



SIP RFID/Keypad Secure Access Control Endpoint Operations Guide

Part #011426

Document Part #931426A for Firmware Version 1.0.0

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

COPYRIGHT NOTICE: © 2018, 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.

CyberData	Technical Support
The IP Endpoint Company	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 Fax: (831) 373-4193 Company and product information is at www.cyberdata.net .

Revision Information

Revision 931426A, which corresponds to firmware version 1.0.0, was released on April 26, 2018.

Browsers Supported

The following browsers have been tested against firmware version 1.0.0:

- Internet Explorer (version: 10)
- Firefox (also called Mozilla Firefox) (version: 33.0)
- Chrome (version 48.0.2564.116)
- Safari (version: 5.1.7)

Pictorial Alert Icons

GENERAL ALERT	General Alert This pictoral alert indicates a potentially hazardous situation. This alert will be followed by a hazard level heading and more specific information about the hazard.
	Ground This pictoral 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!

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

Chapter 1 Product Overview	1
1.1 How to Identify This Product	
1.2 Typical System Installation	
1.3 Product Features	
1.4 Supported Protocols	
1.5 Supported SIP Servers	
1.6 Specifications	
1.7 Compliance	
1.7.1 CE Testing	
1.7.2 FCC Statement	7
Chapter 2 Installing the SIP RFID/Keypad Secure Access Control Endpoint	8
2.1 Parts List	
2.2 SIP RFID/Keypad Secure Access Control Endpoint Components	
2.3 Optimal orientation of the RFID tags and location against the RFID unit	
2.4 Device Setup	
2.4.1 SIP RFID/Keypad Secure Access Control Endpoint Connections	
2.4.2 Using the On-Board Relay	
2.4.3 Wiring the Circuit	
2.4.4 SIP RFID/Keypad Secure Access Control Endpoint Connectors	
2.4.5 Activity and Link LEDs	
2.4.6 RTFM Button	
2.5 Configure the SIP RFID/Keypad Secure Access Control Endpoint Parameters	
2.5.1 Factory Default Settings	
2.5.2 SIP RFID/Keypad Secure Access Control Endpoint Web Page Navigation	
2.5.3 Using the Toggle Help Button	
2.5.4 Log in to the Configuration Home Page	
2.5.5 Configure the Device	
2.5.6 Configure the Network Parameters	
2.5.7 Configure the SIP (Session Initiation Protocol) Parameters	
2.5.8 Configure the RFID Configuration Parameters	
2.5.9 Enrollment Procedure	
2.5.10 Configure the Sensor Configuration Parameters	
2.5.10 Configure the Sensor Configuration Parameters	
2.5.12 Configure the Events Parameters	
2.5.13 Configure the Door Strike Relay	
2.5.14 Configure the Autoprovisioning Parameters	
2.6 Upgrade the Firmware	
2.7 Reboot the Device	
2.7 Reboot the Device	
2.8 Command Interface Post Commands	
Appendix A Mounting the SIP RFID/Keypad Secure Access Control Endpoint	95
A.1 Mounting Components	95
A.2 Dimensions	96
A.3 Network Cable Entry Restrictions	99
A.3.1 Conduit Mounting Restrictions (Side Entry)	
A.4 Service Loop Cable Routing	100
A.5 Securing the Intercom	
A.6 Additional Mounting Options	
A.6.1 Goose Neck Mounting Option (Not Provided)	
Appendix B Setting up a TFTP Server	104
B.1 Set up a TFTP Server	
B.1.1 In a LINUX Environment	
B.1.2 In a Windows Environment	104
Appendix C Troubleshooting/Technical Support	105
C.1 Frequently Asked Questions (FAQ)	

i

Index

107

ii

1 Product Overview

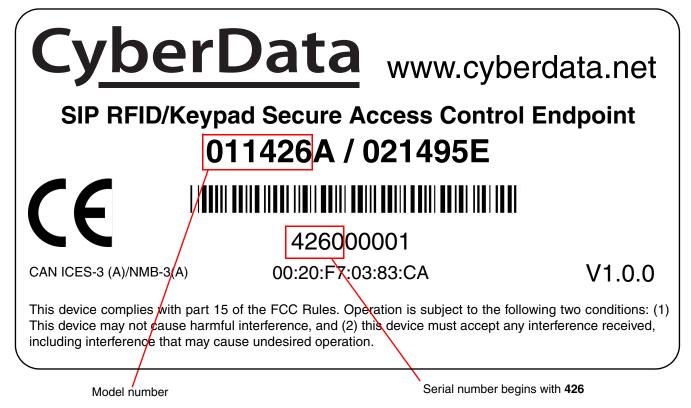
1.1 How to Identify This Product

To identify the SIP RFID/Keypad Secure Access Control Endpoint, 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 011426.
- The serial number on the label should begin with 426.

Figure 1-1. Model Number Label



1.2 Typical System Installation

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

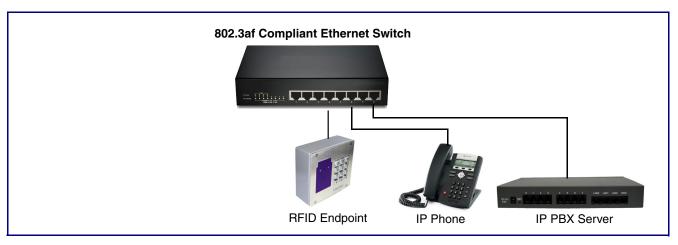
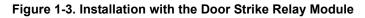
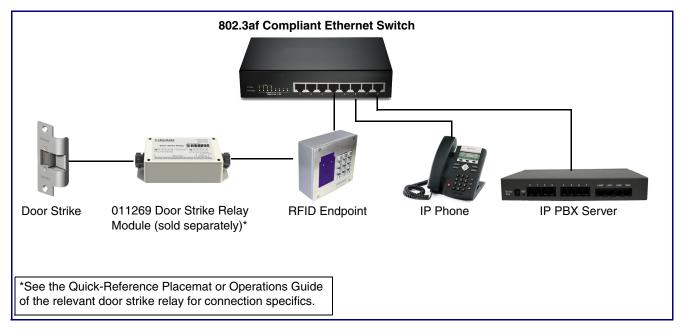
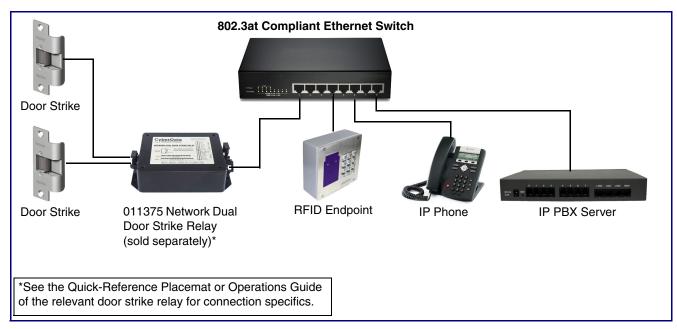


Figure 1-2. Typical Installation









1.3 Product Features

The SIP RFID/Keypad Secure Access Control Endpoint 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
- Optional flush mount kit
- 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
- 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 SIP RFID/Keypad Secure Access Control Endpoint supports the following protocols:

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

Provides an intuitive user interface for easy system configuration and verification of SIP RFID/ Keypad Secure Access Control Endpoint 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)

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

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 ^a	
On-Board Relay	1A at 30 VDC	
Supported RFID cards	Mifare Plus X 2k	
	Mifare Plus X 4k	
Operating Range	Temperature: -40° C to 55° C (-40° F to 131° F)	
	Humidity: 5-95%, non-condensing	
Storage Temperature	-40° C to 70° C (-40° F to 158° F)	
Storage Altitude	Up to 15,000 ft. (4573 m)	
Payload Types	G711, A-law and μ-law, G.722	
Dimensions ^b	5.118 inches [130 mm] Length	
	2.252 inches [57.21 mm] Width	
	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	011426	
	011188 Weather Shroud (sold separately)	

Table 1-1. Specifications

a. 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.

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

1.7 Compliance

1.7.1 CE Testing

CE testing has been performed according to EN ISO/IEC 17050 for Emissions, Immunity, and Safety. The Declaration of Conformity can be supplied upon request.

1.7.2 FCC Statement

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

2 Installing the SIP RFID/Keypad Secure Access Control Endpoint

2.1 Parts List

Table 2-1 illustrates the SIP RFID/Keypad Secure Access Control Endpoint parts.

Note See Appendix A, "Mounting the SIP RFID/Keypad Secure Access Control Endpoint" for physical mounting information.

Quantity	Part Name	Illustration
1	SIP RFID/Keypad Secure Access Control Endpoint Assembly	
1	Installation Quick Reference Guide	
1	SIP RFID/Keypad Secure Access Control Endpoint Mounting Accessory Kit	

Table 2-1. Parts List

2.2 SIP RFID/Keypad Secure Access Control Endpoint Components

Figure 2-1 shows the components of the SIP RFID/Keypad Secure Access Control Endpoint.

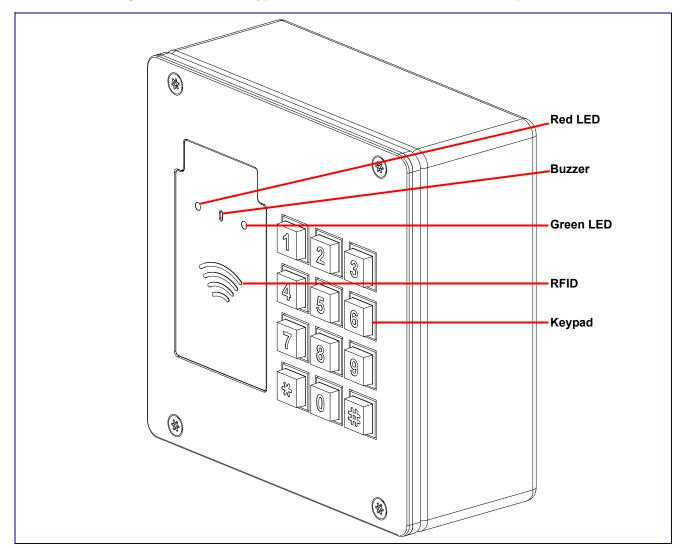
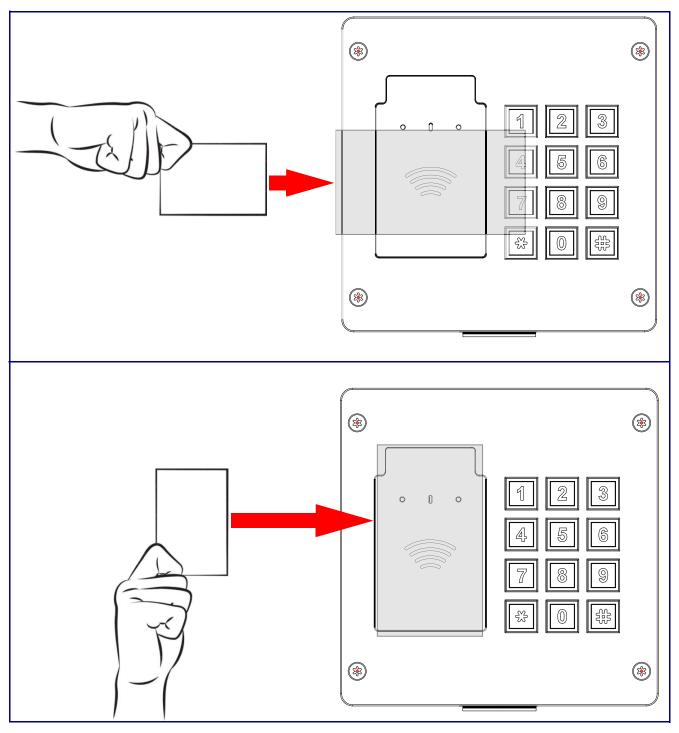


Figure 2-1. SIP RFID/Keypad Secure Access Control Endpoint Components

2.3 Optimal orientation of the RFID tags and location against the RFID unit

For best results, the tag should be oriented and touched to the location shown in Figure 2-2 and held for at least one second.





2.4 Device Setup

2.4.1 SIP RFID/Keypad Secure Access Control Endpoint Connections

Figure 2-3 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.



Caution

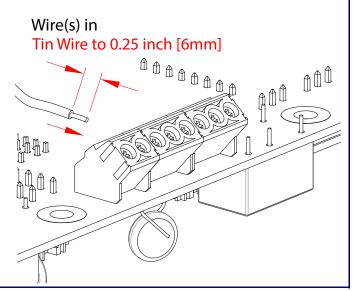
Equipment Hazard: Contacts 1 and 2 on the terminal block are only for powering the device from a non-PoE 12 VDC power source as an alternative to Network PoE power. Use of these contacts for any other purpose will damage the device and void the product warranty.

Figure 2-3. Intercom Connections

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



Terminal block can accept up to 16 AWG wire. Tool required for terminal block screw: Size #00 Phillip Drive Screwdriver



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.

2.4.2 Using the On-Board Relay

GENERAL ALERT	Warning <i>Electrical Hazard:</i> This product should be installed by a licensed electrician according to all local electrical and building codes.
GENERAL ALERT	Warning <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.
GENERAL ALERT	Warning Electrical Hazard: The relay does not support AC powered door strikes. Any use of this relay beyond its normal operating range can cause damage to the product and is not covered under our warranty policy.

The device has a built-in relay that can be activated by a web configurable DTMF string that can be received from a VoIP phone supporting out of band (RFC2833) DTMF as well as a number of other triggering events. See the **Device 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 2.4.3.2, "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.

2.4.3 Wiring the Circuit

2.4.3.1 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 2-4 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 2.4.3.2, "Network Dual Door Strike Relay Wiring Diagram with External Power Source").

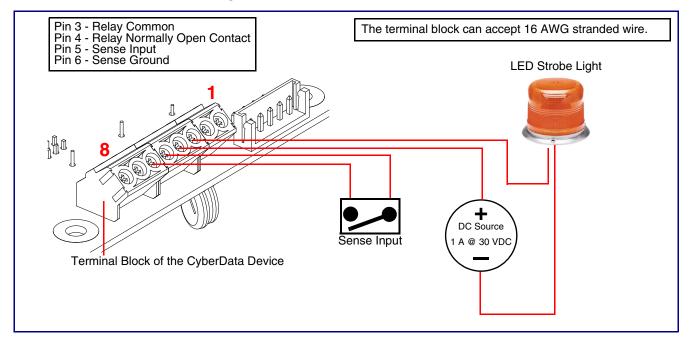


Figure 2-4. Devices Less than 1A at 30 VDC

2.4.3.2 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 2-5 and Figure 2-6 for the wiring diagrams.

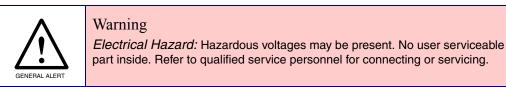
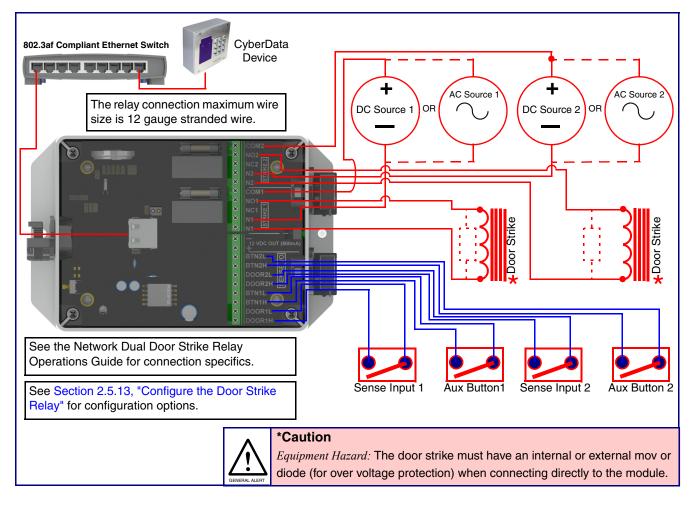


Figure 2-5. Network Dual Door Strike Relay Wiring Diagram with External Power Source



Note When **Activate DSR on Valid RFID** is enabled, a swipe of a valid RFID card will activate Relay 2.

2.4.3.3 Network Dual Door Strike Relay Wiring Diagram Using PoE+

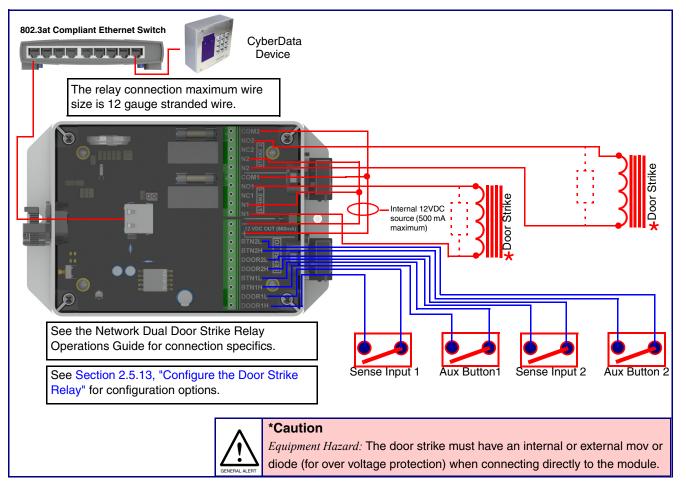


Figure 2-6. Network Dual Door Strike Relay Wiring Diagram Using PoE+

Note When Activate DSR on Valid RFID is enabled, a swipe of a valid RFID card will activate Relay 2.

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

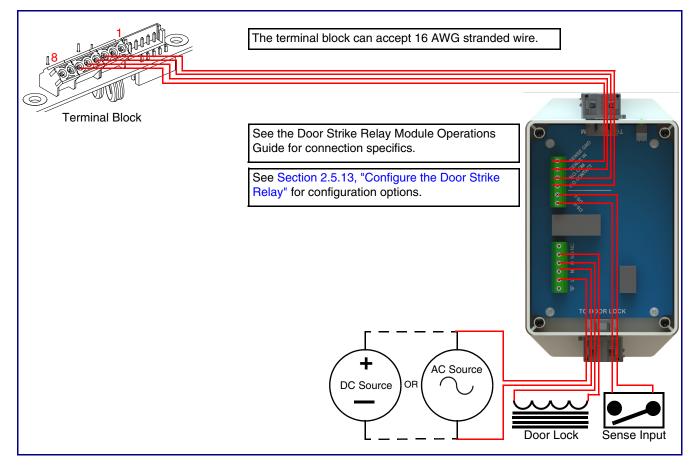
http://support.cyberdata.net/

2.4.3.4 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 2-7 for the wiring diagram.





Note When **Activate DSR on Valid RFID** is enabled, a swipe of a valid RFID card will activate Relay 2.

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/

2.4.4 SIP RFID/Keypad Secure Access Control Endpoint Connectors

See the following figures and tables to identify the connectors and functions of the SIP RFID/Keypad Secure Access Control Endpoint.

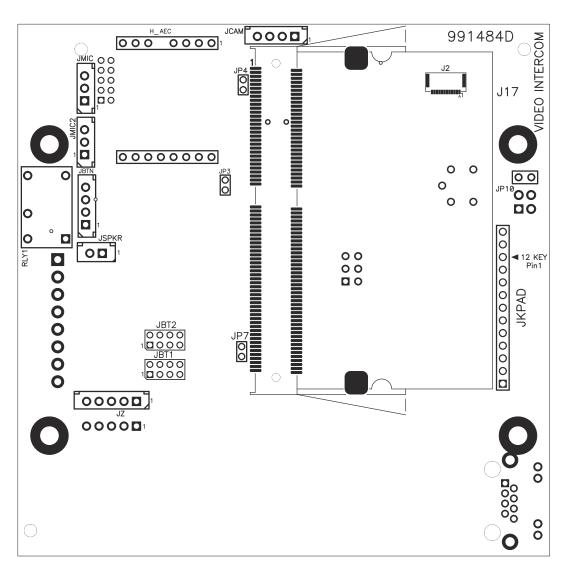


Figure 2-8. Connector Locations

Table 2-2. Connector Functions	Table 2-2.	Connector	Functions
--------------------------------	------------	-----------	-----------

Connector	Function
JCAM	Camera Interface
H_AEC	Echo Cancellation Interface
JBTN	Call Button LED Interface
JMIC	Microphone Interface
JMIC2	Second Microphone Interface — Not Used
JSPKR	Speaker Interface
JKPAD	Keypad Interface — Not Used
JY	Sensor Interface — Not Used
JP3	Audio Mute — Factory Use Only
JP4	Boot from mSD Card — Factory Use Only
JP7	EPROM Write Protect — Factory Use Only
JP10	Disables the intrusion sensor when installed.
J17	Sitara Card Interface — Factory Use Only
JBT1	Touch Button -1 Interface — Not Used
JBT2	Touch Button -2 Interface — Not Used

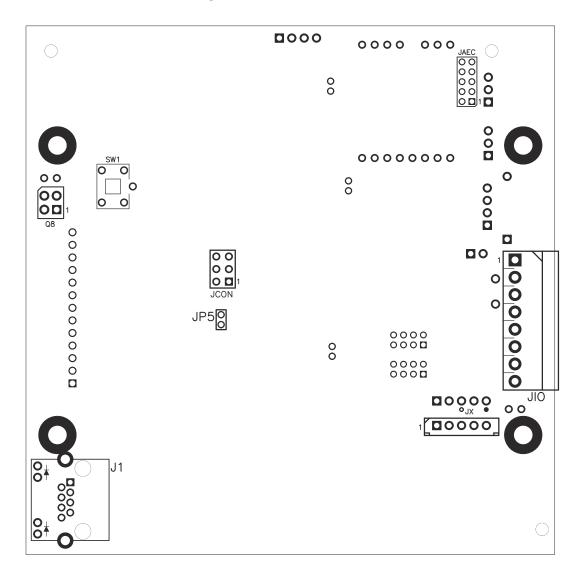


Figure 2-9. Connector Locations

Connector	Function
J1	PoE Network Connection (RJ-45 ethernet)
JP5	Reset jumper ^a
JX	Auxiliary Strobe Interface
Q8	Intrusion Detector
JAEC	AEC Configuration Interface — Factory Use Only
JIO	Terminal Block (see Figure 2-3)
JCON	Console Port — Factory Use Only
JSPI	Reserved — Factory Use Only
SW1	See Section 2.4.6, "RTFM Button"

Table 2-3. Connector Functions

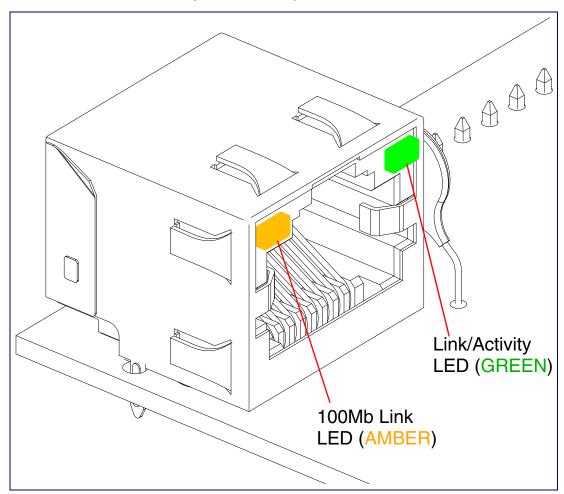
a.Do not install a jumper. Momentary short to reset. Permanent installation of a jumper would prevent the board from running all together.

2.4.5 Activity and Link LEDs

2.4.5.1 Verifying the Network Connectivity and Data Rate

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

- The square, GREEN Link/Activity LED blinks when there is network activity (see Figure 2-10).
- The square, **AMBER 100Mb Link** LED above the Ethernet port indicates that a 100Mb network connection has been established (see Figure 2-10).





2.4.6 RTFM Button

When the SIP RFID/Keypad Secure Access Control Endpoint is operational and linked to the network, you can use the Reset Test Function Management **(RTFM)** button (see **SW1** in Figure 2-11) on the SIP RFID/Keypad Secure Access Control Endpoint board to announce and confirm the SIP RFID/Keypad Secure Access Control Endpoint's IP Address and test to see if the audio is working.

Note You must do these tests prior to final assembly.

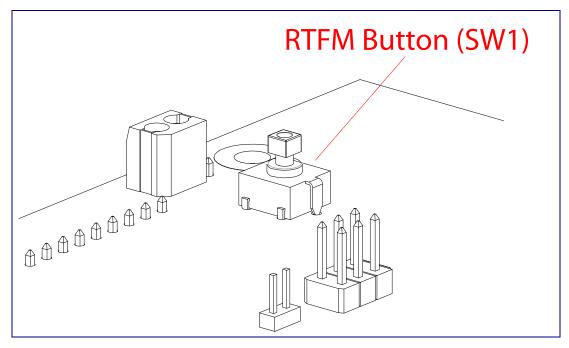
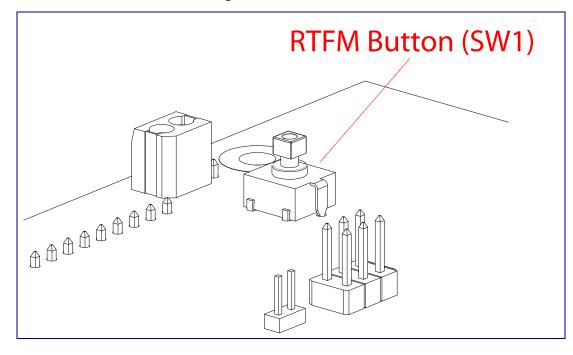


Figure 2-11. RTFM Button

2.4.6.1 Announcing the IP Address

To announce a device's current IP address:

- 1. Press and release the RTFM button (see **SW1** in Figure 2-12) within a five second window.
- **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).
- **Note** Pressing and holding the RTFM button for longer than five seconds will restore the device to the factory default settings.





2.4.6.2 Restoring the Factory Default Settings

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

Note Each SIP RFID/Keypad Secure Access Control Endpoint is delivered with factory set default values.

To restore the factory default settings:

- 1. Press and hold the RTFM button (see SW1 in Figure 2-13) for more than five seconds.
- 2. The device announces that it is restoring the factory default settings.
- **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).

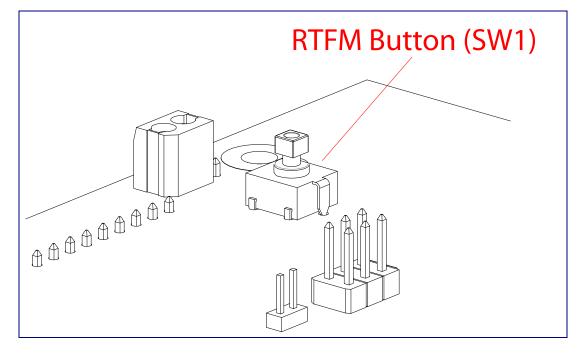


Figure 2-13. RTFM Button

2.5 Configure the SIP RFID/Keypad Secure Access Control Endpoint Parameters

To configure the SIP RFID/Keypad Secure Access Control Endpoint online, use a standard web browser.

Configure each SIP RFID/Keypad Secure Access Control Endpoint and verify its operation *before* you mount it. When you are ready to mount an SIP RFID/Keypad Secure Access Control Endpoint, refer to Appendix A, "Mounting the SIP RFID/Keypad Secure Access Control Endpoint" for instructions.

2.5.1 Factory Default Settings

All SIP RFID/Keypad Secure Access Control Endpoints are initially configured with the following default IP settings:

When configuring more than one SIP RFID/Keypad Secure Access Control Endpoint, attach the SIP RFID/Keypad Secure Access Control Endpoints to the network and configure one at a time to avoid IP address conflicts.

Parameter	Factory Default Setting
IP Addressing	DHCP
IP Address ^a	10.10.10.10
Web Access Username	admin
Web Access Password	admin
Subnet Mask ^a	255.0.0.0
Default Gateway ^a	10.0.0.1

Table 2-4. Factory Default Settings

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

2.5.2 SIP RFID/Keypad Secure Access Control Endpoint Web Page Navigation

Table 2-5 shows the navigation buttons that you will see on every SIP RFID/Keypad Secure Access Control Endpoint web page.

Web Page Item	Description
Home	Link to the Home page.
Device	Link to the Device page.
Network	Link to the Network page.
SIP	Link to go to the SIP page.
RFID	Link to the RFID page.
Sensor	Link to the Sensor page.
Audiofiles	Link to the Audiofiles page.
Events	Link to the Events page.
DSR	Link to the Door Strike Relay page.
Autoprov	Link to the Autoprovisioning page.
Firmware	Link to the Firmware page.

Table 2-5. Web Page Navigation

2.5.3 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 2-14 and Figure 2-15.

Figure 2-14. 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 2-15.

Figure	2-15.	Toggle	Help	Button	and	Question	Marks

Stored Net			
Addressing Mode	?		
hostname:	SipDevice03cab3	?	
IP Address:	10.10.10.10		
Subnet Mask:	255.0.0.0	?	Question mark appears next to the
Default gw_addr:	10.0.0.1	://	web page items
DNS Server 1:	10.0.0.1	?//	
DNS Server 2:	10.0.0.1	?	

3. Move the mouse pointer to hover over the question mark (?), and a short description of the web page item will appear. See Figure 2-16.

	hostname	hostname			
	DHCP server. Guide and DH	See the Oper CP/DNS serv			
Stored Net		tation for more information. to 64 characters.			
Addressing Mode:					
hostname:	SipDevice03cal	3 ?			
IP Address:	10.10.10.10	?			
Subnet Mask:	255.0.0.0	?			
Default gw_addr:	10.0.0.1	?			
DNS Server 1:	10.0.0.1	?			
DNS Server 2:	10.0.0.1	?			
	Question mar	k A short desc			

Figure 2-16. Short Description Provided by the Help Feature

Question mark

A short description of the web page item will appear

2.5.4 Log in to the Configuration Home Page

- 1. Open your browser to the SIP RFID/Keypad Secure Access Control Endpoint 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 SIP RFID/Keypad Secure Access Control Endpoint.
- **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 2-17):

Web Access Username: admin

Web Access Password: admin

Home Device Network REID Sensor Audiofiles Events DSR Autoprov Sip Firmware **CyberData Keypad RFID Current Status Admin Settings** Import Settings Serial Number: 426000001 Browse... No file chosen Username: admin 00:20:f7:03:ca:b3 v1.0.0 Mac Address: Password: Firmware Version: v1.0.0 Confirm Password: Partition 2: Partition 3: v1.0.0 partition 2 **Booting From: Export Settings** Save Toggle Help IP Addressing: **IP Address:** 10.10.0.119 Subnet Mask: 255 0 0 0 Default gw_addr: 10.0.0.1 10.0.1.56 DNS Server 1: DNS Server 2: SIP Mode: Enabled Event Reporting: Disabled Primary SIP Server: Not registered Backup Server 1: Not registered Backup Server 2: Not registered

Figure 2-17. 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. Hollie Page Overview
Web Page Item	Description
Admin Settings	
Username ?	The username to access the web interface. Enter up to 25 characters.
Password ?	The password to access the web interface. Enter up to 25 characters.
Confirm Password ?	Confirm the web interface password.
Current Status	
Serial Number	Shows the device serial number.
Mac Address	Shows the device Mac address.
Firmware Version	Shows the current firmware version.
Partition 2	Contains a complete copy of bootable software.
Partition 3	Contains an alternate, complete copy of boot.
Booting From	Indicates the partition currently used for boot.
Boot From Other Partition	Swap the boot partition.
IP Addressing	Shows the current IP addressing setting (DHCP or static).
IP Address	Shows the current IP address.
Subnet Mask	Shows the current subnet mask address.
Default Gateway	Shows the current default gateway address.
DNS Server 1	Shows the current DNS Server 1 address.
DNS Server 2	Shows the current DNS Server 2 address.
SIP Mode	Shows the current status of the SIP mode.
Event Reporting	Shows the current status of the Event Reporting mode.
Primary SIP Server	Shows the current status of the Primary SIP Server.
Backup Server 1	Shows the current status of Backup Server 1.
Backup Server 2	Shows the current status of Backup Server 2.
Import Settings	
Browse	Use this button to select a configuration file to import.
Import Config	After selecting a configuration file, click Import to import the configuration from the selected file.
Export Settings	
Export Config	Click Export to export the current configuration to a file.

Table 2-6. Home Page Overview

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

Table 2-6. Home Page Overview (continued)

2.5.5 Configure the Device

1. Click the **Device** menu button to open the **Device** page. See Figure 2-18.

Figure 2-18. Device Configuration Page	Figure	2-18.	Device	Configuration	Page
--	--------	-------	--------	---------------	------

Home	Device	Network	Sip	RFID	Sensor	Audiofiles	Events	DSR	Autoprov	Firmwa
		Cv	ber	'Da'	ta K	eypa	d R	FID		
		- J				- J				
Relay Se	ttings					Misc Settin	gs			
Activate Relay	with DTMF code	e: 🗹				Device Name:	1000	CyberData	Keypad RFID	
Relay Pulse Co	de:	123				Keypad Lit when Id	lle:	•		
Relay Pulse Du	iration (in secon	ids): 2				Keypad Brightness		255		
Relay Activatio	n Code:	456				RFID LED Brightne	ss (0-255):	255		
Relay Deactiva	tion Code:	654				Auto-Answer Incor				
ctivate Relay						Disable HTTPS (NC	T recommende	ed):		
ctivate Relay	While Call Activ	re: 🗆								
Play Button To	nes:	Z				Clock Setti	ngs			
						Enable NTP: 🕑				
						and the second	-america.pool.nt	p.org		
							rica/Los Angele			
						Current Time: Tue,				
Save Ret	oot Toggle H	lelp				Test Relay				

- 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.

Web Page Item	Description
Relay Settings	
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).
Activate Relay During Ring ?	When selected, the relay will be activated when the device is contacted and auto answer is disabled. When Auto-Answer Incoming Calls is enabled, this option does nothing.
Activate Relay While Call Active ?	When selected, the relay will be activated as long as the SIP call is active.
Play Button Tones 🛜	Play a tone when the keypad buttons are pressed.
Misc Settings	
Device Name 🛜	Enter up to 25 characters.
Keypad Lit when Idle ?	When selected, the keypad LEDs are illuminated while the device is idle (a call is not in progress).
Keypad Brightness (0-255) ?	The desired keypad LED brightness level. Acceptable values are 0-255, where 0 is the dimmest and 255 is the brightest. Enter up to 3 digits.
RFID LED Brightness (0-255) <mark>?</mark>	The desired brightness of the leds on the rfid reader. Acceptable values are 0-255, where 0 is off and 255 is max brightness. Enter up to 3 digits.
Auto-Answer Incoming Calls ?	When selected, the device will automatically answer incoming calls. When Auto-Answer Incoming Calls is disabled, the device will enter a ringing state until the caller disconnects.
Disable HTTPS (NOT recommended) 🛜	Disables the encrypted connection to the webpage. We do not recommend disabling HTTPS for security reasons.
Clock Settings	
Enable NTP ?	Sync device's local time with the specified NTP Server.
	Note : This function must be selected to limit the times valid for the RFID tags.

Table 2-7. Device Page Parameters

Web Page Item	Description					
NTP Server ?	Use this field to set the address (in IPv4 dotted decimal notation or as a canonical name) for the NTP Server. This field can accept canonical names of up to 64 characters in length.					
Timezone	Enter the tz database string of your timezone.					
	Examples:					
	America/Los_Angeles					
	America/New_York					
	Europe/London					
	America/Toronto					
	See https://en.wikipedia.org/wiki/List of tz database time zones for a full list of valid strings.					
Current Time	Displays the current time.					
Save	Click the Save button to save your configuration settings.					
Reboot	Click on the Reboot button to reboot the system.					
Toggle Help	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.					

Table 2-7. Device Page Parameters (continued)

2.5.6 Configure the Network Parameters

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

Figure 2-19. Network Configuration	n Page
------------------------------------	--------

Home	Device	Network	Sip	RFID	Sensor	Audiofiles	Events	DSR	Autoprov	Firmware
		Cvb	ber	Dat	a Ke	eypa	d Rl	FID		
		-								
Stored Net	twork Se	ettings				VLAN Setti	ngs			
Addressing Mode	: O Static 🖲 D	HCP				VLAN ID (0-4095):	0			
hostname:	SipDevice03	cab3				VLAN Priority (0-7): 0			
IP Address:	10.10.10.10									
Subnet Mask:	255.0.0.0									
Default gw_addr:	10.0.0.1									
DNS Server 1:	10.0.0.1									
DNS Server 2:	10.0.0.1									
	10.10.0.119 255.0.0.0 10.0.0.1	Settings				Save Reboot	Toggle Help			

- 2. On the Network page, enter values for the parameters indicated in Table 2-8.
- **Note** The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Web Page Item	Description
Stored Network Settings	3
Addressing Mode ?	Select either DHCP IP Addressing or Static Addressing by marking the appropriate radio button. DHCP Addressing mode is enabled on default and the device will attempt to resolve network addressing with the local DHCP server upon boot. If DHCP Addressing fails, the device will revert to the last known IP address or the factory default address if no prior DHCP lease was established. See Section 2.5.1, "Factory Default Settings" for factory default settings. Be sure to click Save and Reboot to store changes when configuring a Static address.
Hostname ?	This is the hostname provided by the DHCP server. See the DHCP/DNS server documentation for more information. Enter up to 64 characters.
IP Address ?	Enter the Static IPv4 network address in dotted decimal notation.
Subnet Mask ?	Enter the Subnet Mask in dotted decimal notation.
Default Gateway ?	Enter the Default Gateway IPv4 address in dotted decimal notation.

Table 2-8. Network Configuration Parameters

Web Page Item	Description
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.
VLAN Settings	
VLAN ID (0-4095) ?	Specify the IEEE 802.1Q VLAN ID number. Enter up to 4 digits.
	Note : The device supports 802.1Q VLAN tagging support. The switch port connected to the device will need to be in "trunking mode" for the VLAN tags to propagate.
VLAN Priority (0-7) ?	Specify the IEEE 802.1p VLAN priority level. Enter 1 digit. A value of 0 may cause the VLAN ID tag to be ignored.
Current Network Settings	Shows the current network settings.
IP Address	Shows the current Static IP address.
Subnet Mask	Shows the current Subnet Mask address.
Default Gateway	Shows the current Default Gateway address.
DNS Server 1	Shows the current DNS Server 1 address.
DNS Server 2	Shows the current DNS Server 2 address.
	Click the Save button to save your configuration settings.
Save	Note: You need to reboot for changes to take effect.
Reboot	Click on the Reboot button to reboot the system.
Toggle Help	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.
Note	You must click on the Save button and then the Reboot button for the changes to take effect.

Table 2-8. Network Configuration Parameters (continued)

2.5.7 Configure the SIP (Session Initiation Protocol) Parameters

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

Figure 2-2	0. SIP	Configuration	Page
------------	--------	---------------	------

Home Device Net	twork Sip	RFID	Sensor	Audiofiles	Events	DSR	Autoprov	Firmware	
0									
L C	yber	Daτ	aĸ	eypa		FIL			
SIP Settings				Call Discor	nection				
n - en a como de 1970 - 1970 - 1970 - 1970 - 1970 - 1970 - 1970 - 1970 - 1970 - 1970 - 1970 - 1970 - 1970 - 19						_			
	10.0.0.252			Terminate Call afte	r delay: 0				
	10.0.0.253								
	199 199			RTP Settin	as				
	199				50				
Re-registration Interval (in seconds):				RTP Port (even): 10			-		
te egistration interval (in secondo).	300			Jitter Buffer: 50)				
Backup SIP Server 1:									
Backup SIP User ID:				Save Reboot	Toggle Help				
Backup SIP Auth ID:									
Backup SIP Auth Password:									
Re-registration Interval (in seconds):	360								
Backup SIP Server 2:									
Backup SIP User ID:									
Backup SIP Auth ID:									
Backup SIP Auth Password:									
Re-registration Interval (in seconds):	360								
Remote SIP Port:	5060								
	5060								
Outbound Proxy:									
Outbound Proxy Port:	0								
Use Cisco SRST:									
Register with a SIP Server:	•								
Disable rport Discovery:									
Unregister on Boot:									
Keep Alive Period:	10000								

- 2. On the SIP page, enter values for the parameters indicated in Table 2-9.
- **Note** The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Web Page Item	Description
SIP Settings	
Enable SIP Operation ?	When enabled, the device will transmit, receive, and process SIP messages according to the configured SIP settings below.
Primary SIP Server 🛜	Enter the SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the primary SIP server. This field can accept entries of up to 255 characters in length.
Primary SIP User ID ?	Specify the SIP User ID for the Primary SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the primary SIP server. Enter up to 64 alphanumeric characters.
Primary SIP Auth ID 🛜	Specify the Authenticate ID for the Primary SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Primary SIP Auth Password 🛜	Specify the Authenticate Password for the Primary SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Re-registration Interval (in seconds) ?	The SIP Re-registration interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
Backup SIP Server 1 ?	Enter the backup SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the backup SIP server. This field can accept entries of up to 255 characters in length.
Backup SIP User ID 1 ?	Specify the SIP User ID for the first backup SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the first backup SIP server. Enter up to 64 alphanumeric characters.
Backup SIP Auth ID 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.
Re-registration Interval (in seconds) ?	The SIP Re-registration interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
Backup SIP Server 2 ?	Enter a second backup SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the second backup SIP server. This field can accept entries of up to 255 characters in length.
Backup SIP User ID 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 2-9. SIP Page Parameters

Web Page Item	Description
Re-registration Interval (in seconds) ?	The SIP Re-registration interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
Remote SIP Port 🛜	The Remote SIP Port is the port number the device will use as the destination port when sending SIP messages. The default Remote SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
Local SIP Port ?	The Local SIP Port is the port number the device will use to receive SIP messages. The default Local SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
Outbound Proxy ?	Enter the Outbound Proxy address as an IPv4 address in dotted decimal notation or a fully qualified domain name (FQDN). When an IP address is configured, the device will send all SIP messages to this IP address. When an FQDN is configured, the device will run DNS NAPTR, SRV, and A queries on the FQDN to resolve an IP address to which it will send all SIP messages. This field can accept entries of up to 255 characters in length.
Outbound Proxy Port ?	The Outbound Proxy Port is port number used as the destination port when sending SIP messages to the outbound proxy. A value of 0 will default to 5060. The supported range is 0-65536. Enter up to 5 digits.
Use Cisco SRST 🛜	When enabled, the backup servers are handled according to Cisco SRST (Survivable Remote Site Telephony). It is required for use in clustered Cisco Unified Communications Manager topologies.
Register with a SIP Server 🛜	When enabled, the device will attempt to register to the configured SIP Server(s) on this page. To configure the device to send and receive point-to-point SIP calls, enable SIP Operation and disable Register with a SIP Server (see Section 2.5.7.1, "Point-to-Point Configuration").
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.
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.
Call Disconnection	
Terminate Call After Delay 🛜	Automatically terminate an active call after a given delay in seconds. A value of 0 will disable this function. Enter up to 8 digits.
	Note: This setting does not require a reboot for the changes to take effect.
RTP Settings	
RTP Port (even) ?	Specify the port number used for the RTP stream after establishing a SIP call. This port number must be an even number and defaults to 10500. The supported range is 0-65536. Enter up to 5 digits.
Jitter Buffer ?	Specify the size of the jitter buffer (in milliseconds) used for SIP calls. Valid values are 50-1000.
Save	Click the Save button to save your configuration settings.

Table 2-9. SIP Page Parameters (continued)

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

Table 2-9. SIP Page Parameters (continued)

2.5.7.1 Point-to-Point Configuration

When the device is set to not register with a SIP server (see Figure 2-21), it is possible to set the device to dial out to a specified endpoint.

To make a point to point call, enter the IP address of the remote device in the **Dialout SIP Extension** setting on the RFID page, or the **Dialout Extension** setting of the **Sensor** or **DSR** page. Each of these fields may have the same dialout endpoint, or different ones.

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

Figure 2-21. SIP Page Set to Point-to-Point Mode

Home	Device	Network	Sip RFID	Sensor	Audiofiles	Events	DSR	Autoprov	Firmware
		-							
		Cvb	erDa	ta K	evpa	ad R	FIC)	
		- J							
SIP Set	tinas				Call Discor	nection			
Enable SIP o		a			Terminate Call after				
Primary SIP	·	10.0.0.253			Terminate Can alte	er delay. 0			
Primary SIP		199							
Primary SIP		199			RTP Settin	qs			
	Auth Password:				RTP Port (even): 1				
	on Interval (in sec				Jitter Buffer: 5			-	
					Since Building	•			
Backup SIP	Server 1:								
Backup SIP	User ID:				Save Reboot	Toggle Help			
Backup SIP	Auth ID:								
Backup SIP	Auth Password:								
Re-registrati	on Interval (in sec	onds): 360							
Backup SIP :	Sonvor 2:								
Backup SIP									
Backup SIP									
	Auth Password:								
-	on Interval (in sec	onds): 360							
	(1000							
Remote SIP	Port:	5060							
Local SIP Po	ort:	5060							
Outbound D	-								
Outbound Pr Outbound Pr		0							
Outbound Pr	loxy Port.	U							
Use Cisco Sl	RST:								
Register with	h a SIP Server:	P							
Disable rport		/-							
Unregister o									
Keep Alive P	Period:	10000							

Device is set to NOT register with a SiP server

2.5.8 Configure the RFID Configuration Parameters

1. Click the **RFID** menu button to open the **RFID** page (Figure 2-50).

Figure 2-22. RFID Configuration Page

Home	Device	Network	Sip	RFID	Sensor	A	udiofiles	Events	DSI	2	Autoprov	Firmware
			С	vbe	rDa	ta	ı R	FID				
Current St	tatus		-					ccess Lis		Ехро	ort Acces	s List
Waiting for RFID	tag					Bro	wse	lo file chosen		_		
RFID Pass	sphrase						ort Access	_		Expor	t Access List	
Passphrase			Show			Aco	ess L					
Set Master Key						1	Name Jason	Valid From All	Valid To All	Blacklis	Edit	Delete
Authentica		-				2		All	All	No	Add	Delete
wo Factor Time		4				3		All	All	No	Add	Delete
Relay Sett	tings					4		All	All	No	Add	Delete
ctivate Relay or ctivate DSR on						5		All	All	No	Add	Delete
elay Timeout (s						6		All	All	No	Add	Delete
Buzzer Se	ttings					7		All	All	No	Add	Delete
Buzz while Relay Buzz on Rejected						8		All	All	No	Add	Delete
Sensor Se	ettings					9		All	All	No	Add	Delete
Buzz on Door Op Door Sensor Nor	en Timeout:	□ : O Yes ● No				10		All	All	No	Add	Delete
Sensor Open Tim OSR Open Timeo	neout (in seco	onds): 0				11		All	All	No	Add	Delete
		ls): 0				12		All	All	No	Add	Delete
Blacklist A Play Message to		n 🗆				13		All	All	No	Add	Delete
Dial Out SIP Exte Dial Out SIP ID	ension	666 ext666				14		All	All	No	Add	Delete
Aulticast Audio M	Message					15		All	All	No	Add	Delete
Aulticast Addres Aulticast Port	s	234.6.6.6 666				16		All	All	No	Add	Delete
imes to Play Mu	Ilticast Messa					17		All	All	No	Add	Delete
Save Reboo	t Toggle H	elp				18		All	All	No	Add	Delete

Figure	2-23.	RFID	Configuration Pag	е
--------	-------	------	--------------------------	---

ecurity log	20	All	All	No	Add	Delete
2018-04-10 11:53:57 Waiting for RFID tag 2018-04-10 11:54:04 Deactivating the dsr relay after timeout					Add	Delete
2018-04-10 11:54:04 Deactivating the local relay after timeout 2018-04-10 12:03:38 Device entering RFID Validate Mode 2018-04-10 12:03:38 Waiting for RFID tag	21	All	All	No	Add	Delete
2018-04-10 12:05:38 Waiting for RFID tag 2018-04-10 12:05:04 Device entering RFID Validate Mode 2018-04-10 12:05:04 Waiting for RFID tag	22	All	All	No	Add	Delete
1018-04-10 11:01:38 Device entering RFID Validate Mode 1018-04-10 13: RFID tag	23	All	All	No	Add	Delete
1018-04-10 14:26:39 Received rfid authentication for tag 4 2018-04-10 14:26:39	24	All	All	No	Add	Delete
Set Security Log Refresh Log	25	All	All	No	Add	Delete
	26	All	All	No	Add	Delete
	27	All	All	No	Add	Delete
	28	All	All	No	Add	Delete
	29	All	All	No	Add	Delete
	30	All	All	No	Add	Delete
	31	All	All	No	Add	Delete
	32	All	All	No	Add	Delete
	33	All	All	No	Add	Delete
	34	All	All	No	Add	Delete
	35	All	All	No	Add	Delete
	36	All	All	No	Add	Delete
	37	All	All	No	Add	Delete
	38	All	All	No	Add	Delete
	39	All	All	No	Add	Delete
	40	All	All	No	Add	Delete
	41	All	All	No	Add	Delete
	42	All	All	No	Add	Delete
	43	All	All	No	Add	Delete

- 2. On the Sensor page, enter values for the parameters indicated in Table 2-11.
- **Note** The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Web Page Item	Description							
Current Status	Display the current status of the RFID reader."							
RFID Passphrase								
Passphrase 🛜	The master password or phrase used to setup the authentication tokens for your RFID tags. Make sure to write this down!							
Show	Shows the Master Key.							
Set Master Key	Launches the Set Master Key dialog box, allowing the user to set the master key. Please note that when a master key is set, all cards programmed with the old key will be invalidated.							
Authentication Settings								
Enable Two-Factor Authentication ?	When selected, a registered user must scan a valid rfid card and enter a valid security code to activate the relay. The user name must match in both cases.							
Two Factor Timeout (in seconds) 🛜	The length of time (in seconds) during which the device will wait for the second factor when doing two-factor authentication.							
Relay Settings								
Activate Relay on Valid RFID 🛜	Activates the relay when a valid code is entered. This would likely be used to open a door.							
Activate DSR on Valid RFID 🛜	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.							
Buzzer Settings								
Buzz while Relay Active 💡	When selected, an audible buzz will indicate the relay is active.							
Buzz on Rejected RFID Card ?	When selected, a pattern will play on the buzzer to indicate an invalid code was entered.							
Sensor Settings								
Buzz on Door Open Timeout 🛜	When selected, the buzzer will beep until the on-board door sensor is deactivated.							
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. See the Operations Guide for more information.							
Sensor 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.							

Table 2-10. Sensor Page Parameters

Web Page Item	Description
DSR Open Timeout (in seconds) ?	The time (in seconds) the device will wait before it performs an action when the remote (DSR) door sensor is activated. The action(s) performed are based on the configured Remote Door Sensor Settings below.
Blacklist Settings	
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 Mesage 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.
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" audio file will be played to.
Multicast Port 🛜	The multicast port that the "blacklist" audio file 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.
Import Access List 🛜	After selecting an access list file, click on the Import Access List button to import the access list from the selected file.
Browse	Use this button to select a file to import.
Import Access List	This button imports an access list that it is in .xml format.
Export Access List ?	Click on the Export Access List button to export the current access list to a file.
Browse	Use this button to select a file to export.
Export Access List	This button exports the list of access records in xml format.
Access List	List of Access records.
Name ?	Tag user's name.
Valid From ?	Date and time in the form "DOWHH:MM". The field must contain a three- letter string indicating the day of week, Weekday (Wdy), Weekend (Wnd), or "All". The optional time is in 24 hour format and the range is inclusive.
Valid To ?	Date and time in the form "DOWHH:MM". The field must contain a three- letter string indicating the day of week, Weekday (Wdy), Weekend (Wnd), or "All". The optional time is in 24 hour format and the range is inclusive.
Blacklist ?	Mark this tag for immediate rejection and optional blacklist alerts.
Add	Launches the Configure Access Record edit box, allowing the user to add a new record.

Table 2-10. Sensor Page Parameters (continued)

Veb Page Item	Description
Edit	Launches the Configure Access Record edit box, allowing the user to make changes to an existing record.
Delete	Deletes a record.
Security Log	A file with a maximum of three log files, each 1 M, that records security actions.
Get Security Log	Downloads a file with a maximum of 3 log files, each 1 M.
Clear Security Log	Clears the on screen display of the log.
Refresh Log	Refreshes the on screen display of the log to show the most recent activity.
Save	Click the Save button to save your configuration settings.
Reboot	Click on the Reboot button to reboot the system.
Toggle Help	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

Table 2-10. Sensor Page Parameters (continued)

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

2.5.9 Enrollment Procedure

Welcome to the CyberData Keypad RFID, featuring two-factor authentication. This document illustrates the user friendly, intuitive process you will use to enroll your RFID cards and set keypad codes to enhance your security.

1. From the **Home Page** (Figure 2-24), click on the **RFID** menu button (Figure 2-24) to navigate to the **RFID** page (Figure 2-25).

Figure 2-24. From the Home Page, navigate to the RFID page

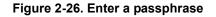
Click on the RFID menu button to navigate to the RFID page

Home Device		Sip RFID Sensor Audiofiles	
Current Status Serial Number: Mac Address: Firmware Version: Partition 2: Partition 3: Persition Forem	425000001 00:20:f7:03:ca:b3 v1.0.0b04 v1.0.0b04 v1.0.0b03	Admin Settings Username: admin Password: ••••• Confirm Password: •••••	Import Settings Choose File No file chosen Import Config
Booting From: Boot From Other Partition IP Addressing: IP Address: Subnet Mask: Default gw_addr:	10.10.0.119 255.0.00 10.0.0.1	Save Reboot Toggle Help	Export Settings
DNS Server 1: DNS Server 2: SIP Mode: Event Reporting: Primary SIP Server: Backup Server 1:	10.0.1.56 Enabled Disabled Not registered Not registered		

Figure 2-25. RFID Page

Home Device	Network	Sip RFID	Sensor	A	udiofiles	Events	s DSF	t Aut	oprov	Firmware
(Cybe	erDat	ta K	e	УŖ	ad	RF	ID		
Current Status				RFIE) Settin	gs				
Waiting for RFID tag				1	Name	Valid From	Valid To All	Blacklist		_
, i i i i i i i i i i i i i i i i i i i				1	Jason	All	All	No	Edit	Delete
RFID Passphrase				2		All	All	No	Add	Delete
Passphrase	· · · · ·	Show		3		All	All	No	Add	Delete
Set Master Key				4		All	All	No		
Authentication Catt						7.0	7.0	NO	Add	Delete
Authentication Sett				5		All	All	No	Add	Delete
Enable Two-Factor Authentication	4			6		All	All	No	Add	Delete
Relay Settings				7		All	All	No	Add	Delete
Activate Relay on Valid RFID				8		All	All	No		
Activate DSR on Valid RFID				0		All	All	NO	Add	Delete
Relay Timeout (seconds) 6				9		All	All	No	Add	Delete
Buzzer Settings				10		All	All	No	Add	Delete
Buzz while Relay Active				11		All	All	No	Add	Delete
Buzz on Rejected RFID Card									Auu	Delete
Sensor Settings				12		All	All	No	Add	Delete
Buzz on Door Open Timeout:				13		All	All	No	Add	Delete
Door Sensor Normally Closed: Sensor Open Timeout (in seconds	O Yes ● No s):0			14		All	All	No	Add	Delete
DSR Open Timeout (in seconds):				15		All	All	No		
Blacklist Actions									Add	Delete
				16		All	All	No	Add	Delete
Play Message to SIP Extension Dial Out SIP Extension	666			17		All	All	No	Add	Delete
Dial Out SIP ID	ext666			18		All	All	No		
Multicast Audio Message									Add	Delete
	234.6.6.6			19		All	All	No	Add	Delete
Multicast Port Times to Play Multicast Message	666			20		All	All	No	Add	Delete
miles to Play multicast message	<u> </u>			21		All	All	No	Add	Delete
Save Reboot Export RFID	Settings Toggle	Help								

2. From the **RFID** page (Figure 2-25), the user will be prompted for a Passphrase that will serve as the Master Key. Enter a passphrase (Figure 2-26), and copy it to a secure location.



RFID	RFID Passphrase			
Passph	rase	myTESTpassphr@se	Hide	
Set M	etter Key	Passphrase has not changed!		
		, 		

Click on the Set Master Key button

- 3. When the user clicks on the **Set Master Key** button (Figure 2-26), a **Set Master Key** dialog box will appear. See Figure 2-27.
- 4. In the dialog box, click on the Set Master Key button. See Figure 2-27.

Figure 2-27. Set Master Key dialog box will appear

Set Master Key
Are you sure you want to set a new master key? This will require that all existing tags be reprogrammed.
Cancel Set Marrier Key
Click on the Set Master Key button

5. The Master Key will be set. See Figure 2-28.

Figure 2-28. The Master Key will be set



6. To enroll a user, select an empty record and click on the **Add** button. See Figure 2-29.

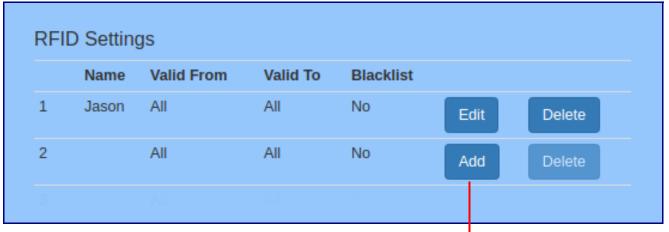
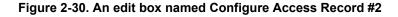


Figure 2-29. Select an empty record and click on the Add button

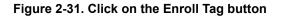
Select an empty record and click on Add button

7. This is action will launch an edit box named **Configure Access Record #2**. See Figure 2-30.



Configure Access	Record #2			×
Name Tag UID Key Code Valid From All Valid To All Blacklist Current Status: Waiting for RFID tag				
	Enroll Tag	Save Changes	Cancel	Toggle Help

8. Click on the Enroll Tag button, and place the card flat against the RFID reader. See Figure 2-31.



Configur	e Access Record #3	×
Name Tag UID Key Code Valid From Valid To Blacklist Current	All	? ? ? ? ?
) tag flat against reader	Save changes after programming!
	Enroll Tag	Save Changes Cancel Toggle Help

Click on the Enroll Tag button, and place the card flat against the RFID reader.

9. The Tag UID field will be populated. See Figure 2-32 and Figure 2-33.



Configur	e Ac	cess Re	cord #2			×
Name		s Smith		?		
Tag UID	04188	10242318	0	?		
Key Code				?		
Valid From	1			?		
Valid To				?		
Blacklist				?		
Current	Statu	s:				
Successful	y prog	ammed R	FID Tag uid=(04188102423180		
				Save	changes after programmin	g!
			Enroll Tag	Save Changes	Cancel Toggle Help	

The **Tag UID** field will be populated



Configu	e Acce	ess Record #2	×
Name Tag UID	James S 0418810		?
Key Code Valid From		UID	
Valid To Blacklist		— was scanned.	que ID of the tag that The UID is programmed nufacturer and is
Current			
Successful	ly progran	nmed RFID Tag uid=	04188102423180 Save changes after programming!
		Enroll Tag	Save Changes Cancel Toggle Help

The **Tag UID** field will be populated

- 10. Click on the Toggle Help button for assistance in populating the other fields. See Figure 2-34.
- 11. Move the mouse pointer to hover over the question mark, and a short description of the web page item will appear.

Configure Access	s Record #2			×
Name Tag UID Key Code Valid From All Valid To All Blacklist		? ? ? ? ? ?		
Current Status: Waiting for RFID tag				
	Enroll Tag	Save Changes	Cancel	Toggle Help

Figure 2-34. Use the Toggle Help button for assistance in populating the other fields

Move the mouse pointer to hover over the question mark, and a short description of the web page item will appear.

Use the **Toggle Help** button for assistance in populating the other fields.

12. Click on the Toggle Help button for assistance in populating the Name field. See Figure 2-35.

Configur	e Access R	ecord #2				×
Name Tag UID Key Code Valid From Valid To Blacklist Current Waiting for	All Status:	Nan Tag	? user's name ? ?			
		Enroll Tag	Save Changes	Cancel	Toggle	e Help

Figure 2-35. Click on the Toggle Help button for assistance in populating the Name fields

For assistance in populating the **Name** field, click on the **Toggle Help** button.

13. Use the **Toggle Help** button for assistance in populating the **Key Code** field. See Figure 2-36.

Figure 2-36. Use the Toggle Help button for assistance in populating the Key Code field

Configur	e Ac	ccess	Record #2			×
Name Tag UID Key Code Valid From Valid To Blacklist Current Waiting for	0410 1234 All All Stat	us:	3180 Key Code	? ? e e. Must be unique.		
Walting for		ug	Enroll Tag	Save Changes	Cancel	Toggle Help

Note In the **Key Code** field, make sure that the key code is unique. See Figure 2-37.

Configur	e Acce	ss Record #2		×	
Key Code Valid From Valid To Blacklist Current	Wdy08:30 Wdy18:00	2423180 D	? ? ? ? ? ?		
		Enroll Tag	Save Changes	Cancel Toggle Help	

Figure 2-37. Be certain that the key code is unique

In the **Key Code** field, make sure that the key code is unique.

14. Use the **Toggle Help** button for assistance in populating the **Valid From** field. See Figure 2-38.

Name James Smith ? Tag UID 041c8402423180 ? Key Code 123456 ? Valid From Wdy08:30 ? Valid To All Valid From Blacklist Date and time in the form Down HH:MM". The field must contain	<
Blacklist Date and time in the form	
Waiting for RFID tag a three-letter string indicating the day of week, Weekday (Wdy), Weekend (Wnd), or "All". The optional time is in 24 hour format and the range is inclusive. Toggle Help]

For assistance in populating the **Valid From** field, click on the **Toggle Help** button

- 15. Use the **Toggle Help** button for assistance in populating the **Valid To** field. See Figure 2-39.
- **Note** The **Enable NTP** setting on the **Device** page must be selected to limit the times valid for the RFID tags.

Figure 2-39. Use the Toggle Help button for assistance in populating the Valid To field	Figure 2-39	. Use the ⁻	Toggle Help	button for	assistance in	populating	the \	Valid To	field
---	-------------	------------------------	-------------	------------	---------------	------------	-------	----------	-------

Configur	e Access	Record #2		×
Name Tag UID Key Code Valid From Valid To Blacklist	James Smit 041c840242 654321 Wdy08:30 Wdy18:00		? ? ? ?	
Current Waiting for	Status: RFID tag	Date and time i "DOWHH:MM" a three-letter st of week, Week (Wnd), or "All".	in the form The field must contain tring indicating the day day (Wdy), Weekend The optional time is in and the range is	ncel Toggle Help
		For oppiston in	nonulating the Valid Ta Sald	aliak on the Teggie Help button

For assistance in populating the Valid To field click on the Toggle Help button

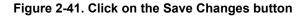
16. Click on the **Toggle Help** button for assistance in populating the **Blacklist** check box. See Figure 2-40.

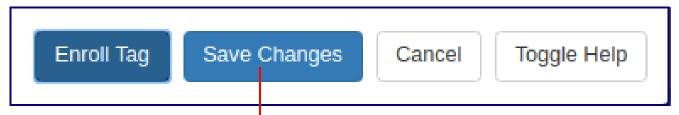
Figure 2-40. Click on the Toggle Help button for assistance in populating the Blacklist check box

Configur	e Access	Record #2			×
Name	James Smit		?		
Tag UID Key Code	041c840242 123456	23180	?		
Valid From	-		?		
Valid To Blacklist	Wdy18:00		?		
Current	Status:	Blacklist			
Waiting for	RFID tag	Mark this tag for and optional bla	immediate rejection cklist alerts.		
		Enroll Tag	Save Changes	Cancel	Toggle Help

- For assistance in populating the **Blacklist** check box, click on the **Toggle Help** button

17. Click on the **Save Changes** button (Figure 2-41), and your record will appear in the web page list. See Figure 2-42.





Click on the Save Changes button

Figure 2-42.	Your record w	vill appear in the	web page list
--------------	---------------	--------------------	---------------

RFID) Settings	i					
	Name		Valid From	Valid To	Blacklist		
1	Jason		All	All	No	Edit	Delete
2	James	Smith	Wdy08:30	Wdy18:00	No	Edit	Delete
3			All	All	No	Add	Delete
4			All	All	No	Add	Delete

Your record will appear in the web page list

- **Note** The CyberData RFID Keypad will accept either an RFID card or a key code. If **Two Factor Authorization** is enabled, the RFID Keypad will require you to use an RFID card and to also enter a key code into the keypad to gain entry.
- 18. To delete a record, click on the **Delete** button. See Figure 2-43.

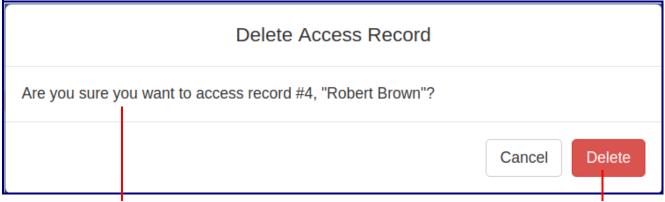
Figure 2-43.	To delete	a record,	select the	Delete button
--------------	-----------	-----------	------------	---------------

RFID	Settings					
	Name	Valid From	Valid To	Blacklist		
1	Jason	All	All	No	Edit	Delete
2	James Smith	Wdy08:30	Wdy18:00	No	Edit	Delete
3	Maria Garcia	All	All	No	Edit	Delete
4	Robert Brown	All	All	No	Edit	Delete

To delete a record, click on the **Delete** button.

- 19. You will be prompted to delete the record. See Figure 2-44.
- 20. Click on the **Delete** button to confirm the deletion. See Figure 2-44.

Figure 2-44. You will be prompted to delete the record



You will be prompted to delete the record.

Click on the Delete button to confirm the deletion

21. The record will no longer appear in your settings. See Figure 2-45.

RFID	Settings						
	Name	Valid From	Valid To	Blacklist			
1	Jason	All	All	No	Edit	Delete	
2	James Smith	Wdy08:30	Wdy18:00	No	Edit	Delete	
3	Maria Garcia	All	All	No	Edit	Delete	
4		All	All	No	Add	Delete	

22. To export the RFID records, to provide a backup copy, or to share the enrolled tags with another device, click on the **Export RFID Settings** button. See Figure 2-46.

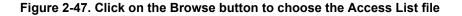
Figure 2-46. Click on the Export RFID Settings button



Click on the Export RFID Settings button

Exporting RFID will create an xml file in the directory specified in your browser's **Downloads** location. Devices that require this file may use **Import Config** setting on the **Home Page**, or use Autoprovisioning (see the Operations Guide.)

To share the configuration via Import Config, navigate to the RFID page of the second device, and click on the Browse (or Choose File) button to choose the Access List file. See Figure 2-47.



Import Access List	Export Access List
Browse No file chosen Import Access List	Export Access List
Access List	

Click on the Browse button to choose the Access list file

Click on the **Import Access List** button to import the records

24. Click on the **Import Config** button (Figure 2-47) to import the records, and they will be added to the RFID page. See Figure 2-48.

Figure 2-48. The imported records will be added to the RFID page

RFID	Settings						
	Name	Valid From	Valid To	Blacklist			
1	Jason	All	All	No	Edit	Delete	
2	James Smith	Wdy08:30	Wdy18:00	No	Edit	Delete	
3	Maria Garcia	All	All	No	Edit	Delete	
4		All	All	No	Add	Delete	

2.5.9.1 Optional RFID Reader Stand—used on the desktop for a dedicated reader for the enrollment process

Note This requires either the 011425 or 011426 reader purchase as shown in Figure 2-49.

011423A is an optional programming stand. This stand is especially useful for users who would like to have a CyberData RFID Reader dedicated to enrolling RFID cards. Follow the enrollment process documented in Section 2.5.9, "Enrollment Procedure".

Figure 2-49. Optional RFID Reader Stand



2.5.10 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 device is removed from the case.

Each sensor can trigger the following actions:

- Activate the relay until the sensor is deactivated
- Call an extension, with optional pre-recorded audio
- **Note** Calling a preset extension can be set up as a point-to-point call, but currently can't send delayed DTMF tones.
- 1. Click Sensor menu button to open the Sensor page (Figure 2-50).

Figure 2-50. Sensor Configuration Page

	Cy	hor	·Da	ta k	Keypa	nd E	FIL	`	
	Сy		Da		cype				
Door Sensor Se	ttings				Intrusion Se	ensor Se	ttings		
Door Sensor Settings Intrusion Sensor Settings Door Sensor Normally Closed: • Yes • No Activate Relay: • Door Open Timeout (in seconds): • Make call to extension: • Activate Relay: Dial Out Extension: • Make call to extension: Dial Out ID: • Dial Out Extension: 204 Dial Out ID: • id204 Play recorded audio: •									
Repeat Sensor Message:	0								
Save Reboot Tog	le Help								

- 2. On the Sensor page, enter values for the parameters indicated in Table 2-11.
- **Note** The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Web Page Item	Description
Door Sensor Settings	
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.
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 Dial Out Extension 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.
Play recorded audio ?	When selected, the device will call the Dial Out Extension and play an audio file to the phone answering the SIP call (corresponds to Door Ajar on the Audiofiles page).
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.
Intrusion Sensor Settings	
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 Dial Out Extension 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.
Play recorded audio ?	When selected, the device will call the Dial Out Extension and play an audio file (corresponds to Intrusion Sensor Triggered on the Audiofiles page) to the phone answering the SIP call when the intrusion sensor is activated.
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.

Table 2-11. Sensor Page Parameters

Web Page Item	Description
Test Door Sensor	Click the Test Door Sensor button to test the door sensor.
Test Intrusion Sensor	Click the Test Intrusion Sensor button to test the Intrusion sensor.
	Click the Save button to save your configuration settings.
Save	Note: You need to reboot for changes to take effect.
Reboot	Click on the Reboot button to reboot the system.
Toggle Help	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

Table 2-11. Sensor Page Parameters (continued)

2.5.11 Configure the Audio Configuration Parameters

The **Audiofiles** page is used to add custom audio to the board. User uploaded audio will take precedence over the audio files shipped with the device.

1. Click on the Audiofiles menu button to open the Audiofiles page (Figure 2-51).

Figure 2-51. Audiofiles Configuration Page

Home Device	Network Sip R	FID Sensor	Audiofiles	Events	DSR	Autoprov	Firmware			
CyberData Keypad RFID										
Cysci Bata Reypud III IB										
		Available Space	ce: 1405MB							
Intrusion Sensor Triggered:	Currently set to: defau	ult Brows	e No file chosen	1		Delete	Save			
Door Ajar:	Currently set to: defau	ult Brows	e No file chosen	i		Delete	Save			
	Currently set to: defau	ult Brows	e No file chosen	1		Delete	Save			
Blacklist Message:										

- 2. On the Audiofiles page, enter values for the parameters indicated in Table 2-12.
- **Note** The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-12. Audiofiles Page Parameters

Web Page Item	Description
Available Space	Shows the space available for the user to save custom audio files if they want to change the message when the door or sensor is triggered.
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.
Browse	Click on the Browse button to navigate to and select an audio file.
Play	The Play button will play that audio file.
Delete	The Delete button will delete any user uploaded audio and restore the stock audio file.
Save	The Save button will download a new user audio file to the board once you've selected the file by using the Browse button. The Save button will delete any pre-existing user-uploaded audio files.

2.5.11.1 User-created Audio Files

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

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

You can use the free utility *Audacity* to convert audio files into this format. See Figure 2-52 through Figure 2-54.

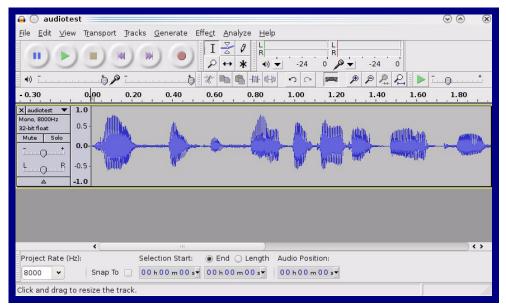


Figure 2-52. Audacity 1

Figure 2-53. Audacity 2

🔒 🕞 Edit Metadata 🚃		$\odot \odot \otimes$
Use arrow keys (or RETURN k	ey after editing) to navigate fi	elds.
Tag Name	Tag Value	
Artist Name		
Track Title		
Album Title		
Track Number		
Year		
Genre		
Comments		
Add	<u>Bemove</u>	r
Genres	Template	
E <u>d</u> it Rese <u>t</u>	Load Save.	S <u>e</u> t Default
	0	Cancel

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

• WAV (Microsoft) signed 16 bit PCM.

🔒 💮 Export File			$\odot \odot $
Name: audiotes	t.wav		
Save in <u>f</u> older: 🛅 tmp			*
✓ Browse for other folders			
	,		
o/ tmp/			Create Fo <u>l</u> der
Places	Name		✓ Modified <a>
🎮 Search	🛅 cscope.4371		Yesterday at 14:30
🛞 Recently Used	🛅 kde-na		Yesterday at 14:26
🛅 na	🛅 kde-root		Yesterday at 14:26
🛅 Desktop	🛅 ksocket-na		09:20
🐻 File System	🛅 orbit-na		Yesterday at 14:32
🔯 250.1 GB Media	ssh-CIPQVD3392		Yesterday at 14:26 🚊
	► v814422		Yesterday at 15:45
₽ Add ≈ <u>R</u> emove)		WAV (Microsoft) signed 16 bit PCM 🔹
	<u>c</u>	ptions	
			⊘ Cancel Save
			/

Figure 2-54. WAV (Microsoft) signed 16 bit PCM

WAV (Microsoft) signed 16 bit PCM

2.5.12 Configure the Events Parameters

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

1. Click on the Events menu button to open the Events page (Figure 2-55).

Figure 2-55. Event Configuration Page

Home	Device	Network	Sip	RFID	Sensor	Audiofiles	Events	DSR	Autoprov	Firmware
		Cv	ber	Dat	ta K	еура	d R	FID		
Enable Event G	eneration:									
						Event Serv	er			
Events						Server IP Address:	10.0.0.250			
Enable Call Sta	rt Events:						8080		_	
	minated Events:							0		
Enable Relay A	ctivated Events:					Server ORL.	xmlparse_engir	le		
	eactivated Event									
Enable Ring Ev	ents:									
	st Start Events:									
Enable Multicas	st Stop Events:									
Enable Power C	On Events:									
Enable Sensor	Events:									
Enable Remote	Relay Events:									
	nd Heartbeat:									

- 2. On the **Events** page, enter values for the parameters indicated in Table 2-13.
- **Note** The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

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.
	Note: Enabling Event Generation requires a reboot for the changes to take effect.
Events	
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.
Enable Relay Deactivated Events ?	When selected, the device will report relay deactivation.
Enable Ring Events ?	When selected, the device will report when it starts ringing upon an incoming SIP call. A Ring Event will not be generated when Auto-Answer Incoming Calls is enabled on the Device page.
Enable Multicast Start Events ?	When selected, the device will report when the device starts playing a multicast audio stream.
Enable Multicast Stop Events ?	When selected, the device will report when the device stops playing a multicast audio stream.
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 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.
Event Server	Note : Changing an Event Server setting requires a reboot for the changes to take effect.
Server IP Address ?	The IPv4 address of the event server in dotted decimal notation.
Server Port 🛜	Specify the event server port number. The supported range is 0-65536. Enter up to 5 digits.
Server URL ?	Generally, the destination URL is the name of the application that receives the events and the string in the HTTP POST command. It can be a script used to parse and process the HTTP POST events. Enter up to 127 characters.
	Click the Save button to save your configuration settings.
Save	Note: You need to reboot for changes to take effect.
Reboot	Click on the Reboot button to reboot the system.

Table 2-13. Events Page Parameters

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

Table 2-13. Events Page Parameters(continued)

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

Note Selecting particular events does not require a reboot for the changes to take effect.

2.5.12.1 Example Packets for Events

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

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

Here are example packets for every event:

```
POST xmlparse engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 197
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>POWERON</event>
</cyberdata>
POST xmlparse engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 199
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>HEARTBEAT</event>
</cyberdata>
POST xmlparse engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 196
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>BUTTON</event>
</cyberdata>
POST xmlparse engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 201
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>CALL ACTIVE</event>
</cyberdata>
POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
```

```
User-Agent: CyberData/1.0.0
Content-Length: 205
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>CALL TERMINATED</event>
</cyberdata>
POST xmlparse engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 197
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>RINGING</event>
</cyberdata>
POST xmlparse engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>MULTICAST START
<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>
```

2.5.13 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 2-56).

- **Note** When **Activate DSR on Valid RFID** is enabled, a swipe of a valid RFID card will activate Relay 2.
- 1. Click on the DSR menu button to open the DSR page (Figure 2-56).

Figure 2-56. DSR Page (not associated with any DSRs)

Home	Devic	e Network	Sip	RFID	Sensor	Audiofi	iles E	vents	DSR	Autoprov	Firmware
		Су	ber	Data	K	eyp	bad	R	FID		
Remote Not associa		Settings _{DSRs}									
Save F	Reboot To	oggle Help						dev	/ice is no	default page ot associat use see the	ed with any
				Discove	ered Re	emote R	elays	mo	re setting	gs and option	
Product Type	IP Address	MAC Address	Serial Number	Name	Version					when the de with a DSR	
DoorLock	10.10.1.45	00:20:F7:02:A7:9A	27000004	LOCK270000004	V2.2AM	View	Associate				
DoorLock	10.10.1.19	00:20:F7:03:54:BE	375000016	LOCK375000016	V4.8T	View	Associate				
	10.10.0.45			LOCK375000046	V4.8T		_				

- 2. On the DSR 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. DSR Configuration Parameters (not associated with any DSRs)

Web Page Item	Description
Remote Relay Settings	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 Not associated with any DSRs .
	Click the Save button to save your configuration settings.
Save	Note: You need to reboot for changes to take effect.
Reboot	Click on the Reboot button to reboot the system.
Toggle Help	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.
Discovered Remote Relays	The Discovered Remote Relays section lists all of the networked door strike relays on the network. To associate your device with a door strike relay, click on the Associate 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.
Discover	Use this button to search for and find any remote relays that are available on the network.
View	Use this button to view the settings of a remote relay that has been "discovered" after pressing the Discover button.
Associate	Use this button to associate the remote relay with the device. Only one relay may be associated with a device.
Disassociate	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.

2.5.14 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 2-57.

Figure 2-57. Autoprovisioning Page

Home Devi	ce Network	Sip RFID	Sensor	Audiofiles	Events	DSR	Autoprov	Firmware
	Cyl	berDa	ta K	еура	d R	FID)	
Autoprovisioning happen The device will first look f f these haven't been con	r: me: pdate (in minutes): 0 HMM): e (in minutes > 10): 0 now to use autoprovision s on boot. or a configured server	oning to configure your dev address and filename. In autoprovisioning server i		^o options and try to d	ownload '0020170	03cab3.xml' ar	nd if this fails, '0000	00cd.xml'.
Download Template	utoprovd: no autoprovo utoprovisioning on boo utoprov found server=' utoprov looking for http utoprov: https downloa utoprov looking for 000 utoprov looking for http	t ' in dhcp option 43 ::///0020f703cab3.xml d failed i000cd.xml at ::///000000cd.xml						Î

- 2. On the **Autoprovisioning** page, you may enter values for the parameters indicated in Table 2-15.
- **Note** The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Web Page Item	Description
Enable Autoprovisioning ?	The device will automatically fetch a configuration file, also known as the 'autoprovisioning file', based on the configured settings below.
Autoprovisioning Server 🛜	Enter the IPv4 address of the provisioning server in dotted decimal notation.
Autoprovisioning Filename 🛜	The autoprovisioning filename is the configuration filename. The default autoprovisioning filename is in the format of <mac address="">.xml</mac> .
	Supported filename extensions are .txt, and .xml. The current filename is denoted by an asterisk at the bottom of the Autoprovisioning Page . Enter up to 256 characters.
	A file may have any name with an xml extension. If a file name is entered, the device will look for the specified file name, and only that file.
Use tftp ?	The device will use TFTP (instead of http) to download autoprovisioning files.
Username 🛜	The username used to authenticate with an autoprovisioning server. Leave this field blank to disable authentication.
Password ?	The password used to authenticate with an autoprovisioning server. Leave this field blank to disable authentication.
Autoprovisioning Autoupdate (in minutes) ?	The reoccurring time (in minutes) the device will wait before checking for new autoprovisioning files. Enter up to 6 digits. A value of 0 will disable this option.
Autoprovision at time (HHMMSS) 🛜	The time of day the device will check for a new autoprovisioning file. The time must be 6 characters in length and in HHMMSS format. An empty value will disable this option.
Autoprovision when idle (in minutes > 10) ?	The idle time (in minutes greater than 10) after which the device will check for a new autoprovisioning file. Enter up to 6 digits. A value of 0 will disable this option.
Save	Click the Save button to save your configuration settings.
Reboot	Click on the Reboot button to reboot the system.
Toggle Help	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

Table 2-15. Autoprovisioning Page Parameters

Web Page Item	Description
Download Template	Press the Download Template button to create an autoprovisioning file for the device. See Section 2.5.14.3, "Download Template Button"
Autoprovisioning log	The autoprovisioning log provides information about the latest autoprovisioning attempt (i.e. dhcp options and server accessed and files parsed or not found).

Table 2-15. Autoprovisioning Page Parameters (continued)

2.5.14.1 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 2.5.14.2, "Sample dhcpd.conf" for an example of how to configure dhcpd to offer autoprovisioning server addresses. If multiple options are set, the device will attempt to download autoprovisioning files from every server.

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

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

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

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

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

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

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

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

The file 0020f7123456.xml contains:

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

</specific>

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

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

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

Checking for New The device will always check for an autoprovisioning files on boot but it can be configured to also Autoprovisioning check after a periodic delay, when idle, or at a specified time. When one of these options is set, the Files after Boot 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.

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

Table 2-16. Autoprovisioning File Name

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

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

For example:

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

The autoprovisioning filename is set to "cyberdata/"

On boot, the device will try to download:

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

...and if this fails:

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

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

Autoprovisioning <FirmwareSettings>

```
Firmware Updates <FirmwareFile>505-uImage-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-uImage-[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>IndoorIntercom31SW</ProductString> <ProductString>IndoorIntercom31SW</ProductString> <ProductString>IndoorKeypad31</ProductString> <ProductString>OfficeRinger31</ProductString> <ProductString>OfficeRinger31SW</ProductString> <ProductString>OfficeRinger31SW</ProductString> <ProductString>OutdoorIntercom31SW</ProductString> <ProductString>OutdoorIntercom31</ProductString> <ProductString>OutdoorIntercom31</ProductString> <ProductString>OutdoorIntercom31SW</ProductString> <ProductString>OutdoorKeypad31</ProductString> <ProductString>OutdoorKeypad31</ProductString> <ProductString>Strobe31</ProductString> <ProductString>Strobe31</ProductString></productString></productString></productString></productString></productString></productString></productString></productString></productString></productString></productString></productString></productString></productString></productString></productString></productString></productString></productString></productString></productString></productString> Autoprovisioning H Example 1

Dning 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:

00000cd.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.
- 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:// autoprovtest.server.net." Device2 sets the SIP User ID to **500**, the password to **ext500**, and the dialout extension to **555**.

Autoprovisioning Here is another ex 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 **10.0.253**, 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)

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** page or by changing the autoprovisioning file with "**default**" set as the file name.

2.5.14.2 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;
                                   "voiplab";
   option domain-name
   option domain-name-servers
                                   10.0.0.252;
    option time-offset
                                   -8;
                                                   # Pacific Standard Time
                                                                     # OPTION 72
#
     option www-server
                                    99.99.99.99;
                                      "10.0.1.52";
                                                                     # OPTION 66
#
     option tftp-server-name
#
     option tftp-server-name
                                     "http://test.cyberdata.net";
                                                                     # OPTION 66
                                                                     # OPTION 150
#
     option option-150
                                      10.0.0.252;
# 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; }

2.5.14.3 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 prompting you to save a configuration file (**.xml**) to a location on your computer (Figure 2-58). The configuration file is the basis for the default configuration settings for your unit).
- 3. Choose a location to save the configuration file and click on OK. See Figure 2-58.

🕘 Ope	ening 0020f702bf18.xml 🔹 🕈 🗆 🗙
You have chosen t	o open:
0020f702bf	18.xml
which is: XML from: https://	. document (11.3 KB) 10.10.1.50
What should Fir	efox do with this file?
Open with	Text Editor (default)
⊖ <u>S</u> ave File	
🗌 Do this <u>a</u> ut	comatically for files like this from now on.
	Cancel OK

Figure 2-58. Configuration File

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

2.6 Upgrade the Firmware

Note CyberData strongly recommends that you do not upgrade the firmware when the device is likely to be in use.

To upgrade the firmware of your device:

- 1. Download the latest firmware file from the **Downloads** tab at the following webpage: <u>http://www.cyberdata.net/voip/011426/</u>
- 2. Unzip the firmware version file. This file may contain the following:
- Firmware file
- Release notes
- Autoprovisioning template
- 3. Log in to the **Home** page as instructed in Section 2.5.4, "Log in to the Configuration Home Page".
- 4. Click on the Firmware menu button to open the Firmware page (Figure 2-59).

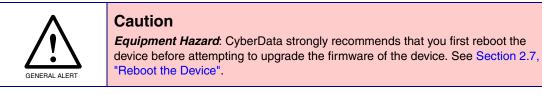


Figure 2-59. Firmware Page



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

6. Select the firmware file. This reveals the **Upload** button (Figure 2-60).

	Hom	ne	Device	Network	Sip	RFID	Sensor	Audiofiles	Events	DSR	Autoprov	Firmware
				Cyt	ber	Dat	a Ke	eypa	d Rl	FID		
				-								
Г	Brow	vse ad										
	Uplo	oad P	rogress							٦		
	Uplo	oad P	ost Proc	essing			-					
		CUS M	essages ^{ed}									
Upl	load b	outton	State	us Messag	jes	Uplo	ad Post P	rocessing ba	ar U	pload Pi	r ogress bar	

Figure 2-60. Upload Button

- 7. Click on the **Upload** button. After selecting the **Upload** button, you will see the progress of the upload in the **Upload Progress** bar.
- 8. When the upload is complete, you will see the words Upload finished under Status Messages.
- 9. At this point, you will see the progress of the upload's post processing in the **Upload Post Processing** bar.
- **Note** Do not reboot the device before the upgrading process is complete.
- 10. When the process is complete, you will see the words **SWUPDATE Successful** under **Status Messages**.
- 11. The device will reboot automatically.
- 12. The **Home** page will display the version number of the firmware and indicate which boot partition is active.

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

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

Table 2-17. Firmware Page Parameters

2.7 Reboot the Device

To reboot the device, complete the following steps:

- 1. Log in to the **Home** page as instructed in Section 2.5.4, "Log in to the Configuration Home Page".
- 2. Click on the **Reboot** button on the **Home** page (Figure 2-61). A normal restart will occur.

Figure 2-61. Home Page

Home	Device	Network	Sip	RFID	Sensor	Audiofiles	Events	DSR	Autoprov	Firmware
		Cyt	oer	Dat	a Ko	eypa	d R	FID		
Current S	tatus	-		Admin	Settings		Im	port Set	tings	
Serial Number: Mac Address: Firmware Version Partition 2: Partition 3:	n: V V	26000001 0:20:f7:03:ca:b3 1.0.0 1.0.0 1.0.0		Username: Password: Confirm Pass	admin ••••• sword: •••••			OWSE No	file chosen	
Booting From: Boot From Othe	pa	artition 2		Save Re	boot Toggle H	Help		port Set	tings	
IP Addressing: IP Address: Subnet Mask: Default gw_addr DNS Server 1: DNS Server 2:	25 : 10	0.10.0.119 55.0.0.0 0.0.0.1 0.0.1.56					Đ	sport Config		
SIP Mode: Event Reporting		nabled isabled								
Primary SIP Serv Backup Server 1 Backup Server 2	: N	ot registered ot registered ot registered								

Reboot

2.8 Command Interface

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

2.8.1 Command Interface Post Commands

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

Device Action	HTTP Post Command ^a
Reboot	wgetuser adminpassword adminauth-no-challengequiet - O /dev/nullno-check-certificate "https://10.10.1.154/command" post-data "request=reboot"
Place call to extension (example: extension 600)	wgetuser adminpassword adminauth-no-challengequiet - O /dev/nullno-check-certificate "https://10.10.1.154/command" post-data "request=call&extension=600"
Test Relay	wgetuser adminpassword adminauth-no-challengequiet - O /dev/nullno-check-certificate "https://10.10.1.154/command" post-data "request=test_relay"
Swap boot partitions	wgetuser adminpassword adminauth-no-challengequiet - O /dev/nullno-check-certificate "https://10.10.1.154/command" post-data "request=swap_boot_partition"

Table 2-18. Command Interface Post Commands

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

Appendix A: Mounting the SIP RFID/ Keypad Secure Access Control Endpoint

A.1 Mounting Components

Before you mount the SIP RFID/Keypad Secure Access Control Endpoint, make sure that you have received all the parts for each SIP RFID/Keypad Secure Access Control Endpoint. Refer to the following tables.

Quantity	Part Name	Illustration
1	T-15H Torx Key	
4	Security Torx Screw	
	Table A-2. Optional Accessor	ies (for gooseneck mounting)
Quantity	Part Name	Illustration
4	Carriage bolt nuts	
4	Carriage bolts	
4	Carriage bolt washers	O(0)O

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

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

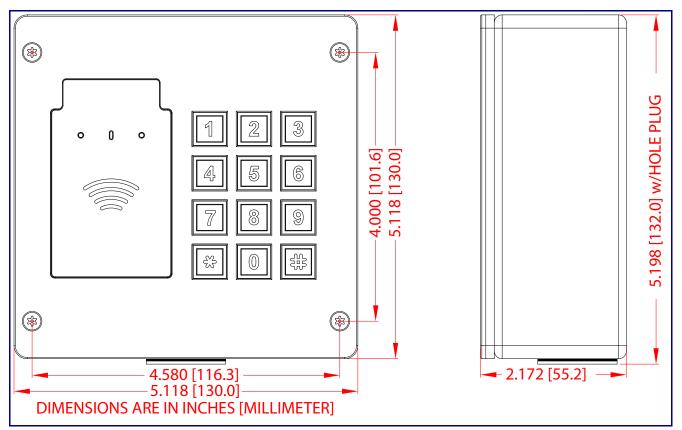


Figure A-1. Unit Dimensions—Front and Side View

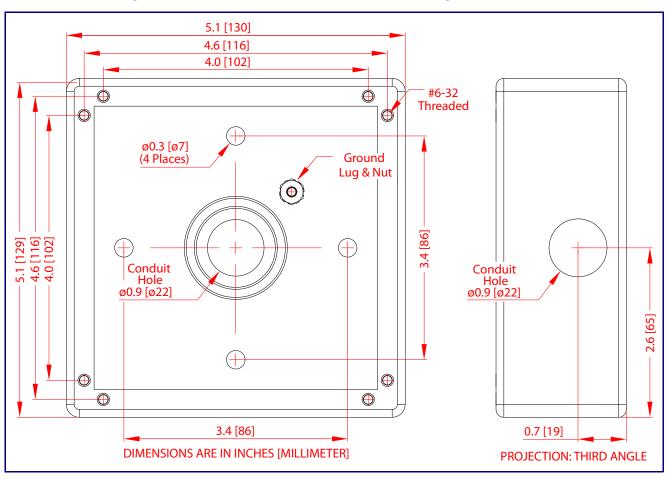


Figure A-2. Unit Dimensions—Rear View with Mounting Hole Locations

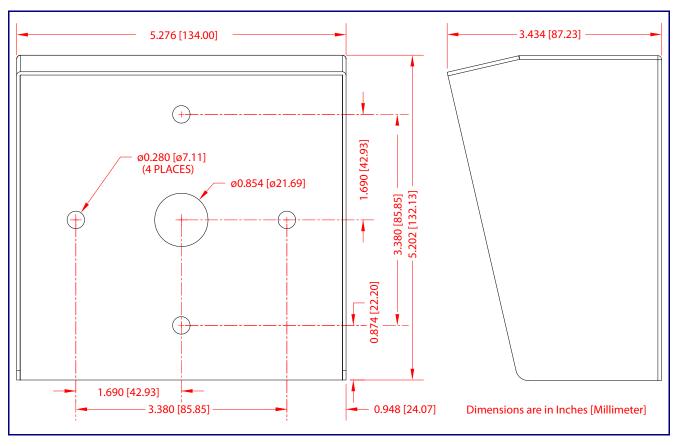


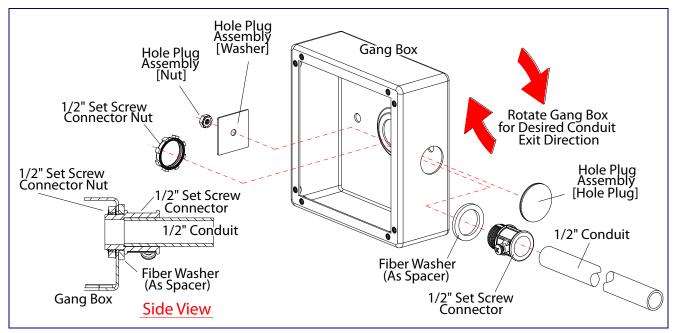
Figure A-3. Shroud Dimensions—Front and Side View with Mounting Hole Locations

A.3 Network Cable Entry Restrictions

A.3.1 Conduit Mounting Restrictions (Side Entry)

See Figure A-4 for the conduit mounting restrictions (side entry).





A.4 Service Loop Cable Routing

Figure A-5 and Figure A-6 illustrate a service loop cable routing option for the SIP RFID/Keypad Secure Access Control Endpoint.

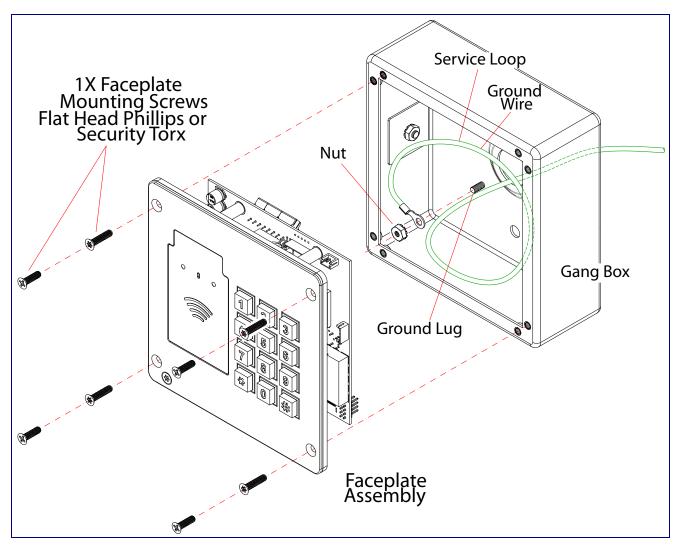


Figure A-5. Ground Cable Service Loop Routing

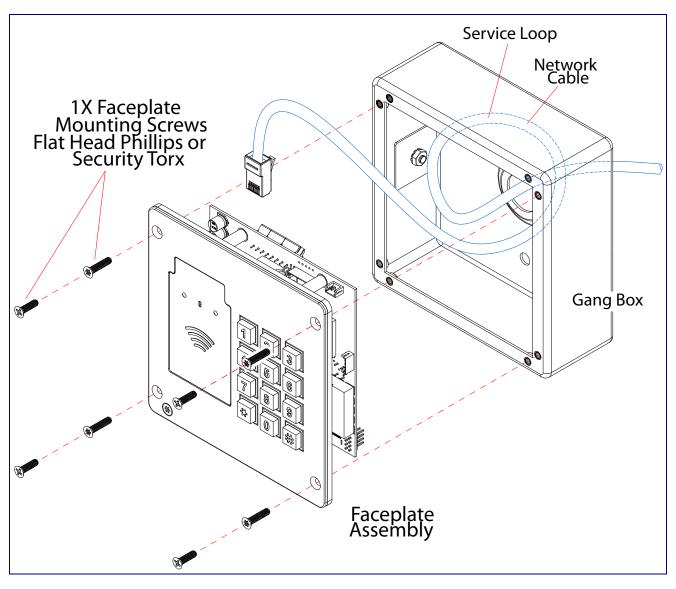


Figure A-6. Network Cable Service Loop Routing

A.5 Securing the Intercom

Figure A-7 illustrates how to secure the SIP RFID/Keypad Secure Access Control Endpoint with Torx screws.

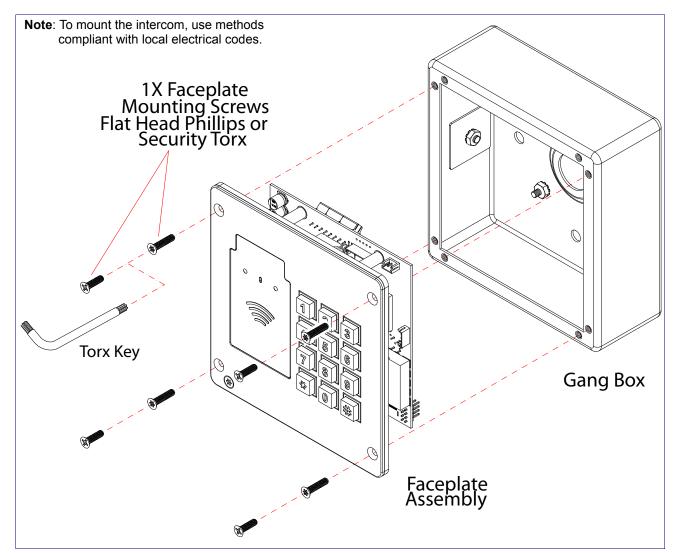
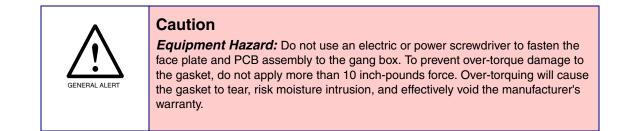


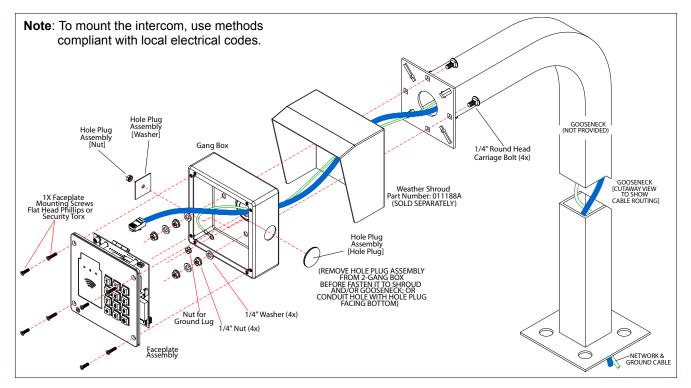
Figure A-7. Securing the Intercom



A.6 Additional Mounting Options

A.6.1 Goose Neck Mounting Option (Not Provided)

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





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/011426/

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/011426/

C.3 Contact Information

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

Sales Sales 831-373-2601, Extension 334

TechnicalThe fastest way to get technical support for your VoIP product is to submit a VoIP TechnicalSupportSupport form at the following website:

http://support.cyberdata.net/

The Support Form initiates a ticket which CyberData uses for tracking customer requests. Most importantly, the Support Form tells us which PBX system and software version that you are using, the make and model of the switch, and other important information. This information is essential for troubleshooting. Please also include as much detail as possible in the **Comments** section of the Support Form.

Phone: (831) 373-2601, Extension 333

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 11

Α

activate relay (door sensor) 66 activate relay (intrusion sensor) 66 activity LED 21 address, configuration login 29 alternative power input 6 announcing a device's IP address 23 audio configuration 68 audio configuration page 68 audio encodings 5 audio files, user-created 69 autoprovision at time (HHMMSS) 80 autoprovision when idle (in minutes > 10) 80 autoprovisioning 81 download template button 81 setting up a TFTP server 104 autoprovisioning autoupdate (in minutes) 80 autoprovisioning configuration 79, 80 autoprovisioning filename 80 autoprovisioning server (IP Address) 80

B

backup SIP server 1 38 backup SIP server 2 38 backup SIP servers, SIP server backups 38

С

changing the web access password 32 Cisco SRST 39 command interface 94 commands 94 concrete wall mounting option (not provided) 103 conduit mounting option (not provided) 103 configurable parameters 33, 35 configuration audio 68 default IP settings 25 door sensor 42, 65 intrusion sensor 42, 65 network 35 SIP 37 configuration home page 29 configuration page configurable parameters 33, 35 contact information 106 contact information for CyberData 106 current network settings 36 CyberData contact information 106

D

default gateway 25 intercom settings 107 IP address 25 subnet mask 25 username and password 25 web login username and password 29 default gateway 25, 35, 36 default intercom settings 24 default IP settings 25 default login address 29 device configuration 32 device configuration parameters 80 the device configuration page 79 device configuration page 32 device configuration parameters 33 device configuration password changing for web configuration access 32 **DHCP** Client 5 dial out extension (door sensor) 66 dial out extension (intrusion sensor) 66 dial out extension strings 41 dimensions 6,96 shroud dimensions and mounting hole locations 98 unit dimensions-front and side view 96 unit dimensions-rear view and mounting hole locations 97 discovery utility program 29 DNS server 36 door sensor 65, 66 activate relay 66 dial out extension 66 door open timeout 66 door sensor normally closed 66 download autoprovisioning template button 81 DTMF tones (using rfc2833) 41

E

electric screwdriver 102 ethernet I/F 6 expiration time for SIP server lease 38, 39 export settings 30

F

factory default settings 24 fastening, gang box 102 firmware where to get the latest firmware 90

G

gang box, fastening 102 gasket, avoid over-torque damage 102 get autoprovisioning template 81 goose neck mounting option (not provided) 103 ground cable installation 100

Η

home page 29 http POST command 94 http web-based configuration 5

identifying your product 1 import settings 30 import/export settings 30 installation, typical intercom system 2 intrusion sensor 65, 66 dial out extension 66 IP address 25, 35, 36 IP addressing default IP addressing setting 25

J

J3 terminal block, 16 AWG gauge wire 11

L

lease, SIP server expiration time 38, 39 LED green link LED 21 yellow activity LED 21 link LED 21 Linux, setting up a TFTP server on 104 local SIP port 39 log in address 29

Μ

mounting 95 additional mounting options 103 concrete wall mounting option (not provided) 103 conduit mounting option (not provided) 103 goose neck mounting option (not provided) 103 ground cable installation 100 optional accessories 95 overview of installation types 95 rear conduit network cable entry restrictions (without shroud) 100 securing the intercom 102 service loop cable routing 100 side conduit network cable entry restrictions 99 mounting components 95 multicast configuration 68

Ν

navigation (web page) 26 navigation table 26 network configuration 35 Nightringer 11, 89 NTP server 33, 34

0

on-board relay 6, 12

Ρ

part number 6 parts list 8 password for SIP server login 38 login 29

restoring the default 25 payload types 6 point-to-point configuration 41, 64 port local SIP 39 remote SIP 39 POST command 94 power input 6 alternative 6 power screwdriver 102 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) 100 reboot 92 remote SIP port 39 reset test function management button 22 resetting the IP address to the default 95, 105 restoring factory default settings 24, 107 RJ-45 20 rport discovery setting, disabling 39 RTFM button 22 RTFM jumper 22, 23, 24 RTP/AVP 5

S

sales 106 securing the device 102 sensor setup page 42, 65, 77 sensor setup parameters 42, 65 sensors 66 server address, SIP 38 service 106 service loop cable routing 100 setting up the device 11 settings, default 24 shroud dimensions and mounting hole locations 98 side conduit network cable entry restrictions 99 SIP

enable SIP operation 38

local SIP port 39 user ID 38 SIP configuration 37 SIP configuration parameters outbound proxy 39 registration and expiration, SIP server lease 38, 39 unregister on reboot 39 user ID, SIP 38 SIP registration 39 SIP remote SIP port 39 SIP server 38 password for login 38 SIP servers supported 5 unregister from 39 user ID for login 38 SIP server configuration 38 SRST 39 subnet mask 25, 35, 36 supported protocols 5

T

tech support 106 technical support, contact information 106 terminal block, 16 AWG gauge wire 11 TFTP server 5, 104

U

unit dimensions—front and side view 96 unit dimensions—rear view and mounting hole locations 97 user ID for SIP server login 38 username changing for web configuration access 32 default for web configuration access 29 restoring the default 25

V

VLAN ID 36 VLAN Priority 36 VLAN tagging support 36 VLAN tags 36

W

warranty policy at CyberData 106

web access password 25 web access username 25 web configuration log in address 29 web page navigation 26 web page navigation 26 wget, free unix utility 94 Windows, setting up a TFTP server on 104 wiring the circuit 13 devices less than 1A at 30 VDC 13