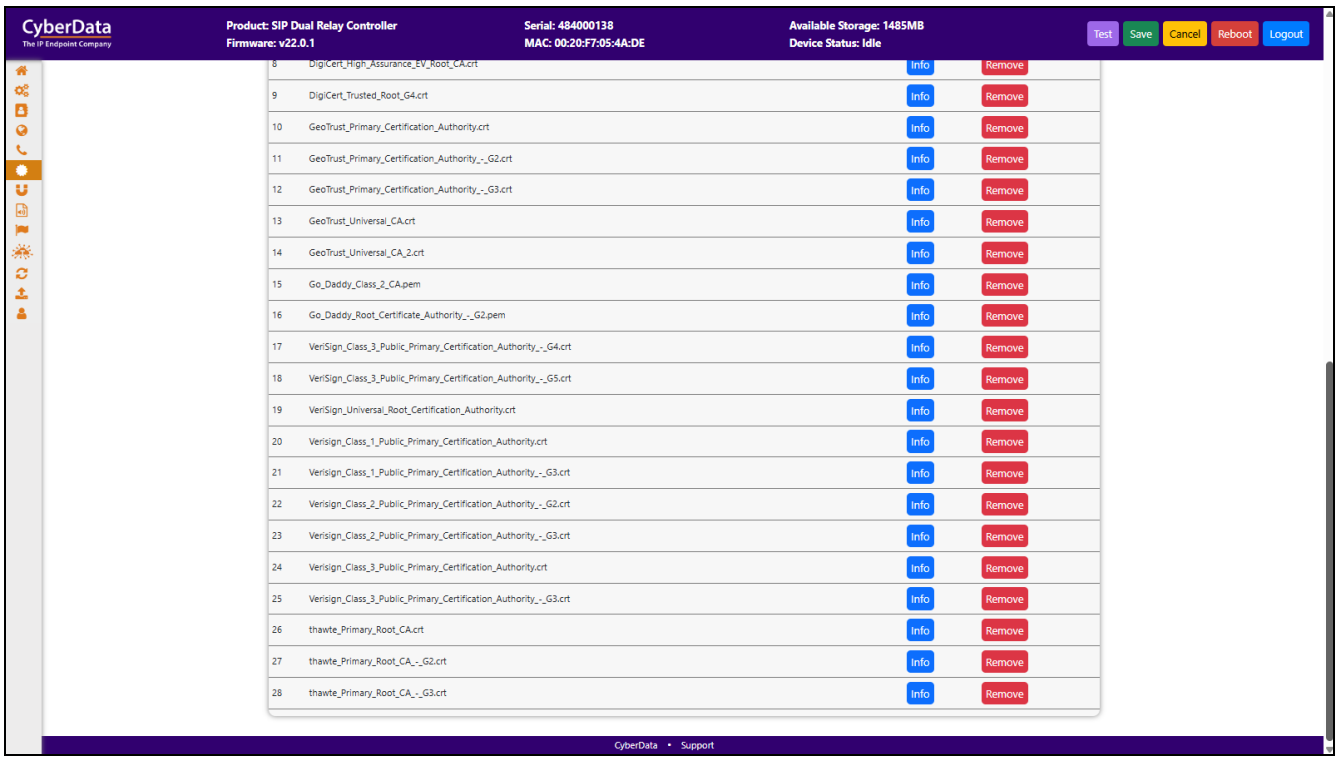
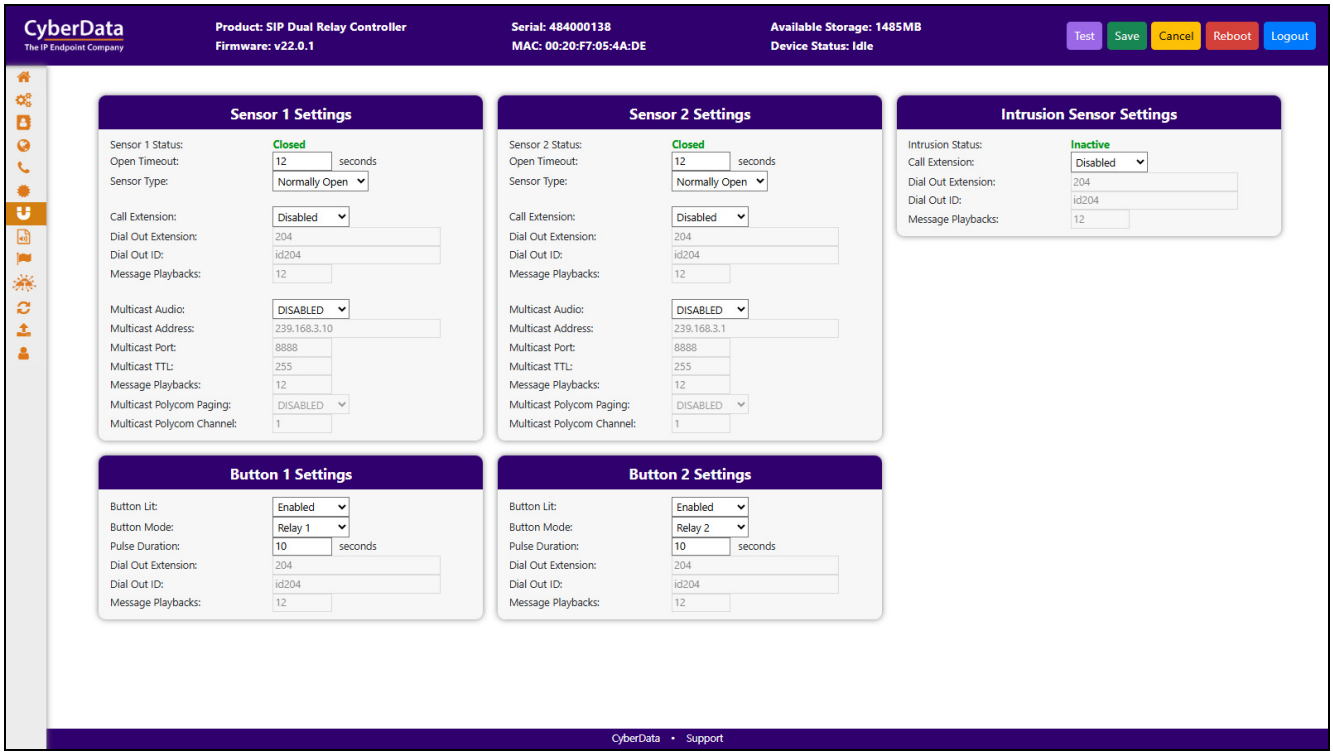


Figure 2-8. SSL Page (2 of 2)



2.8 Sensor

Figure 2-9. Sensor Page



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 2-10. Audiofiles Page (1 of 2)

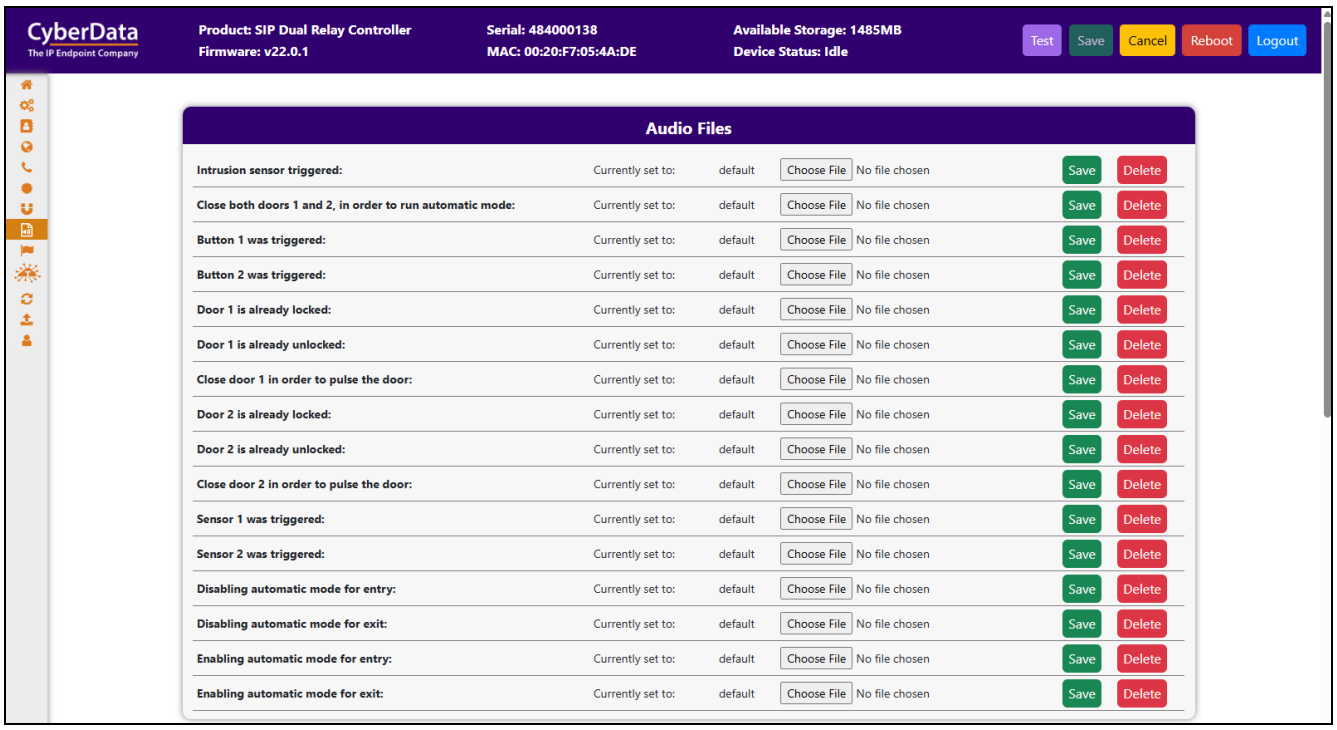
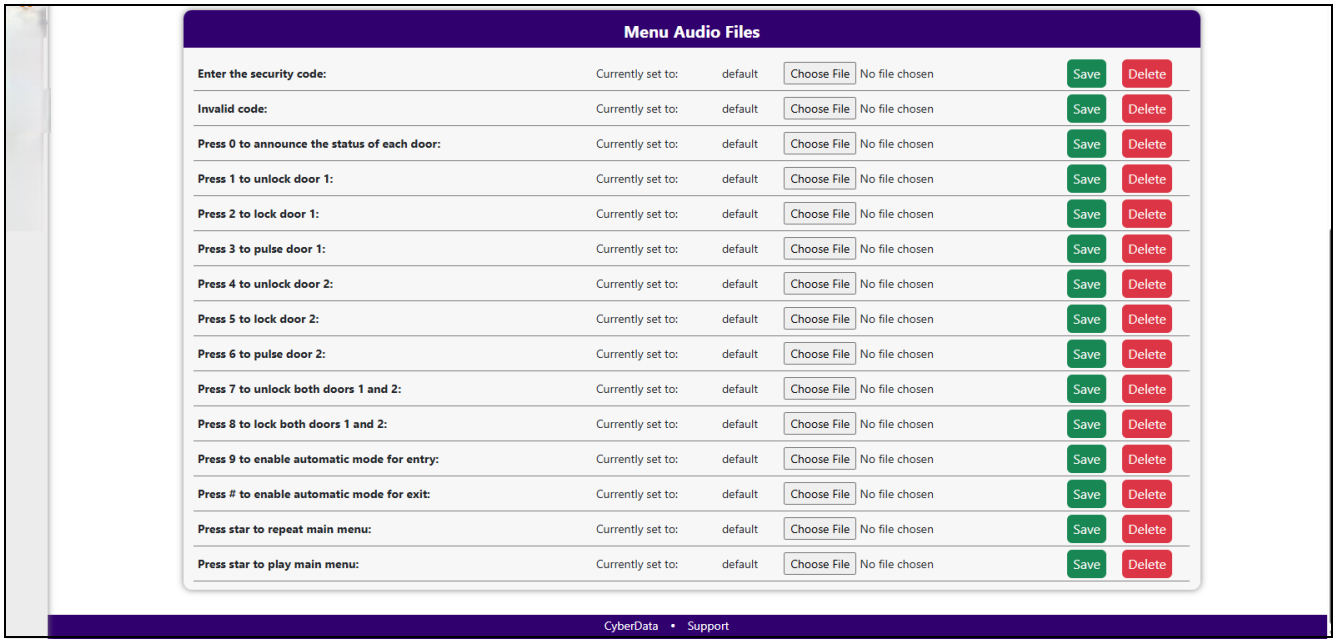


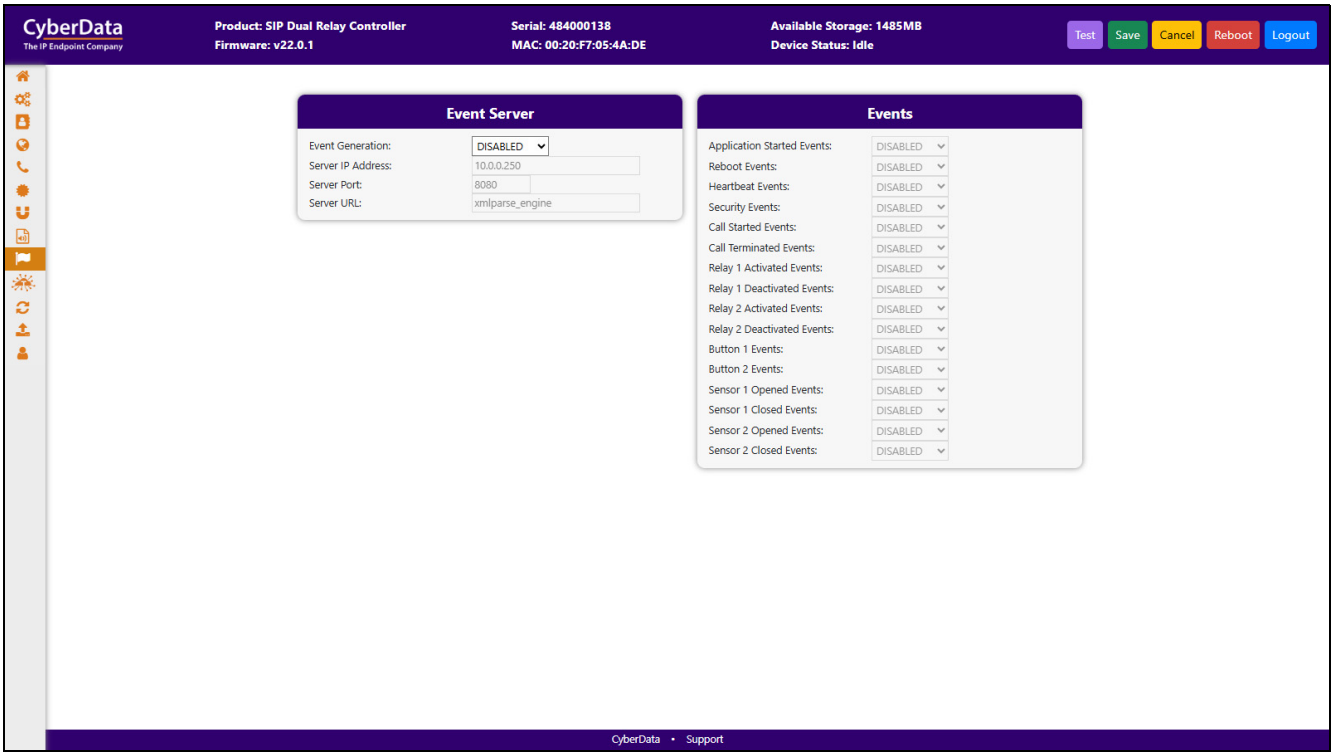
Figure 2-11. Audiofiles Page (2 of 2)



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 2-12. 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>
```

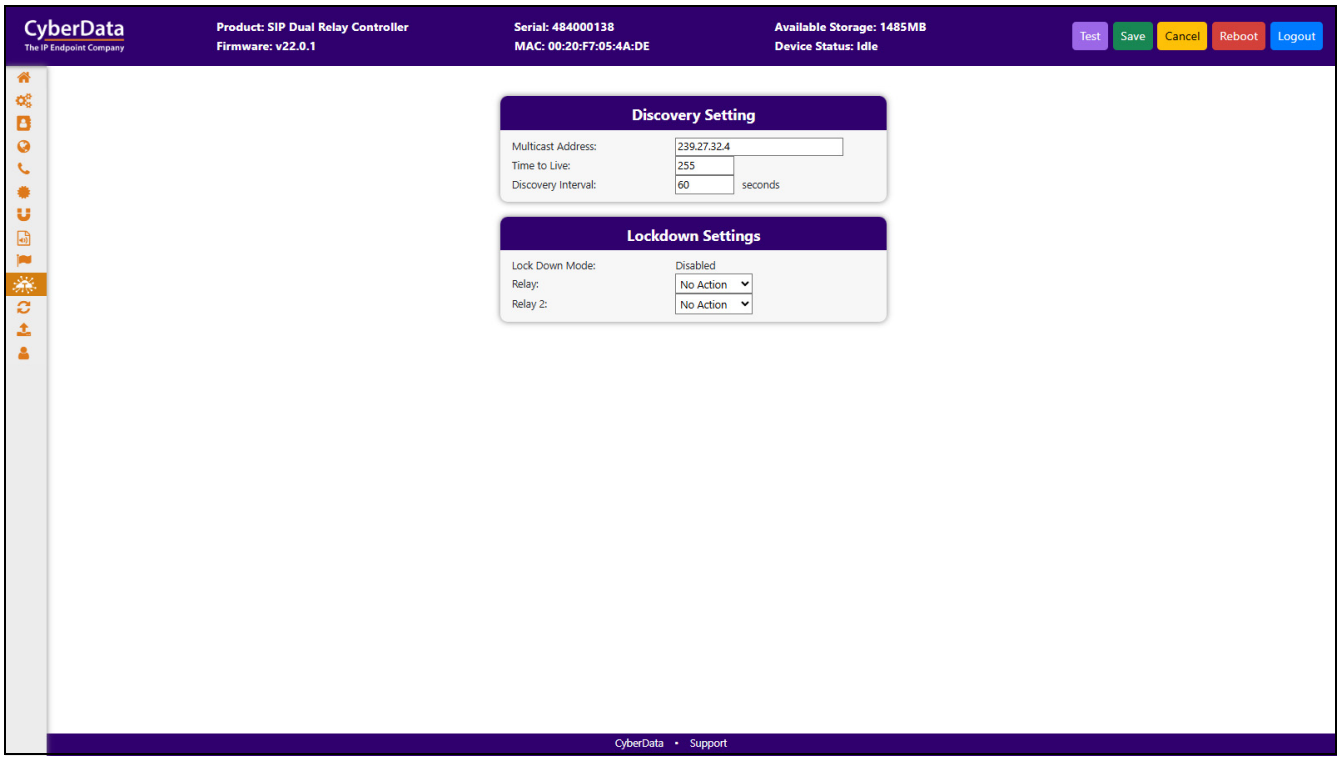
```
POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>RELAY_DEACTIVATED</event>
</cyberdata>

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

2.11 Terminus

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

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

Figure 2-13. Terminus Page



2.12 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.

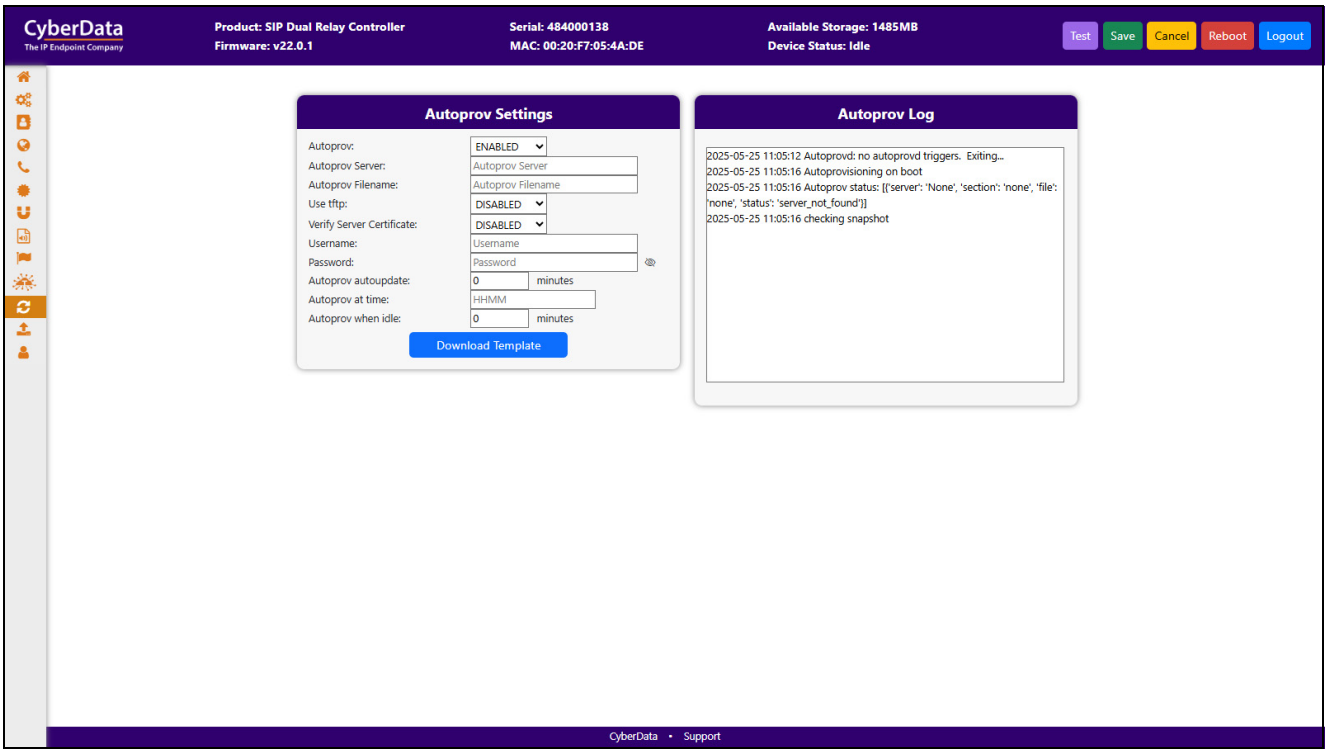
If a file is named, it will be downloaded instead of <mac address>.xml.

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 2-14. Autoprovisioning Page



2.13 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:

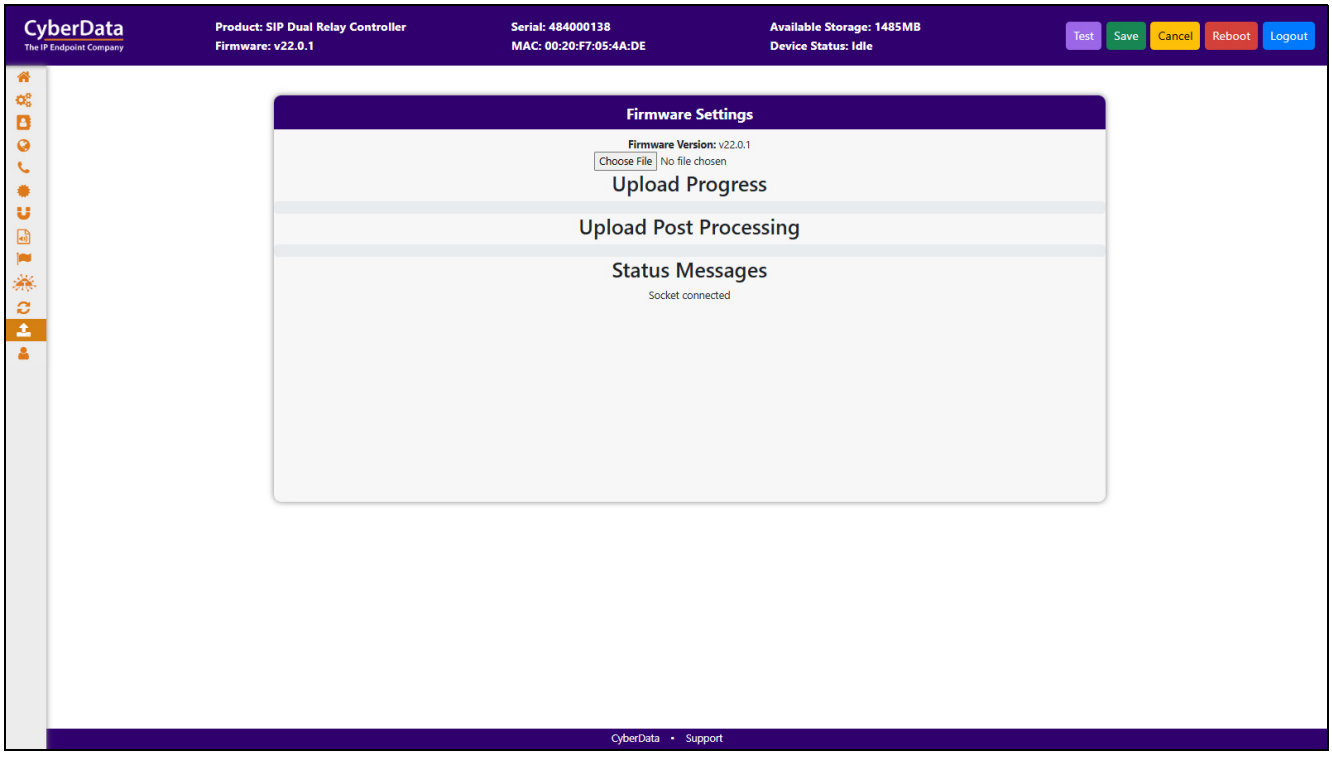
- Firmware file
- Release notes
- Autoprovisioning template

GENERAL ALERT

Caution

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

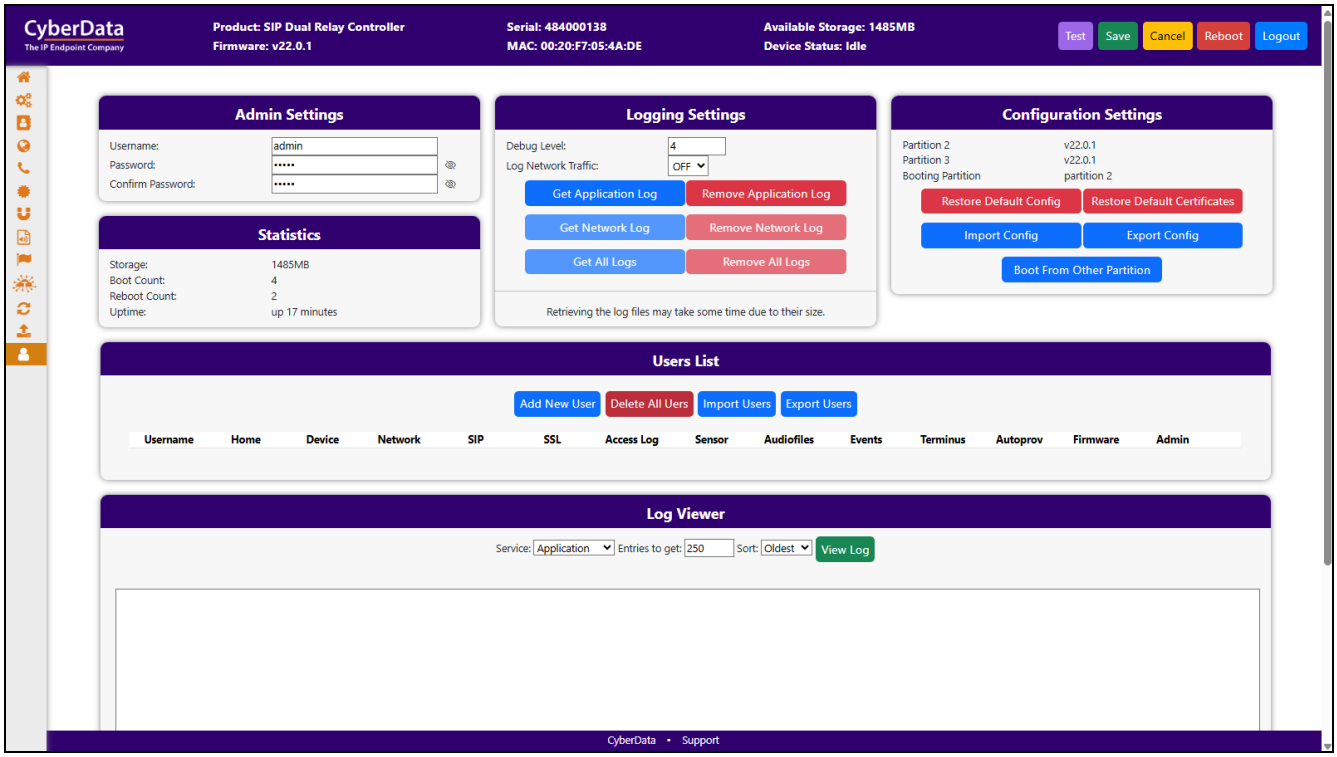
Figure 2-15. Firmware Page



2.14 Admin

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

Figure 2-16. Admin Page



2.15 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.

2.15.1 Command Interface Post Commands

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

Table 2-2. Command Interface Post Commands

Device Action	HTTP Post Command[a]
Reboot	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.154/command" --post-data "request=reboot"
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