



SIP Paging Server + Operations Guide

SIP Compliant
Part #011600, 011601

Document Part #932090A
for Firmware Version 23.1

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

COPYRIGHT NOTICE:
© 2026, 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 932090A, which corresponds to firmware version 23.1, was released on March 28, 2026.

Important Safety Instructions

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

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

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

Pictorial Alert Icons

 GENERAL ALERT	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	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.

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

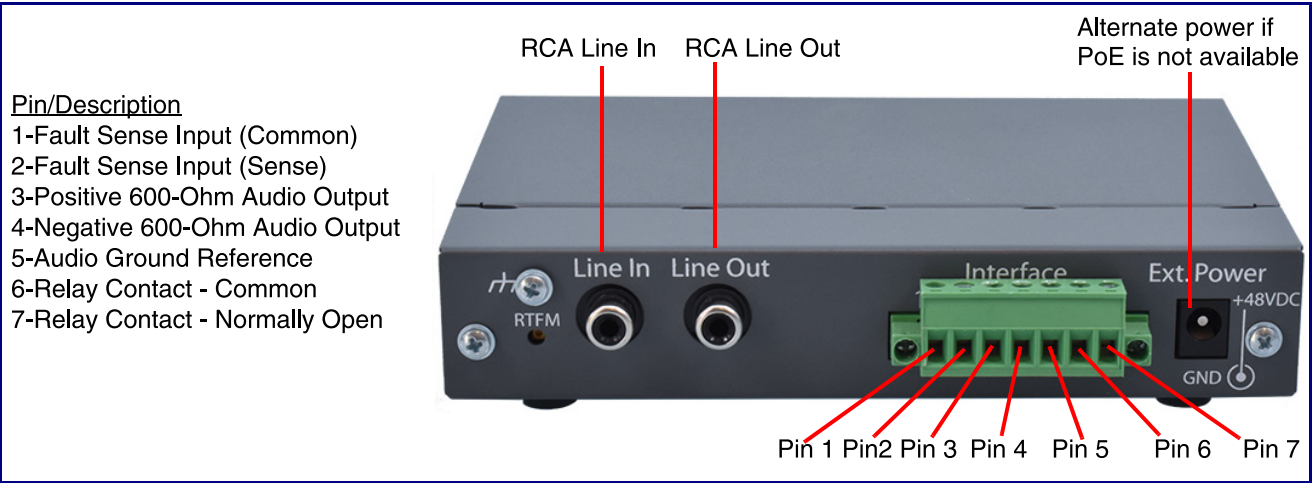
Chapter 1. Product Overview	1
1.1 Connecting the Paging Server Plus	1
1.1.1 Ground Connection	1
1.1.2 Line In	1
1.1.3 Line Out	1
1.1.4 Page Port Output Connections	2
1.1.5 Removable Interface Connector	3
1.1.6 Connect to the Power Source	4
1.1.7 Connect to the Network	5
1.1.8 Confirm that the SIP Paging Server is Up and Running	6
1.2 Announcing the IP Address	7
1.3 Restore the Factory Default Settings	8
Chapter 2. Configure the Device	9
2.1 Log In Page	
2.2 Home Page	10
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 Multicast	20
2.9 Schedules	21
2.10 Fault	23
2.11 Audiofiles	24
2.12 Terminus	26
2.13 Autoprovisioning	27
2.14 Firmware	28
2.15 Admin	29
2.16 Command Interface	30
2.16.1 Command Interface Post Commands	30
Appendix A: Troubleshooting/Technical Support	31
Index	32

Chapter 1. Product Overview

1.1 Connecting the SIP Paging Server +

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

Figure 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. 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.

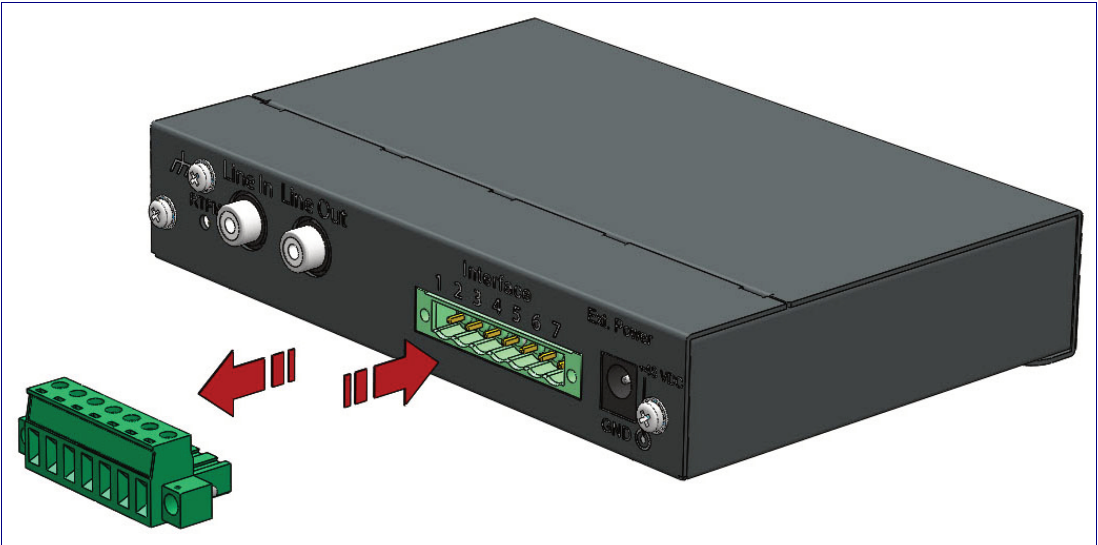
1.1.4.3 Pin 6 and 7—Relay Contact (Common/Normally Open)

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 2 shows the interface connector that is removable on the SIP Paging Server +.

Figure 2. Removable Interface Connector



1.1.6 Connect to the Power Source

To use PoE, plug a Cat 5 Ethernet cable from the device Ethernet port to your network. As an alternative to PoE, you can plug one end of a +48V DC power supply into the device, 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 3.

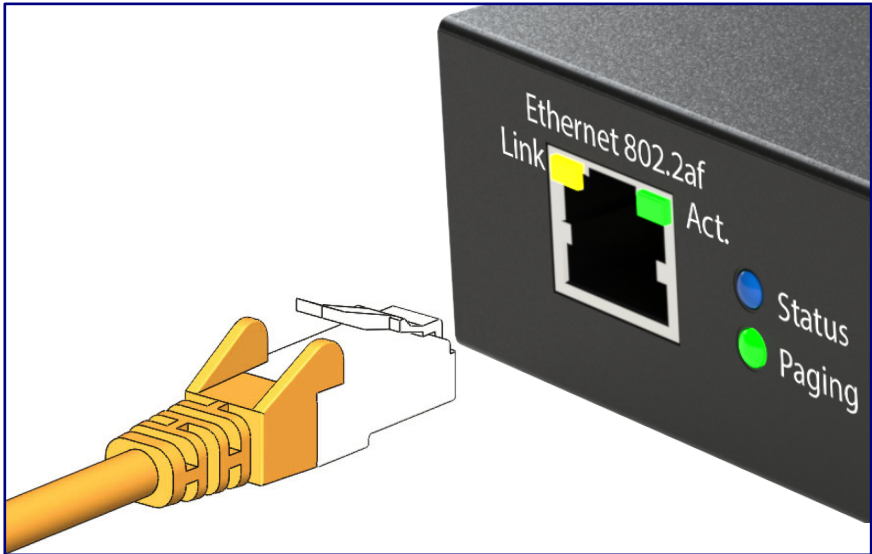
Figure 3. Connecting to the Power Source

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 device 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 device 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 device Ethernet port. Plug the other end into your network.

Figure 4. Connecting to the Network



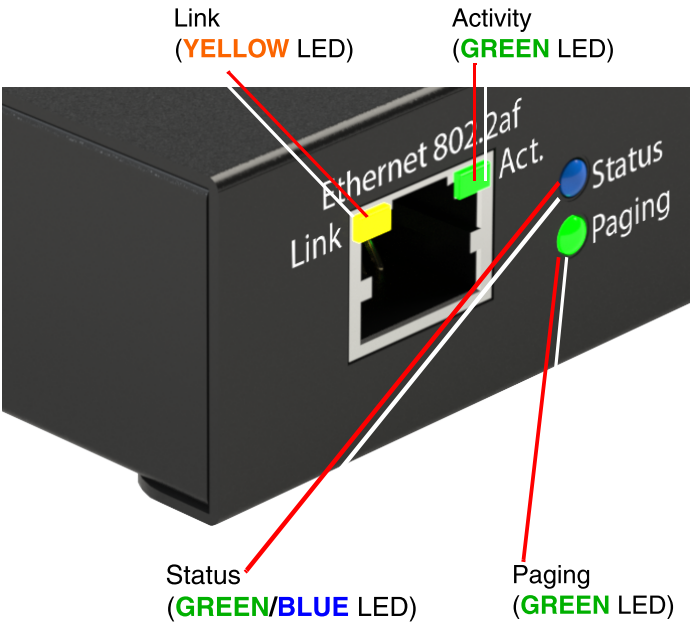
1.1.8 Confirm that the Device is Up and Running

The LEDs on the front of the device verify the unit's operations.

Figure 5. 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 device, briefly press and then quickly release the **RTFM** button. See [Figure 6](#).

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

Figure 6. RTFM Button



1.3 Restore the Factory Default Settings

The device is delivered with factory set default values for the parameters in [Table 2](#). Use the RTFM button (see [Figure 8](#)) on the front of the unit to restore these parameters to the factory default settings.

Figure 7. RTFM Switch



Note When you perform this procedure, the factory default settings are restored. The default parameters for access are shown in [Table 2](#).

Table 2. 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. Use a paper clip to press the **RTFM** switch and hold for 10 seconds.
2. Release the switch. All the Paging Server settings are restored to the factory defaults, and the unit reboots.

Note: The “Restoring Defaults” announcement can be heard if a speaker or amplified speaker is connected to the unit, typically 45 seconds after releasing the switch.

Chapter 2. Configure the Device

2.1 Log In Page

1. Open your browser to the device’s IP address.
- Note

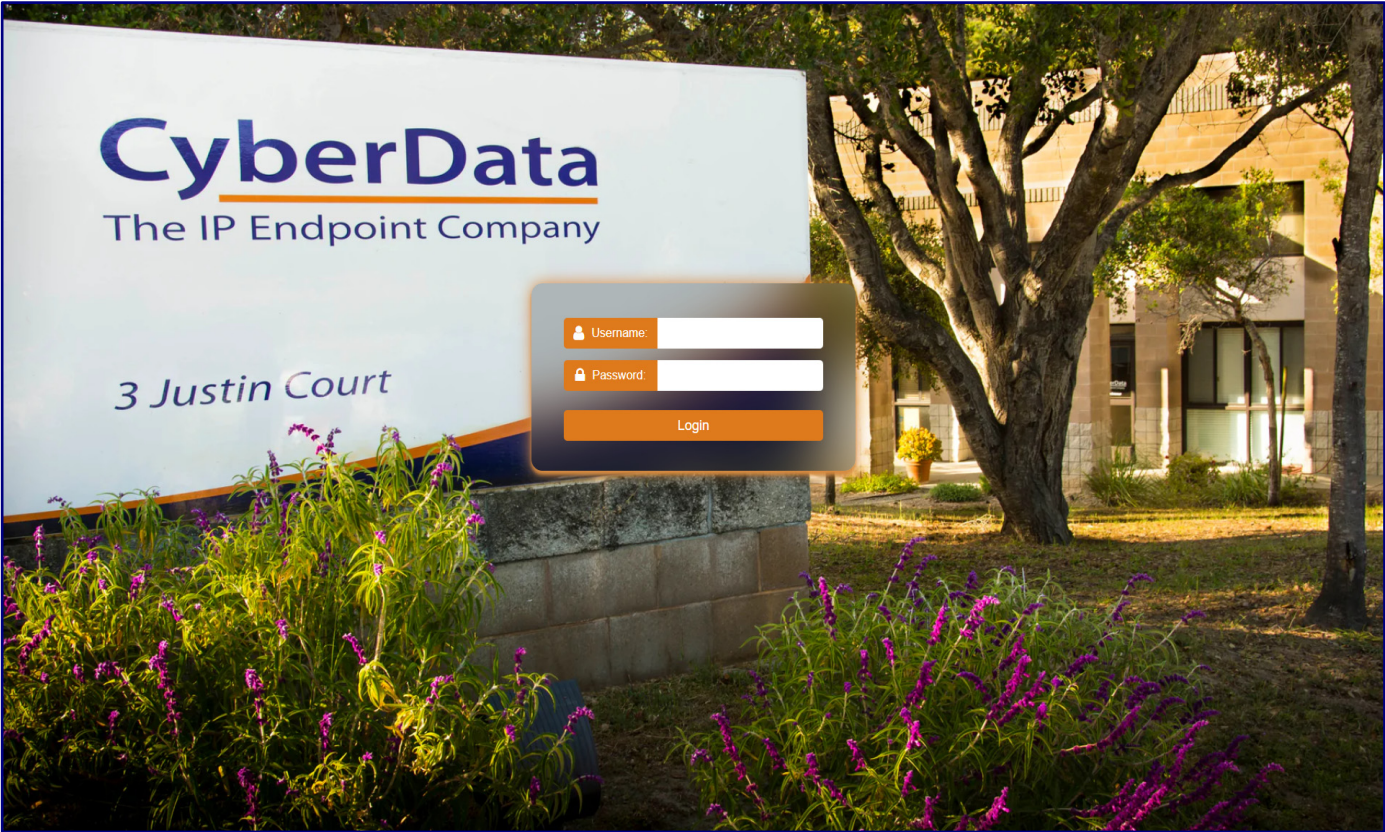
If the network does not have access to a DHCP server, the device will default to an IP address of 192.168.1.23.
- Note

Make sure that the PC is on the same IP network as the device.
- 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 8), use the following default **Web Access Username** and **Web Access Password** to access the **Home Page** (Figure 9):
- Web Access Username: **admin**
- Web Access Password: **admin**

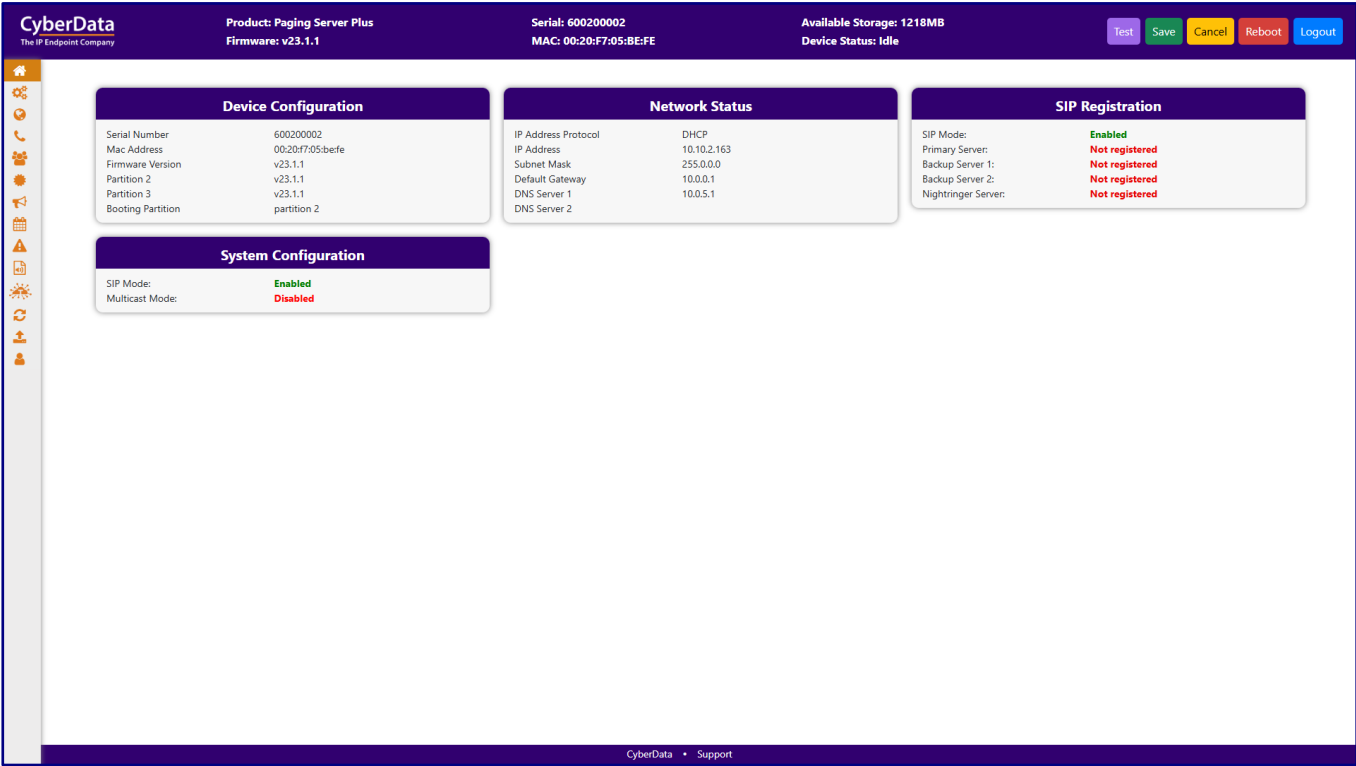
Figure 8. Log In Page



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 9. Home Page



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

Figure 10. 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 11. Device Configuration Page

CyberData

The IP Endpoint Company

Product: Paging Server Plus

Firmware: v23.1.1

Serial: 600200002

MAC: 00:20:F7:05:BE:FE

Available Storage: 1218MB

Device Status: Idle

Test

Save

Cancel

Reboot

Logout

Line-in Settings

Line-in to Line-out Loopback: OFF

Line-in Gain: 127

Line-in Playback Volume: 8

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(s): 45.56.66.53, 162.159.200.1, 45.63.54.13

NTP Timezone: America/Los_Angeles (-8)

Current Time: Sat, 14 Mar 2026 14:08:28

Menu Settings

Require Security Code: DISABLED

Security Code:

Bypass DTMF Menu: DISABLED

DTMF Duration: 500 milliseconds (ms)

Misc Settings

Device Name: Paging Server Plus

Beep on Init: OFF

Multicast TTL: 255

Relay Settings

Relay on Local Audio: OFF

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

Figure 12. InformaCast enabled Device

InformaCast Settings

InformaCast Server:

Host or IP address

InformaCast to Multicast:

DISABLED

Multicast Address:

224.1.7.8

Multicast Port:

5078

Multicast TTL:

255

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 13. Network Page

CyberData
The IP Endpoint Company

Product: Paging Server Plus
Firmware: v23.1.0

Serial: 600200002
MAC: 00:20:F7:05:BE:FE

Available Storage: 1218MB
Device Status: Idle

TestSaveCancelRebootLogout

Network Status

Network Settings

VLAN Settings

IP Address Protocol: DHCP
IP Address: 10.10.2.163
Subnet Mask: 255.0.0.0
Default Gateway: 10.0.0.1
DNS Server 1: 10.0.5.1
DNS Server 2: 10.0.5.1

Addressing Mode: DHCP
Hostname: SipDevice05befe
IP Address: 10.10.10.10
Subnet Mask: 255.0.0.0
Default Gateway: 10.0.0.1
DNS Server 1: 1.1.1.1
DNS Server 2: 8.8.8.8
DHCP Timeout: 60 seconds

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 14. SIP Page

CyberData
The IP Endpoint Company

Product: Paging Server Plus
Firmware: v23.1.0

Serial: 600200002
MAC: 00:20:F7:05:BE:FE

Available Storage: 1218MB
Device Status: Idle

TestSaveCancelRebootLogout

SIP Settings

SIP Server Settings

Nightringer Settings

SIP Operation: ENABLED
SIP Registration: 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

Primary SIP Server Status:
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 Status:
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 Status:
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 SIP Server Status:
Nightringer SIP Server: Host or IP address
Nightringer SIP User ID: User ID
Nightringer SIP Auth ID: Auth ID
Nightringer 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

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

Figure 15. InformaCast enabled Device

InformaCast SIP Config: DISABLED

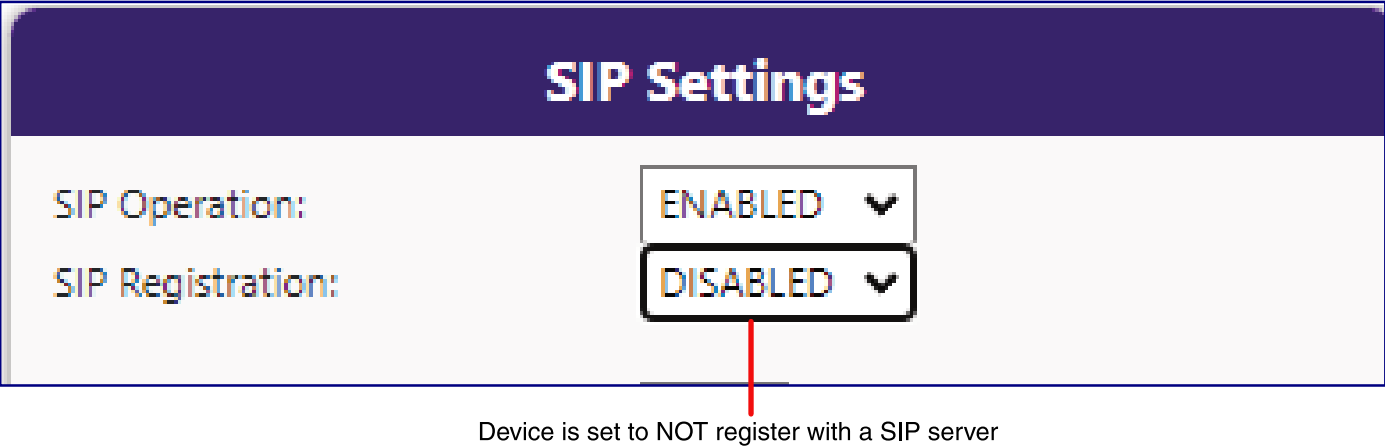
2.5.1 Dial Out Extension Strings and DTMF Tones (using rfc2833)

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 16](#).

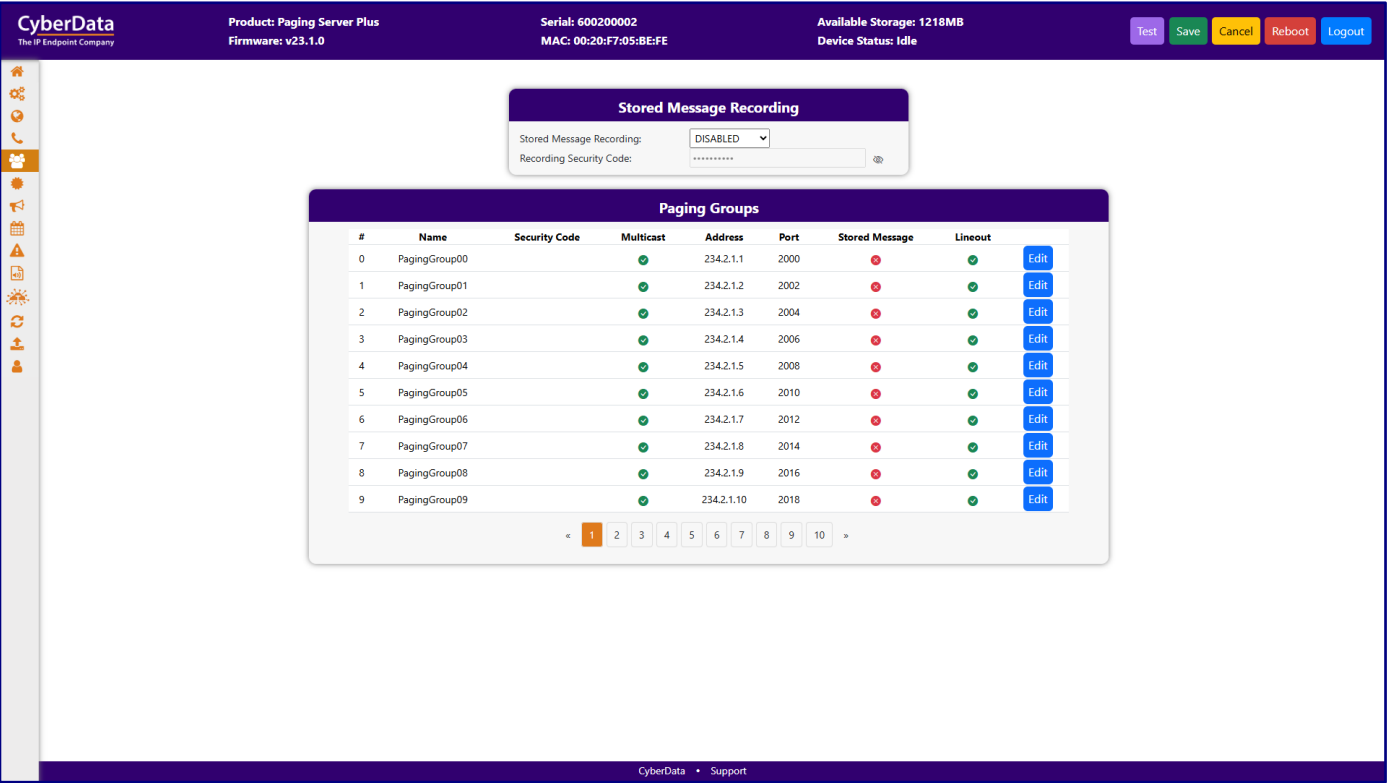
Figure 16. SIP Page Set to Point-to-Point Mode



2.6 Paging Groups (PGROUPS)

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

Figure 17. PGROUPS Page



2.6.1 PGroup Configuration

To use Polycom Group Paging, configure a multicast group with the IP address and port number from the Polycom phone and the next lowest even port number from the Poly phone. e.g., the poly port is the default 5001, the Paging Server should be set to port 5000.

Figure 18. PGroup Configuration

Configure PGROUP

PGROUP

Address

Port

Name

Security Code

TTL

Line-out

Play Stored Message

Audio File

Times to Play

Send Polycom Page

Polycom Transmit Channel

0

234.2.1.1

2000

PagingGroup00

0-9, *, #

255

☒

☐

Choose a MSG

1

☐

1

Zone One (Z1):

Zone Two (Z2):

Zone Three (Z3):

Zone Four (Z4):

ENABLED

ENABLED

ENABLED

ENABLED

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 19. SSL Page (1 of 2)

CyberData

Product: Paging Server Plus

Serial: 600200002

Available Storage: 1218MB

Firmware: v23.1.0

MAC: 00:20:F7:05:BE:FE

Device Status: Idle

Save

Cancel

Reboot

Logout

Web Server Certificate

SIP Client Certificate

Autoprovisioning Client Certificate

Upload CA Certificate

List of Trusted CAs

Figure 20. SSL Page (2 of 2)

CyberData
The IP Endpoint Company

Product: Paging Server Plus
Firmware: v23.1.0

Serial: 600200002
MAC: 00:20:F7:05:BE:FE

Available Storage: 1218MB
Device Status: Idle

TestSaveCancelRebootLogout

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
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 Multicast

The Multicast Configuration page allows the device to join up to ten paging zones for receiving RTP audio streams. A paging zone can consist of one or many CyberData multicast group-enabled products. There is no limit to how many speakers can participate 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. The device will prioritize simultaneous audio streams according to their priority in the list. If both SIP and Multicast is enabled, SIP audio streams are considered priority 4.5. SIP audio will interrupt multicast streams with priority 0 through 4 and will be interrupted by multicast streams with priority 5 through 9.

Ringtones all play at the same priority level. This means that it is possible to have a nightring tone and a normal ringtone playing at the same time.

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 G711mu.

Figure 21. Multicast Page

CyberData
The IP Endpoint Company

Product: Paging Server Plus
Firmware: v23.1.0

Serial: 600200002
MAC: 00:20:F7:05:BE:FE

Available Storage: 1218MB
Device Status: Idle

TestSaveCancelRebootLogout

Receive Multicast Audio:

DISABLED

Polycom Default Channel:

1

Polycom Priority Channel:

24

Polycom Emergency Channel:

25

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

2.9 Schedules

Figure 22. Schedules Page

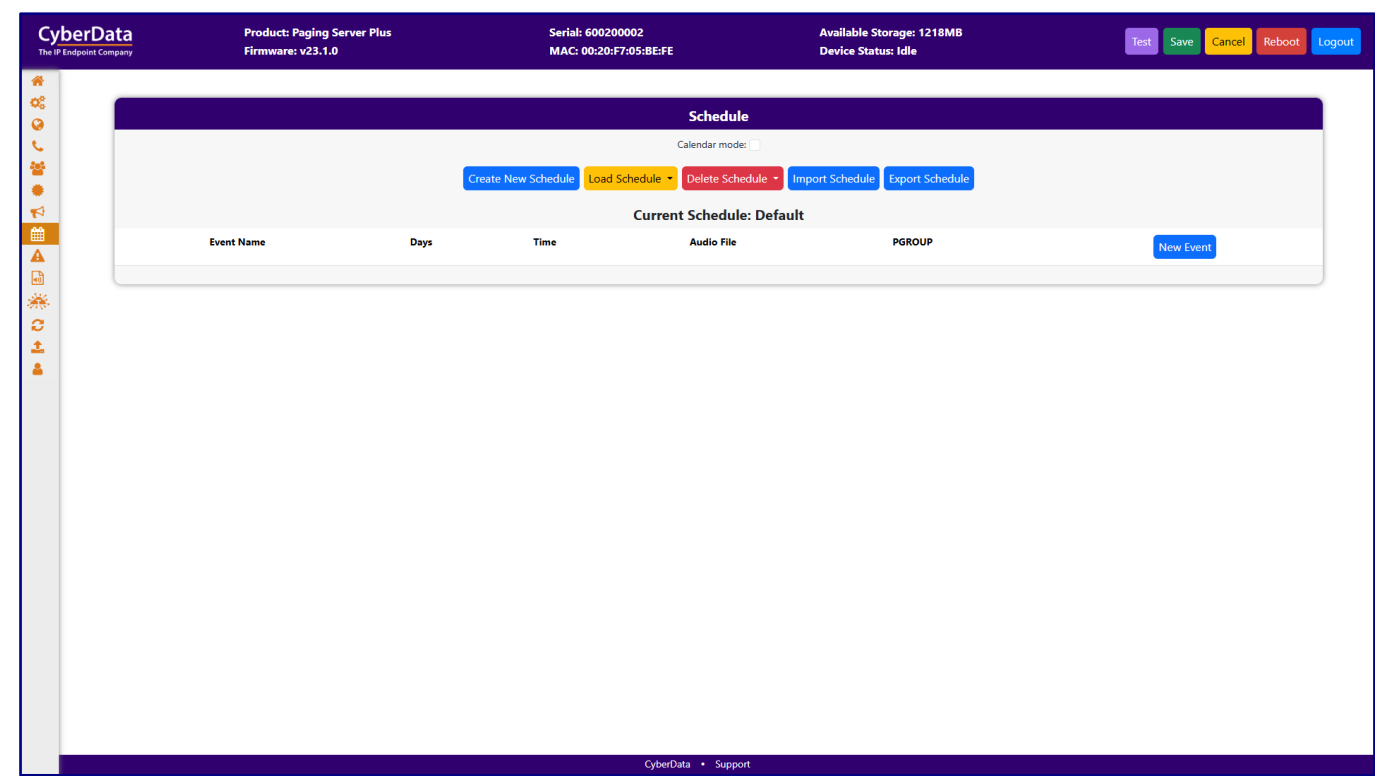
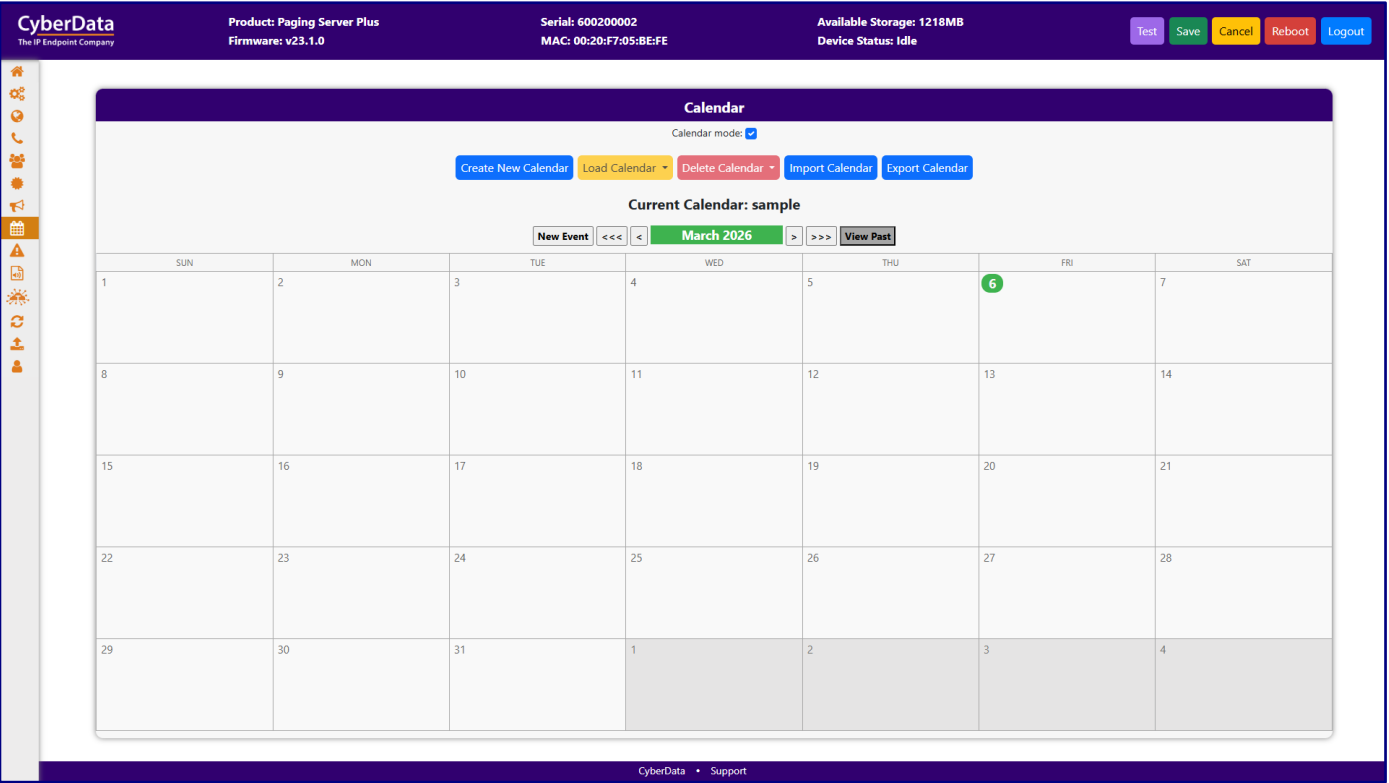


Figure 23. Calendar



2.10 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 24. Fault Page

CyberData
The IP Endpoint Company

Product: Paging Server Plus
Firmware: v23.1.0

Serial: 600200002
MAC: 00:20:F7:05:B8:EFE

Available Storage: 1218MB
Device Status: Idle

TestSaveCancelRebootLogout

Fault Detection Settings

Message Playbacks:

Play Message Locally:

DISABLED ▾

Call to Extension:

DISABLED ▾

Dial Out Extension:

Dial Out ID:

Multicast Audio:

DISABLED ▾

Multicast Address:

Multicast Port:

Polycom Paging:

DISABLED ▾

Polycom Paging Channel:

CyberData • Support

2.11 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 25. Audiofiles Page (1 of 3)

CyberData

The IP Endpoint Company

Product: Pager Server Plus

Firmware: v23.1.0

Serial: 600200002

MAC: 00-20-F7-05-BE-FE

Available Storage: 1218MB

Device Status: Idle

Test

Save

Cancel

Reboot

Logout

🏠

🔧

🔍

📊

📅

🔒

🔄

👤

🏠

🔧

🔍

📊

📅

🔒

🔄

👤

Audio Files

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

CyberData

Support

Figure 26. 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 27. Audiofiles Page (3 of 3)

Stored Messages

Choose File

No file chosen

Upload Message

Delete All Messages

Bells

Choose File

No file chosen

Upload Bell

Delete All Bells

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 28. Terminus Page

CyberData
The IP Endpoint Company

Product: Paging Server Plus
Firmware: v23.1.1

Serial: 600200002
MAC: 00:20:F7:05:BE:FE

Available Storage: 1218MB
Device Status: Idle

TestSaveCancelRebootLogout

Cloud Configuration

Cloud EnrollmentTerminus Service: ENABLED

Enrollment Server:

Enrollment Server

Discovery Setting

Multicast Address:

239.27.32.4

Time to Live:

255

Discovery Interval:

60

seconds

Lockdown Settings

Lock Down Mode:

Disabled

Relay:

No Action

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.

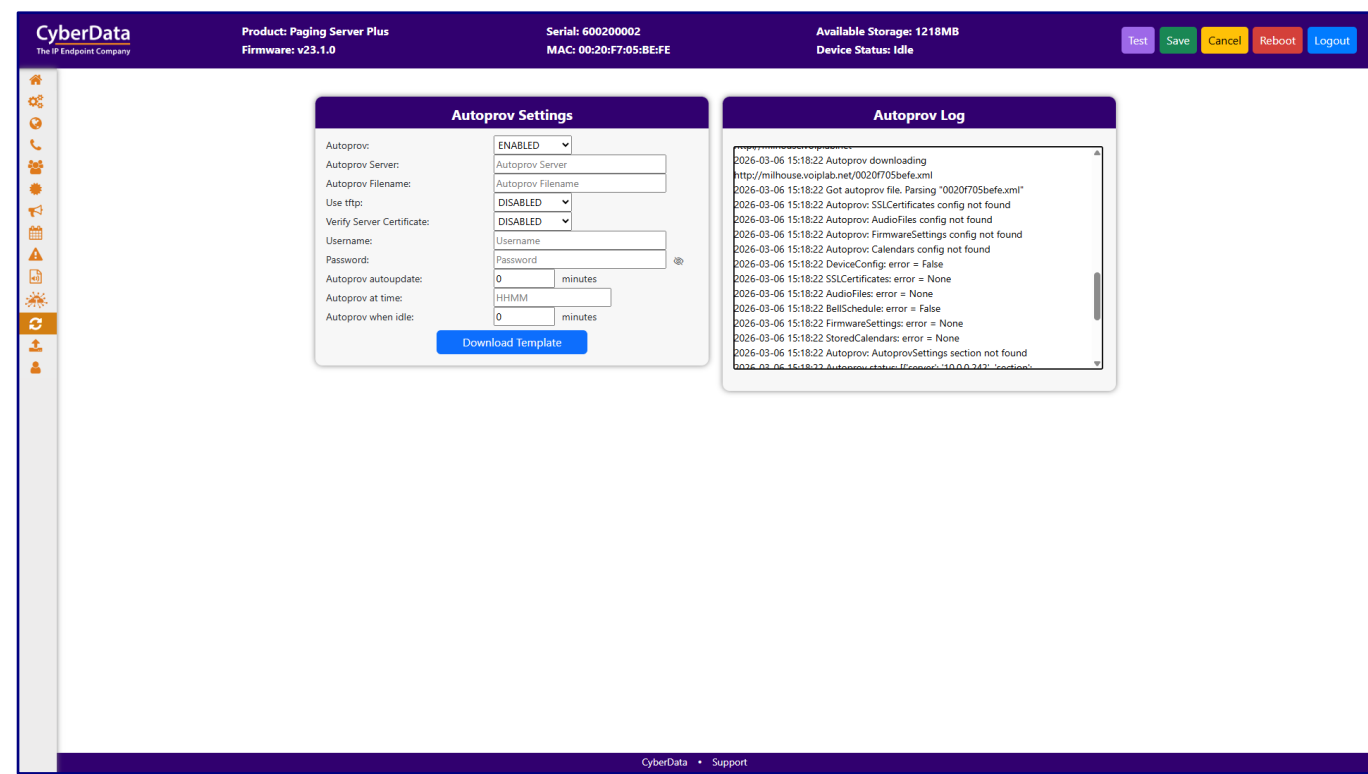
If a file is named, it will be downloaded instead of <mac address>.xml.

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 29. Autoprovisioning Page



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>
<https://www.cyberdata.net/collections/singlewire> (for InformaCast Enabled devices)

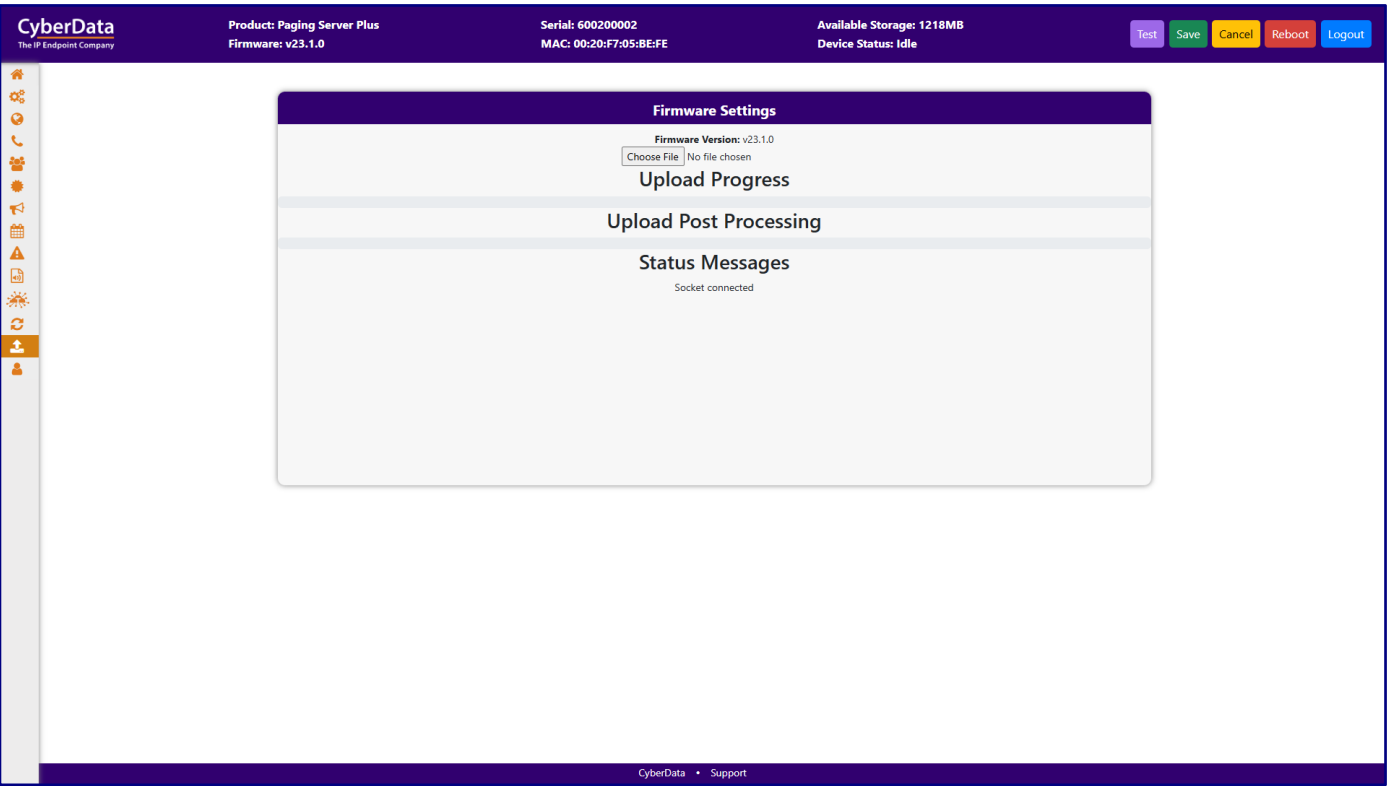
2. Unzip the firmware version file. This file may contain the following:

- 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 30. Firmware Page

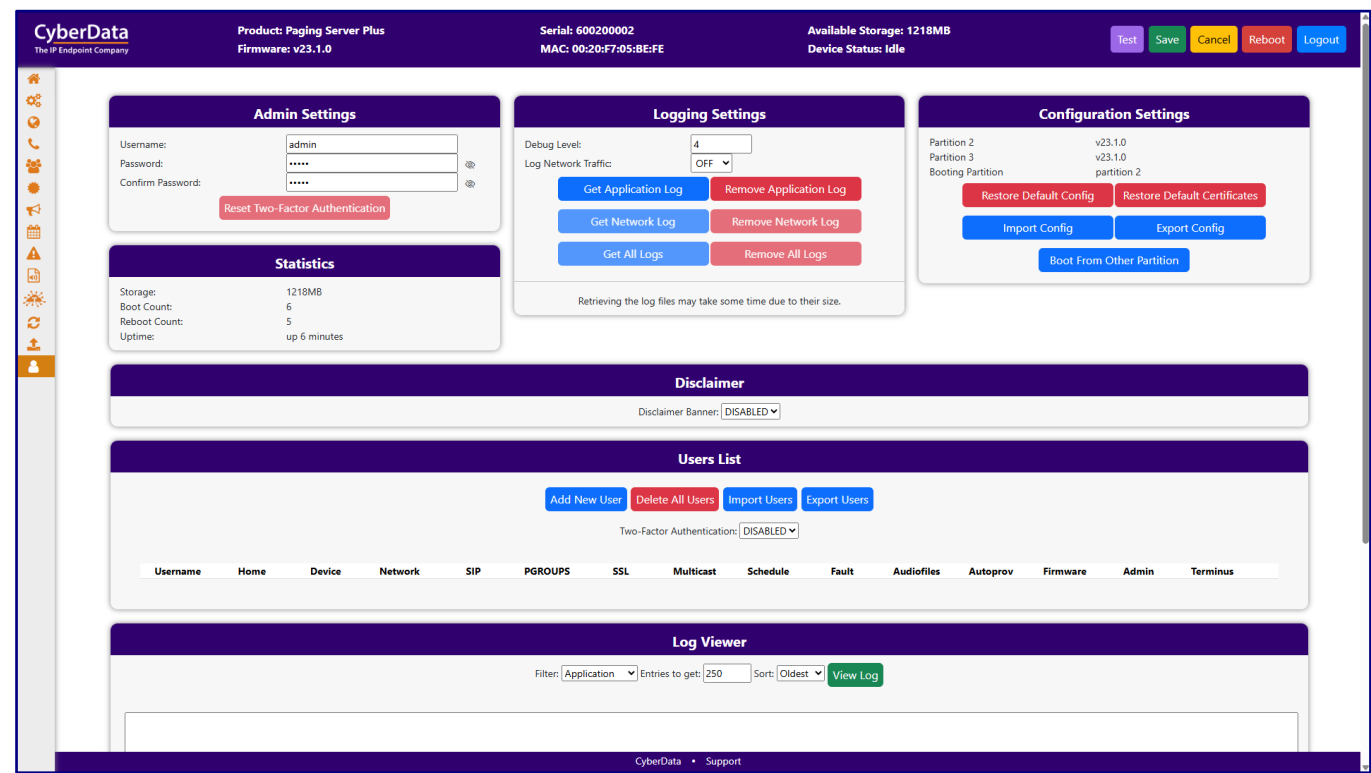


2.15 Admin

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

Note Two factor authentication is enabled here.

Figure 31. Admin Page



2.16 Command Interface

Some functions on the device can be activated using simple POST commands to the web interface. The examples in Table 3 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

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

Table 3. Command Interface Post Commands

Device Action	HTTP Post Command ¹
Reboot	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"
Place call to extension (example: extension 600)	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.154/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://10.10.1.154/"
Test Relay	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"
Activate Relay	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.154/command" -- post-data "request=activate_relay"
Deactivate Relay	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null --no-check-certificate "https://10.10.1.154/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://10.10.1.154/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://10.10.1.154/command" --post-data "request=test_audio"
Swap boot partitions	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"

¹Type and enter all of each http POST command on one line.

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/>

A	Admin 35
	Autoprovisioning 33
C	Command Interface 36
	Command Interface Post Commands 36
D	
	Device 13
E	
	Events 28
F	
	Firmware 34
H	
	Home Page 1, 10
M	
	Multicast 22
N	
	Network 15
S	
	SIP (Session Initiation Protocol) 16
	SSL 20
T	
	Terminus 32