



SIP Paging Server Operations Guide

*SIP Compliant
Part #011146*

Document Part #931803G
for Firmware Version 22.0

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

Operations Guide 931803G
SIP Compliant 011146

COPYRIGHT NOTICE:

© 2025, 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

Fax: (831) 373-4193

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

Revision Information

Revision 931803G, which corresponds to firmware version 22.0, was released on November 19, 2024, and has the following changes:

- Updates the following text in [Section 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/Ring Group.](#)
- Adds the following text in [Section 2.6, “Paging Groups \(PGROUPS\)”](#):
[The PGroups page allows for configuration of the PGroup\(s\) including stored message playback and Polycom Paging.](#)
- Adds [Section 2.6.1, “PGroup Configuration”](#)

Pictorial Alert Icons

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

Hazard Levels

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

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

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

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

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

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.



Warning

Electrical Hazard: This product should be installed by a licensed electrician according to all local electrical and building codes.



Warning

Electrical Hazard: To prevent injury, this apparatus must be securely attached to the floor/wall in accordance with the installation instructions.



Warning

The PoE connector is intended for intra-building connections only and does not route to the outside plant.

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

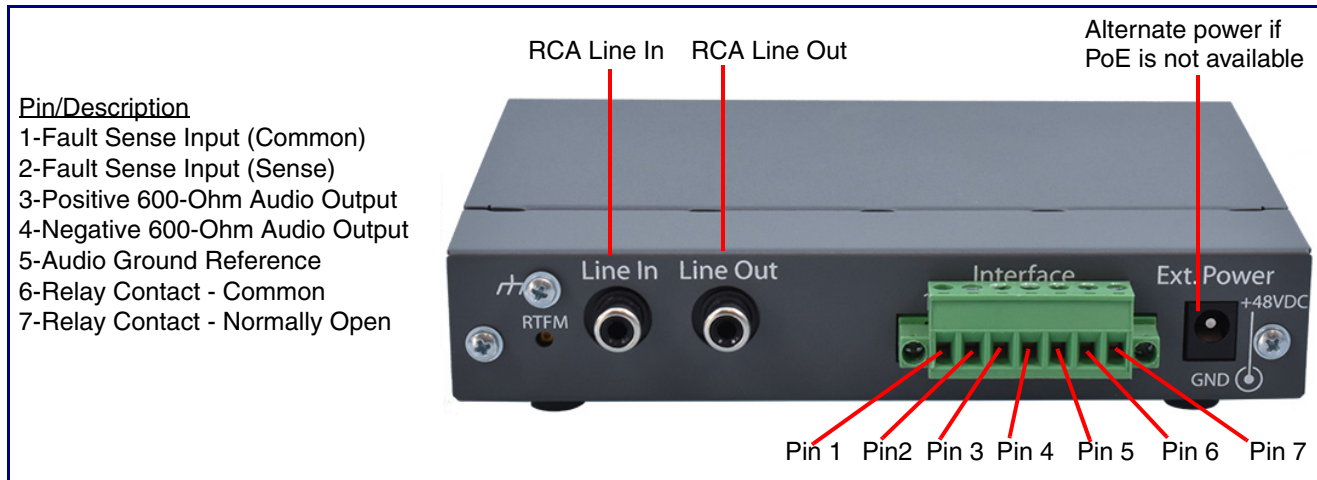
Chapter 1 Setting Up the SIP Paging Server	1
1.1 Connecting the SIP Paging Server	1
1.1.1 Ground Connection	1
1.1.2 Line In	1
1.1.3 Line Out	1
1.1.4 Page Port Output Connections	2
Pin 1 and 2—Fault Sense Input (Common/Sense)	2
Pin 3, 4, and 5—Positive/Negative 600-Ohm Audio Output/Audio Ground Reference	2
Pin 6 and 7—Relay Contact (Common/Normally Open)	2
1.1.5 Removable Interface Connector	3
1.1.6 Connect to the Power Source	4
Non-Poe	4
Chassis Ground	4
Poe	4
1.1.7 Connect to the Network	5
1.1.8 Confirm that the SIP Paging Server is Up and Running	6
Verify Network Activity	6
1.2 Announcing the IP Address	7
1.3 Restore the Factory Default Settings	8
1.4 Configuring the SIP Paging Server	9
1.4.1 Gather the Required Configuration Information	9
Static or DHCP Addressing?	9
Username and Password for Configuration GUI	9
SIP Settings	9
Chapter 2 Configure the Device	10
2.1 Log In Page	10
2.2 Home Page	11
2.3 Device	12
2.4 Network	13
2.5 SIP (Session Initiation Protocol)	14
2.5.1 Dial Out Extension Strings and DTMF Tones (using rfc2833)	15
2.5.2 Point-to-Point Configuration	15
2.6 Paging Groups (PGROUPS)	16
2.6.1 PGroup Configuration	17
2.7 SSL	18
2.8 Schedules	20
2.9 Fault	22
2.10 Audiofiles	23
2.11 Events	25
2.11.1 Example Packets for Events	26
2.12 Terminus	29
2.13 Autoprovisioning	30
2.14 Firmware	31
2.15 Admin	32
2.16 Command Interface	33
2.16.1 Command Interface Post Commands	33
Appendix A Troubleshooting/Technical Support	34
A.1 Contact Information	34
A.2 Warranty and RMA Information	34

1 Setting Up the SIP Paging Server

1.1 Connecting the SIP Paging Server

See [Figure 1-1](#) for the connection options that are available for the SIP Paging Server.

Figure 1-1. Connection Options



This equipment may be sensitive to ESD discharges. A certain level of performance might be impacted if this happens. Please take this precaution when installing and operating the equipment.

1.1.1 Ground Connection

This connection allows you to connect the device to an electrical ground.

1.1.2 Line In

This RCA 10K Ohm Hi-Z input connection allows you to connect the device to The RCA line-out (10K Ohm Hi-Z) of an external audio amplifier.

1.1.3 Line Out

This RCA 10K Ohm Hi-Z output connection allows you to connect the device to The RCA line-in (10K Ohm Hi-Z) of an external audio amplifier.

1.1.4 Page Port Output Connections

Table 1-1. Page Port Output Connections

Pin	Description
Pin 1	Fault Sense Input (Common). See Section 1.1.4.1, "Pin 1 and 2—Fault Sense Input (Common/Sense)" .
Pin 2	Fault Sense Input (Sense). See Section 1.1.4.1, "Pin 1 and 2—Fault Sense Input (Common/Sense)" .
Pin 3	Positive 600-Ohm Audio Output ^a . See Section 1.1.4.2, "Pin 3, 4, and 5—Positive/Negative 600-Ohm Audio Output/Audio Ground Reference" .
Pin 4	Negative 600-Ohm Audio Output ^a . See Section 1.1.4.2, "Pin 3, 4, and 5—Positive/Negative 600-Ohm Audio Output/Audio Ground Reference" .
Pin 5	Audio Ground Reference. See Section 1.1.4.2, "Pin 3, 4, and 5—Positive/Negative 600-Ohm Audio Output/Audio Ground Reference" .
Pin 6	Relay Contact - Common ^b . See Section 1.1.4.3, "Pin 6 and 7—Relay Contact (Common/Normally Open)" .
Pin 7	Relay Contact - Normally Open ^b . See Section 1.1.4.3, "Pin 6 and 7—Relay Contact (Common/Normally Open)" .

a. The 600-Ohm audio output of the page port is also suited for interfaces with lower input impedances.

b. 1 Amp at 30 VDC for continuous loads

1.1.4.1 Pin 1 and 2—Fault Sense Input (Common/Sense)

This input was designed as a method of monitoring an external amplifier that is equipped with a fault sense relay.

When enabled via the web interface ([Section 2.9, "Fault"](#)), this input (when closed) will play a user uploadable audio file out of the line-out connection and/or place a SIP call to a pre-determined extension and play that file.

1.1.4.2 Pin 3, 4, and 5—Positive/Negative 600-Ohm Audio Output/Audio Ground Reference

This output allows direct connection to paging amplifiers requiring a "Page Port" type input that meets a balanced 600 Ohm 5VPP signal.

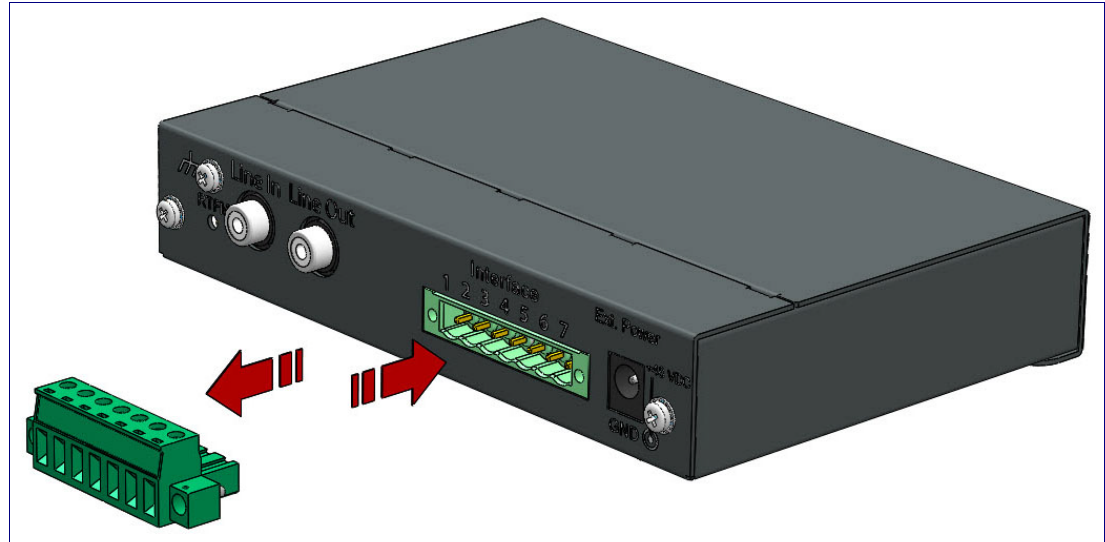
1.1.4.3 Pin 6 and 7—Relay Contact (Common/Normally Open)

When enabled on the web interface ([Section 2.3, "Device"](#)), every time an audio file is played out of the local line-out or 600 Ohm output, the relay will close, thereby enabling amplifiers with a remote turn-on capability to become active.

1.1.5 Removable Interface Connector

Figure 1-2 shows the interface connector that is removable on the SIP Paging Server.

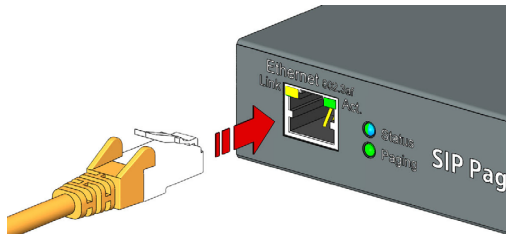
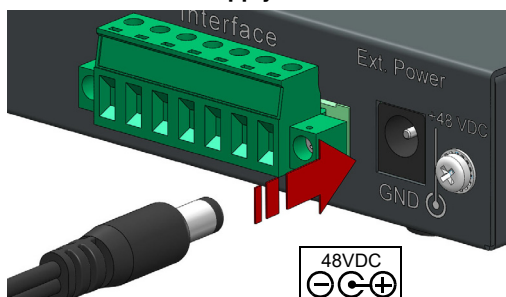
Figure 1-2. Removable Interface Connector



1.1.6 Connect to the Power Source

To use PoE, plug a Cat 5 Ethernet cable from the SIP Paging Server **Ethernet** port to your network. As an alternative to PoE, you can plug one end of a +48V DC power supply into the Paging Server, and plug the other end into a receptacle. If required, connect the earth grounding wire to the chassis ground on the back of the unit. See [Figure 1-3](#).

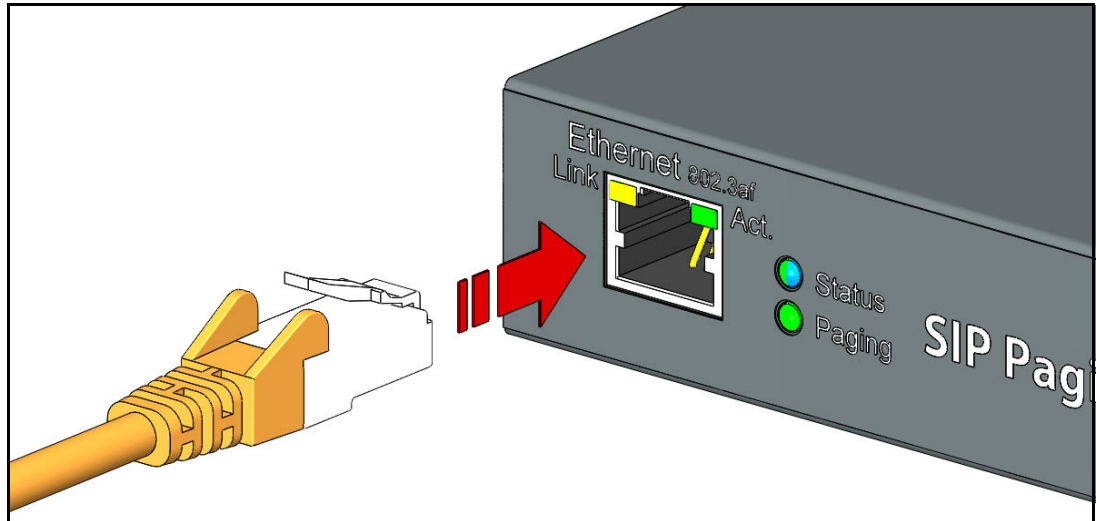
Figure 1-3. Connecting to the Power Source

PoE 	To set up the device, connect the device to your network: Poe For PoE, plug one end of an 802.3af Ethernet cable into the SIP Paging Server Ethernet port. Plug the other end of the Ethernet cable into your network. See the figure on the left.
Non PoE with 48 VDC Power Supply 	Non-Poe - For Non-PoE, connect the SIP Paging Server to a 48VDC power supply. See the figure on the left. Note: Do not use both PoE and external power.
Chassis Ground 	Chassis Ground If required, connect the earth grounding wire to the Chassis Ground. See the figure on the left.

1.1.7 Connect to the Network

Plug one end of a standard Ethernet cable into the SIP Paging Adapter **Ethernet** port. Plug the other end into your network.

Figure 1-4. Connecting to the Network



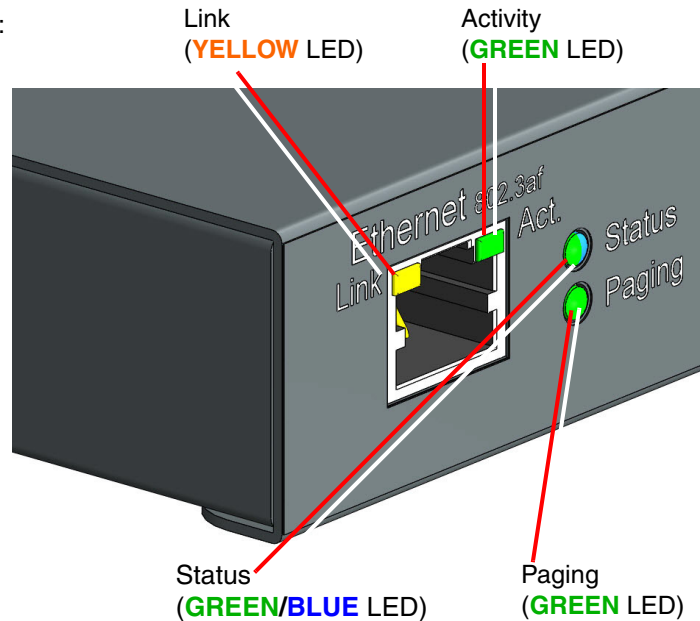
1.1.8 Confirm that the SIP Paging Server is Up and Running

The LEDs on the front of the SIP Paging Server verify the unit's operations.

Figure 1-5. SIP Paging Adapter LEDs

When you plug in the Ethernet cable or power supply:

- The **GREEN/BLUE Status** LED and the **GREEN Paging** LED both blink at a rate of 10 times per second during the initial network setup.
- The round, **GREEN/BLUE Status** LED on the front of the SIP Paging Server comes on indicating that the power is on. Once the device has been initialized, this LED blinks at one second intervals.
- The square, **YELLOW Link** LED above the Ethernet port indicates that the network connection has been established at 100Mbit speed.
- The **GREEN Paging** LED comes on after the device is booted and initialized. This LED blinks when a page is in progress. You can disable **Beep on Initialization** on the **Device Configuration** page.



1.1.8.1 Verify Network Activity

The square, **GREEN Activity** LED blinks when there is network traffic.

1.2 Announcing the IP Address

To announce the IP address for the SIP Paging Server, briefly press and then quickly release the **RTFM** button. See [Figure 1-6](#).

Note The IP address announcement can be heard if a speaker or amplified speaker is connected to the unit.

Figure 1-6. RTFM Button



1.3 Restore the Factory Default Settings

The SIP Paging Server is delivered with factory set default values for the parameters in [Table 1-1](#). Use the **RTFM** button (see [Figure 1-7](#)) on the back of the unit to restore these parameters to the factory default settings.

Figure 1-7. RTFM Button



Note When you perform this procedure, the factory default settings are restored. The default parameters for access are shown in [Table 1-1](#).

Table 1-1. 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.

To restore these parameters to the factory default settings:

1. Press and hold the **RTFM** button until the status and paging lights come on.
2. Continue to press the button until after the indicator lights go off, and then release it.

Note The “Restoring Defaults” announcement can be heard if a speaker or amplified speaker is connected to the unit.

3. The SIP Paging Server settings are restored to the factory defaults.

1.4 Configuring the SIP Paging Server

Use this section to configure the VoIP paging server.

1.4.1 Gather the Required Configuration Information

Have the following information available before you configure the SIP Paging Server.

1.4.1.1 Static or DHCP Addressing?

Know whether your system uses static or dynamic (DHCP) IP addressing. If it uses static addressing, you also need to know the values to assign to the following SIP Paging Server parameters:

- IP Address
- Subnet Mask
- Default Gateway

1.4.1.2 Username and Password for Configuration GUI

Determine the Username and Password that will replace the defaults after you initially log in to the configuration GUI.

- The Username is case-sensitive, and must be from four to 25 alphanumeric characters long.
- The Password is case-sensitive, and must be from four to 20 alphanumeric characters long.

1.4.1.3 SIP Settings

To configure the SIP parameters, determine whether you want to register with the server. If you do, determine the number of minutes the registration lease remains valid, and whether you want to automatically unregister when you reboot. To configure the SIP parameters, you also need to determine the values for these parameters:

- SIP Server IP Address
- Remote and Local SIP Port Numbers
- SIP User ID, and Authenticate ID and Password for this User ID

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 Paging Server.

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>

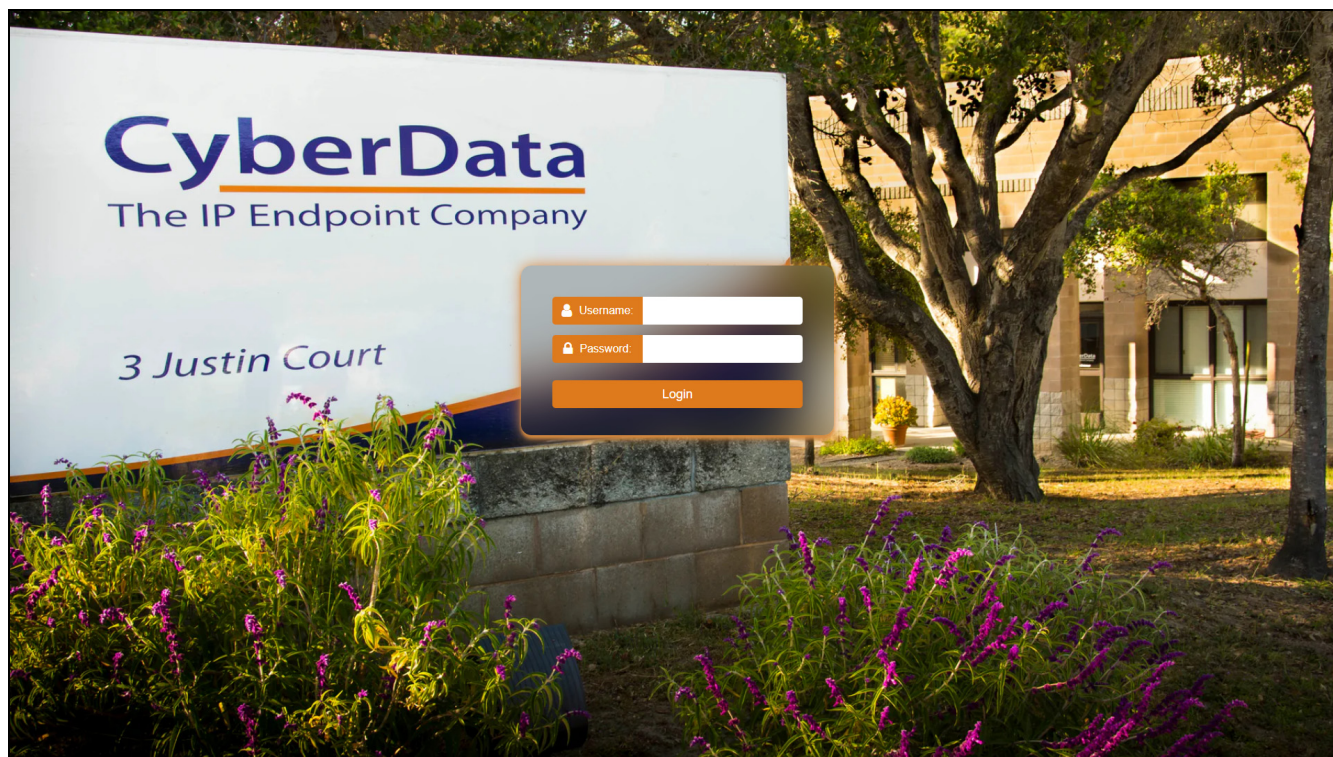
Note The Intercom ships in DHCP mode. To get to the **Home** page, use the discovery utility to scan for the device on the network and open your browser from there.

2. On the Log In Page (Figure 2-8), use the following default **Web Access Username** and **Web Access Password** to access the **Home Page** (Figure 2-9):

Web Access Username: **admin**

Web Access Password: **admin**

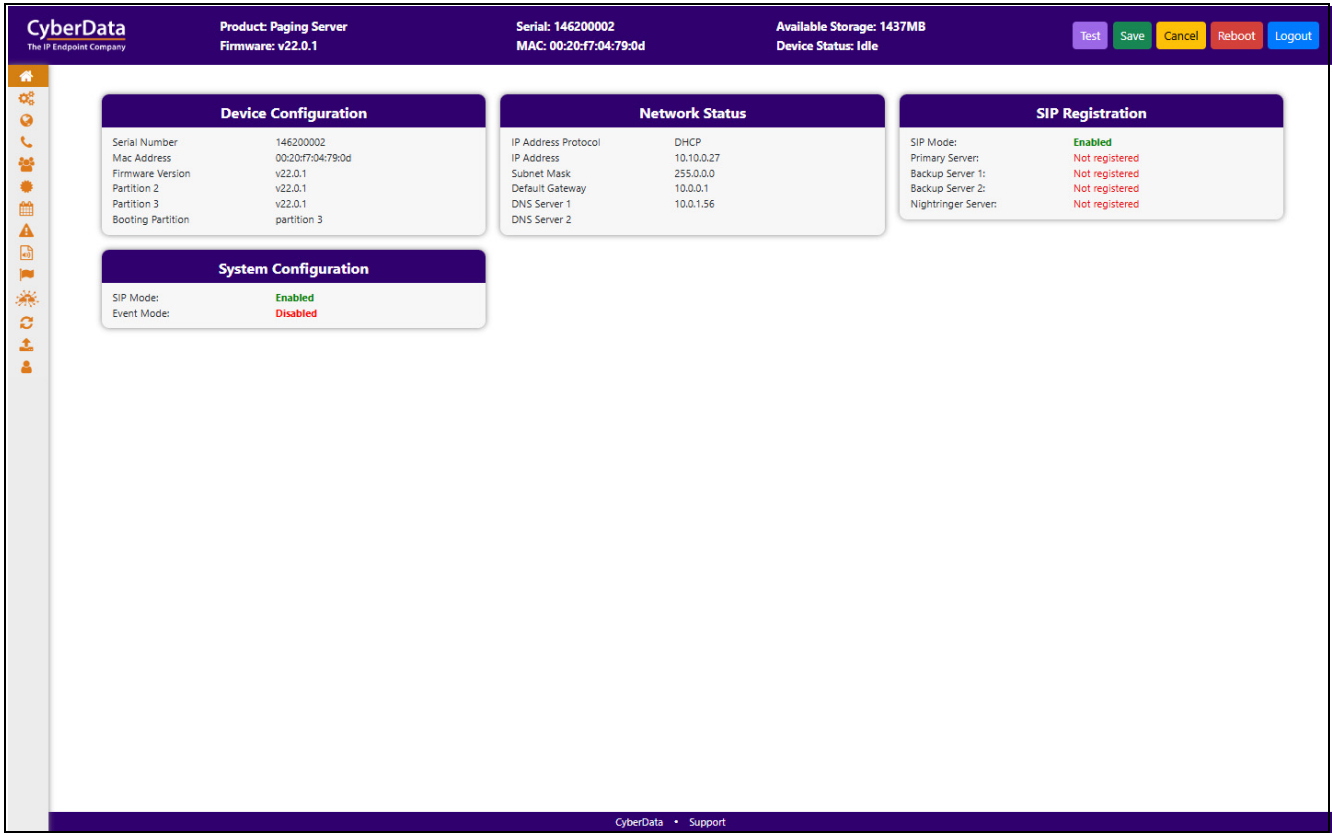
Figure 2-8. Log In Page



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 2-9. Home Page



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 2-10. Device Page

CyberData
The IP Endpoint Company

Product: Paging Server
Firmware: v22.0.1

Serial: 146200002
MAC: 00:20:f7:04:79:0d

Available Storage: 1437MB
Device Status: Idle

TestSaveCancelRebootLogout

Line-in Settings

Line-in to Line-out Loopback: OFF
Line-in to Multicast: OFF
Multicast Address: 224.1.2.3
Multicast Port: 2000
Detect Line-in Silence: OFF
Multicast Polycom Paging: OFF
Multicast Polycom Channel: 1

Time Settings

NTP Server: north-america.pool.ntp.org
NTP Timezone: America/Los_Angeles (-8)
Current Time: Sun, 17 Nov 2024 08:47:02

Misc Settings

Device Name: Paging Server
Bypass DTMF Menu: DISABLED
Beep on Init: OFF
Multicast TTL: 255

Relay Settings

Relay on Local Audio: OFF

CyberData • 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 2-11. Network Page

CyberData
The IP Endpoint Company

Product: Paging Server
Firmware: v22.0.1

Serial: 146200002
MAC: 00:20:f7:04:79:0d

Available Storage: 1437MB
Device Status: Idle

TestSaveCancelRebootLogout

Network Status

IP Address Protocol: DHCP
IP Address: 10.10.0.27
Subnet Mask: 255.0.0.0
Default Gateway: 10.0.0.1
DNS Server 1: 10.0.1.56
DNS Server 2:

Network Settings

Addressing Mode: DHCP
Hostname: SipDevice04790d
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/Ring 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 2-12. SIP Page

CyberData The IP Endpoint Company

Product: Paging Server
Firmware: v22.0.1

Serial: 146200002
MAC: 00:20:f7:04:79:0d

Available Storage: 1437MB
Device Status: Idle

Test Save Cancel Reboot Logout

SIP Settings

SIP Operation: ☐ ENABLED

SIP Registrations: ☐ ENABLED

Buffer SIP Calls: ☐ DISABLED

Beep Before Paging: ☐ OFF

Remote SIP Port: 5060

Local SIP Port: 5060

SIP Transport Protocol: ☐ UDP

TLS Version: 1.2

Verify Server Certificate: ☐ OFF

Outbound Proxy: Outbound Proxy

Outbound Proxy Port: 0

Cisco SRST: ☐ OFF

Disable rport Discovery: ☐ OFF

Keep Alive Timeout: 10000 milliseconds (ms)

Terminate call after delay: 0 seconds

Audio Codec: Auto Select

RTP Port (even): 10500

Asymmetric RTP: ☐ OFF

Jitter Buffer: 50

RTP Encryption (SRTP): ☐ DISABLED

SIP Server Settings

Primary SIP Server: 10.0.0.253

Primary SIP User ID: 199

Primary SIP Auth ID: 199

Primary SIP Auth Password: *****

Registration Interval: 360 seconds

Backup SIP Server 1: Host or IP address

Backup SIP User ID: Backup SIP User ID

Backup SIP Auth ID: Backup SIP Auth ID

Backup SIP Auth Password: Backup SIP Auth Password

Registration Interval: 360 seconds

Backup SIP Server 2: Host or IP address

Backup SIP User ID: Backup SIP User ID

Backup SIP Auth ID: Backup SIP Auth ID

Backup SIP Auth Password: Backup SIP Auth Password

Registration Interval: 360 seconds

Nightringer Settings

SIP Server: Host or IP address

SIP User ID: User ID

SIP Auth ID: Auth ID

SIP Auth Password: Password

Registration Interval: 360 seconds

Nightringer to Multicast: ☐ OFF

Multicast Address: 224.1.2.32

Multicast Port: 2020

Polycom Paging: ☐ OFF

Polycom Channel: 1

CyberData • Support

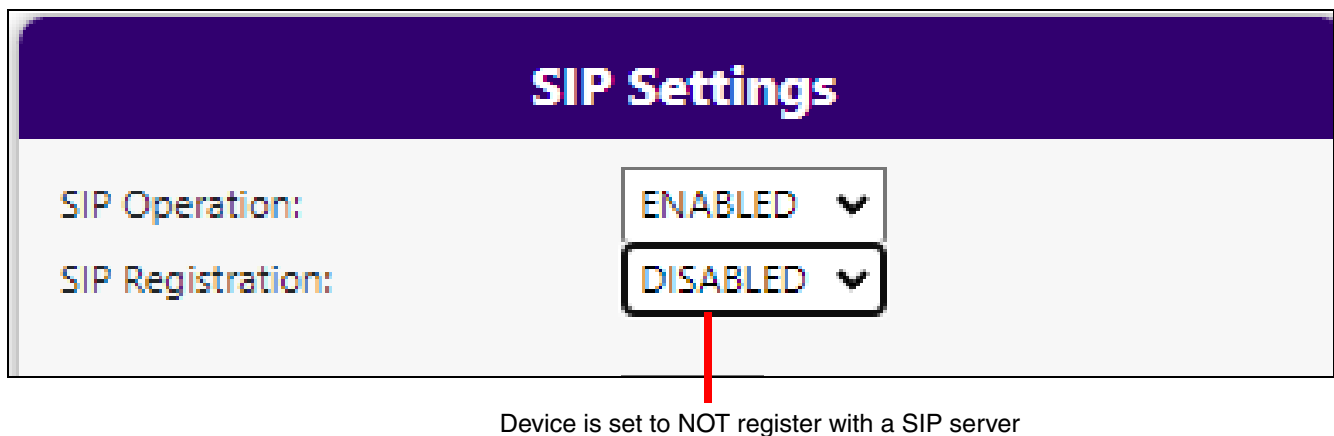
2.5.1 Dial Out Extension Strings and DTMF Tones (using rfc2833)

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 2-13](#).

Figure 2-13. SIP Page Set to Point-to-Point Mode



2.6 Paging Groups (PGROUPS)

The **PGroups** page allows for configuration of the PGroup(s) including stored message playback and Polycom Paging.

Figure 2-14. PGROUPS Page

CyberData
The IP Endpoint Company

HOME
DEVICE
NETWORK
SIP
PGROUPS
SSL
SCHEDULE
FAULT
AUDIOFILES
EVENTS
TERMINUS
AUTOPROV
FIRMWARE
ADMIN

Product: Paging Server
Firmware: v22.0.1

Serial: 146200002
MAC: 00:20:f7:04:79:0d

Available Storage: 1437MB
Device Status: Idle

Test Save Cancel Reboot Logout

Stored Message Recording

Stored Message Recording:

DISABLED

Recording Security Code:

Paging Groups

#	Address	Port	Name	Code	TTL	Lineout	
0	234.2.1.1	2000	PagingGroup00		255	Yes	Edit
1	234.2.1.2	2002	PagingGroup01		255	Yes	Edit
2	234.2.1.3	2004	PagingGroup02		255	Yes	Edit
3	234.2.1.4	2006	PagingGroup03		255	Yes	Edit
4	234.2.1.5	2008	PagingGroup04		255	Yes	Edit
5	234.2.1.6	2010	PagingGroup05		255	Yes	Edit
6	234.2.1.7	2012	PagingGroup06		255	Yes	Edit
7	234.2.1.8	2014	PagingGroup07		255	Yes	Edit
8	234.2.1.9	2016	PagingGroup08		255	Yes	Edit
9	234.2.1.10	2018	PagingGroup09		255	Yes	Edit

<

1

2

3

4

5

6

7

8

9

10

>

CyberData • Support

2.6.1 PGroup Configuration

To use Polycom Group Paging, configure a multicast group with the IP address and port number of the Polycom phone. The default is 224.0.1.116, port 5001, but can be configured through the phone. Polycom defaults to channels 1, 24, and 25, but can also be configured. The payload should be 20 ms and the codec G711.Mu.

Figure 2-15. PGroup Configuration

Configure PGROUP

PGROUP	0
Address	234.2.1.1
Port	2000
Name	PagingGroup00
Security Code	0-9, *, #
TTL	255
Line-out	☒
Play Stored Message	☐
Audio File	Choose a MSG
Times to Play	1
Send Polycom Page	☐
Polycom Transmit Channel	1

Save

Cancel

2.7 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 2-16. SSL Page (1 of 2)

The screenshot displays the CyberData SSL configuration interface. At the top, a header bar shows the CyberData logo, product information (Paging Server, v22.0.1), serial number (146200002), MAC address (00:20:f7:04:79:0d), available storage (1437MB), and device status (Idle). Navigation buttons (Test, Save, Cancel, Reboot, Logout) are on the right.

Below the header, three main sections are visible:

- Web Server Certificate:** Displays certificate details (subject, countryName, stateOrProvinceName, localityName, organizationName, commonName, notBefore, notAfter) and buttons for 'Import Web Certificate' and 'Restore Web Certificate'.
- SIP Client Certificate:** Displays certificate details and buttons for 'Import SIP Certificate' and 'Restore SIP Certificate'. A 'Password (optional):' field is present.
- Autoprovisioning Client Certificate:** Displays certificate details and buttons for 'Import Autoprovisioning Certificate' and 'Restore Autoprovisioning Certificate'. A 'Password (optional):' field is present.

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

List of Trusted CAs	
Upload CA Certificate: Choose Files No file chosen Import CA Certificate	
Download CyberData CA Generate Cyberdata CSR Remove All Restore Defaults	
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

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

Figure 2-17. SSL Page (2 of 2)

CyberData
The IP Endpoint Company

Product: Paging Server
Firmware: v22.0.1

Serial: 146200002
MAC: 00-20-f7:04:79-0d

Available Storage: 1437MB
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

2.8 Schedules

Figure 2-18. Schedules Page

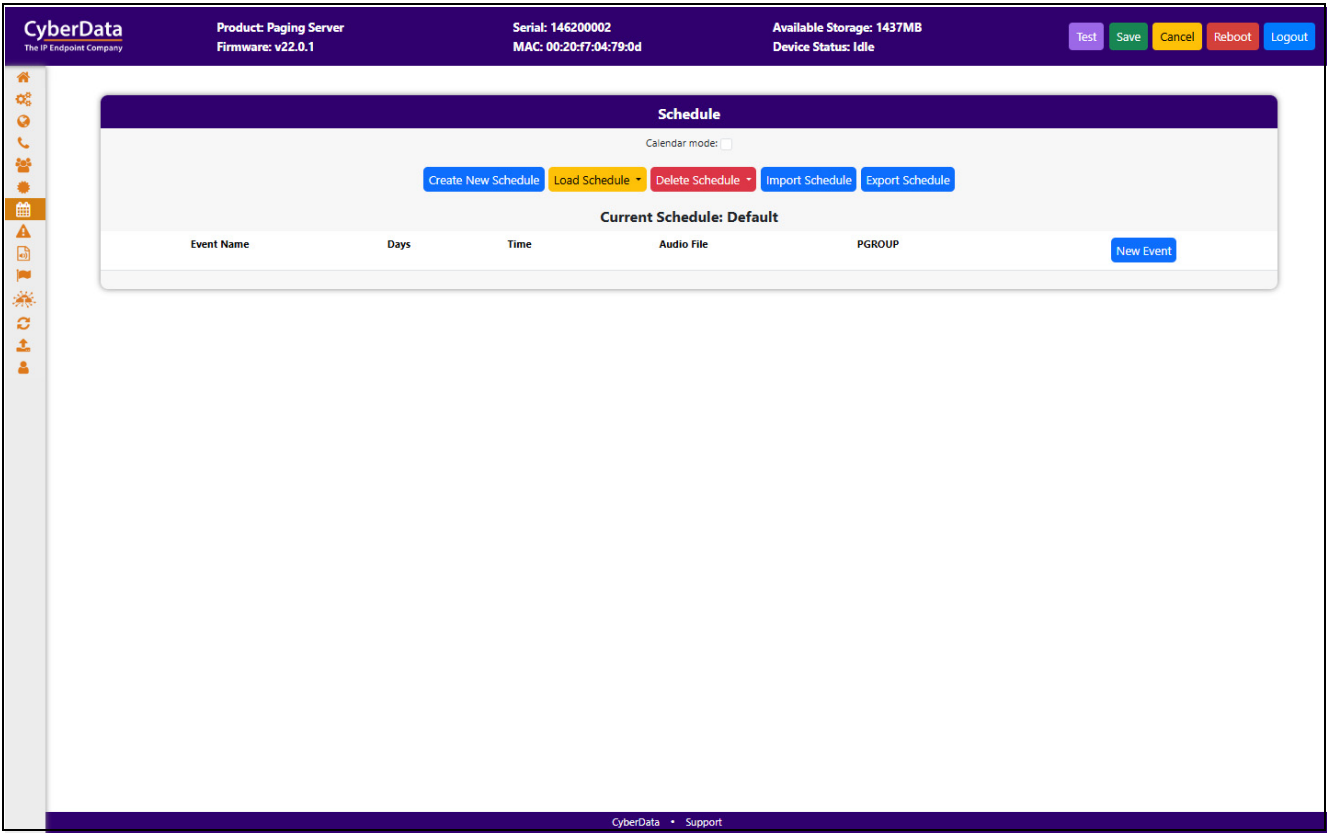


Figure 2-19. Calendar

CyberData
The IP Endpoint Company

Product: Paging Server
Firmware: v22.0.1

Serial: 146200002
MAC: 00:20:17:04:79:0d

Available Storage: 1437MB
Device Status: Idle

Test Save Cancel Reboot Logout

Calendar

Calendar model: ☒

Create New Calendar Load Calendar Delete Calendar Import Calendar Export Calendar

Current Calendar: sample

New Event <<< < November 2024 > >>> View Past

SUN	MON	TUE	WED	THU	FRI	SAT
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

CyberData • Support

2.9 Fault

The **Fault** page controls configuration of all Fault or sensor related capabilities of the unit. This can include the fault sensor that is used to have the device take action based on a physical input to the device.

Figure 2-20. Fault Page

The screenshot displays the CyberData web interface for a Paging Server. The top header bar contains the following information:

- CyberData** The IP Endpoint Company
- Product:** Paging Server
- Serial:** 146200002
- Available Storage:** 1437MB
- Firmware:** v22.0.1
- MAC:** 00:20:f7:04:79:0d
- Device Status:** Idle

On the right side of the header, there are buttons for **Test**, **Save**, **Cancel**, **Reboot**, and **Logout**.

The left sidebar contains the following navigation links:

- HOME
- DEVICE
- NETWORK
- SIP
- PGROUPS
- SSL
- SCHEDULE
- FAULT** (highlighted)
- AUDIOFILES
- EVENTS
- TERMINUS
- AUTOPROV
- FIRMWARE
- ADMIN

The main content area displays the **Fault Detection Settings** form with the following fields:

- Message Playbacks:** 0
- Play Message Locally:** DISABLED
- Call to Extension:** DISABLED
- Dial Out Extension:** 204
- Dial Out ID:** id204
- Multicast Audio:** DISABLED
- Multicast Address:** 239.168.3.1
- Multicast Port:** 8888
- Polycom Paging:** DISABLED
- Polycom Paging Channel:** 1

At the bottom of the interface, there is a footer bar with the text **CyberData • Support**.

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 2-21. Audiofiles Page (1 of 3)

Name	Current set to	default	Choose File	No file chosen	Play	Save	Delete
0:		default	Choose File	No file chosen	Play	Save	Delete
1:		default	Choose File	No file chosen	Play	Save	Delete
2:		default	Choose File	No file chosen	Play	Save	Delete
3:		default	Choose File	No file chosen	Play	Save	Delete
4:		default	Choose File	No file chosen	Play	Save	Delete
5:		default	Choose File	No file chosen	Play	Save	Delete
6:		default	Choose File	No file chosen	Play	Save	Delete
7:		default	Choose File	No file chosen	Play	Save	Delete
8:		default	Choose File	No file chosen	Play	Save	Delete
9:		default	Choose File	No file chosen	Play	Save	Delete
Audio Test:		default	Choose File	No file chosen	Play	Save	Delete
Dot:		default	Choose File	No file chosen	Play	Save	Delete
Night Ring:		default	Choose File	No file chosen	Play	Save	Delete
Page Tone:		default	Choose File	No file chosen	Play	Save	Delete
Rebooting:		default	Choose File	No file chosen	Play	Save	Delete
Restoring Default:		default	Choose File	No file chosen	Play	Save	Delete
Ringback Tone:		default	Choose File	No file chosen	Play	Save	Delete
Ring Tone:		default	Choose File	No file chosen	Play	Save	Delete
Sensor Triggered:		default	Choose File	No file chosen	Play	Save	Delete
Stored Message File Not Found:		default	Choose File	No file chosen	Play	Save	Delete
Your IP Address Is:		default	Choose File	No file chosen	Play	Save	Delete
Enter Zone:		default	Choose File	No file chosen	Play	Save	Delete
Confused:		default	Choose File	No file chosen	Play	Save	Delete

Figure 2-22. Audiofiles Page (2 of 3)

Menu Audio Files					
Cancel:	Currently set to:	default	Choose File No file chosen	Play	Save Delete
Currently Playing:	Currently set to:	default	Choose File No file chosen	Play	Save Delete
Invalid Entry:	Currently set to:	default	Choose File No file chosen	Play	Save Delete
Page:	Currently set to:	default	Choose File No file chosen	Play	Save Delete
Play Stored Message:	Currently set to:	default	Choose File No file chosen	Play	Save Delete
Pound (#):	Currently set to:	default	Choose File No file chosen	Play	Save Delete
Press:	Currently set to:	default	Choose File No file chosen	Play	Save Delete
Stored Message:	Currently set to:	default	Choose File No file chosen	Play	Save Delete
To:	Currently set to:	default	Choose File No file chosen	Play	Save Delete
Enter Code:	Currently set to:	default	Choose File No file chosen	Play	Save Delete
Enter Recording Security Code:	Currently set to:	default	Choose File No file chosen	Play	Save Delete
Invalid Code:	Currently set to:	default	Choose File No file chosen	Play	Save Delete
Press Start To Record Message:	Currently set to:	default	Choose File No file chosen	Play	Save Delete
Or:	Currently set to:	default	Choose File No file chosen	Play	Save Delete
Record Message Prompt:	Currently set to:	default	Choose File No file chosen	Play	Save Delete
Save Record Message Prompt:	Currently set to:	default	Choose File No file chosen	Play	Save Delete
Assign Zone To Message:	Currently set to:	default	Choose File No file chosen	Play	Save Delete
Message Saved Successfully:	Currently set to:	default	Choose File No file chosen	Play	Save Delete
Message Not Saved Successfully:	Currently set to:	default	Choose File No file chosen	Play	Save Delete
You Recorded:	Currently set to:	default	Choose File No file chosen	Play	Save Delete

Figure 2-23. Audiofiles Page (3 of 3)

Recorded Messages	
Choose File No file chosen	Upload Message Delete All Messages

Bells	
Choose File No file chosen	Upload Bell Delete All Bells

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 2-24. Events Page

CyberData
The IP Endpoint Company

Product: Paging Server
Firmware: v22.0.1

Serial: 146200002
MAC: 00:20:f7:04:79:0d

Available Storage: 1438MB
Device Status: Idle

Test Save Cancel Reboot Logout

Event Server

Event Generation: DISABLED

Server IP Address:

Server Port:

Server URL:

Events

Application Started Events: DISABLED

Heartbeat Events: DISABLED

Call Started Events: DISABLED

Call Terminated Events: DISABLED

Ring Events: DISABLED

Nightring Events: DISABLED

Multicast Started Events: DISABLED

Multicast Stopped Events: DISABLED

Relay Activated Events: DISABLED

Relay Deactivated Events: DISABLED

Fault Events: DISABLED

CyberData • Support

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>APPLICATION_STARTED</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 2-25. Terminus Page

The screenshot displays the Terminus configuration interface. The header bar is purple and contains the following information:

- CyberData** The IP Endpoint Company
- Product:** Paging Server
- Firmware:** v22.0.1
- Serial:** 146200002
- MAC:** 00:20:f7:04:79:0d
- Available Storage:** 1438MB
- Device Status:** Idle
- Buttons: Test, Save, Cancel, Reboot, Logout

The main configuration area is divided into three sections:

- Cloud Configuration:** Includes a "Cloud Enrollment" button and a "Terminus Service" dropdown menu set to "ENABLED".
- Discovery Setting:** Includes input fields for "Multicast Address" (239.27.32.4), "Time to Live" (255), and "Discovery Interval" (60 seconds).
- Lockdown Settings:** Includes a "Lock Down Mode" dropdown set to "Disabled" and a "Relay" dropdown set to "No Action".

A sidebar on the left contains icons for various system functions. The footer at the bottom of the page shows the CyberData logo and a link to "Support".

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:

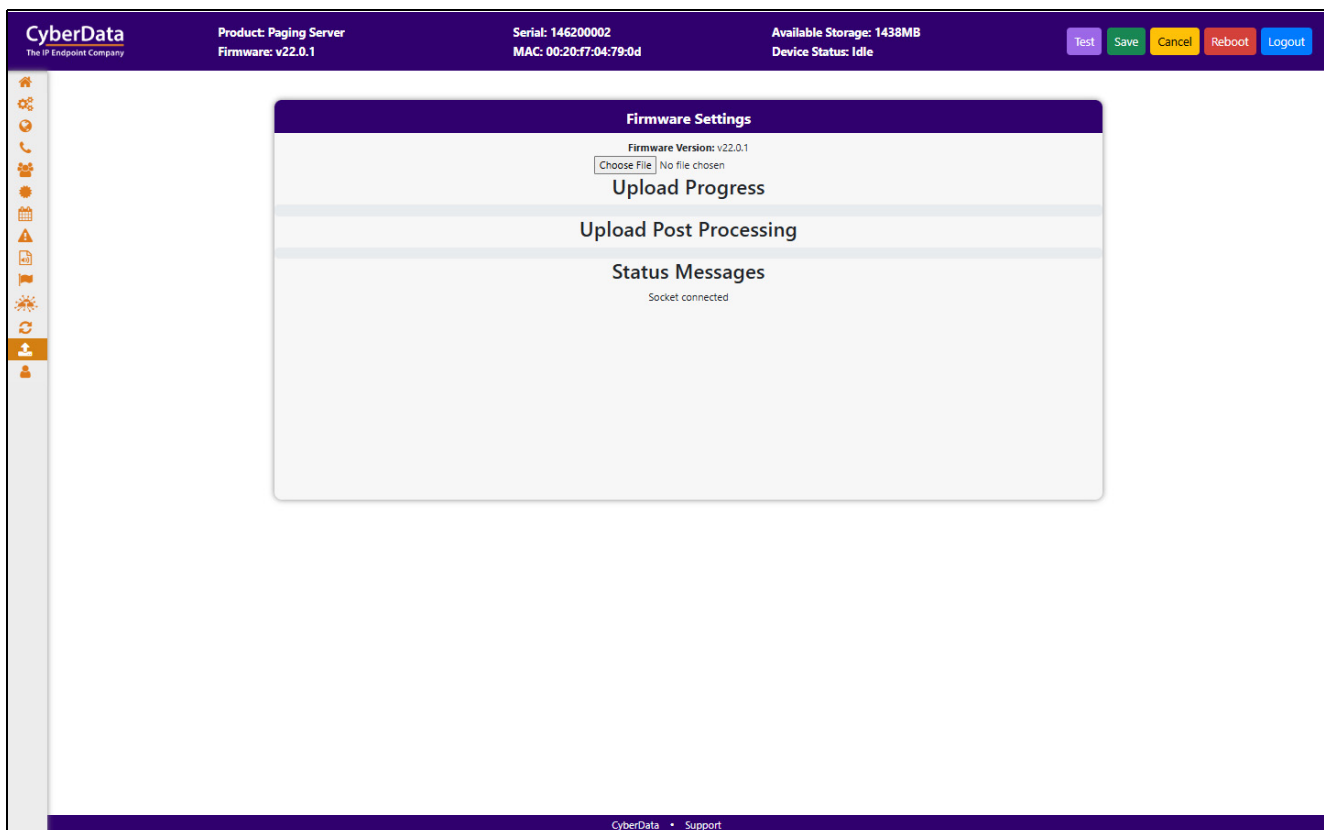
<https://www.cyberdata.net/collections/sip>

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

- Firmware file
- Release notes
- Autoprovisioning template

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

Figure 2-27. 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 2-28. Admin Page

The screenshot displays the CyberData Admin Page interface. At the top, a header bar contains the CyberData logo, product information (Paging Server, v22.0.1), serial and MAC addresses, available storage (1438MB), and device status (Idle). Navigation buttons (Test, Save, Cancel, Reboot, Logout) are on the right. A left sidebar shows a vertical menu of icons. The main content area is divided into several sections:

- Admin Settings:** Fields for Username (admin), Password (masked), and Confirm Password (masked).
- Statistics:** Displays Storage (1438MB), Boot Count (40), Reboot Count (37), and Uptime (up 3 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. A note states: "Retrieving the log files may take some time due to their size."
- Configuration Settings:** Shows Partition 2 (v22.0.1), Partition 3 (v22.0.1), 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:** Features buttons for Add New User, Delete All Users, Import Users, and Export Users. Below is a table with columns: Username, Home, Device, Network, SIP, PGROUPS, SSL, Schedule, Fault, Audiofiles, Events, Autoprov, Firmware, Admin, Terminus, Edit, and Delete. One user, 'sked', is listed.
- Log Viewer:** Includes a Service dropdown (Application), Entries to get (250), Sort dropdown (Oldest), and a View Log button.

The footer of the page shows "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

The commands in [Table 2-2](#) 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	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.247/command" --post-data "request=reboot"
Place call to extension (example: extension 600)	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.247/command" --post-data "request=call&extension=600"
Terminate a call	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.247/command" --post-data "request=terminate"
Test Relay	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.247/command" --post-data "request=test_relay"
Activate Relay	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.247/command" --post-data "request=activate_relay"
Deactivate Relay	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.247/command" --post-data "request=deactivate_relay"
Speak IP Address	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.247/command" --post-data "request=speak_ip_address"
Test Audio	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.247/command" --post-data "request=test_audio"
Swap Boot partitions	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.10.1.81/command" --post-data "request=swap_boot_partition"

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 32
Audiofiles 23
Autoprovisioning 30

C

Calendar 21
Command Interface 33
Contact Information 34

D

Device 12
Dial Out Extension Strings and DTMF Tones 15
Discovery Utility program 10

E

Events 25

F

Fault 22
Firmware 31

H

Home Page 11

P

Paging Groups (PGROUPS) 16
Point-to-Point Configuration 15

S

Schedules 20
SSL 18

T

Terminus 29
Troubleshooting/Technical Support 34

W

Warranty and RMA Information 34