



SIP Dual Relay Controller Operations Guide

Part #011484
Document Part #931778B
for Firmware Version 20.1.0

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

SIP Dual Relay Controller Operations Guide 931778B
Part # 011484

COPYRIGHT NOTICE:

© 2022, 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

Fax: (831) 373-4193

Company and product information is at www.cyberdata.net.




Revision Information

Revision 931778B, which corresponds to firmware version 20.1.0, was released on November 2, 2023.



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>Warning <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>Warning <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>Warning 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>	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

Chapter 1 Product Overview and Setup	1
1.1 How to Identify This Product	1
1.2 Typical System Installation	2
1.3 Features	5
1.4 Specifications	6
1.5 Compliance	7
1.5.1 RoHS Statement	7
1.5.2 FCC Statement	7
1.5.3 Industry Canada (IC) Compliance Statement	7
1.6 Dimensions	8
1.7 Assembly	9
1.8 LED Behavior	10
1.9 Wiring the SIP Dual Relay Controller	11
1.9.1 SIP Dual Relay Controller Wiring Diagram with External Power Source	11
1.9.2 Example Diagram Using PoE Power and One SIP Dual Relay Controller with the 011508 Remote Call Button	12
1.10 Terminal Block Wiring Connections	13
1.11 Jumper Definitions	14
1.12 Reset to Factory Defaults	15
Chapter 2 Installing the SIP Dual Relay Controller	17
2.1 Parts List	17
2.2 SIP Dual Relay Controller Components	17
2.3 Configure the SIP Dual Relay Controller Parameters	18
2.3.1 Factory Default Settings	18
2.3.2 SIP Dual Relay Controller Web Page Navigation	19
2.3.3 Using the Toggle Help Button	20
2.3.4 Log in to the Configuration Home Page	22
2.3.5 Configure the Device	26
2.3.6 Configure the Network Parameters	29
2.3.7 Configure the SIP (Session Initiation Protocol) Parameters	31
2.3.8 Configure the SSL Parameters	36
2.3.9 Configure the Access Log Parameters	42
2.3.10 Configure the Sensor Configuration Parameters	44
2.3.11 Configure the Audio Configuration Parameters	48
2.3.12 Configure the Events Parameters	55
2.3.13 Configure the Autoprovisioning Parameters	61
2.4 Upgrade the Firmware	72
2.5 Reboot the Device	75
2.6 Command Interface	76
2.6.1 Command Interface Post Commands	76
Appendix A Setting up a TFTP Server	77
A.1 Set up a TFTP Server	77
A.1.1 In a LINUX Environment	77
A.1.2 In a Windows Environment	77
Appendix B Troubleshooting/Technical Support	78
B.1 Frequently Asked Questions (FAQ)	78
B.2 Documentation	78
B.3 Contact Information	79
B.4 Warranty and RMA Information	79
Index	80

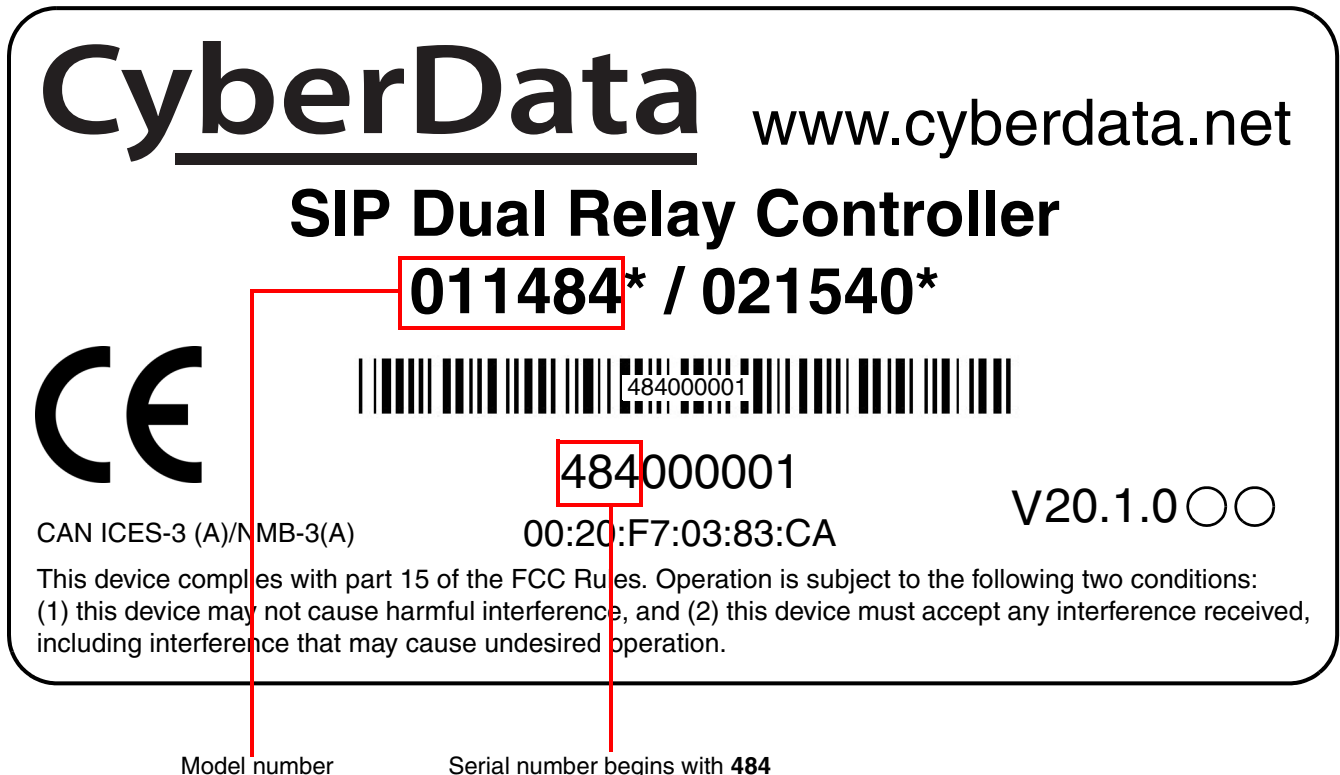
1 Product Overview and Setup

1.1 How to Identify This Product

To identify the SIP Dual Relay Controller, look for a model number label similar to the one shown in [Figure 1-1](#). Confirm the following:

- The model number on the label should be **011484**.
- The serial number on the label should begin with **484**.

Figure 1-1. Model Number Label



1.2 Typical System Installation

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


	<p>Warning <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 1-2. Single Door Typical Use Case

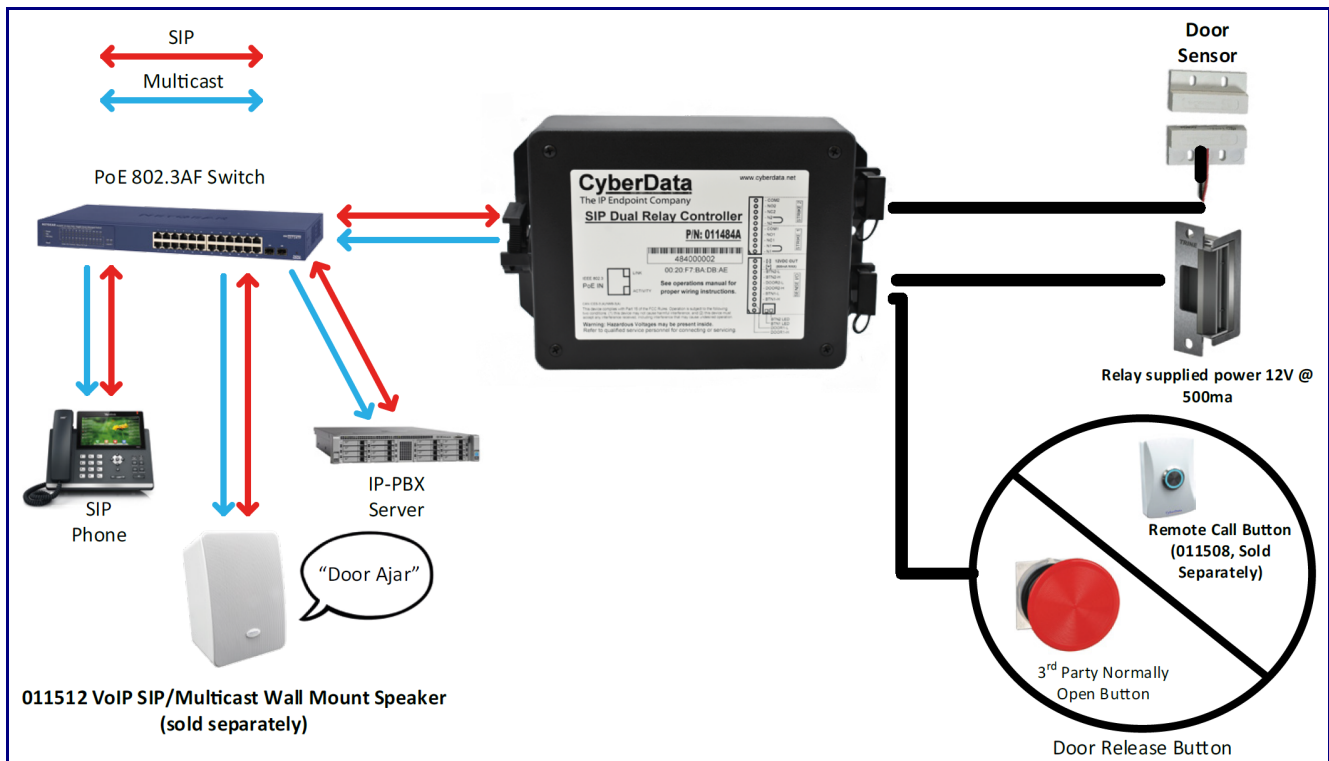


Figure 1-3. Typical Air Lock Use Case

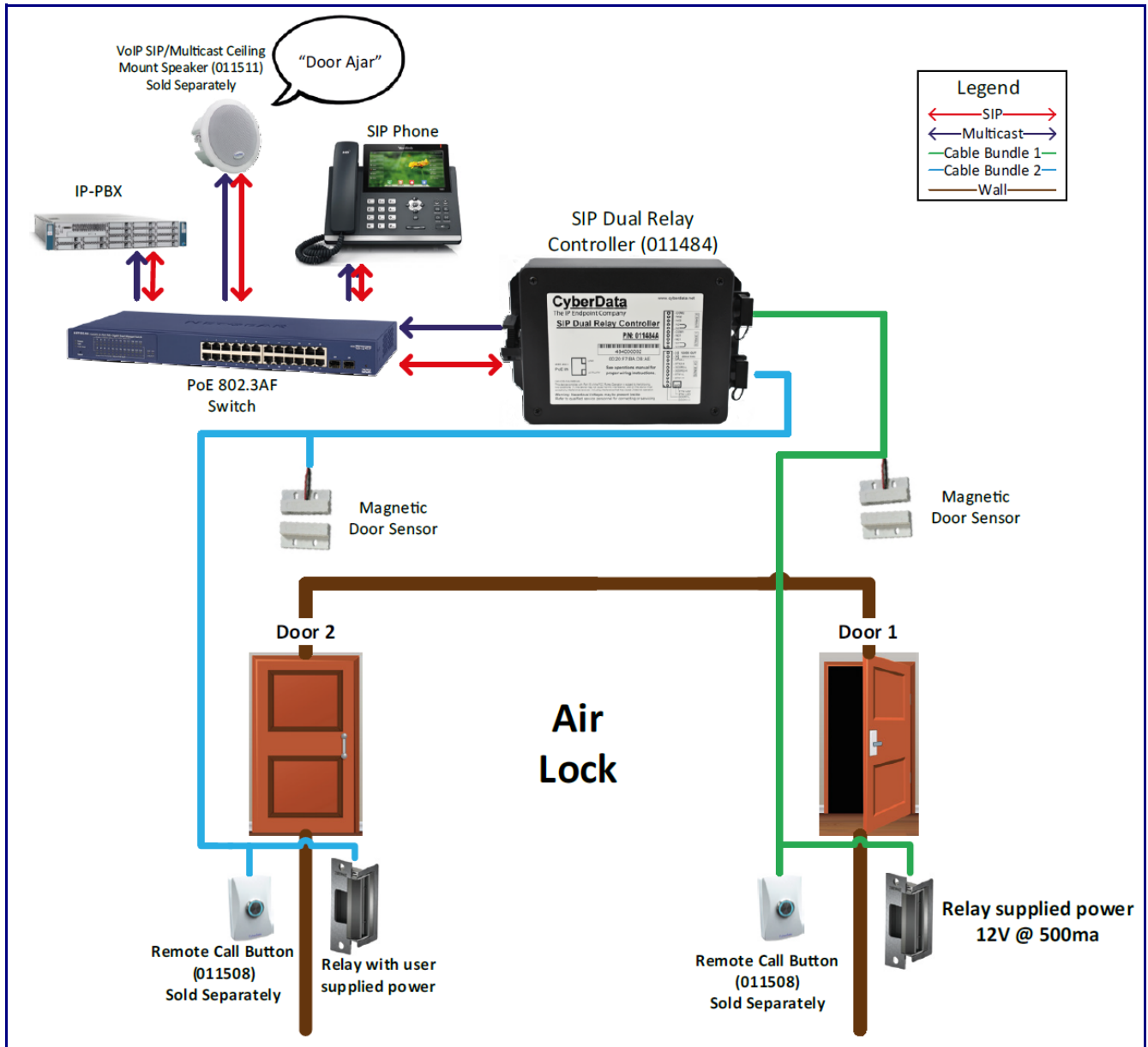
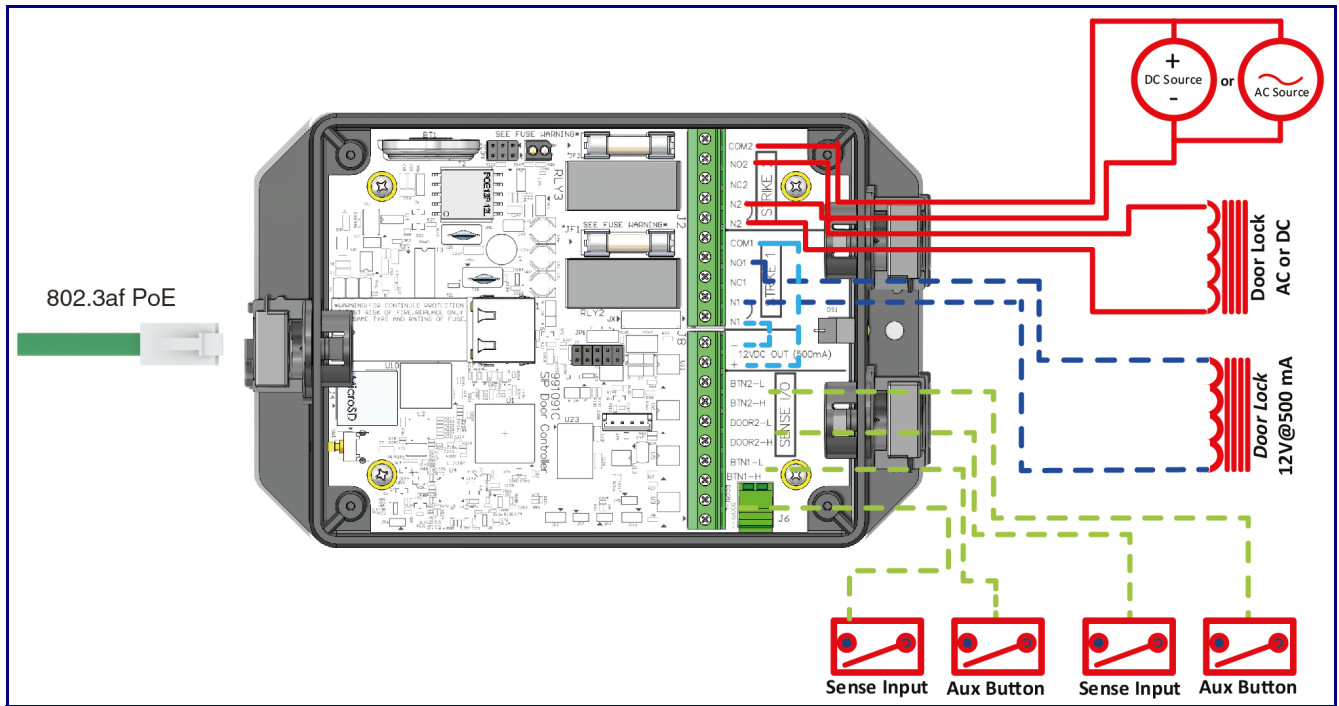


Figure 1-4. Wiring



1.3 Features

- Two high amperage relays, activated by DTMF or the web, can activate for a set time (pulse), indefinitely, or as an airlock
- Tamper alert can generate a SIP call to an extension
- Multicast page and/or SIP call on state of the sensor as configured by the user
- Time stamped access log
- Support for security code to prevent unwanted SIP calls
- Supports user-uploadable messages

- Dual 12A relays
- NO/NC contacts
- 12V @ 500 mA for direct powered strikes
- Opto-isolated sense inputs
- Device status LED
- Wall mounting
- Cable strain relief

- TLS 1.2 and SRTP enhanced security for IP endpoints in a local or cloud-based environment
- Autoprovisioning via HTTP, HTTPS, or TFTP
- HTTPS web based configuration
- Configurable event generation for device health and status monitoring
- 802.11q VLAN tagging
- Web-based upgradeable firmware
- Support for Cisco SRST resiliency

1.4 Specifications

Table 1-1. Specifications

Specifications	
Ethernet I/F	10/100 Mbps
Protocol	SIP RFC 3261 Compatible
Power Input	802.3af PoE
Relay Voltage/Current	12A@250VAC 12A@24VDC
Network Security	TLS 1.2, SRTP, HTTPS
Operating Range	Temperature: -40° C to 55° C (-40° F to 131° F) Humidity: 5-95%, non-condensing
Storage Temperature	-40° C to 70° C (-40° F to 158° F)
Storage Altitude	Up to 15,000 ft. (4573 m)
Dimensions ^a	6.586 inches [167.3 millimeter] Length 4.338 inches [110.3 millimeter] Width 2.600 inches [66 millimeter] Height
Weight	0.5 lbs [.23 kg]
Boxed Weight	1.0 lbs [.45 kg]
Compliance	RoHS Compliant; FCC Part 15 Class; Industry Canada ICES-3 Class A; IEEE 802.3 Compliant; TAA Compliant
Warranty	2 Years Limited
Part Number	011484

a. Dimensions are measured from the perspective of the product being upright with the front of the product facing you.

1.5 Compliance

1.5.1 RoHS Statement

RoHS Compliant. Flammability rating on all components is 94V-0.

1.5.2 FCC Statement



This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CAUTION: Changes or modifications not expressly approved by the manufacturer responsible for compliance could void the user's authority to operate the equipment.

1.5.3 Industry Canada (IC) Compliance Statement

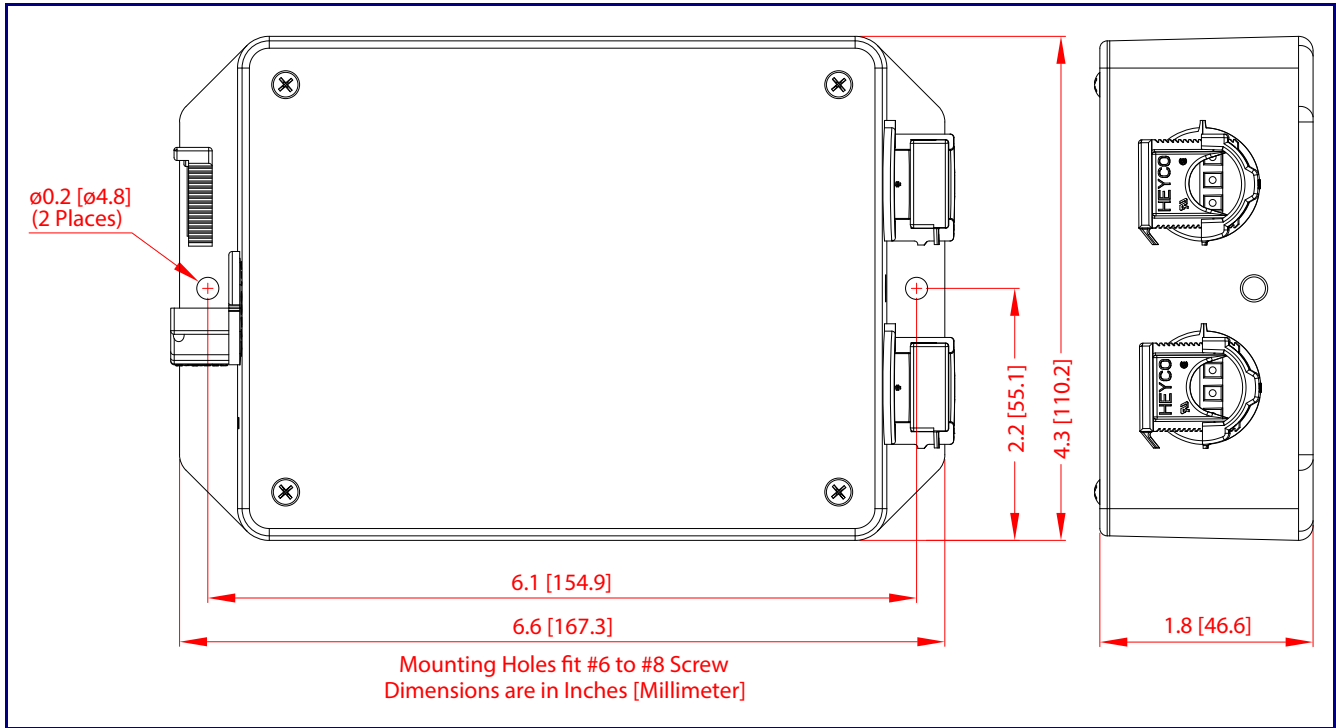
Operation is subject to the following two conditions:

1. This device may not cause interference, and
2. This device must accept any interference, including interference that may cause undesired operations of the device.

ICES-3 Class A

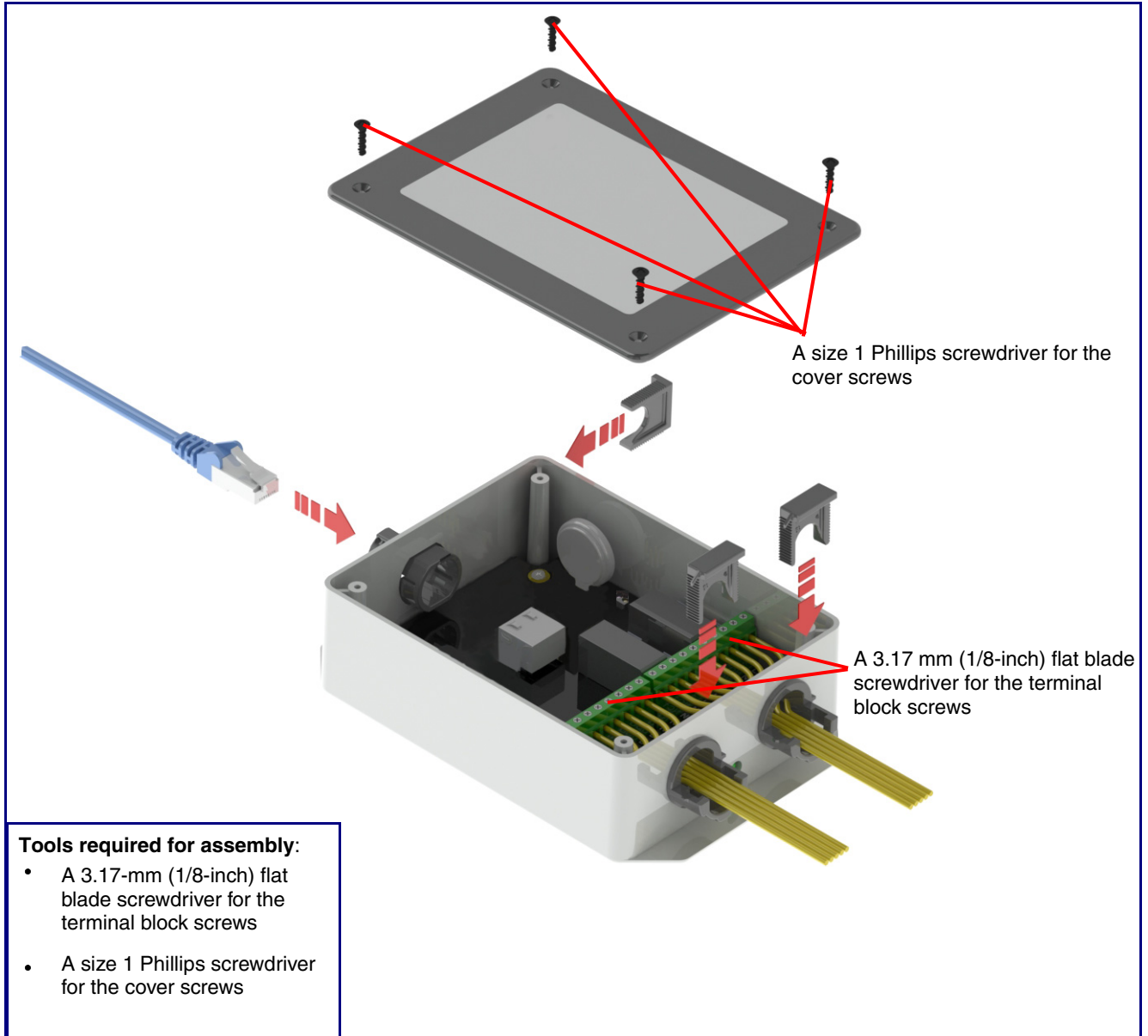
1.6 Dimensions

Figure 1-5. Dimensions



1.7 Assembly

Figure 1-6. Assembly



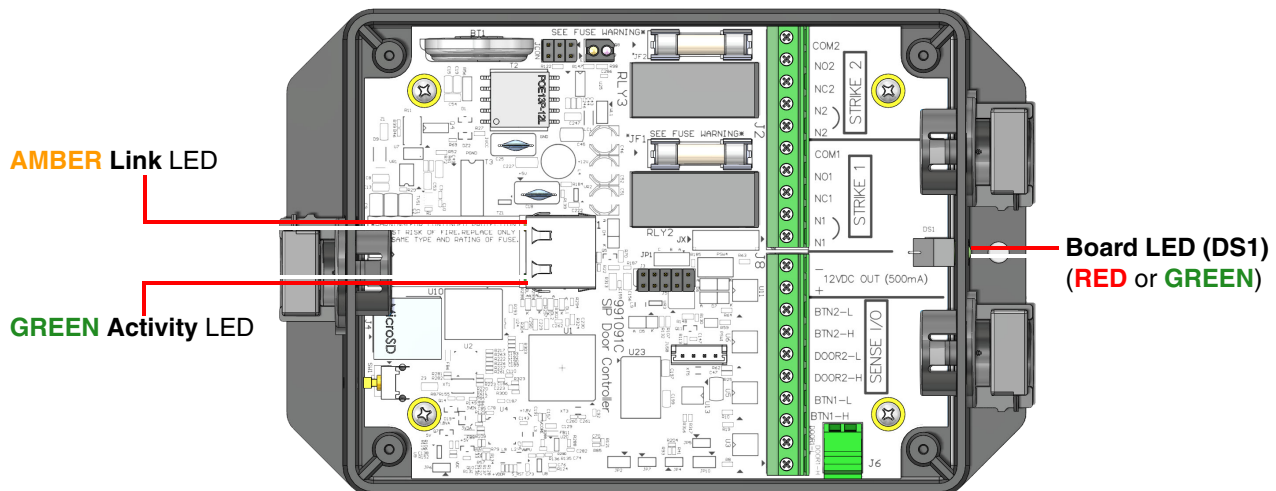
1.8 LED Behavior

See [Table 1-2](#) and [Figure 1-7](#) for the meaning of the device's LED behavior.

Table 1-2. 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: <ul style="list-style-type: none"> • Relay 1 and Relay 2 • Relay 1 and Sensor 2 • Sensor 1 and Relay 2 • Sensor 1 and Sensor 2

Figure 1-7. LEDs



1.9 Wiring the SIP Dual Relay Controller

1.9.1 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 1-8](#) and [Figure 1-9](#) for the wiring diagrams.


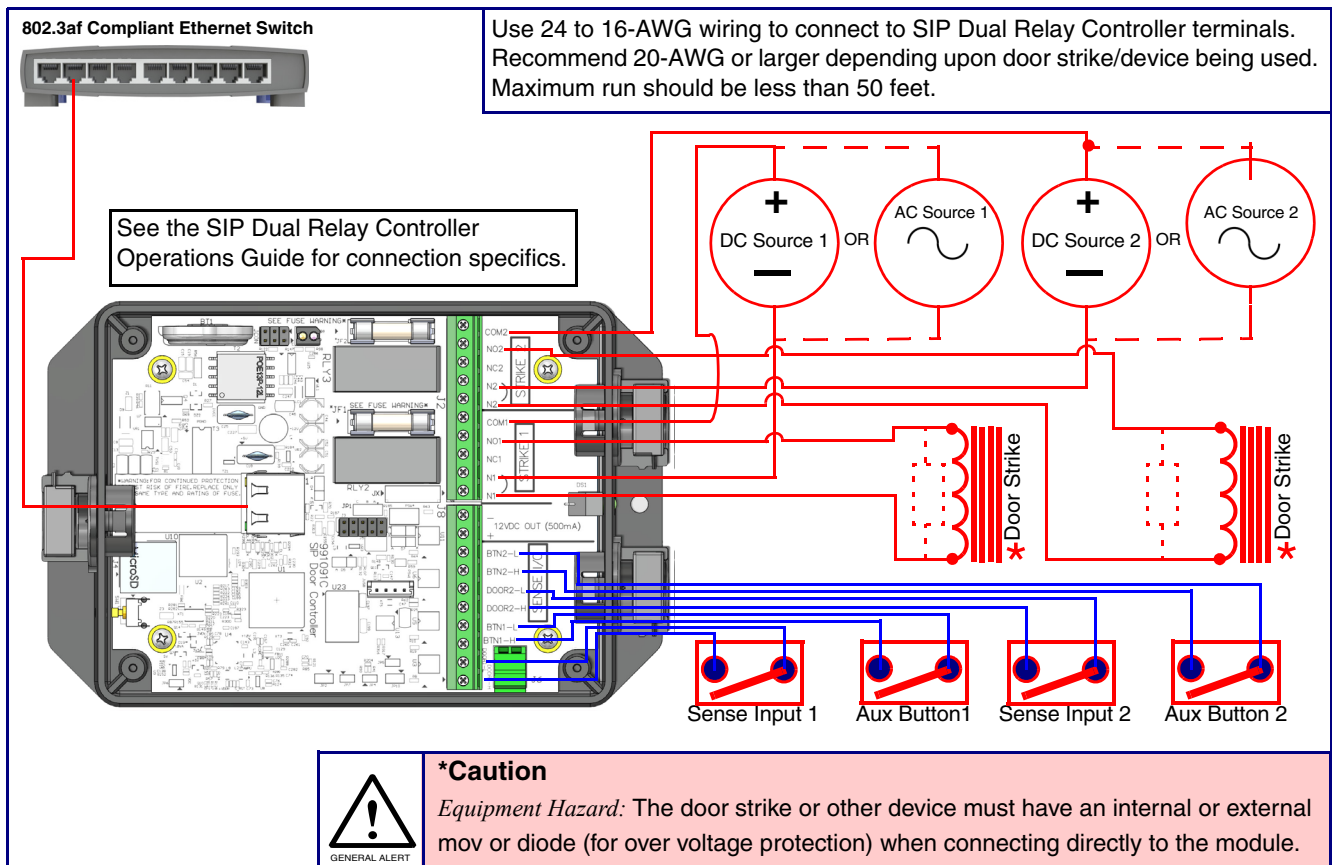
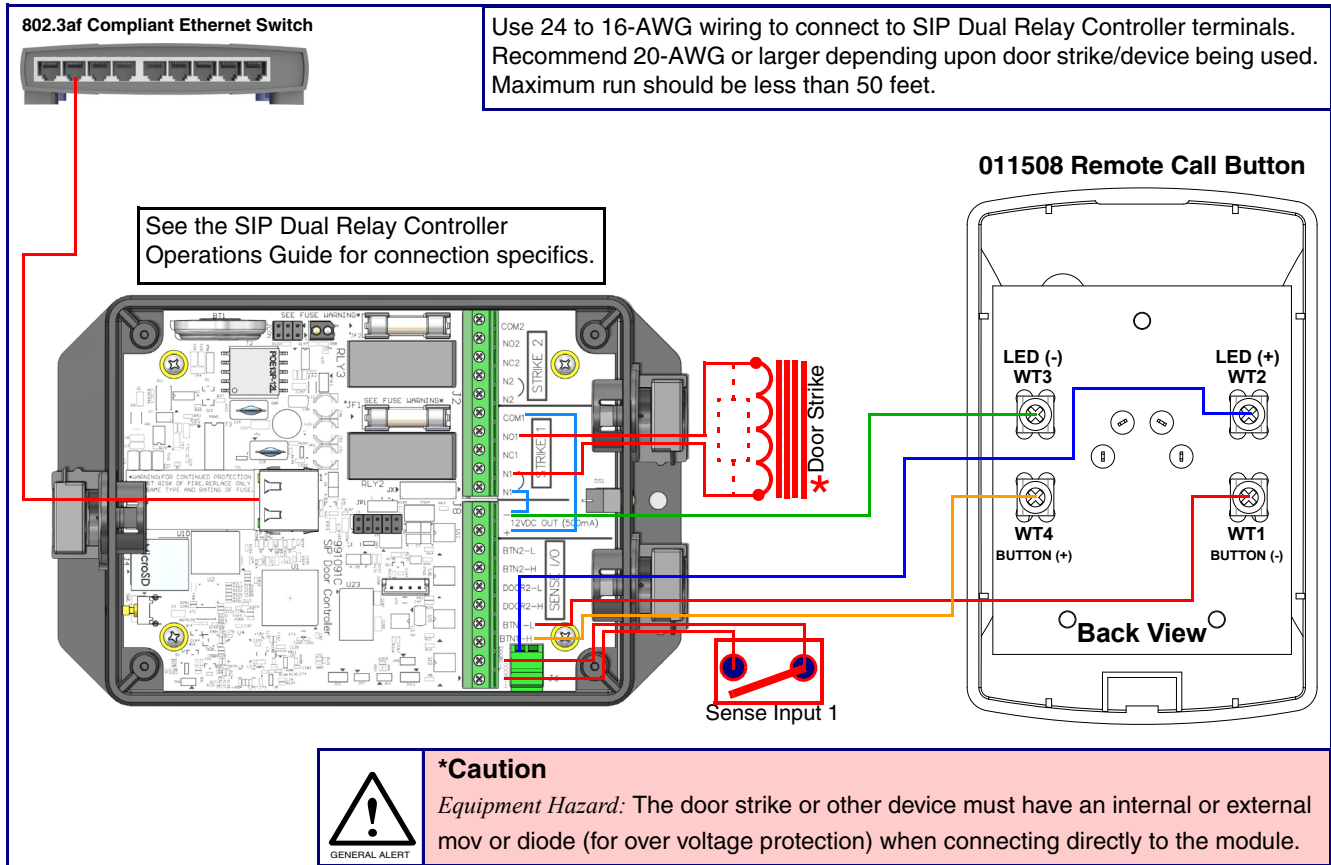
 <p>GENERAL ALERT</p>	<p>Warning</p> <p><i>Electrical Hazard:</i> Hazardous voltages may be present. No user serviceable part inside. Refer to qualified service personnel for connecting or servicing.</p>
--	--

Figure 1-8. SIP Dual Relay Controller Wiring Diagram with External Power Source



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

Figure 1-9. Diagram Using PoE Power and One SIP Dual Relay Controller with the 011508 Remote Call Button¹



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.

1.10 Terminal Block Wiring Connections

See Figure 1-10 and Table 1-3 for the terminal block wiring connections.

Figure 1-10. Terminal Block Wiring Connections

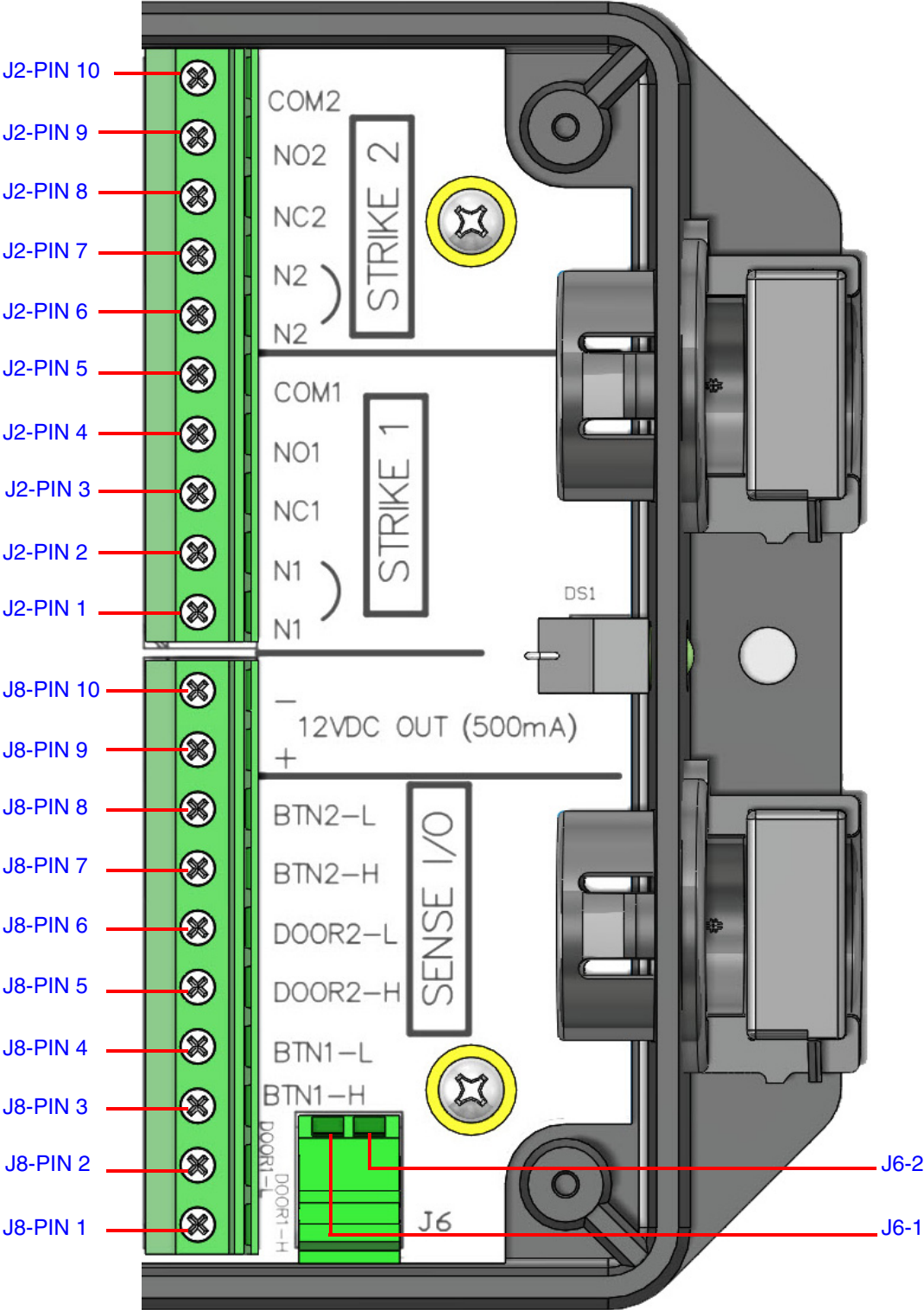


Table 1-3. Terminal Block Wiring Connections

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(+)

1.11 Jumper Definitions

See [Table 1-3](#) for the jumper definitions.

Table 1-4. Jumper Definitions

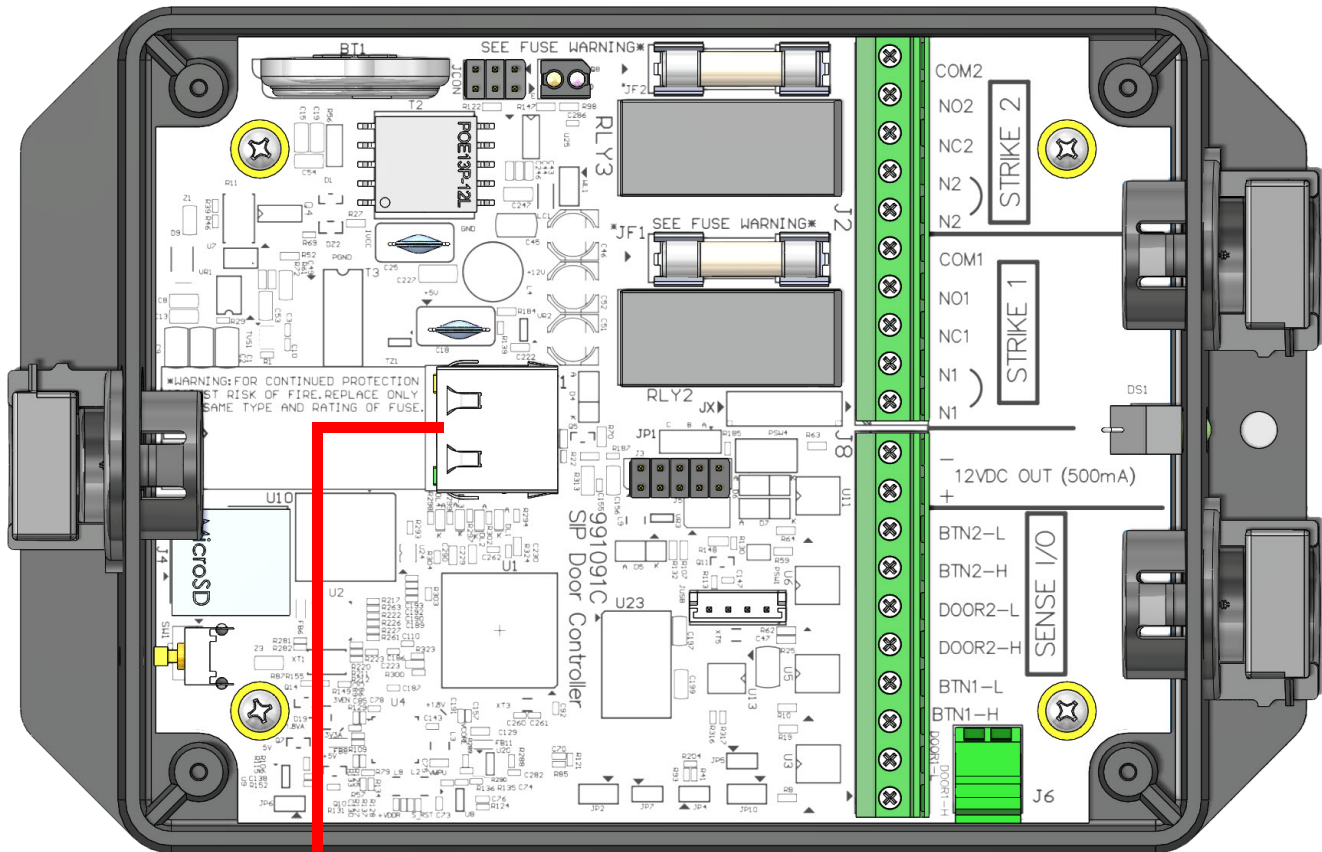
Jumper	Description
JP5	Missing Installed—Held in reset
JP10	Missing—Intrusion sensor enabled Installed—Intrusion sensor disabled

1.12 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.

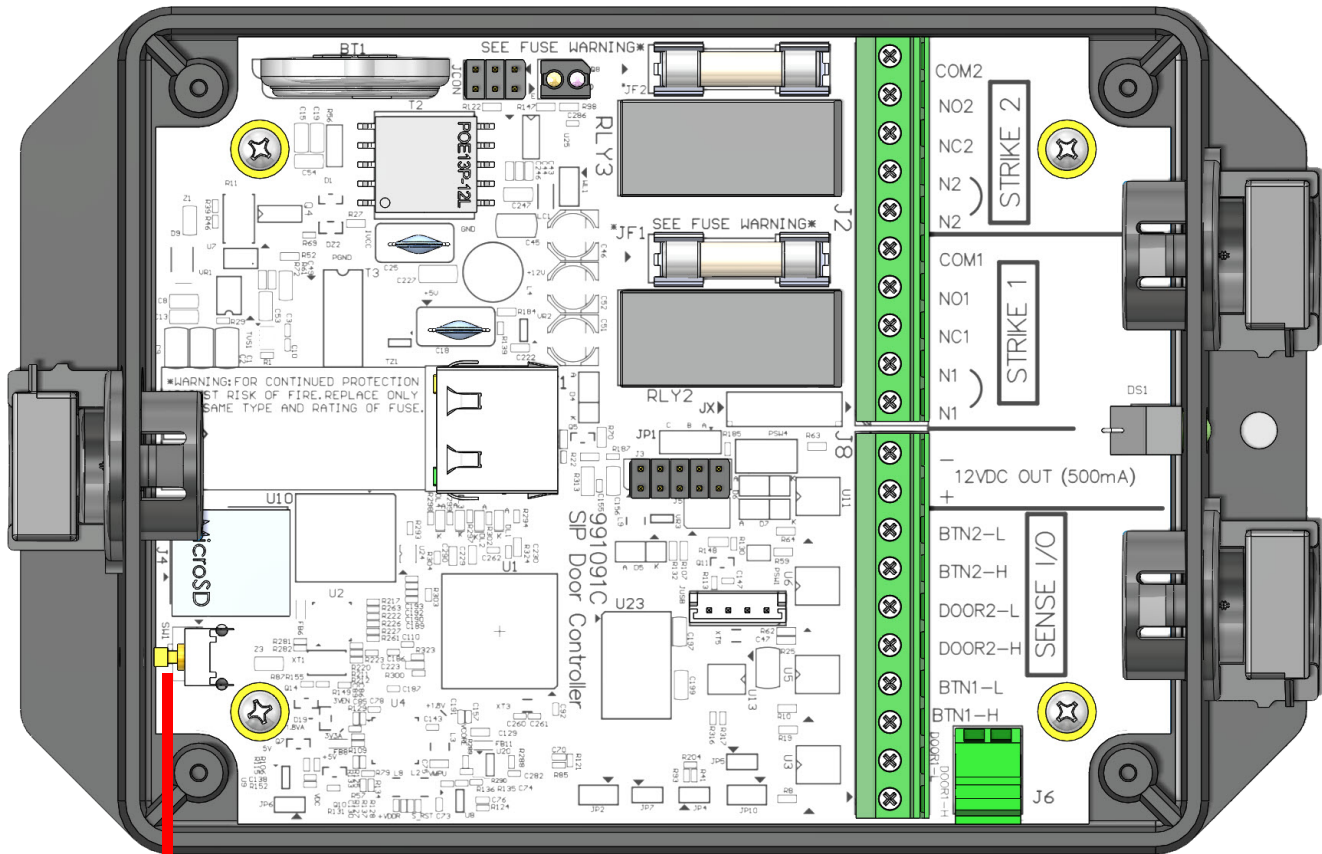
Figure 1-11. Connect a PoE network ethernet cable to J1



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 1-12. Press and hold the RTFM button for three to five seconds






Press and hold the RTFM button for three to five seconds

2 Installing the SIP Dual Relay Controller

2.1 Parts List

Table 2-1 illustrates the SIP Dual Relay Controller parts.

Table 2-1. Parts List

Quantity	Part Name	Illustration
1	SIP Dual Relay Controller Assembly	
1	Installation Quick Reference Guide	
1	SIP Dual Relay Controller Mounting Accessory Kit	

2.2 SIP Dual Relay Controller Components

Figure 2-1 shows the components of the SIP Dual Relay Controller.

Figure 2-1. SIP Dual Relay Controller Components



2.3 Configure the SIP Dual Relay Controller Parameters

To configure the SIP Dual Relay Controller online, use a standard web browser.

Configure each SIP Dual Relay Controller and verify its operation *before* you mount it.

2.3.1 Factory Default Settings

All SIP Dual Relay Controllers are initially configured with the following default IP settings:

When configuring more than one SIP Dual Relay Controller, attach the SIP Dual Relay Controllers to the network and configure one at a time to avoid IP address conflicts.

Table 2-2. Factory Default Settings

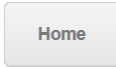
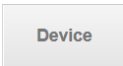



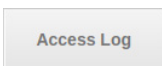

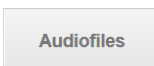
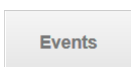
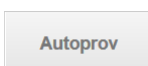

Parameter	Factory Default Setting
IP Addressing	DHCP
IP Address ^a	IPv4 Link Local
Web Access Username	admin
Web Access Password	admin
Subnet Mask ^a	IPv4 Link Local
Default Gateway ^a	IPv4 Link Local

a. Default if there is not a DHCP server present.

2.3.2 SIP Dual Relay Controller Web Page Navigation

Table 2-3 shows the navigation buttons that you will see on every SIP Dual Relay Controller web page.

Table 2-3. Web Page Navigation

Web Page Item	Description
	Link to the Home page.
	Link to the Device page.
	Link to the Network page.
	Link to go to the SIP page.
	Link to the SSL page.
	Link to the Access Log page.
	Link to the Sensor page.
	Link to the Audiofiles page.
	Link to the Events page.
	Link to the Autoprovisioning page.
	Link to the Firmware page.

2.3.3 Using the Toggle Help Button

The **Toggle Help** button allows you to see a short description of some of the settings on the webpage. To use the **Toggle Help** button, do the following:

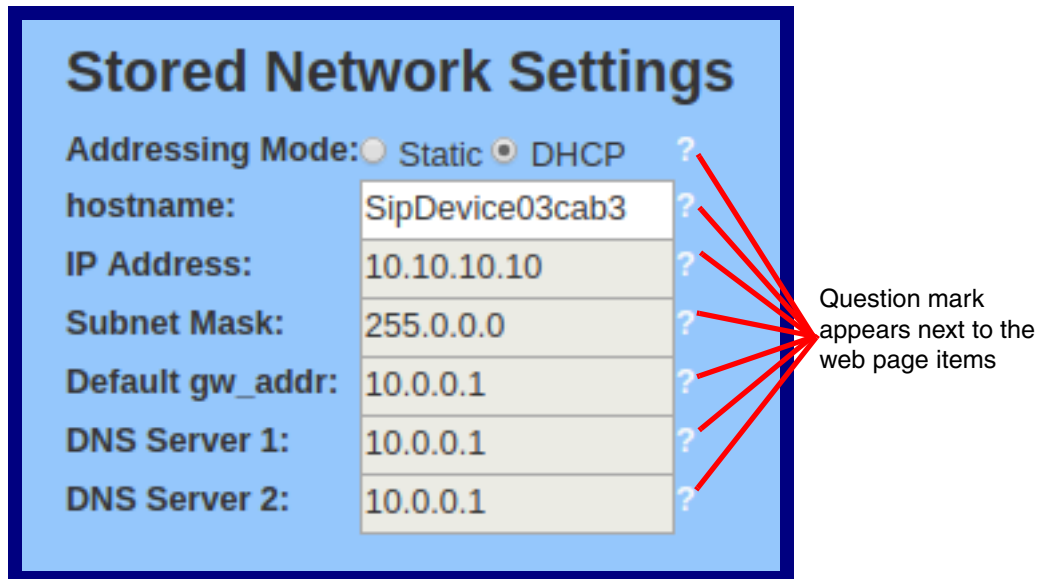
1. Click on the **Toggle Help** button that is on the UI webpage. See [Figure 2-2](#) and [Figure 2-3](#).

Figure 2-2. Toggle/Help Button



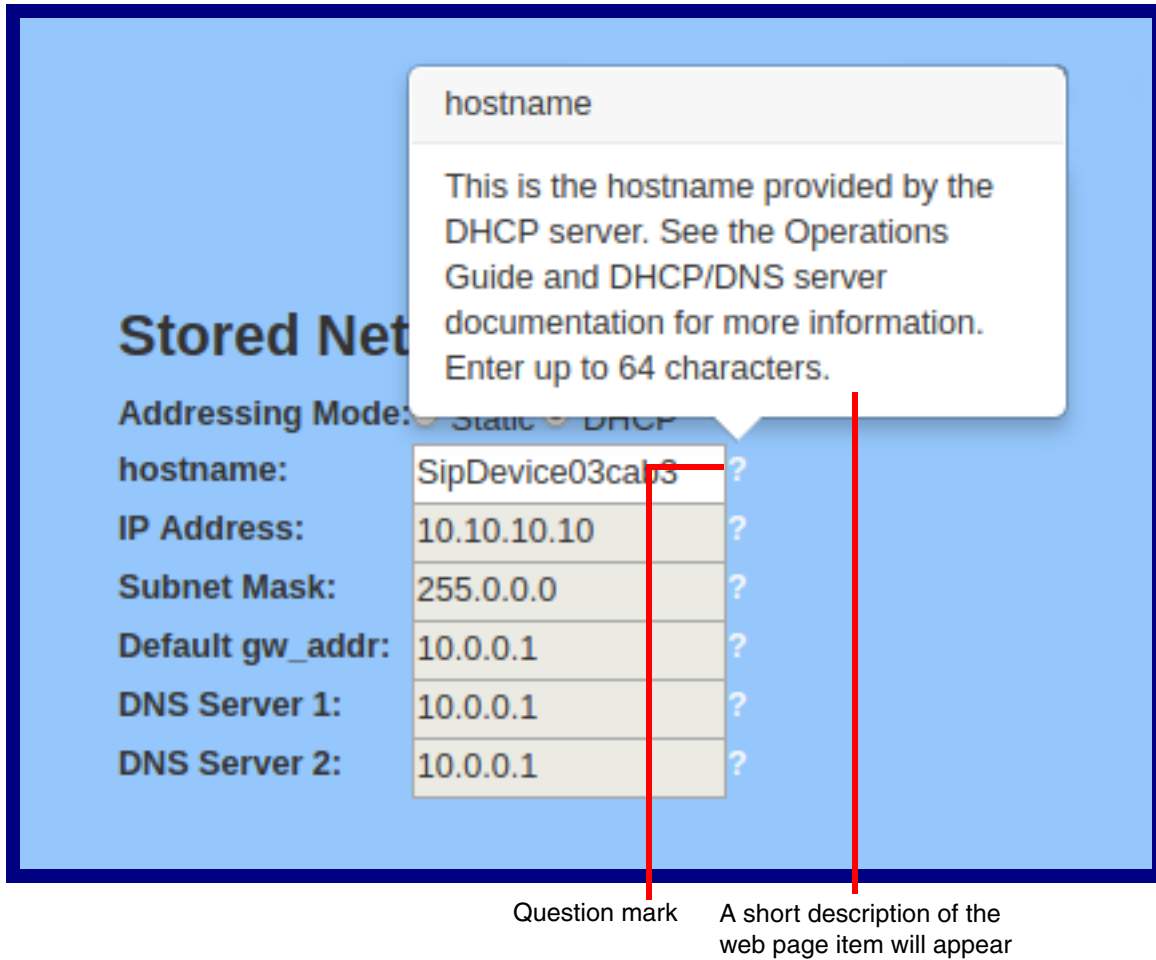
2. You will see a question mark (?) appear next to each web page item that has been provided with a short description by the Help feature. See [Figure 2-3](#).

Figure 2-3. Toggle Help Button and Question Marks



3. Move the mouse pointer to hover over the question mark (?), and a short description of the web page item will appear. See [Figure 2-4](#).

Figure 2-4. Short Description Provided by the Help Feature



2.3.4 Log in to the Configuration Home Page

1. Open your browser to the SIP Dual Relay Controller IP address.

Note If the network does not have access to a DHCP server, the device will default to an IP address of IPv4 Link Local.

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 device 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. When prompted, use the following default **Web Access Username** and **Web Access Password** to access the **Home Page** (Figure 2-5):

Web Access Username: **admin**

Web Access Password: **admin**

Figure 2-5. Home Page

The screenshot displays the home page of the SIP Dual Relay Controller web interface. At the top, there is a navigation bar with tabs for Home, Device, Network, SIP, SSL, Access Log, Sensor, Audiofiles, Events, Autoprov, and Firmware. The main heading is "SIP Dual Relay Controller".

Device Status

Serial Number:	48400001
Mac Address:	00:20:f7:04:de:7e
Firmware Version:	v20.1.0
Partition 2:	v20.1.0
Partition 3:	v20.1.0
Bootling From:	partition 2

[Boot From Other Partition](#)

IP Addressing: DHCP

IP Address:	10.10.0.208
Subnet Mask:	255.0.0.0
Default Gateway:	10.0.0.1
DNS Server 1:	10.0.1.56
DNS Server 2:	

SIP Mode: Enabled
Event Reporting: Disabled

Primary SIP Server: **Not registered**
Backup Server 1: Not registered
Backup Server 2: Not registered

Sensor Status

Relay 1 Status:	Locked
Sensor 1 Status:	Closed
Relay 2 Status:	Locked
Sensor 2 Status:	Closed
Intrusion:	Closed

Admin Settings

Username:

Password:

Confirm Password:

[Save](#) [Reboot](#) [Toggle Help](#)

Import Settings

[Browse...](#) No file chosen

[Import Config](#)

Export Settings

[Export Config](#)

3. On the **Home** page, review the setup details and navigation buttons described in [Table 2-4](#).

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-4. Home Page Overview







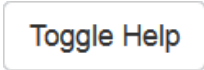
Web Page Item	Description
Admin Settings	
Username ?	The username to access the web interface. Enter up to 25 characters.
Password ?	The password to access the web interface. Enter up to 25 characters.
Confirm Password ?	Confirm the web interface password.
Device Status	
Serial Number	Shows the device serial number.
Mac Address	Shows the device Mac address.
Firmware Version	Shows the current firmware version.
Partition 2	Contains a complete copy of bootable software.
Partition 3	Contains an alternate, complete copy of bootable software.
Bootting From	Indicates the partition currently used for boot.
	Allows the user to boot from the alternate partition.
IP Addressing	Shows the current IP addressing setting (DHCP or static).
IP Address	Shows the current IP address.
Subnet Mask	Shows the current subnet mask address.
Default Gateway	Shows the current default gateway address.
DNS Server 1	Shows the current DNS Server 1 address.
DNS Server 2	Shows the current DNS Server 2 address.
SIP Mode	Shows the current status of the SIP mode.
Event Reporting	Shows the current status of the Event Reporting mode.
Primary SIP Server	Shows the current status of the Primary SIP Server.
Backup Server 1	Shows the current status of Backup Server 1.
Backup Server 2	Shows the current status of Backup Server 2.
Sensor Status	
Relay 1 Status	Shows the current status of relay 1 when the Home Page is refreshed.
Sensor 1 Status	Shows the current status of sensor 1 when the Home Page is refreshed.
Relay 2 Status	Shows the current status of relay 2 when the Home Page is refreshed.
Sensor 2 Status	Shows the current status of sensor 2 when the Home Page is refreshed.
Intrusion	Shows the current status of the intrusion sensor when the Home Page is refreshed.
Import Settings	
	Use this button to select a configuration file to import.

Table 2-4. Home Page Overview (continued)

Web Page Item	Description
	After selecting a configuration file, click Import to import the configuration from the selected file.
Export Settings	
	Click Export to export the current configuration to a file.
	Click the Save button to save your configuration settings.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

2.3.5 Configure the Device

1. Click the **Device** menu button to open the **Device** page. See [Figure 2-6](#).

Figure 2-6. Device Configuration Page

The screenshot shows the 'Device Configuration Page' for the 'SIP Dual Relay Controller'. The page has a light blue background and a dark blue border. At the top, there is a navigation menu with buttons for 'Home', 'Device', 'Network', 'SIP', 'SSL', 'Access Log', 'Sensor', 'Audiofiles', 'Events', 'Autoprov', and 'Firmware'. The 'Device' button is highlighted. Below the navigation menu, the title 'SIP Dual Relay Controller' is displayed in a large, bold, black font. The page is divided into three main sections: 'Clock Settings', 'DTMF Settings', and 'MISC Settings'.
Clock Settings: Includes 'Enable NTP' (checked), 'NTP Server' (north-america.pool.ntp.org), 'Timezone' (America/Los_Angeles), and 'Current Time' (Fri, 08 Apr 2022 11:08:35).
DTMF Settings: Includes 'Require Security Code' (unchecked), 'Security Code' (masked with dots), 'Relay 1 Pulse Duration' (10), 'Relay 2 Pulse Duration' (10), 'Relay 1 Automatic Mode Duration' (10), and 'Relay 2 Automatic Mode Duration' (10).
MISC Settings: Includes 'Device Name' (SIP Dual Relay Controller).
 At the bottom of the settings sections, there are buttons for 'Test Relay 1', 'Test Relay 2', 'Save', 'Reboot', and 'Toggle Help'.
 On the right side of the page, there is a table with two columns: 'DTMF' and 'Action'. The table lists various DTMF codes and their corresponding actions.

DTMF	Action
0	Announce current status of each relay
1	Activate relay 1
2	Deactivate relay 1
3	Pulse relay 1
4	Activate relay 2
5	Deactivate relay 2
6	Pulse relay 2
7	Activate both relays
8	Deactivate both relays
9	Automatic mode for entry
#	Automatic mode for exit
*	Play main menu

2. On the **Device** page, you may enter values for the parameters indicated in [Table 2-5](#).

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-5. Device Configuration Parameters






Web Page Item	Description
Clock Settings	
Enable NTP ?	Sync device's local time with the specified NTP Server.
NTP Server ?	Use this field to set the address (in IPv4 dotted decimal notation or as a canonical name) for the NTP Server. This field can accept canonical names of up to 64 characters in length.
Timezone	Enter the tz database string of your timezone. Examples: America/Los_Angeles America/New_York Europe/London America/Toronto See https://en.wikipedia.org/wiki/List_of_tz_database_time_zones for a full list of valid strings.
Current Time	Displays the current time.
Misc Settings	
Device Name ?	Type the device name. Enter up to 25 characters.
DTMF Settings	
Require Security Code ?	Requires each SIP connection to enter a security code for gaining access to the system's DTMF menu.
Security Code ?	Set the security code value, which must ONLY use digit characters '0-9.' The security code max length is 10 characters.
Relay 1 Pulse Duration ?	Time in seconds that relay 1 will be activated. Max time is 3600 seconds or one hour.
Relay 2 Pulse Duration ?	Time in seconds that relay 2 will be activated. Max time is 3600 seconds or one hour.
Relay 1 Automatic Mode Duration ?	Time in seconds that relay 1 will be activated during automatic mode. Max time is 3600 seconds or one hour.
Relay 2 Automatic Mode Duration ?	Time in seconds that relay 2 will be activated during automatic mode. Max time is 3600 seconds or one hour.
	Click on the Test Relay 1 button to do a relay 1 test.
	Click on the Test Relay 2 button to do a relay 2 test.
	Click the Save button to save your configuration settings.

Table 2-5. Device Configuration Parameters (continued)

Web Page Item	Description
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

2.3.6 Configure the Network Parameters

1. Click the **Network** menu button to open the **Network** page (Figure 2-7).

Figure 2-7. Network Configuration Page

Home Device **Network** SIP SSL Access Log Sensor Audiofiles Events Autoprov Firmware

SIP Dual Relay Controller

Stored Network Settings

Addressing Mode: Static DHCP

Hostname:

IP Address:

Subnet Mask:

Default Gateway:

DNS Server 1:

DNS Server 2:

Current Network Settings

IP Address: 10.10.0.208
Subnet Mask: 255.0.0.0
Default Gateway: 10.0.0.1
DNS Server 1: 10.0.1.56
DNS Server 2:

VLAN Settings




VLAN ID (0-4095):

VLAN Priority (0-7):

2. On the **Network** page, enter values for the parameters indicated in [Table 2-6](#).

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-6. Network Configuration Parameters

Web Page Item	Description
Stored Network Settings	
Addressing Mode ?	Select either DHCP IP Addressing or Static Addressing by marking the appropriate radio button. DHCP Addressing mode is enabled on default and the device will attempt to resolve network addressing with the local DHCP server upon boot. If DHCP Addressing fails, the device will revert to the last known IP address or the factory default address if no prior DHCP lease was established. See Section 2.3.1, "Factory Default Settings" for factory default settings. Be sure to click Save and Reboot to store changes when configuring a Static address.
Hostname ?	This is the hostname provided by the DHCP server. See the DHCP/DNS server documentation for more information. Enter up to 64 characters.
IP Address ?	Enter the Static IPv4 network address in dotted decimal notation.
Subnet Mask ?	Enter the Subnet Mask in dotted decimal notation.
Default Gateway ?	Enter the Default Gateway IPv4 address in dotted decimal notation.
DNS Server 1 ?	Enter the primary DNS Server IPv4 address in dotted decimal notation.
DNS Server 2 ?	Enter the secondary DNS Server IPv4 address in dotted decimal notation.
Current Network Settings	
IP Address	Shows the current Static IP address.
Subnet Mask	Shows the current Subnet Mask address.
Default Gateway	Shows the current Default Gateway address.
DNS Server 1	Shows the current DNS Server 1 address.
DNS Server 2	Shows the current DNS Server 2 address.
VLAN Settings	
VLAN ID (0-4095) ?	Specify the IEEE 802.1Q VLAN ID number. Enter up to 4 digits. A value of 0 disables vlan. Note: The device supports 802.1Q VLAN tagging support. The switch port connected to the device will need to be in "trunking mode" for the VLAN tags to propagate.
VLAN Priority (0-7) ?	Specify the IEEE 802.1p VLAN priority level. Enter 1 digit. A value of 0 may cause the VLAN ID tag to be ignored.
	Click the Save button to save your configuration settings.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

2.3.7 Configure the SIP (Session Initiation Protocol) Parameters

1. Click on the **SIP** menu button to open the **SIP** page (Figure 2-8).

Figure 2-8. SIP Configuration Page

SIP Settings

Enable SIP operation:

Register with a SIP Server:

Primary SIP Server:

Primary SIP User ID:

Primary SIP Auth ID:

Primary SIP Auth Password:

Re-registration Interval (in seconds):

Backup SIP Server 1:

Backup SIP User ID:

Backup SIP Auth ID:

Backup SIP Auth Password:

Re-registration Interval (in seconds):

Backup SIP Server 2:

Backup SIP User ID:

Backup SIP Auth ID:

Backup SIP Auth Password:

Re-registration Interval (in seconds):

Remote SIP Port:

Local SIP Port:

SIP Transport Protocol:

TLS Version:

Verify Server Certificate:

Outbound Proxy:

Outbound Proxy Port:

Use Cisco SRST:

Disable rport Discovery:

Keep Alive Period:

Call Disconnection

Terminate Call after delay:

Audio Codec Selection

Codec:

RTP Settings

RTP Port (even):

Asymmetric RTP:

Jitter Buffer:

RTP Encryption (SRTP):

2. On the **SIP** page, enter values for the parameters indicated in [Table 2-7](#).

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.








Table 2-7. SIP Configuration Parameters

Web Page Item	Description
SIP Settings	
Enable SIP Operation ?	When enabled, the device will transmit, receive, and process SIP messages according to the configured SIP settings below.
Register with a SIP Server ?	When enabled, the device will attempt to register to the configured SIP Server(s) on this page. To configure the device to send and receive point-to-point SIP calls, enable SIP Operation and disable Register with a SIP Server (see Section 2.3.7.2, "Point-to-Point Configuration").
Primary SIP Server ?	Enter the SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the primary SIP server. This field can accept entries of up to 255 characters in length.
Primary SIP User ID ?	Specify the SIP User ID for the Primary SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the primary SIP server. Enter up to 64 alphanumeric characters.
Primary SIP Auth ID ?	Specify the Authenticate ID for the Primary SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Primary SIP Auth Password ?	Specify the Authenticate Password for the Primary SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Re-registration Interval (in seconds) ?	The SIP Re-registration interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
Backup SIP Server 1 ?	Enter the backup SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the backup SIP server. This field can accept entries of up to 255 characters in length.
Backup SIP User ID 1 ?	Specify the SIP User ID for the first backup SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the first backup SIP server. Enter up to 64 alphanumeric characters.
Backup SIP Auth ID ?	Specify the Authenticate ID for the first backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Auth Password ?	Specify the Authenticate Password for the first backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Re-registration Interval (in seconds) ?	The SIP Re-registration interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
Backup SIP Server 2 ?	Enter a second backup SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the second backup SIP server. This field can accept entries of up to 255 characters in length.
Backup SIP User ID ?	Specify the SIP User ID for the second backup SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the second backup SIP server. Enter up to 64 alphanumeric characters.
Backup SIP Auth ID ?	Specify the Authenticate ID for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.

Table 2-7. SIP Configuration Parameters (continued)

Web Page Item	Description
Backup SIP Auth Password ?	Specify the Authenticate Password for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Re-registration Interval (in seconds) ?	The SIP Re-registration interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
Remote SIP Port ?	The Remote SIP Port is the port number the device will use as the destination port when sending SIP messages. The default Remote SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
Local SIP Port ?	The Local SIP Port is the port number the device will use to receive SIP messages. The default Local SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
SIP Transport Protocol ?	Choose the transport protocol for SIP signaling. This will affect all extensions, including the Nightringer. Default is UDP.
TLS Version ?	Choose the TLS version for SIP over TLS. Modern security standards strongly recommend using TLS 1.2.
Verify Server Certificate ?	When enabled, the device will verify the authenticity of the server during the TLS handshake by its certificate and common name. The TLS handshake will be aborted if the server is deemed to be inauthentic and SIP registration will not proceed.
Outbound Proxy ?	Enter the Outbound Proxy address as an IPv4 address in dotted decimal notation or a fully qualified domain name (FQDN). When an IP address is configured, the device will send all SIP messages to this IP address. When an FQDN is configured, the device will run DNS NAPTR, SRV, and A queries on the FQDN to resolve an IP address to which it will send all SIP messages. This field can accept entries of up to 255 characters in length.
Outbound Proxy Port ?	The Outbound Proxy Port is port number used as the destination port when sending SIP messages to the outbound proxy. A value of 0 will default to 5060. The supported range is 0-65536. Enter up to 5 digits.
Use Cisco SRST ?	When enabled, the backup servers are handled according to Cisco SRST (Survivable Remote Site Telephony). It is required for use in clustered Cisco Unified Communications Manager topologies.
Disable rport Discovery ?	Disabling rport Discovery will prevent the device from including the public WAN IP address and port number in the contact information that is sent to the remote SIP servers. This will generally only need to be enabled when using an SBC or SIP ALG in conjunction with a remote SIP server.
Keep Alive Period ?	The minimum time in milliseconds between keep-alive packets sent for nat traversal. A value of 0 will disable keep alive packets.
Call Disconnection	
Terminate Call After Delay ?	Automatically terminate an active call after a given delay in seconds. A value of 0 will disable this function. Enter up to 8 digits.
Audio Codec Selection	
Codec ?	Select the desired codec (only one may be chosen).
RTP Settings	
RTP Port (even) ?	Specify the port number used for the RTP stream after establishing a SIP call. This port number must be an even number and defaults to 10500. The supported range is 0-65536. Enter up to 5 digits.

Table 2-7. SIP Configuration Parameters (continued)

Web Page Item	Description
Asymmetric RTP 	<p>Specify if the remote endpoint will send and receive RTP packets on different ports. If set to false, the device will track the address/port that is sending RTP packets during a SIP call. If the address/port changes mid-stream, the device will disregard the SDP and send all further RTP packets to this new address.</p> <p>If set to true, this device will ignore the sending address/port and send RTP as specified in the SDP. Warning! Enabling asymmetric RTP can cause the RTP stream to be lost.</p> <p>Most installations should not enable asymmetric RTP.</p>
Jitter Buffer 	Specify the size of the jitter buffer (in milliseconds) used for SIP calls. Valid values are 50-1000.
RTP Encryption (SRTP) 	When enabled, a SIP call's audio streams are encrypted using SRTP.
	Click the Save button to save your configuration settings.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark () appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

Note For specific server configurations, go to the following website address:
<https://www.cyberdata.net/pages/connecting-to-ip-pbx-servers>

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

On the [SIP Configuration Page](#), dial out extensions support the addition of comma delimited pauses and sending additional DTMF tones (using rfc2833). The first comma will pause three seconds after a call is first established with a remote device. Subsequent commas will pause for 2 seconds. A pause of one second will be sent after each numerical digit.

Table 2-8. Examples of Dial-Out Extension Strings

Extension String	Resulting Action
302	Dial out extension 302 and establish a call
302,2	Dial out extension 302 and establish a call, wait 3 seconds then send the DTMF tone '2'
302,25,,,4,,1	Dial out extension 302 and establish a call, wait 3 seconds then send the DTMF tone '2', send out DTMF tone 5, wait 6 seconds, send out DTMF tone 4, wait 4 seconds, send out DTMF tone 1

Note The maximum number of total characters in the dial-out field is 64.

2.3.7.2 Point-to-Point Configuration

When the device is set to not register with a SIP server (see [Figure 2-9](#)), it is possible to set the device to dial out to a single endpoint.

In this case, the dial-out extension should be the IP address of the remote device. The device can also receive Point-to-Point calls. The delayed DTMF functionality is available in the Point-to-Point Mode.

Note Receiving point-to-point SIP calls may not work with all phones.

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



Device is set to NOT register with a SIP server

2.3.7.3 Delayed DTMF

On the **SIP Configuration** page the dial out extension supports the addition of comma delimited pauses and sending additional DTMF tones (using rfc2833). The first comma will pause three seconds after a call is first established with a remote device. Subsequent commas will pause for 2 seconds. A pause of one second will be sent after each numerical digit.

Table 2-9. Examples of Dial-Out Extension Strings

Extension String	Resulting Action
302	Dial out extension 302 and establish a call
302,2	Dial out extension 302 and establish a call, wait 3 seconds then send the DTMF tone '2'
302,25,,,4,,1	Dial out extension 302 and establish a call, wait 3 seconds then send the DTMF tone '2', send out DTMF tone 5, wait 6 seconds, send out DTMF tone 4, wait 4 seconds, send out DTMF tone 1

Note The maximum number of total characters in the dial-out field is 25.

2.3.8 Configure the SSL Parameters

1. Click **SSL** menu button to open the **SSL** page (Figure 2-16).

Figure 2-10. SSL Configuration Page

The screenshot displays the SSL Configuration page for the SIP Dual Relay Controller. The page is organized into three main sections for certificate management: Web Server Certificate, SIP Client Certificate, and Autoprovisioning Client Certificate. Each section includes a pre-filled certificate details box, a file selection button, an import button, and a restore button. Additionally, there are optional password fields for each certificate type. The bottom of the page features a 'Test TLS Connection' section with server and port input fields, a 'Download CyberData_CA.pem' button, and a 'List of Trusted CAs' section with an upload button and a table of existing certificates.

Index	CA Certificate Name	Info	Remove
1	CyberData_CA.pem	Info	Remove
2	DST_Root_CA_X3.crt	Info	Remove
3	DigiCert_Assured_ID_Root_CA.crt	Info	Remove
4	DigiCert_Assured_ID_Root_G2.crt	Info	Remove
5	DigiCert_Assured_ID_Root_G3.crt	Info	Remove
6	DigiCert_Global_Root_CA.crt	Info	Remove
7	DigiCert_Global_Root_G2.crt	Info	Remove

Figure 2-11. SSL Configuration Page

7	DigiCert_Global_Root_G2.crt	Info	Remove
8	DigiCert_Global_Root_G3.crt	Info	Remove
9	DigiCert_High_Assurance_EV_Root_CA.crt	Info	Remove
10	DigiCert_Trusted_Root_G4.crt	Info	Remove
11	GeoTrust_Global_CA.crt	Info	Remove
12	GeoTrust_Primary_Certification_Authority.crt	Info	Remove
13	GeoTrust_Primary_Certification_Authority_-_G2.crt	Info	Remove
14	GeoTrust_Primary_Certification_Authority_-_G3.crt	Info	Remove
15	GeoTrust_Universal_CA.crt	Info	Remove
16	GeoTrust_Universal_CA_2.crt	Info	Remove
17	Go_Daddy_Class_2_CA.pem	Info	Remove
18	Go_Daddy_Root_Certificate_Authority_-_G2.pem	Info	Remove
19	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G4.crt	Info	Remove
20	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5.crt	Info	Remove
21	VeriSign_Universal_Root_Certification_Authority.crt	Info	Remove
22	Verisign_Class_1_Public_Primary_Certification_Authority.crt	Info	Remove
23	Verisign_Class_1_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
24	Verisign_Class_2_Public_Primary_Certification_Authority_-_G2.crt	Info	Remove
25	Verisign_Class_2_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
26	Verisign_Class_3_Public_Primary_Certification_Authority.crt	Info	Remove
27	Verisign_Class_3_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
28	thawte_Primary_Root_CA.crt	Info	Remove
29	thawte_Primary_Root_CA_-_G2.crt	Info	Remove
30	thawte_Primary_Root_CA_-_G3.crt	Info	Remove

2. On the **SSL** page, enter values for the parameters indicated in [Table 2-10](#).

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-10. SSL Configuration Parameters

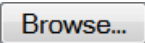


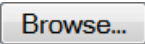


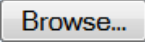
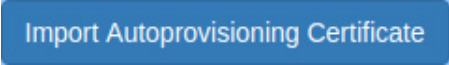
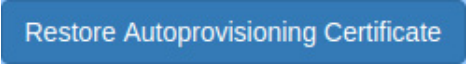
Web Page Item	Description
Web Server Certificate	Certificate used by the web server.
	Click Browse to select a certificate to import.
	After selecting a certificate, click Import Web Certificate to import it as the certificate used by this device's web server.
	Restore the device's default web server certificate. This will remove the user-uploaded Web Server Certificate.(Server CAs and Trusted CAs are unaffected).
SIP Client Certificate	When doing mutual authentication this device will present a client certificate with these parameters.
	Click Browse to select a certificate to import.
	After selecting a certificate, click Import SIP Certificate to import it as the certificate used by the device during SIP transactions.
	Restore the device's default sip client certificate. This will remove any user-uploaded sip client certificates (Server CAs and Trusted CAs are unaffected).
Optional Password	Enter the optional password for the SIP certificate's private key. Note: When using a password, it must be entered and saved before importing the certificate.
Autoprovisioning Client Certificate	When doing mutual authentication this device will present a client certificate with these parameters.
	Click Browse to select a certificate to import.
	After selecting a certificate, click Import Autoprovisioning Certificate to import it as this device's certificate. This certificate will be used when requesting files during autoprovisioning.
	Restore the device's default autoprovisioning certificate. This will remove any user-uploaded autoprovisioning certificates. (Server CAs and Trusted CAs are unaffected).
Optional Password ?	Enter the optional password for the Autoprovisioning certificate's private key. Note: When using a password, it must be entered and saved before importing the certificate.
Cyberdata CA ?	Right click and Save Link As... to get the Cyberdata CA used to sign this client certificate.

Table 2-10. SSL Configuration Parameters (continued)



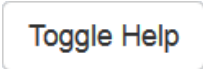




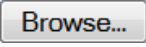




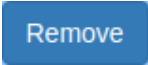
Web Page Item	Description
	Click the Save button to save your configuration settings.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.
Test TLS Connection	
Server 	The ssl test server address as a fully qualified domain name or in IPv4 dotted decimal notation.
Port 	The supported range is 0-65536. SIP connections over TLS to port 5060 are modified to connect to port 5061. This test button will do the same.
	Use this button to test a TLS connection to a remote server using the sip client key and password. This will attempt to make a socket connection to the configured test server and port and report the success or failure. This can be used to debug TLS connection issues separate from SIP registration issues.
	Use this button to test a TLS connection to a remote server using the autoprovisioning client key and password. This will attempt to make a socket connection to the configured test server and port and report the success or failure. This can be used to debug TLS connection issues with secure autoprovisioning.
List of Trusted CAs	
	Use this button to select a configuration file to import.
	Click Browse to select a CA certificate to import. After selecting a server certificate authority (CA), click Import CA Certificate to import it to the list of trusted CAs. CAs are used to validate the certificate presented by the server when establishing a TLS connection.
	Restore Defaults will restore the default list of registered CAs and Remove All will remove all registered CAs.
	Restore Defaults will restore the default list of registered CAs and Remove All will remove all registered CAs.
	Provides details of the certificate. After clicking on this button, the Certificate Info Window appears. See Section 2.3.8.1, "Certificate Info Window" .

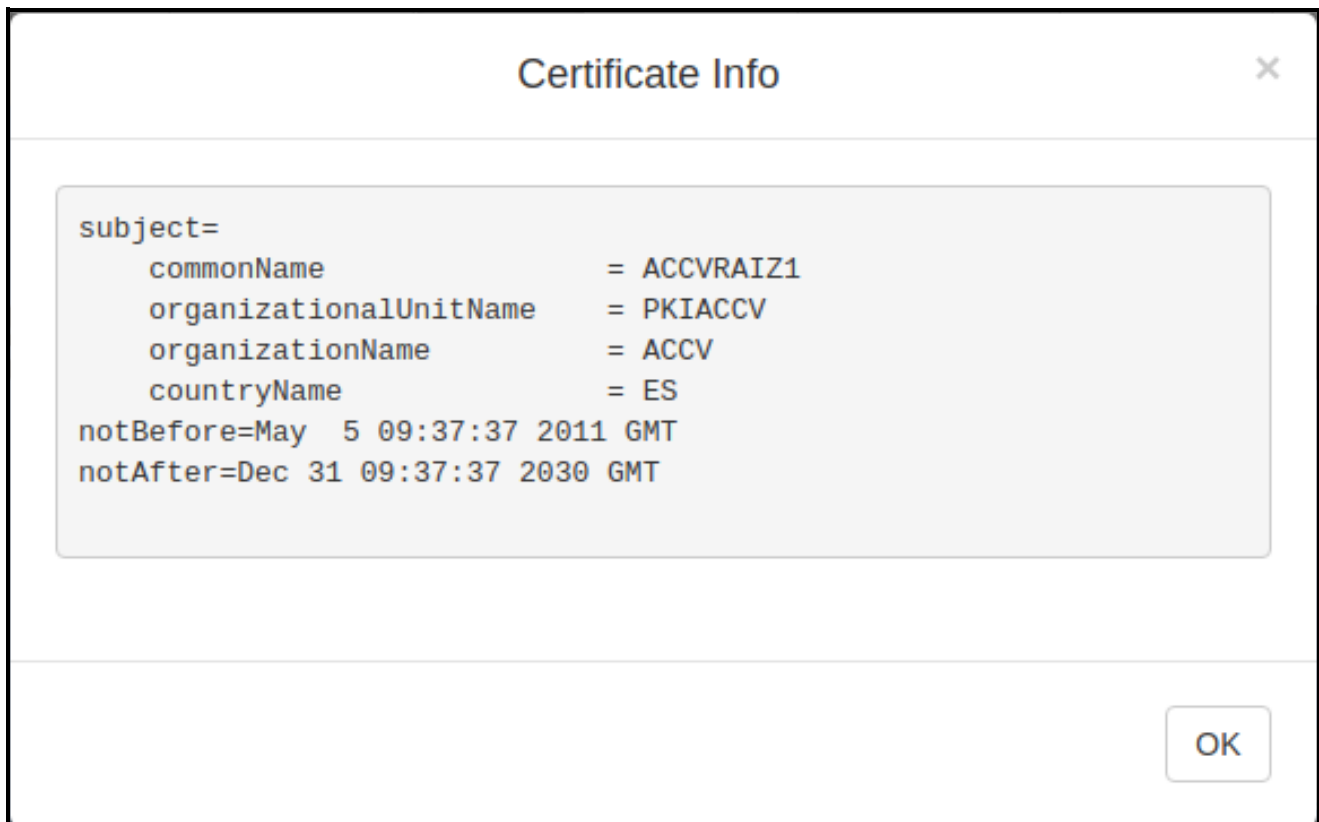
Table 2-10. SSL Configuration Parameters (continued)

Web Page Item	Description
	Removes this certificate from the list of trusted certificates. After clicking on this button, the Remove Server Certificate Window appears. See Section 2.3.8.2, "Remove Server Certificate Window" .

2.3.8.1 Certificate Info Window

The **Certificate Info Window** provides details of the certificate. This window appears after clicking on the **Info** button. See [Figure 2-12](#).

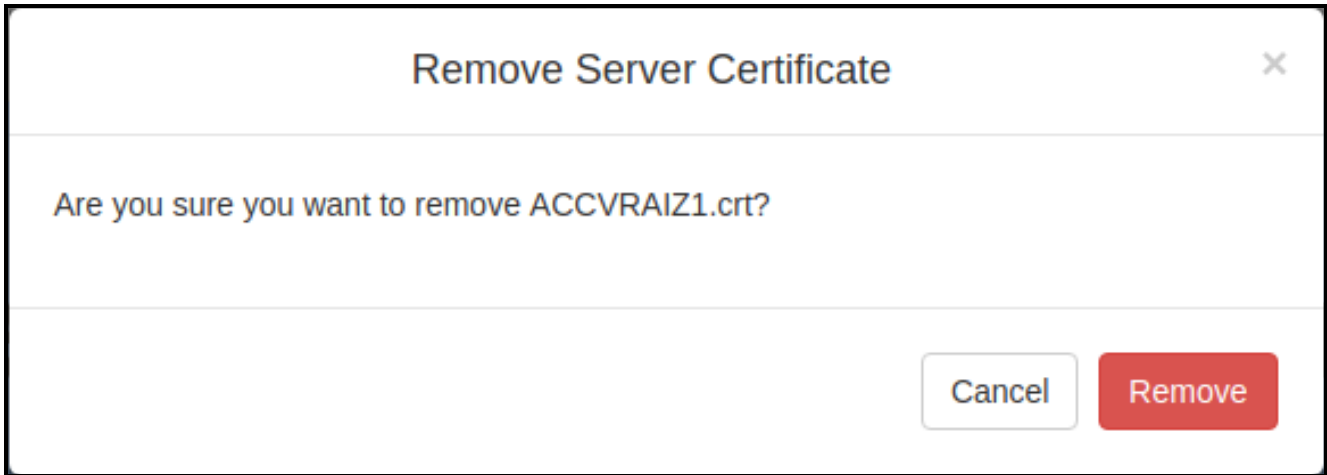
Figure 2-12. Certificate Info Window



2.3.8.2 Remove Server Certificate Window

The **Remove Server Certificate Window** will ask if the user wants to remove a certificate from the list of trusted certificates. This window appears after clicking on the **Remove** button. See [Figure 2-13](#).

Figure 2-13. Remove Server Certificate Window



2.3.9 Configure the Access Log Parameters

1. Click the **Access Log** menu button to open the **Access Log** page (Figure 2-16).

Figure 2-14. Access Log Page

The screenshot shows the 'Access Log' page of the SIP Dual Relay Controller. The page has a light blue background and a dark blue border. At the top, there is a navigation menu with buttons for Home, Device, Network, SIP, SSL, Access Log (selected), Sensor, Audiofiles, Events, Autoprov, and Firmware. Below the menu, the title 'SIP Dual Relay Controller' is displayed in large, bold, black font. Underneath the title, the text 'Access Log' is centered. There are three buttons: 'Refresh', 'Clear', and 'Download'. To the right of these buttons is a search box with the placeholder text 'Search'. Below the search box is a table with the following data:










Event #	Timestamp	Action	Caller ID	Info
7	Fri 2022-04-08 10:44:17 AM	Intrusion Sensor Activated		
6	Fri 2022-04-08 10:13:13 AM	Intrusion Sensor Activated		
5	Thu 2022-04-07 14:44:27 PM	Intrusion Sensor Activated		
4	Thu 2022-04-07 14:22:09 PM	Intrusion Sensor Activated		
3	Thu 2022-04-07 14:19:33 PM	Intrusion Sensor Activated		
2	Thu 2022-04-07 14:16:35 PM	Intrusion Sensor Activated		
1	Thu 2022-04-07 14:11:11 PM	Intrusion Sensor Activated		

Showing 1 to 7 of 7 rows

- On the **Access Log** page, enter values for the parameters indicated in [Table 2-10](#).

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

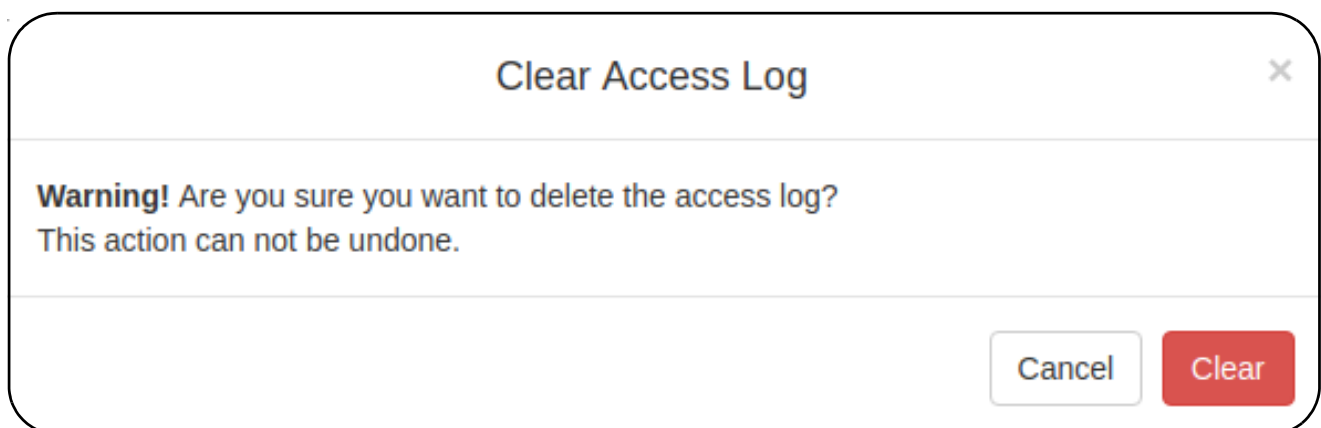
Table 2-11. Access Log Configuration Parameters

Web Page Item	Description
Access Log	
	Refresh the web page view new log entries.
	Erases the log. When pressed, the Clear Access Log Confirmation Window appears. See Section 2.3.9.1, "Clear Access Log Confirmation Window" .
	Downloads the access log.
Search 	Search the access log.
Event # 	System generated number to identify the event.
Timestamp 	Displays the time of the event (Day of week Year-Month-Day Hour:Minute:Seconds AM/PM).
Action 	Describes the event.
User ID 	Displays the ID number of the user.
User Name 	Displays the name of the user.

2.3.9.1 Clear Access Log Confirmation Window

The **Clear Access Log Confirmation Window** will ask if the user wants to delete the access log. This window appears after clicking on the **Clear** button. See [Figure 2-15](#).

Figure 2-15. Clear Access Log Confirmation Window



2.3.10 Configure the Sensor Configuration Parameters

1. Click **Sensor** menu button to open the **Sensor** page (Figure 2-16).

Figure 2-16. Sensor Configuration Page

The screenshot displays the 'Sensor Configuration Page' for the SIP Dual Relay Controller. The page has a light blue background and a navigation bar at the top with tabs for Home, Device, Network, SIP, SSL, Access Log, Sensor (selected), Audiofiles, Events, Autoprov, and Firmware. The main heading is 'SIP Dual Relay Controller'. Below this, there are five configuration sections: Sensor 1, Sensor 2, Intrusion Sensor, Button 1, and Button 2. Each section contains various input fields and checkboxes. The Intrusion Sensor section also includes several action buttons: Test Intrusion Sensor, Test Sensor 1, Test Sensor 2, Test Button 1, Test Button 2, Save, Reboot, and Toggle Help.

Section	Parameter	Value
Sensor 1	Sensor Activated Timeout	12 seconds
	Sensor Type	Normally Open
	Call to Extension	<input type="checkbox"/>
	Dial Out Extension	204
	Dial Out ID	id204
	Audio Playbacks	12
	Multicast Audio	Disabled
	Multicast Address	239.168.3.10
	Multicast Port	8888
	Multicast TTL	255
Sensor 2	Sensor Activated Timeout	12 seconds
	Sensor Type	Normally Open
	Call to Extension	<input type="checkbox"/>
	Dial Out Extension	204
	Dial Out ID	id204
	Audio Playbacks	12
	Multicast Audio	Disabled
	Multicast Address	239.168.3.1
	Multicast Port	8888
	Multicast TTL	255
Intrusion Sensor	Call to Extension	<input type="checkbox"/>
	Dial Out Extension	204
	Dial Out ID	id204
	Audio Playbacks	12
Button 1	Button Lit	<input checked="" type="checkbox"/>
	Button Mode	Relay 1
	Pulse Duration	10 seconds
	Dial Out Extension	204
	Dial Out ID	id204
	Audio Playbacks	12
Button 2	Button Lit	<input checked="" type="checkbox"/>
	Button Mode	Relay 2
	Pulse Duration	10 seconds
	Dial Out Extension	204
	Dial Out ID	id204
	Audio Playbacks	12

- On the **Sensor** page, enter values for the parameters indicated in [Table 2-12](#).

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-12. Sensor Configuration Parameters

Web Page Item	Description
Sensor 1	
Sensor Activated Timeout ?	If sensor 1 is activated longer than the set time, a call or multicast will be made if settings are enabled. Enter a value from 1 - 60 seconds.
Sensor Type ?	Select whether sensor 1 is normally closed (NC) or normally open (NO).
Call to Extension ?	Enable the device to call an extension when "Sensor Activated Timeout" for sensor 1 has been reached.
Dial Out Extension ?	Specify the call extension. Enter up to 10 alphanumeric characters.
Dial Out ID ?	Specify the caller identification for outbound calls. Enter up to 10 alphanumeric characters.
Audio Playbacks ?	The number of times the corresponding audio message will be played during a call operation. Enter a value from 1-60.
Multicast Audio ?	Enable the device to multicast when "Sensor Activated Timeout" for sensor 1 has been reached.
Multicast Address ?	Specify the IP address for multicasting.
Multicast Port ?	Specify the port number for multicasting. Range: 0 - 65535
Multicast TTL ?	Specify the "Time to live" to limit the lifespan of multicast operation. Range: 1 - 255
Audio Playbacks ?	The number of times an audio message will be played during a multicast operation. Enter a value from 1 - 60.
Sensor 2	
Sensor Activated Timeout ?	If sensor 2 is activated longer than the set time, a call or multicast will be made if settings are enabled. Enter a value from 1 - 60 seconds.
Sensor Type ?	Select whether sensor 2 is normally closed (NC) or normally open (NO).
Call to Extension ?	Enable the device to call an extension when "Sensor Activated Timeout" for sensor 2 has been reached.
Dial Out Extension ?	Specify the call extension. Enter up to 10 alphanumeric characters.
Dial Out ID ?	Specify the caller identification for outbound calls. Enter up to 10 alphanumeric characters.
Audio Playbacks ?	The number of times the corresponding audio message will be played during a call operation. Enter a value from 1-60.
Multicast Audio ?	Enable the device to multicast when "Sensor Activated Timeout" for sensor 2 has been reached.
Multicast Address ?	Specify the IP address for multicasting.
Multicast Port ?	Specify the port number for multicasting. Range: 0 - 65535
Multicast TTL ?	Specify the "Time to live" to limit the lifespan of multicast operation. Range: 1 - 255
Audio Playbacks ?	The number of times an audio message will be played during a multicast operation. Enter a value from 1 - 60.

Table 2-12. Sensor Configuration Parameters (continued)
























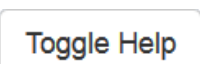
Web Page Item	Description
Button 1	
Button Lit 	When selected, the button's LED is illuminated.
Button 1 Mode 	Select the mode for button 1. When set to "Control Relay 1", the button can pulse relay 1 for the user-defined duration. When set to "SIP Call", the button can initiate a SIP call with user-defined extension.
Pulse Duration 	When "Control Relay 1" is selected, relay 1 will be pulsed for the user-defined time. Enter a value from 1-15.
Dial Out Extension 	Specify the call extension. Enter up to 10 alphanumeric characters.
Dial Out ID 	Specify the caller identification for outbound calls. Enter up to 10 alphanumeric characters.
Audio Playbacks 	The number of times the corresponding audio message will be played during a call operation. Enter a value from 1-60.
Button 2	
Button Lit 	When selected, the button's LED is illuminated.
Button 2 Mode 	Select the mode for button 2. When set to "Control Relay 2", the button can pulse relay 2 for the user-defined duration. When set to "SIP Call", the button can initiate a SIP call with user-defined extension.
Pulse Duration 	When "Control Relay 2" is selected, relay 2 will be pulsed for the user-defined time. Enter a value from 1-15.
Dial Out Extension 	Specify the call extension. Enter up to 10 alphanumeric characters.
Dial Out ID 	Specify the caller identification for outbound calls. Enter up to 10 alphanumeric characters.
Audio Playbacks 	The number of times the corresponding audio message will be played during a call operation. Enter a value from 1-60.
Intrusion Sensor	
Call to Extension 	Enable the device to call an extension when intrusion sensor has been activated.
Dial Out Extension 	Specify the call extension. Enter up to 10 alphanumeric characters.
Dial Out ID 	Specify the caller identification for outbound calls. Enter up to 10 alphanumeric characters.
Fault Message Playbacks 	The number of times an audio message will be played during a call operation. Enter a value from 1 - 60.
	Click the Test Intrusion Sensor button to test the Intrusion Sensor.
	Click the Test Sensor 1 button to test Sensor 1.

Table 2-12. Sensor Configuration Parameters (continued)

Web Page Item	Description
	Click the Test Sensor 2 button to test Sensor 2.
	Click the Test Button 1 button to test Button 1.
	Click the Test Button 2 button to test Button 2.
	Click the Save button to save your configuration settings.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

2.3.11 Configure the Audio Configuration Parameters

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.

1. Click on the **Audiofiles** menu button to open the **Audiofiles** page (Figure 2-17).

Figure 2-17. Audiofiles Configuration Page

Home Device Network SIP SSL Access Log Sensor **Audiofiles** Events Autoprov Firmware

SIP Dual Relay Controller

Available Space: 1485MB

Audio Files

Intrusion sensor triggered:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Close both doors 1 and 2, in order to run automatic mode:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Button 1 was triggered:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Button 2 was triggered:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Door 1 is already locked:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Door 1 is already unlocked:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Close door 1 in order to pulse the door:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Door 2 is already locked:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Door 2 is already unlocked:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Close door 2 in order to pulse the door:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Sensor 1 was triggered:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Sensor 2 was triggered:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>

Figure 2-18. Audiofiles Configuration Page

Disabling automatic mode for entry:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Disabling automatic mode for exit:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Enabling automatic mode for entry:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Enabling automatic mode for exit:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Menu Audio Files					
Enter the security code:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Invalid code:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Press 0 to announce the status of each door:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Press 1 to unlock door 1:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Press 2 to lock door 1:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Press 3 to pulse door 1:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Press 4 to unlock door 2:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Press 5 to lock door 2:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Press 6 to pulse door 2:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Press 7 to unlock both doors 1 and 2:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Press 8 to lock both doors 1 and 2:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Press 9 to enable automatic mode for entry:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>

Figure 2-19. Audiofiles Page

Enter the security code:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Invalid code:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Press 0 to announce the status of each door:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Press 1 to unlock door 1:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Press 2 to lock door 1:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Press 3 to pulse door 1:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Press 4 to unlock door 2:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Press 5 to lock door 2:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Press 6 to pulse door 2:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Press 7 to unlock both doors 1 and 2:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Press 8 to lock both doors 1 and 2:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Press 9 to enable automatic mode for entry:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Press # to enable automatic mode for exit:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Press star to repeat main menu:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>
Press star to play main menu:	Currently set to: default	<input type="button" value="Browse..."/>	No file chosen	<input type="button" value="Delete"/>	<input type="button" value="Save"/>


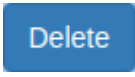

2. On the **Audiofiles** page, enter values for the parameters indicated in [Table 2-13](#).

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-13. Audiofiles Configuration Parameters

Web Page Item	Description
Available Space	Shows the space available for the user to save custom audio files if they want to change the message when the door or sensor is triggered.
Audio Files	
Intrusion sensor triggered	Corresponds to the message "Intrusion sensor triggered."
Close both doors 1 and 2, in order to run automatic mode	Corresponds to the message "Intrusion sensor triggered."
Button 1 was triggered	Corresponds to the message "Button 1 was triggered."
Button 2 was triggered	Corresponds to the message "Button 2 was triggered."
Door 1 is already locked	Corresponds to the message "Door 1 is already locked."
Door 1 is already unlocked	Corresponds to the message "Door 1 is already unlocked."
Close door 1 in order to pulse the door	Corresponds to the message "Close door 1 in order to pulse the door."
Door 2 is already locked	Corresponds to the message "Door 2 is already locked."
Door 2 is already unlocked	Corresponds to the message "Door 2 is already unlocked."
Close door 2 in order to pulse the door	Corresponds to the message "Close door 2 in order to pulse the door."
Sensor 1 was triggered	Corresponds to the message "Intrusion sensor 1 was triggered."
Sensor 2 was triggered	Corresponds to the message "Intrusion sensor 2 was triggered."
Disabling automatic mode for entry	Corresponds to the message "Disabling automatic mode for entry."
Disabling automatic mode for exit	Corresponds to the message "Disabling automatic mode for exit."
Enabling automatic mode for entry	Corresponds to the message "Enabling automatic mode for entry."
Enabling automatic mode for exit	Corresponds to the message "Enabling automatic mode for exit."
Menu Audio Files	
Enter the security code	Corresponds to the message "Enter the security code."
Invalid code	Corresponds to the message "Invalid code."
Press 0 to announce the status of each door	Corresponds to the message "Press 0 to announce the status of each door."
Press 1 to unlock door 1	Corresponds to the message "Press 1 to unlock door 1."
Press 2 to lock door 1	Corresponds to the message "Press 2 to lock door 1."
Press 3 to pulse door 1	Corresponds to the message "Press 3 to pulse door 1."
Press 4 to unlock door 2	Corresponds to the message "Press 4 to unlock door 2."
Press 5 to lock door 2	Corresponds to the message "Press 2 to lock door 2."
Press 6 to pulse door 2	Corresponds to the message "Press 3 to pulse door 2."

Table 2-13. Audiofiles Configuration Parameters (continued)

Web Page Item	Description
Press 7 to unlock both doors 1 and 2	Corresponds to the message “Press 7 to unlock both doors 1 and 2.”
Press 8 to lock both doors 1 and 2	Corresponds to the message “Press 8 to lock both doors 1 and 2.”
Press 9 to enable automatic mode for entry	Corresponds to the message “Press 9 to enable automatic mode for entry.”
Press # to enable automatic mode for exit	Corresponds to the message “Press # to enable automatic mode for exit.”
Press star to repeat main menu	Corresponds to the message “Press star to repeat main menu.”
Press start to play main menu	Corresponds to the message “Press start to play main menu.”
	Click on the Browse button to navigate to and select an audio file.
	The Delete button will delete any user uploaded audio and restore the stock audio file.
	The Save button will download a new user audio file to the board once you've selected the file by using the Browse button. The Save button will delete any pre-existing user-uploaded audio files.

2.3.11.1 User-created Audio Files

User created audio files should be saved in the following format:

RIFF (little-endian) data, WAVE audio, Microsoft PCM, 16 bit, mono 8000 Hz

You can use the free utility *Audacity* to convert audio files into this format. See [Figure 2-20](#) through [Figure 2-22](#).

Figure 2-20. Audacity 1

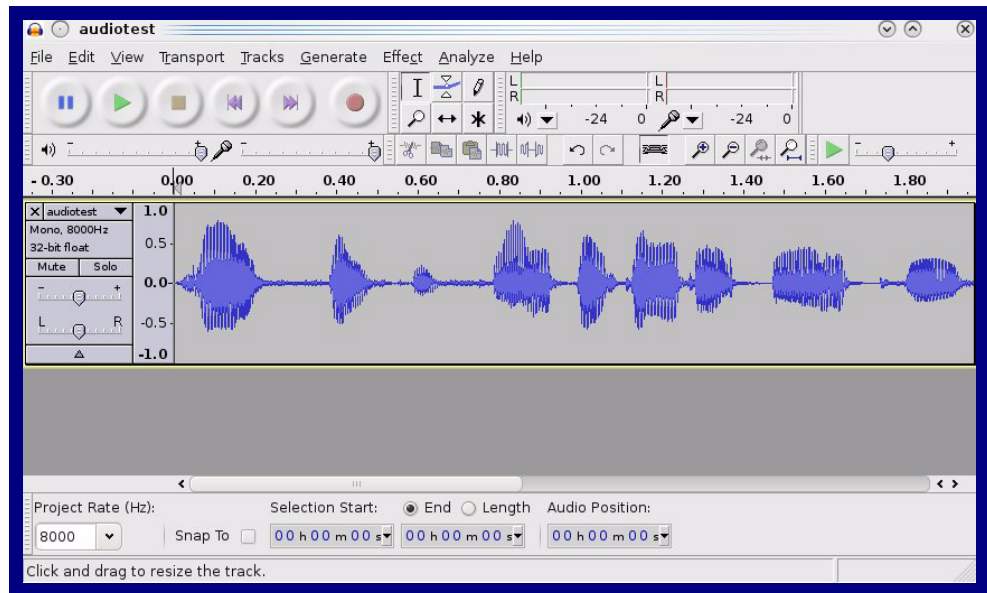
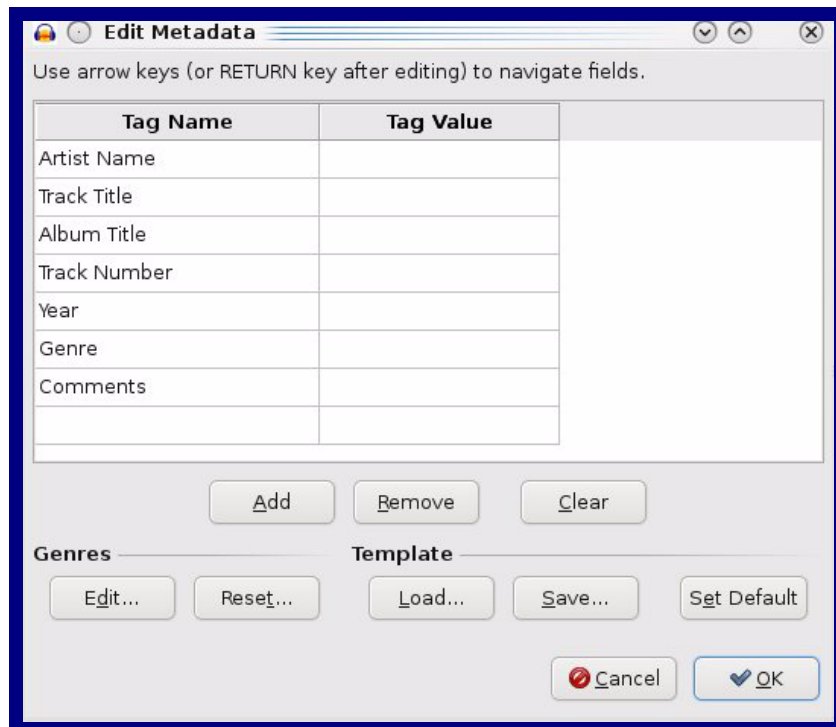


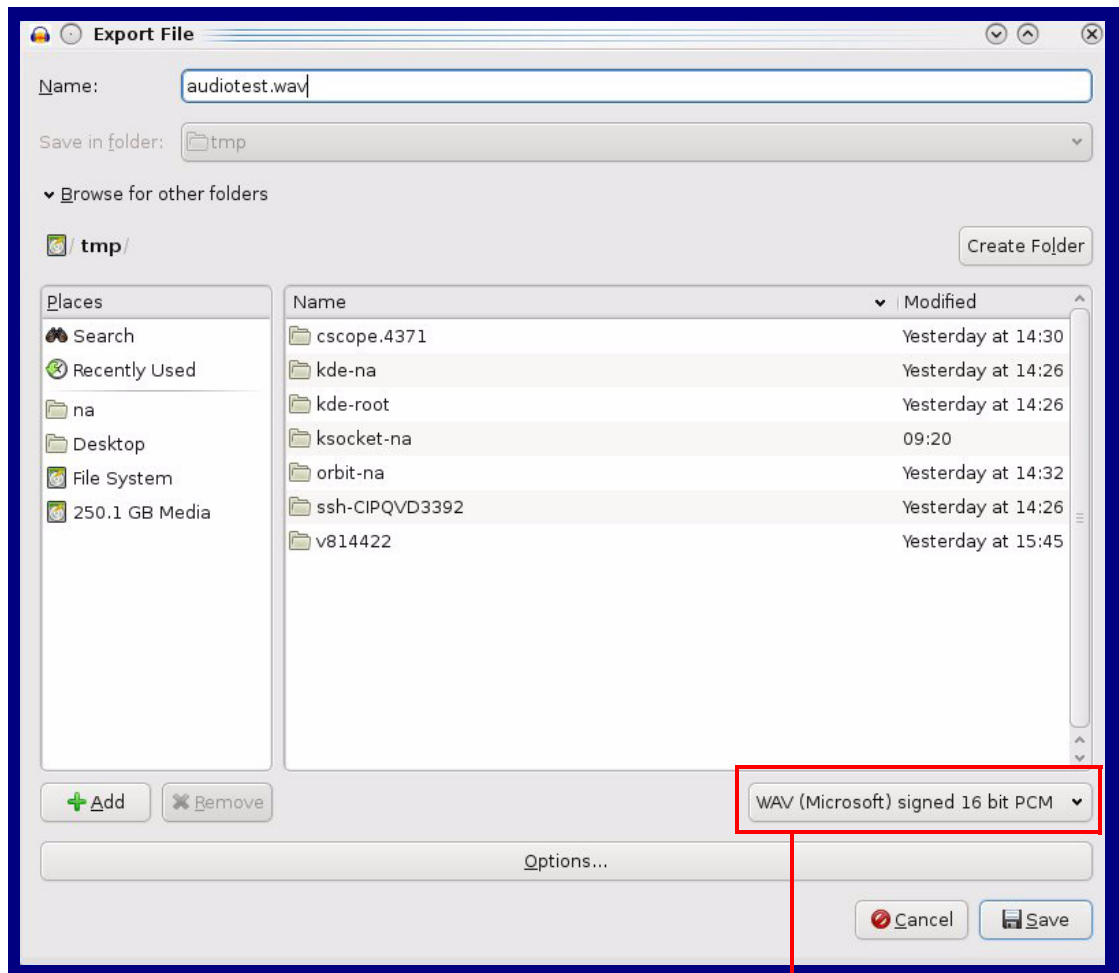
Figure 2-21. Audacity 2



When you export an audio file with Audacity, save the output as:

- **WAV (Microsoft) signed 16 bit PCM.**

Figure 2-22. WAV (Microsoft) signed 16 bit PCM



WAV (Microsoft) signed 16 bit PCM

2.3.12 Configure the Events Parameters

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

1. Click on the **Events** menu button to open the **Events** page (Figure 2-23).

Figure 2-23. Event Configuration Page

Home Device Network SIP SSL Access Log Sensor Audiofiles **Events** Autopro Firmware

SIP Dual Relay Controller

Enable Event Generation:

Events

Enable Relay 1 Activated Events:
Enable Relay 1 Deactivated Events:
Enable Relay 2 Activated Events:
Enable Relay 2 Deactivated Events:
Enable Sensor 1 Opened Events:
Enable Sensor 1 Closed Events:
Enable Sensor 2 Opened Events:
Enable Sensor 2 Closed Events:
Enable Button 1 Pressed Events:
Enable Button 2 Pressed Events:
Enable Call Start Events:
Enable Call Terminated Events:
Enable Power On Events:
Enable Security Events:
Enable 60 Second Heartbeat:

Event Server

Server IP Address:
Server Port:
Server URL:

2. On the **Events** page, enter values for the parameters indicated in [Table 2-14](#).

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-14. Events Configuration Parameters



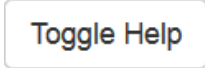
Web Page Item	Description
Enable Event Generation ?	The device will send HTTP POST events to the specified remote server and port number whenever a certain action takes place. Select an event type below to generate an HTTP POST event.
Events	
Enable Relay 1 Activated Events ?	When selected, the device will report relay 1 activation.
Enable Relay 1 Deactivated Events ?	When selected, the device will report relay 1 deactivation.
Enable Relay 2 Activated Events ?	When selected, the device will report relay 2 activation.
Enable Relay 2 Deactivated Events ?	When selected, the device will report relay 2 deactivation.
Enable Sensor 1 Opened Events ?	When selected, the device will report when sensor 1 opens.
Enable Sensor 1 Closed Events ?	When selected, the device will report when sensor 1 closes.
Enable Sensor 2 Opened Events ?	When selected, the device will report when sensor 2 opens.
Enable Sensor 2 Closed Events ?	When selected, the device will report when sensor 2 closes.
Enable Button 1 Pressed Events ?	When selected, the device will report when button 1 presses.
Enable Button 2 Pressed Events ?	When selected, the device will report when button 2 presses.
Enable Call Start Events ?	When selected, the device will report the start of a SIP call.
Enable Call Terminated Events ?	When selected, the device will report the end of a SIP call.
Enable Power On Events ?	When selected, the device will report when it boots.
Enable Security Events ?	When enabled, the device will report when the intrusion sensor is activated.
Enable 60 Second Heartbeat Events ?	When enabled, the device will report a Heartbeat event every 60 seconds. SIP registration is not required to generate Heartbeat events.
Check All	Click on Check All to select all of the events on the page.
Uncheck All	Click on Uncheck All to de-select all of the events on the page.
Event Server	
Server IP Address ?	The IPv4 address of the event server in dotted decimal notation.
Server Port ?	Specify the event server port number. The supported range is 0-65536. Enter up to 5 digits.
Server URL ?	Generally, the destination URL is the name of the application that receives the events and the string in the HTTP POST command. It can be a script used to parse and process the HTTP POST events. Enter up to 127 characters.
	Click the Save button to save your configuration settings.

Table 2-14. Events Configuration Parameters(continued)

Web Page Item	Description
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

2.3.12.1 Example Packets for Events

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

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

Here are example packets for every event:

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

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

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

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

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

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

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

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>CALL_ACTIVE</event>
</cyberdata>
POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
```

```
User-Agent: CyberData/1.0.0
Content-Length: 205
Content-Type: application/x-www-form-urlencoded

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

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

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

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

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

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

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

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

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

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

2.3.13 Configure the Autoprovisioning Parameters

Autoprovisioning can be used to automatically configure your device. The autoprovisioning file is an xml file with the device configuration. Values found in this file will override values stored in on-board memory.

Note By default, the device will try to set up its configuration with autoprovisioning.

1. Click the **Autoprov** menu button to open the **Autoprovisioning** page. See [Figure 2-24](#).

Figure 2-24. Autoprovisioning Page





The screenshot shows the 'Autoprov' configuration page for the SIP Dual Relay Controller. At the top, there is a navigation menu with buttons for Home, Device, Network, SIP, SSL, Access Log, Sensor, Audiofiles, Events, Autoprov (selected), and Firmware. The main heading is 'SIP Dual Relay Controller'. Below this, there are several configuration fields: 'Enable Autoprovisioning' (checked), 'Autoprovisioning Server' (text input), 'Autoprovisioning Filename' (text input), 'Use tftp' (unchecked), 'Verify Server Certificate' (unchecked), 'Username' (text input), 'Password' (text input), 'Autoprovisioning autoupdate (in minutes):' (input with '0'), 'Autoprovision at time (HHMM):' (input), and 'Autoprovision when idle (in minutes > 10):' (input with '0'). Below the fields, there are three buttons: 'Save', 'Reboot', and 'Toggle Help'. A 'Download Template' button is also present. At the bottom, there is an 'Autoprovisioning log' section with a scrollable text area containing the following log entries:

```
2022-04-07 14:21:50 Autoprovd: no autoprov triggers. Exiting...
2022-04-07 14:21:53 Autoprovisioning on boot
2022-04-07 14:21:53 Autoprov found server='http://10.0.0.242' in dhcp option 43
2022-04-07 14:21:53 Autoprov looking for 0020f704de7e.xml at http://10.0.0.242
2022-04-07 14:21:53 Autoprov downloading http://10.0.0.242/0020f704de7e.xml
2022-04-07 14:21:53 Autoprov: download failed
2022-04-07 14:21:53 Autoprov looking for 000000cd.xml at http://10.0.0.242
2022-04-07 14:21:53 Autoprov downloading http://10.0.0.242/000000cd.xml
2022-04-07 14:21:53 Autoprov: download failed
2022-04-07 14:21:53 Autoprov: Failed to fetch autoprov file
```


- On the **Autoprovisioning** page, you may enter values for the parameters indicated in [Table 2-15](#).

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed..

Table 2-15. Autoprovisioning Page Parameters

Web Page Item	Description
Enable Autoprovisioning ?	The device will automatically fetch a configuration file, also known as the 'autoprovisioning file', based on the configured settings below.
Autoprovisioning Server ?	Enter the IPv4 address of the provisioning server in dotted decimal notation.
Autoprovisioning Filename ?	The autoprovisioning filename is the configuration filename. The default autoprovisioning filename is in the format of <mac address>.xml. Supported filename extensions are .txt, and .xml. The current filename is denoted by an asterisk at the bottom of the Autoprovisioning Page . Enter up to 256 characters. A file may have any name with an xml extension. If a file name is entered, the device will look for the specified file name, and only that file.
Use tftp ?	The device will use TFTP (instead of http) to download autoprovisioning files.
Verify Server Certificate ?	When using ssl to download autoprovisioning files, reject connections where the server address doesn't match the server certificate's common name.
Username ?	The username used to authenticate with an autoprovisioning server. Leave this field blank to disable authentication.
Password ?	The password used to authenticate with an autoprovisioning server. Leave this field blank to disable authentication.
Autoprovisioning Autoupdate (in minutes) ?	The reoccurring time (in minutes) the device will wait before checking for new autoprovisioning files. Enter up to 6 digits. A value of 0 will disable this option.
Autoprovision at time (HHMMSS) ?	The time of day the device will check for a new autoprovisioning file. The time must be 6 characters in length and in HHMMSS format. An empty value will disable this option.
Autoprovision when idle (in minutes > 10) ?	The idle time (in minutes greater than 10) after which the device will check for a new autoprovisioning file. Enter up to 6 digits. A value of 0 will disable this option.
	Click the Save button to save your configuration settings.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.
	Press the Download Template button to create an autoprovisioning file for the device. See Section 2.3.13.3, "Download Template Button"
Autoprovisioning log	The autoprovisioning log provides information about the latest autoprovisioning attempt (i.e. dhcp options and server accessed and files parsed or not found).

Note You must click on the **Save** button for the changes to take effect.

2.3.13.1 Autoprovisioning

On boot, the device will look for an autoprovisioning server configured on the [Autoprovisioning Page](#) or specified as a DHCP option. When it finds a server, it will try to download the following (in order of preference):

1. The file configured on the autoprovisioning page.
2. A file named according to it's mac address (for example: 0020f7350058.xml).
3. The file 000000cd.xml

The file can be hosted using a standard web server (like apache, IIS, or nginx), and the device can download over SSL. The file server can be an ipv4 address in dotted decimal notation or a fully qualified domain name.

By default, the device will get its autoprovisioning server from the DHCP options. See [Section 2.3.13.2, "Sample dhcpd.conf"](#) for an example of how to configure dhcpd to offer autoprovisioning server addresses. If multiple options are set, the device will attempt to download autoprovisioning files from every server.

The DHCP option determines the protocol used to download the autoprovisioning file. The device looks for DHCP options in the following order:

1. Option 43 - a FQDN or an IP address to an http server
2. Option 72 - an IP address to an http server
3. Option 150 - an IP address to a tftp server
4. Option 66 - an IP address to a tftp server or if the entry starts with 'http', a FQDN to a http server.

You can download an autoprovisioning template file from the [Autoprovisioning Page](#) using the **Download Template** button (see [Table 2-15](#)). This file contains every configuration option that can be set on the board.

Autoprovisioning files can contain the whole configuration or a subset of this file. The first autoprovisioning file can also contain links to other autoprovisioning files.

The `<MiscSettings>` section contains some examples of additional autoprovisioning files:

```
<MiscSettings>
    <DeviceName>CyberData VoIP Device</DeviceName>
<!-- <AutoprovFile>common.xml</AutoprovFile>-->
<!-- <AutoprovFile>sip_reg[macaddress].xml</AutoprovFile>-->
<!-- <AutoprovFile>audio[macaddress]</AutoprovFile>-->
<!-- <AutoprovFile>device[macaddress].xml</AutoprovFile>-->
</MiscSettings>
```

After downloading the first autoprovisioning file, the device will step through up to twenty additional `<AutoprovFile>` entries and try to download these files from the same server.

When the device finds a filename with the string `[macaddress]`, it will replace this string with the mac address.

As an example, the user has configured option 43 on their DHCP server to “http://example.com,” and on their server, they have a file named **0020f7123456.xml** (the same as the mac address of the device).

The file 0020f7123456.xml contains:

```
<?xml version="1.0" encoding="utf-8" ?>
<specific>
<MiscSettings>
<DeviceName>Newname</DeviceName>
<AutoprovFile>common.xml</AutoprovFile>
<AutoprovFile>sip_reg[macaddress].xml</AutoprovFile>
<AutoprovFile>audio[macaddress]</AutoprovFile>
<AutoprovFile>device.xml</AutoprovFile>
</MiscSettings>
</specific>
```

1. The device will first set it's name to 'Newname'.
2. It will try to download http://example.com/common.xml.
3. It will try to download http://example.com/sip_reg0020f7123456.xml.
4. It will try to download http://example.com/audio0020f7123456.
5. It will try to download http://example.com/device.xml.

The device is reconfigured every time it downloads a new file so if two files configure the same option the last one will be the one that is saved.

It is possible to autoprovision autoprovisioning values (for example, to disable autoprovisioning or to configure a time to check for new files).

Checking for New Autoprovisioning Files after Boot

The device will always check for an autoprovisioning files on boot but it can be configured to also check after a periodic delay, when idle, or at a specified time. When one of these options is set, the device will download its autoprovisioning files again, and if it finds any differences from the files it downloaded on boot, it will force a reboot and reconfigure.

The
 Autoprovisioning
 Filename

The autoprovisioning filename can contain a file, a file path, or a directory.

Table 2-16. Autoprovisioning File Name

Autoprovisioning Filename	Autoprovisioning Server	File Downloaded
config.xml	10.0.1.3	10.0.1.3/config.xml
/path/to/config.xml	10.0.1.3	10.0.1.3/path/to/config.xml
subdirectory/path/	10.0.1.3	10.0.1.3/subdirectory/path/0020f7020002.xml

TFTP options may not support subdirectories. If a directory is set in the filename field, firmware and audio files will also be downloaded from this subdirectory.

If the filename ends with a forward slash “/,” the device will treat it as a subdirectory.

For example:

The autoprovisioning server is set to “https://www.example.com”

The autoprovisioning filename is set to “cyberdata/”

On boot, the device will try to download:

https://www.example.com/cyberdata/0020f7123456.xml

...and if this fails:

https://www.example.com/cyberdata/000000cd.xml

Audio files and firmware files will also add “cyberdata” to the URL before downloading.

```

Autoprovisioning <FirmwareSettings>
Firmware Updates <FirmwareFile>505-uImage-ceilingsspeaker</FirmwareFile>
                  <FirmwareServer>10.0.1.3</FirmwareServer>
                  <DeviceName30>firmware_file_v9.3.0</DeviceName30>
                  <DeviceName31>firmware_file_v10.3.0</DeviceName31>
                  <DeviceName31>firmware_file_v10.3.0</DeviceName31>
                  </FirmwareSettings>
  
```

In the <FirmwareSettings> section, the <FirmwareServer> element can be used to specify a different server for hosting firmware files. When this element is not available, the device will try to download the file from the autoprovisioning server.

The device will use the filename to determine when to autoprovision firmware updates. The default configuration is blank, so the first time you set a value in your autoprovisioning file, it may force a firmware update even if the firmware version has not changed.

The <FirmwareFile> name can contain path elements (i.e. /path/to/firmware/10.3.0-ulmage-[device_file_name]).

The device also supports product strings for downloading firmware. If the <FirmwareFile> option is not set, the device will look for its particular product string for a firmware filename. In this way, a generic autoprovisioning file can specify unique firmware for a range of products.

The list of valid product strings:

```

<ProductString>CallButton31</ProductString>
<ProductString>EmergencyIntercom31</ProductString>
<ProductString>EmergencyIntercom31SW</ProductString>
<ProductString>IndoorIntercom31</ProductString>
<ProductString>IndoorIntercom31SW</ProductString>
<ProductString>IndoorKeypad31</ProductString>
<ProductString>IndoorKeypad31SW</ProductString>
<ProductString>OfficeRinger31</ProductString>
<ProductString>OfficeRinger31SW</ProductString>
<ProductString>OutdoorIntercom31</ProductString>
<ProductString>OutdoorIntercom31SW</ProductString>
<ProductString>OutdoorKeypad31</ProductString>
<ProductString>OutdoorKeypad31SW</ProductString>
<ProductString>Strobe31</ProductString>
<ProductString>Strobe31SW</ProductString>
  
```

Autoprovisioning
 Example 1

Here's a simple example using four autoprovisioning files to configure two devices:

We boot up two devices with mac addresses **00:20:f7:02:00:01** and **00:20:f7:02:00:02** (Device1 and Device2).

The devices are set to use DHCP and that server provides an autoprovisioning server address with option 43. The address is "https://autoprovtest.server.net." The files on this server are as follows:

000000cd.xml

```
<MiscSettings>
<DeviceName>CyberData Autoprovisioned</DeviceName>
<AutoprovFile>sip_common.xml</AutoprovFile>
<AutoprovFile>sip_[macaddress].xml</AutoprovFile>
</MiscSettings>
```

sip_common.xml

```
<SIPSettings>
<SIPServer>10.0.0.253</SIPServer>
<RemoteSIPPort>5060</RemoteSIPPort>
</SIPSettings>
```

sip_0020f7020001.xml

```
<SIPSettings>
<SIPUserID>198</SIPUserID>
<SIPAuthPassword>ext198</SIPAuthPassword>
<DialoutExtension0>204</DialoutExtension0>
</SIPSettings>
```

sip_0020f7020002.xml

```
<SIPSettings>
<SIPUserID>500</SIPUserID>
<SIPAuthPassword>ext500</SIPAuthPassword>
<DialoutExtension0>555</DialoutExtension0>
</SIPSettings>
```

On boot, Device1 tries to fetch the file **0020f7023614.xml** from "https://autoprovtest.server.net". This file is not available, so device1 then tries to fetch the file **000000cd.xml**. This file exists, and Device1 parses the three elements.

1. Device1 changes its device name to **CyberData Autoprovisioned**.
2. Device1 finds an AutoprovFile element containing the filename **sip_common.xml**. The device downloads **sip_common.xml** from "https://autoprovtest.server.net," and imports this configuration, setting the sip server to **10.0.0.253** and the remote port to **5060.3**.
3. Device1 finds another AutoprovFile element containing the filename **sip_[macaddress].xml**. The device replaces the **[macaddress]** with its own mac address value creating **sip_0020f7020001.xml**, downloads this file from "https://autoprovtest.server.net," and imports this configuration. This sets the user ID to **198**, the password to **ext198**, and the dialout extension to **204**. Device1 is now finished with autoprovisioning.

Device2 goes through the same steps by setting its device name to **CyberData Autoprovisioned**, its SIP server to **10.0.0.253**, and its port to **5060**. When Device2 “sees” **sip_[macaddress].xml**, Device2 replaces it with its own mac address and downloads **sip_0020f7020002.xml** from “https://autoprovttest.server.net.” Device2 sets the SIP User ID to **500**, the password to **ext500**, and the dialout extension to **555**.

Autoprovisioning
 Example 2

Here is another example of setting up your autoprovisioning files:

We boot up two devices with mac addresses **00:20:f7:02:00:01** and **00:20:f7:02:00:02** (Device1 and Device2) and boot them on a network with a DHCP server configured with an autoprovisioning server at **10.0.1.3** on option **150**. Our TFTP server has three files:

0020f7020001.xml

```
<MiscSettings>
<AutoprovFile>common_settings.xml</AutoprovFile>
</MiscSettings>
<SIPSettings>
<SIPUserID>198</SIPUserID>
<SIPAuthPassword>ext198</SIPAuthPassword>
<DialoutExtension0>204</DialoutExtension0>
</SIPSettings>
```

0020f7020002.xml

```
<MiscSettings>
<AutoprovFile>common_settings.xml</AutoprovFile>
</MiscSettings>
<SIPSettings>
<SIPUserID>500</SIPUserID>
<SIPAuthPassword>ext500</SIPAuthPassword>
<DialoutExtension0>555</DialoutExtension0>
</SIPSettings>
```

common_settings.xml

```
<MiscSettings>
<DeviceName>CyberData Autoprovisioned</DeviceName>
</MiscSettings>
<SIPSettings> <SIPServer>10.0.0.253</SIPServer>
<RemoteSIPPort>5060</RemoteSIPPort>
</SIPSettings>
```

1. On boot, Device1 downloads **0020f7020001.xml** from **10.0.1.3** and imports these values. The SIP User ID is **198**, the password is **ext198**, and the dialout extension is **204**.

2. Device1 then gets the filename **common_settings.xml** from the AutoprovFile element and downloads this file from the TFTP server at **10.0.1.3**. and imports these settings. The device name is set to **CyberData Autoprovisioned**, the SIP server is set to **10.0.0.253**, and the port is set to **5060**.

Device2 does the same except it downloads **0020f7020002.xml** on boot and imports these values instead. The Sip User ID is **500**, password is **ext500**, and dialout extension is **555**. Device2 then downloads the **common_settings.xml** file and imports those values. The device name is set to **CyberData Autoprovisioned**, the SIP server is set to **10.0.0.253**, and the port is set to **5060**.

XML Files

XML files can contain <AutoprovFile> elements. If multiple DHCP options are specified, the device will try to download auto provisioning files from each in turn. The device will only look for <AutoprovFile> elements in the first file downloaded from each server. You can specify up to 20 <AutoprovFile> elements in the first auto provisioning file.

There are numerous ways to change an element of the **configuration(xml)** file. Using **sip ext** as an example, the extension can be changed:

Within the device-specific xml, i.e. **[macaddress].xml**, via the AutoprovFile element:<SIPSettings>/<SIPExt>

From the device specific xml, a pointer to a sip_common file

From the device specific xml, a pointer to the device specific sip_[macaddress].xml

From the common file, a pointer to sip_common.xml

From the common file, a pointer to the device specific (sip_[macaddress].xml)

Autoprovisioned Audio Files

Audio files are stored in non-volatile memory and an auto provisioned audio file will only have to be downloaded once for each device. Loading many audio files to the device from the web page could cause it to appear unresponsive. If this happens, wait until the transfer is complete and then refresh the page.

The device uses the file name to determine when to download a new audio file. This means that if you used auto provisioning to upload a file and then changed the contents of this file at the TFTP server, the device will not recognize that the file has changed (because the file name is the same).

Since audio files are stored in non-volatile memory, if auto provisioning is disabled after they have been loaded to the board, the audio file settings will not change. You can force a change to the audio files on the board by clicking **Restore Default** on the **Audio** page or by changing the auto provisioning file with “**default**” set as the file name.

2.3.13.2 Sample dhcpd.conf

```
#
# Sample configuration file for ISC dhcpd for Debian
#

ddns-update-style none;

option domain-name "voiplab";
option domain-name-servers 10.0.0.252;
option option-150 code 150 = ip-address;
option ntp-servers north-america.pool.ntp.org;
option space VendorInfo;
option VendorInfo.text code 10 = { text };
authoritative;
log-facility local7;

subnet 10.0.0.0 netmask 255.0.0.0 {
    max-lease-time 3600;
    default-lease-time 3600;

    option routers                10.0.0.1;
    option subnet-mask            255.0.0.0;

    option domain-name            "voiplab";
    option domain-name-servers    10.0.0.252;

    option time-offset            -8;          # Pacific Standard Time

#   option www-server             99.99.99.99;      # OPTION 72

#   option tftp-server-name       "10.0.1.52";     # OPTION 66
#   option tftp-server-name       "http://test.cyberdata.net"; # OPTION 66

#   option option-150             10.0.0.252;      # OPTION 150

# These two lines are needed for option 43
#   vendor-option-space VendorInfo;                # OPTION 43
#   option VendorInfo.text "http://test.cyberdata.net"; # OPTION 43

    range 10.10.0.1 10.10.2.1; }

```

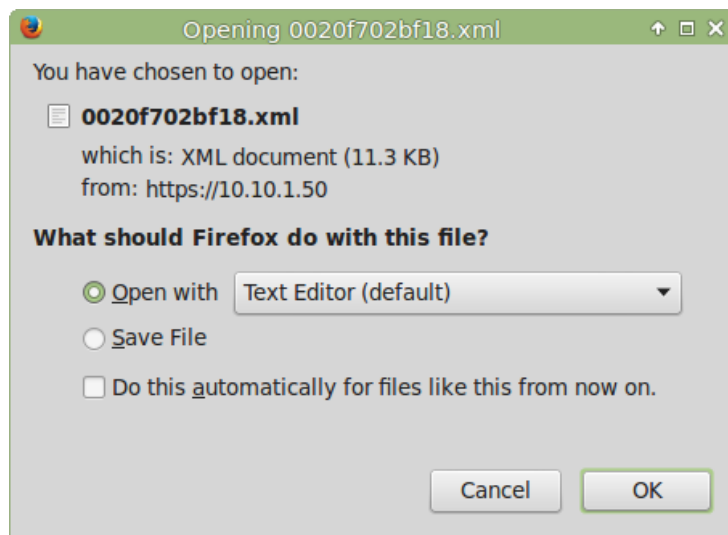
2.3.13.3 Download Template Button

The **Download Template** button allows the user to generate, download, edit, and then store an auto provisioning template on the server that serves the auto provisioning files for devices.

To generate an auto provisioning template directly from the device, complete the following steps:

1. On the **Auto provisioning** page, click on the **Download Template** button.
2. You will see a window prompting you to save a configuration file (**.xml**) to a location on your computer (Figure 2-25). The configuration file is the basis for the default configuration settings for your unit).
3. Choose a location to save the configuration file and click on **OK**. See Figure 2-25.

Figure 2-25. Configuration File



4. At this point, you can open and edit the auto provisioning template to change the configuration settings in the template for the unit.
5. You can then upload the auto provisioning file to a TFTP or HTTP server where the file can be loaded onto other devices.

2.4 Upgrade the 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 file from the **Downloads** tab at the following webpage:
<https://www.cyberdata.net/products/011186>
2. Unzip the firmware version file. This file may contain the following:
 - Firmware file
 - Release notes
 - Autoprovisioning template
3. Log in to the **Home** page as instructed in [Section 2.3.4, "Log in to the Configuration Home Page"](#).
4. Click on the **Firmware** menu button to open the **Firmware** page ([Figure 2-26](#)).


	<p>Caution <i>Equipment Hazard:</i> CyberData strongly recommends that you first reboot the device before attempting to upgrade the firmware of the device. See Section 2.4, "Upgrade the Firmware".</p>
--	---

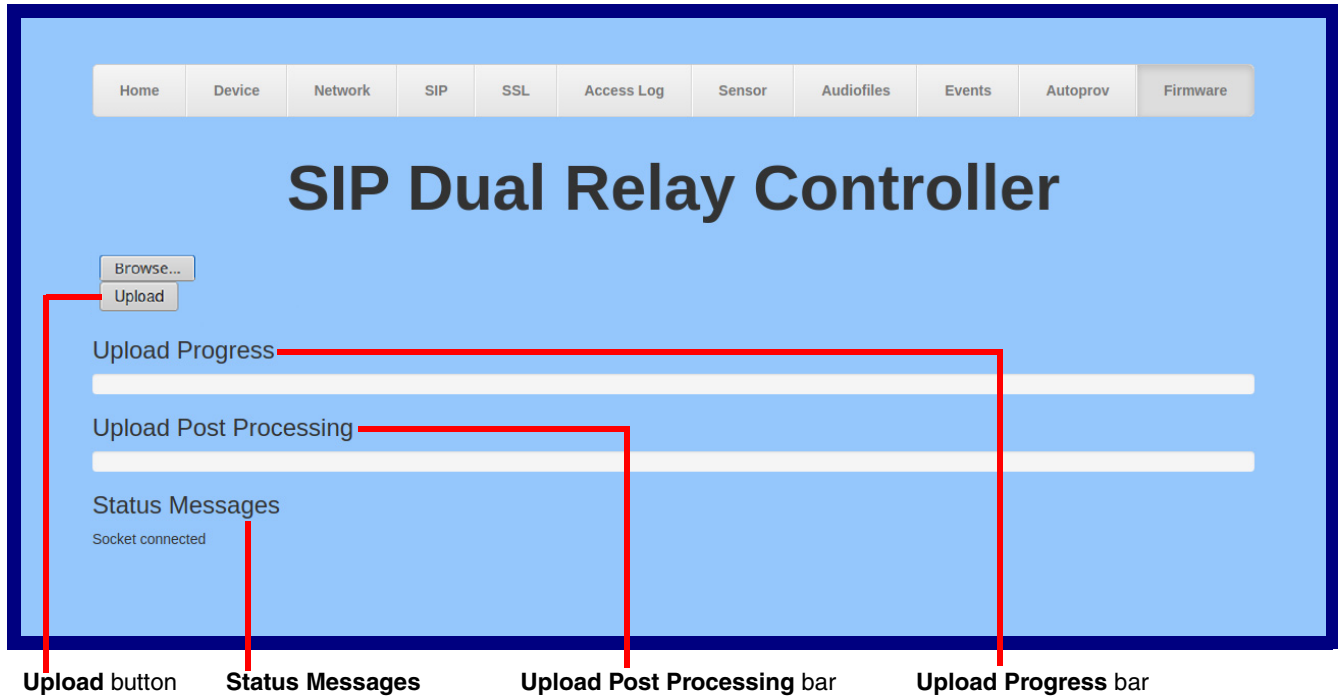
Figure 2-26. Firmware Page



5. Click on the **Browse** button, and then navigate to the location of the firmware file.

6. Select the firmware file. This reveals the **Upload** button (Figure 2-27).

Figure 2-27. Upload Button



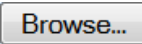
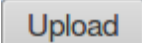
7. Click on the **Upload** button. After selecting the **Upload** button, you will see the progress of the upload in the **Upload Progress** bar.
8. When the upload is complete, you will see the words **Upload finished** under **Status Messages**.
9. At this point, you will see the progress of the upload's post processing in the **Upload Post Processing** bar.

Note Do not reboot the device before the upgrading process is complete.

10. When the process is complete, you will see the words **SWUPDATE Successful** under **Status Messages**.
11. The device will reboot automatically.
12. The **Home** page will display the version number of the firmware and indicate which boot partition is active.

Table 2-17 shows the web page items on the **Firmware** page.

Table 2-17. Firmware Page Parameters

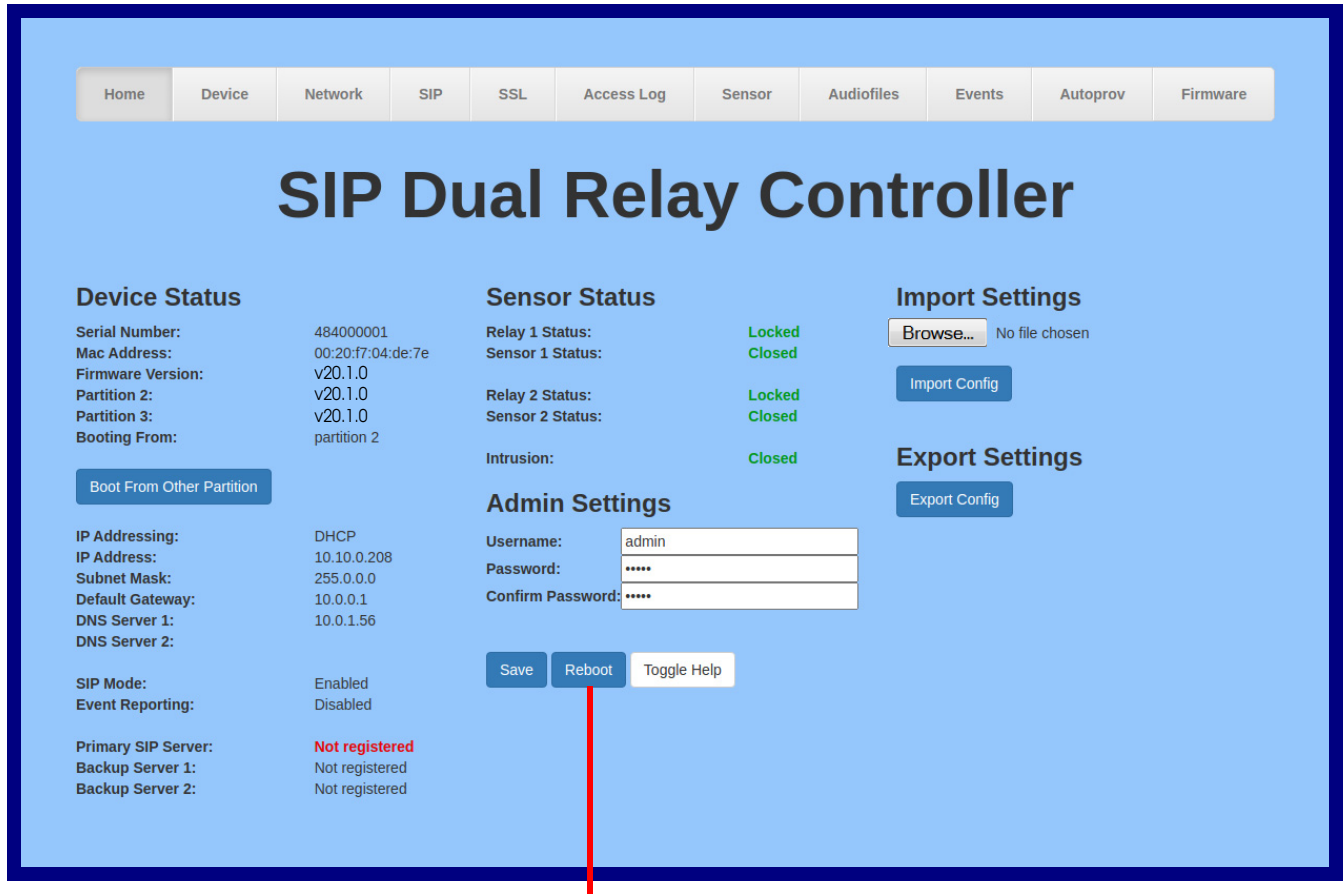
Web Page Item	Description
	Use the Browse button to navigate to the location of the firmware file that you want to upload.
	Click on the Upload button to automatically upload the selected firmware and reboot the system. Note: This button only appears after the user has selected a firmware file.
Upload progress	Status bar indicates the progress in uploading the file.
Upload Post Processing	Status bar indicates the progress of the software installation.
Status Messages	Messages relevant to the firmware update process appear here.

2.5 Reboot the Device

To reboot the device, complete the following steps:

1. Log in to the **Home** page as instructed in [Section 2.3.4, "Log in to the Configuration Home Page"](#).
2. Click on the **Reboot** button on the **Home** page ([Figure 2-28](#)). A normal restart will occur.

Figure 2-28. Home Page



Reboot

2.6 Command Interface

Some functions on the device can be activated using simple POST commands to the web interface. The examples in [Table 2-18](#) use the free unix utility, **wget** commands. However, any program that can send HTTP POST commands to the device should work.

2.6.1 Command Interface Post Commands

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

Table 2-18. 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: Setting up a TFTP Server

A.1 Set up a TFTP Server

Autoprovisioning requires a TFTP server for hosting the configuration file.

A.1.1 In a LINUX Environment

To set up a TFTP server on LINUX:

1. Create a directory dedicated to the TFTP server, and move the files to be uploaded to that directory.
2. Run the following command where `/tftpboot/` is the path to the directory you created in [Step 1](#): the directory that contains the files to be uploaded. For example:

```
in.tftpd -l -s /tftpboot/your_directory_name
```

A.1.2 In a Windows Environment

You can find several options online for setting up a Windows TFTP server. This example explains how to use the Solarwinds freeware TFTP server, which you can download from the following website address:

<https://www.cyberdata.net/pages/solarwinds>

To set up a TFTP server on Windows:

1. Install and start the software.
2. Select **File/Configure/Security** tab/**Transmit Only**.
3. Make a note of the default directory name, and then move the firmware files to be uploaded to that directory.

Appendix B: Troubleshooting/Technical Support

B.1 Frequently Asked Questions (FAQ)

To see a list of frequently asked questions for your product, do one of the following:

1. Go to the following URL:

<https://www.cyberdata.net/products/011484/>

2. Click on the **FAQs** tab.

B.2 Documentation

The documentation for this product is released in an English language version only. You can download PDF copies of CyberData product documentation by doing one of the following:

1. Go to the following URL:

<https://www.cyberdata.net/products/011484/>

2. Click on the **Downloads** tab.

B.3 Contact Information

Contact CyberData Corporation
 3 Justin Court
 Monterey, CA 93940 USA
 www.CyberData.net
 Phone: 800-CYBERDATA (800-292-3732)
 Fax: 831-373-4193

Sales Sales 831-373-2601, Extension 334

Technical The fastest way to get technical support for your VoIP product is to submit a VoIP Technical
Support 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

B.4 Warranty and RMA Information

The most recent warranty and RMA information is available at the following website address:

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

Index

A

- address, configuration login 22
- audio configuration 48
- audio configuration page 48
- audio files, user-created 53
- autoprovision at time (HHMMSS) 62
- autoprovision when idle (in minutes > 10) 62
- autoprovisioning 62, 63
 - download template button 62
 - setting up a TFTP server 77
- autoprovisioning autoupdate (in minutes) 62
- autoprovisioning configuration 61, 62
- autoprovisioning filename 62
- autoprovisioning server (IP Address) 62

B

- backup SIP server 1 32
- backup SIP server 2 32
- backup SIP servers, SIP server
 - backups 32

C

- changing
 - the web access password 26
- Cisco SRST 33
- configurable parameters 27, 30, 32
- configuration
 - audio 48
 - default IP settings 18
 - door sensor 36, 42, 44
 - intrusion sensor 36, 42, 44
 - network 29
 - SIP 31
- configuration home page 22
- configuration page
 - configurable parameters 27, 30, 32
- contact information 79
- contact information for CyberData 78, 79
- current network settings 30
- CyberData contact information 79

D

- default
 - gateway 18
 - IP address 18
 - subnet mask 18
 - username and password 18
 - web login username and password 22
- default gateway 18, 30
- default IP settings 18
- default login address 22
- device configuration 26
 - device configuration parameters 62
 - the device configuration page 61
- device configuration page 26
- device configuration parameters 27
- device configuration password
 - changing for web configuration access 26
- dial out extension (door sensor) 45, 46
- dial out extension (intrusion sensor) 46
- dial out extension strings 34
- dial-out extension strings 35
- discovery utility program 22
- DNS server 30
- door sensor 46
 - dial out extension 45, 46
 - door open timeout 45, 46
 - door sensor normally closed 45, 46
- download autoprovisioning template button 62
- DTMF tones 34, 35
- DTMF tones (using rfc2833) 34

E

- expiration time for SIP server lease 32, 33
- export settings 24, 25

F

- firmware
 - where to get the latest firmware 72

G

- get autoprovisioning template 62

H

home page 22

I

identifying your product 1
 import settings 24, 25
 import/export settings 24, 25
 installation, typical system 2
 intrusion sensor 46
 dial out extension 46
 IP address 18, 30
 IP addressing
 default
 IP addressing setting 18

L

lease, SIP server expiration time 32, 33
 Linux, setting up a TFTP server on 77
 local SIP port 33
 log in address 22

M

multicast configuration 48

N

navigation (web page) 19
 navigation table 19
 network configuration 29
 Nightringer 71
 NTP server 27

P

part number 6
 parts list 17
 password
 for SIP server login 32
 login 22
 restoring the default 18
 point-to-point configuration 35
 port

 local SIP 33
 remote SIP 33
 product overview
 product specifications 6
 typical system installation 2
 product specifications 6

R

reboot 74
 remote SIP port 33
 rport discovery setting, disabling 33

S

sales 79
 sensor setup page 13, 36, 42, 44
 sensor setup parameters 36, 42, 44
 sensors 45
 server address, SIP 32
 service 79
 SIP
 enable SIP operation 32
 local SIP port 33
 user ID 32
 SIP configuration 31
 SIP configuration parameters
 outbound proxy 33
 registration and expiration, SIP server lease 32, 33
 user ID, SIP 32
 SIP registration 32
 SIP remote SIP port 33
 SIP server 32
 password for login 32
 user ID for login 32
 SIP server configuration 32
 SRST 33
 subnet mask 18, 30

T

tech support 79
 technical support, contact information 79
 TFTP server 77

U

user ID
 for SIP server login 32

- username
 - changing for web configuration access 26
 - default for web configuration access 22
 - restoring the default 18

V

- VLAN ID 30
- VLAN Priority 30
- VLAN tagging support 30
- VLAN tags 30

W

- warranty policy at CyberData 79
- web access password 18
- web access username 18
- web configuration log in address 22
- web page
 - navigation 19
- web page navigation 19
- Windows, setting up a TFTP server on 77