



# *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**

**COPYRIGHT NOTICE:**

© 2025, CyberData Corporation, ALL RIGHTS RESERVED.

This manual and related materials are the copyrighted property of CyberData Corporation. No part of this manual or related materials may be reproduced or transmitted, in any form or by any means (except for internal use by licensed customers), without prior express written permission of CyberData Corporation. This manual, and the products, software, firmware, and/or hardware described in this manual are the property of CyberData Corporation, provided under the terms of an agreement between CyberData Corporation and recipient of this manual, and their use is subject to that agreement and its terms.

**DISCLAIMER:** Except as expressly and specifically stated in a written agreement executed by CyberData Corporation, CyberData Corporation makes no representation or warranty, express or implied, including any warranty or merchantability or fitness for any purpose, with respect to this manual or the products, software, firmware, and/or hardware described herein, and CyberData Corporation assumes no liability for damages or claims resulting from any use of this manual or such products, software, firmware, and/or hardware. CyberData Corporation reserves the right to make changes, without notice, to this manual and to any such product, software, firmware, and/or hardware.

**OPEN SOURCE STATEMENT:** Certain software components included in CyberData products are subject to the GNU General Public License (GPL) and Lesser GNU General Public License (LGPL) “open source” or “free software” licenses. Some of this Open Source Software may be owned by third parties. Open Source Software is not subject to the terms and conditions of the CyberData COPYRIGHT NOTICE or software licenses. Your right to copy, modify, and distribute any Open Source Software is determined by the terms of the GPL, LGPL, or third party, according to who licenses that software.

Software or firmware developed by CyberData that is unrelated to Open Source Software is copyrighted by CyberData, subject to the terms of CyberData licenses, and may not be copied, modified, reverse-engineered, or otherwise altered without explicit written permission from CyberData Corporation.

**TRADEMARK NOTICE:** CyberData Corporation and the CyberData Corporation logos are trademarks of CyberData Corporation. Other product names, trademarks, and service marks may be the trademarks or registered trademarks of their respective owners.



Technical Support

The fastest way to get technical support for your VoIP product is to submit a VoIP Technical Support form at the following website:  
<https://support.cyberdata.net/>

Phone: (831) 373-2601, Ext. 333

Email: [support@cyberdata.net](mailto:support@cyberdata.net)

Fax: (831) 373-4193

Company and product information is at [www.cyberdata.net](http://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!**

 <p>GENERAL ALERT</p>	<p><b>Warning</b> <i>Electrical Hazard:</i> This product should be installed by a licensed electrician according to all local electrical and building codes.</p>
--	--

 <p>GENERAL ALERT</p>	<p><b>Warning</b> <i>Electrical Hazard:</i> To prevent injury, this apparatus must be securely attached to the floor/wall in accordance with the installation instructions.</p>
--	---

 <p>GENERAL ALERT</p>	<p><b>Warning</b> The PoE connector is intended for intra-building connections only and does not route to the outside plant.</p>
--	--

---

## Pictorial Alert Icons

 <p>GENERAL ALERT</p>	<b>General Alert</b> 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.
	<b>Ground</b> 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

<b>Abbreviation or Term</b>	<b>Definition</b>
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

<b>Chapter 1 Product Overview and Setup</b>	<b>1</b>
1.1 Typical System Installation .....	1
1.2 Dimensions .....	5
1.3 SIP Dual Relay Controller Components .....	5
1.4 Assembly .....	6
1.5 LED Behavior .....	7
1.6 Wiring the SIP Dual Relay Controller .....	8
1.6.1 SIP Dual Relay Controller Wiring Diagram with External Power Source .....	8
1.6.2 Example Diagram Using PoE Power and One SIP Dual Relay Controller with the 011508 Remote Call Button .....	9
1.7 Terminal Block Wiring Connections .....	10
1.8 Jumper Definitions .....	11
1.9 Reset to Factory Defaults .....	12
<b>Chapter 2 Configure the Device</b>	<b>14</b>
2.1 Log In Page .....	14
2.2 Home Page .....	15
2.3 Device .....	16
2.4 Access Log .....	17
2.5 Network .....	18
2.6 SIP (Session Initiation Protocol) .....	19
2.7 SSL .....	20
2.8 Sensor .....	22
2.9 Audiofiles .....	23
2.10 Events .....	24
2.10.1 Example Packets for Events .....	25
2.11 Terminus .....	28
2.12 Autoprovisioning .....	29
2.13 Firmware .....	30
2.14 Admin .....	31
2.15 Command Interface .....	32
2.15.1 Command Interface Post Commands .....	32
<b>Appendix A Troubleshooting/Technical Support</b>	<b>33</b>
A.1 Contact Information .....	33
A.2 Warranty and RMA Information .....	33
<b>Index</b>	<b>34</b>

# 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.

	<p><b>Warning</b> <i>Electrical Hazard:</i> Hazardous voltages may be present. No user serviceable part inside. Refer to qualified service personnel for connecting or servicing.</p>
---	---

**Figure 1-1. Single Door Typical Use Case**

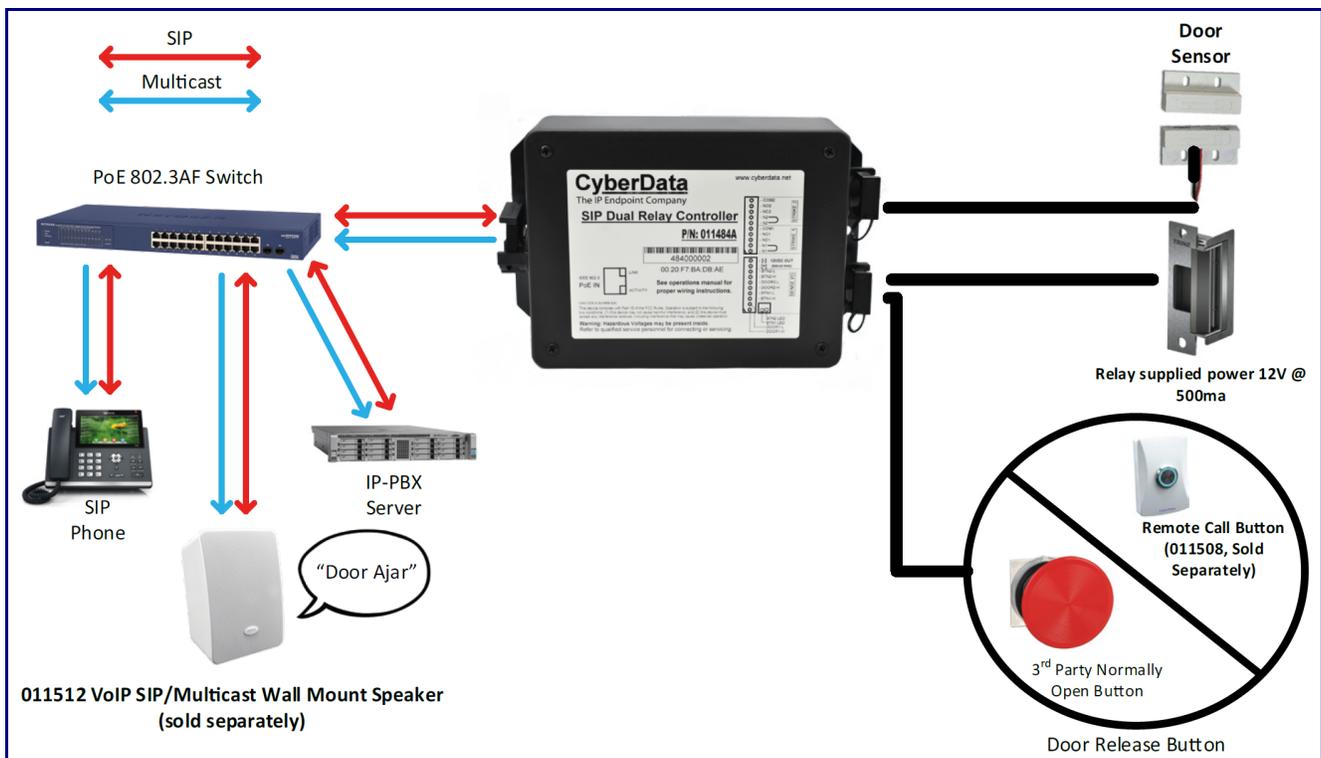


Figure 1-2. Typical Air Lock Use Case

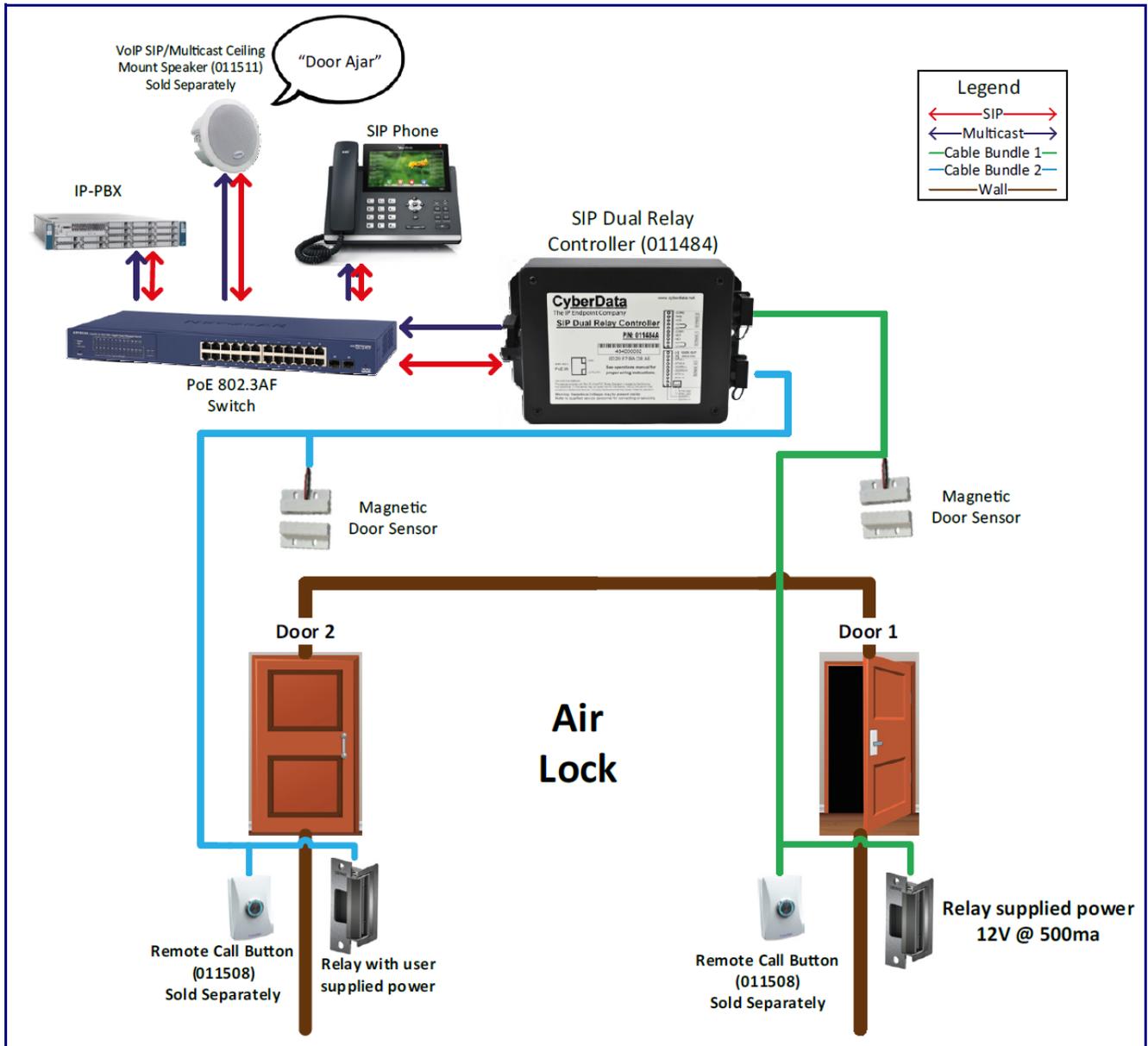


Figure 1-3. Wiring

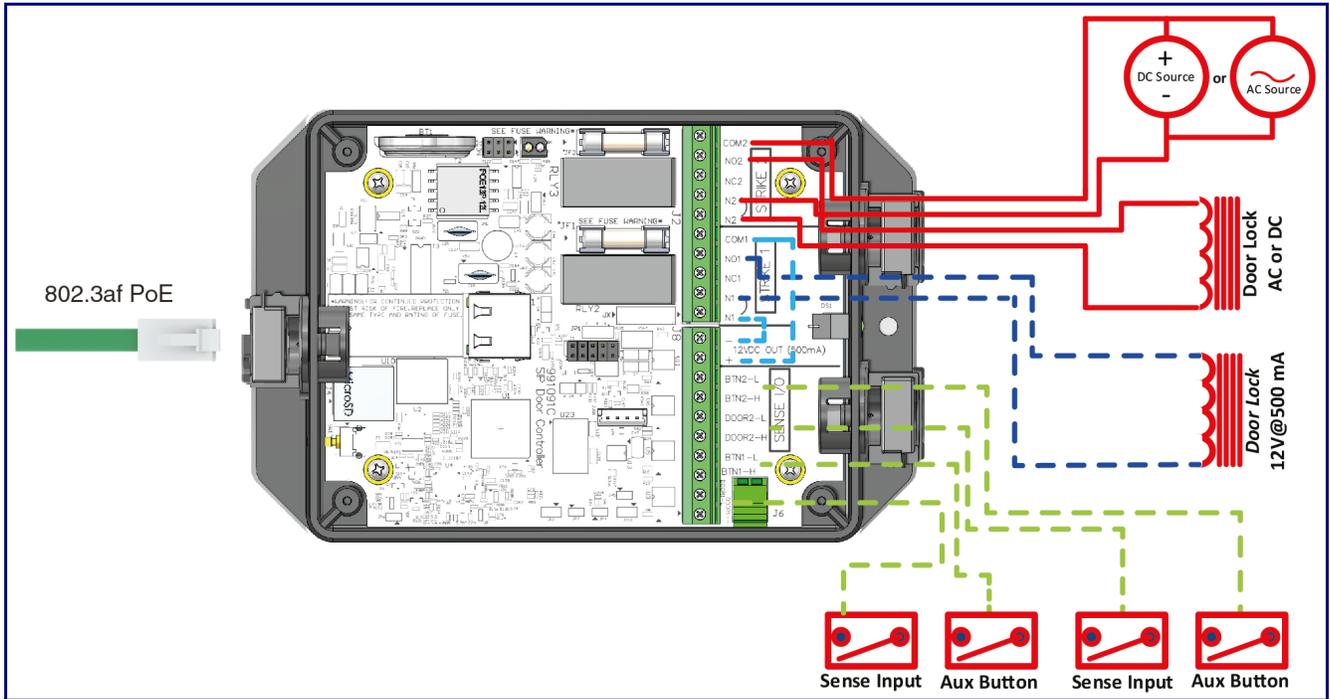


Figure 1-4. Wiring Example with a HES 1500 Electric Strike Using Internal Power Supply

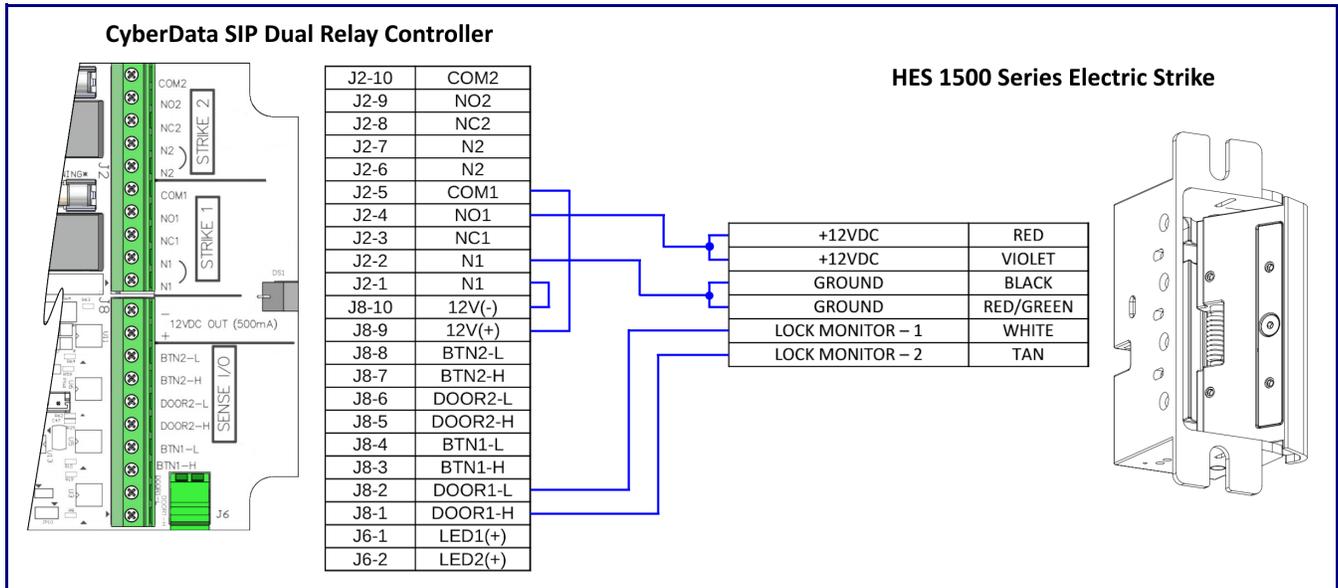
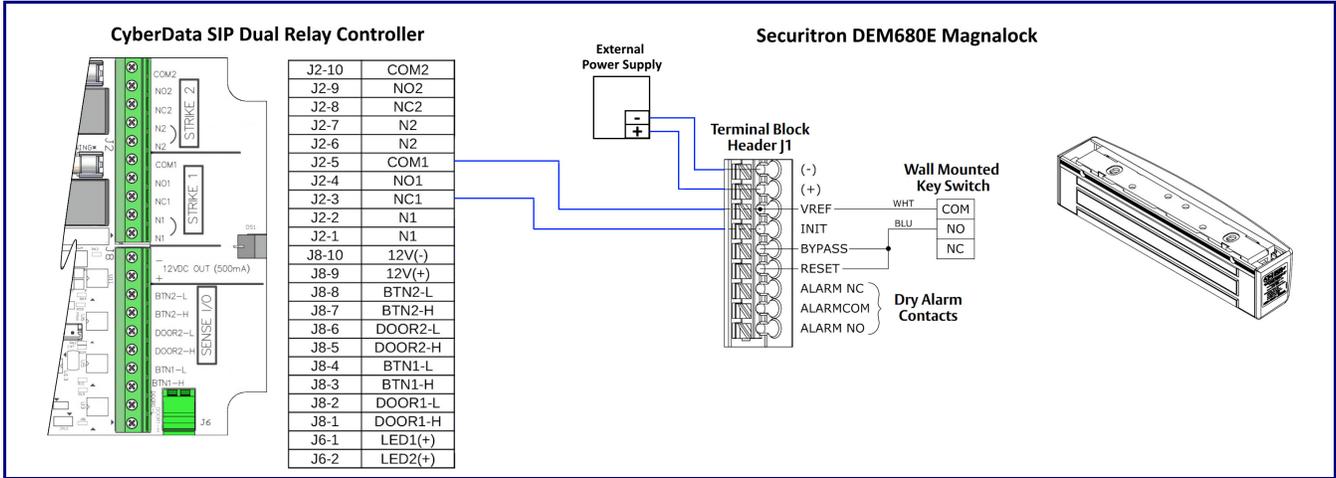
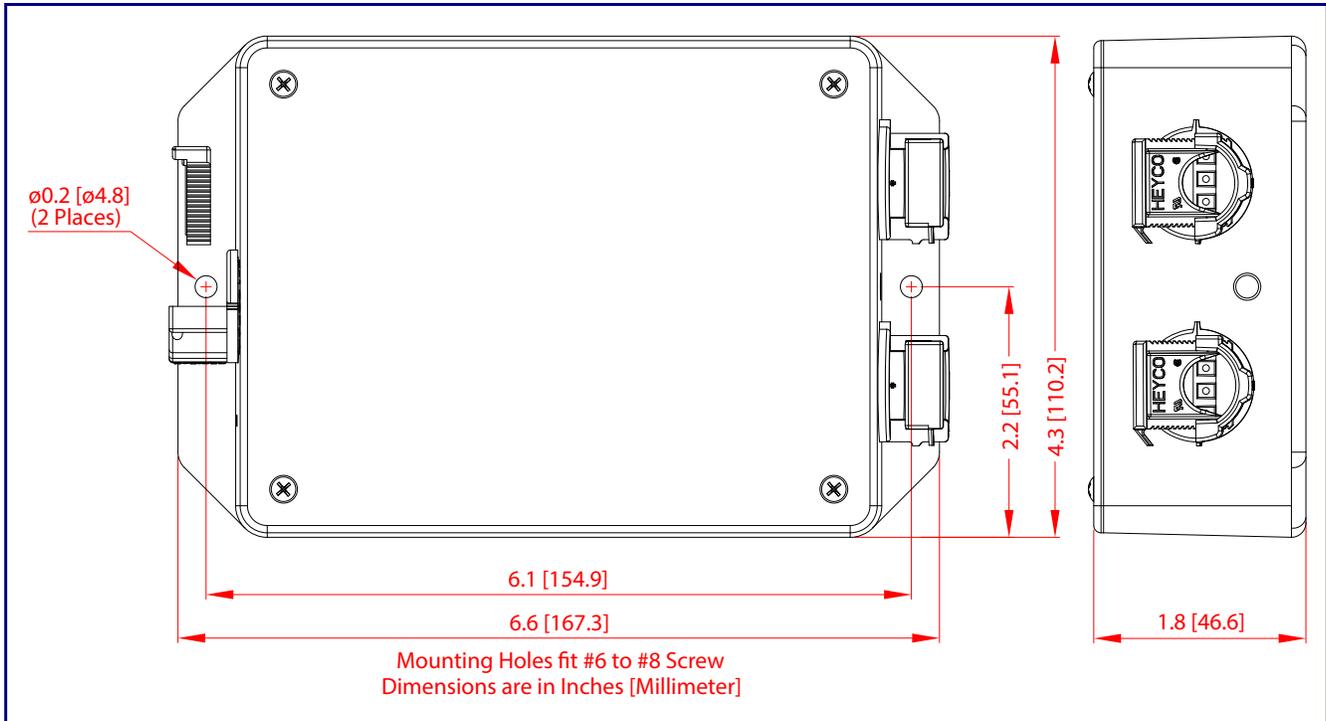


Figure 1-5. Wiring Example with a Securitron DEM680E Magnalock Using External Power Supply



## 1.2 Dimensions

Figure 1-6. Dimensions



## 1.3 SIP Dual Relay Controller Components

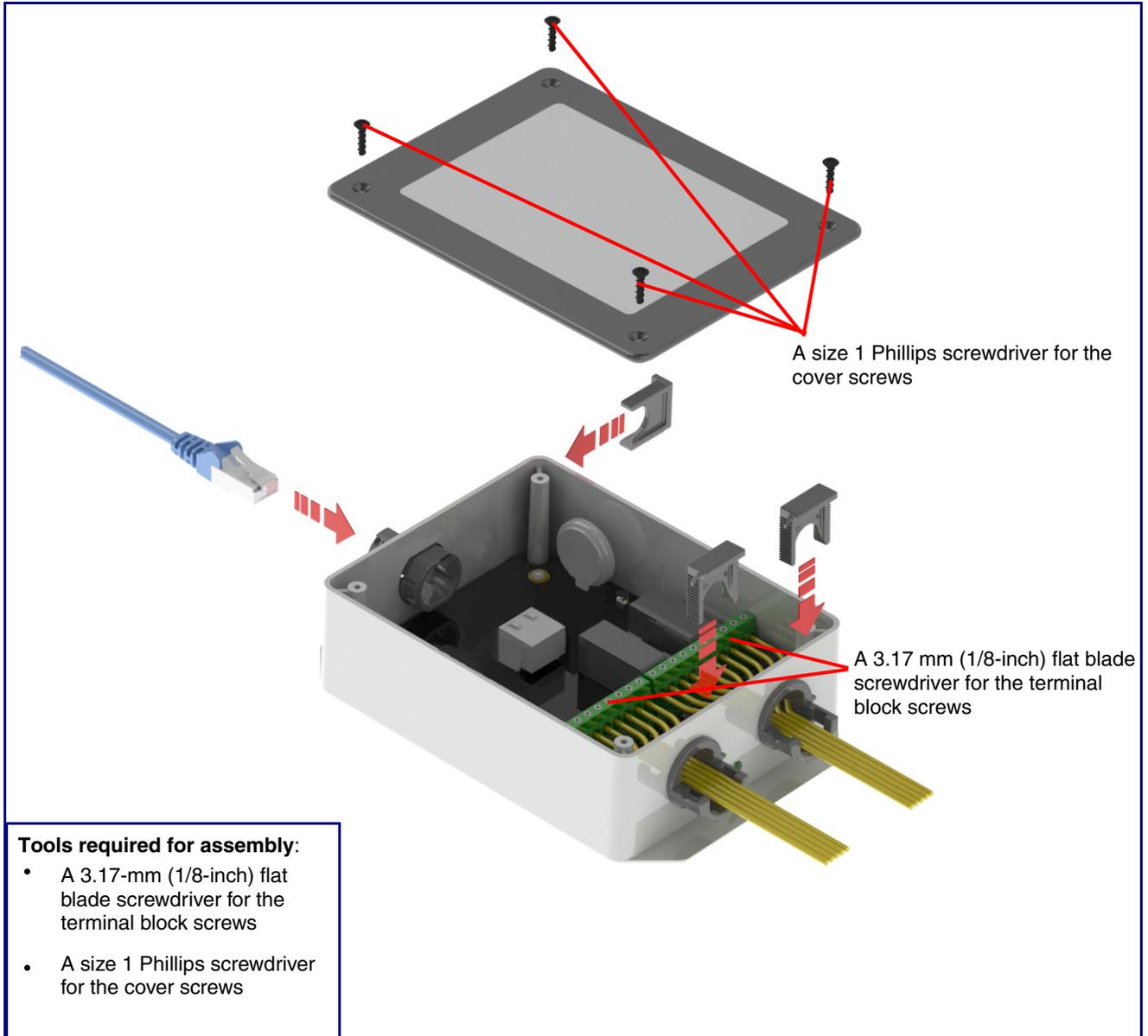
Figure 1-7 shows the components of the SIP Dual Relay Controller.

Figure 1-7. SIP Dual Relay Controller Components



## 1.4 Assembly

Figure 1-8. Assembly



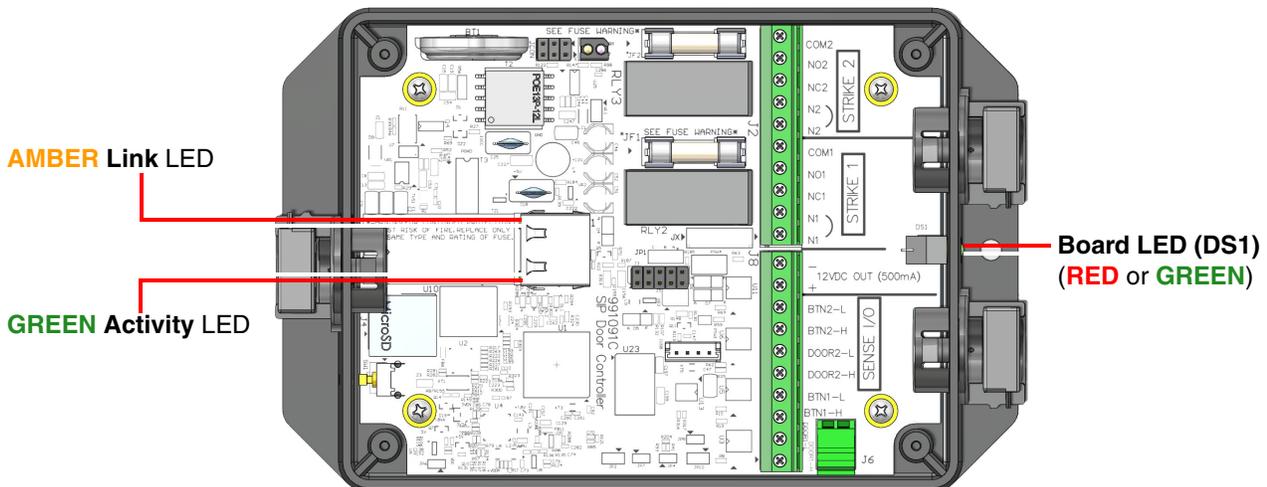
# 1.5 LED Behavior

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 <b>AMBER Status</b> LED is on and the <b>GREEN Link</b> LED is on and blinking.	No fault detected. The device is on the network and the device is not active.
<b>Note:</b> On boot, within approximately three seconds, the <b>AMBER Status</b> LED and the <b>GREEN Link</b> LED come on with the <b>GREEN Link</b> LED beginning to blink almost immediately.	
Board LED (DS1):	
LED Behavior	Means
On and solid <b>GREEN</b>	Neither relays nor sensors are active
Slow blinking <b>GREEN</b>	Either the relay or the sensor is active for Door/Device 2
Fast blinking <b>GREEN</b>	Either the relay or the sensor is active for Door/Device 1
On and solid <b>RED</b>	Either both relays, or a relay and a sensor are active: <ul style="list-style-type: none"> <li>• Relay 1 and Relay 2</li> <li>• Relay 1 and Sensor 2</li> <li>• Sensor 1 and Relay 2</li> <li>• Sensor 1 and Sensor 2</li> </ul>

**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.

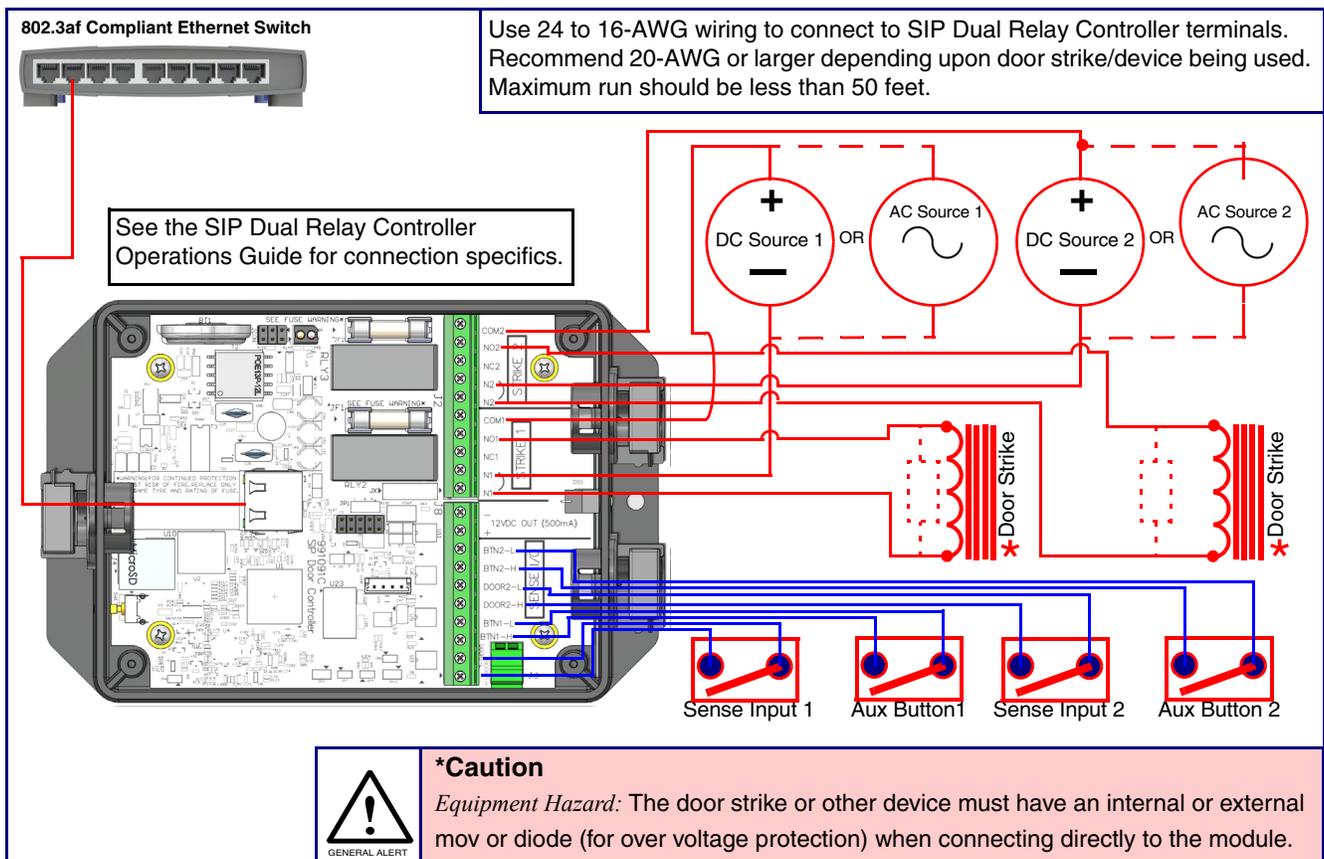


GENERAL ALERT

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

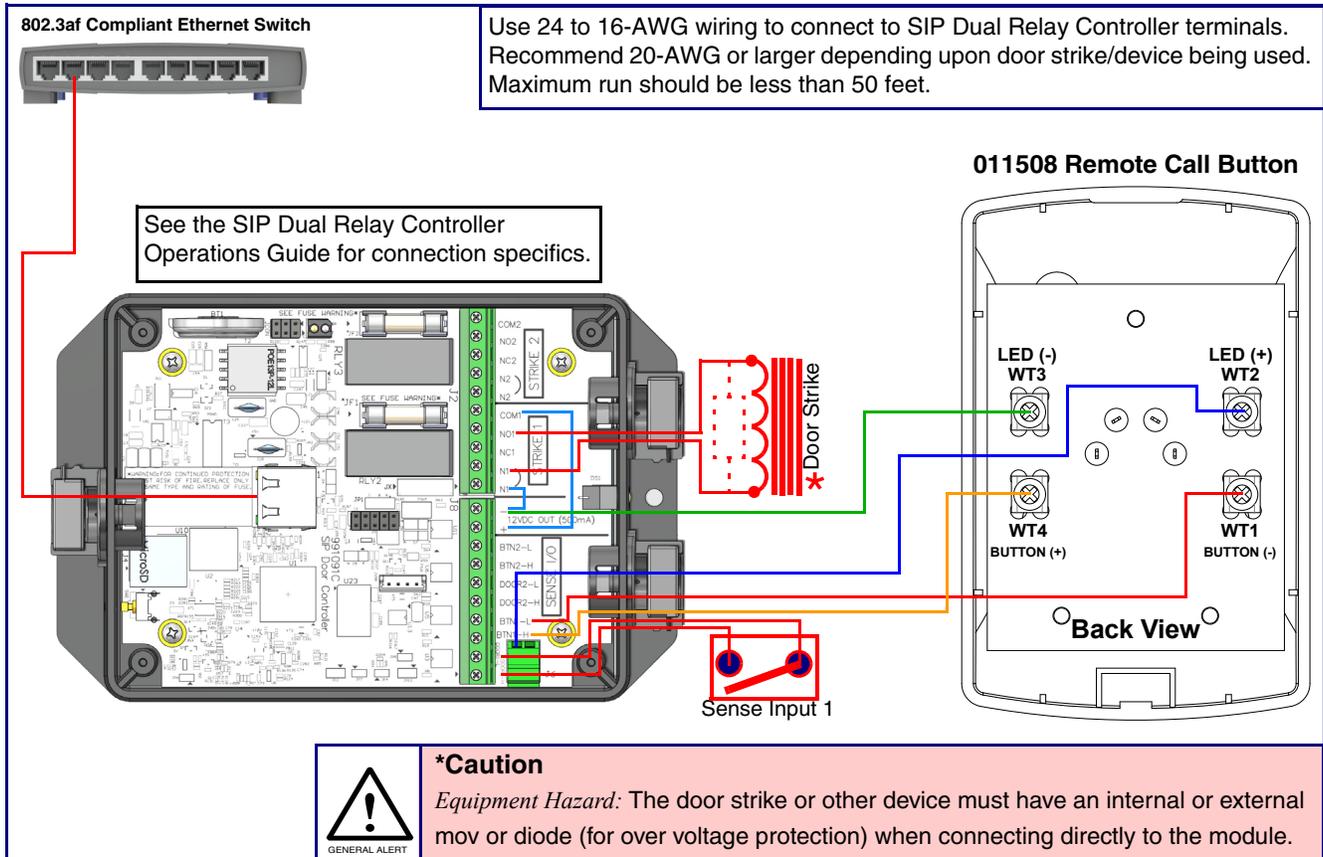


**Figure 1-10. SIP Dual Relay Controller Wiring Diagram with External Power Source**



## 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<sup>1</sup>



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

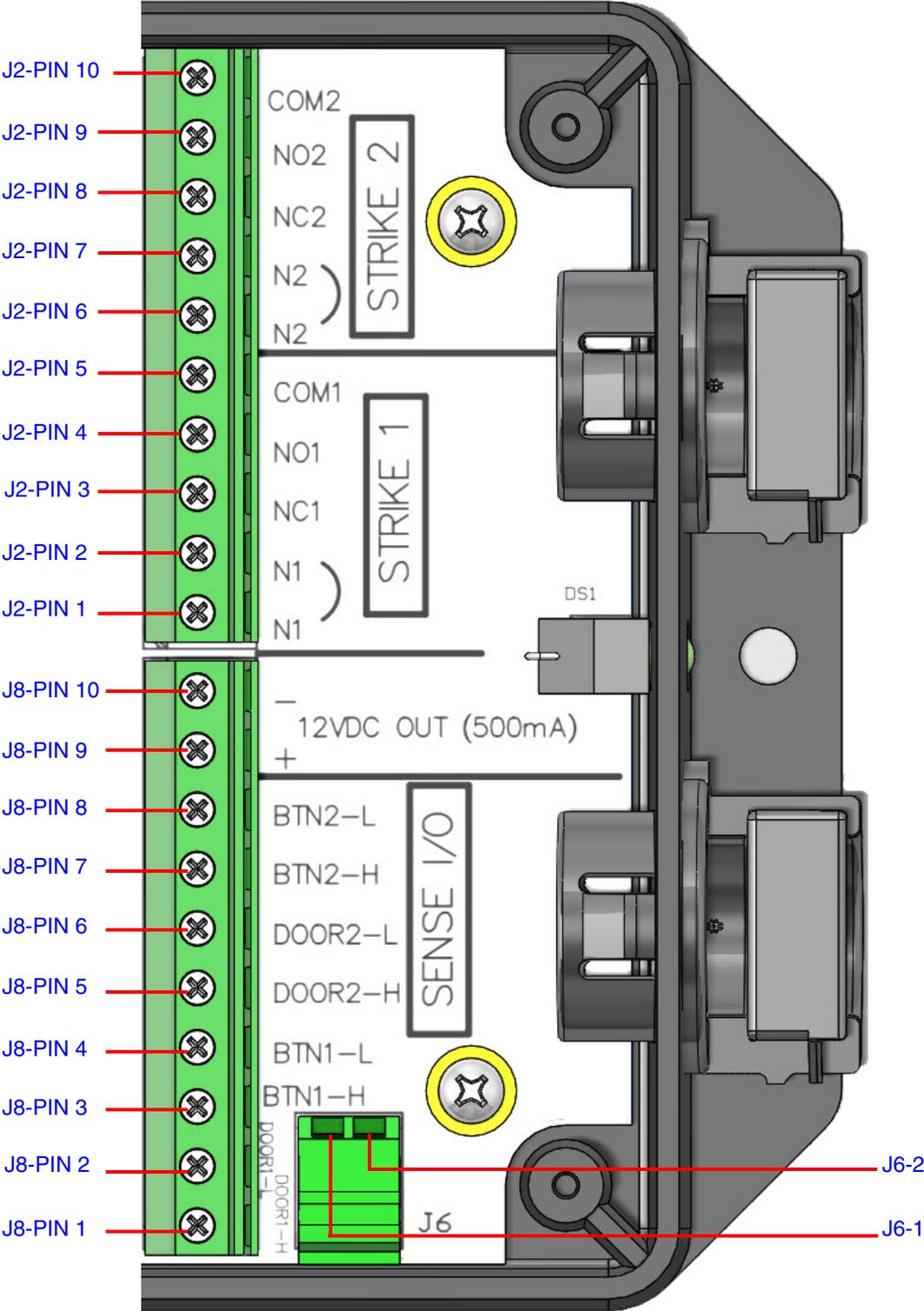
<https://support.cyberdata.net/>

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**

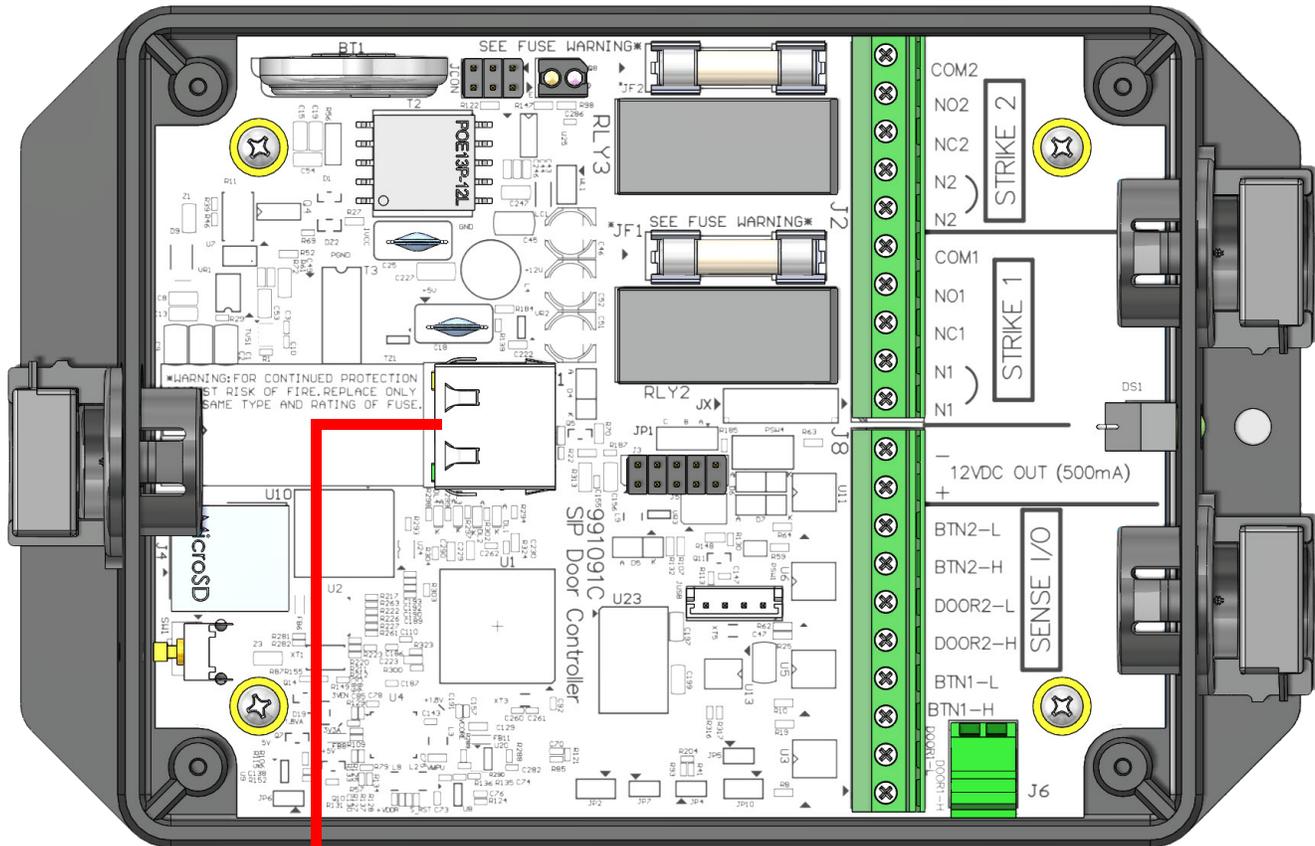
Jumper	Description
JP5	Missing Installed—Held in reset
JP10	Missing—Intrusion sensor enabled Installed—Intrusion sensor disabled

## 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.

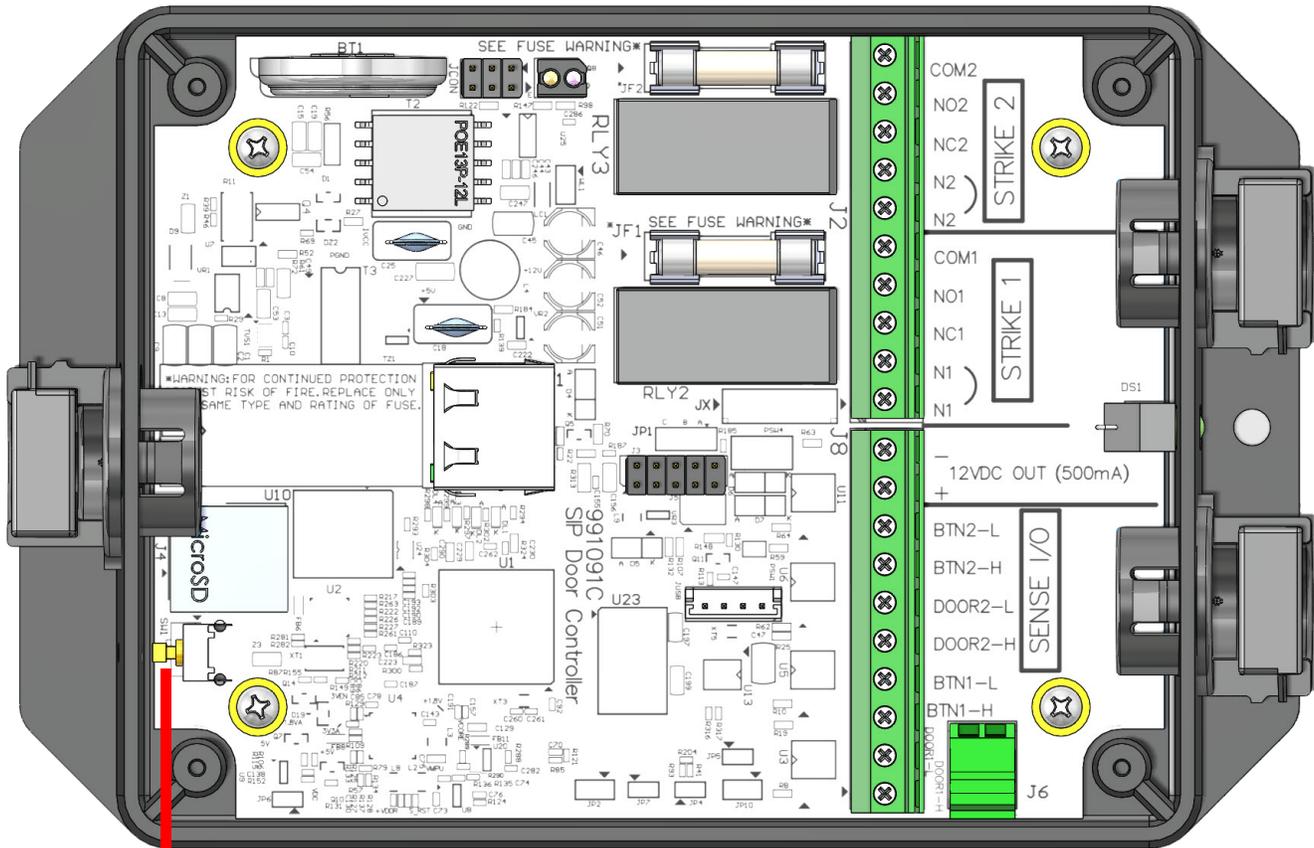
**Figure 1-13. Connect a PoE network ethernet cable to J1**



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 <sup>a</sup>	192.168.1.23
Web Access Username	admin
Web Access Password	admin
Subnet Mask <sup>a</sup>	255.255.255.0
Default Gateway <sup>a</sup>	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>

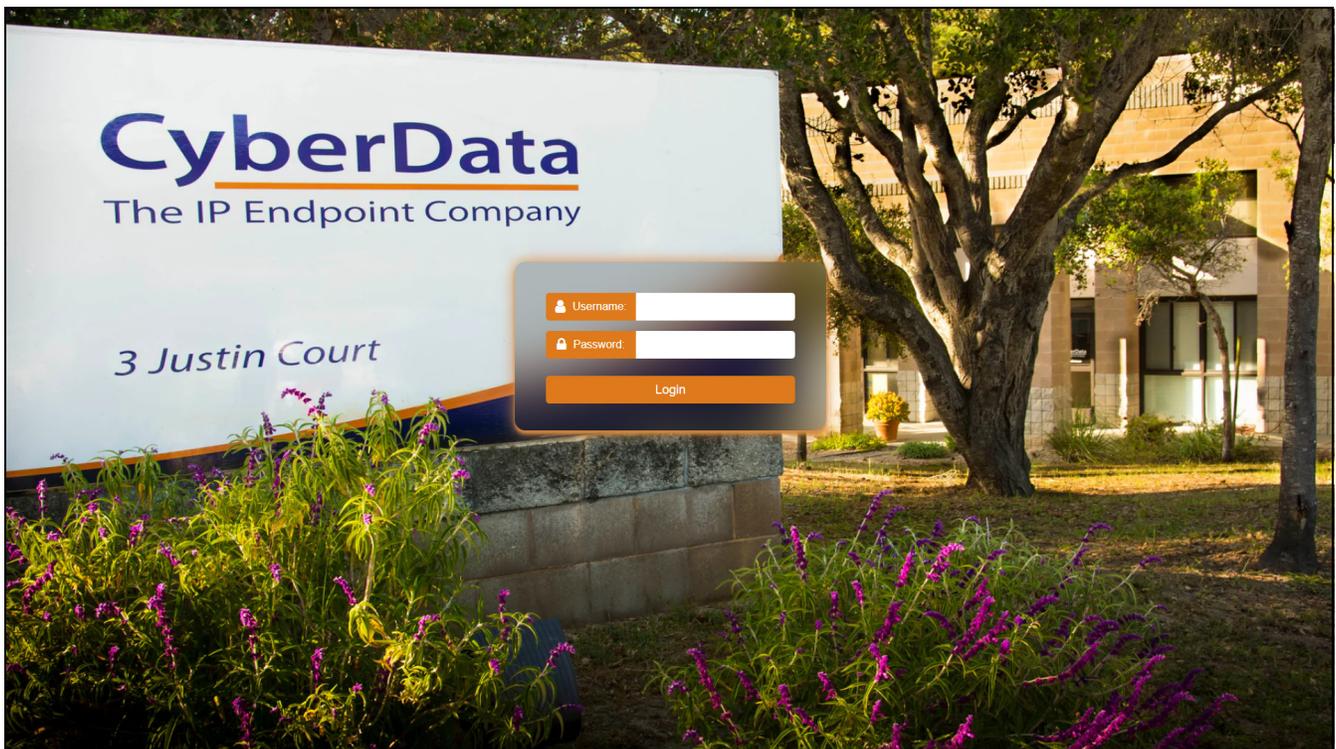
**Note** The Intercom ships in DHCP mode. To get to the **Home** page, use the discovery utility to scan for the device on the network and open your browser from there.

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

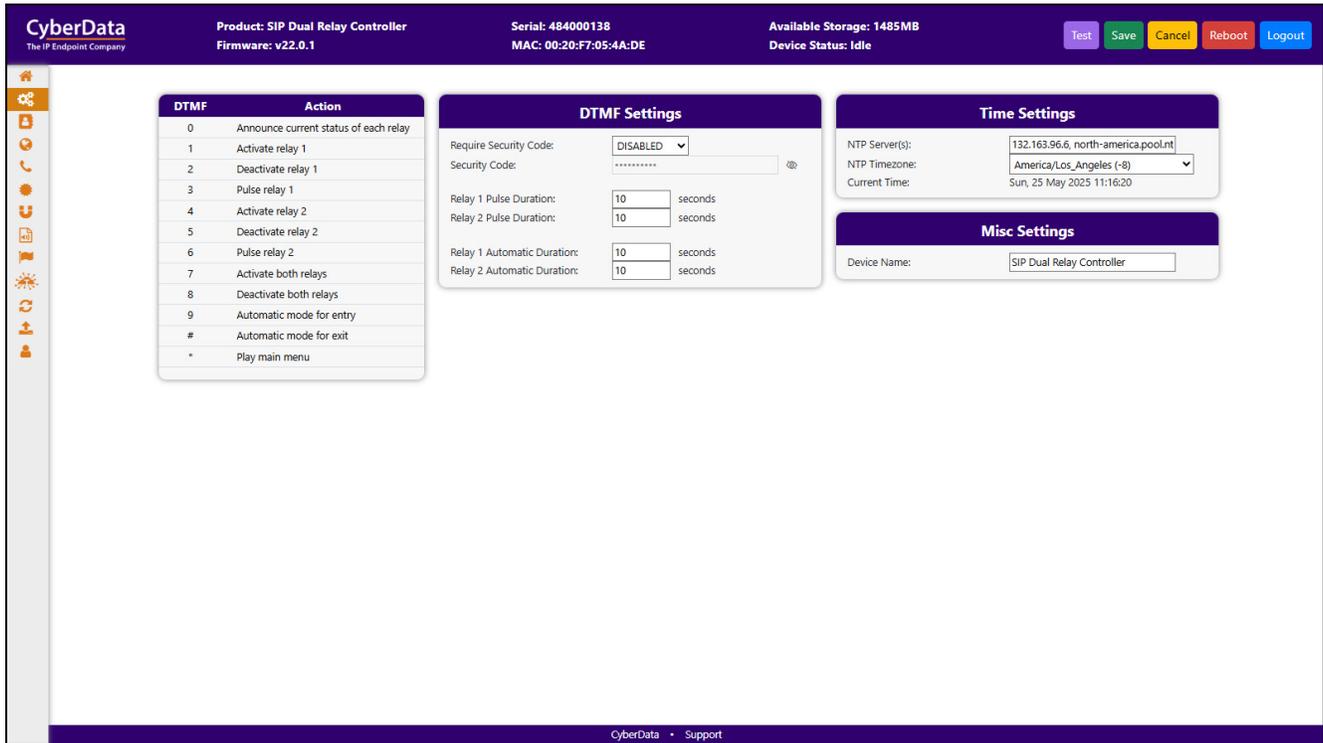
The screenshot displays the CyberData Home Page for a SIP Dual Relay Controller. The page features a top navigation bar with the CyberData logo and company name, product and firmware information, serial and MAC addresses, available storage, and device status. A sidebar on the left contains various system icons. The main content area is divided into five panels: Device Configuration, Network Status, SIP Registration, Sensor Status, and System Configuration. Each panel displays key system parameters and their current status.

Parameter	Value/Status
Serial Number	484000138
Mac Address	00:20:F7:05:4A:DE
Firmware Version	v22.0.1
Partition 2	v22.0.1
Partition 3	v22.0.1
Booting Partition	partition 2
IP Address Protocol	DHCP
IP Address	192.168.0.67
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.1
DNS Server 1	192.168.0.1
DNS Server 2	
SIP Mode	Enabled
Primary Server	Not registered
Backup Server 1	Not registered
Backup Server 2	Not registered
Relay 1 Status	Locked
Relay 2 Status	Locked
Sensor 1 Status	Closed
Sensor 2 Status	Closed
Intrusion Status	Inactive
SIP Mode	Enabled
Event Mode	Disabled

## 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 <b>Sensor</b> 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**

The screenshot displays the CyberData web interface for the Access Log page. At the top, the header includes the CyberData logo, product information (SIP Dual Relay Controller, v22.0.1), serial and MAC addresses, available storage (1485MB), and device status (Idle). A navigation bar contains buttons for Test, Save, Cancel, Reboot, and Logout. The main content area features a search bar and three action buttons: Clear Log, Download Log, and Refresh Log. Below these is a table with the following data:

Event #	Timestamp	Action	User ID	User Name
11	Wed 2025-05-28 13:50:40 PM	DTMF 9 pressed	601@10.10.0.178	Automatic Mode for entry
10	Wed 2025-05-28 13:50:38 PM	Call connected	601@10.10.0.178	
9	Wed 2025-05-28 13:50:37 PM	Call received		
8	Wed 2025-05-28 13:26:37 PM	Call terminated	601@10.10.0.178	
7	Wed 2025-05-28 13:26:19 PM	DTMF 9 pressed	601@10.10.0.178	Automatic Mode for entry
6	Wed 2025-05-28 13:26:15 PM	DTMF 2 pressed	601@10.10.0.178	Lock Door 1
5	Wed 2025-05-28 13:26:08 PM	DTMF 1 pressed	601@10.10.0.178	Unlock Door 1
4	Wed 2025-05-28 13:26:04 PM	DTMF * pressed	601@10.10.0.178	Playing Main Menu
3	Wed 2025-05-28 13:25:56 PM	DTMF 0 pressed	601@10.10.0.178	Announce Status
2	Wed 2025-05-28 13:25:52 PM	Call connected	601@10.10.0.178	

At the bottom of the table, it indicates 'Showing 11 to 20 of 21 rows' and '10 rows per page'. A pagination control shows page 2 of 3.

## 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**

**CyberData** The IP Endpoint Company

Product: SIP Dual Relay Controller  
Firmware: v22.0.1

Serial: 484000138  
MAC: 00:20:F7:05:4A:DE

Available Storage: 1485MB  
Device Status: Idle

Test Save Cancel Reboot Logout

### Network Status

IP Address Protocol	DHCP
IP Address	192.168.0.67
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.1
DNS Server 1	192.168.0.1
DNS Server 2	192.168.0.1

### Network Settings

Addressing Mode:

Hostname:

IP Address:

Subnet Mask:

Default Gateway:

DNS Server 1:

DNS Server 2:

DHCP Timeout:  seconds

### VLAN Settings

VLAN ID:

VLAN Priority:

CyberData • Support

## 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)

The screenshot displays the CyberData SSL configuration interface. At the top, the header includes the CyberData logo, product information (SIP Dual Relay Controller, Firmware: v22.0.1), device details (Serial: 484000138, MAC: 0020:F7:05:4A:DE), and system status (Available Storage: 1485MB, Device Status: Idle). Action buttons for Test, Save, Cancel, Reboot, and Logout are present.

Three main certificate configuration panels are shown:

- Web Server Certificate:** Displays X.509 details (countryName: US, stateOrProvinceName: California, localityName: Monterey, organizationName: Cyberdata, commonName: 8028F7954ade) and options to 'Choose Files', 'Import Web Certificate', and 'Restore Web Certificate'.
- SIP Client Certificate:** Displays identical X.509 details and options to 'Choose Files', 'Import SIP Certificate', and 'Restore SIP Certificate'. Includes an optional password field.
- Autoprovisioning Client Certificate:** Displays identical X.509 details and options to 'Choose Files', 'Import Autoprovisioning Certificate', and 'Restore Autoprovisioning Certificate'. Includes an optional password field.

Below these panels is the **List of Trusted CAs** section, which includes an 'Upload CA Certificate' button and a table of installed certificates:

Index	CA Name	Info	Remove
1	CyberData_CA.pem	Info	Remove
2	DigiCert_Assured_ID_Root_CA.crt	Info	Remove
3	DigiCert_Assured_ID_Root_G2.crt	Info	Remove
4	DigiCert_Assured_ID_Root_G3.crt	Info	Remove
5	DigiCert_Global_Root_CA.crt	Info	Remove
6	DigiCert_Global_Root_G2.crt	Info	Remove
7	DigiCert_Global_Root_G3.crt	Info	Remove
8	DigiCert_High_Assurance_EV_Root_CA.crt	Info	Remove

Additional controls for the CA list include 'Download CyberData CA', 'Generate Cyberdata CSR', 'Remove All', and 'Restore Defaults' buttons.

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

The screenshot displays the SSL configuration interface for a CyberData device. At the top, the header includes the CyberData logo, product information (SIP Dual Relay Controller, Firmware: v22.0.1), serial and MAC addresses, available storage (1485MB), and device status (Idle). Action buttons for Test, Save, Cancel, Reboot, and Logout are also present.

ID	Certificate Name	Info	Remove
8	DigiCert_High_Assurance_EV_Root_CA.crt	Info	Remove
9	DigiCert_Trusted_Root_G4.crt	Info	Remove
10	GeoTrust_Primary_Certification_Authority.crt	Info	Remove
11	GeoTrust_Primary_Certification_Authority_-_G2.crt	Info	Remove
12	GeoTrust_Primary_Certification_Authority_-_G3.crt	Info	Remove
13	GeoTrust_Universal_CA.crt	Info	Remove
14	GeoTrust_Universal_CA_2.crt	Info	Remove
15	Go_Daddy_Class_2_CA.pem	Info	Remove
16	Go_Daddy_Root_Certificate_Authority_-_G2.pem	Info	Remove
17	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G4.crt	Info	Remove
18	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5.crt	Info	Remove
19	VeriSign_Universal_Root_Certification_Authority.crt	Info	Remove
20	VeriSign_Class_1_Public_Primary_Certification_Authority.crt	Info	Remove
21	VeriSign_Class_1_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
22	VeriSign_Class_2_Public_Primary_Certification_Authority_-_G2.crt	Info	Remove
23	VeriSign_Class_2_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
24	VeriSign_Class_3_Public_Primary_Certification_Authority.crt	Info	Remove
25	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
26	thawte_Primary_Root_CA.crt	Info	Remove
27	thawte_Primary_Root_CA_-_G2.crt	Info	Remove
28	thawte_Primary_Root_CA_-_G3.crt	Info	Remove

The interface includes a sidebar with navigation icons and a footer with 'CyberData • Support'.

## 2.8 Sensor

Figure 2-9. Sensor Page

**CyberData** The IP Endpoint Company

Product: SIP Dual Relay Controller  
Firmware: v22.0.1

Serial: 484000138  
MAC: 00:20:F7:05:4A:DE

Available Storage: 1485MB  
Device Status: Idle

Test Save Cancel Reboot Logout

---

**Sensor 1 Settings**

Sensor 1 Status: **Closed**

Open Timeout: 12 seconds

Sensor Type: Normally Open

Call Extension: Disabled

Dial Out Extension: 204

Dial Out ID: id204

Message Playbacks: 12

Multicast Audio: DISABLED

Multicast Address: 239.168.3.10

Multicast Port: 8888

Multicast TTL: 255

Message Playbacks: 12

Multicast Polycom Paging: DISABLED

Multicast Polycom Channel: 1

**Sensor 2 Settings**

Sensor 2 Status: **Closed**

Open Timeout: 12 seconds

Sensor Type: Normally Open

Call Extension: Disabled

Dial Out Extension: 204

Dial Out ID: id204

Message Playbacks: 12

Multicast Audio: DISABLED

Multicast Address: 239.168.3.1

Multicast Port: 8888

Multicast TTL: 255

Message Playbacks: 12

Multicast Polycom Paging: DISABLED

Multicast Polycom Channel: 1

**Intrusion Sensor Settings**

Intrusion Status: **Inactive**

Call Extension: Disabled

Dial Out Extension: 204

Dial Out ID: id204

Message Playbacks: 12

**Button 1 Settings**

Button Lit: Enabled

Button Mode: Relay 1

Pulse Duration: 10 seconds

Dial Out Extension: 204

Dial Out ID: id204

Message Playbacks: 12

**Button 2 Settings**

Button Lit: Enabled

Button Mode: Relay 2

Pulse Duration: 10 seconds

Dial Out Extension: 204

Dial Out ID: id204

Message Playbacks: 12

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 device.

Figure 2-10. Audiofiles Page (1 of 2)

The screenshot shows the 'Audio Files' configuration page. At the top, there is a header with the CyberData logo and device information: Product: SIP Dual Relay Controller, Serial: 484000138, Available Storage: 1485MB, Firmware: v22.0.1, MAC: 00:20:F7:05:4A:DE, and Device Status: Idle. There are also buttons for Test, Save, Cancel, Reboot, and Logout. The main content is a table with 14 rows, each representing a different event. Each row has a 'Currently set to:' field (all set to 'default'), a 'Choose File' button, a 'No file chosen' status, and 'Save' and 'Delete' buttons.

Event	Currently set to:	Choose File	No file chosen	Save	Delete
Intrusion sensor triggered:	default	Choose File	No file chosen	Save	Delete
Close both doors 1 and 2, in order to run automatic mode:	default	Choose File	No file chosen	Save	Delete
Button 1 was triggered:	default	Choose File	No file chosen	Save	Delete
Button 2 was triggered:	default	Choose File	No file chosen	Save	Delete
Door 1 is already locked:	default	Choose File	No file chosen	Save	Delete
Door 1 is already unlocked:	default	Choose File	No file chosen	Save	Delete
Close door 1 in order to pulse the door:	default	Choose File	No file chosen	Save	Delete
Door 2 is already locked:	default	Choose File	No file chosen	Save	Delete
Door 2 is already unlocked:	default	Choose File	No file chosen	Save	Delete
Close door 2 in order to pulse the door:	default	Choose File	No file chosen	Save	Delete
Sensor 1 was triggered:	default	Choose File	No file chosen	Save	Delete
Sensor 2 was triggered:	default	Choose File	No file chosen	Save	Delete
Disabling automatic mode for entry:	default	Choose File	No file chosen	Save	Delete
Disabling automatic mode for exit:	default	Choose File	No file chosen	Save	Delete
Enabling automatic mode for entry:	default	Choose File	No file chosen	Save	Delete
Enabling automatic mode for exit:	default	Choose File	No file chosen	Save	Delete

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

The screenshot shows the 'Menu Audio Files' configuration page. It features a table with 15 rows, each representing a menu item. Each row has a 'Currently set to:' field (all set to 'default'), a 'Choose File' button, a 'No file chosen' status, and 'Save' and 'Delete' buttons.

Event	Currently set to:	Choose File	No file chosen	Save	Delete
Enter the security code:	default	Choose File	No file chosen	Save	Delete
Invalid code:	default	Choose File	No file chosen	Save	Delete
Press 0 to announce the status of each door:	default	Choose File	No file chosen	Save	Delete
Press 1 to unlock door 1:	default	Choose File	No file chosen	Save	Delete
Press 2 to lock door 1:	default	Choose File	No file chosen	Save	Delete
Press 3 to pulse door 1:	default	Choose File	No file chosen	Save	Delete
Press 4 to unlock door 2:	default	Choose File	No file chosen	Save	Delete
Press 5 to lock door 2:	default	Choose File	No file chosen	Save	Delete
Press 6 to pulse door 2:	default	Choose File	No file chosen	Save	Delete
Press 7 to unlock both doors 1 and 2:	default	Choose File	No file chosen	Save	Delete
Press 8 to lock both doors 1 and 2:	default	Choose File	No file chosen	Save	Delete
Press 9 to enable automatic mode for entry:	default	Choose File	No file chosen	Save	Delete
Press # to enable automatic mode for exit:	default	Choose File	No file chosen	Save	Delete
Press star to repeat main menu:	default	Choose File	No file chosen	Save	Delete
Press star to play main menu:	default	Choose File	No file chosen	Save	Delete

## 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

The screenshot displays the CyberData web interface for configuring events. The top navigation bar includes the CyberData logo, product information (SIP Dual Relay Controller, Firmware: v22.0.1), device details (Serial: 484000138, MAC: 00:20:F7:05:4A:DE), and storage status (Available Storage: 1485MB, Device Status: Idle). Action buttons for Test, Save, Cancel, Reboot, and Logout are visible in the top right.

The main content area is divided into two panels:

- Event Server:**
  - Event Generation:
  - Server IP Address:
  - Server Port:
  - Server URL:
- Events:**
  - Application Started Events:
  - Reboot Events:
  - Heartbeat Events:
  - Security Events:
  - Call Started Events:
  - Call Terminated Events:
  - Relay 1 Activated Events:
  - Relay 1 Deactivated Events:
  - Relay 2 Activated Events:
  - Relay 2 Deactivated Events:
  - Button 1 Events:
  - Button 2 Events:
  - Sensor 1 Opened Events:
  - Sensor 1 Closed Events:
  - Sensor 2 Opened Events:
  - Sensor 2 Closed Events:

The footer of the page contains the text "CyberData • Support".

---

## 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**

The screenshot displays the Terminus configuration page within the CyberData web interface. The interface features a purple header bar with the CyberData logo and product information. Below the header, there are two main configuration sections: 'Discovery Setting' and 'Lockdown Settings'. The 'Discovery Setting' section includes fields for Multicast Address (239.27.32.4), Time to Live (255), and Discovery Interval (60 seconds). The 'Lockdown Settings' section includes a dropdown for Lock Down Mode (Disabled) and two dropdowns for Relay 1 and Relay 2 (both set to No Action). A sidebar on the left contains various navigation icons, and a footer at the bottom provides support information.

Discovery Setting	
Multicast Address:	239.27.32.4
Time to Live:	255
Discovery Interval:	60 seconds

Lockdown Settings	
Lock Down Mode:	Disabled
Relay 1:	No Action
Relay 2:	No Action

## 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

The screenshot displays the Autoprovisioning configuration page for a CyberData SIP Dual Relay Controller. The page header includes the CyberData logo, product name (SIP Dual Relay Controller), serial number (484000138), MAC address (00:20:F7:05:4A:DE), available storage (1485MB), and device status (Idle). Navigation buttons (Test, Save, Cancel, Reboot, Logout) are located in the top right.

The main content area is divided into two panels:

- Autoprov Settings:** Contains configuration options for Autoprov (ENABLED), Autoprov Server, Autoprov Filename, Use tftp (DISABLED), Verify Server Certificate (DISABLED), Username, Password, Autoprov autoupdate (0 minutes), Autoprov at time (HHMM), and Autoprov when idle (0 minutes). A "Download Template" button is located at the bottom of this panel.
- Autoprov Log:** Displays a log of autoprovisioning events, including timestamps and status messages such as "no autoprov triggers. Exiting...", "Autoprovisioning on boot", and "checking snapshot".

The footer of the page contains the text "CyberData • Support".

## 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:

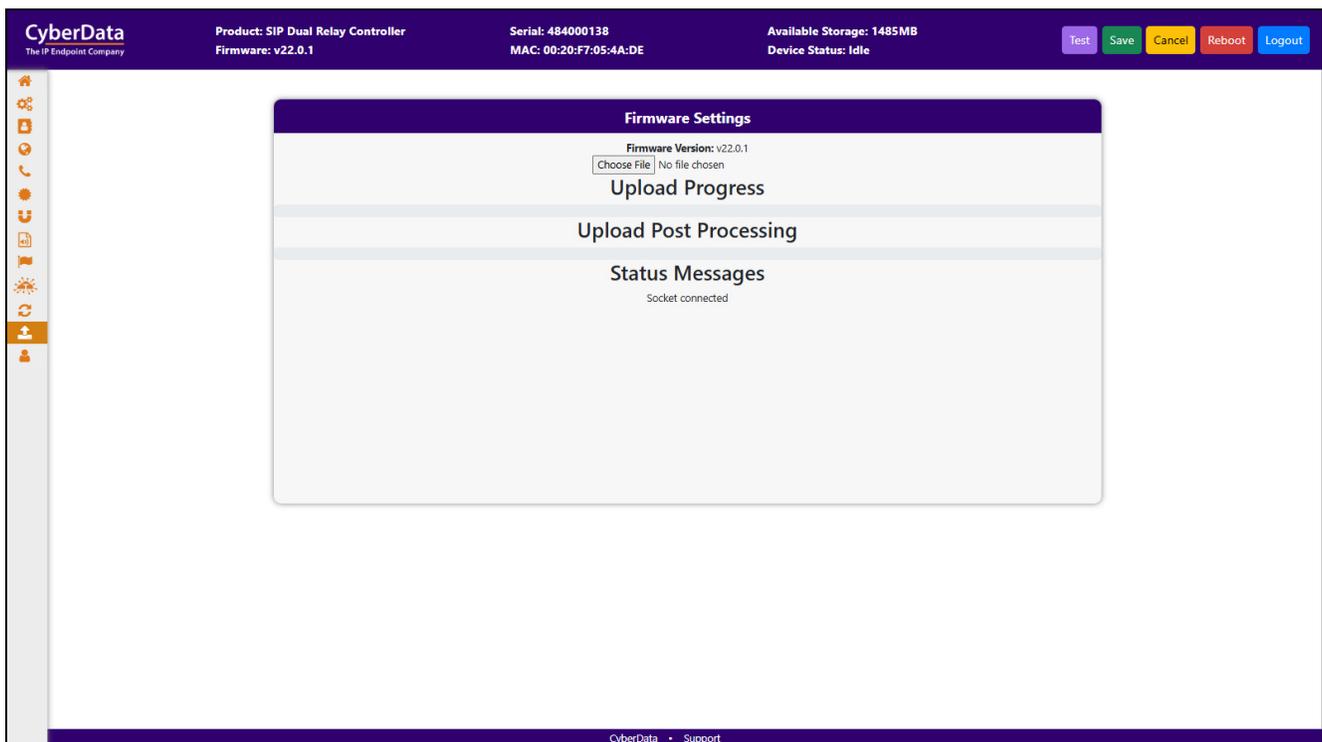
<https://www.cyberdata.net/collections/sip>

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

- Firmware file
- Release notes
- Autoprovisioning template

 GENERAL ALERT	<b>Caution</b> <b>Equipment Hazard:</b> 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

The screenshot displays the CyberData Admin Page interface. At the top, the header includes the CyberData logo, product information (SIP Dual Relay Controller, Firmware v22.0.1), serial and MAC addresses, available storage (1485MB), and device status (Idle). Navigation buttons for Test, Save, Cancel, Reboot, and Logout are present.

The main content area is divided into several sections:

- Admin Settings:** Fields for Username (admin), Password, and Confirm Password.
- Statistics:** Storage (1485MB), Boot Count (4), Reboot Count (2), and Uptime (up 17 minutes).
- Logging Settings:** Debug Level (4), Log Network Traffic (OFF), and buttons for Get/Remove Application, Network, and All Logs.
- Configuration Settings:** Partition information and buttons for Restore Default Config/Certificates, Import/Export Config, and Boot From Other Partition.
- Users List:** Buttons for Add New User, Delete All Users, Import Users, and Export Users. Below is a table with columns: Username, Home, Device, Network, SIP, SSL, Access Log, Sensor, Audiofiles, Events, Terminus, Autopro, Firmware, and Admin.
- Log Viewer:** Service dropdown (Application), Entries to get (250), Sort dropdown (Oldest), and View Log button.

The footer contains the text "CyberData • Support".

---

## 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 <sup>a</sup>
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](http://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

---

## A

Admin 31  
Audiofiles 23  
Autoprovisioning 29

## C

Command Interface 32  
Command Interface Post Commands 32  
Contact Information 33

## D

Device 16  
Dial Out Extension Strings and DTMF Tones 20  
Discovery Utility program 14  
Door Strike Relay 28

## E

Events 24

## F

Firmware 30

## H

Home Page 15

## I

Installation 1

## L

Log In Page 14

## N

Network 18

## S

Sensor 22  
SIP (Session Initiation Protocol) 19  
SSL 20

## T

Terminus 28  
Troubleshooting/Technical Support 33

## W

Warranty and RMA Information 33