



# *Secure Access Control Keypad Operations Guide*

Part #011433

Document Part #931384A  
for Firmware Version 1.0.0

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

---

---

**Secure Access Control Keypad Operations Guide 931384A**  
**Part # 011433**

**COPYRIGHT NOTICE:**

© 2017, 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:  
<http://support.cyberdata.net/>

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

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

Fax: (831) 373-4193

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

---

## Revision Information

Revision 931384A, which corresponds to firmware version 1.0.0, was released on September 19, 2017.

---

## Browsers Supported

The following browsers have been tested against firmware version 1.0.0:

- Chrome (version 57.0.2987.98)
- Firefox: (version 55.0.2)
- Internet Explorer (version 11.0.9600.18314)

---

## Pictorial Alert Icons

|                                                                                                    |                                                                                                                                                                                                 |
|----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <br>GENERAL ALERT | <b>General Alert</b><br>This pictorial alert indicates a potentially hazardous situation. This alert will be followed by a hazard level heading and more specific information about the hazard. |
|                   | <b>Ground</b><br>This pictorial alert indicates the Earth grounding connection point.                                                                                                           |

---

## Hazard Levels

**Danger:** Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury. This is limited to the most extreme situations.

**Warning:** Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.

**Caution:** Indicates a potentially hazardous situation which, if not avoided, could result in minor or moderate injury. It may also alert users against unsafe practices.

**Notice:** Indicates a statement of company policy (that is, a safety policy or protection of property).

The safety guidelines for the equipment in this manual do not purport to address all the safety issues of the equipment. It is the responsibility of the user to establish appropriate safety, ergonomic, and health practices and determine the applicability of regulatory limitations prior to use. Potential safety hazards are identified in this manual through the use of words Danger, Warning, and Caution, the specific hazard type, and pictorial alert icons.

---

# Important Safety Instructions

1. Read these instructions.
2. Keep these instructions.
3. Heed all warnings.
4. Follow all instructions.
5. Do not use this apparatus near water.
6. Clean only with dry cloth.
7. Do not block any ventilation openings. Install in accordance with the manufacturer's instructions.
8. Do not install near any heat sources such as radiators, heat registers, stoves, or other apparatus (including amplifiers) that produce heat.
9. Do not defeat the safety purpose of the polarized or grounding-type plug. A polarized plug has two blades with one wider than the other. A grounding type plug has two blades and a third grounding prong. The wide blade or the third prong are provided for your safety. If the provided plug does not fit into your outlet, consult an electrician for replacement of the obsolete outlet.
10. Protect the power cord from being walked on or pinched particularly at plugs, convenience receptacles, and the point where they exit from the apparatus.
11. Only use attachments/accessories specified by the manufacturer.
12. Refer all servicing to qualified service personnel. Servicing is required when the apparatus has been damaged in any way, such as power-supply cord or plug is damaged, liquid has been spilled or objects have fallen into the apparatus, the apparatus has been exposed to rain or moisture, does not operate normally, or has been dropped.
13. Prior to installation, consult local building and electrical code requirements.

**14. WARNING: The Intercom enclosure is not rated for any AC voltages!**

|                                                                                                      |                                                                                                                                                                                        |
|------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <br>GENERAL ALERT | <p><b>Warning</b></p> <p><i>Electrical Hazard:</i> This product should be installed by a licensed electrician according to all local electrical and building codes.</p>                |
| <br>GENERAL ALERT | <p><b>Warning</b></p> <p><i>Electrical Hazard:</i> To prevent injury, this apparatus must be securely attached to the floor/wall in accordance with the installation instructions.</p> |
| <br>GENERAL ALERT | <p><b>Warning</b></p> <p>The PoE connector is intended for intra-building connections only and does not route to the outside plant.</p>                                                |

|                                                                        |               |
|------------------------------------------------------------------------|---------------|
| <b>Chapter 1 Product Overview</b>                                      | <b>1</b>      |
| 1.1 How to Identify This Product .....                                 | 1             |
| 1.2 Typical System Installation .....                                  | 2             |
| 1.3 Product Features .....                                             | 4             |
| 1.4 Supported Protocols .....                                          | 5             |
| 1.5 Supported SIP Servers .....                                        | 5             |
| 1.6 Specifications .....                                               | 6             |
| <br><b>Chapter 2 Installing the Secure Access Control Keypad</b>       | <br><b>7</b>  |
| 2.1 Parts List .....                                                   | 7             |
| 2.2 Intercom Components .....                                          | 8             |
| 2.3 Secure Access Control Keypad Setup .....                           | 9             |
| 2.3.1 Intercom Connections .....                                       | 9             |
| 2.3.2 Using the On-Board Relay .....                                   | 10            |
| 2.3.3 Wiring the Circuit .....                                         | 11            |
| 2.3.4 Connectors and Functions .....                                   | 15            |
| 2.3.5 Activity and Link LEDs .....                                     | 17            |
| 2.3.6 Restoring the Factory Default Settings .....                     | 18            |
| 2.4 Configure the Intercom Parameters .....                            | 19            |
| 2.4.1 Factory Default Settings .....                                   | 19            |
| 2.4.2 Intercom Web Page Navigation .....                               | 20            |
| 2.4.3 Using the Toggle Help Button .....                               | 21            |
| 2.4.4 Log in to the Configuration Home Page .....                      | 23            |
| 2.4.5 Configure the Device .....                                       | 27            |
| 2.4.6 Configure the Security .....                                     | 33            |
| 2.4.7 Configure the Network Parameters .....                           | 40            |
| 2.4.8 Configure the SIP (Session Initiation Protocol) Parameters ..... | 43            |
| 2.4.9 Configure the Sensor Configuration Parameters .....              | 47            |
| 2.4.10 Configure the Audio Configuration Parameters .....              | 50            |
| 2.4.11 Configure the Events Parameters .....                           | 53            |
| 2.4.12 Configure the Door Strike Relay .....                           | 58            |
| 2.4.13 Configure the Autoprovisioning Parameters .....                 | 60            |
| 2.5 Upgrade the Firmware and Reboot the Intercom .....                 | 72            |
| 2.5.1 Downloading the Firmware .....                                   | 72            |
| 2.5.2 Reboot the Device .....                                          | 75            |
| 2.6 Command Interface .....                                            | 76            |
| 2.6.1 Command Interface Post Commands .....                            | 76            |
| <br><b>Appendix A Mounting the Intercom</b>                            | <br><b>77</b> |
| A.1 Mounting Components .....                                          | 77            |
| A.2 Dimensions .....                                                   | 78            |
| A.3 Overview of Installation Types .....                               | 80            |
| A.4 Service Loop Cable Routing .....                                   | 81            |
| A.5 Securing the Enclosure .....                                       | 82            |
| A.6 Additional Mounting Options .....                                  | 83            |
| A.6.1 Conduit Mounting (Side Entry) (Not Provided) .....               | 83            |
| A.6.2 Goose Neck Mounting Option (Not Provided) .....                  | 84            |
| <br><b>Appendix B Setting up a TFTP Server</b>                         | <br><b>85</b> |
| B.1 Set up a TFTP Server .....                                         | 85            |
| B.1.1 In a LINUX Environment .....                                     | 85            |
| B.1.2 In a Windows Environment .....                                   | 85            |
| <br><b>Appendix C Troubleshooting/Technical Support</b>                | <br><b>86</b> |
| C.1 Frequently Asked Questions (FAQ) .....                             | 86            |
| C.2 Documentation .....                                                | 86            |
| C.3 Contact Information .....                                          | 87            |
| C.4 Warranty and RMA Information .....                                 | 87            |



# 1 Product Overview

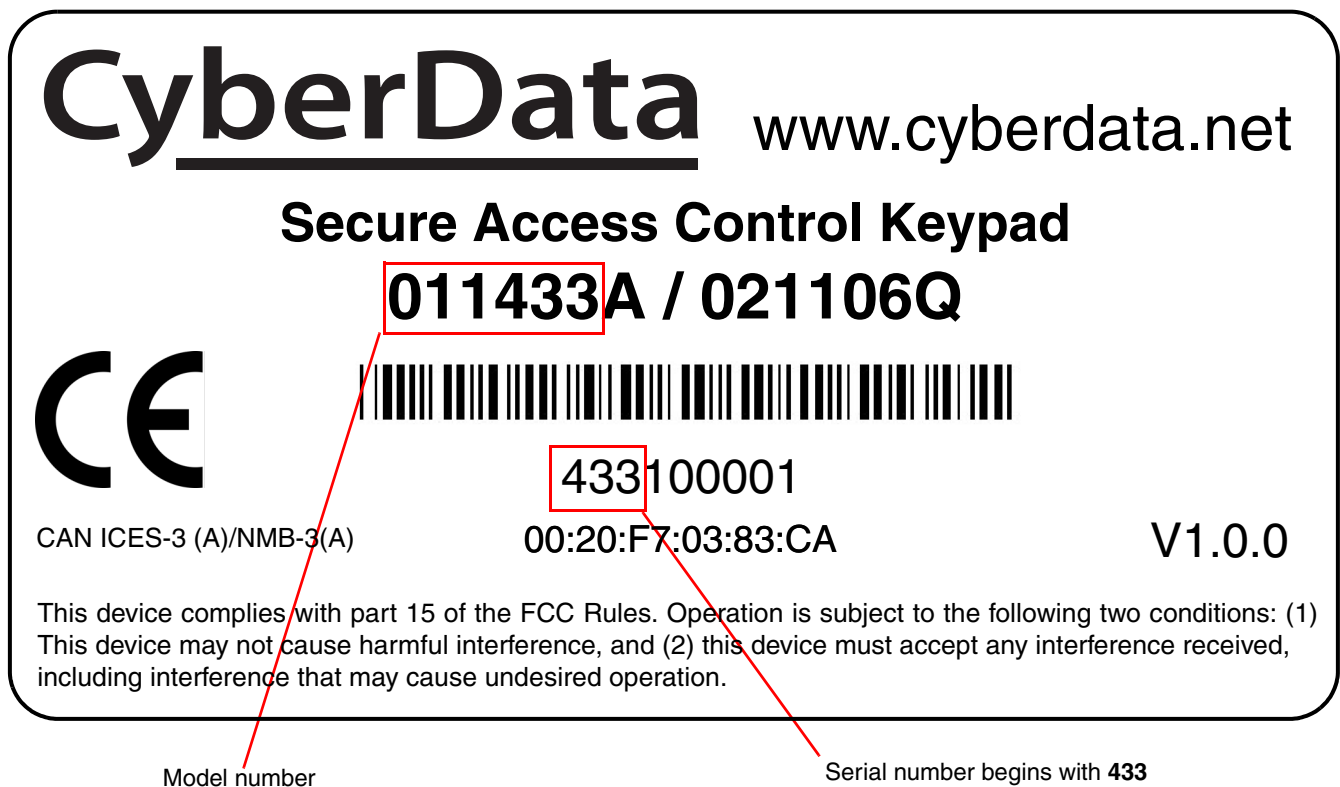
## 1.1 How to Identify This Product

To identify the Secure Access Control Keypad, 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 **011433**.
- The serial number on the label should begin with **433**.

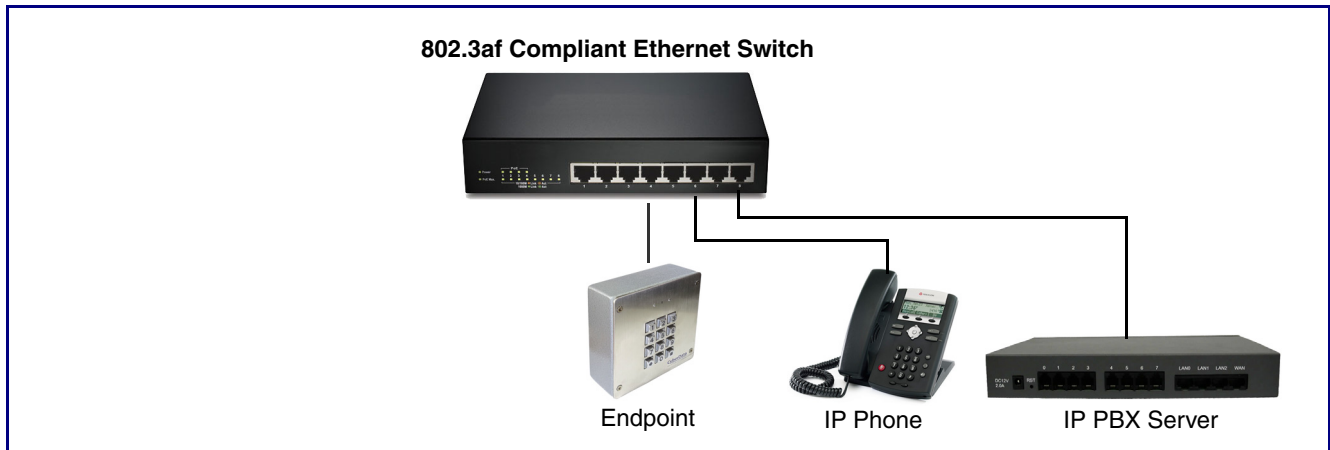
**Figure 1-1. Model Number Label**



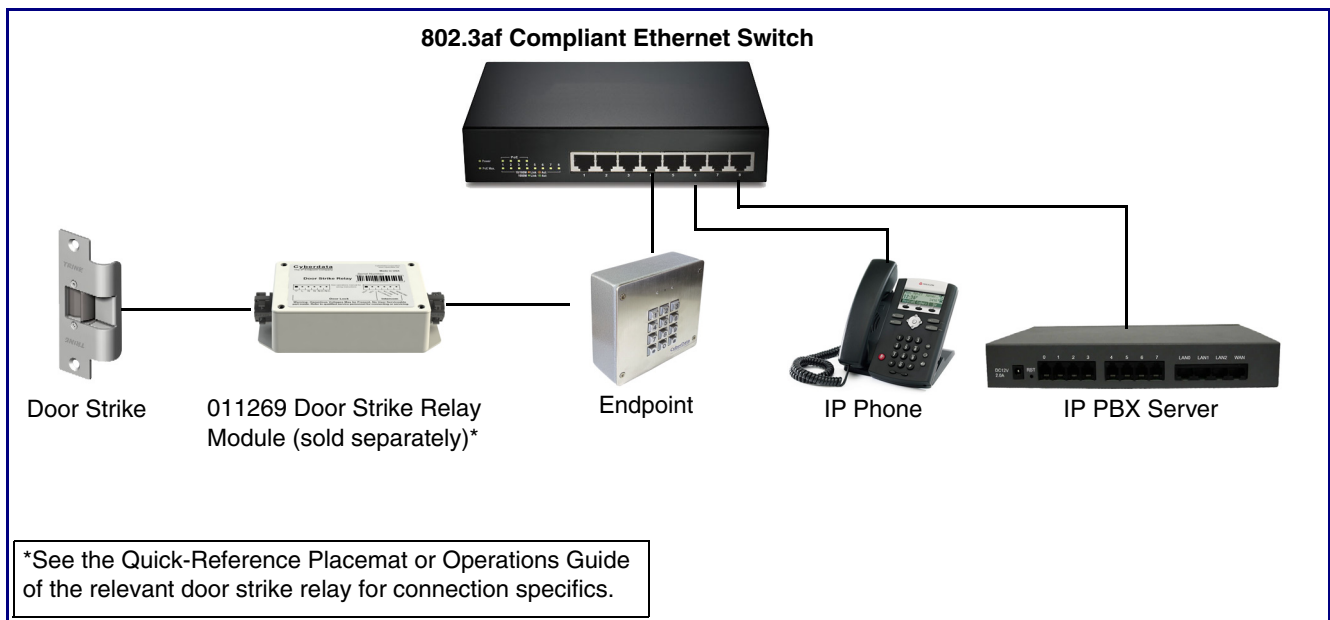
## 1.2 Typical System Installation

The following figures illustrate how the Secure Access Control Keypad can be installed as part of a VoIP phone system.

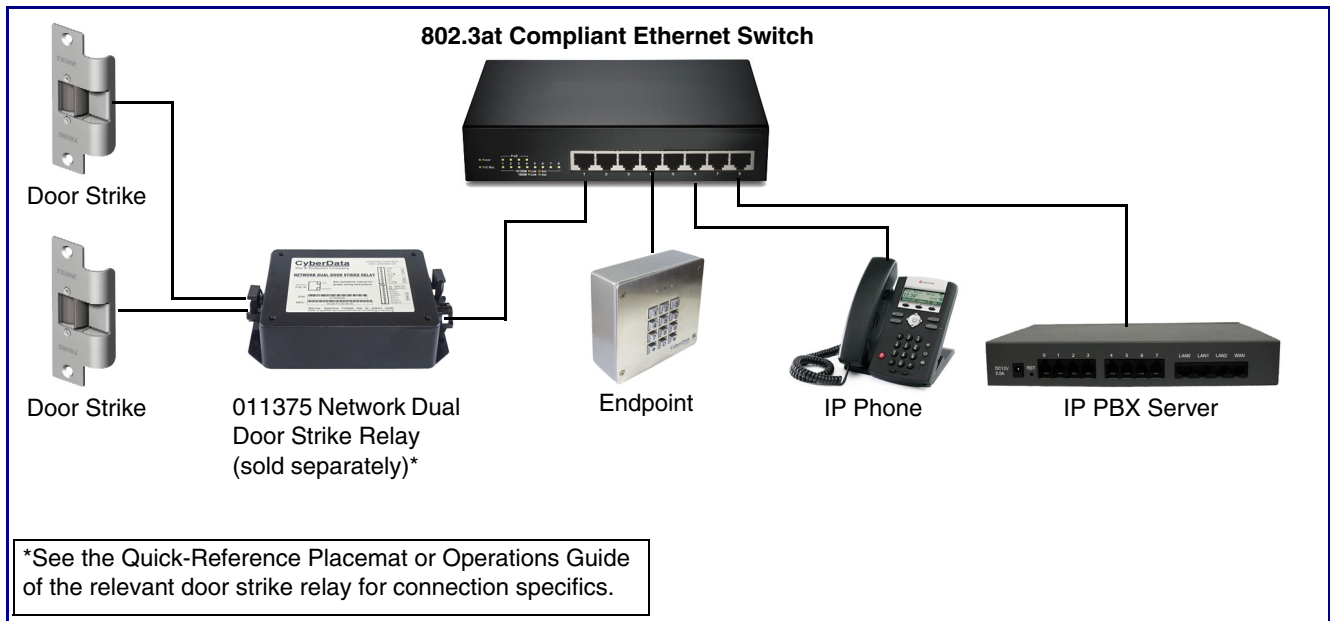
**Figure 1-2. Typical Installation**



**Figure 1-3. Installation with the Door Strike Relay Module**



**Figure 1-4. Installation with the Network Dual Door Strike Relay**



---

## 1.3 Product Features

The SIP Outdoor Intercom has the following features:

- SIP compliant
- PoE 802.3af enabled (Powered-over-Ethernet)
- IP 65 outdoor-rated
- Optional weather shroud for even greater weather protection
- Alert buzzer
- Red/Green lock status lights
- Can operate in standalone mode. PBX not required. Future-proof and adaptable when upgrading to new VoIP PBX
- Built in time of access scheduler
- Local and remote logging with time stamp
- NTP time support
- Network web management
- Supports 500 Access Codes
- Blacklisted code alert via dialout and multicast stored message
- Network downloadable firmware
- Dry contact relay to trigger door lock or unlock gates
- Door closure and tamper alert signal
- Support for CyberData's Networked Dual Door Strike Relay (part# 011375) and Intermediate Door Strike Relay (part# 011269)
- Security Torx screws with driver kit included

---

## 1.4 Supported Protocols

The Intercom supports the following protocols:

- SIP (session initiation protocol)
- HTTP Web-based configuration

Provides an intuitive user interface for easy system configuration and verification of Intercom operations.

- DHCP Client

Dynamically assigns IP addresses in addition to the option to use static addressing.

- TFTP Client

Facilitates hosting for the Autoprovisioning configuration file.

- RTP

- Facilitates autoprovisioning configuration values on boot

- Audio Encodings

PCMU (G.711 mu-law)

PCMA (G.711 A-law)

G.722

Packet Time 20 ms

---

## 1.5 Supported SIP Servers

The following link contains information on how to configure the device for the supported SIP servers:

<http://www.cyberdata.net/connecting-to-ip-pbx-servers/>

## 1.6 Specifications

**Table 1-1. Specifications**

| Specifications          |                                                                                                                                                                                |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ethernet I/F            | 10/100 Mbps                                                                                                                                                                    |
| Protocol                | SIP RFC 3261 Compatible                                                                                                                                                        |
| Power Input             | PoE 802.3af compliant or +8 to +12VDC @ 1000mA Regulated Power Supply <sup>a</sup>                                                                                             |
| On-Board Relay          | 1A at 30 VDC                                                                                                                                                                   |
| Operating Range         | Temperature: -40° C to 55° C (-40° F to 131° F)<br>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)                                                                                                                                                      |
| IP Rating               | IP65                                                                                                                                                                           |
| Payload Types           | G711, A-law and $\mu$ -law, G.722                                                                                                                                              |
| Dimensions <sup>b</sup> | 5.118 inches [130 mm] Length<br>2.172 inches [55.2 mm] Width<br>5.118 inches [130 mm] Height                                                                                   |
| Weight                  | 2.0 lbs. (0.90 kg)                                                                                                                                                             |
| Boxed Weight            | 3.0 lbs. (1.36 kg)                                                                                                                                                             |
| Compliance              | CE; EMC Directive – Class A EN 55032 & EN 55024, LV Safety Directive – EN 60950-1, RoHS Compliant, FCC; Part 15 Class A, Industry Canada; ICES-3 Class A, IEEE 802.3 Compliant |
| Part Number             | 011433<br>011188 Weather Shroud (sold separately)                                                                                                                              |

a. Contacts 1 and 2 on the J3 terminal block are only for powering the device from a non-PoE 12VDC power source as an alternative to Network PoE power. Use of these contacts for any other purpose will damage the device and void the product warranty.

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

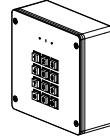
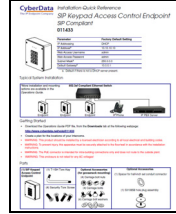
# 2 Installing the Secure Access Control Keypad

## 2.1 Parts List

[Table 2-1](#) illustrates the SIP Outdoor Intercom parts.

**Note** See [Appendix A, "Mounting the Intercom"](#) for physical mounting information.

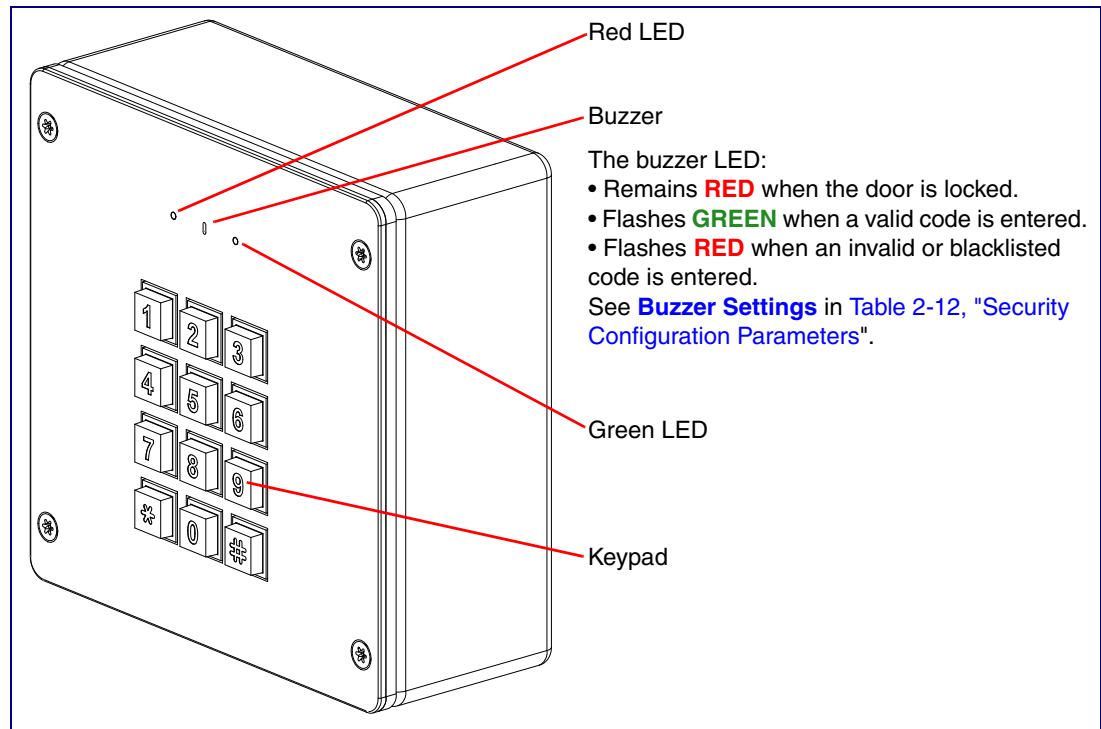
**Table 2-1. Parts List**

| Quantity | Part Name                          | Illustration                                                                          |
|----------|------------------------------------|---------------------------------------------------------------------------------------|
| 1        | Intercom Assembly                  |    |
| 1        | Installation Quick Reference Guide |   |
| 1        | Intercom Mounting Accessory Kit    |  |

## 2.2 Intercom Components

Figure 2-1 shows the components of the Intercom.

**Figure 2-1. Intercom Components**



## 2.3 Secure Access Control Keypad Setup

### 2.3.1 Intercom Connections

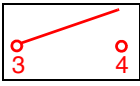
Figure 2-2 shows the pin connections on the terminal block. This terminal block can accept 16 AWG gauge wire.

**Note** As an alternative to using PoE power, you can supply +8 to +12VDC @ 1000mA Regulated Power Supply into the terminal block.

|                                                                                                    |                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <br>GENERAL ALERT | <p><b>Caution</b></p> <p><i>Equipment Hazard:</i> Contacts 1 and 2 on the terminal block are only for powering the device from a non-PoE 12 VDC power source as an alternative to Network PoE power. Use of these contacts for any other purpose will damage the device and void the product warranty.</p> |
|----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**Figure 2-2. Connections and Alternate Power Input**

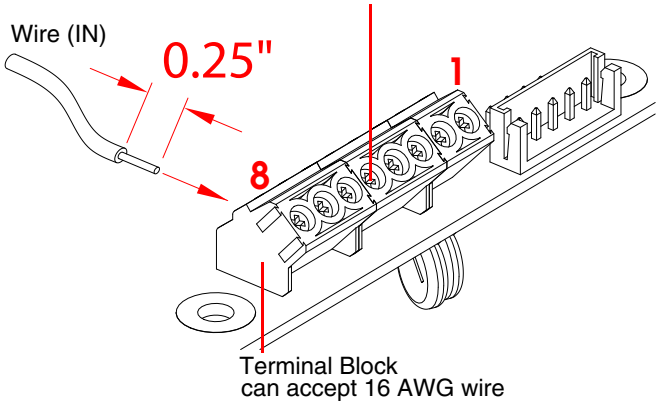
Alternate Power Input:  
1 = +8 to +12VDC @ 1000mA Regulated Power Supply\*  
2 = Power Ground\*



Relay Contact:  
(1 A at 30 VDC for continuous loads)  
3 = Relay Common  
4 = Relay Normally Open Contact  
5 = Sense Input  
6 = Sense Ground  
7 = Remote Switch "A"  
8 = Remote Switch "B"

\*Contacts 1 and 2 on the terminal block are only for powering the device from a non-PoE 12VDC power source as an alternative to Network PoE power. Use of these contacts for any other purpose will damage the device and void the product warranty.

Use a 3.17 mm (1/8-inch) flat blade screwdriver for the terminal block screws



## 2.3.2 Using the On-Board Relay

|                                                                                                    |                                                                                                                                                                                                                                                  |
|----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <br>GENERAL ALERT | <p><b>Warning</b></p> <p><i>Electrical Hazard:</i> This product should be installed by a licensed electrician according to all local electrical and building codes.</p>                                                                          |
| <br>GENERAL ALERT | <p><b>Warning</b></p> <p><i>Electrical Hazard:</i> The relay contacts are dry and provided for a normally open and momentarily closed configuration. Neither the alternate power input nor PoE power can be used to drive a door strike.</p>     |
| <br>GENERAL ALERT | <p><b>Warning</b></p> <p><i>Electrical Hazard:</i> The relay does not support AC powered door strikes. Any use of this relay beyond its normal operating range can cause damage to the product and is not covered under our warranty policy.</p> |

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

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

We highly recommend that inductive load and high current devices use our Networked Dual Door Strike Relay (CD# 011375) (see [Section 2.3.3.2, "Network Dual Door Strike Relay Wiring Diagram with External Power Source"](#)).

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

For more information on the sensor options, see the [Sensor Configuration Page](#) on the web interface.

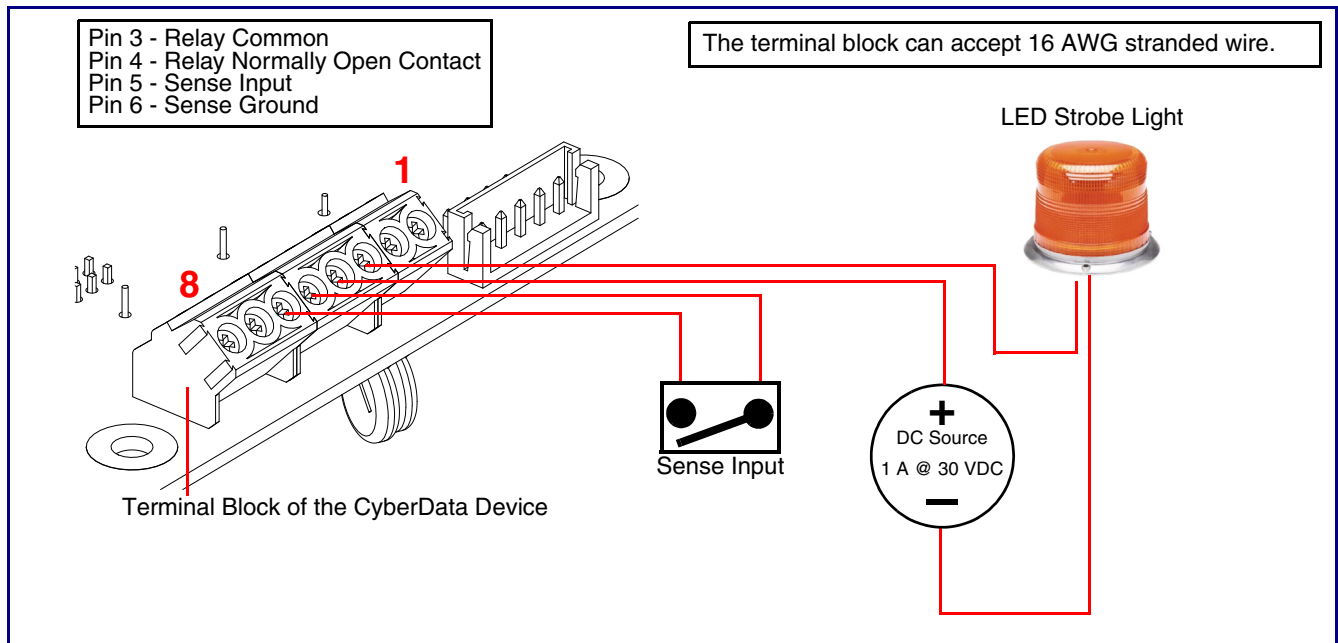
## 2.3.3 Wiring the Circuit

### 2.3.3.1 Devices Less than 1A at 30 VDC

If the power for the device is less than 1A at 30 VDC and is not an inductive load, then see [Figure 2-3](#) for the wiring diagram.

When configuring with an inductive load, please use an intermediary relay with a High PIV Ultrafast Switching Diode. We recommend using the Network Dual Door Strike Relay (CD# 011375) (see [Section 2.3.3.2, "Network Dual Door Strike Relay Wiring Diagram with External Power Source"](#)).

**Figure 2-3. Devices Less than 1A at 30 VDC**



### 2.3.3.2 Network Dual Door Strike Relay Wiring Diagram with External Power Source

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

This product provides an easier method of connecting standard door strikes as well as AC and higher voltage devices. See [Figure 2-4](#) and [Figure 2-5](#) for the wiring diagrams.

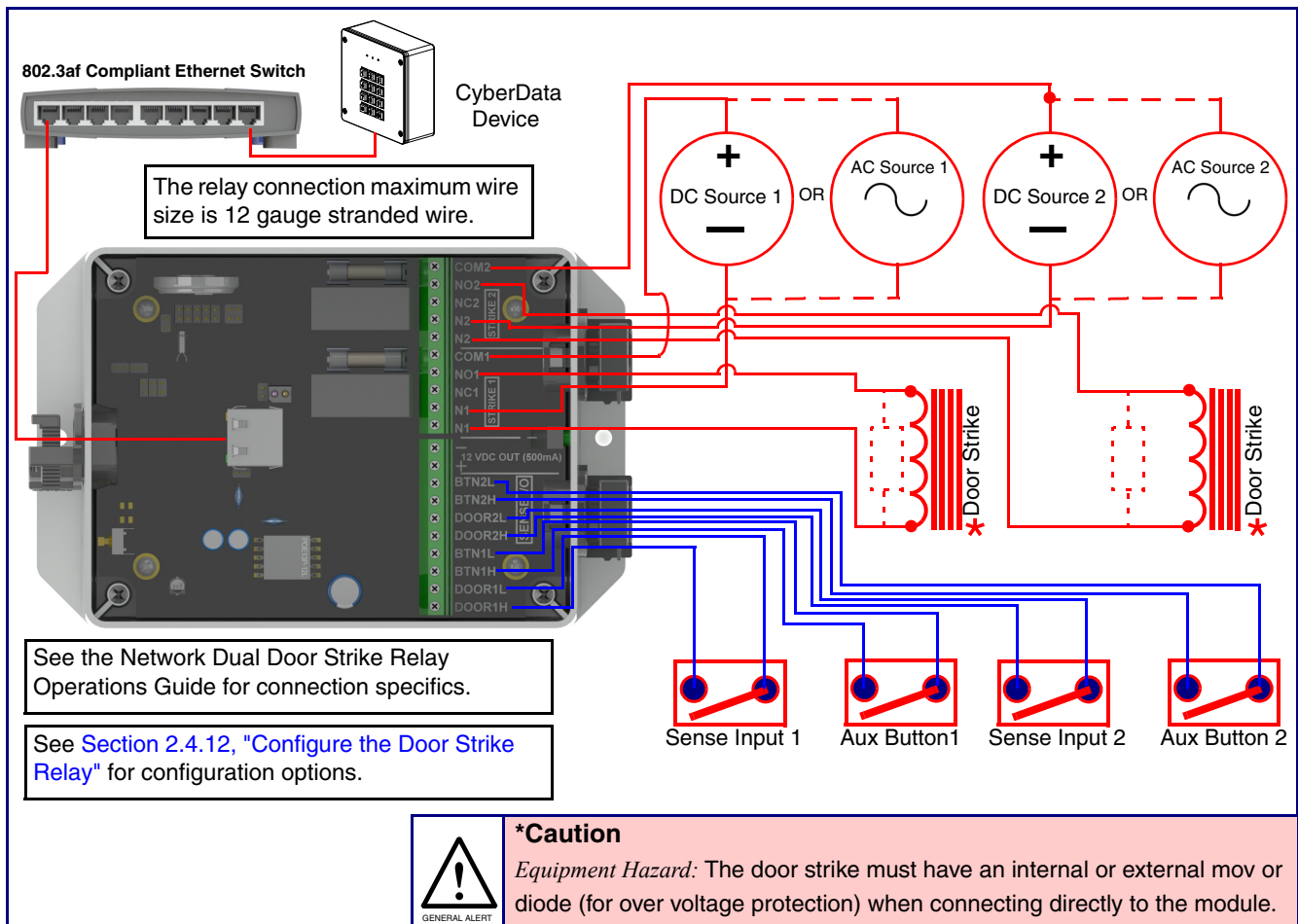


GENERAL ALERT

**Warning**

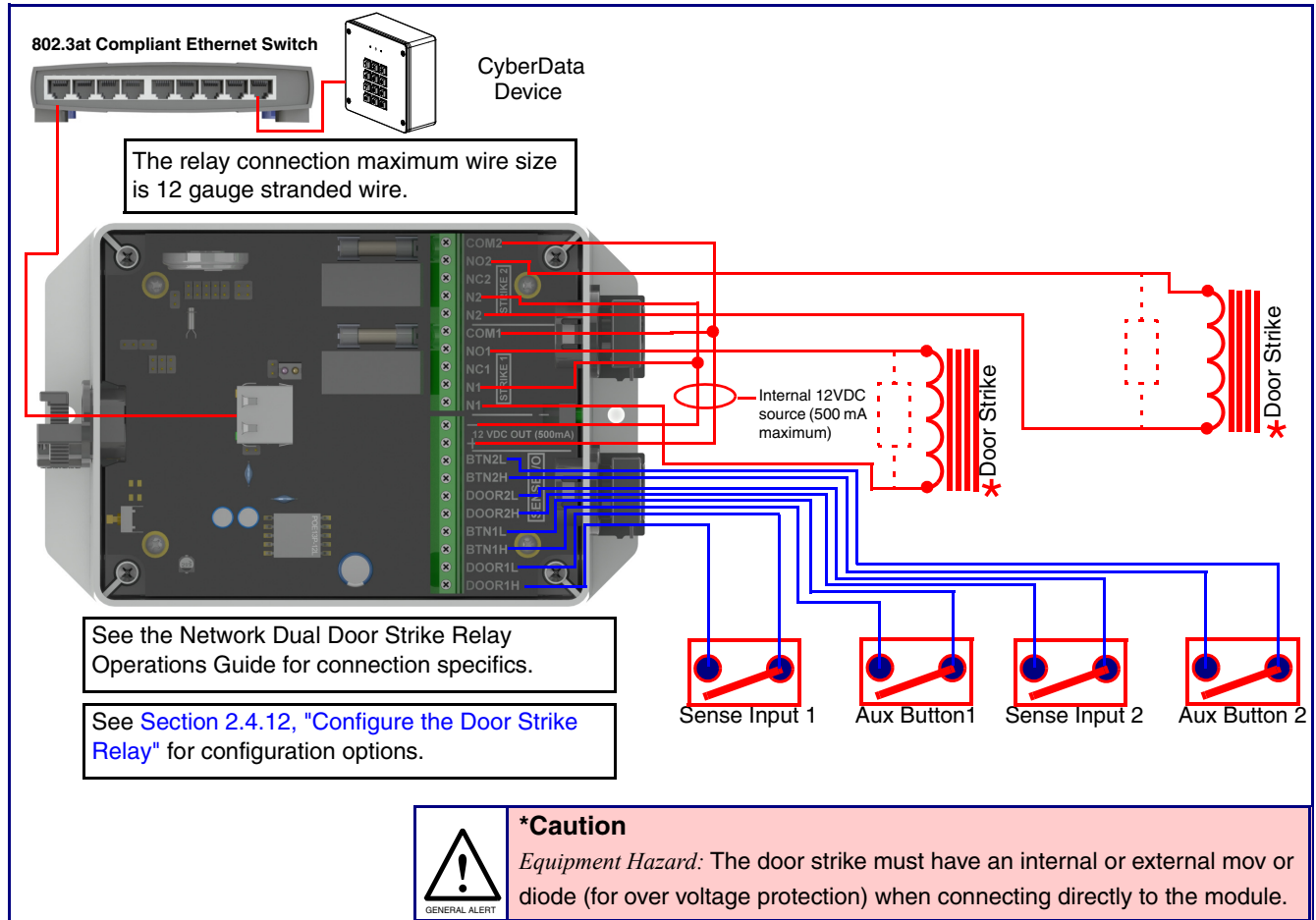
*Electrical Hazard:* Hazardous voltages may be present. No user serviceable part inside. Refer to qualified service personnel for connecting or servicing.

**Figure 2-4. Network Dual Door Strike Relay Wiring Diagram with External Power Source**



### 2.3.3.3 Network Dual Door Strike Relay Wiring Diagram Using 802.3at

**Figure 2-5. Network Dual Door Strike Relay Wiring Diagram Using 802.3at**



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

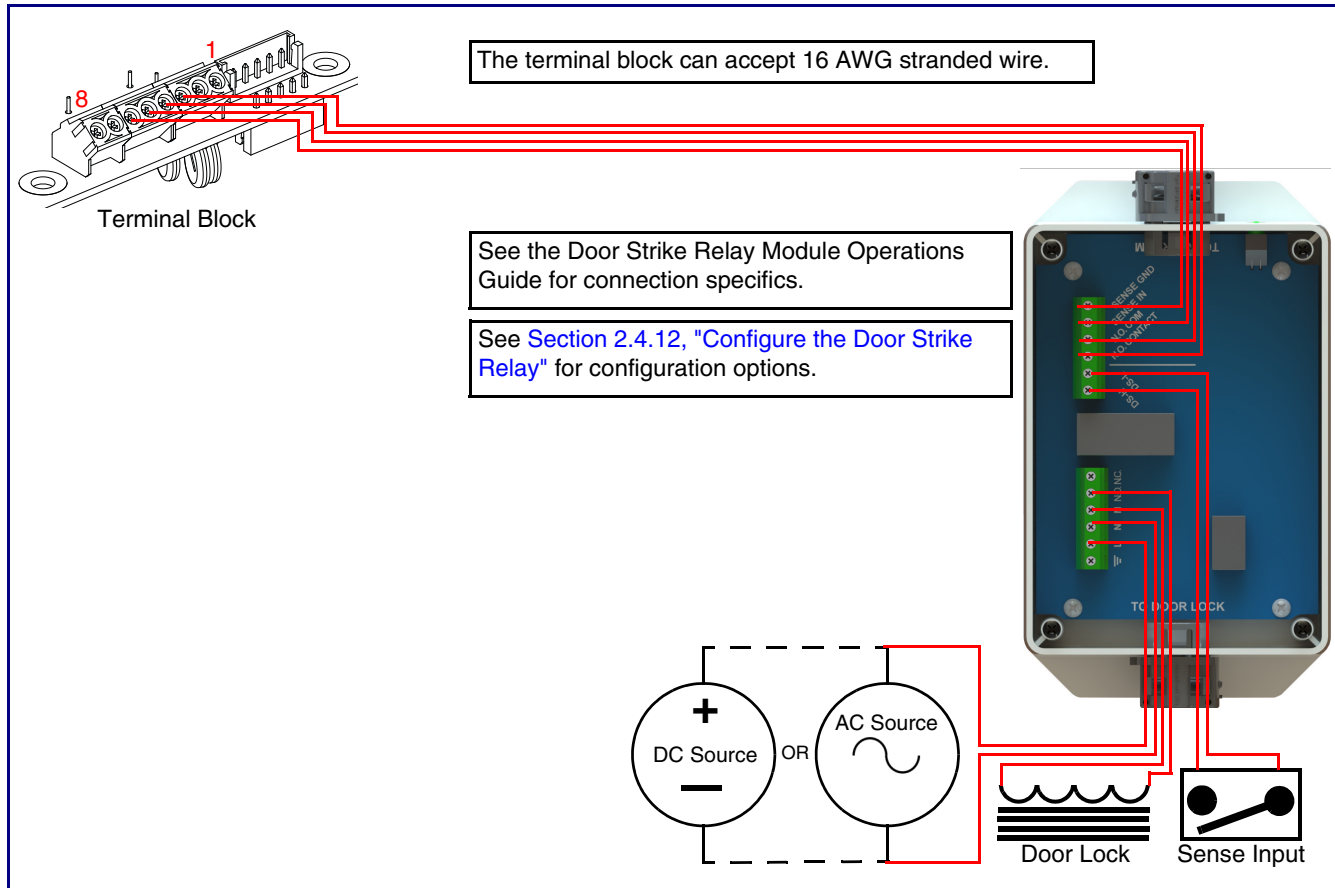
<http://support.cyberdata.net/>

### 2.3.3.4 Door Strike Relay Module Wiring Diagram from the Device

For wiring an electronic door strike, we recommend the use of our external Door Strike Relay Module (CD# 011269).

This product provides an easier method of connecting standard door strikes as well as AC and higher voltage devices. See [Figure 2-6](#) for the wiring diagram.

**Figure 2-6. Door Strike Relay Module Wiring Diagram from the Device**



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

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

### 2.3.4 Connectors and Functions

See the following figures and tables to identify the connectors and functions.

Figure 2-7. Connector Locations

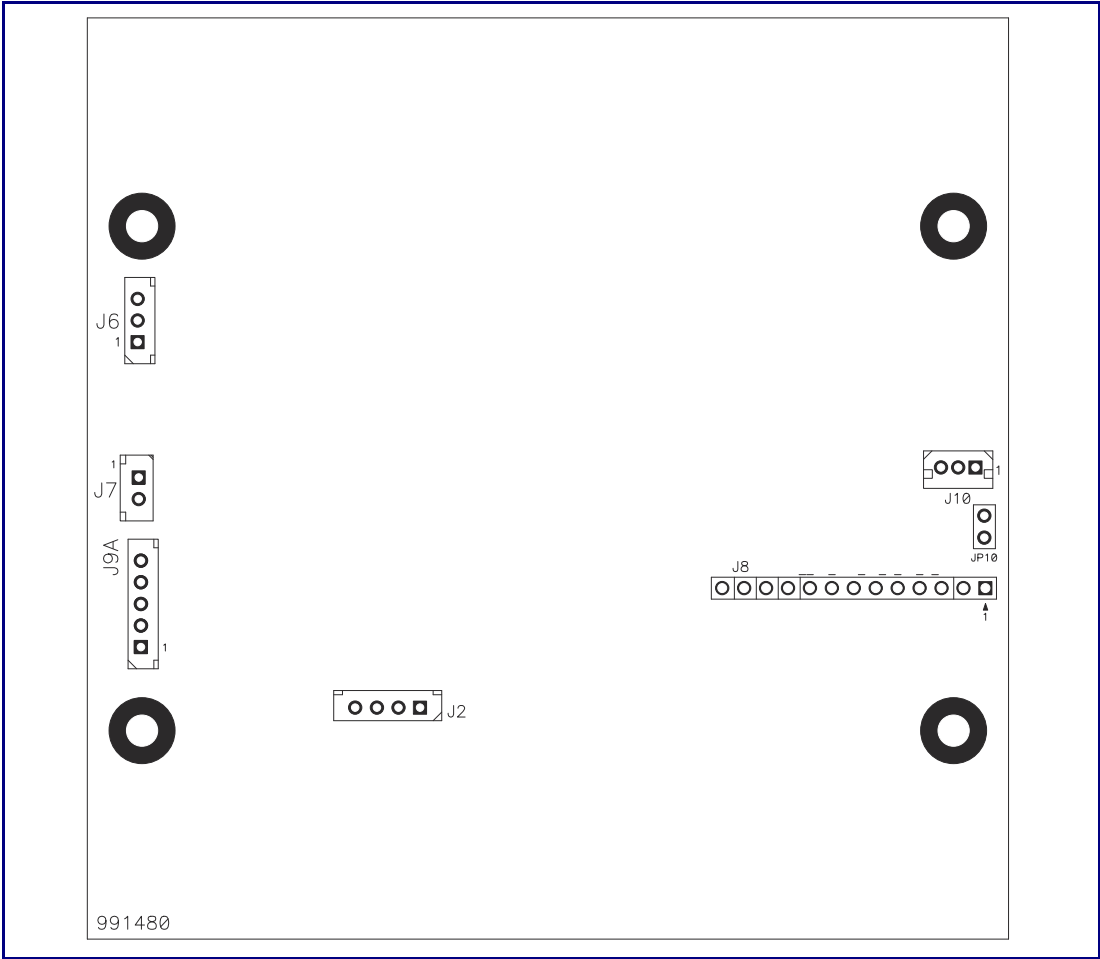
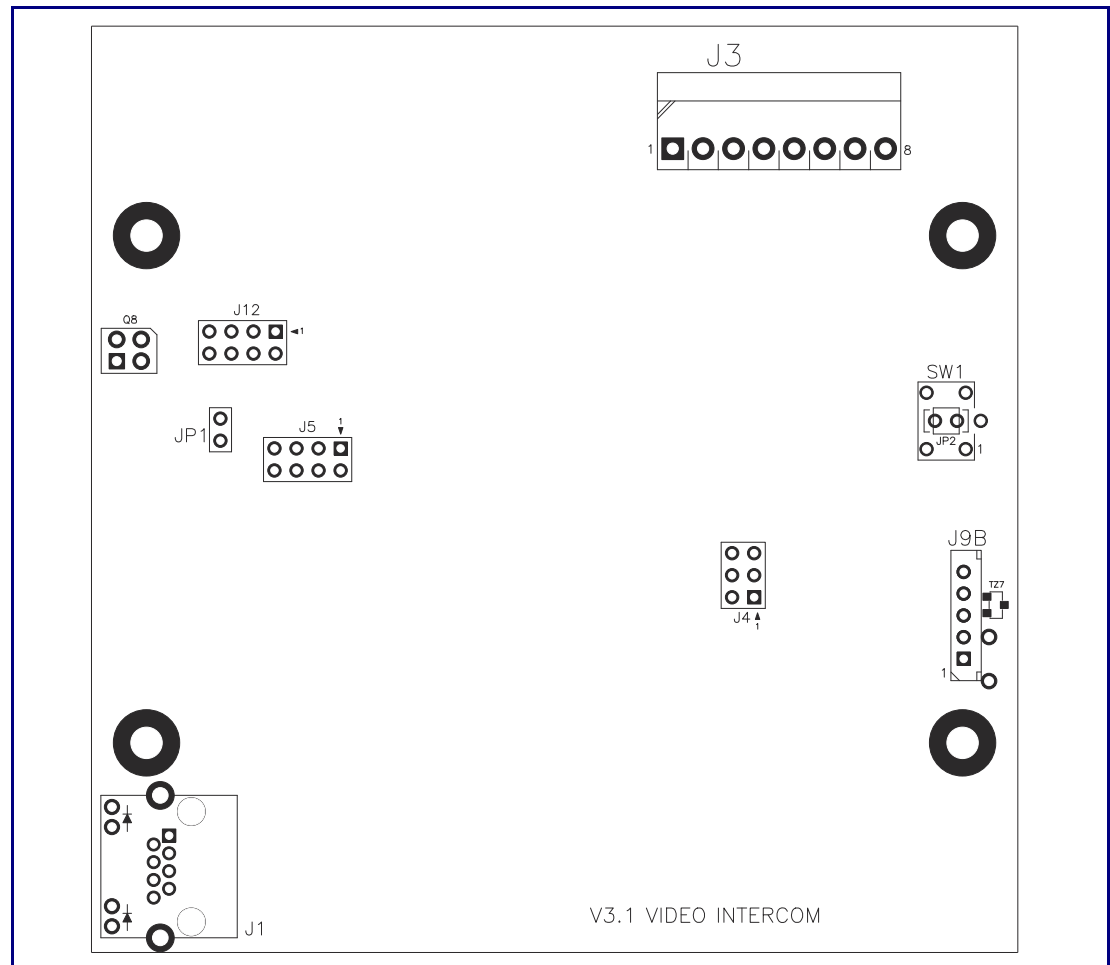


Table 2-2. Connector Functions

| Connector | Function                                      |
|-----------|-----------------------------------------------|
| J2        | Call Button LED Interface                     |
| J6        | Microphone Interface                          |
| J7        | Speaker Interface                             |
| J8        | Keypad Interface (Not Used)                   |
| J9A       | I2C 5V Peripheral Bus                         |
| JP10      | Disables the intrusion sensor when installed. |

**Figure 2-8. Connector Locations**



**Table 2-3. Connector Functions**

| Connector | Function                                                                    |
|-----------|-----------------------------------------------------------------------------|
| J1        | PoE Network Connection (RJ-45 ethernet)                                     |
| J3        | Terminal Block (see <a href="#">Figure 2-2</a> )                            |
| J4        | Console Port (Factory Use Only)                                             |
| JP1       | Reset Jumper <sup>a</sup>                                                   |
| J12       | Reserved (Factory Use Only)                                                 |
| J5        | JTAG (Factory Use Only)                                                     |
| J9B       | Buzzer/LED Board Interface                                                  |
| SW1       | See <a href="#">Section 2.3.6, "Restoring the Factory Default Settings"</a> |
| Q8        | Intrusion Sensor                                                            |

a. Do not install a jumper. Momentary short to reset. Permanent installation of a jumper would prevent the board from running all together.

---

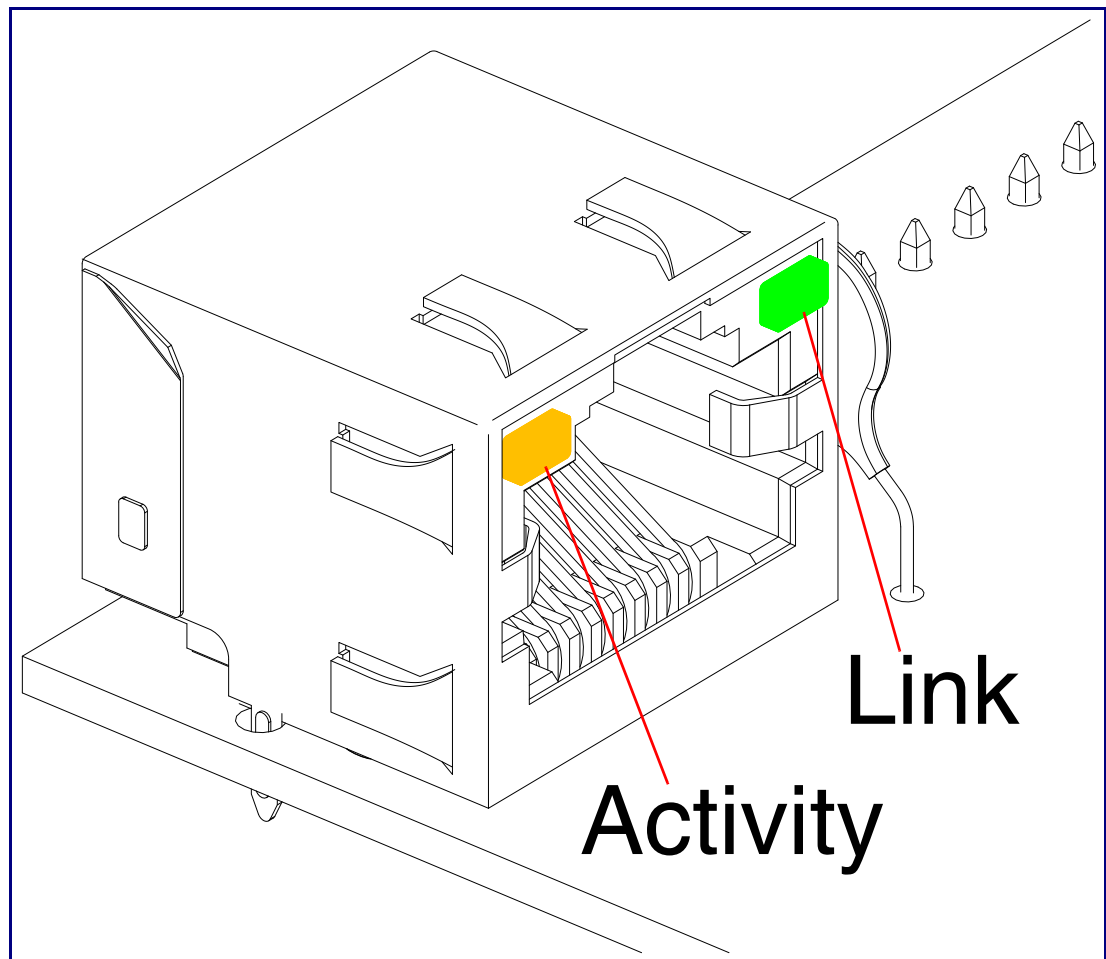
## 2.3.5 Activity and Link LEDs

### 2.3.5.1 Verifying the Network Connectivity and Data Rate

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

- The square, **AMBER Link/Activity** LED blinks when there is network activity (see [Figure 2-9](#)).
- The square, **GREEN 100Mb Link** LED above the Ethernet port indicates that the network connection has been established (see [Figure 2-9](#)).

**Figure 2-9. Activity and Link LED**



## 2.3.6 Restoring the Factory Default Settings

When troubleshooting configuration problems, it is sometimes convenient to restore the device to a known state.

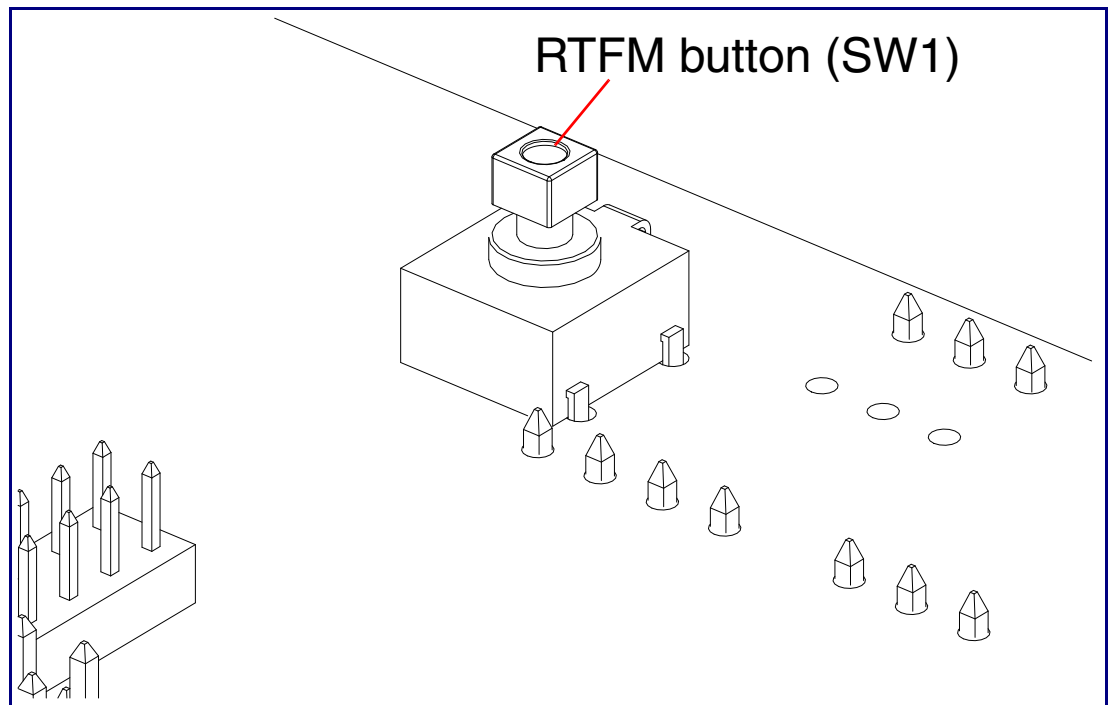
**Note** Each device is delivered with factory set default values.

To restore the factory default settings:

1. Press and hold the **RTFM button** (see **SW1** in [Figure 2-10](#)) for more than five seconds.
2. When the RTFM button is pressed, the keypad lights turn off (if the brightness is not set to 0).
3. The keypad lights blink during the boot process, turn off briefly, and then remain on and solid.

**Note** THE device will use DHCP to obtain the new IP address (DHCP-assigned address or default to 10.10.10.10 if a DHCP server is not present).

**Figure 2-10. RTFM Button**



---

## 2.4 Configure the Intercom Parameters

To configure the Intercom online, use a standard web browser.

Configure each Intercom and verify its operation *before* you mount it. When you are ready to mount an Intercom, refer to [Appendix A, "Mounting the Intercom"](#) for instructions.

---

### 2.4.1 Factory Default Settings

All Intercoms are initially configured with the following default IP settings:

When configuring more than one Intercom, attach the Intercoms to the network and configure one at a time to avoid IP address conflicts.

**Table 2-4. Factory Default Settings**

| Parameter                    | Factory Default Setting |
|------------------------------|-------------------------|
| IP Addressing                | DHCP                    |
| IP Address <sup>a</sup>      | 10.10.10.10             |
| Web Access Username          | admin                   |
| Web Access Password          | admin                   |
| Subnet Mask <sup>a</sup>     | 255.0.0.0               |
| Default Gateway <sup>a</sup> | 10.0.0.1                |

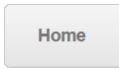
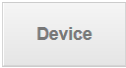
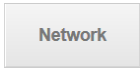
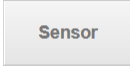
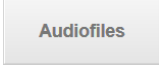
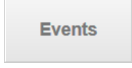
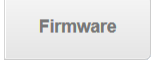
a. Default if there is not a DHCP server present.

---

## 2.4.2 Intercom Web Page Navigation

Table 2-5 shows the navigation buttons that you will see on every Intercom web page.

**Table 2-5. Web Page Navigation**

| Web Page Item                                                                       | Description                                |
|-------------------------------------------------------------------------------------|--------------------------------------------|
|    | Link to the <b>Home</b> page.              |
|    | Link to the <b>Device</b> page.            |
|    | Link to the <b>Security</b> page.          |
|    | Link to the <b>Network</b> page.           |
|    | Link to go to the <b>SIP</b> page.         |
|   | Link to the <b>Sensor</b> page.            |
|  | Link to the <b>Audiofiles</b> page.        |
|  | Link to the <b>Events</b> page.            |
|  | Link to the <b>Door Strike Relay</b> page. |
|  | Link to the <b>Autoprovisioning</b> page.  |
|  | Link to the <b>Firmware</b> page.          |

## 2.4.3 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:

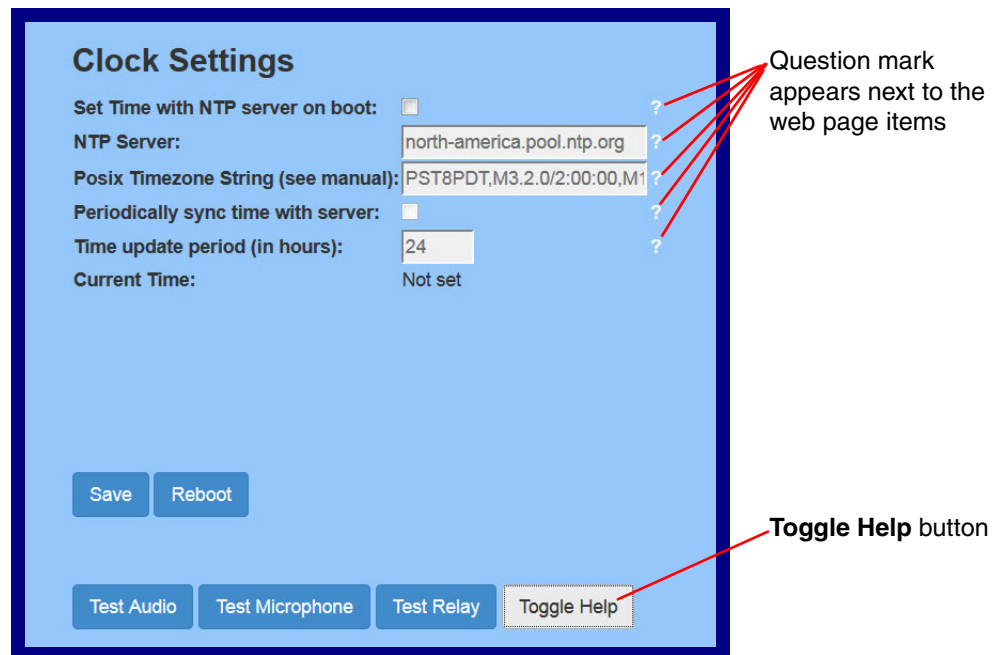
1. Click on the **Toggle Help** button that is on the UI webpage. See [Figure 2-11](#) and [Figure 2-12](#).

**Figure 2-11. Toggle/Help Button**



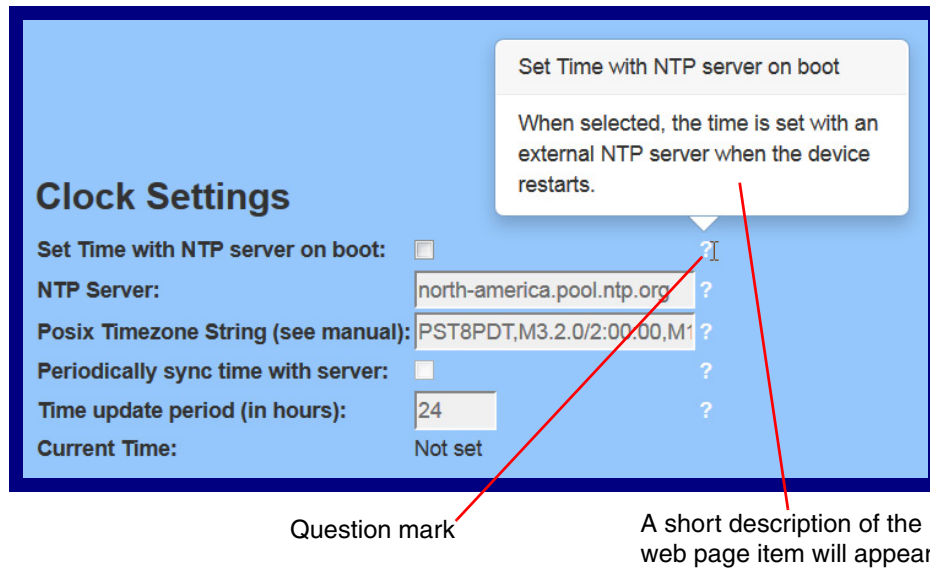
2. You will see a question mark (?) appear next to each web page item that has been provided with a short description by the Help feature. See [Figure 2-12](#).

**Figure 2-12. 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 2-13](#).

**Figure 2-13. Short Description Provided by the Help Feature**



---

## 2.4.4 Log in to the Configuration Home Page

1. Open your browser to the Intercom IP address.

**Note** If the network does not have access to a DHCP server, the device will default to an IP address of 10.10.10.10.

**Note** Make sure that the PC is on the same IP network as the Intercom.

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

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

<http://www.cyberdata.net/assets/common/discovery.zip>

**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 2-14):

Web Access Username: **admin**

Web Access Password: **admin**

Figure 2-14. Home Page



3. On the **Home** page, review the setup details and navigation buttons described 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. Home Page Overview**

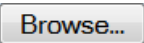
| Web Page Item                                                                       | Description                                                                                                                                          |
|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Admin Settings</b>                                                               |                                                                                                                                                      |
| 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.                                                                                                                  |
| <b>Current Status</b>                                                               |                                                                                                                                                      |
| Serial Number                                                                       | Shows the device serial number.                                                                                                                      |
| Mac Address                                                                         | Shows the device Mac address.                                                                                                                        |
| Firmware Version                                                                    | Shows the current firmware version.                                                                                                                  |
| IP Addressing                                                                       | Shows the current IP addressing setting ( <b>DHCP</b> or <b>static</b> ).                                                                            |
| 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.                                                                                                         |
| <b>Import Settings</b>                                                              |                                                                                                                                                      |
|  | Use this button to select a configuration file to import.                                                                                            |
|  | After selecting a configuration file, click Import to import the configuration from the selected file. Then, click Save and Reboot to store changes. |
| <b>Export Settings</b>                                                              |                                                                                                                                                      |
|  | Click Export to export the current configuration to a file.                                                                                          |
|  | Click the <b>Save</b> button to save your configuration settings.<br><b>Note:</b> You need to reboot for changes to take effect.                     |
|  | Click on the <b>Reboot</b> button to reboot the system.                                                                                              |

Table 2-6. Home Page Overview (continued)

| Web Page Item                                                                     | Description                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | Click on the <b>Toggle Help</b> button to see a short description of some of the web page items. First click on the <b>Toggle Help</b> 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** The user name and password will be saved immediately, but the user will not be prompted to enter them until there is a reboot. It is advisable to restart the web browser after this change.

## 2.4.5 Configure the Device

1. Click the **Device** menu button to open the **Device** page. See [Figure 2-15](#).

Figure 2-15. Device Configuration Page

HomeDeviceSecurityNetworkSIPSensorAudiofilesEventsDSRAutoprovFirmware

CyberData Security Keypad

Clock Settings

Set Time with NTP server on boot: ☒

NTP Server:

Posix Timezone String (see manual):

Periodically sync time with server: ☒

Time update period (in hours):

Current Time: 14:05:50

Relay Settings

Activate Relay with DTMF code: ☒

Relay Pulse Code:

Relay Pulse Duration (in seconds):

Relay Activation Code:

Relay Deactivation Code:

Misc Settings

Device Name:

Keypad Brightness (0-255):

Disable HTTPS (NOT recommended): ☐

SaveReboot

Test RelayToggle Help

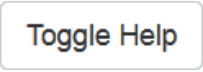
2. On the **Device** page, you may enter values for the parameters indicated in [Table 2-7](#).

**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. Device Configuration Parameters**

| Web Page Item                        | Description                                                                                                                                                                                                                                                                                  |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Clock Settings</b>                |                                                                                                                                                                                                                                                                                              |
| Set Time with NTP Server on boot ?   | When selected, the time is set with an external NTP server when the device restarts.                                                                                                                                                                                                         |
| 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.                                                                                                       |
| Posix Timezone String ?              | See <a href="#">Section 2.4.5.1, "Time Zone Strings"</a> for information about how to use the Posix Timezone String to specify time zone and daylight savings time where applicable. Enter up to 63 characters.                                                                              |
| Periodically sync time with server ? | When selected, the time is periodically updated with the NTP server at the configured interval below.                                                                                                                                                                                        |
| Time update period (in hours) ?      | The time interval after which the device will contact the NTP server to update the time. Enter up to 4 digits.                                                                                                                                                                               |
| Current Time                         | Allows you to input the current time. (6 character limit)                                                                                                                                                                                                                                    |
| <b>Relay Settings</b>                |                                                                                                                                                                                                                                                                                              |
| Activate Relay with DTMF Code ?      | Activates the relay when the DTMF Activation Code is entered on the phone during a SIP call with the device. RFC2833 DTMF payload types are supported.                                                                                                                                       |
| Relay Pulse Code ?                   | DTMF code used to pulse the relay when entered on a phone during a SIP call with the device. Relay will activate for Relay Pulse Duration seconds then deactivate. Activate Relay with DTMF Code must be enabled. Enter up to 25 digits (* and # are supported).                             |
| Relay Pulse Duration (in seconds) ?  | The length of time (in seconds) during which the relay will be activated when the DTMF Relay Activation Code is detected. Enter up to 5 digits.                                                                                                                                              |
| Relay Activation Code ?              | Activation code used to activate the relay when entered on a phone during a SIP call with the device. Relay will be active indefinitely, or until the DTMF Relay Deactivation code is entered. Activate Relay with DTMF Code must be enabled. Enter up to 25 digits (* and # are supported). |
| Relay Deactivation Code ?            | Code used to deactivate the relay when entered on a phone during a SIP call with the device. Activate Relay with DTMF Code must be enabled. Enter up to 25 digits (* and # are supported).                                                                                                   |
| <b>Misc Settings</b>                 |                                                                                                                                                                                                                                                                                              |
| Device Name ?                        | Type the device name. Enter up to 25 characters.                                                                                                                                                                                                                                             |
| Keypad Brightness (0-255) ?          | The desired keypad brightness level. Acceptable values are 0-255, where 0 is the dimmest and 255 is the brightest. Enter up to three digits.                                                                                                                                                 |

Table 2-7. Device Configuration Parameters (continued)

| Web Page Item                                                                     | Description                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Disable HTTPS (NOT recommended) ?                                                 | Disables the encrypted connection to the webpage. We do not recommend disabling HTTPS for security reasons.                                                                                                                                                                                                                                 |
|  | Click on the <b>Test Relay</b> button to do a relay test.                                                                                                                                                                                                                                                                                   |
|  | Click the <b>Save</b> button to save your configuration settings.<br><b>Note:</b> You need to reboot for changes to take effect.                                                                                                                                                                                                            |
|  | Click on the <b>Reboot</b> button to reboot the system.                                                                                                                                                                                                                                                                                     |
|  | Click on the <b>Toggle Help</b> button to see a short description of some of the web page items. First click on the <b>Toggle Help</b> 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** You must click on the **Save** button and then the **Reboot** button for the changes to take effect.

**Note** The **NTP Server** setting needs to be restarted to spawn NTP or to change the server. Syncing and changing the **Time update period (in hours)** setting does not require a reboot for the changes to take effect.

**Note** None of the **Relay Settings** require a reboot for the changes to take effect.

**Note** The **Disable HTTPS (NOT recommended)** setting requires a reboot for the changes to take effect.

### 2.4.5.1 Time Zone Strings

The posix time zone string tells the internal date and time utilities how to handle daylight savings time for different time zones. [Table 2-8](#) shows some common strings.

**Table 2-8. Common Time Zone Strings**

| Time Zone                    | Time Zone String                       |
|------------------------------|----------------------------------------|
| US Pacific time              | PST8PDT,M3.2.0/2:00:00,M11.1.0/2:00:00 |
| US Mountain time             | MST7MDT,M3.2.0/2:00:00,M11.1.0/2:00:00 |
| US Eastern Time              | EST5EDT,M3.2.0/2:00:00,M11.1.0/2:00:00 |
| Phoenix Arizona <sup>a</sup> | MST7                                   |
| US Central Time              | CST6DST,M3.2.0/2:00:00,M11.1.0/2:00:00 |

a. Phoenix, Arizona does not use daylight savings time.

[Table 2-9](#) shows a breakdown of the parts that constitute the following time zone string:

- ***CST6DST,M3.2.0/2:00:00,M11.1.0/2:00:00***

**Table 2-9. Time Zone String Parts**

| Time Zone String Part | Meaning                                                                          |
|-----------------------|----------------------------------------------------------------------------------|
| CST6CDT               | The time zone offset from GMT and three character identifiers for the time zone. |
| CST                   | Central Standard Time                                                            |
| 6                     | The (hour) offset from GMT/UTC                                                   |
| CDT                   | Central Daylight Time                                                            |
| M3.2.0/2:00:00        | The date and time when daylight savings begins.                                  |
| M3                    | The third month (March)                                                          |
| .2                    | The 2nd occurrence of the day (next item) in the month                           |
| .0                    | Sunday                                                                           |
| /2:00:00              | Time of day to change                                                            |
| M11.1.0/2:00:00       | The date and time when daylight savings ends.                                    |
| M11                   | The eleventh month (November)                                                    |
| .1                    | The 1st occurrence of the day (next item) in the month                           |
| .0                    | Sunday                                                                           |
| /2:00:00              | Time of day to change                                                            |

Time Zone String  
Examples

Table 2-10 has some more examples of time zone strings.

**Table 2-10. Time Zone String Examples**

| Time Zone           | Time Zone String                  |
|---------------------|-----------------------------------|
| Tokyo <sup>a</sup>  | IST-9                             |
| Berlin <sup>b</sup> | CET-1MET,M3.5.0/1:00,M10.5.0/1:00 |

a. Tokyo does not use daylight savings time.

b. For Berlin, daylight savings time starts on the last Sunday in March at 01:00 UTC, and ends on the last Sunday in October at 01:00 UTC, and is one hour ahead of UTC.

**Time Zone Identifier** A user-definable three or four character time zone identifier (such as PST, EDT, IST, MUT, etc) is needed at the beginning of the posix time zone string to properly set the time. However, the specific letters or numbers used for the time zone identifier are not important and can be any three or four letter or number combination that is chosen by the user. However, the time zone identifier cannot be blank.

**Figure 2-16. Three or Four Character Time Zone Identifier**

You can also use the following URL when a certain time zone applies daylight savings time:

<http://www.timeanddate.com/time/dst/2011.html>

World GMT Table

Table 2-11 has information about the GMT time in various time zones.

**Table 2-11. World GMT Table**

| Time Zone | City or Area Zone Crosses   |
|-----------|-----------------------------|
| GMT-12    | Eniwetok                    |
| GMT-11    | Samoa                       |
| GMT-10    | Hawaii                      |
| GMT-9     | Alaska                      |
| GMT-8     | PST, Pacific US             |
| GMT-7     | MST, Mountain US            |
| GMT-6     | CST, Central US             |
| GMT-5     | EST, Eastern US             |
| GMT-4     | Atlantic, Canada            |
| GMT-3     | Brazilia, Buenos Aries      |
| GMT-2     | Mid-Atlantic                |
| GMT-1     | Cape Verdes                 |
| GMT       | Greenwich Mean Time, Dublin |
| GMT+1     | Berlin, Rome                |
| GMT+2     | Israel, Cairo               |
| GMT+3     | Moscow, Kuwait              |
| GMT+4     | Abu Dhabi, Muscat           |

**Table 2-11. World GMT Table (continued)**

| <b>Time Zone</b> | <b>City or Area Zone Crosses</b> |
|------------------|----------------------------------|
| GMT+5            | Islamabad, Karachi               |
| GMT+6            | Almaty, Dhaka                    |
| GMT+7            | Bangkok, Jakarta                 |
| GMT+8            | Hong Kong, Beijing               |
| GMT+9            | Tokyo, Osaka                     |
| GMT+10           | Sydney, Melbourne, Guam          |
| GMT+11           | Magadan, Solomon Is.             |
| GMT+12           | Fiji, Wellington, Auckland       |

## 2.4.6 Configure the Security

1. Click the **Security** menu button to open the **Security** page. See [Figure 2-15](#).

Figure 2-17. Security Configuration Page

HomeDeviceSecurityNetworkSIPSensorAudiofilesEventsDSRAutoprovFirmware

# CyberData Security Keypad

### Security Configuration

| Name      | Code    | Valid From | Valid To | Blacklist |      |        |
|-----------|---------|------------|----------|-----------|------|--------|
| Jason     | 123456  | Mon12:00   | Mon13:00 | no        | Edit | Delete |
| Emma      | 21654   | All        | All      | no        | Edit | Delete |
| James     | 3214789 | Wed        | Wed      | no        | Edit | Delete |
| Mary      | 47185   | Wdy9:00    | Wdy18:00 | no        | Edit | Delete |
| John      | 54123   | Wnd        | Wnd      | no        | Edit | Delete |
| Patricia  | 528749  | Mon12:00   | Thu16:00 | no        | Edit | Delete |
| Robert    | 775214  | All        | All      | no        | Edit | Delete |
| Jennifer  | 81234   | Wnd12:00   | Wnd16:00 | yes       | Edit | Delete |
| Michael   | 998521  | Wdy        | Wdy      | no        | Edit | Delete |
| Elizabeth | 101010  | Mon10:00   | Thu10:00 | no        | Edit | Delete |
| William   | 19875   | Wnd        | Wnd      | no        | Edit | Delete |
| Linda     | 1212456 | Fri12:00   | Mon12:00 | no        | Edit | Delete |
| David     | 130905  | All        | All      | no        | Edit | Delete |
| Barbara   | 87254   | Mon08:30   | Sat18:00 | no        | Edit | Delete |
| Richard   | 35746   | Mon05:00   | Sat17:00 | no        | Edit | Delete |
| Susan     | 090516  | All        | All      | no        | Edit | Delete |
|           |         |            |          |           |      | New    |

### Relay Settings

Activate Relay on Valid Entry ☒

Activate DSR on Valid Entry ☐

Relay Timeout (seconds)

### Buzzer Settings

Buzz while Relay Active ☐

Buzz on Invalid Code Entry ☒

Buzz on Keypad Button Press ☐

### Sensor Settings

Buzz on Door Open Timeout: ☐

Door Sensor Normally Closed: ☐ Yes ☐ No

Sensor Open Timeout (in seconds):

DSR Open Timeout (in seconds):

### Blacklist Actions

Play Message to SIP Extension ☐

Dial Out SIP Extension

Dial Out SIP ID

Repeat SIP Message

Multicast Audio Message ☐

Multicast Address

Multicast Port

Times to Play Multicast Message

### Security log

2017-09-05 15:07:08 Deactivating the local relay after timeout

2017-09-05 15:07:01 Security code for Robert activating the local relay

2017-09-05 15:07:01 Checking security code 775214

2017-09-05 15:06:49 Bad security code

2017-09-05 15:06:49 Checking security code 11512

2017-09-05 15:06:35 Security code match for Jennifer blacklisted!

2017-09-05 15:06:35 Checking security code 81234

2017-09-05 15:06:31 Deactivating the local relay after timeout

2017-09-05 15:06:24 Security code for Barbara activating the local relay

2017-09-05 15:06:24 Checking security code 87254

Get Security Log

Clear Security Log

Refresh Log

Save

Reboot

Toggle Help

2. On the **Security** page, you may 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. Security Configuration Parameters**

| Web Page Item                                                                                                                                                                | Description                                                                                                                                                                                                                                                    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Security Configuration (Record)</b>                                                                                                                                       |                                                                                                                                                                                                                                                                |
| Name ?                                                                                                                                                                       | Displays the name associated with this security record.                                                                                                                                                                                                        |
| Code ?                                                                                                                                                                       | Displays the security code associated with this security record.                                                                                                                                                                                               |
| Valid From ?                                                                                                                                                                 | See <a href="#">Section 2.4.6.2, "The "Valid From" and "Valid To" Settings"</a> .                                                                                                                                                                              |
| Valid To ?                                                                                                                                                                   | See <a href="#">Section 2.4.6.2, "The "Valid From" and "Valid To" Settings"</a> .                                                                                                                                                                              |
| Blacklist ?                                                                                                                                                                  | Displays the Blacklisted status of this security record. Blacklist is used to deny entry to the specified security code. Entering a blacklisted code will trigger the buzzer, and can trigger a call to an extension or a multicast of a pre-recorded message. |
|                                                                                             | Opens the <a href="#">Configure Security Code Page</a> . See <a href="#">Section 2.4.6.1, "Configure the Security Code Page"</a> .                                                                                                                             |
|                                                                                             | Removes the security code record.                                                                                                                                                                                                                              |
|                                                                                           | Opens a new Configure Security Code window.                                                                                                                                                                                                                    |
| <b>Relay Settings</b>                                                                                                                                                        |                                                                                                                                                                                                                                                                |
| Activate Relay on Valid Entry ?                                                                                                                                              | Activates the relay when a valid code is entered. This would likely be used to open a door.                                                                                                                                                                    |
| Activate DSR on Valid Entry ?                                                                                                                                                | Activates the remote relay when a valid code is entered. This would likely be used to open a door.                                                                                                                                                             |
| Relay Timeout (seconds) ?                                                                                                                                                    | Specifies how many seconds the relay will be activated after a valid code entry. In a typical use case, this would specify how long the door is unlocked.                                                                                                      |
| <b>Buzzer Settings</b>                                                                                                                                                       |                                                                                                                                                                                                                                                                |
| <b>Note: The buzzer LED remains red when the door is locked, flashes green when a valid code is entered, and flashes red when an invalid or blacklisted code is entered.</b> |                                                                                                                                                                                                                                                                |
| Buzz while Relay Active ?                                                                                                                                                    | When selected, an audible buzz will indicate the relay is active.<br><br>The buzzer LED remains red when the door is locked, flashes green when a valid code is entered, and flashes red when an invalid or blacklisted code is entered.                       |
| Buzz on Invalid Code Entry ?                                                                                                                                                 | When selected, a pattern will play on the buzzer to indicate an invalid code was entered.                                                                                                                                                                      |
| Buzz on Keypad Button Press ?                                                                                                                                                | When selected, an audible buzz will play to indicate that a button has been pressed.                                                                                                                                                                           |
| <b>Sensor Settings</b>                                                                                                                                                       |                                                                                                                                                                                                                                                                |
| Buzz on Door Open Timeout ?                                                                                                                                                  | When selected, the buzzer will beep until the on board sensor is deactivated.                                                                                                                                                                                  |

**Table 2-12. Security Configuration Parameters (continued)**

| Web Page Item                      | Description                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Door Sensor Normally Closed ?      | Select the inactive state of the door sensor. The door sensor is also known as the Sense Input on the device's terminal block.                                                                                                                                                                                                              |
| Sensor Open Timeout (in seconds) ? | The time (in seconds) the device will wait before it triggers the buzzer when the door sensor is active.                                                                                                                                                                                                                                    |
| DSR Open Timeout (in seconds) ?    | The time (in seconds) the device will wait before it triggers the buzzer when the remote door sensor (DSR) is active.                                                                                                                                                                                                                       |
| <b>Blacklist Actions</b>           |                                                                                                                                                                                                                                                                                                                                             |
| Play Message to SIP Extension ?    | When selected, the device will make a SIP call and play the "blacklist" audio file when a blacklisted code is entered.                                                                                                                                                                                                                      |
| Dial Out SIP Extension ?           | The extension that will be dialed if "Play Message to SIP Extension" is selected above. Enter up to 64 alphanumeric characters.                                                                                                                                                                                                             |
| Dial Out SIP ID ?                  | Additional caller identification string added to outbound calls. Enter up to 64 alphanumeric characters.                                                                                                                                                                                                                                    |
| Repeat SIP Message ?               | The number of times to repeat the "blacklist" audio file played during the SIP call. Enter a value between 0 and 65535. 0 will cause the message to play indefinitely, until the call is terminated.                                                                                                                                        |
| Multicast Audio Message ?          | When selected, the device will multicast the "blacklist" audio file to the specified address and port.                                                                                                                                                                                                                                      |
| Multicast Address ?                | The multicast address that the "blacklist" audiofile will be played to.                                                                                                                                                                                                                                                                     |
| Multicast Port ?                   | The multicast port that the "blacklist" audiofile will be played to.                                                                                                                                                                                                                                                                        |
| Times to Play Multicast Message ?  | The number of times the "blacklist" audio file will be played via multicast. Enter a value between 1 and 65535.                                                                                                                                                                                                                             |
| <b>Get Security Log</b>            | Downloads a file with a maximum of 3 log files, each 1 M.                                                                                                                                                                                                                                                                                   |
| <b>Clear Security Log</b>          | Clears the on screen display of the log.                                                                                                                                                                                                                                                                                                    |
| <b>Refresh Log</b>                 | Refreshes the on screen display of the log to show the most recent activity.                                                                                                                                                                                                                                                                |
| <b>Save</b>                        | Click the <b>Save</b> button to save your configuration settings.<br><b>Note:</b> You need to reboot for changes to take effect.                                                                                                                                                                                                            |
| <b>Reboot</b>                      | Click on the <b>Reboot</b> button to reboot the system.                                                                                                                                                                                                                                                                                     |
| <b>Toggle Help</b>                 | Click on the <b>Toggle Help</b> button to see a short description of some of the web page items. First click on the <b>Toggle Help</b> 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. |

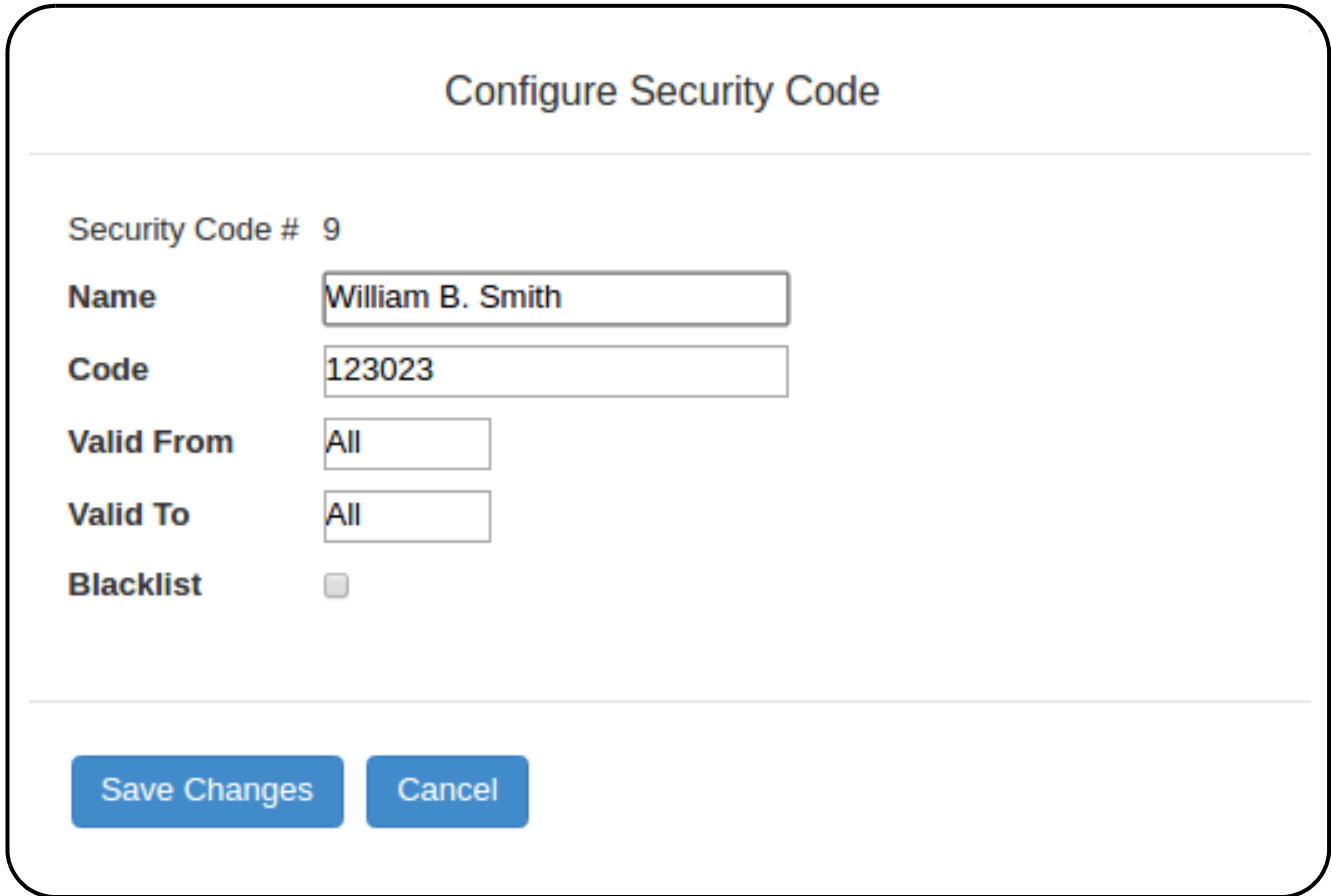
**Note** You must click on the **Save** button and then the **Reboot** button for the changes to take effect.

**Note** The device must set time with an **NTP Server** (see the **Device Configuration Page**). If an NTP server is not used, all **Valid From** and **Valid To** fields must be set to **All**.

### 2.4.6.1 Configure the Security Code Page

1. Click the **Edit** button to open the **Configure Security Code** page. See [Figure 2-18](#).

**Figure 2-18. Configure Security Code Page**



**Configure Security Code**

---

Security Code # 9

**Name** William B. Smith

**Code** 123023

**Valid From** All

**Valid To** All

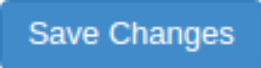
**Blacklist** ☐

---

**Save Changes** **Cancel**

2. On the **Configure Security Code** page, you may enter values for the parameters indicated in [Table 2-12](#).

**Table 2-13. Security Code Page Parameters**

| Web Page Item                                                                                | Description                                                                                                                                                                                           |
|----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Security Configuration</b>                                                                |                                                                                                                                                                                                       |
| Name        | Enter name.                                                                                                                                                                                           |
| Code        | Enter a security code, maximum 8 digits, must be distinct.                                                                                                                                            |
| Valid From  | See <a href="#">Section 2.4.6.2, "The "Valid From" and "Valid To" Settings"</a> .                                                                                                                     |
| Valid To    | See <a href="#">Section 2.4.6.2, "The "Valid From" and "Valid To" Settings"</a> .                                                                                                                     |
| Blacklist   | Blacklist is used to deny entry to the specified security code. Entering a blacklisted code will trigger the buzzer, and can trigger a call to an extension or a multicast of a pre-recorded message. |
|             | Saves the changes of the security configuration.                                                                                                                                                      |
|             | Cancels the changes of the security configuration.                                                                                                                                                    |

## 2.4.6.2 The “Valid From” and “Valid To” Settings

**ValidFrom** and **ValidTo** fields specify the day(s) a security code is valid, and, optionally the time, in 24:00 format.

The Day of the week can be **Mon**, **Tue**, **Wed**, **Thu**, **Fri**, **Sat**, **Sun**, or one of the special identifiers: **All**, **Wdy**, and **Wnd**.

**Wdy** indicates weekdays (Monday-Friday).

**Wnd** indicates weekends (Saturday-Sunday).

**All** allows entrance at all times.

A valid string consists of a day of the week or a special identifier, plus an optional time, except if using **All**, which will not use a time.

Some examples:

`<ValidFrom0>Mon9:00</ValidFrom0>`

`<ValidTo0>Fri17:00</ValidTo0>`    monday through friday 9am to 5pm

`<ValidFrom0>All</ValidFrom0>`

`<ValidTo0>All</ValidTo0>`                    all day every day

`<ValidFrom0>All</ValidFrom0>`

`<ValidTo0>All12:00</ValidTo0>`    every day till 12:00

`<ValidFrom0>Mon12:00</ValidFrom0>`

`<ValidTo0>Mon12:00</ValidTo0>`    times are inclusive - this code is only valid on monday at 12:00

`<ValidFrom0>Wdy9:00</ValidFrom0>`

`<ValidTo0>Wdy17:00</ValidTo0>`    Weekdays from 9am to 5pm

**Note**    The identifiers in **to** and **from** must match (for example, **named day/named day**, **Wdy/Wdy**, **Wdy/Wnd**, **All/All**).

## 2.4.7 Configure the Network Parameters

1. Click the **Network** menu button to open the **Network** page (Figure 2-19).

Figure 2-19. Network Configuration Page

HomeDeviceSecurityNetworkSIPSensorAudiofilesEventsDSRAutoprovFirmware

CyberData Security Keypad

Stored Network Settings

Addressing Mode: 

StaticDHCP

Hostname: 

SipDevice034ada

IP Address: 

10.10.10.10

Subnet Mask: 

255.0.0.0

Default Gateway: 

10.0.0.1

DNS Server 1: 

10.0.0.1

DNS Server 2: 

10.0.0.1

DHCP Timeout in seconds\*: 

60

\* A value of -1 will retry forever

VLAN Settings

VLAN ID (0-4095): 

0

VLAN Priority (0-7): 

0

Current Network Settings

IP Address: 10.10.1.69

Subnet Mask: 255.0.0.0

Default Gateway: 10.0.0.1

DNS Server 1: 10.0.1.56

DNS Server 2:

Save

Reboot

Toggle Help

2. On the **Network** 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. Network Configuration Parameters**

| Web Page Item                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Stored Network Settings</b>  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 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 <a href="#">Section 2.4.1, "Factory Default Settings"</a> for factory default settings. Be sure to click <b>Save</b> and <b>Reboot</b> 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| DHCP Timeout in seconds ?       | Specify the desired time-out duration (in seconds) that the device will wait for a response from the DHCP server before reverting back to the stored static IP address. The stored static IP address may be the last known IP address or the factory default address if no prior DHCP lease was established. Enter up to 8 characters. A value of -1 will retry forever.                                                                                                                                                                                                                      |
| <b>VLAN Settings</b>            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| VLAN ID (0-4095) ?              | Specify the IEEE 802.1Q VLAN ID number. Enter up to 4 digits.<br><br><b>Note:</b> 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Current Network Settings</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

Table 2-14. Network Configuration Parameters (continued)

| Web Page Item                                                                     | Description                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | Click the <b>Save</b> button to save your configuration settings.<br><b>Note:</b> You need to reboot for changes to take effect.                                                                                                                                                                                                            |
|  | Click on the <b>Reboot</b> button to reboot the system.                                                                                                                                                                                                                                                                                     |
|  | Click on the <b>Toggle Help</b> button to see a short description of some of the web page items. First click on the <b>Toggle Help</b> 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** You must click on the **Save** button and then the **Reboot** button for the changes to take effect.

## 2.4.8 Configure the SIP (Session Initiation Protocol) Parameters

1. Click on the **SIP** menu button to open the **SIP** page (Figure 2-20).

Figure 2-20. SIP Configuration Page

**Home** **Device** **Security** **Network** **SIP** **Sensor** **Audiofiles** **Events** **DSR** **Autoprov** **Firmware**

# CyberData Security Keypad

### SIP Settings

Enable SIP operation: ☒

Register with a SIP Server: ☒

Use Cisco SRST: ☐

Primary SIP Server:

Primary SIP User ID:

Primary SIP Auth ID:

Primary SIP Auth Password:

Backup SIP Server 1:

Backup SIP User ID 1:

Backup SIP Auth ID 1:

Backup SIP Auth Password 1:

Backup SIP Server 2:

Backup SIP User ID 2:

Backup SIP Auth ID 2:

Backup SIP Auth Password 2:

Remote SIP Port:

Local SIP Port:

Outbound Proxy:

Outbound Proxy Port:

Disable rport Discovery: ☐

Re-registration Interval (in seconds):

Unregister on Boot: ☐

Keep Alive Period:

### Call Disconnection

Terminate Call after delay:

### Codec Selection

Force Selected Codec: ☐

Codec:

### RTP Settings

RTP Port (even):

Jitter Buffer:

2. On the **SIP** page, 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. SIP Configuration Parameters**

| Web Page Item                | Description                                                                                                                                                                                                                                                                                                       |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SIP Settings</b>          |                                                                                                                                                                                                                                                                                                                   |
| 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.                                                                                                                                                                                                                   |
| 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.                                                                                                                     |
| 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.                                                                                                                                             |
| 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 1 ?       | 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 1 ? | Specify the Authenticate Password for the first backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.                                                                                                                                        |
| 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 2 ?       | 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 2 ?       | Specify the Authenticate ID for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.                                                                                                                                             |
| Backup SIP Auth Password 2 ? | Specify the Authenticate Password for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.                                                                                                                                       |

**Table 2-15. SIP Configuration Parameters (continued)**

| Web Page Item                                                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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.                                                                                                                                                                                                                                                                    |
| 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.                                                                                                                                                                                                                                   |
| 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.                                                                                                                                                 |
| 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.                                                                                                                                                                                                                                                                       |
| Unregister on Boot ?                                                                | When enabled, the device will send one registration with an expiry of 0 on boot.                                                                                                                                                                                                                                                                                                                                                                |
| 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.                                                                                                                                                                                                                                                                                                               |
| <b>Call Disconnection</b>                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 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.                                                                                                                                                                                                                                                                                                           |
| <b>Codec Selection</b>                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Force Selected Codec ?                                                              | When configured, this option will allow you to force the device to negotiate for the selected codec. Otherwise, the device will perform codec negotiation using the default list of supported codecs.                                                                                                                                                                                                                                           |
| Codec ?                                                                             | Select the desired codec (only one may be chosen).                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>RTP Settings</b>                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 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.                                                                                                                                                                                                                                             |
| Jitter Buffer ?                                                                     | Specify the size of the jitter buffer (in milliseconds) used for SIP calls. Valid values are 50-1000.                                                                                                                                                                                                                                                                                                                                           |
|  | Click the <b>Save</b> button to save your configuration settings.<br><b>Note:</b> You need to reboot for changes to take effect.                                                                                                                                                                                                                                                                                                                |
|  | Click on the <b>Reboot</b> button to reboot the system.                                                                                                                                                                                                                                                                                                                                                                                         |

**Table 2-15. SIP Configuration Parameters (continued)**

| Web Page Item                                                                     | Description                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | Click on the <b>Toggle Help</b> button to see a short description of some of the web page items. First click on the <b>Toggle Help</b> 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** You must click on the **Save** button and then the **Reboot** button for the changes to take effect.

**Note** The **Terminate Call After Delay** setting does not require a reboot for the changes to take effect.

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

## 2.4.9 Configure the Sensor Configuration Parameters

The door sensor (pins 5 and 6) on the header can be used to monitor a door's open or closed state. There is an option on the **Sensor** page to trigger on an open or short condition on these pins. The door sensor alarm will be activated when the **Door Open Timeout** parameter has been met.

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

Each sensor can activate the relay, or make a call to an extension and play a pre-recorded audio file.

1. Click **Sensor** menu button to open the **Sensor** page ([Figure 2-21](#)).

Figure 2-21. Sensor Configuration Page

HomeDeviceSecurityNetworkSIPSensorAudiofilesEventsDSRAutoprovFirmware

CyberData Security Keypad

Door Sensor Settings

Door Sensor Normally Closed: ☐ Yes ☒ No

Buzz on Door Open Timeout: ☐

Door Open Timeout (in seconds):

Activate Relay: ☐

Make call to extension: ☒

Dial Out Extension:

Dial Out ID:

Repeat Sensor Message:

Intrusion Sensor Settings

Activate Relay: ☐

Make call to extension: ☒

Dial Out Extension:

Dial Out ID:

Repeat Intrusion Message:

SaveRebootToggle Help

Test Door SensorTest Intrusion Sensor

2. On the **Sensor** page, enter values for the parameters indicated in [Table 2-16](#).

**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 2-16. Sensor Configuration Parameters**

| Web Page Item                    | Description                                                                                                                                                                                                               |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Door Sensor Settings</b>      |                                                                                                                                                                                                                           |
| Door Sensor Normally Closed ?    | Select the inactive state of the door sensor. The door sensor is also known as the Sense Input on the device's terminal block.                                                                                            |
| Buzz on Door Open Timeout ?      | When selected, the buzzer will beep until the on board sensor is deactivated.                                                                                                                                             |
| Door Open Timeout (in seconds) ? | The time (in seconds) the device will wait before it performs an action when the on-board door sensor is activated. The action(s) performed are based on the configured Door Sensor Settings below. Enter up to 5 digits. |
| Activate Relay ?                 | When selected, the device's on-board relay will be activated until the on-board door sensor is deactivated.                                                                                                               |
| Make call to extension ?         | When selected, the device will call an extension when the on-board door sensor is activated. Use the <b>Dial Out Extension</b> field below to specify the extension the device will call.                                 |
| Dial Out Extension ?             | Specify the extension the device will call when the on-board door sensor is activated. Enter up to 64 alphanumeric characters.                                                                                            |
| Dial Out ID ?                    | An additional Caller identification string added to outbound calls. Enter up to 64 alphanumeric characters.                                                                                                               |
| Repeat Sensor Message ?          | The number of times to repeat the audio message through the local speaker or to the remote endpoint. A value of 0 will repeat forever. Enter a value from 0-65536.                                                        |
| <b>Intrusion Sensor Settings</b> |                                                                                                                                                                                                                           |
| Activate Relay ?                 | When selected, the device's on-board relay will be activated until the intrusion sensor is deactivated.                                                                                                                   |
| Make call to extension ?         | When selected, the device will call an extension when the intrusion sensor is activated. Use the <b>Dial Out Extension</b> field below to specify the extension the device will call.                                     |
| Dial Out Extension ?             | Specify the extension the device will call when the intrusion sensor is activated. Enter up to 64 alphanumeric characters.                                                                                                |
| Dial Out ID ?                    | An additional Caller identification string added to outbound calls. Enter up to 64 alphanumeric characters.                                                                                                               |
| Repeat Intrusion Message ?       | The number of times to repeat the audio message through the local speaker or to the remote endpoint. A value of 0 will repeat forever. Enter a value from 0-65536.                                                        |
| <b>Test Door Sensor</b>          | Click the <b>Test Door Sensor</b> button to test the door sensor.                                                                                                                                                         |
| <b>Test Intrusion Sensor</b>     | Click the <b>Test Intrusion Sensor</b> button to test the Intrusion sensor.                                                                                                                                               |

Table 2-16. Sensor Configuration Parameters (continued)

| Web Page Item                                                                     | Description                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | Click the <b>Save</b> button to save your configuration settings.<br><b>Note:</b> You need to reboot for changes to take effect.                                                                                                                                                                                                            |
|  | Click on the <b>Reboot</b> button to reboot the system.                                                                                                                                                                                                                                                                                     |
|  | Click on the <b>Toggle Help</b> button to see a short description of some of the web page items. First click on the <b>Toggle Help</b> 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** You must click on the **Save** button for the changes to take effect.
- Note** None of the **Sensor Configuration Page** settings require a reboot for the changes to take effect.

## 2.4.10 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 2-22).

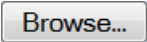
Figure 2-22. Audiofiles Configuration Page



2. On the **Audiofiles** page, enter values for the parameters indicated in Table 2-17.

**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 2-17. Audiofiles Configuration Parameters

| Web Page Item                                                                       | Description                                                                                                                                                                                                             |
|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Intrusion Sensor Triggered                                                          | Corresponds to the message “Intrusion Sensor Triggered” (24 character limit).                                                                                                                                           |
| Door Ajar                                                                           | Corresponds to the message “Door Ajar” (24 character limit).                                                                                                                                                            |
| Blacklist Message                                                                   | The audio file that will play if a blacklisted security code is entered.                                                                                                                                                |
|  | Click on the <b>Browse</b> button to navigate to and select an audio file.                                                                                                                                              |
|  | The <b>Delete</b> button will delete any user uploaded audio and restore the stock audio file.                                                                                                                          |
|  | The <b>Save</b> button will download a new user audio file to the board once you've selected the file by using the <b>Browse</b> button. The <b>Save</b> button will delete any pre-existing user-uploaded audio files. |

2.4.10.1 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 2-23](#) through [Figure 2-25](#).

Figure 2-23. Audacity 1

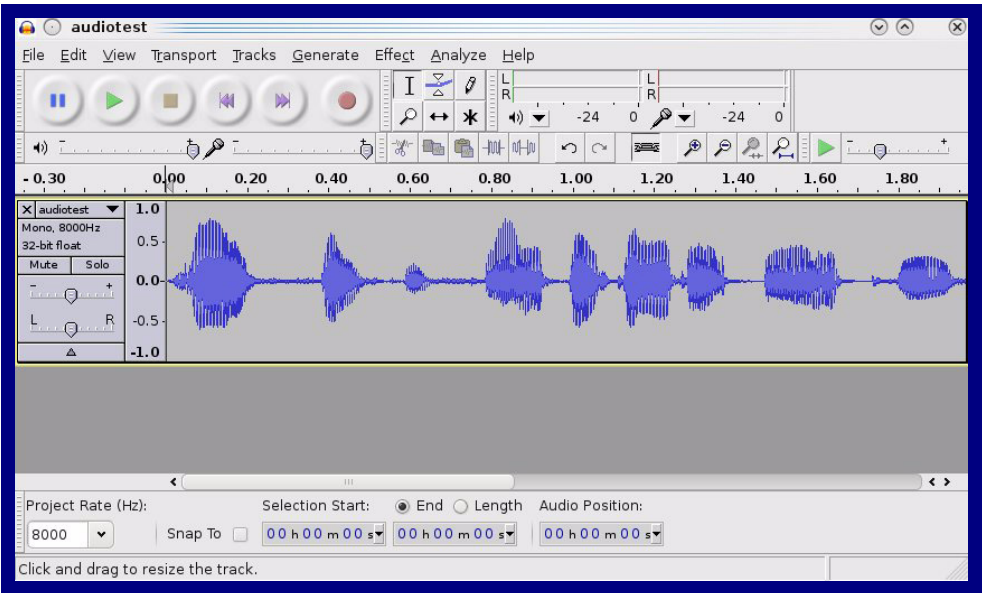
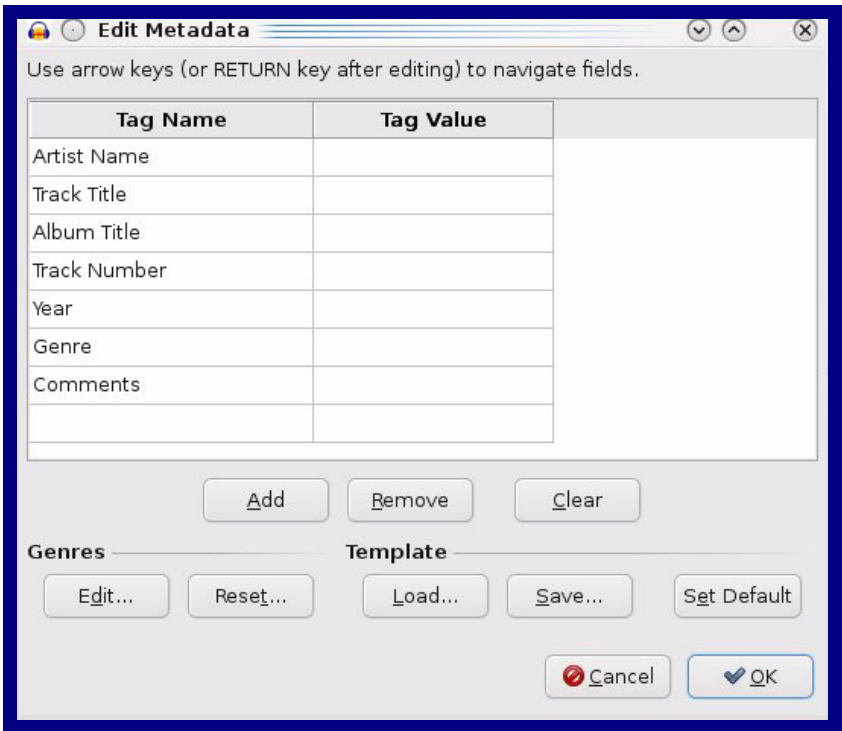


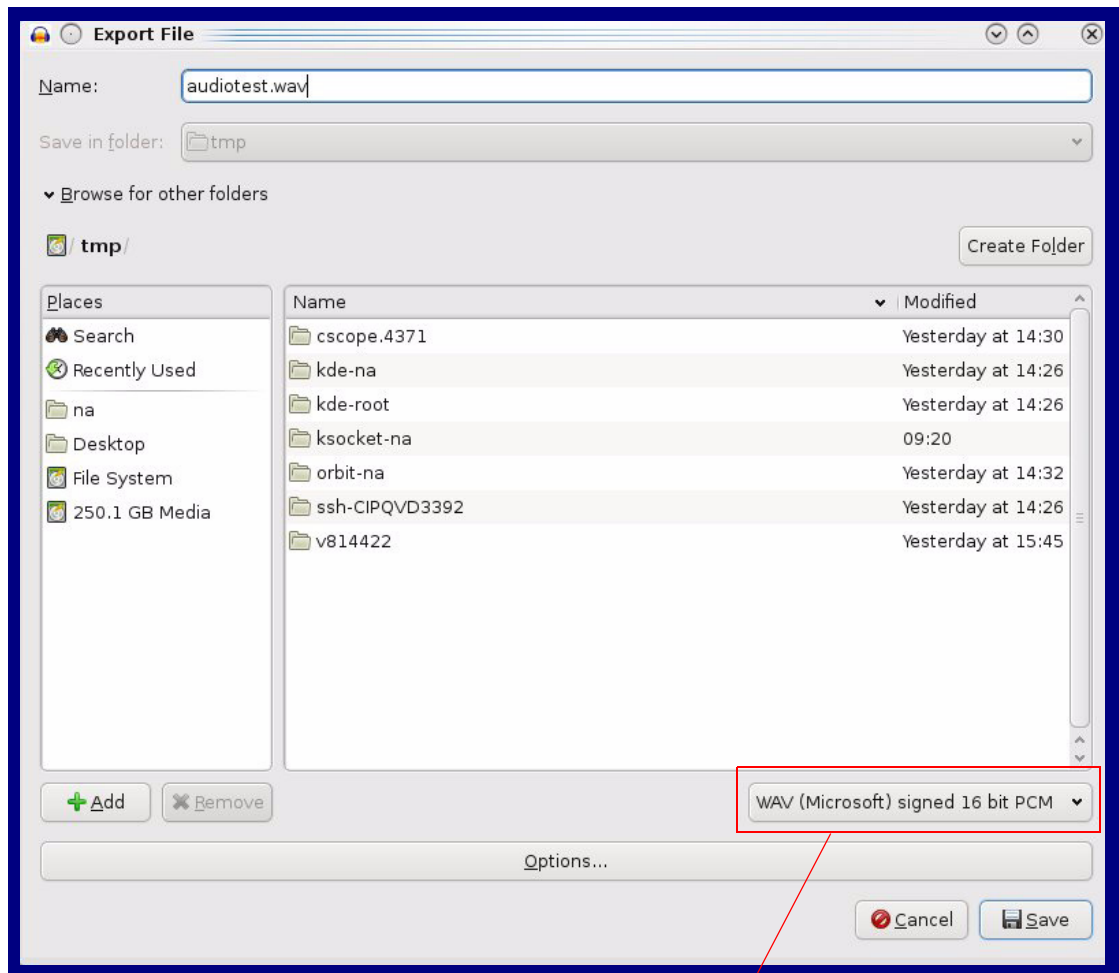
Figure 2-24. Audacity 2



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

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

**Figure 2-25. WAV (Microsoft) signed 16 bit PCM**



WAV (Microsoft) signed 16 bit PCM

### 2.4.11 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 2-26).

Figure 2-26. Event Configuration Page



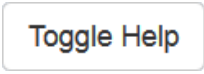
2. On the **Events** page, enter values for the parameters indicated in Table 2-18.

**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 2-18. 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. |
| <b>Events</b>                   |                                                                                                                                                                                        |
| 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 Relay Activated Events ? | When selected, the device will report relay activation.                                                                                                                                |

**Table 2-18. Events Configuration Parameters(continued)**

| Web Page Item                                                                       | Description                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable Relay Deactivated Events ?                                                   | When selected, the device will report relay deactivation.                                                                                                                                                                                                                                                                                   |
| Enable Power On Events ?                                                            | When selected, the device will report when it boots.                                                                                                                                                                                                                                                                                        |
| Enable Sensor Events ?                                                              | When selected, the device will report when the on-board sensor is activated.                                                                                                                                                                                                                                                                |
| Enable Remote Relay Events ?                                                        | When selected, the device will report when the remote relay (DSR) is activated.                                                                                                                                                                                                                                                             |
| Enable Security Events ?                                                            | When enabled, the device will report when the intrusion sensor is activated or a valid security code is entered.                                                                                                                                                                                                                            |
| 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 <b>Check All</b> to select all of the events on the page.                                                                                                                                                                                                                                                                          |
| Uncheck All                                                                         | Click on <b>Uncheck All</b> to de-select all of the events on the page.                                                                                                                                                                                                                                                                     |
| <b>Event Server</b>                                                                 |                                                                                                                                                                                                                                                                                                                                             |
| 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 <b>Save</b> button to save your configuration settings.<br><b>Note:</b> You need to reboot for changes to take effect.                                                                                                                                                                                                            |
|  | Click on the <b>Reboot</b> button to reboot the system.                                                                                                                                                                                                                                                                                     |
|  | Click on the <b>Toggle Help</b> button to see a short description of some of the web page items. First click on the <b>Toggle Help</b> 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** You must click on the **Save** button for the changes to take effect.

**Note** Enabling Event Generation or changing an **Event Server** setting requires a reboot for the changes to take effect.

**Note** Selecting particular events, **Check All**, or **Uncheck All** does not require a reboot for the changes to take effect.

### 2.4.11.1 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>
```

## 2.4.12 Configure the Door Strike Relay

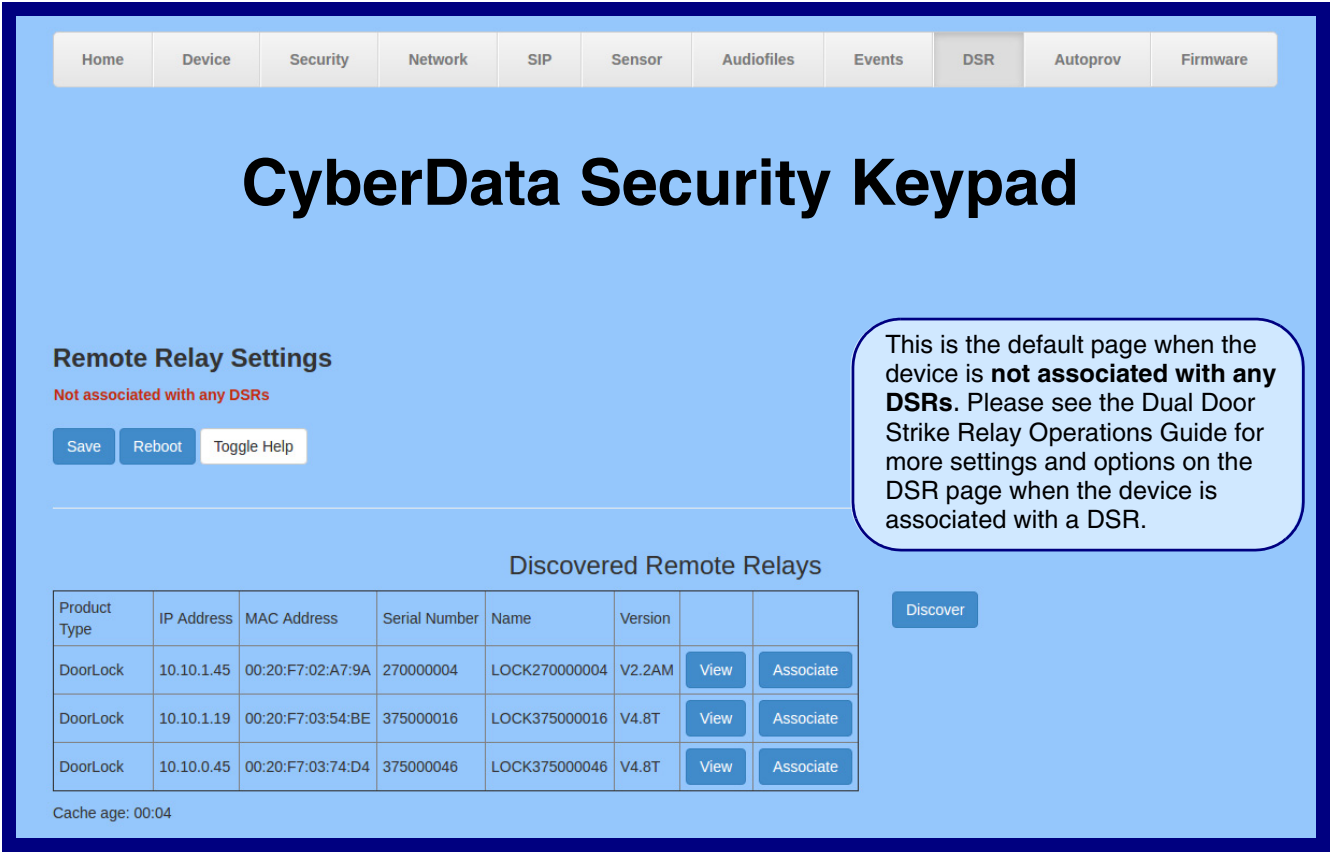
The Door Strike Relay (DSR) is a network device designed to control an electronic door strike. The DSR is meant to be used as a replacement for (or an addition to) the on-board relay. In addition to being a drop-in 12 Amp relay, the DSR can monitor and record when the door is open or closed.

The DSR can be configured to trigger in the following ways: on the entry of a DTMF code, manually through the web interface, or by using a Windows application.

This section describes operations for running firmware version 4.8 or later of the Dual Door Strike Relay. If you have an older version of the firmware, then please contact CyberData Technical Support. The version number appears in the **Discovered Remote Relays** section on the **DSR** page ([Figure 2-27](#)).

1. Click on the **DSR** menu button to open the **DSR** page ([Figure 2-27](#)).

Figure 2-27. DSR Page (not associated with any DSRs)



2. On the **DSR** page, enter values for the parameters indicated in [Table 2-19](#).

**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 2-19. DSR Configuration Parameters (not associated with any DSRs)**

| Web Page Item                   | Description                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Remote Relay Settings</b>    | The settings in this section will activate an associated door strike relay. If a door strike relay is not associated with the device, then you will only see the words <b>Not associated with any DSRs</b> .                                                                                                                                     |
| <b>Save</b>                     | Click the <b>Save</b> button to save your configuration settings.<br><b>Note:</b> You need to reboot for changes to take effect.                                                                                                                                                                                                                 |
| <b>Reboot</b>                   | Click on the <b>Reboot</b> button to reboot the system.                                                                                                                                                                                                                                                                                          |
| <b>Toggle Help</b>              | Click on the <b>Toggle Help</b> button to see a short description of some of the web page items. First click on the <b>Toggle Help</b> 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.      |
| <b>Discovered Remote Relays</b> | The <b>Discovered Remote Relays</b> section lists all of the networked door strike relays on the network. To associate your device with a door strike relay, click on the <b>Associate</b> button. This action allows the user to configure the door strike relay. Keep in mind that a device may only be associated with one door strike relay. |
| Product Type                    | Displays the product type of the remote relay.                                                                                                                                                                                                                                                                                                   |
| IP Address                      | Displays the IP address of the remote relay.                                                                                                                                                                                                                                                                                                     |
| MAC Address                     | Displays the MAC address of the remote relay.                                                                                                                                                                                                                                                                                                    |
| Serial Number                   | Displays the serial number of the remote relay.                                                                                                                                                                                                                                                                                                  |
| Name                            | Displays the name of the remote relay.                                                                                                                                                                                                                                                                                                           |
| Version                         | Displays the version of the remote relay.                                                                                                                                                                                                                                                                                                        |
| <b>Discover</b>                 | Use this button to search for and find any remote relays that are available on the network.                                                                                                                                                                                                                                                      |
| <b>View</b>                     | Use this button to view the settings of a remote relay that has been “discovered” after pressing the <b>Discover</b> button.                                                                                                                                                                                                                     |
| <b>Associate</b>                | Use this button to associate the remote relay with the device. Only one relay may be associated with a device.                                                                                                                                                                                                                                   |
| <b>Disassociate</b>             | Use this button to disassociate the remote relay from the device. Only one relay may be associated with a device. This button is only available when a relay is associated with a device.                                                                                                                                                        |

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

**Note** Associating a DSR does not require a reboot. However, you should reboot the device after disassociating a DSR.

### 2.4.13 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 2-28](#).

Figure 2-28. Autoprovisioning Page

HomeDeviceSecurityNetworkSIPSensorAudiofilesEventsDSRAutoprovFirmware

CyberData Security Keypad

Disable Autoprovisioning:☐

Autoprovisioning Server:

Autoprovisioning Filename:

Use tftp:☐

Username:

Password:

Autoprovisioning autoupdate (in minutes):

Autoprovision at time (HHMMSS):

Autoprovision when idle (in minutes > 10):

See the manual to learn how to use autoprovisioning to configure your device.

Autoprovisioning happens on boot.

The device will first look for a configured server address and filename.

If these haven't been configured, it will look for an autoprovisioning server in your list of DHCP options and try to download '0020f7034ada.xml' and if this fails, '000000cd.xml'.

SaveRebootToggle Help

Download Template

Autoprovisioning log

47:43 Autoprovisioning Device...

47:43 Autoprov found option 43 in DHCP server="http://10.0.0.242"

47:43 Autoprov looking for 0020f7034ada.xml at http://10.0.0.242

47:43 Got autoprov file. Parsing "0020f7034ada.xml"

47:44 Autoprov found option 72 in DHCP server="10.0.0.252"

47:44 Autoprov looking for 0020f7034ada.xml at 10.0.0.252

47:44 Autoprov: didn't find autoprov file

47:44 Autoprov looking for 000000cd.xml at 10.0.0.252

47:44 Autoprov: didn't find autoprov file

47:44 Failed to fetch autoprov file

2. On the **Autoprovisioning** page, you may enter values for the parameters indicated in [Table 2-20](#).

**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 2-20. Autoprovisioning Configuration Parameters**

| Web Page Item                                                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Disable Autoprovisioning ?                                                          | Prevent the device from automatically trying to download a configuration file. See <a href="#">Section 2.4.13.1, "Autoprovisioning"</a> for more information.                                                                                                                                                                                                                                                                                                                                                         |
| Autoprovisioning Server ?                                                           | Enter the IPv4 address of the provisioning server in dotted decimal notation.                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Autoprovisioning Filename ?                                                         | <p>The autoprovisioning filename is the configuration filename. The default autoprovisioning filename is in the format of <b>&lt;mac address&gt;.xml</b>.</p> <p>Supported filename extensions are .txt, and .xml. The current filename is denoted by an asterisk at the bottom of the <a href="#">Autoprovisioning Page</a>. Enter up to 256 characters.</p> <p>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.</p> |
| Use tftp ?                                                                          | The device will use TFTP (instead of http) to download autoprovisioning files.                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 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) ?                                          | <p>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.</p> <p><b>Note:</b> To use the auto update options, enable the <a href="#">Set Time with NTP Server on boot</a> setting on the <a href="#">Device Configuration Page</a> (see <a href="#">Table 2-7</a>).</p>                                                                                                                                  |
| Autoprovision at time (HHMMSS) ?                                                    | <p>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.</p> <p><b>Note:</b> To use the auto update options, enable the <a href="#">Set Time with NTP Server on boot</a> setting on the <a href="#">Device Configuration Page</a> (see <a href="#">Table 2-7</a>).</p>                                                                                                                        |
| Autoprovision when idle (in minutes > 10) ?                                         | <p>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.</p> <p><b>Note:</b> To use the auto update options, enable the <a href="#">Set Time with NTP Server on boot</a> setting on the <a href="#">Device Configuration Page</a> (see <a href="#">Table 2-7</a>).</p>                                                                                                                           |
|  | <p>Click the <b>Save</b> button to save your configuration settings.</p> <p><b>Note:</b> You need to reboot for changes to take effect.</p>                                                                                                                                                                                                                                                                                                                                                                           |

Table 2-20. Autoprovisioning Configuration Parameters (continued)

| Web Page Item                                                                     | Description                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | Click on the <b>Reboot</b> button to reboot the system.                                                                                                                                                                                                                                                                                     |
|  | Click on the <b>Toggle Help</b> button to see a short description of some of the web page items. First click on the <b>Toggle Help</b> 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 <b>Download Template</b> button to create an autoprovisioning file for the device. See <a href="#">Section 2.4.13.3, "Download Template Button"</a>                                                                                                                                                                               |
| 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 and then the **Reboot** button for the changes to take effect.

### 2.4.13.1 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 2.4.13.2, "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 2-20](#)). This file contains every configuration option that can be set on the board.

2.4.13.1 Autoprovisioning files can contain the whole configuration or a subset of this file, but the order must not be changed. 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 SIP 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](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 2-21. Autoprovisioning File Name

| Autoprovisioning<br>Filename | Autoprovisioning<br>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  
Firmware Updates

```
<FirmwareSettings>
  <FirmwareFile>505-ulmage-ceilingspeaker</FirmwareFile>
  <FirmwareServer>10.0.1.3</FirmwareServer>
  <OutdoorIntercom30>firmware_file_v9.3.0</OutdoorIntercom30>
  <OutdoorIntercom31>firmware_file_v10.3.0</OutdoorIntercom31>
  <CallButton31>firmware_file_v10.3.0</CallButton31>
</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://autoprotest.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 autoprovisioning 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 autoprovisioning 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 autoprovisioned 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 autoprovisioning 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 autoprovisioning 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 Configuration** page or by changing the autoprovisioning file with “**default**” set as the file name.

### 2.4.13.2 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; }
```

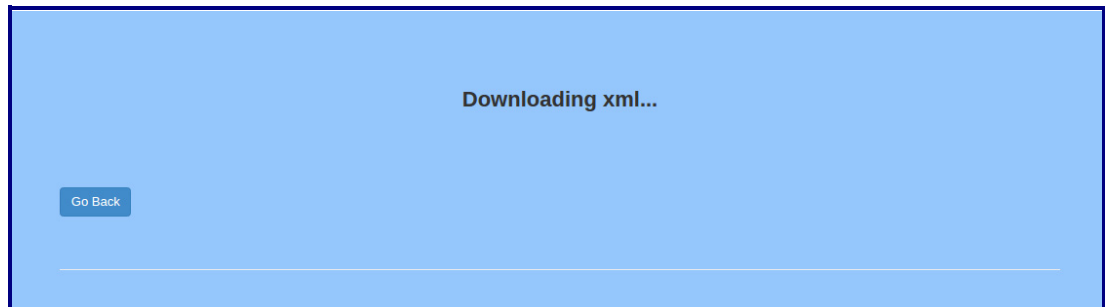
### 2.4.13.3 Download Template Button

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

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

1. On the **Autoprovisioning** page, click on the **Download Template** button.
2. You will see a window that displays the words **Downloading xml...** (Figure 2-29). The template that downloads is the basis for the default configuration settings for your unit. The file will be saved in the location specified in your web browser for downloaded files.

**Figure 2-29. Configuration File**



3. At this point, you can open and edit the autoprovisioning template to change the configuration settings in the template for the unit. Save this file as the mac address of your device .xml to use DHCP autoprovisioning options.
4. You can then upload the autoprovisioning file to a TFTP or HTTP server where the file can be loaded onto other devices.

---

## 2.5 Upgrade the Firmware and Reboot the Intercom



### Caution

**Equipment Hazard:** Devices with a serial number that begins with 4331xxxxx can only run firmware versions 10.0.0 or later.

---

### 2.5.1 Downloading the Firmware

To download the firmware to your computer:

1. Download the latest firmware file from the **Downloads** tab at the following webpage:  
<http://www.cyberdata.net/voip/011433/>
2. Unzip the firmware version file. This file may contain the following:
  - Firmware file
  - Release notes
3. Log in to the Intercom home page as instructed in [Section 2.4.4, "Log in to the Configuration Home Page"](#).

4. Click on the **Firmware** menu button to open the **Firmware** page. See [Figure 2-30](#).



**Caution**  
***Equipment Hazard:*** CyberData strongly recommends that you first reboot the device before attempting to upgrade the firmware of the device. See [Section 2.5.2, "Reboot the Device"](#).

Figure 2-30. Firmware Page



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

**Note** Do not reboot the device after clicking on the **Upload** button.

**Note** This starts the upgrade process. Once the Intercom has uploaded the file, the **Uploading Firmware** countdown page appears, indicating that the firmware is being written to flash. The Intercom will automatically reboot when the upload is complete. When the countdown finishes, the **Firmware** page will refresh. The uploaded firmware filename should be displayed in the system configuration (indicating a successful upload and reboot).



**Caution**  
***Equipment Hazard:*** Restore the factory defaults after upgrading the firmware. See [Section 2.5.2, "Reboot the Device"](#).

8. [Table 2-22](#) shows the web page items on the **Firmware** page.

Table 2-22. Firmware Parameters

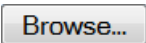
| Web Page Item                                                                       | Description                                                                                            |
|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| Current Firmware Version                                                            | Shows the current firmware version.                                                                    |
|  | Use the <b>Browse</b> button to navigate to the location of the firmware file that you want to upload. |

Table 2-22. Firmware Parameters (continued)

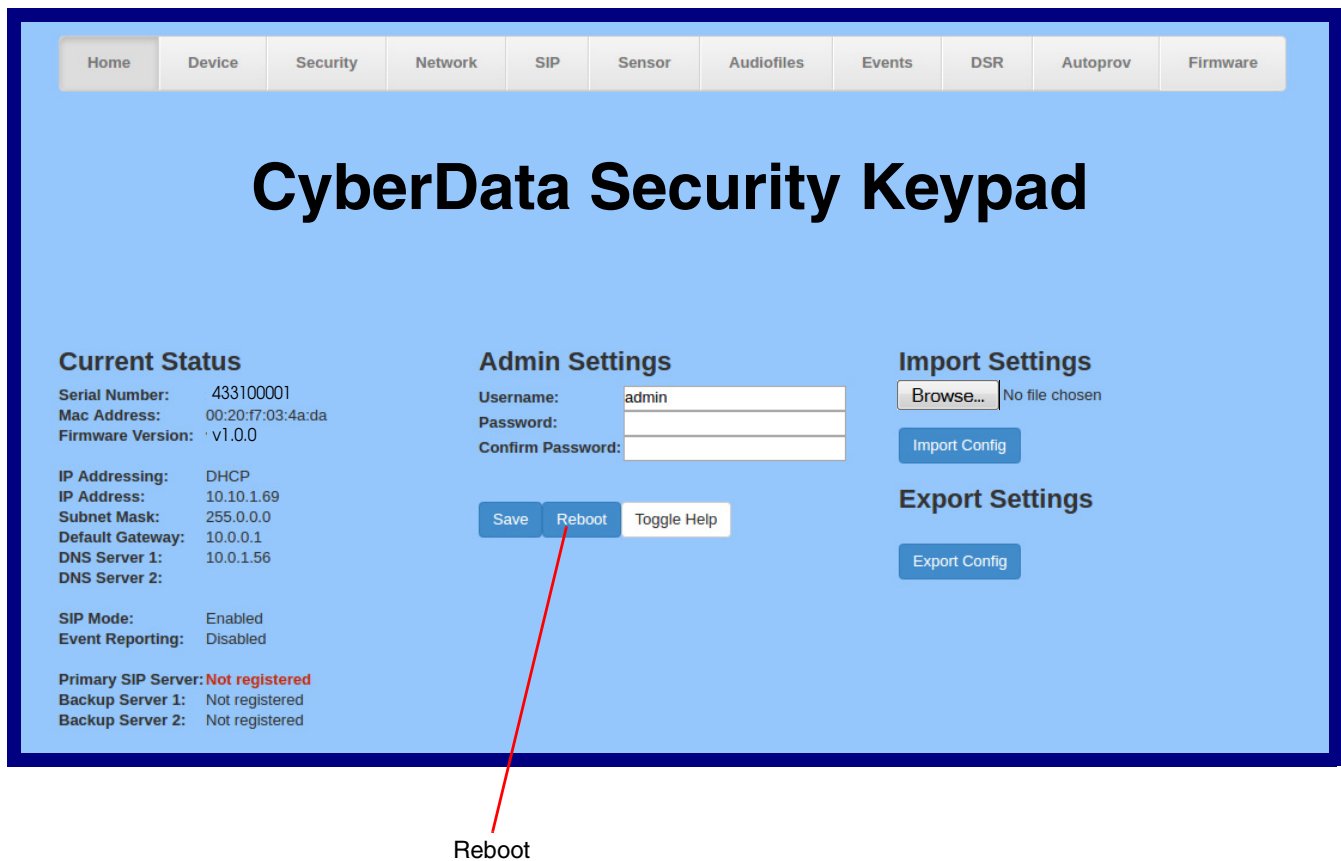
| Web Page Item                                                                     | Description                                                                                            |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
|  | Click on the <b>Upload</b> button to automatically upload the selected firmware and reboot the system. |

## 2.5.2 Reboot the Device

To reboot a Intercom, log in to the web page as instructed in [Section 2.4.4, "Log in to the Configuration Home Page"](#).

1. Click on the **Reboot** button on the **Home** page ([Figure 2-31](#)). A normal restart will occur.

Figure 2-31. Home Page



## 2.6 Command Interface

Some functions on the device can be activated using simple POST commands to the web interface. The examples in [Table 2-23](#) 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

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

**Table 2-23. Command Interface Post Commands**

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

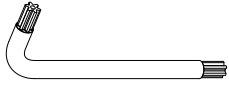
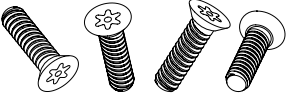
a. Type and enter all of each http POST command on one line.

# Appendix A: Mounting the Intercom

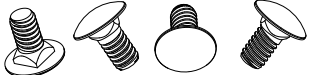
## A.1 Mounting Components

Before you mount the Intercom, make sure that you have received all the parts for each Intercom. Refer to the following tables.

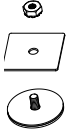
**Table A-1. Mounting Components (Part of the Accessory Kit)**

| Quantity | Part Name           | Illustration                                                                        |
|----------|---------------------|-------------------------------------------------------------------------------------|
| 1        | T-15H Torx Key      |  |
| 4        | Security Torx Screw |  |

**Table A-2. Optional Accessories (for gooseneck mounting)**

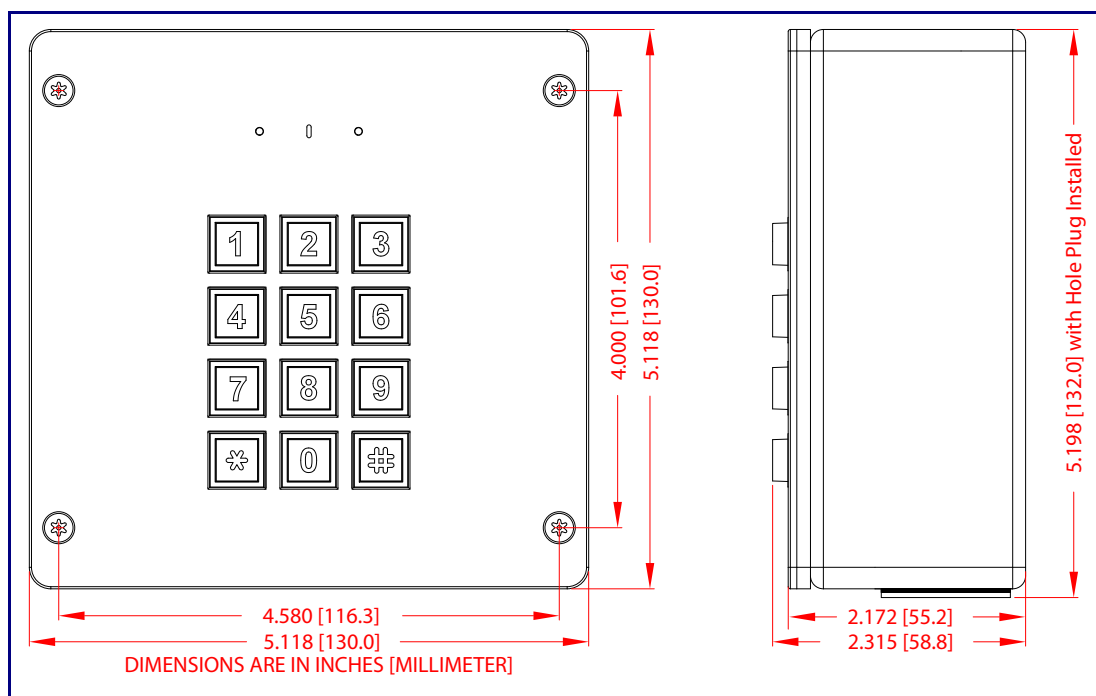
| Quantity | Part Name             | Illustration                                                                          |
|----------|-----------------------|---------------------------------------------------------------------------------------|
| 4        | Carriage bolt nuts    |   |
| 4        | Carriage bolts        |  |
| 4        | Carriage bolt washers |  |

**Table A-3. Optional Accessories**

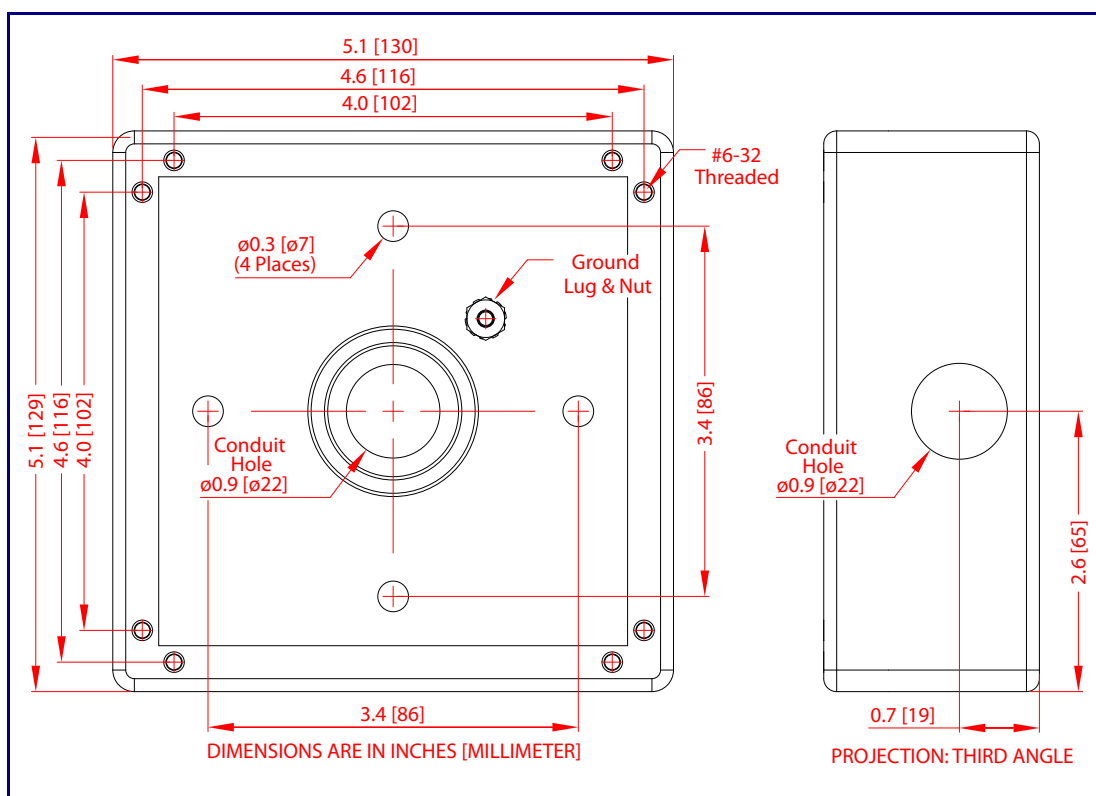
| Quantity | Part Name                                  | Illustration                                                                          |
|----------|--------------------------------------------|---------------------------------------------------------------------------------------|
| 1        | Spacer for half-inch set conduit connector |  |
| 1        | 531085B hole plug assembly                 |  |

## A.2 Dimensions

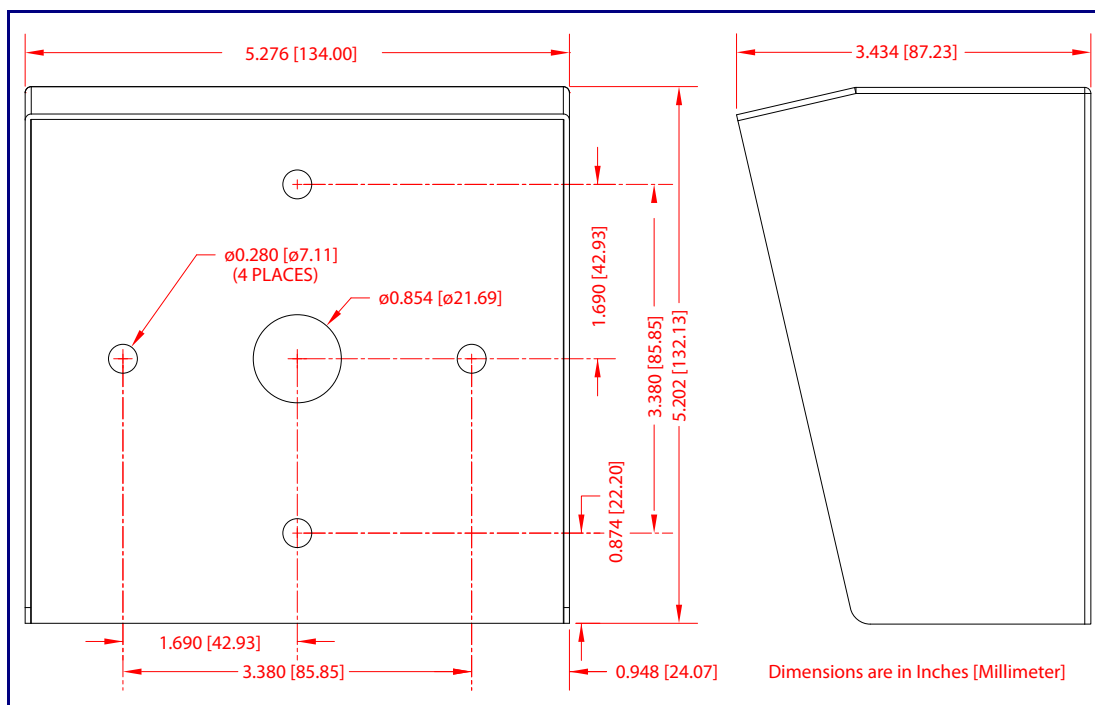
**Figure A-1. Unit Dimensions—Front and Side View**



**Figure A-2. Unit Dimensions—Rear View with Mounting Hole Locations**



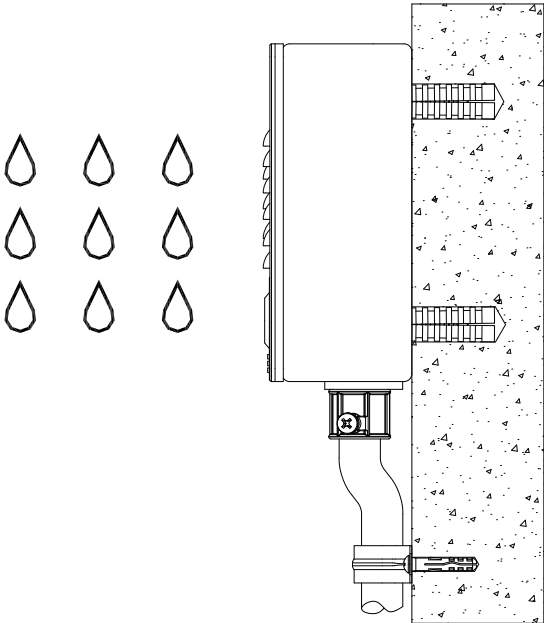
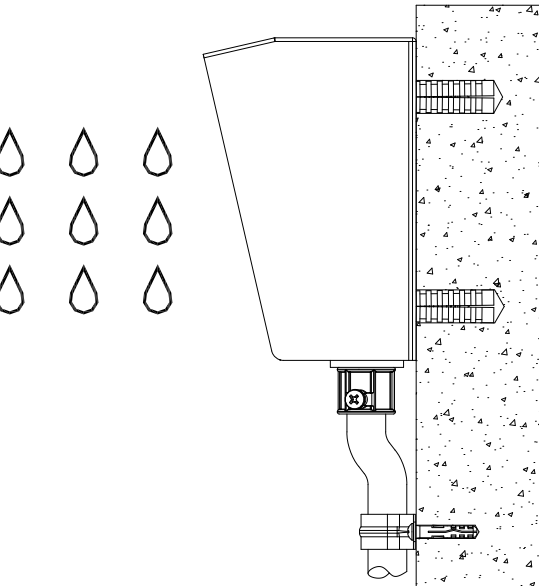
**Figure A-3. Shroud Dimensions—Front and Side View with Mounting Hole Locations**



# A.3 Overview of Installation Types

An overview of the installation types and the required components are provided in [Table A-4](#).

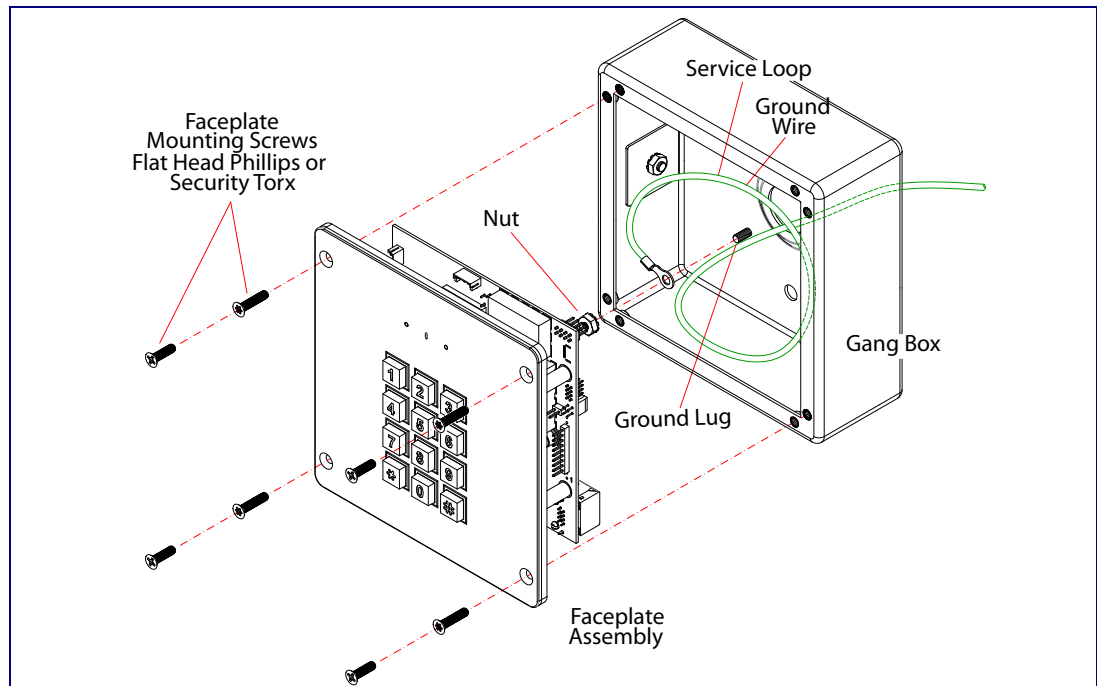
**Table A-4. Overview of Installation Types**

| Installation Type                                                                   | What You Need                                            |
|-------------------------------------------------------------------------------------|----------------------------------------------------------|
| Outdoor, on surface                                                                 | 011433 Device only                                       |
|   |                                                          |
| Outdoor, on surface with shroud (increased resistance)                              | 011433 Device<br>011188 Weather Shroud (sold separately) |
|  |                                                          |

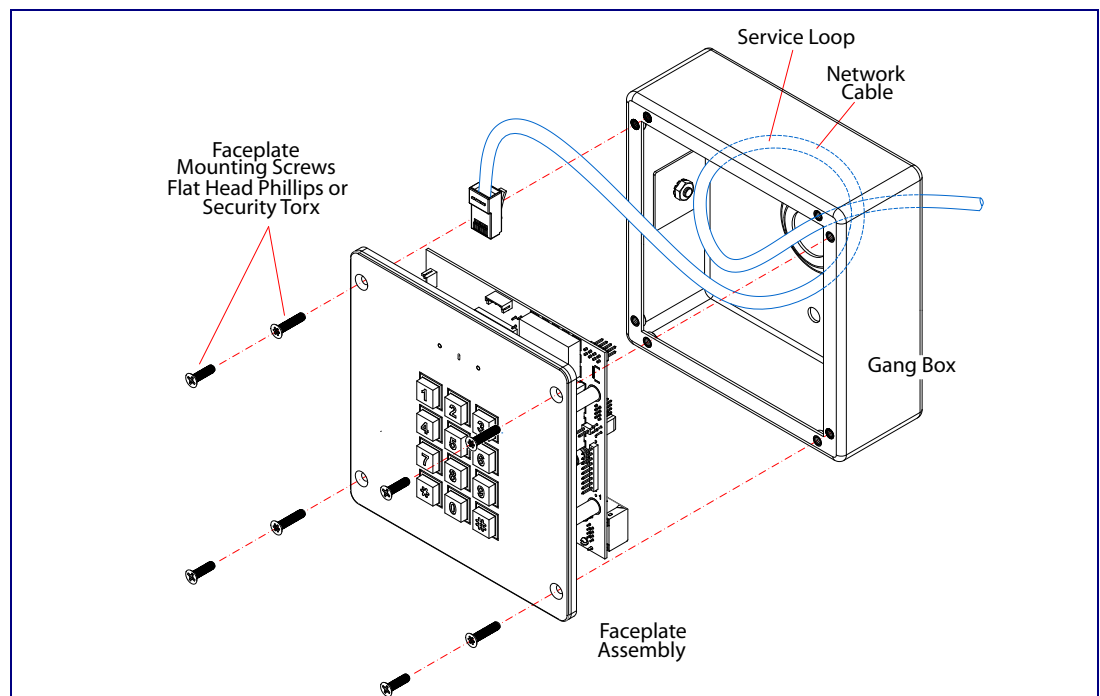
## A.4 Service Loop Cable Routing

Figure A-4 and Figure A-5 illustrate a service loop cable routing option for the Secure Access Control Keypad.

**Figure A-4. Ground Cable Service Loop Routing**



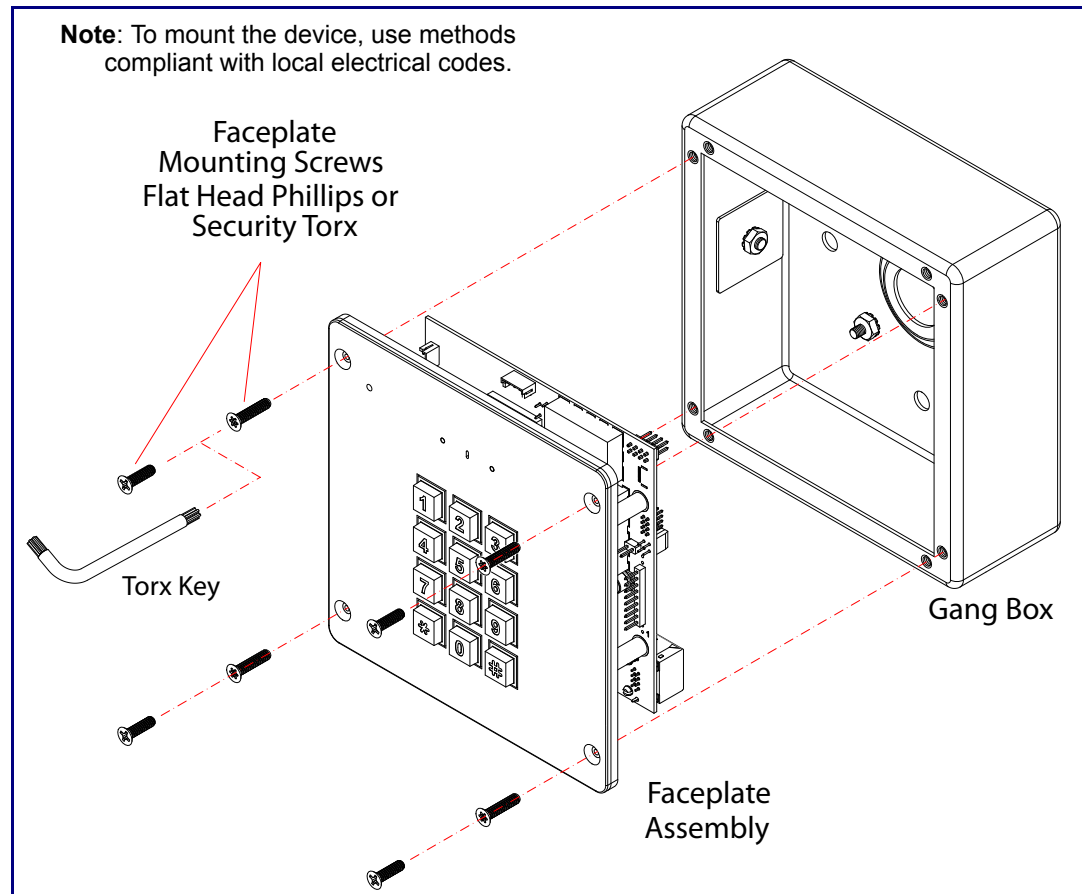
**Figure A-5. Network Cable Service Loop Routing**



## A.5 Securing the Enclosure

Figure A-6 illustrates how to secure the Secure Access Control Keypad with Torx screws.

**Figure A-6. Securing the Enclosure**



GENERAL ALERT

### Caution

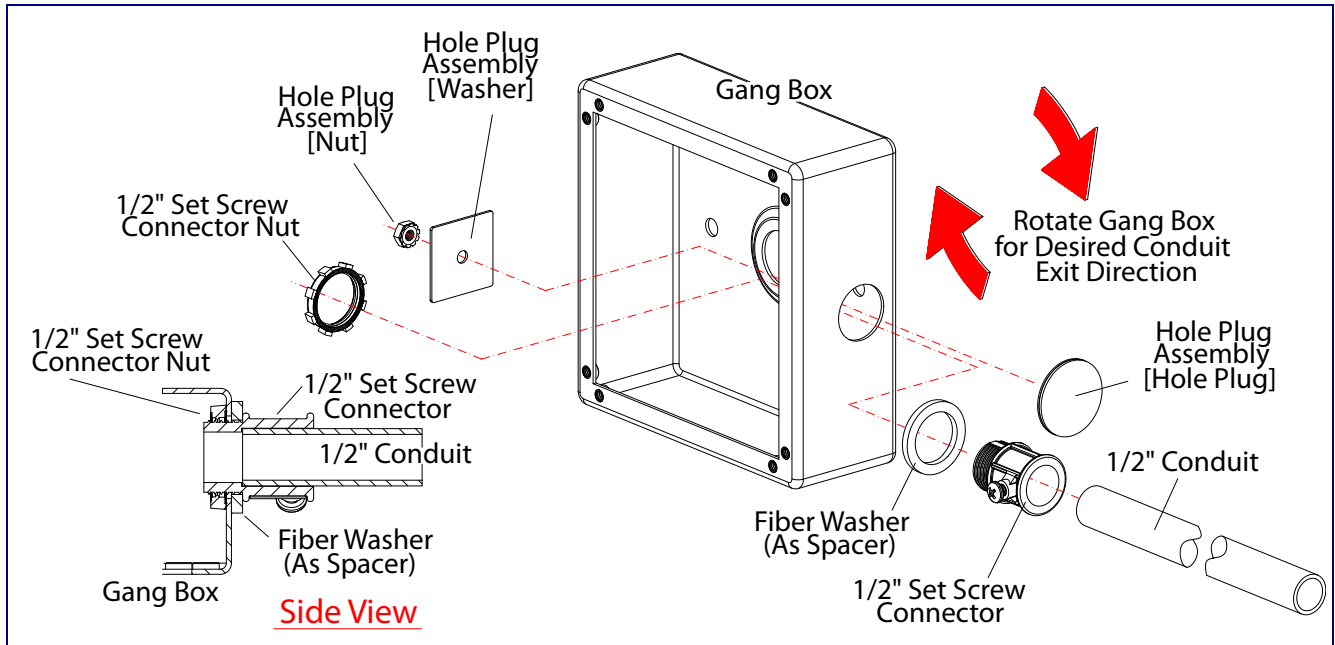
**Equipment Hazard:** Do not use an electric or power screwdriver to fasten the face plate and PCB assembly to the gang box. To prevent over-torque damage to the gasket, do not apply more than 10 inch-pounds force. Over-torquing will cause the gasket to tear, risk moisture intrusion, and effectively void the manufacturer's warranty.

## A.6 Additional Mounting Options

### A.6.1 Conduit Mounting (Side Entry) (Not Provided)

See [Figure A-7](#) for the conduit mounting option (side entry).

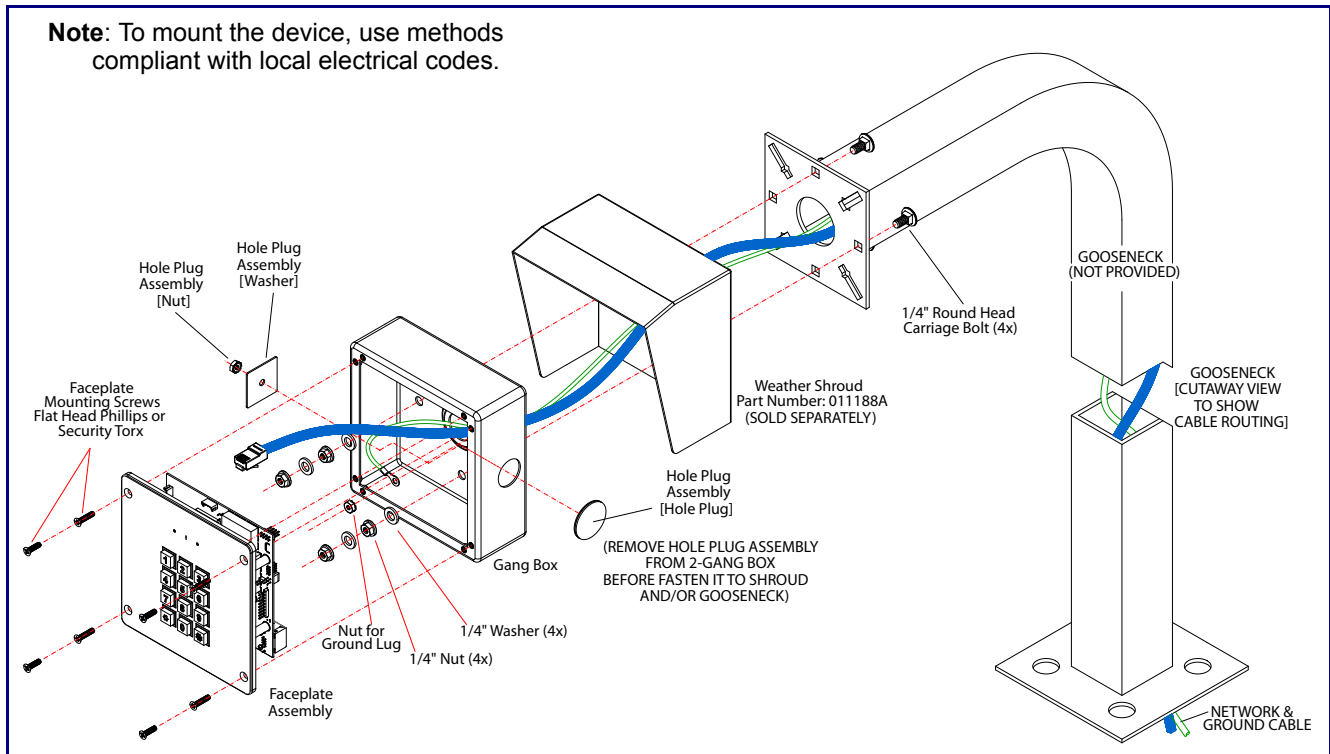
**Figure A-7. Conduit Mounting (Side Entry)**



## A.6.2 Goose Neck Mounting Option (Not Provided)

Figure A-8 illustrates a gooseneck mounting option for the Secure Access Control Keypad.

**Figure A-8. Optional Goose Neck Mounting**



# Appendix B: Setting up a TFTP Server

---

## B.1 Set up a TFTP Server

Autoprovisioning requires a TFTP server for hosting the configuration file.

---

### B.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
```

---

### B.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:

<http://www.cyberdata.net/assets/common/Solarwinds.zip>

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 C: Troubleshooting/Technical Support

---

## C.1 Frequently Asked Questions (FAQ)

To see a list of frequently asked questions for your product, click on the **FAQs** tab at the following webpage:

<http://www.cyberdata.net/voip/011433/>

---

## C.2 Documentation

The documentation for this product is released in an English language version only.

To download PDF copies of CyberData product documentation, click on the **Downloads** tab at the following webpage:

<http://www.cyberdata.net/voip/011433/>

---

## C.3 Contact Information

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Contact           | <p>CyberData Corporation<br/>3 Justin Court<br/>Monterey, CA 93940 USA<br/><a href="http://www.CyberData.net">www.CyberData.net</a><br/>Phone: 800-CYBERDATA (800-292-3732)<br/>Fax: 831-373-4193</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Sales             | <p>Sales 831-373-2601, Extension 334</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Technical Support | <p>The fastest way to get technical support for your VoIP product is to submit a VoIP Technical Support form at the following website:</p> <p><a href="http://support.cyberdata.net/">http://support.cyberdata.net/</a></p> <p>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 <b>Comments</b> section of the Support Form.</p> <p>Phone: (831) 373-2601, Extension 333</p> |

---

## C.4 Warranty and RMA Information

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

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

# Index

---

## Numerics

16 AWG gauge wire 9

## A

activate relay (door sensor) 48  
 activate relay (intrusion sensor) 48  
 activity LED 17  
 address, configuration login 23  
 alternative power input 6  
 audio configuration 50  
 audio configuration page 50  
 audio encodings 5  
 audio files, user-created 51  
 autoprovision at time (HHMMSS) 61  
 autoprovision when idle (in minutes > 10) 61  
 autoprovisioning 62  
     download template button 62  
     setting up a TFTP server 85  
 autoprovisioning autoupdate (in minutes) 61  
 autoprovisioning configuration 60, 61  
 autoprovisioning filename 61  
 autoprovisioning server (IP Address) 61

## B

backup SIP server 1 44  
 backup SIP server 2 44  
 backup SIP servers, SIP server  
     backups 44

## C

changing  
     the web access password 27  
 Cisco SRST 44  
 command interface 76  
 commands 76  
 conduit mounting option (not provided) 84  
 configurable parameters 28, 41  
 configuration  
     audio 50  
     default IP settings 19  
     door sensor 47  
     intrusion sensor 47

network 40  
     SIP 43  
 configuration home page 23  
 configuration page  
     configurable parameters 28, 41  
 contact information 87  
 contact information for CyberData 87  
 current network settings 41  
 CyberData contact information 87

## D

default  
     gateway 19  
     IP address 19  
     subnet mask 19  
     username and password 19  
     web login username and password 23  
 default gateway 19, 41  
 default intercom settings 18  
 default IP settings 19  
 default login address 23  
 default settings 88  
 device configuration 27  
     device configuration parameters 61  
     the device configuration page 60  
 device configuration page 27  
 device configuration parameters 28  
 device configuration password  
     changing for web configuration access 27  
 DHCP Client 5  
 dial out extension (door sensor) 48  
 dial out extension (intrusion sensor) 48  
 dial out extension strings 47  
 dimensions 6, 78  
     shroud dimensions and mounting hole locations 79  
     unit dimensions—front and side view 78  
     unit dimensions—rear view and mounting hole  
         locations 78  
 discovery utility program 23  
 DNS server 41  
 door sensor 47, 48  
     activate relay 48  
     dial out extension 48  
     door open timeout 48  
     door sensor normally closed 35, 48  
 download autoprovisioning template button 62  
 DTMF tones (using rfc2833) 47

## E

electric screwdriver 82  
 ethernet I/F 6  
 expiration time for SIP server lease 45  
 export settings 25

## F

factory default settings 18  
 fastening, gang box 82  
 firmware  
     where to get the latest firmware 72

## G

gang box, fastening 82  
 gasket, avoid over-torque damage 82  
 get autoprovisioning template 62  
 GMT table 31  
 GMT time 31  
 goose neck mounting option (not provided) 84  
 ground cable installation 81

## H

home page 23  
 http POST command 76  
 http web-based configuration 5

## I

identifier names (PST, EDT, IST, MUT) 31  
 identifying your product 1  
 import settings 25  
 import/export settings 25  
 installation, typical intercom system 2  
 intrusion sensor 47, 48  
     activate relay 48  
     dial out extension 48  
 IP address 19, 41  
 IP addressing  
     default  
     IP addressing setting 19

## J

J3 terminal block, 16 AWG gauge wire 9

## L

lease, SIP server expiration time 45  
 LED  
     green link LED 17  
     yellow activity LED 17  
 link LED 17  
 Linux, setting up a TFTP server on 85  
 local SIP port 45  
 log in address 23

## M

mounting 77  
     additional mounting options 83  
     conduit mounting option (not provided) 84  
     goose neck mounting option (not provided) 84  
     ground cable installation 81  
     optional accessories 77  
     overview of installation types 77, 80  
     rear conduit network cable entry restrictions (without shroud) 81  
     securing the intercom 82  
     service loop cable routing 81  
     side conduit network cable entry restrictions 81  
 mounting components 77  
 multicast configuration 50

## N

navigation (web page) 20  
 navigation table 20  
 network configuration 40  
 Nightringer 9, 71  
 NTP server 28

## O

on-board relay 6, 10  
 overview of installation types 80

## P

- packet time 5
- part number 6
- parts list 7
- password
  - for SIP server login 44
  - login 23
  - restoring the default 19
- payload types 6
- port
  - local SIP 45
  - remote SIP 45
- posix timezone string
  - timezone string 28
- POST command 76
- power input 6
  - alternative 6
- power screwdriver 82
- product features 4
- product overview
  - product features 4
  - product specifications 6
  - supported protocols 5
  - supported SIP servers 5
  - typical system installation 2
- product specifications 6
- protocol 6
- protocols supported 5

## R

- rear conduit network cable entry restrictions (without shroud) 81
- reboot 74, 75
- remote SIP port 45
- resetting the IP address to the default 77, 86
- restoring factory default settings 18, 88
- RJ-45 16
- rport discovery setting, disabling 45
- RTFM jumper 18
- RTP/AVP 5

## S

- sales 87
- securing the device 82
- sensor setup page 47, 58
- sensor setup parameters 47
- sensors 48
- server address, SIP 44
- service 87

- service loop cable routing 81
- set time with external NTP server on boot 28
- setting up the device 9
- settings, default 18
- shroud dimensions and mounting hole locations 79
- side conduit network cable entry restrictions 81
- SIP
  - enable SIP operation 44
  - local SIP port 45
  - user ID 44
- SIP configuration 43
- SIP configuration parameters
  - outbound proxy 45
  - registration and expiration, SIP server lease 45
  - unregister on reboot 45
  - user ID, SIP 44
- SIP registration 44
- SIP remote SIP port 45
- SIP server 44
  - password for login 44
  - SIP servers supported 5
  - unregister from 45
  - user ID for login 44
- SIP server configuration 44
- SRST 44
- subnet mask 19, 41
- supported protocols 5

## T

- tech support 87
- technical support, contact information 87
- terminal block, 16 AWG gauge wire 9
- TFTP server 5, 85
- time zone string examples 31

## U

- unit dimensions—front and side view 78
- unit dimensions—rear view and mounting hole locations 78
- user ID
  - for SIP server login 44
- username
  - changing for web configuration access 27
  - default for web configuration access 23
  - restoring the default 19

## V

- VLAN ID 41

VLAN Priority 41  
VLAN tagging support 41  
VLAN tags 41

## W

warranty policy at CyberData 87  
web access password 19  
web access username 19  
web configuration log in address 23  
web page  
    navigation 20  
web page navigation 20  
wget, free unix utility 76  
Windows, setting up a TFTP server on 85  
wiring the circuit 11  
    devices less than 1A at 30 VDC 11