



SIP Call Button Operations Guide

Part #011049, 011491

Document Part #932062A
for Firmware Version 22.0

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

SIP Call Button Operations Guide 932062A
Part # 011049, 011491

COPYRIGHT NOTICE:

© 2024, CyberData Corporation, ALL RIGHTS RESERVED.

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

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

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

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

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



Technical Support

The fastest way to get technical support for your VoIP product is to submit a VoIP Technical Support form at the following website:

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

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

Email: support@cyberdata.net



Fax: (831) 373-4193

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

Revision Information

Revision 932062A, which corresponds to firmware version 22.0, was released on November 19, 2024.

Pictorial Alert Icons

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

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 SIP Call Button enclosure is not rated for any AC voltages!

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

Abbreviations and Terms

Abbreviation or Term	Definition
A-law	A standard companding algorithm, used in European digital communications systems to optimize, i.e., modify, the dynamic range of an analog signal for digitizing.
AVP	Audio Video Profile
Cat 5	TIA/EIA-568-B Category 5
DHCP	Dynamic Host Configuration Protocol
LAN	Local Area Network
LED	Light Emitting Diode
Mbps	Megabits per Second.
NTP	Network Time Protocol
PBX	Private Branch Exchange
PoE	Power over Ethernet (as per IEEE 802.3af standard)
RTFM	Reset Test Function Management
SIP	Session Initiated Protocol
SRTP	Secure Real Time Protocol
u-law	A companding algorithm, primarily used in the digital telecommunication
UC	Unified Communications
VoIP	Voice over Internet Protocol

Contents

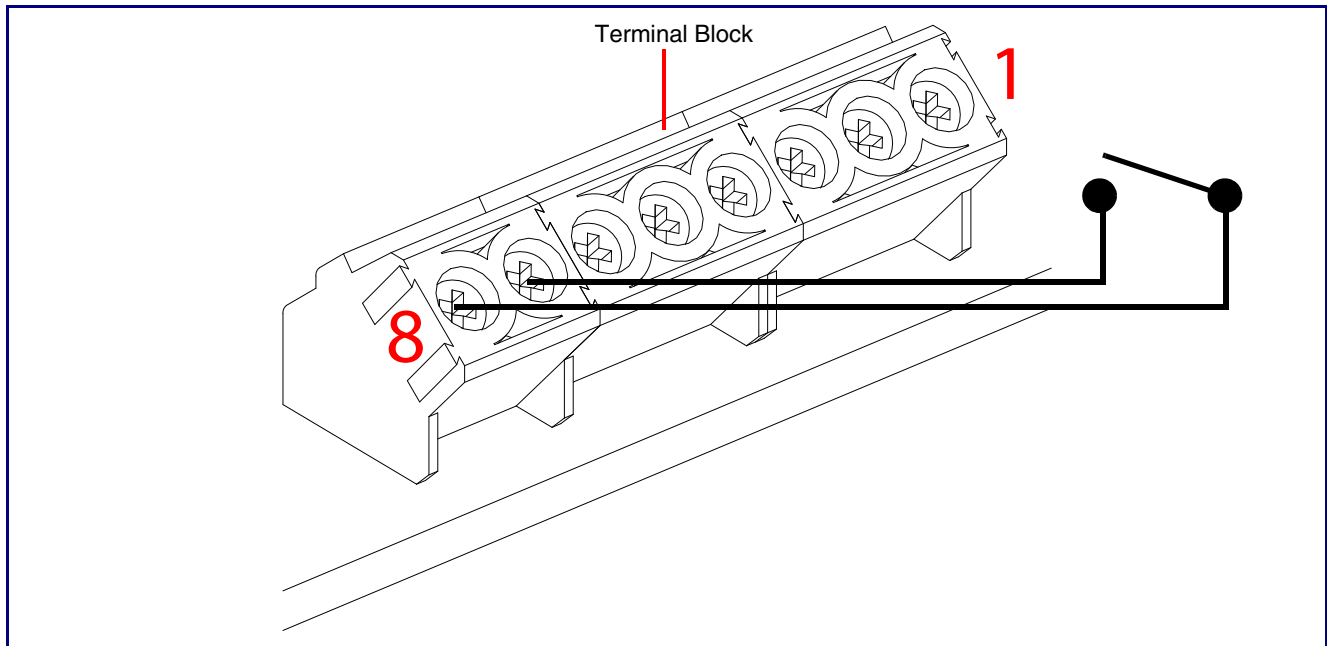
Chapter 1 Installing the SIP Call Button	1
1.1 Remote Switch Connection	1
1.1.1 Using the On-Board Relay	2
1.2 Wiring the Circuit	3
1.2.1 Devices Less than 1A at 30 VDC	3
1.2.2 Network Dual Door Strike Relay Wiring Diagram with External Power Source	4
1.2.3 Network Dual Door Strike Relay Wiring Diagram Using PoE+	5
1.3 Activity and Link LEDs	6
1.3.1 Verifying the Network Connectivity and Data Rate	6
1.4 Call Button and the Call Button LED	7
1.4.1 Calling with the The Call Button	7
1.4.2 Call Button LED Function	7
Chapter 2 Configure the Device	8
2.1 Log In Page	8
2.1.1 Restoring Defaults and Announcing the IP Address	9
2.2 Home Page	10
2.3 Device	11
2.4 Network	12
2.5 SIP (Session Initiation Protocol)	13
2.5.1 Dial Out Extension Strings and DTMF Tones (using rfc2833)	14
2.5.2 Point-to-Point Configuration	14
2.6 SSL	15
2.7 Sensor	17
2.8 Strobe	18
2.9 Audiofiles	20
2.10 Events	22
2.10.1 Example Packets for Events	23
2.11 Remote Relay	26
2.12 Terminus	27
2.13 Autoprovisioning	28
2.14 Firmware	29
2.15 Admin	30
2.16 Command Interface	31
2.16.1 Command Interface Post Commands	31
Appendix A Troubleshooting/Technical Support	32
A.1 Contact Information	32
A.2 Warranty and RMA Information	32
Index	33

1 Installing the SIP Call Button




1.1 Remote Switch Connection

Wiring pins 7 and 8 of the terminal block to a switch will initiate a SIP call when the switch is closed. The call will go to the extension specified as the dial out extension on the **SIP** page.

Figure 1-1. Remote Switch Connection



1.1.1 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 <i>Electrical Hazard:</i> The relay does not support AC powered door strikes. Any use of this relay beyond its normal operating range can cause damage to the product and is not covered under our warranty policy.

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 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 Network Dual Door Strike Relay (CD# 011375) (see [Section 1.2.2, "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 Page](#) on the web interface.

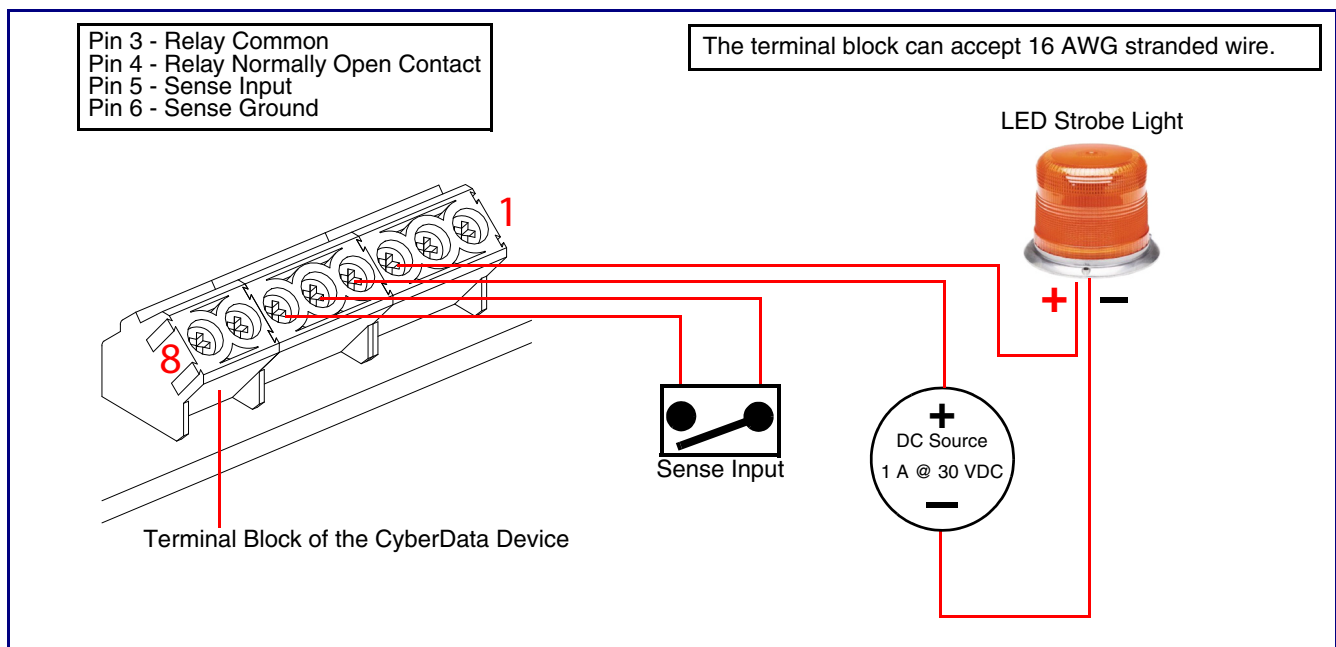
1.2 Wiring the Circuit

1.2.1 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 1-2](#) 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 1.2.2, "Network Dual Door Strike Relay Wiring Diagram with External Power Source"](#)).

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



1.2.2 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 1-3](#) and [Figure 1-4](#) for the wiring diagrams.


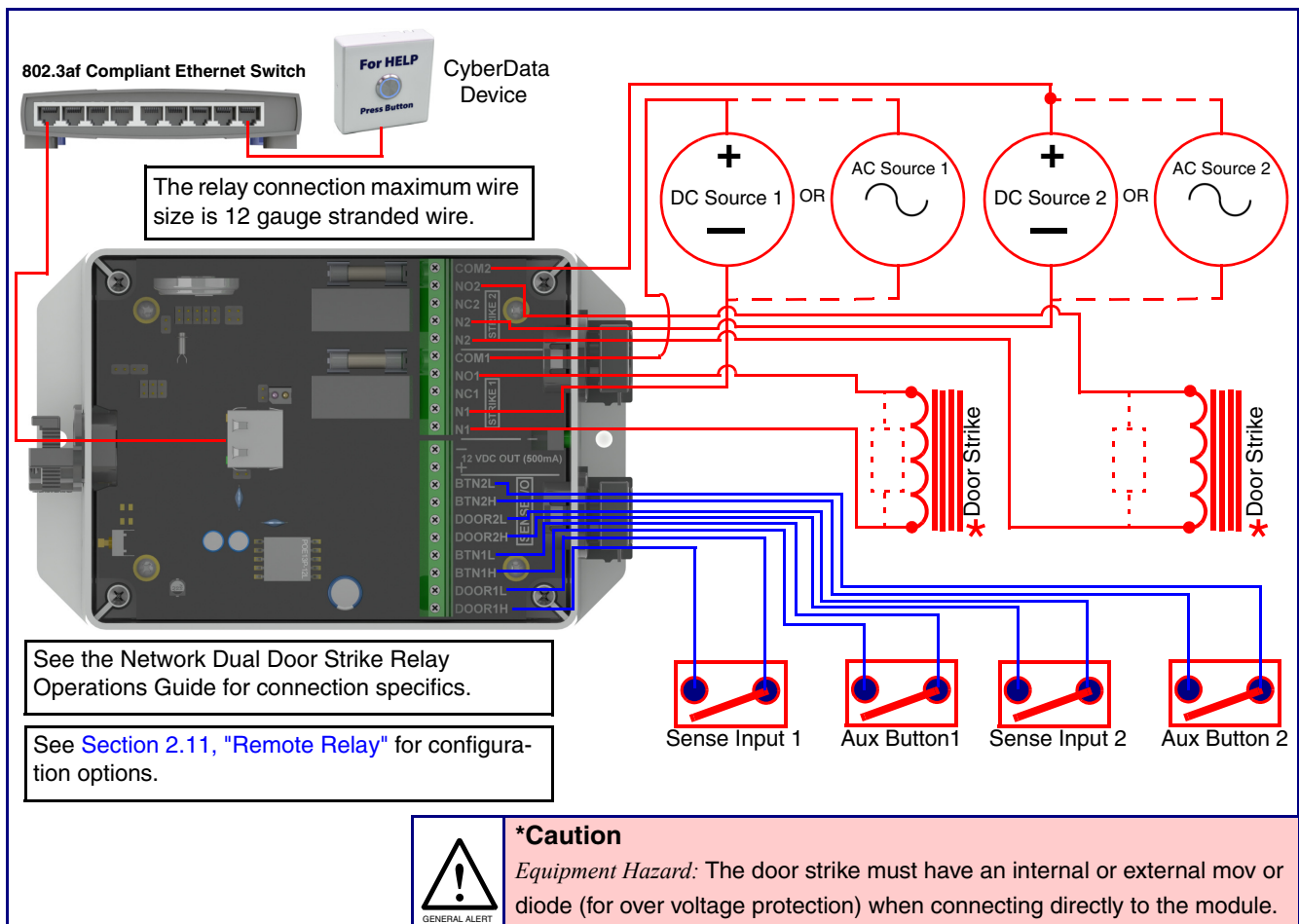
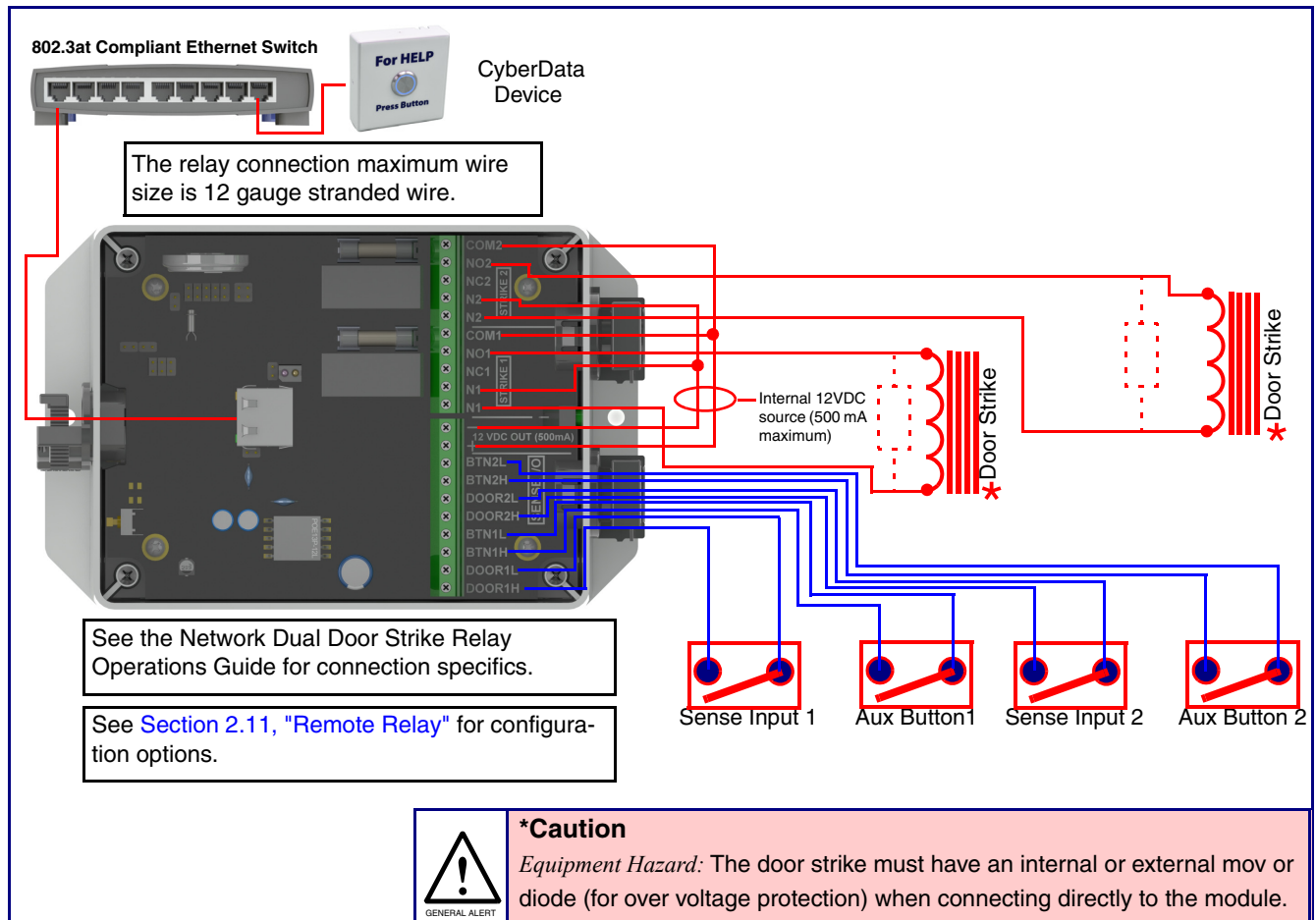
 <small>GENERAL ALERT</small>	<p>Warning</p> <p><i>Electrical Hazard:</i> Hazardous voltages may be present. No user serviceable part inside. Refer to qualified service personnel for connecting or servicing.</p>
---	--

Figure 1-3. Network Dual Door Strike Relay Wiring Diagram with External Power Source



1.2.3 Network Dual Door Strike Relay Wiring Diagram Using PoE+

Figure 1-4. Network Dual Door Strike Relay Wiring Diagram Using PoE+



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

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

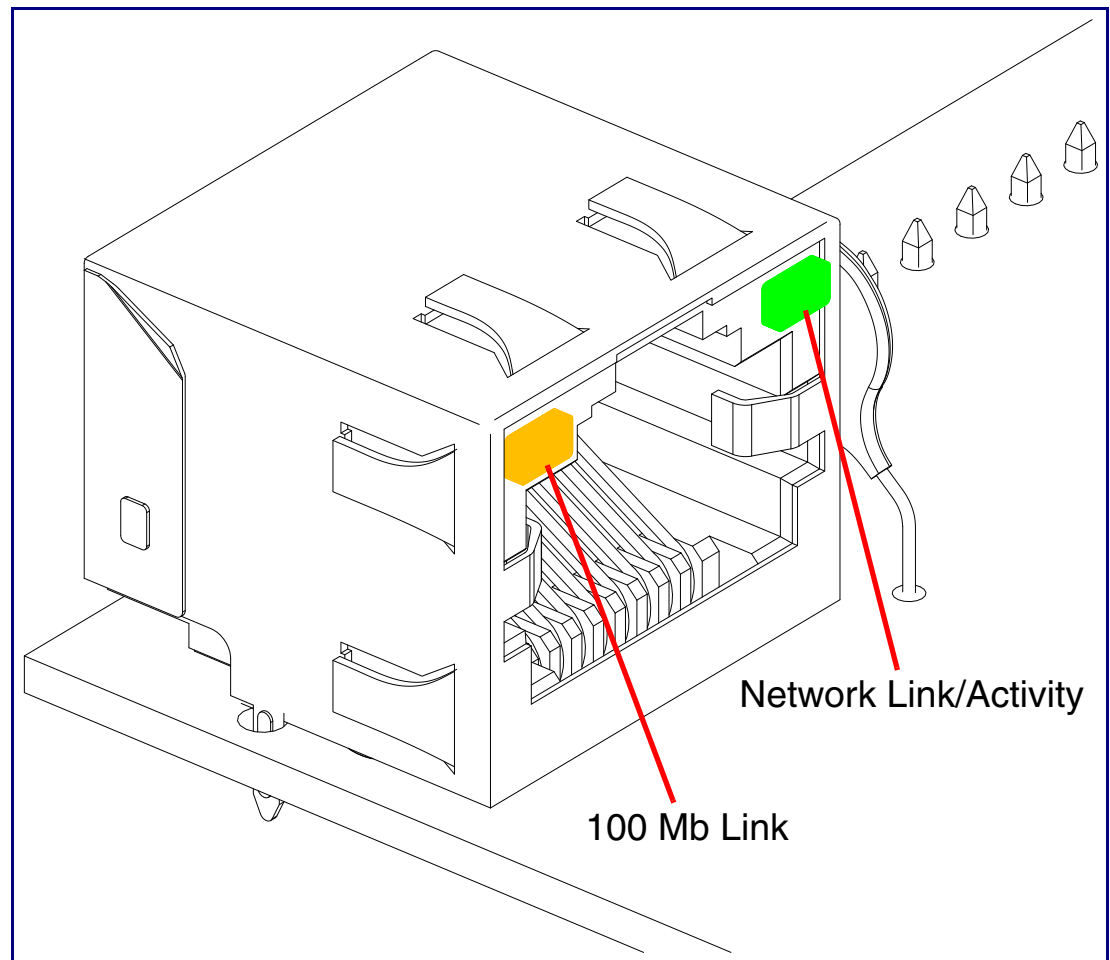
1.3 Activity and Link LEDs

1.3.1 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 Network Link/Activity** LED blinks when there is network activity (see [Figure 1-5](#)).
- The square, **AMBER 100 Mb Link** LED above the Ethernet port indicates that the network 100 Mb connection has been established (see [Figure 1-5](#)).

Figure 1-5. Activity and Link LED



1.4 Call Button and the Call Button LED

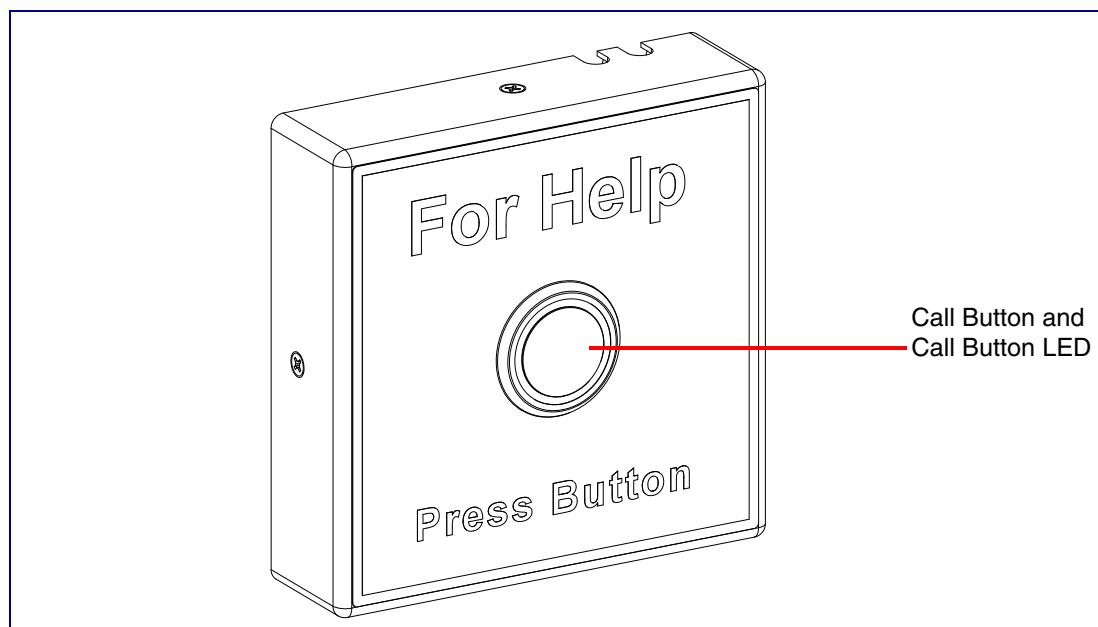
1.4.1 Calling with the The Call Button

- You may initiate a call by pressing the Call Button.
- An active call is indicated by the Call Button LED blinking at one second intervals.
- The device automatically answers an incoming call.
- You can press the Call Button to terminate an active call.

1.4.2 Call Button LED Function

- Upon initial power or reset, the Call Button LED will illuminate.
- On boot, the Call Button LED will flash ten times a second while setting up the network and downloading autoprovisioning files.
- The device “autoprovisions” by default, and the initial process may take several minutes as the device searches for and downloads updates. The Call Button LED will blink during this process. During the initial provisioning, or after the factory defaults have been reset, the device may download firmware twice. The device will blink, remain solid for 10 to 20 seconds, and then resume blinking. This process will take longer if there are many audio files downloading.
- When the software has finished initialization, the Call Button LED will blink twice.
- When a call is established (not just ringing), the Call Button LED will blink.
- On the **Device Page** (see [Section 2.3, "Device"](#)), there is an option called **Button Lit When Idle**. This option sets the normal state for the indicator LED. The Call Button LED will still blink during initialization and calls.
- The Call Button LED flashes briefly at the beginning of RTFM mode.

Figure 1-6. Call Button and Call Button LED



2 Configure the Device

2.1 Log In Page

1. Open your browser to the device IP address.

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

Note Make sure that the PC is on the same IP network as the SIP Call Button.

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

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

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

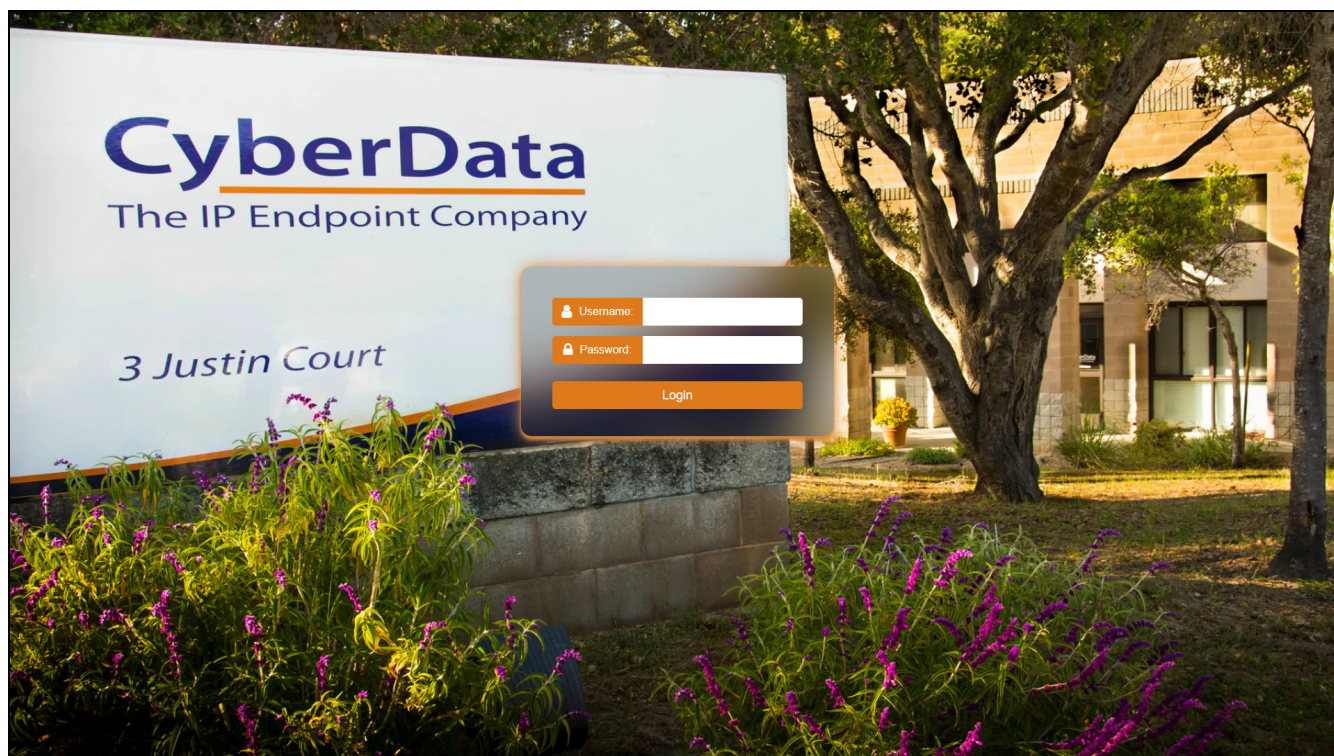
Note The device ships in DHCP mode. To get to the **Home** page, use the discovery utility to scan for the device on the network and open your browser from there.

2. On the Log In Page (Figure 2-1), use the following default **Web Access Username** and **Web Access Password** to access the **Home Page** (Figure 2-3):

Web Access Username: **admin**

Web Access Password: **admin**

Figure 2-1. Log In Page



2.1.1 Restoring Defaults and Announcing the IP Address

The RTFM button is located on the back of the device.

To restore the device to its factory default settings (Table 2-1), hold the RTFM button for approximately seven seconds.

The device will default to DHCP to obtain an IP address, or will use 192.168.1.23 if a DHCP server is not present.

Figure 2-2. RTFM Button

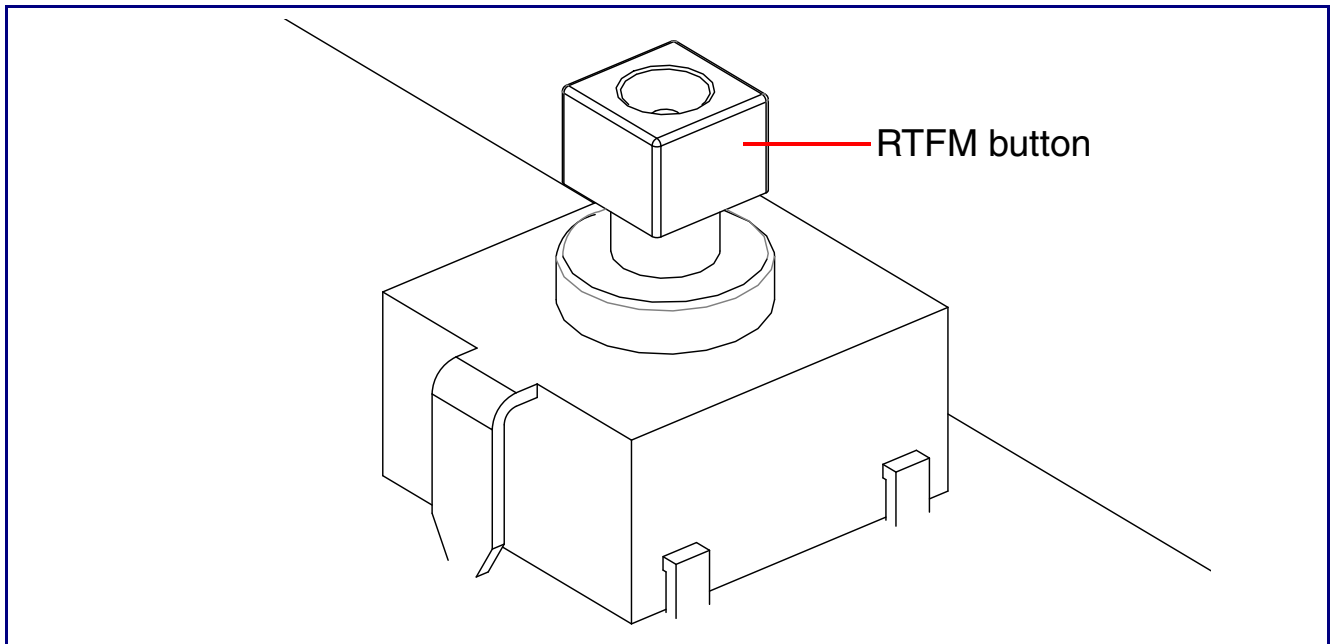


Table 2-1. Factory Default Settings

Parameter	Factory Default Setting
IP Addressing	DHCP
IP Address ^a	192.168.1.23
Web Access Username	admin
Web Access Password	admin
Subnet Mask ^a	255.255.255.0
Default Gateway ^a	192.168.1.1

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

2.2 Home Page

The **Home** page provides device specific information such as Serial Number, Mac Address, and Firmware version. This page is designed as an initial landing page to provide general information on the status of the device.

Figure 2-3. Home Page

The screenshot displays the CyberData Home Page interface. At the top, a dark blue header contains the CyberData logo and key device information: Product: Call Button, Firmware: v22.0.3, Serial: 049204479, MAC: 00:20:f7:05:2a:97, Available Storage: 1485MB, and Device Status: Idle. Action buttons for Test, Save, Cancel, Reboot, and Logout are visible on the right. A vertical sidebar on the left contains navigation icons. The main content area is divided into five panels:

- Device Configuration:**

Serial Number	049204479
Mac Address	00:20:f7:05:2a:97
Firmware Version	v22.0.3
Partition 2	v22.0.3b01
Partition 3	v22.0.3
Bootling Partition	partition 3
- Network Status:**

IP Address Protocol	DHCP
IP Address	10.10.0.14
Subnet Mask	255.0.0.0
Default Gateway	10.0.0.1
DNS Server 1	10.0.1.56
DNS Server 2	
- SIP Registration:**

SIP Mode:	Enabled
Primary Server:	Not registered
Backup Server 1:	Not registered
Backup Server 2:	Not registered
- Sensor Status:**

Relay Status:	Locked
Door Status:	Closed
Intrusion:	Inactive
RGB Strobe:	Installed
- System Configuration:**

SIP Mode:	Enabled
Event Mode:	Disabled

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

2.3 Device

The **Device** page allows for adjustment of settings that pertain to the physical device such as relay settings and time zone.

Figure 2-4. Device Page

The screenshot displays the CyberData Device Page configuration interface. At the top, the header includes the CyberData logo, product information (Product: Call Button, Firmware: v22.0.3), serial and MAC addresses (Serial: 049204479, MAC: 00:20:f7:05:2a:97), available storage (1485MB), and device status (Idle). Action buttons for Test, Save, Cancel, Reboot, and Logout are visible on the right.

The main configuration area is divided into three sections:

- Relay Settings:**
 - Control Relay with DTMF Code: ON
 - DTMF Pulse Code: 123
 - DTMF Pulse Code Duration: 2 seconds
 - DTMF Activation Code: 456
 - DTMF Deactivation Code: 654
 - Relay While Call Active: OFF
 - Relay On Button Press: OFF
 - Relay On Button Press Duration: 3 seconds
- Time Settings:**
 - NTP Server: north-america.pool.ntp.org
 - NTP Timezone: America/Los_Angeles (-8)
 - Current Time: Tue, 19 Nov 2024 16:56:48
- Stored Message Recording:**
 - Stored Message Recording: DISABLED
 - Recording Security Code: *****
- Misc Settings:**
 - Device Name: Call Button
 - Button Hold Timeout: 2000 millisecond (ms)
 - Button LED Lit when Idle: ON
 - Button LED Brightness: 255
 - Prevent Call Termination: OFF

A sidebar on the left contains navigation icons for Home, Call, Settings, and other functions. The footer of the page includes the CyberData logo and a link to Support.

2.4 Network

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

Figure 2-5. Network Page

The screenshot displays the CyberData Network configuration interface. At the top, a purple header bar contains the CyberData logo, product information (Call Button, v22.0.3), device details (Serial: 049204479, MAC: 00:20:f7:05:2a:97), storage status (1485MB), and device status (Idle). Action buttons for Test, Save, Cancel, Reboot, and Logout are also present.

The main content area is divided into three panels:

- Network Status:** A table showing current network parameters:

IP Address Protocol	DHCP
IP Address	10.10.0.14
Subnet Mask	255.0.0.0
Default Gateway	10.0.0.1
DNS Server 1	10.0.0.1
DNS Server 2	10.0.1.56
- Network Settings:** A form for configuring network parameters:

Addressing Mode:	DHCP
Hostname:	SipDevice052a97
IP Address:	10.10.10.10
Subnet Mask:	255.0.0.0
Default Gateway:	10.0.0.1
DNS Server 1:	10.0.0.1
DNS Server 2:	10.0.0.1
DHCP Timeout:	60 seconds
- VLAN Settings:** A form for configuring VLAN parameters:

VLAN ID:	0
VLAN Priority:	0

A vertical sidebar on the left contains navigation icons for Home, Network, System, and other functions. The footer of the page includes the text "CyberData • Support".

2.5 SIP (Session Initiation Protocol)

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

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

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

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

Figure 2-6. SIP Page

The screenshot displays the CyberData SIP configuration interface. At the top, it shows the product name 'Call Button', firmware version 'v22.0.3', serial number '049204479', MAC address '00:20:f7:05:2a:97', and available storage '1485MB'. The device status is 'Idle'. The interface is divided into three main configuration panels:

- SIP Settings:**
 - SIP Operation: ENABLED
 - SIP Registration: ENABLED
 - Remote SIP Port: 5060
 - Local SIP Port: 5060
 - SIP Transport Protocol: UDP
 - TLS Version: 1.2
 - Verify Server Certificate: OFF
 - Outbound Proxy: (empty)
 - Outbound Proxy Port: 0
 - Cisco SRST: OFF
 - Disable rport Discovery: OFF
 - Keep Alive Timeout: 10000 milliseconds (ms)
 - Terminate call after delay: 10 seconds
 - Audio Codec: PCMA (G.71)
 - RTP Port (even): 10500
 - Asymmetric RTP: OFF
 - Jitter Buffer: 50
 - RTP Encryption (SRTP): MANDATOR
- SIP Server Settings:**
 - Primary SIP Server: 10.10.0.178
 - Primary SIP User ID: 602
 - Primary SIP Auth ID: s5BNmzujem
 - Primary SIP Auth Password: (masked)
 - Registration Interval: 360 seconds
 - Backup SIP Server 1: (empty)
 - Backup SIP User ID: (empty)
 - Backup SIP Auth ID: (empty)
 - Backup SIP Auth Password: (empty)
 - Registration Interval: 360 seconds
 - Backup SIP Server 2: (empty)
 - Backup SIP User ID: (empty)
 - Backup SIP Auth ID: (empty)
 - Backup SIP Auth Password: (empty)
 - Registration Interval: 360 seconds
- Dial Out Settings:**
 - Dialout Extension: 603
 - Extension ID: id204
 - Send Multicast Audio: DISABLED
 - Multicast Address: 224.5.5.5
 - Multicast Port: 5050
 - Repeat Message: 1

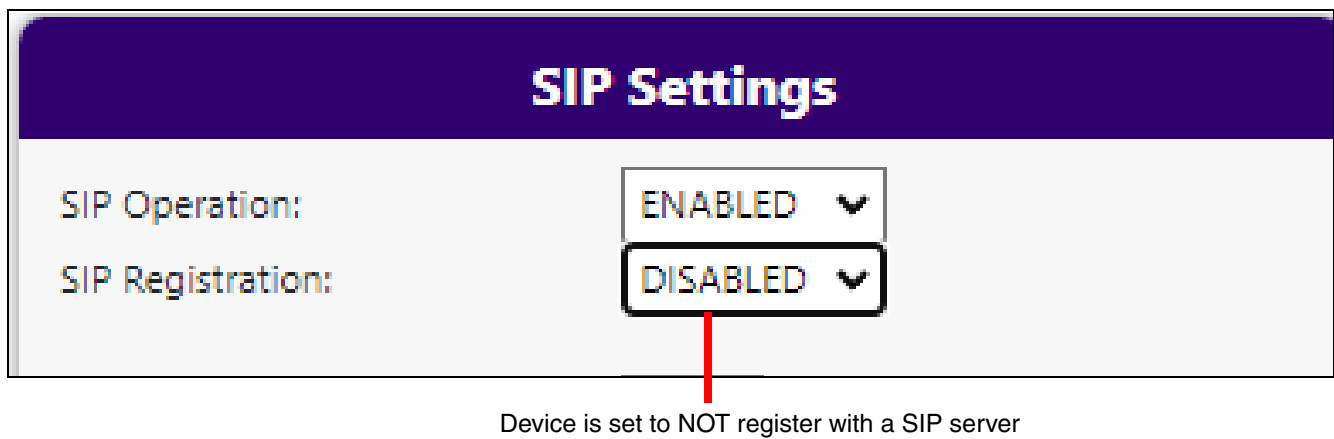
2.5.1 Dial Out Extension Strings and DTMF Tones (using rfc2833)

Outgoing calls support delayed DTMF (rfc2833) with the first comma pausing 2 seconds and subsequent commas pausing 1 second.

2.5.2 Point-to-Point Configuration

Dialing point-to-point allows the device to call and a single endpoint. All CyberData endpoints and many phones can use this option. To do this, enable **SIP Operation**, do not enable **SIP Registration**, and use the endpoint's IP address as the Dial Out extension. Delayed DTMF is supported. See [Figure 2-7](#).

Figure 2-7. SIP Page Set to Point-to-Point Mode



2.6 SSL

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

Figure 2-8. SSL Page (1 of 2)

The screenshot displays the CyberData SSL configuration interface. At the top, the header includes the CyberData logo, product information (Call Button, v22.0.3), device serial (049204479), MAC (00:20:f7:05:2a:97), available storage (1485MB), and device status (Idle). Navigation buttons for Test, Save, Cancel, Reboot, and Logout are present.

Three main certificate configuration panels are shown:

- Web Server Certificate:** Shows X.509 details (country: US, state: California, locality: Monterey, organization: Cyberdata, commonName: @e2f7852a97) and buttons for 'Import Web Certificate' and 'Restore Web Certificate'.
- SIP Client Certificate:** Shows identical X.509 details and buttons for 'Import SIP Certificate' and 'Restore SIP Certificate'.
- Autoprovisioning Client Certificate:** Shows identical X.509 details and buttons for 'Import Autoprovisioning Certificate' and 'Restore Autoprovisioning Certificate'.

Each panel includes a 'Choose Files' button and a 'Password (optional):' field.

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

Index	CA Certificate Name	Info	Remove
1	CyberData_CA.pem	Info	Remove
2	DigiCert_Assured_ID_Root_CA.crt	Info	Remove
3	DigiCert_Assured_ID_Root_G2.crt	Info	Remove
4	DigiCert_Assured_ID_Root_G3.crt	Info	Remove
5	DigiCert_Global_Root_CA.crt	Info	Remove
6	DigiCert_Global_Root_G2.crt	Info	Remove
7	DigiCert_Global_Root_G3.crt	Info	Remove
8	DigiCert_High Assurance EV Root CA.crt	Info	Remove

Additional buttons in the 'List of Trusted CAs' section include 'Download CyberData CA', 'Generate Cyberdata CSR', 'Remove All', and 'Restore Defaults'.

Figure 2-9. SSL Page (2 of 2)

CyberData The IP Endpoint Company

Product: Call Button
Firmware: v22.0.3

Serial: 049204479
MAC: 00:20:f7:05:2a:97

Available Storage: 1485MB
Device Status: Idle

Test Save Cancel Reboot Logout

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

CyberData • Support

2.7 Sensor

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 device board and will be activated when the device is removed from the case.

Each sensor can trigger up to three different actions:

- Flash the LED until the sensor is deactivated (roughly 10 times/second)
- Activate the relay until the sensor is deactivated
- Call an extension and play a pre-recorded audio file

Note Calling a preset extension can be set up as a point-to-point call, but currently can't send delayed DTMF tones.

Figure 2-10. Sensor Page

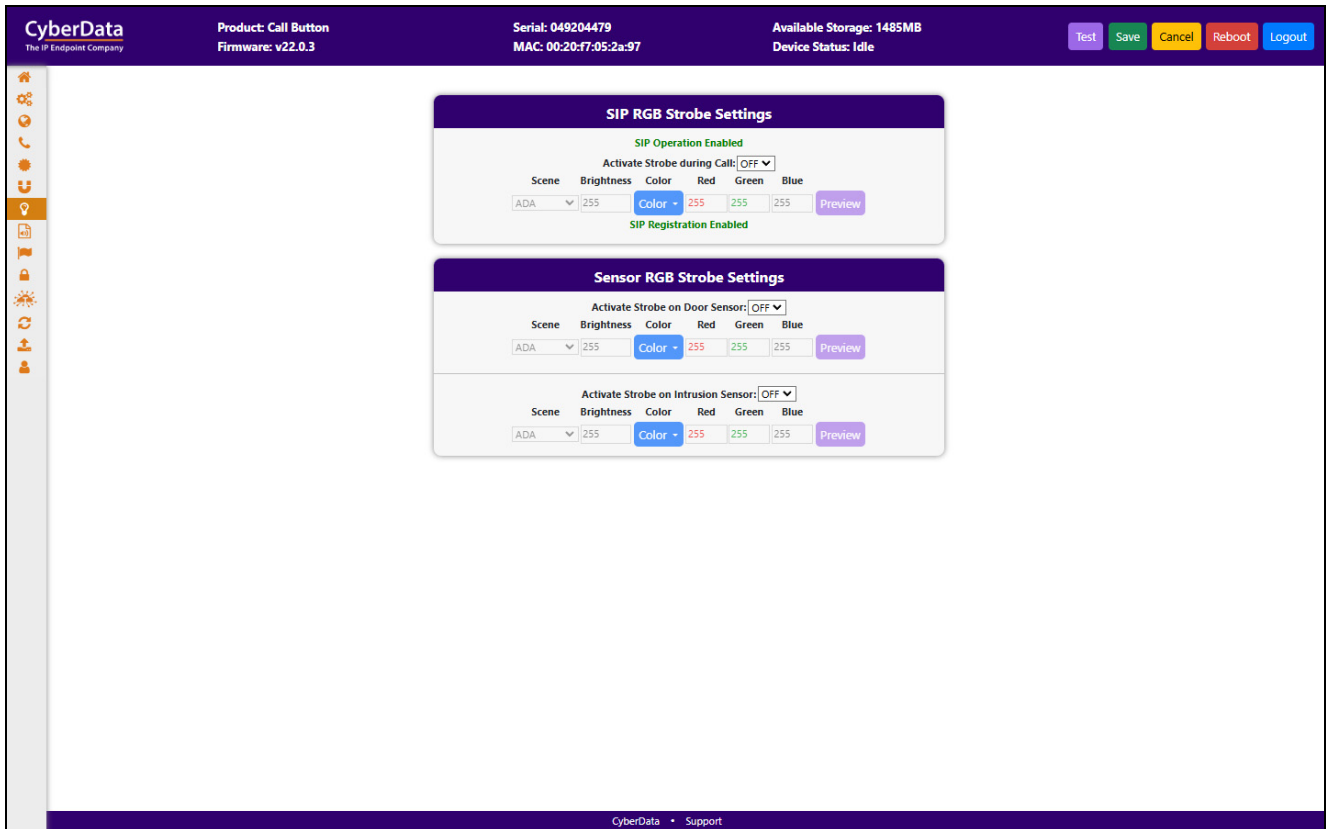
The screenshot displays the CyberData web interface for configuring sensors. The top header includes the CyberData logo, product information (Call Button, v22.0.3), serial and MAC addresses, available storage (1485MB), and device status (Idle). Action buttons for Test, Save, Cancel, Reboot, and Logout are visible. The main content area is divided into two settings panels:

- Door Sensor Settings:**
 - Sensor Type: Normally Open
 - Open Timeout: 0 seconds
 - Flash Button LED: Disabled
 - Activate Relay: Disabled
 - Call Extension: Disabled
 - Dial Out Extension: 204
 - Dial Out ID: id204
 - Play Recorded Audio: Disabled
 - Message Playbacks: 0
- Intrusion Sensor Settings:**
 - Flash Button LED: Disabled
 - Activate Relay: Disabled
 - Call Extension: Disabled
 - Dial Out Extension: 204
 - Dial Out ID: id204
 - Play Recorded Audio: Disabled
 - Message Playbacks: 0

The footer contains the text "CyberData • Support".

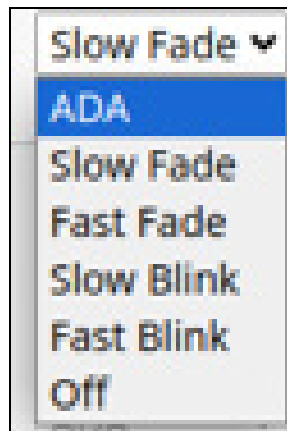
2.8 Strobe

Figure 2-11. Strobe Page



For each option, there are 5 scenes available:

Figure 2-12. 5 Scenes Available



Use the red, green, and blue values to create custom colors.

The ADA scene flashes white at maximum brightness (255). Other scenes can adjust the brightness, from 0 to 255.

Figure 2-13. 10 Colors



2.9 Audiofiles

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

Figure 2-14. Audiofiles Page (1 of 2)

The screenshot displays the CyberData web interface for configuring audio files. The top navigation bar shows the following information:

- CyberData** The IP Endpoint Company
- Product:** Call Button
- Firmware:** v22.0.3
- Serial:** 049204479
- MAC:** 00:20:F7:05:2a:97
- Available Storage:** 1485MB
- Device Status:** Idle
- Control buttons: Test, Save, Cancel, Reboot, Logout

The main content area is divided into two sections:

Audio Files

0:	Currently set to:	default	<input type="button" value="Choose File"/>	No file chosen	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
1:	Currently set to:	default	<input type="button" value="Choose File"/>	No file chosen	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
2:	Currently set to:	default	<input type="button" value="Choose File"/>	No file chosen	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
3:	Currently set to:	default	<input type="button" value="Choose File"/>	No file chosen	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
4:	Currently set to:	default	<input type="button" value="Choose File"/>	No file chosen	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
5:	Currently set to:	default	<input type="button" value="Choose File"/>	No file chosen	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
6:	Currently set to:	default	<input type="button" value="Choose File"/>	No file chosen	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
7:	Currently set to:	default	<input type="button" value="Choose File"/>	No file chosen	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
8:	Currently set to:	default	<input type="button" value="Choose File"/>	No file chosen	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
9:	Currently set to:	default	<input type="button" value="Choose File"/>	No file chosen	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
Door Ajar:	Currently set to:	default	<input type="button" value="Choose File"/>	No file chosen	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
Intrusion Sensor Triggered:	Currently set to:	default	<input type="button" value="Choose File"/>	No file chosen	<input type="button" value="Save"/>	<input type="button" value="Delete"/>

Menu Audio Files

Invalid Entry:	Currently set to:	default	<input type="button" value="Choose File"/>	No file chosen	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
Press:	Currently set to:	default	<input type="button" value="Choose File"/>	No file chosen	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
Enter Recording Security Code:	Currently set to:	default	<input type="button" value="Choose File"/>	No file chosen	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
Invalid Code:	Currently set to:	default	<input type="button" value="Choose File"/>	No file chosen	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
Or:	Currently set to:	default	<input type="button" value="Choose File"/>	No file chosen	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
Record Message Prompt:	Currently set to:	default	<input type="button" value="Choose File"/>	No file chosen	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
Save Record Message Prompt:	Currently set to:	default	<input type="button" value="Choose File"/>	No file chosen	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
Message Saved Successfully:	Currently set to:	default	<input type="button" value="Choose File"/>	No file chosen	<input type="button" value="Save"/>	<input type="button" value="Delete"/>

The bottom of the page shows the footer: CyberData • Support

Figure 2-15. Audiofiles Page (2 of 2)

The screenshot displays the 'Audiofiles' configuration page for a CyberData device. The top navigation bar includes the CyberData logo, product information (Product: Call Button, Firmware: v22.0.3), serial number (049204479), MAC address (00:20:F7:05:2a:97), available storage (1485MB), and device status (Idle). Action buttons for Test, Save, Cancel, Reboot, and Logout are present.

The main content area is organized into several sections:

- Intrusion Sensor Triggered:** Currently set to: default. Includes a 'Choose File' button and 'Save/Delete' buttons.
- Menu Audio Files:** A list of 11 audio prompts, each with a 'Choose File' button and 'Save/Delete' buttons:
 - Invalid Entry: Currently set to: default
 - Press: Currently set to: default
 - Enter Recording Security Code: Currently set to: default
 - Invalid Code: Currently set to: default
 - Or: Currently set to: default
 - Record Message Prompt: Currently set to: default
 - Save Record Message Prompt: Currently set to: default
 - Message Saved Successfully: Currently set to: default
 - Message Not Saved Successfully: Currently set to: default
 - You Recorded: Currently set to: default
 - To Record SIP Button Message: Currently set to: default
 - To Record Multicast Button Message: Currently set to: default
- Stored Messages:** Two entries:
 - SIP Button Message: Currently set to: default
 - Multicast Button Message: Currently set to: default
- Recorded Messages:** Includes a 'Choose File' button, 'No file chosen' text, and 'Upload Message' and 'Delete All Messages' buttons.

2.10 Events

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

Figure 2-16. Events Page

The screenshot displays the CyberData configuration interface for the 'Events' page. At the top, the header includes the CyberData logo, product information (Call Button, v22.0.3), device details (Serial: 049204479, MAC: 00:20:f7:05:2a:97), storage status (1485MB), and device status (Idle). Action buttons for Test, Save, Cancel, Reboot, and Logout are visible.

The main content area is divided into two panels:

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

A footer at the bottom of the page reads 'CyberData • Support'.

2.10.1 Example Packets for Events

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

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

Here are example packets for every event:

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

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

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

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

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

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

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

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

```
POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 205
Content-Type: application/x-www-form-urlencoded

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

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

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

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

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

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

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

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

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

2.11 Remote Relay

Figure 2-17. Remote Relay Page

The screenshot displays the Remote Relay configuration page. At the top, the device information is shown: Product: Call Button, Firmware: v22.0.3, Serial: 049204479, MAC: 00:20:f7:05:2a:97, Available Storage: 1485MB, and Device Status: Idle. Action buttons for Test, Save, Cancel, Reboot, and Logout are located in the top right. A sidebar on the left contains various navigation icons. The main content area features a table titled "Discovered Remote Relays" with the following data:

Product Type	IP Address	MAC Address	Serial Number	Name	Version	
DoorLock	10.10.0.51	00:20:f7:05:5e:21	375200300	LOCK375200300	v5.0.4	View Associate

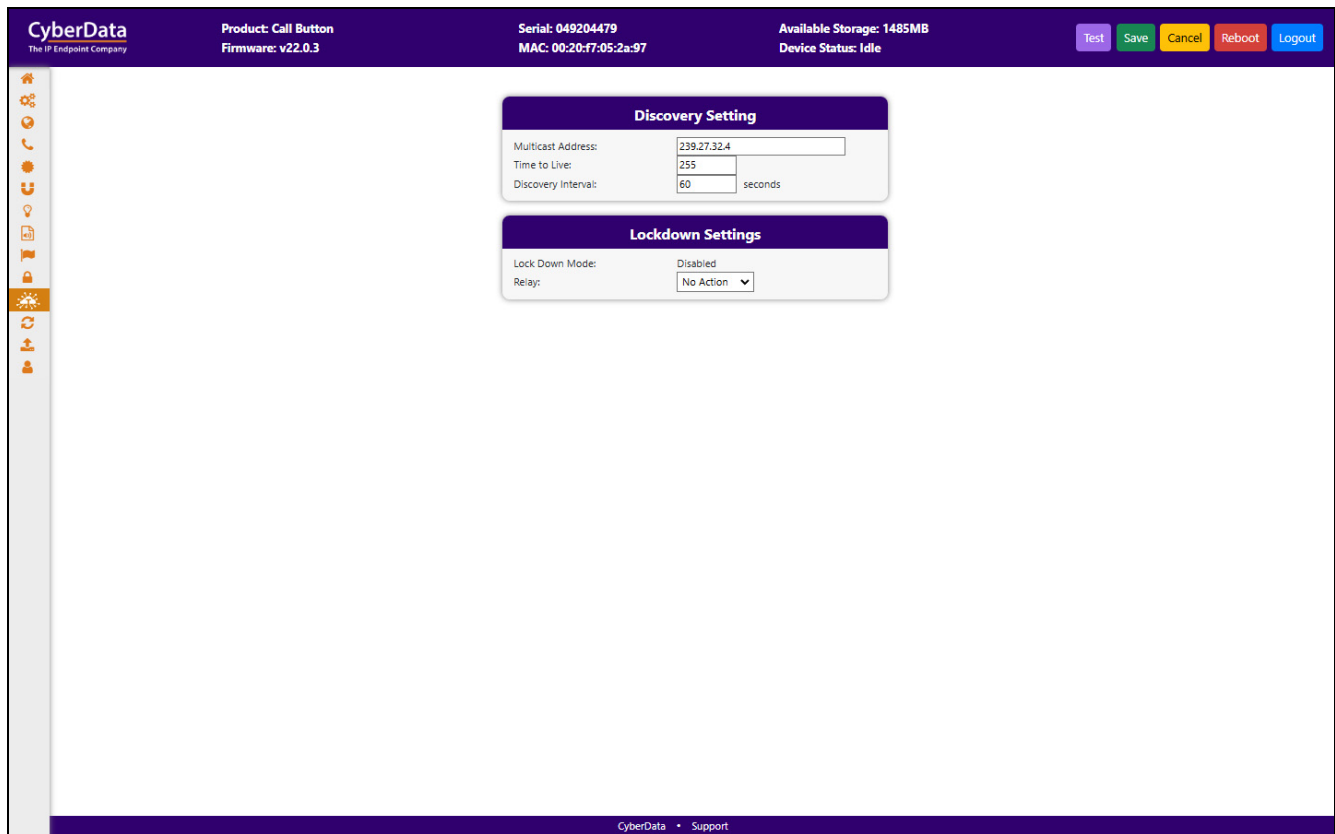
Additional buttons for Discover, View, and Associate are visible next to the table entries. The footer of the page includes the CyberData logo and a link to Support.

2.12 Terminus

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

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

Figure 2-18. Terminus Page



2.13 Autoprovisioning

Enabling autoprovisioning allows the device to download provisioning files from a server. It defaults to using DHCP, with options configured in dhcpd.conf on the DHCP server. The file name is <mac address>.xml and if not found, 000000cd.xml.

If a server is named, DHCP is bypassed, and the device will look for a file on the named server..

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

If a server is named, **Use tftp** searches for the file on a tftp server instead of http. If the server is secured (with a password), use **Verify Server Certificate** (username/password) to access it. When using DHCP, these options are configured in dhcpd.conf.

Autoprov autoupdate, **Autoprov at time**, and **Autoprov when idle** options are available with either DHCP or a named server.

The template is an xml file with all options set to default values.

Figure 2-19. Autoprovisioning Page

The screenshot displays the Autoprovisioning configuration page in the CyberData management interface. At the top, the device's product (Call Button), serial number (049204479), MAC address (00:20:f7:05:2a:97), and available storage (1484MB) are shown. The Autoprov Settings panel includes fields for enabling autoprovisioning, specifying a server and filename, choosing between http and tftp, and configuring certificate verification and update schedules. A 'Download Template' button is provided. The Autoprov Log panel shows a real-time log of the provisioning process, indicating successful completion of all steps.

2.14 Firmware

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

To upgrade the firmware of your device:

1. Download the latest firmware from the following CyberData web site, and locate your device:

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

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

- Firmware file
- Release notes
- Autoprovisioning template


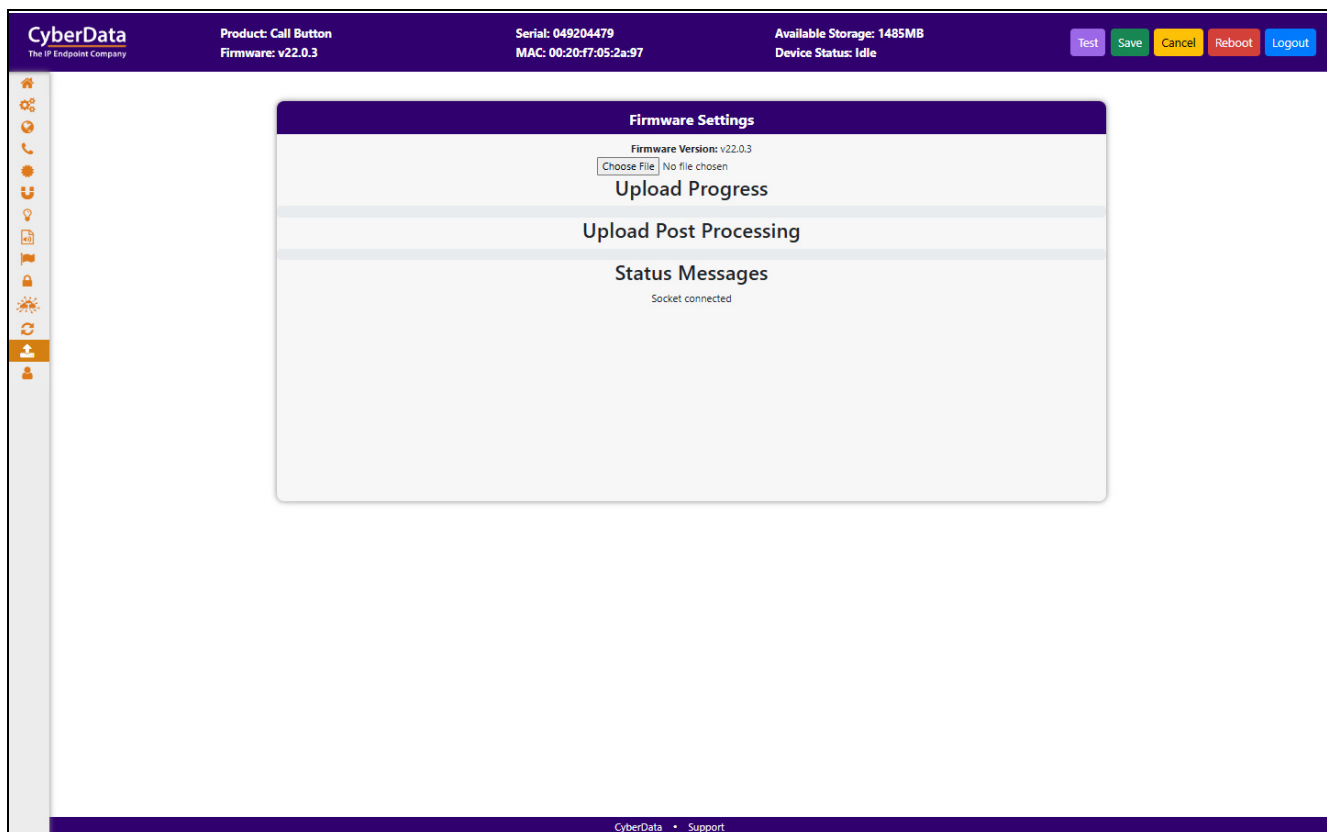
 GENERAL ALERT	<p>Caution Equipment Hazard: Do not reboot the device. It will reboot automatically when the process is complete.</p>
--	--

Figure 2-20. Firmware Page



2.15 Admin

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

Figure 2-21. Admin Page

The screenshot displays the CyberData Admin interface. At the top, a purple header bar contains the CyberData logo and device information: Product: Call Button, Firmware: v22.0.3, Serial: 049204479, MAC: 00:20:f7:05:2a:97, Available Storage: 1485MB, and Device Status: Idle. Action buttons for Test, Save, Cancel, Reboot, and Logout are on the right.

The main content area is divided into several sections:

- Admin Settings:** Fields for Username (admin), Password, and Confirm Password.
- Logging Settings:** Debug Level (4), Log Network Traffic (OFF), and buttons for Get/Remove Application, Network, and All Logs.
- Configuration Settings:** Partition information (v22.0.3b01, v22.0.3, partition 3) and buttons for Restore Default Config, Restore Default Certificates, Import/Export Config, and Boot From Other Partition.
- Statistics:** Storage (1485MB), Boot Count (76), Reboot Count (66), and Uptime (up 4 minutes).
- Users List:** A table with columns for Username, Home, Device, Network, SIP, SSL, Sensor, Strobe, Audiofiles, Events, DSR, Terminus, Autoprov, Firmware, and Admin. Two users are listed: 'term' and 'ssl1', each with Edit and Delete buttons. Action buttons for Add New User, Delete All Users, Import Users, and Export Users are at the top.
- Log Viewer:** A section with a Service dropdown (Application), Entries to get (250), Sort dropdown (Oldest), and a View Log button.

A footer bar at the bottom contains the text "CyberData • Support".

2.16 Command Interface

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

2.16.1 Command Interface Post Commands

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

Table 2-2. Command Interface Post Commands

Device Action	HTTP Post Command ^a
Reboot	<code>wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.154/command" --post-data "request=reboot"</code>
Place call to extension (example: extension 600)	<code>wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.154/command" --post-data "request=call&extension=600"</code>
Test Relay	<code>wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.154/command" --post-data "request=test_relay"</code>
Swap boot partitions	<code>wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.154/command" --post-data "request=swap_boot_partition"</code>

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

Appendix A: Troubleshooting/Technical Support

A.1 Contact Information

Contact CyberData Corporation
3 Justin Court
Monterey, CA 93940 USA
www.cyberdata.net
Phone: 831-373-2601
Fax: 831-373-4193

Sales Sales 831-373-2601, Extension 334

Technical Support The fastest way to get technical support for your VoIP product is to submit a VoIP Technical Support form at the following website:

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

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

Phone: (831) 373-2601, Extension 333

A.2 Warranty and RMA Information

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

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

Index

A

Admin 30
Audiofiles 20
Autoprovisioning 28

C

Contact Information 32

D

Device 11
Dial Out Extension Strings and DTMF Tones 14

E

Events 22

F

Firmware 29

H

Home Page 10

N

Network 12

P

Point-to-Point Configuration 14

S

Sensor 17
SIP (Session Initiation Protocol) 13

SSL 15
Strobe 18

T

Terminus 27

W

Warranty and RMA Information 32