



# *RGB (Multi-Color) Strobe Operations Guide*

Part #011376, 011377, 011479, 011489

Document Part #932063A  
for Firmware Version 22.0

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

---

---

**RGB (Multi-Color) Strobe Operations Guide 932063A**  
**Part # 011376, 011377, 011479, 011489**

**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](mailto:support@cyberdata.net)

Fax: (831) 373-4193

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

---

# Revision Information

Revision 932063A, which corresponds to firmware version 22.0, was released on November 19, 2024.

---

## Pictorial Alert Icons

	<p><b>General Alert</b> This pictorial alert indicates a potentially hazardous situation. This alert will be followed by a hazard level heading and more specific information about the hazard.</p>
	<p><b>Ground</b> 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 RGB (Multi-Color) Strobe enclosure is not rated for any AC voltages!**

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

---

# Abbreviations and Terms

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

# Contents

---

<b>Chapter 1 Device Set-Up</b>	<b>1</b>
1.1 Activity and Link LEDs .....	1
1.1.1 Verifying the Network Connectivity and Data Rate .....	1
<b>Chapter 2 Configure the Device</b>	<b>2</b>
2.1 Log In Page .....	2
2.1.1 Restoring Defaults and Announcing the IP Address .....	3
2.2 Home Page .....	4
2.3 Device .....	6
2.4 Network .....	7
2.5 SIP (Session Initiation Protocol) .....	8
2.5.1 Dial Out Extension Strings and DTMF Tones (using rfc2833) .....	8
2.5.2 Point-to-Point Configuration .....	9
2.6 SSL .....	10
2.7 Multicast .....	12
2.8 Sensor .....	13
2.9 Strobe .....	14
2.10 Audiofiles .....	16
2.11 Events .....	17
2.11.1 Example Packets for Events .....	18
2.12 Terminus .....	21
2.13 Autoprovisioning .....	22
2.14 Firmware .....	23
2.15 Admin .....	24
2.16 Command Interface .....	25
2.16.1 Command Interface Post Commands .....	25
<b>Appendix A Troubleshooting/Technical Support</b>	<b>26</b>
A.1 Contact Information .....	26
A.2 Warranty and RMA Information .....	26
<b>Index</b>	<b>27</b>

# 1 Device Set-Up

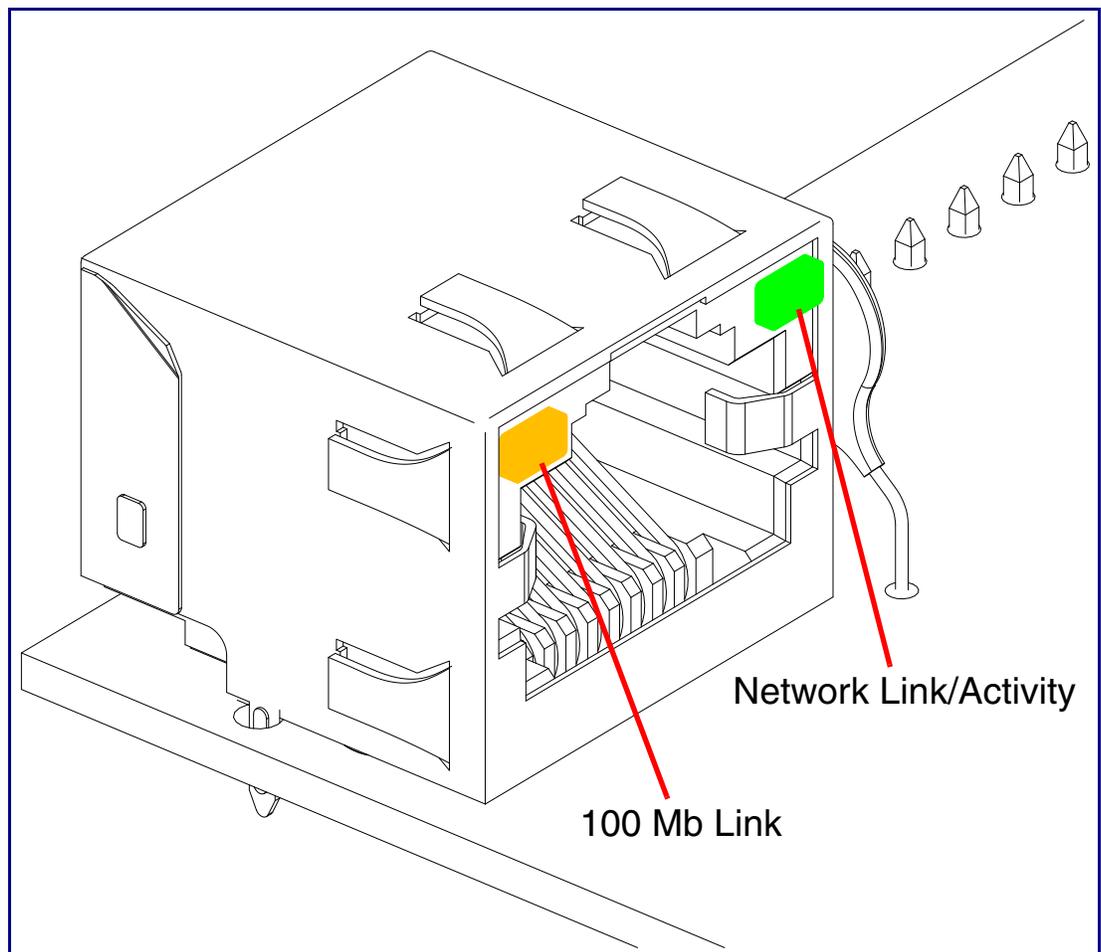
## 1.1 Activity and Link LEDs

### 1.1.1 Verifying the Network Connectivity and Data Rate

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

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

**Figure 1-1. Activity and Link 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 RGB (Multi-Color) Strobe.

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

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

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

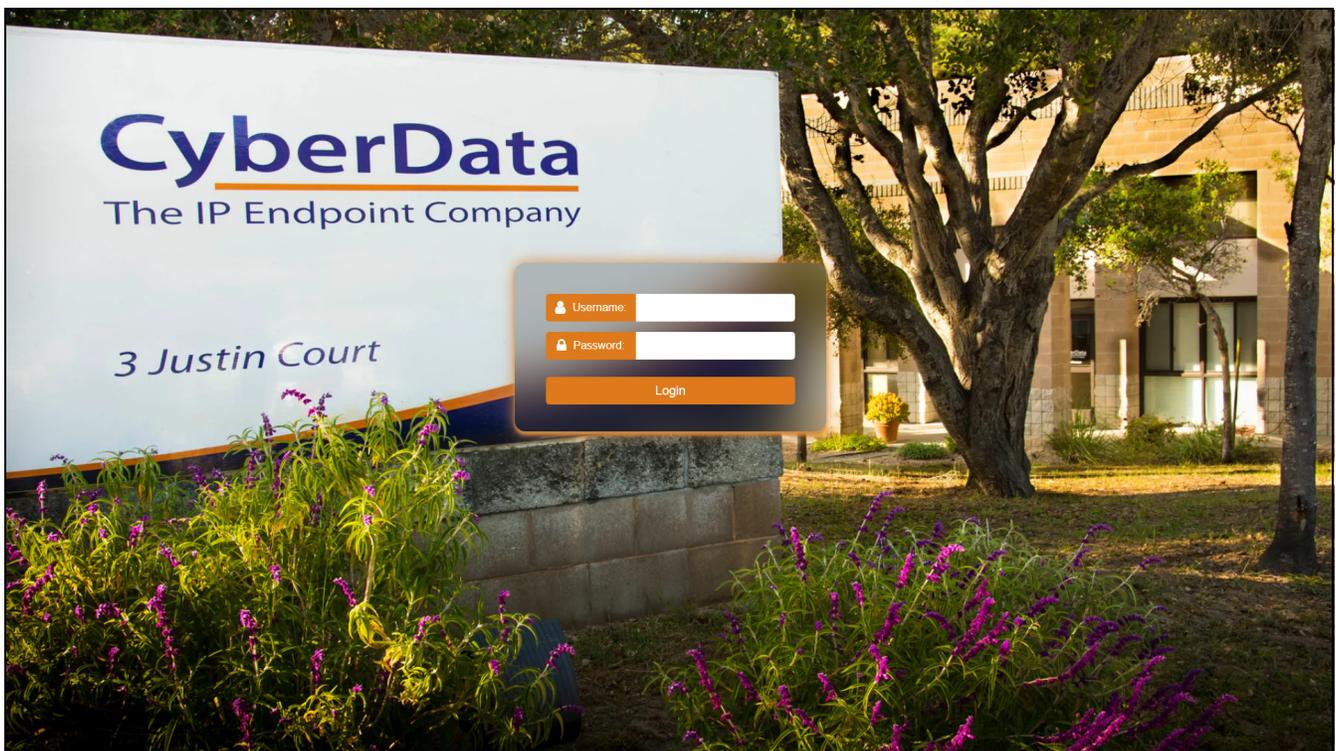
**Note** The Intercom ships in DHCP mode. To get to the **Home** page, use the discovery utility to scan for the device on the network and open your browser from there.

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

Web Access Username: **admin**

Web Access Password: **admin**

Figure 2-1. Log In Page



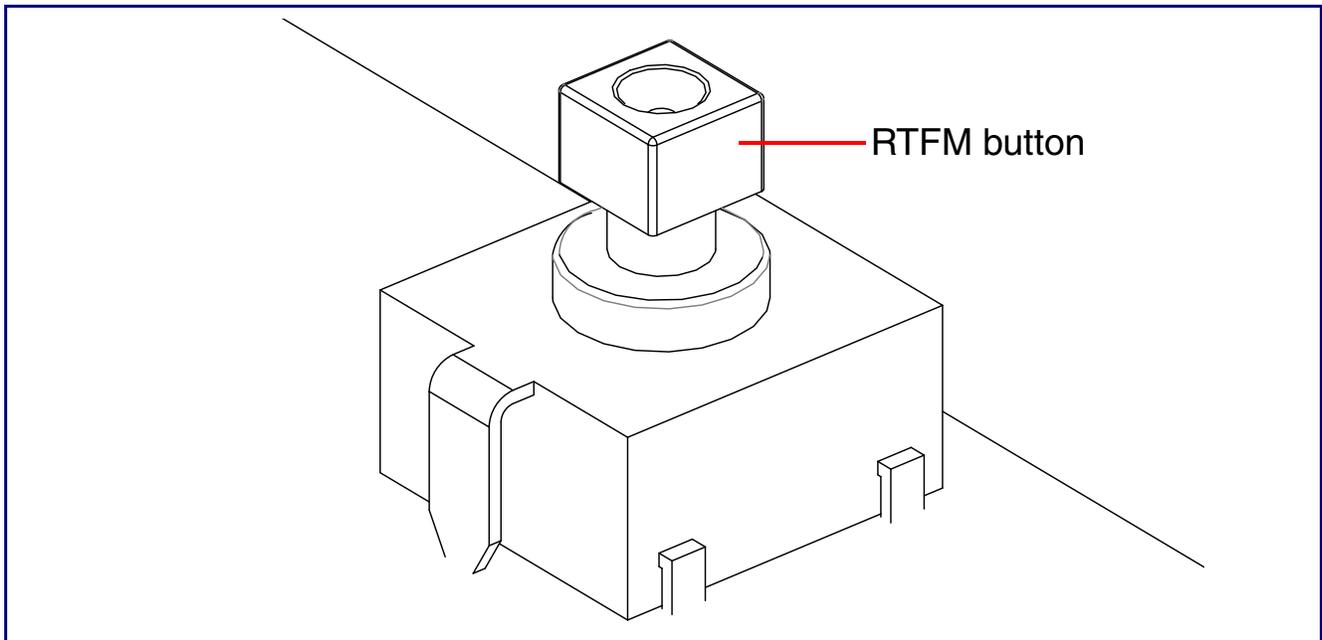
## 2.1.1 Restoring Defaults and Announcing the IP Address

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 <sup>a</sup>	192.168.1.23
Web Access Username	admin
Web Access Password	admin
Subnet Mask <sup>a</sup>	255.255.255.0
Default Gateway <sup>a</sup>	192.168.1.1

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

## 2.2 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 purple header bar contains the CyberData logo, product information (Multicolor Strobe, v22.0.0), serial and MAC addresses, available storage (1381MB), and device status (Idle). Action buttons for Test, Save, Cancel, Reboot, and Logout are also present.

The main content area is divided into five panels:

- Device Configuration:**

Serial Number	479000248
Mac Address	00:20:f7:05:69:b7
Firmware Version	v22.0.0
Partition 2	v22.0.0
Partition 3	v22.0.0
Booting Partition	partition 3
- Network Status:**

IP Address Protocol	DHCP
IP Address	192.168.0.174
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.1
DNS Server 1	192.168.0.1
DNS Server 2	
- SIP Registration:**

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

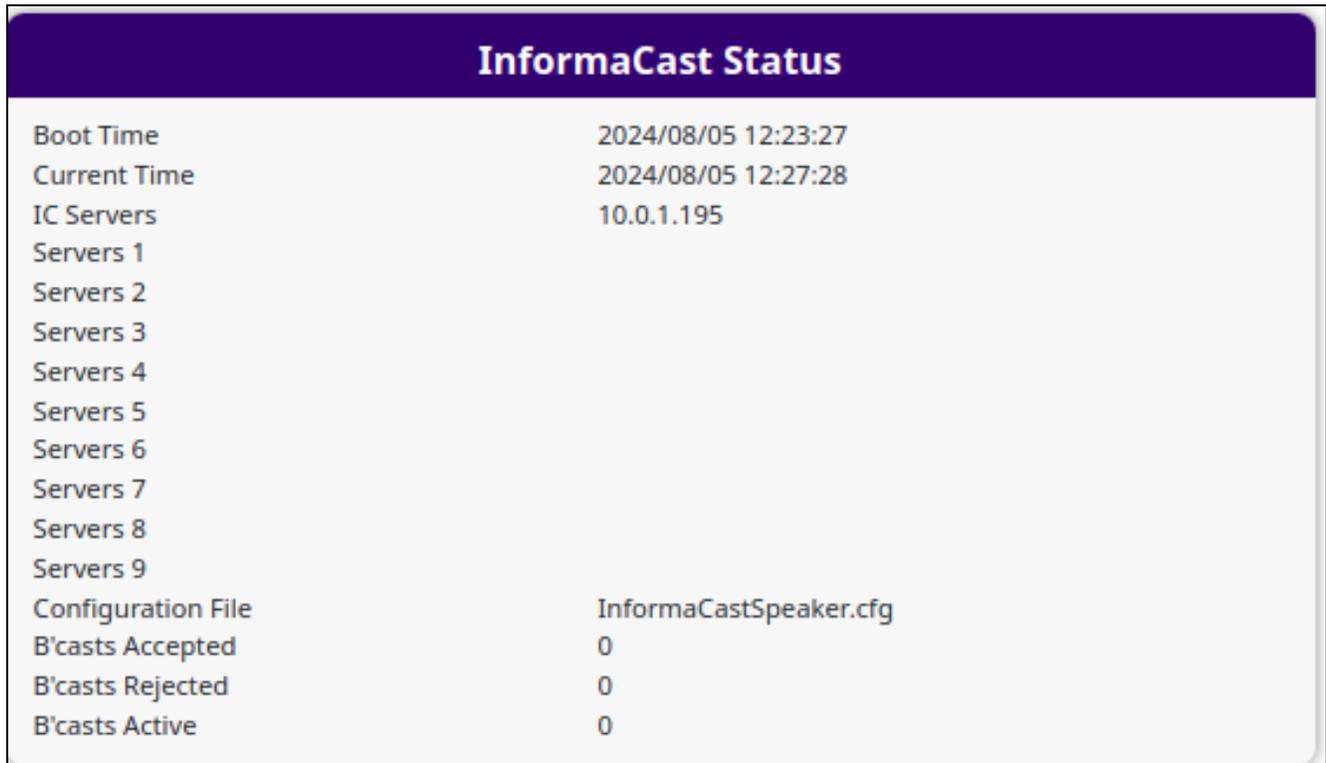
Relay Status:	Locked
Door Status:	
Intrusion:	Active
- System Configuration:**

SIP Mode:	Enabled
Multicast Mode:	Disabled
Event Mode:	Disabled

The footer of the page shows "CyberData • Support".

If you are using an InformaCast enabled device, you will see the following:

**Figure 2-4. InformaCast enabled Device**

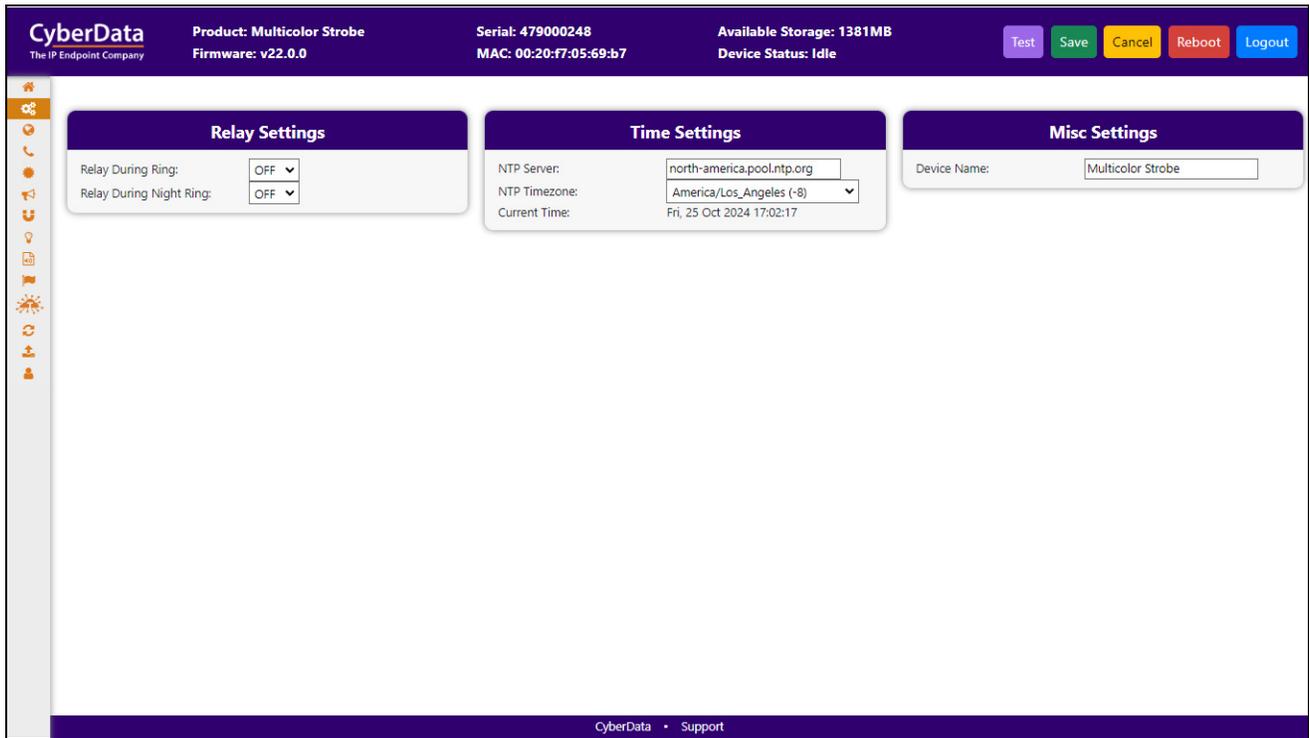


InformaCast Status	
Boot Time	2024/08/05 12:23:27
Current Time	2024/08/05 12:27:28
IC Servers	10.0.1.195
Servers 1	
Servers 2	
Servers 3	
Servers 4	
Servers 5	
Servers 6	
Servers 7	
Servers 8	
Servers 9	
Configuration File	InformaCastSpeaker.cfg
B'casts Accepted	0
B'casts Rejected	0
B'casts Active	0

## 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 2-5. Device Page**



If you are using an InformaCast enabled device, you will see the following:

**Figure 2-6. InformaCast enabled Device**



## 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 2-7. Network Page

**CyberData** The IP Endpoint Company

Product: Multicolor Strobe  
Firmware: v22.0.0

Serial: 479000248  
MAC: 00:20:f7:05:69:b7

Available Storage: 1381MB  
Device Status: Idle

Test Save Cancel Reboot Logout

### Network Status

IP Address Protocol	DHCP
IP Address	192.168.0.174
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.1
DNS Server 1	192.168.0.1
DNS Server 2	192.168.0.1

### Network Settings

Addressing Mode:	DHCP
Hostname:	SipDevice0569b7
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

VLAN ID:	0
VLAN Priority:	0

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 2-8. SIP Page

The screenshot shows the CyberData SIP configuration interface. At the top, there is a header with the CyberData logo and device information: Product: Multicolor Strobe, Serial: 479000248, Available Storage: 1381MB, Firmware: v22.0.0, MAC: 00:20:F7:05:69:b7, and Device Status: Idle. Action buttons for Test, Save, Cancel, Reboot, and Logout are visible. The main content area is divided into three panels:

- SIP Settings:** Includes SIP Operation (ENABLED), SIP Registration (ENABLED), Remote/Local SIP Ports (5060), SIP Transport Protocol (UDP), TLS Version (1.2), Verify Server Certificate (OFF), Outbound Proxy (0), Cisco SRST (OFF), Disable rport Discovery (OFF), Keep Alive Timeout (10000 ms), Terminate call after delay (0 seconds), Audio Codec (Auto Selec), RTP Port (10500), Asymmetric RTP (OFF), Jitter Buffer (50), and RTP Encryption (DISABLED).
- SIP Server Settings:** Configures Primary and Backup SIP Servers. Primary server: 10.0.0.253, User ID: 199, Auth ID: 199, Password: \*\*\*\*\*. Backup servers have fields for Host or IP address, User ID, Auth ID, Password, and Registration Interval (360 seconds).
- Nightringer Settings:** Configures a Nightringer server with fields for Host or IP address, User ID, Auth ID, Password, and Registration Interval (360 seconds).

If you are using an InformaCast enabled device, you will see the following:

Figure 2-9. InformaCast enabled Device

The screenshot shows a dropdown menu for 'InformaCast SIP Config:' which is currently set to 'DISABLED'.

### 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 2-10](#).

**Figure 2-10. 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 2-11. SSL Page (1 of 3)

The screenshot displays the CyberData SSL configuration interface. At the top, the header includes the CyberData logo, product information (Multicolor Strobe, Firmware: v22.0.0), device serial (479000248), MAC (00:20:F7:05:69:b7), available storage (1381MB), and device status (Idle). Navigation buttons for Test, Save, Cancel, Reboot, and Logout are present.

The main content area is divided into three certificate management panels:

- Web Server Certificate:** Shows certificate details (subject, country, state, locality, organization, common name) and validity dates. It includes a 'Choose Files' button, an 'Import Web Certificate' button, and a 'Restore Web Certificate' button.
- SIP Client Certificate:** Similar to the Web Server Certificate panel, with an 'Import SIP Certificate' button and a 'Restore SIP Certificate' button. It also features a 'Password (optional):' field.
- Autoprovisioning Client Certificate:** Similar to the other panels, with an 'Import Autoprovisioning Certificate' button and a 'Restore Autoprovisioning Certificate' button. It also features a 'Password (optional):' field.

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

Index	CA Name	Info	Remove
1	CyberData_CA.pem	Info	Remove
2	DigiCert_Assured_ID_Root_CA.crt	Info	Remove

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

Figure 2-12. SSL Page (2 of 3)

The screenshot displays the SSL configuration page for a Multicolor Strobe device. The header includes the CyberData logo, product name, serial number (479000248), MAC address (00:20:F7:05:69:b7), available storage (1381MB), and device status (Idle). Action buttons for Test, Save, Cancel, Reboot, and Logout are visible. The main content is a table listing certificates with their IDs, names, and associated Info and Remove buttons.

ID	Certificate Name	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
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

Figure 2-13. SSL Page (3 of 3)

The screenshot displays the SSL configuration page for a Multicolor Strobe device, showing certificates 15 through 29. The header and navigation elements are consistent with the previous page.

ID	Certificate Name	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

## 2.7 Multicast

The Multicast page allows the device to join up to ten paging zones that will activate the strobe when a stream is sent to its address.

A paging zone can consist of one or many CyberData multicast group-enabled products. There is no limit to how many endpoints can be in a given paging zone. Each multicast group is defined by a multicast address and port number.

Each multicast group is assigned a priority, allowing simultaneously arriving pages to be serviced based on importance. Multicast groups are compatible with IGMP through version 3. The device supports simultaneous SIP and Multicast.

**Figure 2-14. Multicast Page**

**CyberData** The IP Endpoint Company  
**Product: Multicolor Strobe**  
**Firmware: v22.0.3**  
**Serial: 479000002**  
**MAC: 00:20:f7:04:0b:f9**  
**Available Storage: 1381 MB**  
**Device Status: Idle** [Test] [Save] [Cancel] [Reboot] [Logout]

**Multicast Settings**

Recieve Multicast Audio:

Polycom Default Channel:

Polycom Priority Channel:

Polycom Emergency Channel:

Priority	Address	Port	Name	Relay
0	239.168.3.1	2000	Background Music	DISABLED
1	239.168.3.2	3000	MG1	DISABLED
2	239.168.3.3	4000	MG2	DISABLED
3	239.168.3.4	5000	MG3	DISABLED
4	239.168.3.5	6000	MG4	DISABLED
5	239.168.3.6	7000	MG5	DISABLED
6	239.168.3.7	8000	MG6	DISABLED
7	239.168.3.8	9000	MG7	DISABLED
8	239.168.3.9	10000	MG8	DISABLED
9	239.168.3.10	11000	Emergency	DISABLED

*SIP calls: Priority 4.5*  
*Port range: 2000-65535*  
*Priority: 9 is the highest, 0 is the lowest*  
*Audio Streams: Higher priority supersedes lower ones*  
*Priority 9: Plays at maximum volume*

CyberData • Support

## 2.8 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 Intercom board and will be activated when the Intercom is removed from the case.

Each sensor can trigger up to three different actions:

- Activate the relay until the sensor is deactivated
- Call an extension and play a pre-recorded audio file
- Flash a strobe scene

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

Figure 2-15. Sensor Page

The screenshot displays the CyberData web interface for configuring sensors. The top navigation bar includes the CyberData logo, product information (Multicolor Strobe, Firmware: v22.0.0), serial and MAC addresses (479000248, 00:20:f7:05:69:b7), available storage (1381MB), and device status (Idle). Action buttons for Test, Save, Cancel, Reboot, and Logout are present. The main content area is divided into two panels: Door Sensor Settings and Intrusion Sensor Settings. The Door Sensor Settings panel includes fields for Sensor Type (Normally Open), Open Timeout (0 seconds), Activate Relay (Disabled), Call Extension (Disabled), Dial Out Extension (204), Dial Out ID (id204), and Repeat Sensor Message (0). The Intrusion Sensor Settings panel includes fields for Activate Relay (Disabled), Call Extension (Disabled), Dial Out Extension (204), Dial Out ID (id204), and Audio Playbacks (0). A sidebar with navigation icons is on the left, and the footer shows CyberData Support.

Setting	Value
Sensor Type	Normally Open
Open Timeout	0 seconds
Activate Relay	Disabled
Call Extension	Disabled
Dial Out Extension	204
Dial Out ID	id204
Repeat Sensor Message	0

Setting	Value
Activate Relay	Disabled
Call Extension	Disabled
Dial Out Extension	204
Dial Out ID	id204
Audio Playbacks	0

## 2.9 Strobe

Figure 2-16. Strobe Page

**SIP RGB Strobe Settings**

SIP Operation Enabled

Activate Strobe on Ring: OFF

Scene	Brightness	Color	Red	Green	Blue
ADA	255	Color	255	255	255

Activate Strobe during Call: OFF

Scene	Brightness	Color	Red	Green	Blue
ADA	255	Color	255	255	255

SIP Registration Enabled

Activate Strobe on MWI: OFF

Scene	Brightness	Color	Red	Green	Blue
ADA	255	Color	255	255	255

Activate Strobe on Nightring: OFF

Scene	Brightness	Color	Red	Green	Blue
ADA	255	Color	255	255	255

**Sensor RGB Strobe Settings**

Activate Strobe on Door Sensor: OFF

Scene	Brightness	Color	Red	Green	Blue
ADA	255	Color	255	255	255

Activate Strobe on Intrusion Sensor: OFF

Scene	Brightness	Color	Red	Green	Blue
ADA	255	Color	255	255	255

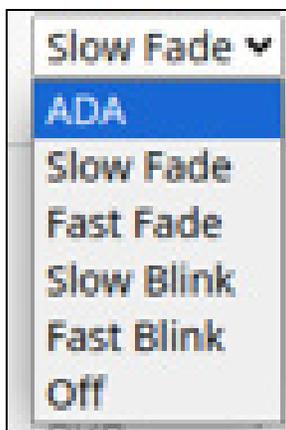
**Multicast RGB Strobe Settings**

Multicast Disabled

Priority	Scene	Brightness	Color	Red	Green	Blue
0	ADA	255	Color	255	255	255
1	ADA	255	Color	255	255	255
2	ADA	255	Color	255	255	255
3	ADA	255	Color	255	255	255
4	ADA	255	Color	255	255	255
5	ADA	255	Color	255	255	255
6	ADA	255	Color	255	255	255
7	ADA	255	Color	255	255	255
8	ADA	255	Color	255	255	255
9	ADA	255	Color	255	255	255

For each option, there are 5 scenes available:

Figure 2-17. 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 2-18. 10 Colors**



If you are using an InformaCast enabled device, you will see the following:

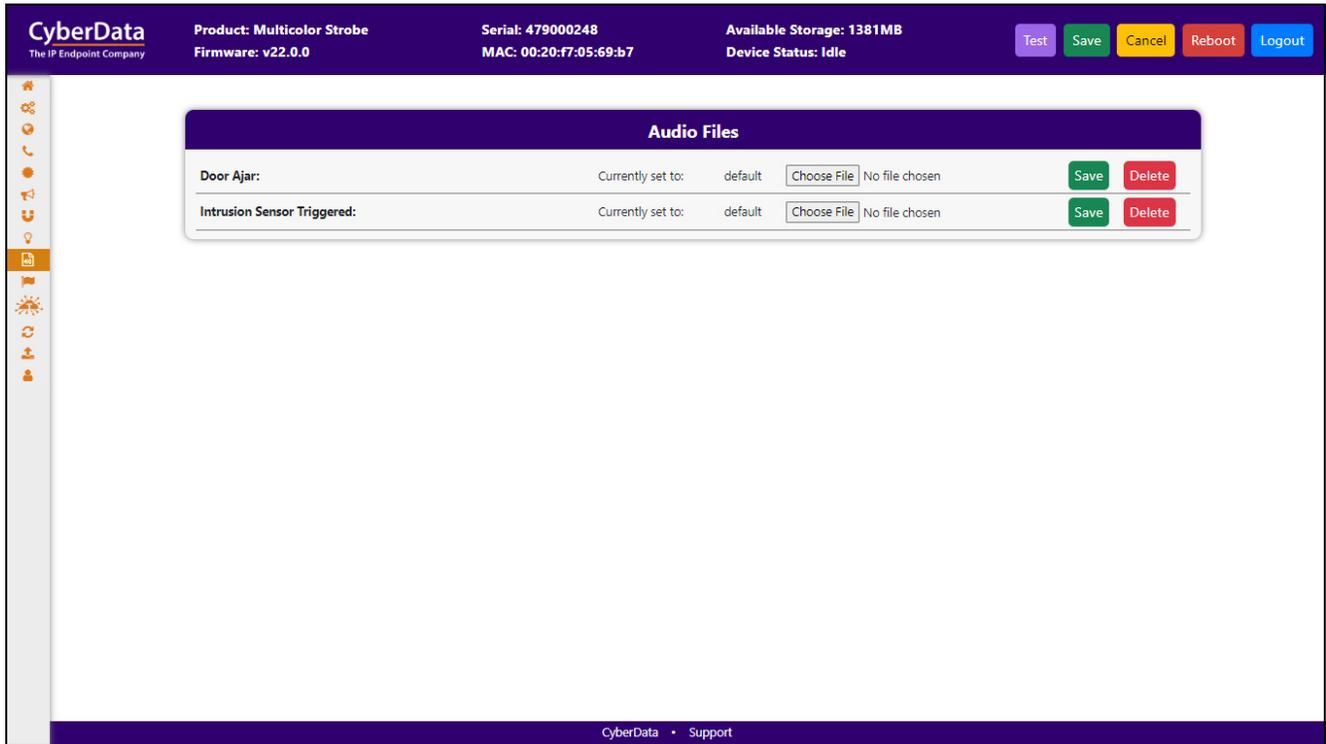
**Figure 2-19. InformaCast enabled Device**

InformaCast RGB Strobe Settings							
Priority	Scene	Brightness	Color	Red	Green	Blue	
0	ADA	255	Color	255	255	255	Preview
1	ADA	255	Color	255	255	255	Preview
2	ADA	255	Color	255	255	255	Preview
3	ADA	255	Color	255	255	255	Preview
4	ADA	255	Color	255	255	255	Preview
5	ADA	255	Color	255	255	255	Preview
6	ADA	255	Color	255	255	255	Preview
7	ADA	255	Color	255	255	255	Preview
8	ADA	255	Color	255	255	255	Preview
9	ADA	255	Color	255	255	255	Preview

## 2.10 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 2-20. Audiofiles Page



## 2.11 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 2-21. Events Page**

If you are using an InformaCast enabled device, you will see the following:

**Figure 2-22. InformaCast enabled Device**

---

## 2.11.1 Example Packets for Events

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

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

Here are example packets for every event:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## 2.12 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 2-23. Terminus Page**

The screenshot displays the Terminus configuration interface. At the top, a purple header bar contains the CyberData logo and the following information: Product: Multicolor Strobe, Firmware: v22.0.0, Serial: 479000248, MAC: 00:20:f7:05:69:b7, Available Storage: 1381MB, and Device Status: Idle. On the right side of the header are buttons for Test, Save, Cancel, Reboot, and Logout. A vertical sidebar on the left contains various navigation icons. The main content area features two configuration panels:

- Discovery Setting**:
  - Multicast Address:
  - Time to Live:
  - Discovery Interval:  seconds
- Lockdown Settings**:
  - Lock Down Mode:
  - Relay:

The footer of the page shows "CyberData • Support".

## 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 2-24. Autoprovisioning Page**

The screenshot displays the Autoprovisioning configuration page. At the top, the interface shows the CyberData logo and system information: Product: Multicolor Strobe, Serial: 479000248, Available Storage: 1381MB, Firmware: v22.0.0, MAC: 00:20:f7:05:69:b7, and Device Status: Idle. Action buttons for Test, Save, Cancel, Reboot, and Logout are visible.

The main content area is divided into two panels:

- Autoprov Settings:** This panel contains several configuration fields:
  - Autoprov: A dropdown menu set to "ENABLED".
  - Autoprov Server: A text input field containing "Autoprov Server".
  - Autoprov Filename: A text input field containing "Autoprov Filename".
  - Use tftp: A dropdown menu set to "DISABLED".
  - Verify Server Certificate: A dropdown menu set to "DISABLED".
  - Username: A text input field.
  - Password: A text input field.
  - Autoprov autoupdate: A numeric input field set to "0" with a "minutes" label.
  - Autoprov at time: A text input field set to "HHMM".
  - Autoprov when idle: A numeric input field set to "0" with a "minutes" label.
 A blue "Download Template" button is located at the bottom of this panel.
- Autoprov Log:** This panel displays a scrollable log of events:
  - 2024-11-06 13:52:36 Autoprov: no autoprov triggers. Exiting...
  - 2024-11-06 13:52:38 Autoprovisioning on boot
  - 2024-11-06 13:52:38 Autoprov found server='http://10.0.0.242' in dhcp option 43
  - 2024-11-06 13:52:38 Autoprov looking for 0020f70569b7.xml at http://10.0.0.242
  - 2024-11-06 13:52:38 Autoprov downloading http://10.0.0.242/0020f70569b7.xml
  - 2024-11-06 13:52:39 Got autoprov file. Parsing "0020f70569b7.xml"
  - 2024-11-06 13:52:39 Autoprov: Processing ssl certificates
  - 2024-11-06 13:52:39 No certificate elements in SSLCertificates
  - 2024-11-06 13:52:39 Autoprov: Processing audio files
  - 2024-11-06 13:52:39 Autoprov: FirmwareSettings config not found
  - 2024-11-06 13:52:39 DeviceConfig: error = False
  - 2024-11-06 13:52:39 SSLCertificates: error = None
  - 2024-11-06 13:52:39 AudioFiles: error = False
  - 2024-11-06 13:52:39 BellSchedule: error = False
  - 2024-11-06 13:52:39 FirmwareSettings: error = None

The footer of the page includes the CyberData logo and a "Support" link.

## 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:

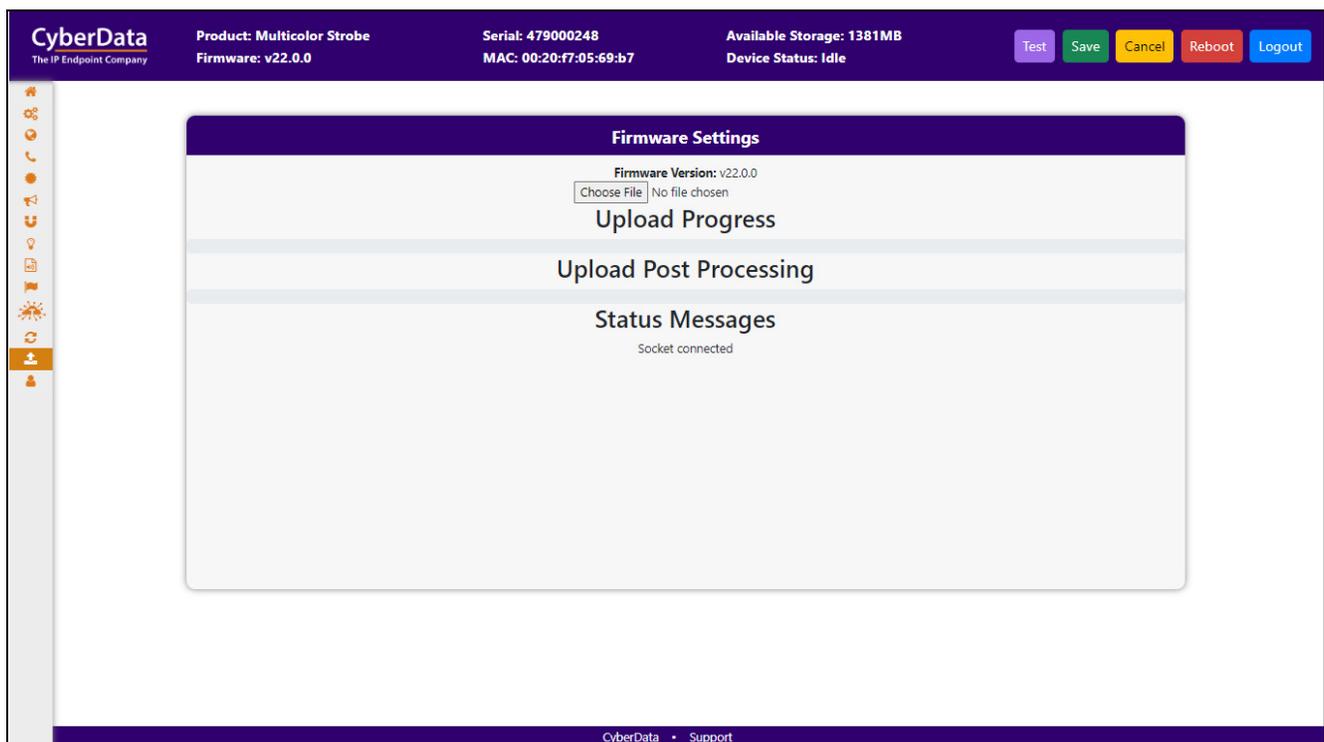
<https://www.cyberdata.net/collections/sip>

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

- Firmware file
- Release notes
- Autoprovisioning template

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

Figure 2-25. 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 2-26. Admin Page

The screenshot displays the CyberData Admin Page interface. At the top, the header includes the CyberData logo, product information (Multicolor Strobe, Firmware v22.0.0), device details (Serial: 479000248, MAC: 00:20:F7:05:69:b7), and storage/status information (Available Storage: 1381MB, Device Status: Idle). Action buttons for Test, Save, Cancel, Reboot, and Logout are visible in the top right.

The main content area is divided into several sections:

- Admin Settings:** Fields for Username (admin), Password, and Confirm Password.
- Statistics:** A table showing system metrics:
 

Storage:	1381MB
Boot Count:	20
Reboot Count:	15
Uptime:	up 1 hour, 28 minutes
- Logging Settings:** Includes Debug Level (4) and Log Network Traffic (OFF). Buttons for Get Application Log, Remove Application Log, Get Network Log, Remove Network Log, Get All Logs, and Remove All Logs are present.
- Configuration Settings:** Shows Partition 2 (v22.0.0), Partition 3 (v22.0.0), and Booting Partition (partition 3). Buttons for Restore Default Config, Restore Default Certificates, Import Config, Export Config, and Boot From Other Partition are available.
- Users List:** A table with columns: Username, Home, Device, Network, SIP, SSL, Multicast, Sensor, Strobe, Audiofiles, Events, Terminus, Autoprov, Firmware, Admin. Action buttons for Add New User, Delete All Users, Import Users, and Export Users are located above the table.
- Log Viewer:** A section for viewing logs with a Service dropdown (Application), Entries to get (250), and Sort dropdown (Oldest). A View Log button is also present.

A vertical sidebar on the left contains various system icons. The footer of the page includes 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 <sup>a</sup>
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&amp;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](http://www.cyberdata.net)  
Phone: 831-373-2601  
Fax: 831-373-4193

Sales                         Sales 831-373-2601, Extension 334

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

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

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

Phone: (831) 373-2601, Extension 333

---

## A.2 Warranty and RMA Information

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

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

# Index

---

## A

Admin 24  
Audiofiles 16  
Autoprovisioning 22

## C

Command Interface 25  
Contact Information 26

## D

Device 6  
Dial Out Extension Strings and DTMF Tones 8  
Discovery Utility program 2  
door sensor 13

## E

Events 17

## F

Firmware 23

## H

Home Page 4

## I

intrusion sensor 13

## N

Network 7

## P

Point-to-Point Configuration 9

## S

SIP (Session Initiation Protocol) 8  
SSL 10

## T

Technical Support 26  
Terminus 21

## W

Warranty and RMA Information 26