CyberData

The IP Endpoint Company

InformaCast Enabled Paging Adapter

Operations Guide

Part #*011280C*

Document Part #*931767A*
for Firmware Version *20.0.0*

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

InformaCast Enabled Paging Adapter Operations Guide 931767A
Part #011280C

CyberData
The IP Endpoint Company

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:
http://support.cyberdata.net/

Phone: (831) 373-2601, Ext. 333
Email: support@cyberdata.net
Fax: (831) 373-4193
Company and product information is at **www.cyberdata.net**.

Revision Information

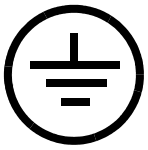
Revision 931767A, which corresponds to firmware version 20.0.0, was released on July 2, 2020.

Browsers Supported

The following browsers have been tested against firmware version 20.0.0:

- Microsoft Edge: 83.0.478.5.4
- Chrome: 83.0.4103.106
- Firefox: 77.0.1

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 *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

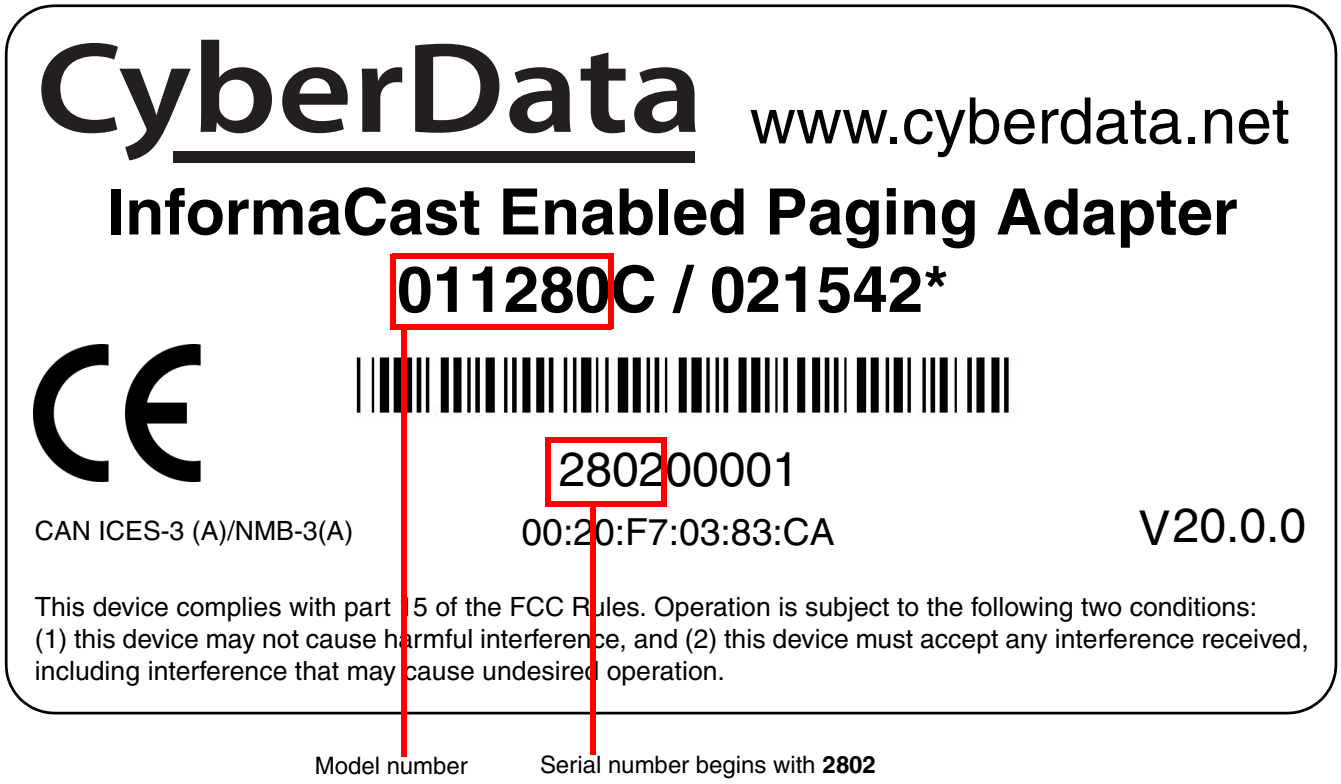
1 Product Overview

1.1 How to Identify This Product

To identify the InformaCast Enabled Paging Adapter, look for a model number label similar to the one shown in Figure 1-1. Confirm the following:

- The model number on the label should be **011280C**.
- The serial number on the label should begin with **2802**.

Figure 1-1. Model Number Label



1.2 Product features

- Compatible with Singlewire InformaCast v12.1, including support for downloading SIP credentials from InformaCast
- Supports Singlewire InformaCast High Quality Audio
- Capable of receiving Singlewire InformaCast, SIP, and Multicast messages
- Support for InformaCast resiliency
- Support for Cisco SRST resiliency

- Compatible with most analog amplifiers in the market
- Paging Prioritization
- Support for 10 multicast paging groups
- Loud/Night Ringer function - second SIP extension
- 9 user-uploadable page messages
- Supports delayed pages with call buffering
- Support for security code to prevent unwanted SIP calls
- Can receive pages directly from Poly phones as well as other devices that can send standard multicast
- Sense input capable of generating events or SIP calls

- Built-in diagnostics
- Line-in for background music
- Line-out connector
- Remote amp fault sensor
- Audio controlled relay/remote amplifier enable
- DTMF entries for analog paging zones
- Rack mountable

- HTTP command interface
- HTTPS or HTTP web based configuration. HTTPS is enabled by default.
- Autoprovisioning via HTTPS, HTTP or TFTP
- Configurable event generation for device health and status monitoring
- TLS 1.2 and SRTP enhanced security for IP Endpoints in a local or cloud-based environment
- 802.11q VLAN tagging
- Support for Cisco SRST resiliency

1.3 Product Specifications

Table 1-1. Product Specifications

Specifications	
Ethernet I/F	10/100 Mbps
Protocol	SIP RFC 3261 Compatible
Notification Software	Singlewire InformaCast v4.0 and above
Power Input	PoE 802.3af or 48VDC
Line In:	
Input Signal Amplitudes	2.0 VPP maximum
Input Impedance	10k Ohm
Line Out:	
Output Signal Amplitudes	2.0 VPP maximum
Output Level	+2dBm nominal
Total Harmonic Distortion	0.5% maximum
Output Impedance	10k Ohm
Page Port Output	Balanced 600 Ohm 5VPP
Payload Types	G.711 a-law, G.711 μ-law, G.722, and G.729
Network Security	TLS/SSL 1.2 and SRTP
Operating Range	Temperature: -40° C to 55° C (-40° F to 131° F) Humidity: 5-95%, non-condensing
Storage Temperature	-40° C to 70° C (-40° F to 158° F)
Storage Altitude	Up to 15,000 ft. (4573 m)
Dimensions[a]	6.11 inches [155.19 mm] Length 4.05 inches [102.87 mm] Width 1.15 inches [29.21 mm] Height
Weight	1.2 lbs. [.54 kg]
Boxed Weight	1.8 lbs. [.82 kg]
Compliance	UL 62368-1, RoHS Compliant, FCC; Part 15 Class A, IEEE 802.3 Compliant; Reference Number for UL: E129569 Vol 4 Sec 1
Warranty	2 Years Limited
Part Number	011280C

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

1.4 Compliance

1.4.1 Safety

This product is listed by UL. Representative samples of this product have been evaluated by UL and meet applicable safety standards. (Standard: UL 62368-1). This applies to the following products: 011145, 011146, 011233, 011280, 011295, 011368, 011372

Note You can download the Declaration of Conformity document from the **Downloads** tab of the product's webpage.

1.4.2 FCC Statement

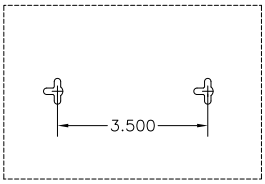
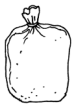
This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates,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

2 Installing the InformaCast Enabled Paging Adapter

2.1 Parts List

The packaging for the InformaCast Enabled Paging Adapter includes the parts in Table 2-2.

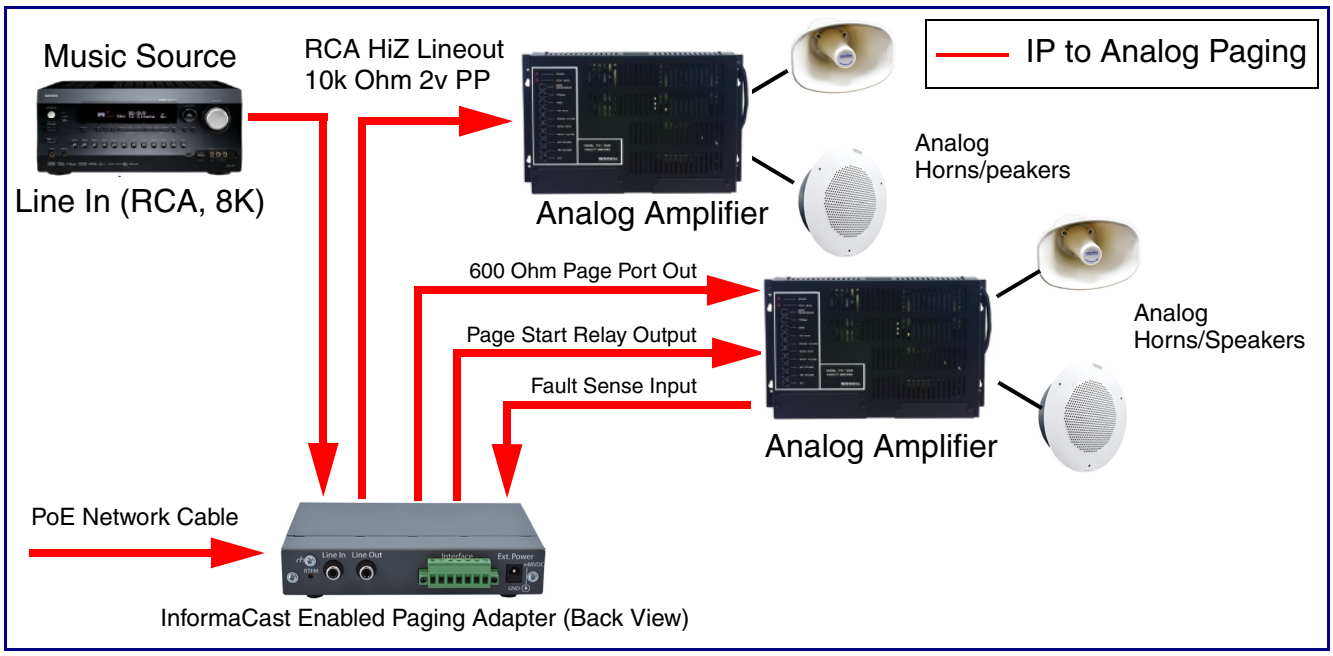
Table 2-2. Parts List

Quantity	Part Name	Illustration
1	InformaCast Enabled Paging Adapter	
1	Installation Quick Reference Guide	
1	Mounting Template (located on the last page of the *Installation Quick Reference*)	
1	Mounting Kit (part #121007*) which includes: (2) Knotting Anchors (2) #6 x 1.25" Self-Tapping Screws	

2.2 Typical Installation

Figure 2-1 illustrates how the InformaCast Enabled Paging Adapter is normally installed as part of a paging system.

Figure 2-1. Typical Installation

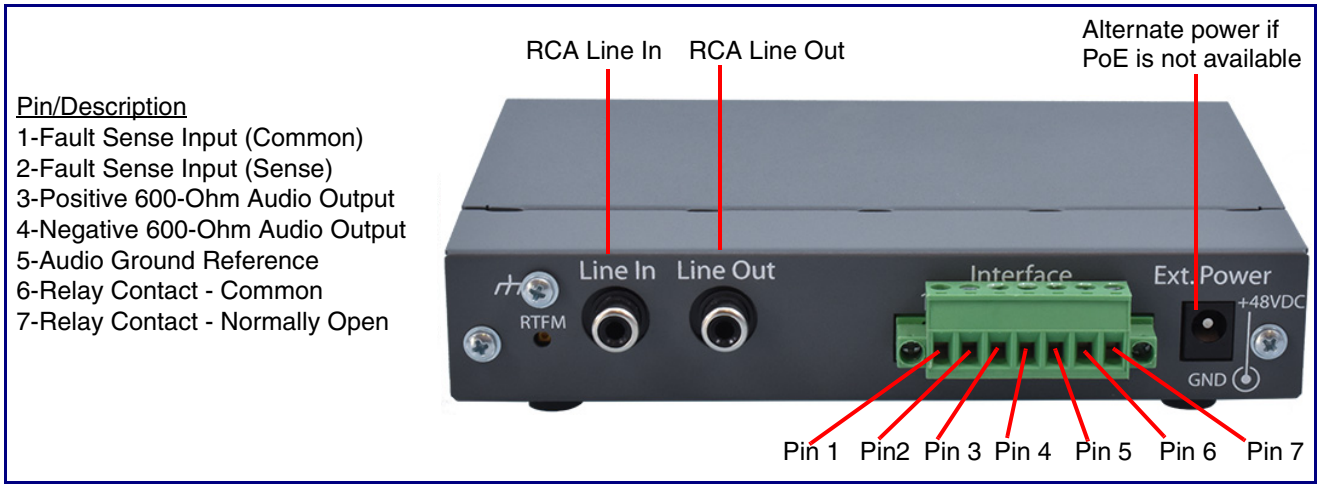


2.3 Connecting the InformaCast Enabled Paging Adapter

Before you connect the InformaCast Enabled Paging Adapter, be sure that you have received all of the parts described in Section 2.1, "Parts List".

See Figure 2-2 for the connection options that are available for the InformaCast Enabled Paging Adapter.

Figure 2-2. Connection Options



2.3.1 Ground Connection

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

2.3.2 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. The level of this input can be controlled by the potentiometer located on the front of the device (see Section 2.5.9, "Configure the Fault Detection Parameters").

2.3.3 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.

2.3.4 Page Port Output Connections

Table 2-1. Page Port Output Connections

Pin	Description
Pin 1	Fault Sense Input (Common). See Section 2.3.4.1, "Pin 1 and 2—Fault Sense Input (Common/Sense)".
Pin 2	Fault Sense Input (Sense). See Section 2.3.4.1, "Pin 1 and 2—Fault Sense Input (Common/Sense)".
Pin 3	Positive 600-Ohm Audio Output[a]. See Section 2.3.4.2, "Pin 3, 4, and 5—Positive/Negative 600-Ohm Audio Output/Audio Ground Reference".
Pin 4	Negative 600-Ohm Audio Output.[a]. See Section 2.3.4.2, "Pin 3, 4, and 5—Positive/Negative 600-Ohm Audio Output/Audio Ground Reference".
Pin 5	Audio Ground Reference. See Section 2.3.4.2, "Pin 3, 4, and 5—Positive/Negative 600-Ohm Audio Output/Audio Ground Reference".
Pin 6	Relay Contact - Common[b]. See Section 2.3.4.3, "Pin 6 and 7—Relay Contact (Common/Normally Open)".
Pin 7	Relay Contact - Normally Open[b]. See Section 2.3.4.3, "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

2.3.4.1 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 2.5.9, "Configure the Fault Detection Parameters"), 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.

2.3.4.2 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.

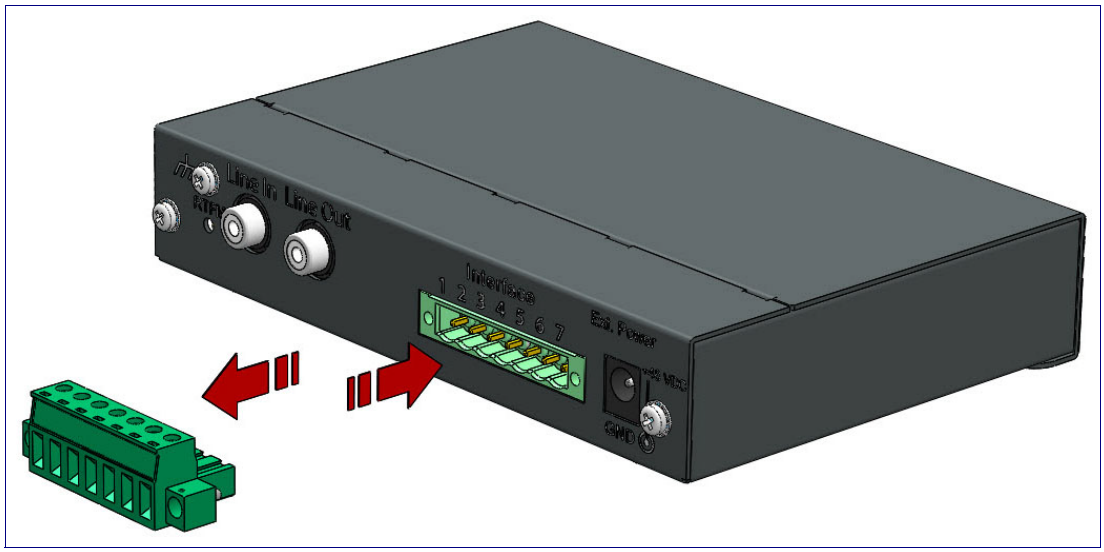
2.3.4.3 Pin 6 and 7—Relay Contact (Common/Normally Open)

When enabled on the web interface (Section 2.5.4, "Configure the Device Parameters"), 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.

2.3.5 Removable Interface Connector

Figure 2-3 shows the interface connector that is removable on the InformaCast Enabled Paging Adapter.

Figure 2-3. Removable Interface Connector

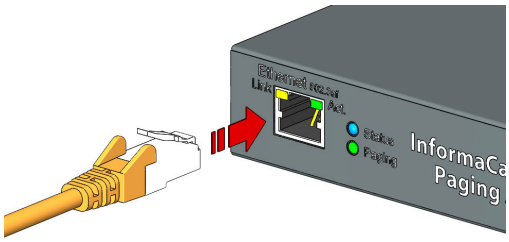


2.3.6 Connect to the Power Source

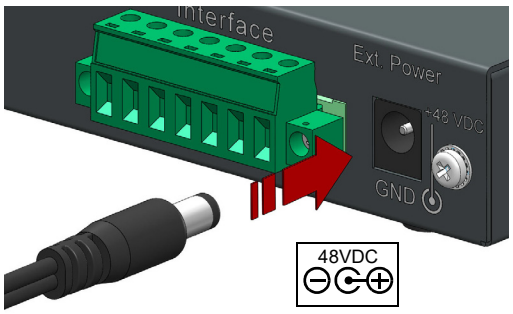
To use PoE, plug a Cat 5 Ethernet cable from the InformaCast Enabled Paging Adapter **Ethernet** port to your network. As an alternative to PoE, you can plug one end of a +48V DC power supply into the SIP Paging Adapter, and plug the other end into a receptacle. If required, connect the earth grounding wire to the chassis ground on the back of the unit. See Figure 2-4.

Figure 2-4. Connecting to the Power Source

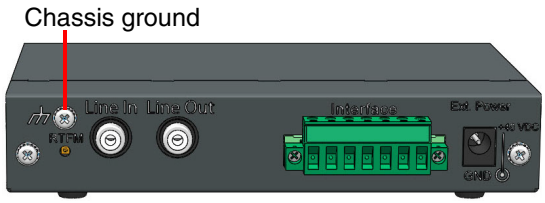
PoE



Non PoE with 48 VDC Power Supply



Chassis Ground



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 InformaCast Enabled Paging Adapter Ethernet port. Plug the other end of the Ethernet cable into your network. See the figure on the left.

Non-Poe

- For Non-PoE, connect the InformaCast Enabled Paging Adapter to a 48VDC power supply. See the figure on the left.
- **Note**: Do not use both PoE and external power.

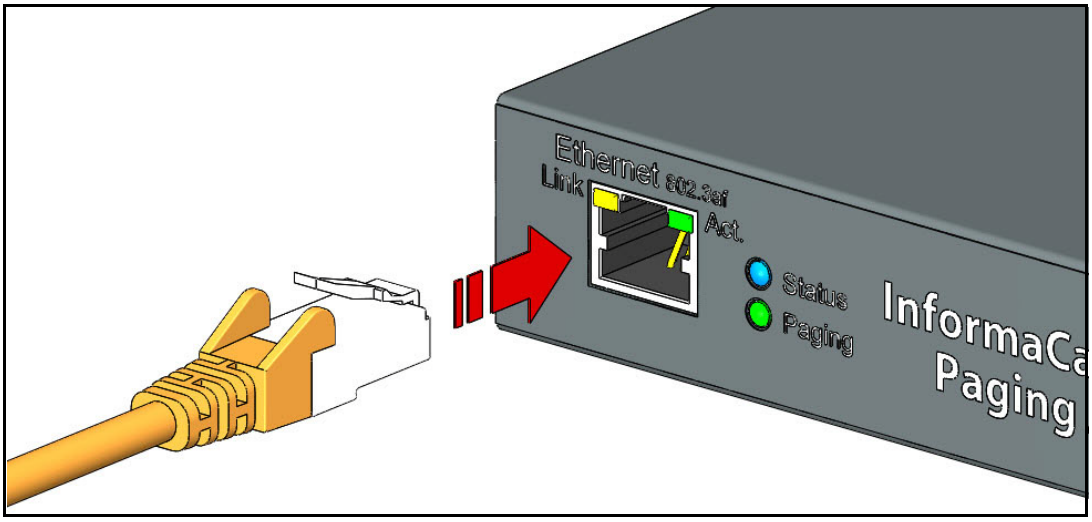
Chassis Ground

- If required, connect the earth grounding wire to the Chassis Ground. See the figure on the left.

2.3.7 Connect to the Network

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

Figure 2-5. Connecting to the Network



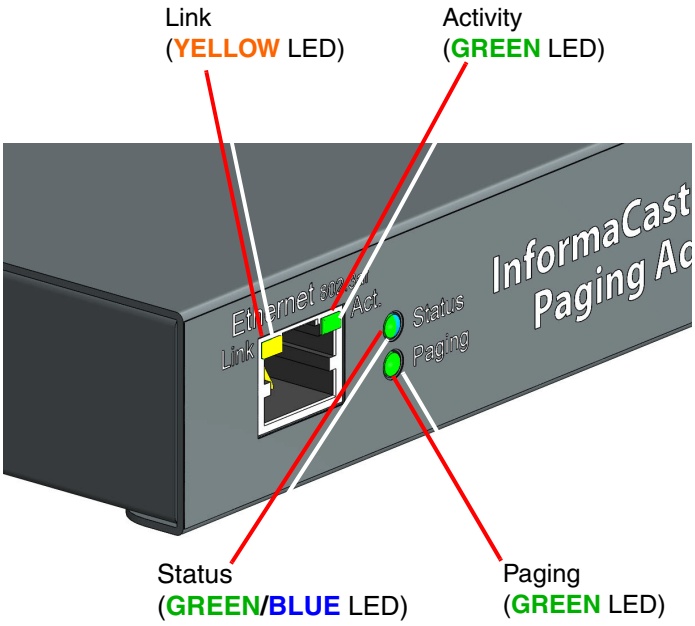
2.3.8 Confirm that the InformaCast Enabled Paging Adapter is Up and Running

The LEDs on the front of the InformaCast Enabled Paging Adapter verify the unit's operations.

Figure 2-6. 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 InformaCast Enabled Paging Adapter 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.



2.3.8.1 Verify Network Activity

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

2.4 Announcing the IP Address

To announce the IP address for the InformaCast Enabled Paging Adapter, briefly press and then quickly release the **RTFM** switch. See Figure 2-7.

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

Figure 2-7. RTFM Switch

2.5 Restore the Factory Default Settings

The InformaCast Enabled Paging Adapter is delivered with factory set default values for the parameters in Table 2-3. Use the **RTFM** switch (see Figure 2-8) on the back of the unit to restore these parameters to the factory default settings.

Figure 2-8. RTFM Switch

Note When you perform this procedure, the factory default settings are restored. The default parameters for access are shown in Table 2-3.

Table 2-3. Factory Default Settings

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

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** switch until the status and paging lights come on.
2. Continue to press the switch until after the indicator lights go off, and then release it.

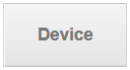
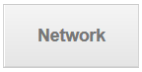
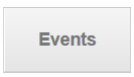
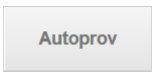
Note The “Restoring Defaults” announcement can be heard if a speaker or amplified speaker is connected to the unit.

3. The InformaCast Enabled Paging Adapter settings are restored to the factory defaults.

2.5.1 InformaCast Enabled Paging Adapter Web Page Navigation

Table 2-4 shows the navigation buttons that you will see on every InformaCast Enabled Paging Adapter web page.

Table 2-4. Web Page Navigation

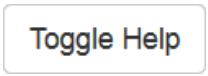
Web Page Item	Description
	Link to the **Home** page.
	Link to the **Device** page.
	Link to the **Network** page.
	Link to go to the **SIP** page.
	Link to the **SSL** page.
	Link to the **Multicast** page.
	Link to the **Fault** page.
	Link to the **Audiofiles** page.
	Link to the **Events** page.
	Link to the **Autoprovisioning** page.
	Link to the **Firmware** page.

2.5.2 Using the Toggle Help Button

The **Toggle Help** button allows you to see a short description of some of the settings on the webpage. To use the **Toggle Help** button, do the following:

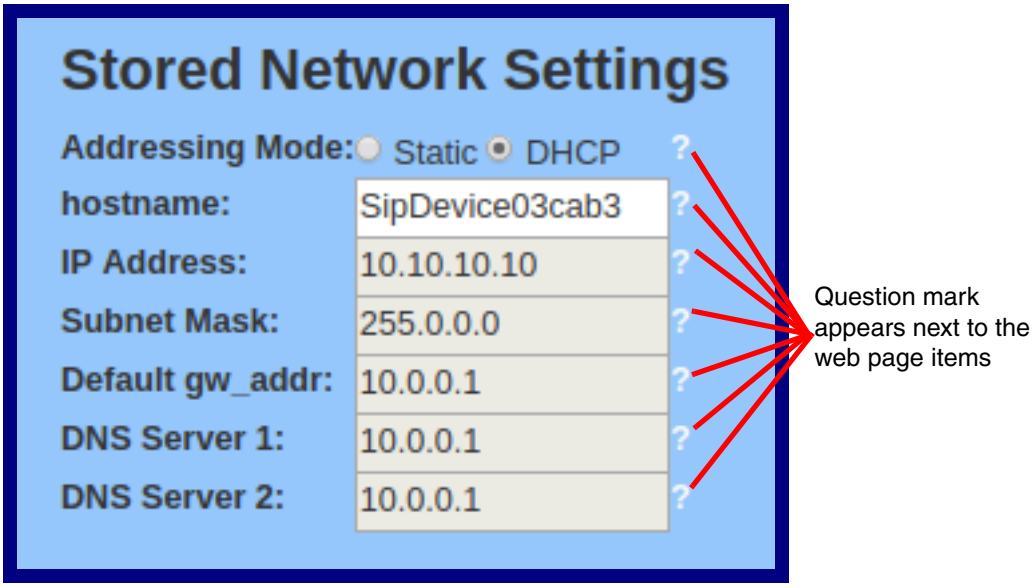
1. Click on the **Toggle Help** button that is on the UI webpage. See Figure 2-9 and Figure 2-10.

Figure 2-9. Toggle/Help Button



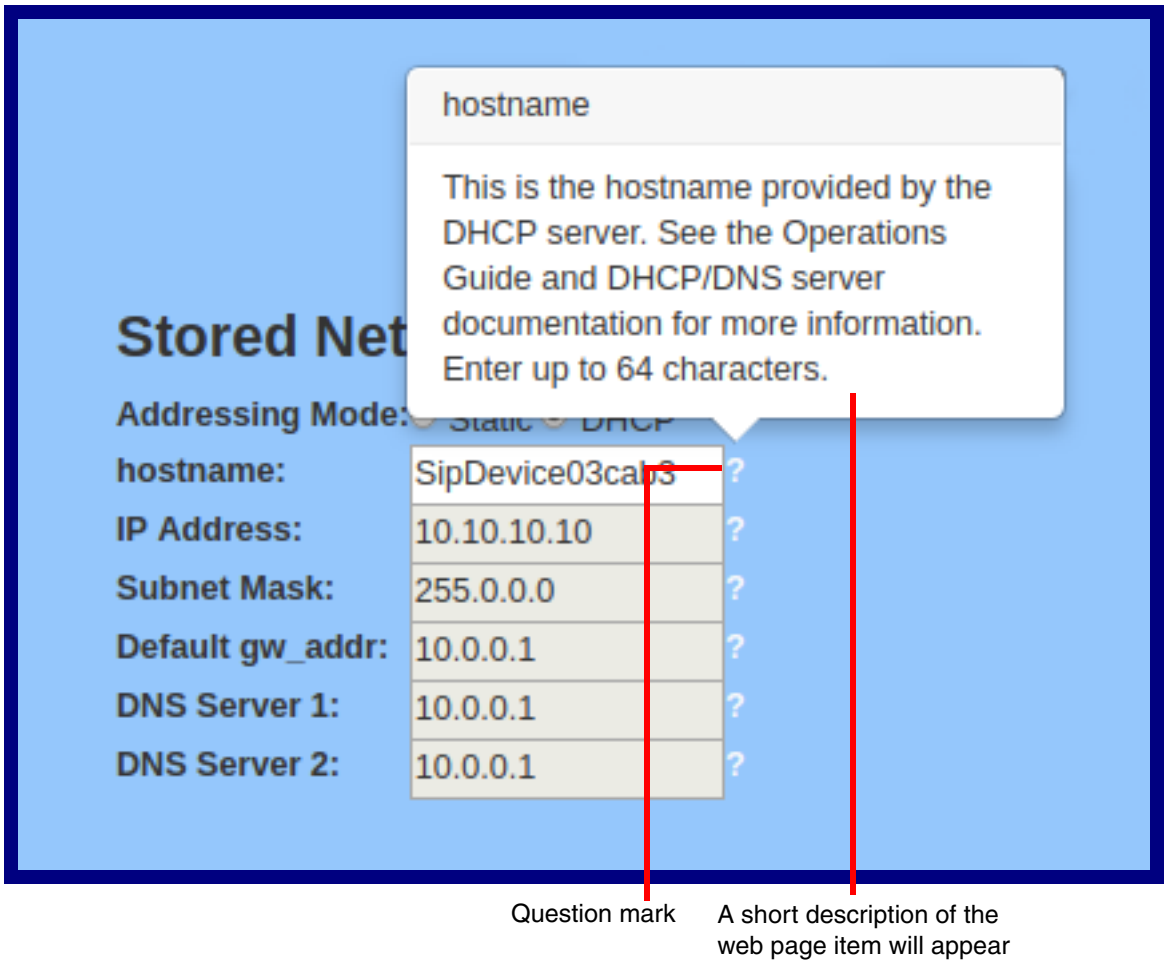
2. You will see a question mark (?) appear next to each web page item that has been provided with a short description by the Help feature. See Figure 2-10.

Figure 2-10. Toggle Help Button and Question Marks



3. Move the mouse pointer to hover over the question mark (?), and a short description of the web page item will appear. See Figure 2-11.

Figure 2-11. Short Description Provided by the Help Feature



2.5.3 Log in to the Configuration GUI

1. Open your browser to the InformaCast Enabled Paging Adapter IP address.

Note If the network does not have access to a DHCP server, the device will default to an IP address of 10.10.10.10.

Note Make sure that the PC is on the same IP network as the InformaCast Enabled Paging Adapter.

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

The unit 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.

Note To work with the InformaCast Enabled Paging Adapter configuration *after* the initial configuration, log in using the IP address you assign to the device. Section 2.5.5, "Configure the Network Parameters" provides instructions for entering the IP address.

2. When prompted, use the following default **Username** and **Password** to open the configuration Home page:

   Username: **admin**

   Password: **admin**

Change the Default Username and Password

To change the default Web access Username and Password:

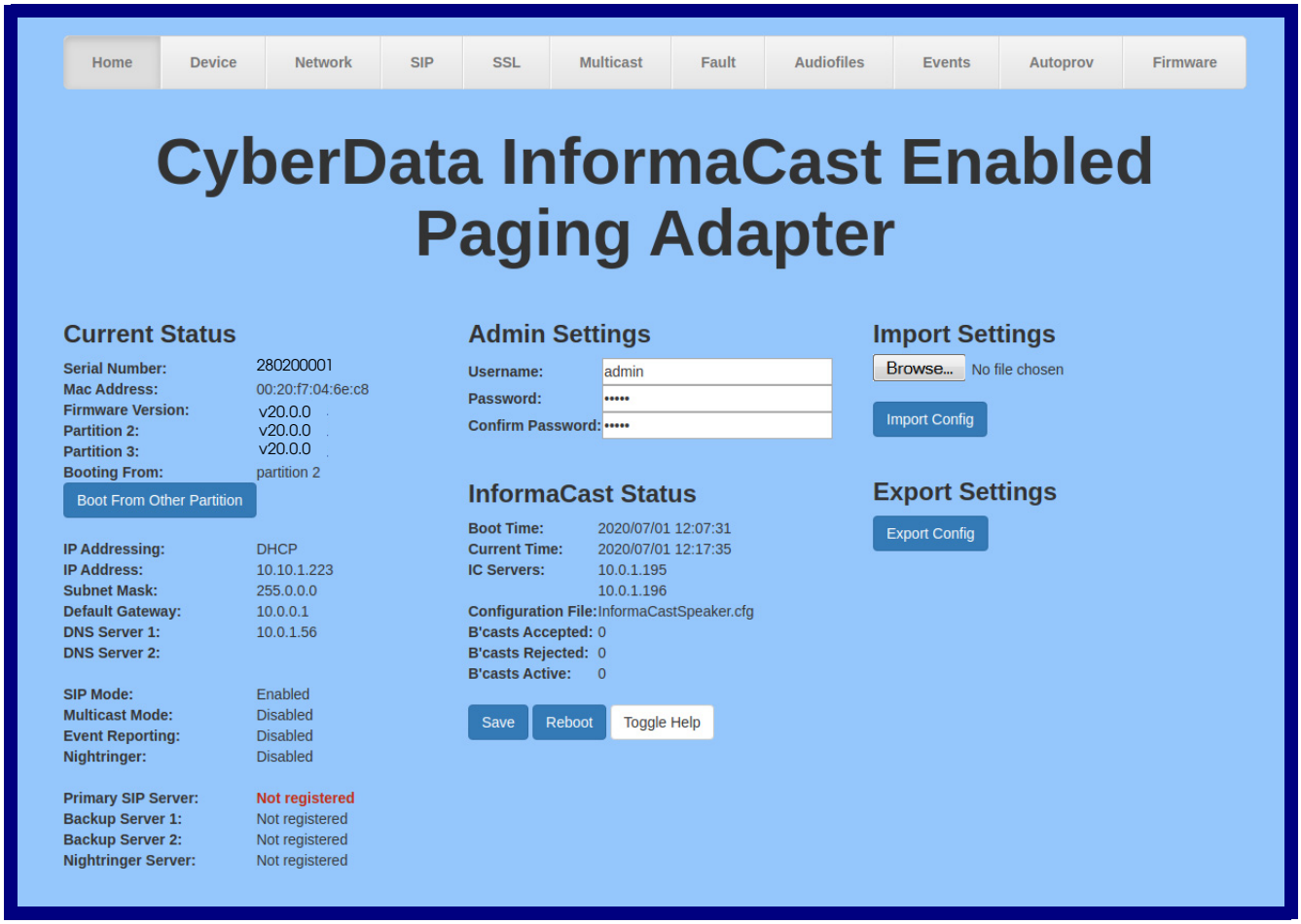
1. Enter the new Username from four to 25 alphanumeric characters in the **Change Username** field. The Username is case-sensitive.

2. Enter the new Password from four to 25 alphanumeric characters in the **Change Password** field. The Password is case-sensitive.

3. Enter the new password again in the **Re-enter New Password** field.

   Click **Save Settings**.

Figure 2-12. Home Page



4. On the **Home Page**, review the setup details and navigation buttons described in Table 2-5

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-5. Home Page Overview

Web Page Item	Description
Admin Settings	
Username ?	The username to access the web interface. Enter up to 25 characters.
Password ?	The password to access the web interface. Enter up to 25 characters.
Confirm Password ?	Confirm the web interface password.
Current Status	
Serial Number	Shows the device serial number.
Mac Address	Shows the device Mac address.
Firmware Version	Shows the current firmware version.
IP Addressing	Shows the current IP addressing setting (**DHCP** or **static**).
IP Address	Shows the current IP address.
Subnet Mask	Shows the current subnet mask address.
Default Gateway	Shows the current default gateway address.
DNS Server 1	Shows the current DNS Server 1 address.
DNS Server 2	Shows the current DNS Server 2 address.
SIP Mode	Shows the current status of the SIP mode.
Multicast Mode	Shows the current status of the Multicast mode.
Event Reporting	Shows the current status of the Event Reporting mode.
Nightringer	Shows the current status of the Nightringer mode.
Primary SIP Server	Shows the current status of the Primary SIP Server.
Backup Server 1	Shows the current status of Backup Server 1.
Backup Server 2	Shows the current status of Backup Server 2.
Nightringer Server	Shows the current status of Nightringer Server.
InformaCast Status	
Boot Time	Shows the boot time.
Current Time	Shows the current time.
IC Servers	Shows the InformaCast Server IP address.
Configuration File	Shows the configuration file.
B'casts Accepted	Shows the number of B'casts accepted.
B'casts Rejected	Shows the number of B'casts rejected.
B'casts Active	Shows the number of active B'casts.
Import Settings	
Browse...	Use this button to select a configuration file to import.

Table 2-5. Home Page Overview (continued)

Web Page Item	Description
Import Config	After selecting a configuration file, click Import to import the configuration from the selected file. Click Save.
Export Settings	
Export Config	Click Export to export the current configuration to a file.
Save	Click the **Save** button to save your configuration settings.
Reboot	Click on the **Reboot** button to reboot the system.
Toggle Help	Click on the **Toggle Help** button to see a short description of some of the web page items. First click on the **Toggle Help** button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

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

At this point you can:

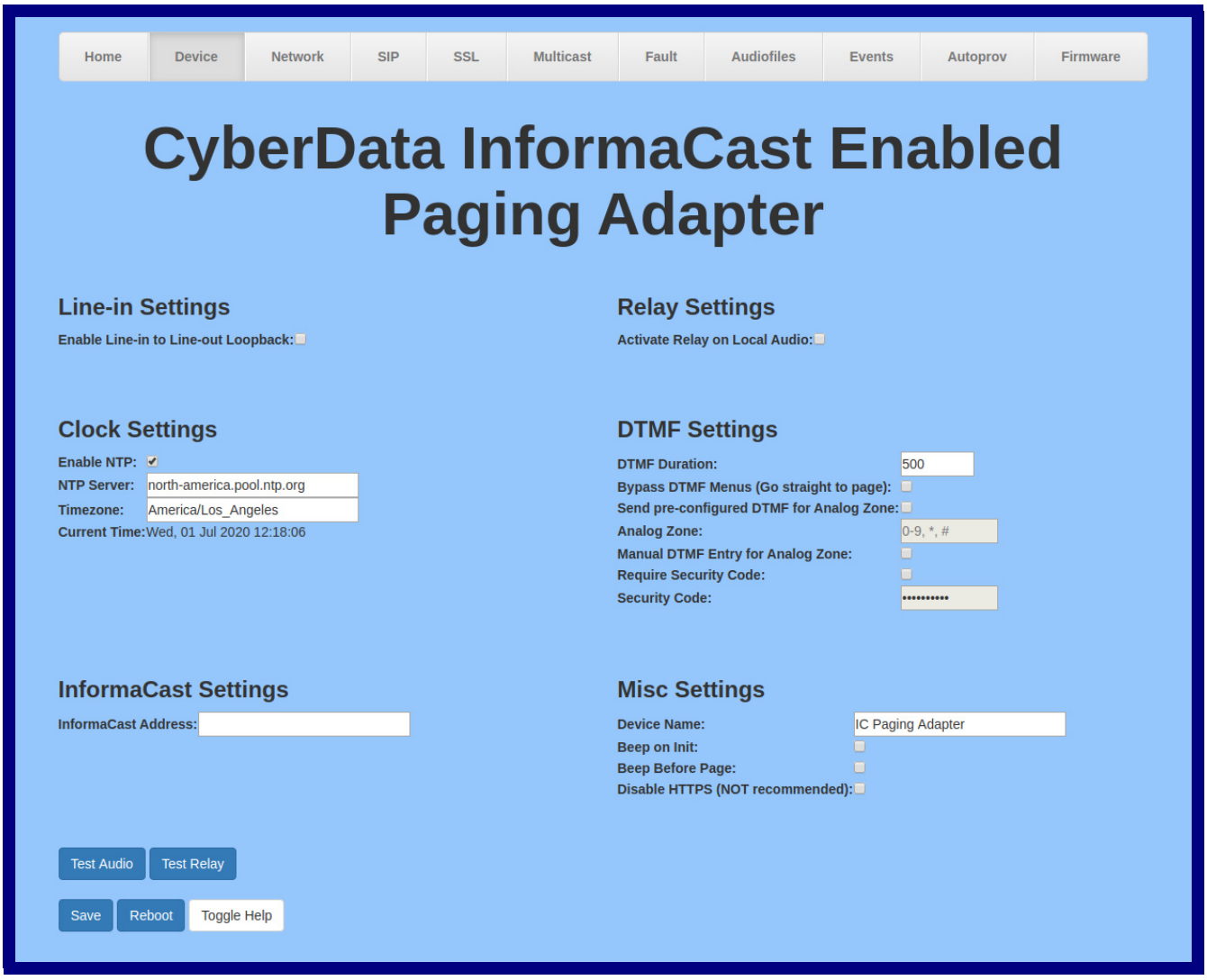
- Review the InformaCast Enabled Paging Adapter's **Current Settings**. Use the RTFM switch to restore the factory default settings. See Section 2.5, "Restore the Factory Default Settings".
- Configure the device parameters. Click on the **Device** button and see Section 2.5.4, "Configure the Device Parameters".
- Configure the network parameters. Click on the **Network** button and refer to Section 2.5.5, "Configure the Network Parameters" for instructions.
- Configure the SIP parameters. Click on the **SIP** button and see Section 2.5.6, "Configure the SIP Parameters".
- Configure the multicast parameters. Click on the **Multicast** button and see Section 2.5.8, "Configure the Multicast Parameters" for instructions.
- Configure the fault detection parameters. Click on the **Fault** button and see Section 2.5.9, "Configure the Fault Detection Parameters".
- Configure the audio parameters. Click on the **Audiofiles** button and see Section 2.5.10, "Configure the Audio Parameters" for instructions.
- Configure the event parameters. Click on the **Events** button and see Section 2.5.11, "Configure the Event Parameters" for instructions.
- Configure the autoprovisioning parameters. Click on the **Autoprov** button and see Section 2.5.12, "Configure the Autoprovisioning Parameters" for instructions.

Note Click on the **Firmware** button any time you need to upload new versions of the firmware. See Section 2.6, "Upgrade the Firmware" for instructions.

2.5.4 Configure the Device Parameters

1. Click on the **Device** button to open the **Device** page. See Figure 2-13.

Figure 2-13. Device Page



2. On the **Device** page, you may enter values for the parameters indicated in Table 2-6.

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-6. Device Configuration Parameters

Web Page Item	Description
Line-in Settings	
Enable Line-in to Line-out Loopback ?	Line-in audio will play back out the device's audio output ports. This is the lowest priority audio and will be preempted by any other audio stream.
Clock Settings	
Enable NTP ?	Sync device's local time with the specified NTP Server.
NTP Server ?	Use this field to set the address (in IPv4 dotted decimal notation or as a canonical name) for the NTP Server. This field can accept canonical names of up to 64 characters in length.
Timezone	Enter the tz database string of your timezone. Examples: America/Los_Angeles America/New_York Europe/London America/Toronto See **https://en.wikipedia.org/wiki/List_of_tz_database_time_zones** for a full list of valid strings.
Current Time	Displays the current time.
InformaCast Settings	
InformaCast Address ?	Use this field to set the address of your InformaCast server. This will override any InformaCast server addresses received via SLP or DHCP. If using TFTP for configuration, simply enter an IP address (eg. 10.0.1.195) If using HTTP for configuration, enter the full URL to the path that contains the configuration file. Do not input the file name (e.g.http://10.0.1.195:8081/InformaCast/resources/).If the HTTP protocol is not specified with **http://**, then TFTP will be used.
Misc Settings	
Device Name ?	Type the device name. Enter up to 25 characters.
Beep on Init ?	Device will play the user defined “pagetone” audio file when it boots.
Beep on Page ?	Device will play the user defined “pagetone” audio file before playing a SIP page.
Disable HTTPS (NOT recommended) ?	Disables the encrypted connection to the webpage. We do not recommend disabling HTTPS for security reasons.
Relay Settings	
Activate Relay on Local Audio ?	The relay will be activated (closed) when the device is playing audio. Use this to activate an external amplifier when the device is playing audio.

Table 2-6. Device Configuration Parameters (continued)

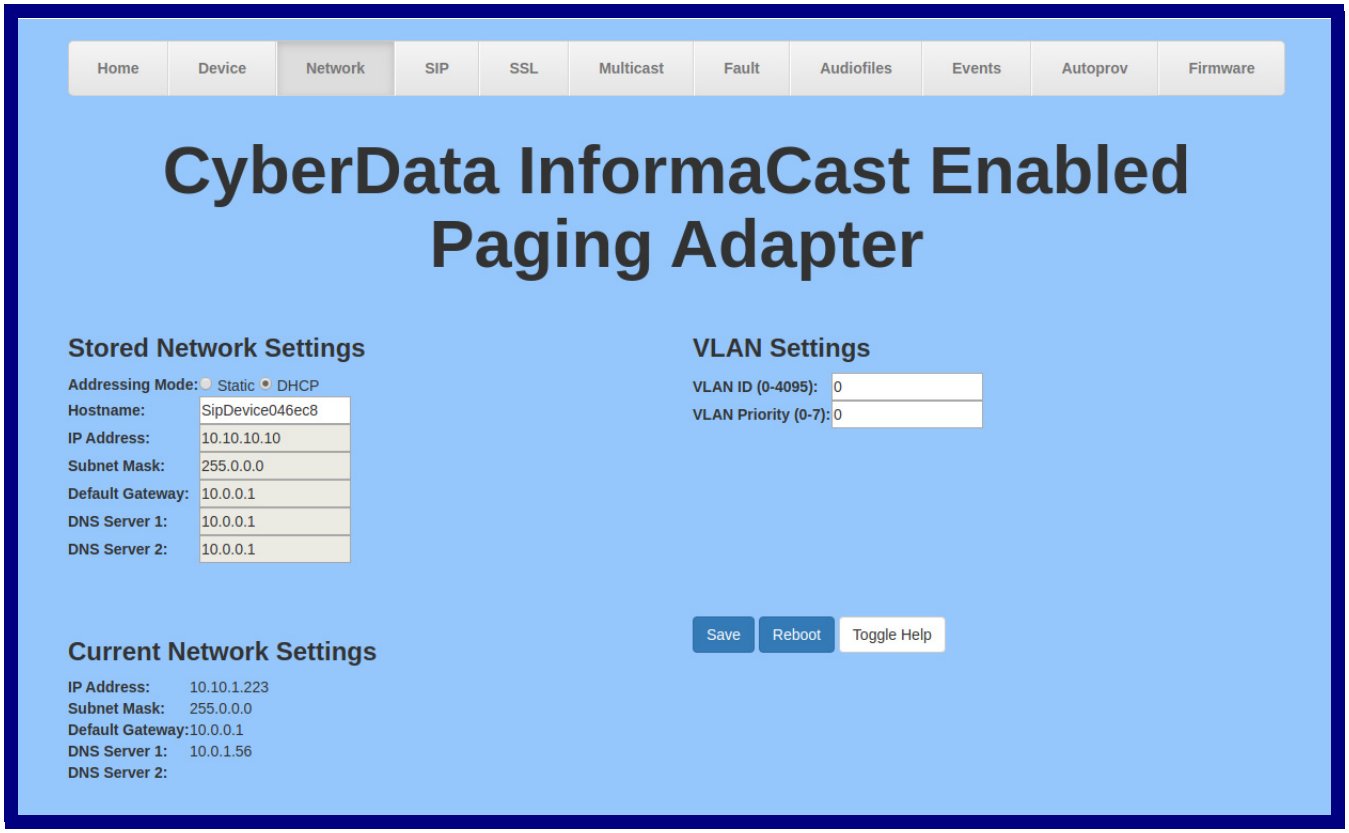
Web Page Item	Description
DTMF Settings	
DTMF Duration	The duration, in milliseconds, of DTMF tones played out of the device's analog audio ports (1-65535).
Bypass DTMF Menus (Go straight to page)	When selected, the DTMF menu options are bypassed when a page is sent, and the device begins a live/buffered page no ability to send stored messages).
Send pre-configured DTMF for Analog Zone	When selected, a pre-configured DTMF sequence is sent to activate an analog zone when Bypass DTMF Menus (Go straight to page) setting is enabled.
Zone	Type the pre-configured DTMF sequence for the analog zone.
Manual DTMF Entry for Analog Zone	When selected, the device will prompt the caller to enter a DTMF sequence to activate an analog zone before prompting the caller to press 1 through 9 to send a stored message or press 0 to page. **Note**: The user must press the **#** key after entering the zone.
Require Security Code	When selected, the user will be prompted to enter a Security Code (entered on the Device Page) before being able to execute a page when calling the device.
Security Code	Type the security code in this field.
Test Audio	Click on the **Test Audio** button to do an audio test. When the **Test Audio** button is pressed, you will hear a voice message for testing the device audio quality and volume.
Test Relay	Click on the **Test Relay** button to do a relay test.
Save	Click the **Save** button to save your configuration settings.
Reboot	Click on the **Reboot** button to reboot the system.
Toggle Help	Click on the **Toggle Help** button to see a short description of some of the web page items. First click on the **Toggle Help** button, and you will see a question mark ( ) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

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

2.5.5 Configure the Network Parameters

Configuring the network parameters enables your network to recognize the InformaCast Enabled Paging Adapter and communicate with it. Click the **Network** button on the **Home** page to open the **Network** page.

Figure 2-14. Network Page



On the **Network** page, enter values for the parameters indicated in Table 2-7.

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-7. Network Configuration Parameters

Web Page Item	Description
Stored Network Settings	
Addressing Mode ?	Select either DHCP IP Addressing or Static Addressing by marking the appropriate radio button. DHCP Addressing mode is enabled on default and the device will attempt to resolve network addressing with the local DHCP server upon boot. If DHCP Addressing fails, the device will revert to the last known IP address or the factory default address if no prior DHCP lease was established. See Section 2.5, "Restore the Factory Default Settings" for factory default settings. Be sure to click **Save** and **Reboot** to store changes when configuring a Static address.
Hostname ?	This is the hostname provided by the DHCP server. See the DHCP/DNS server documentation for more information. Enter up to 64 characters.
IP Address ?	Enter the Static IPv4 network address in dotted decimal notation.
Subnet Mask ?	Enter the Subnet Mask in dotted decimal notation.
Default Gateway ?	Enter the Default Gateway IPv4 address in dotted decimal notation.
DNS Server 1 ?	Enter the primary DNS Server IPv4 address in dotted decimal notation.
DNS Server 2 ?	Enter the secondary DNS Server IPv4 address in dotted decimal notation.
DHCP Timeout in seconds ?	Specify the desired time-out duration (in seconds) that the device will wait for a response from the DHCP server before reverting back to the stored static IP address. The stored static IP address may be the last known IP address or the factory default address if no prior DHCP lease was established. Enter up to 8 characters. A value of -1 will retry forever.
VLAN Settings	
VLAN ID (0-4095) ?	Specify the IEEE 802.1Q VLAN ID number. Enter up to 4 digits. **Note**: The device supports 802.1Q VLAN tagging support. The switch port connected to the device will need to be in “trunking mode” for the VLAN tags to propagate.
VLAN Priority (0-7) ?	Specify the IEEE 802.1p VLAN priority level. Enter 1 digit. A value of 0 may cause the VLAN ID tag to be ignored.
Current Network Settings	Shows the current network settings.
IP Address	Shows the current Static IP address.
Subnet Mask	Shows the current Subnet Mask address.
Default Gateway	Shows the current Default Gateway address.
DNS Server 1	Shows the current DNS Server 1 address.
DNS Server 2	Shows the current DNS Server 2 address.

Table 2-7. Network Configuration Parameters (continued)

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

On this page:

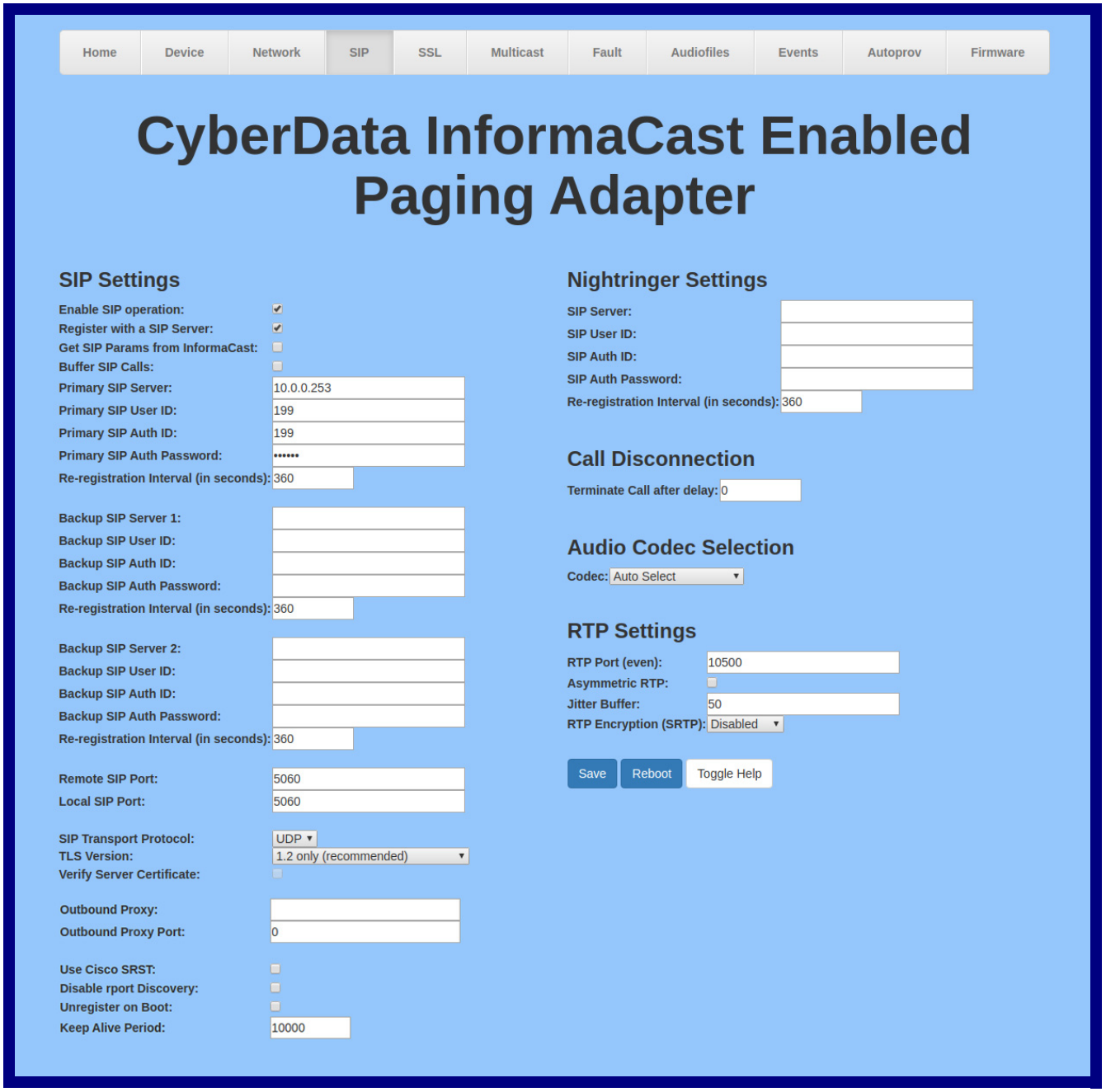
1. Specify whether you use **Static** or **DHCP IP Addressing** by marking the appropriate radio button. If you select **Static IP Addressing**, go to Step 2.
2. For Static IP Addressing, also enter values for the following parameters:
   - The InformaCast Enabled Paging Adapter's **IP Address**: The InformaCast Enabled Paging Adapter is delivered with a factory default IP address. Change the default address to the correct IP address for your system.
   - The **Subnet Mask.**
   - The **Default Gateway.**

Note You must click on the **Save** button and then the **Reboot** button for the changes to take effect.

2.5.6 Configure the SIP Parameters

The SIP parameters enable the InformaCast Enabled Paging Adapter to contact and register with the SIP server. Click on the **SIP** button to open the **SIP** page.

Figure 2-15. SIP Page



On the **SIP** page, enter values for the parameters indicated in Table 2-8.

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-8. SIP Configuration Parameters

Web Page Item	Description
SIP Settings	
Enable SIP Operation ?	When enabled, the device will transmit, receive, and process SIP messages according to the configured SIP settings below.
SIP Transport Protocol ?	Choose the transport protocol for SIP signaling. This will affect all extensions, including the Nightringer. Default is UDP.
TLS Version ?	Choose the TLS version for SIP over TLS. Modern security standards strongly recommend using TLS 1.2.
Verify Server Certificate ?	When enabled, the device will verify the authenticity of the server during the TLS handshake by its certificate and common name. The TLS handshake will be aborted if the server is deemed to be inauthentic and SIP registration will not proceed.
Register with a SIP Server ?	When enabled, the device will attempt to register to the configured SIP Server(s) on this page. To configure the device to send and receive point-to-point SIP calls, enable **SIP Operation** and disable **Register with a SIP Server** (see Section 2.5.9, "Configure the Fault Detection Parameters").
Get SIP Params from InformaCast ?	When enabled, the device will get its SIP configuration parameters from the InformaCast server. This will override the manually entered/auto provisioned SIP configuration.
Use Cisco SRST ?	When enabled, the backup servers are handled according to Cisco SRST (Survivable Remote Site Telephony). It is required for use in clustered Cisco Unified Communications Manager topologies.
Primary SIP Server ?	Enter the SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the primary SIP server. This field can accept entries of up to 255 characters in length.
Primary SIP User ID ?	Specify the SIP User ID for the Primary SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the primary SIP server. Enter up to 64 alphanumeric characters.
Primary SIP Auth ID ?	Specify the Authenticate ID for the Primary SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Primary SIP Auth Password ?	Specify the Authenticate Password for the Primary SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Server 1 ?	Enter the backup SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the backup SIP server. This field can accept entries of up to 255 characters in length.
Backup SIP User ID 1 ?	Specify the SIP User ID for the first backup SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the first backup SIP server. Enter up to 64 alphanumeric characters.
Backup SIP Auth ID 1 ?	Specify the Authenticate ID for the first backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Auth Password 1 ?	Specify the Authenticate Password for the first backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.

Table 2-8. SIP Configuration Parameters (continued)

Web Page Item	Description
Backup SIP Server 2	Enter a second backup SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's extension on the second backup SIP server. This field can accept entries of up to 255 characters in length.
Backup SIP User ID 2	Specify the SIP User ID for the second backup SIP Server. This parameter becomes the user portion of the SIP-URI for the device's extension on the second backup SIP server. Enter up to 64 alphanumeric characters.
Backup SIP Auth ID 2	Specify the Authenticate ID for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Backup SIP Auth Password 2	Specify the Authenticate Password for the second backup SIP server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Remote SIP Port	The Remote SIP Port is the port number the device will use as the destination port when sending SIP messages. The default Remote SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
Local SIP Port	The Local SIP Port is the port number the device will use to receive SIP messages. The default Local SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
Outbound Proxy	Enter the Outbound Proxy address as an IPv4 address in dotted decimal notation or a fully qualified domain name (FQDN). When an IP address is configured, the device will send all SIP messages to this IP address. When an FQDN is configured, the device will run DNS NAPTR, SRV, and A queries on the FQDN to resolve an IP address to which it will send all SIP messages. This field can accept entries of up to 255 characters in length.
Outbound Proxy Port	The Outbound Proxy Port is port number used as the destination port when sending SIP messages to the outbound proxy. A value of 0 will default to 5060. The supported range is 0-65536. Enter up to 5 digits.
Disable rport Discovery	Disabling rport Discovery will prevent the device from including the public WAN IP address and port number in the contact information that is sent to the remote SIP servers. This will generally only need to be enabled when using an SBC or SIP ALG in conjunction with a remote SIP server.
Buffer SIP Calls	Also referred to as "delayed paging." Device will buffer up to four minutes of audio then play back the recording after hang up or after the buffer is full. **Note**: Pressing the '#' key while recording a buffered SIP call will end the call and cancel the page before it is sent.
Re-registration Interval (in seconds)	The SIP Re-registration interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
Unregister on Boot	When enabled, the device will send one registration with an expiry of 0 on boot.
Keep Alive Period	The minimum time in milliseconds between keep-alive packets sent for nat traversal. A value of 0 will disable keep alive packets.
RTP Settings	
RTP Port (even)	Specify the port number used for the RTP stream after establishing a SIP call. This port number must be an even number and defaults to 10500. The supported range is 0-65536. Enter up to 5 digits.

Table 2-8. SIP Configuration Parameters (continued)

Web Page Item	Description
Nightringer Settings	
Enable Nightringer	When Nightringer is enabled, the device will attempt to register a second extension with the SIP server. Any calls made to this extension will play a ringtone (corresponds to **Night Ring** on the **Audiofiles** page). By design, it is not possible to answer a call to the Nightringer extension.
SIP Server	Enter the SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's Nightringer extension on the SIP server. This field can accept entries of up to 255 characters in length.
Remote SIP Port	The Remote SIP Port is the port number the device will use as the destination port when sending SIP messages for the Nightringer extension. The default Remote SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
Local SIP Port	The Local SIP Port is the port number the device will use to receive SIP messages for the Nightringer extension. This value cannot be the same as the **Local SIP Port** for the primary extension. The default Local SIP Port is 5061. The supported range is 0-65536. Enter up to 5 digits.
Outbound Proxy	Enter the Outbound Proxy address as an IPv4 address in dotted decimal notation or a fully qualified domain name (FQDN). When an IP address is configured, the device will send all SIP messages to this IP address for the Nightringer extension. When an FQDN is configured, the device will run DNS NAPTR, SRV, and A queries on the FQDN to resolve an IP address to which it will send all SIP messages for the Nightringer extension. This field can accept entries of up to 255 characters in length.
Outbound Proxy Port	The Outbound Proxy Port is port number used as the destination port when sending SIP messages to the outbound proxy for the Nightringer extension. A value of 0 will default to 5060. The supported range is 0-65536. Enter up to 5 digits.
User ID	Specify the SIP User ID for the SIP server. This parameter becomes the user portion of the SIP-URI for the device's Nightringer extension. Enter up to 64 alphanumeric characters.
Authenticate ID	Specify the Authenticate ID for the SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Authenticate Password	Specify the Authenticate Password for the SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Re-registration Interval (in seconds)	The SIP Re-registration Interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
Call Disconnection	
Terminate Call After Delay	Automatically terminate an active call after a given delay in seconds. A value of 0 will disable this function. Enter up to 8 digits.
Codec Selection	
Force Selected Codec	When configured, this option will allow you to force the device to negotiate for the selected codec [PCMU(G.711, u-law), PCMA(G.711, a-law), G.722, or G.729. Otherwise, the device will perform codec negotiation using the default list of supported codecs.
Codec	Select desired codec (only one may be chosen).

Table 2-8. SIP Configuration Parameters (continued)

Web Page Item	Description
RTP Settings	
RTP Port (even)	Specify the port number used for the RTP stream after establishing a SIP call. This port number must be an even number and defaults to 10500. The supported range is 0-65536. Enter up to 5 digits.
Asymmetric RTP	Specify if the remote endpoint will send and receive RTP packets on different ports. If set to false, the device will track the address/port that is sending RTP packets during a SIP call. If the address/port changes mid-stream, the device will disregard the SDP and send all further RTP packets to this new address. If set to true, this device will ignore the sending address/port and send RTP as specified in the SDP. Warning! Enabling asymmetric RTP can cause the RTP stream to be lost. Most installations should not enable asymmetric RTP.
Jitter Buffer	Specify the size of the jitter buffer (in milliseconds) used for SIP calls. Valid values are 50-1000.
RTP Encryption (SRTP)	When enabled, a SIP call's audio streams are encrypted using SRTP.
Save	Click the **Save** button to save your configuration settings.
Reboot	Click on the **Reboot** button to reboot the system.
Toggle Help	Click on the **Toggle Help** button to see a short description of some of the web page items. First click on the **Toggle Help** button, and you will see a question mark ( ) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

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

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

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

1. Enter the IP address of the **SIP Server**.
2. Enter the port numbers used for SIP signaling:
   a. **Remote SIP Port**
   b. **Local SIP Port**
3. Enter the SIP registration parameters:
   a. **SIP User ID**
   b. **Authenticate ID**
   c. **Authenticate Password**
4. For **SIP Registration**, designate whether you want the VoIP Paging Server to register with your SIP server.
5. At **Unregister on Reboot**:

a. Select **Yes** to automatically unregister the InformaCast Enabled Paging Adapter when you reboot it.

b. Select **No** to keep the InformaCast Enabled Paging Adapter registered when you reboot it.

6. In the **Register Expiration** field, enter the number of seconds the InformaCast Enabled Paging Adapter registration lease remains valid with the SIP Server. The InformaCast Enabled Paging Adapter automatically re-registers with the SIP server before the lease expiration timeout.

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

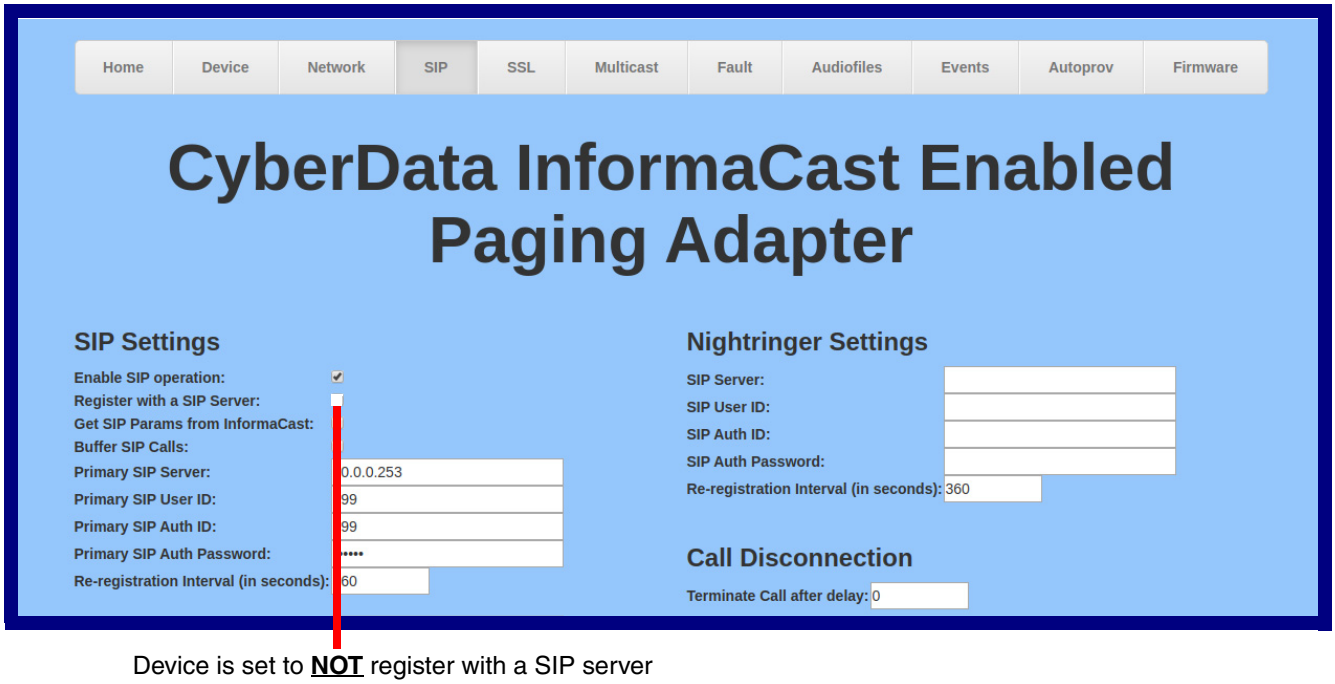
2.5.6.1 Point-to-Point Configuration

When the board is set to not register with a SIP server, it's possible to set the device to dial out to a single endpoint. To do this, do the following:

1. On the **SIP** page (Figure 2-16), make sure that the **Register with a SIP Server** parameter is not selected.
2. Type the IP address of the remote device that you want to contact into the **Dial out Extension** field

Note Establishing point-to-point SIP calls may not work with all phones.

Figure 2-16. SIP Page Set to Point-to-Point Mode



Device is set to **NOT** register with a SIP server

2.5.7 Configure the SSL Parameters

1. Click **SSL** menu button to open the **SSL** page (Figure 2-17 and Figure 2-18).

Figure 2-17. SSL Configuration Page

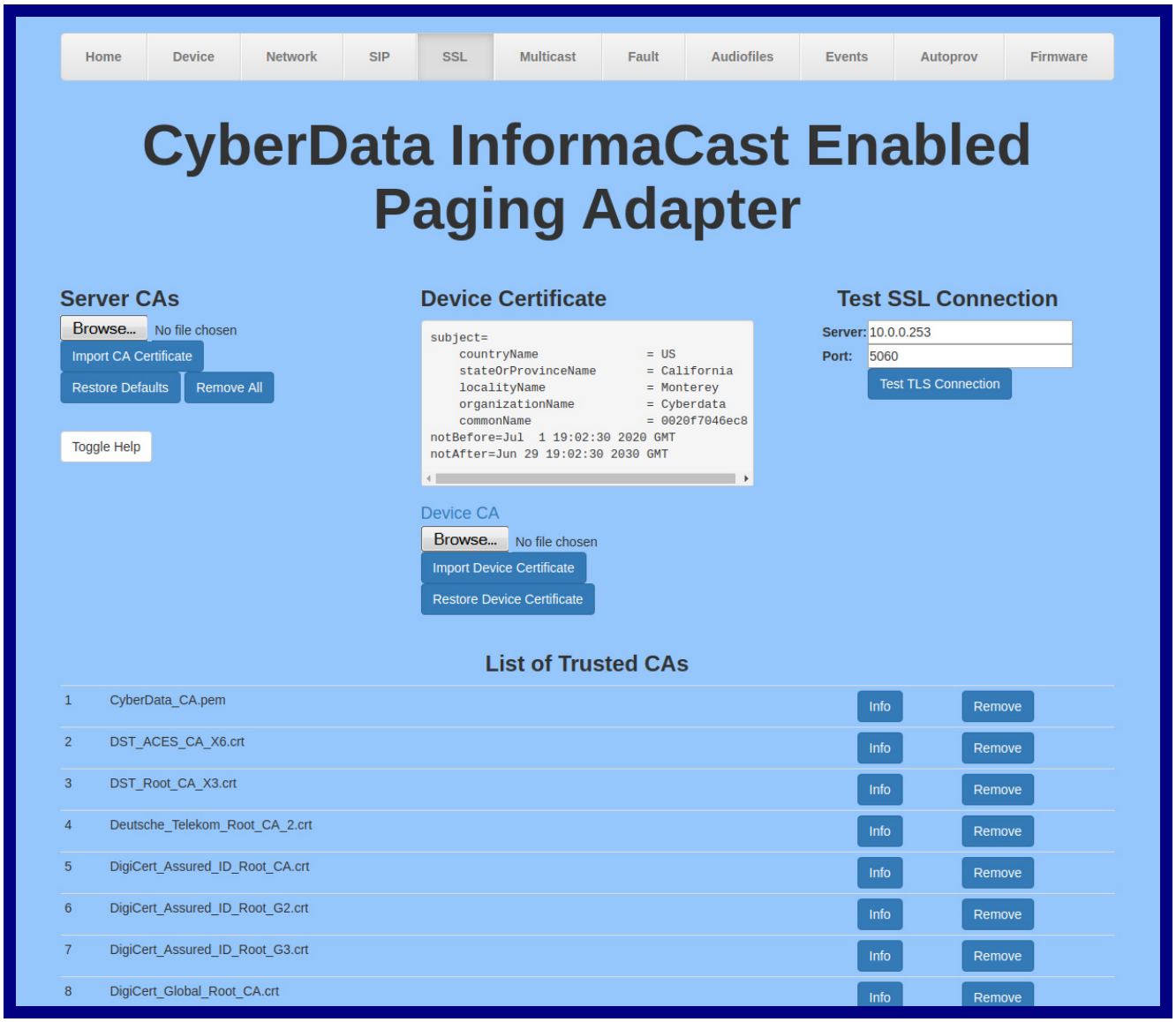


Figure 2-18. SSL Configuration Page

12	DigiCert_Trusted_Root_G4.crt	Info	Remove
13	Equifax_Secure_CA.crt	Info	Remove
14	Equifax_Secure_Global_eBusiness_CA.crt	Info	Remove
15	Equifax_Secure_eBusiness_CA_1.crt	Info	Remove
16	GeoTrust_Global_CA.crt	Info	Remove
17	GeoTrust_Global_CA_2.crt	Info	Remove
18	GeoTrust_Primary_Certification_Authority.crt	Info	Remove
19	GeoTrust_Primary_Certification_Authority_-_G2.crt	Info	Remove
20	GeoTrust_Primary_Certification_Authority_-_G3.crt	Info	Remove
21	GeoTrust_Universal_CA.crt	Info	Remove
22	GeoTrust_Universal_CA_2.crt	Info	Remove
23	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G4.crt	Info	Remove
24	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5.crt	Info	Remove
25	VeriSign_Universal_Root_Certification_Authority.crt	Info	Remove
26	Verisign_Class_1_Public_Primary_Certification_Authority.crt	Info	Remove
27	Verisign_Class_1_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
28	Verisign_Class_2_Public_Primary_Certification_Authority_-_G2.crt	Info	Remove
29	Verisign_Class_2_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
30	Verisign_Class_3_Public_Primary_Certification_Authority.crt	Info	Remove
31	Verisign_Class_3_Public_Primary_Certification_Authority_-_G3.crt	Info	Remove
32	thawte_Primary_Root_CA.crt	Info	Remove
33	thawte_Primary_Root_CA_-_G2.crt	Info	Remove
34	thawte_Primary_Root_CA_-_G3.crt	Info	Remove

2. On the **SSL** page, enter values for the parameters indicated in Table 2-9.

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-9. SSL Configuration Parameters

Web Page Item	Description
Server CAs	
Browse...	Use this button to select a configuration file to import.
Import CA Certificate	Click **Browse** to select a CA certificate to import. After selecting a server certificate authority (CA), click **Import CA Certificate** to import it to the list of trusted CAs. CAs are used to validate the certificate presented by the server when establishing a TLS connection.
Restore Defaults	**Restore Defaults** will restore the default list of registered CAs and **Remove All** will remove all registered CAs.
Remove All	**Restore Defaults** will restore the default list of registered CAs and **Remove All** will remove all registered CAs.
Device Certificate	When doing mutual authentication this device will present a client certificate with these parameters.
Device CA ?	Right click and **Save Link As...** to get the Cyberdata Device CA used to sign this client certificate.
Browse...	Use this button to select a configuration file to import.
Import Device Certificate	Click **Browse** to select a CA certificate to import. After selecting a server certificate authority (CA), click **Import Device Certificate** to import it to the list of trusted Device Certificates. Device Certificates are used to validate the certificate presented by the server when establishing a TLS connection.
Restore Device Certificate	**Restore Device Certificate** will restore the default list of registered Device Certificates.
Test SSL Connection	
Server ?	The ssl test server address as a fully qualified domain name or in IPv4 dotted decimal notation.
Port ?	The ssl test server port. The supported range is 0-65536. SIP connections over TLS to port 5060 will do the same.
Test TLS connection	Use this button to test a TLS connection to a remote server. This will attempt to make a socket connection to the configured test server and port and report the success or failure. This can be used to debug TLS connection issues separate from SIP registration issues.
List of Trusted CAs	

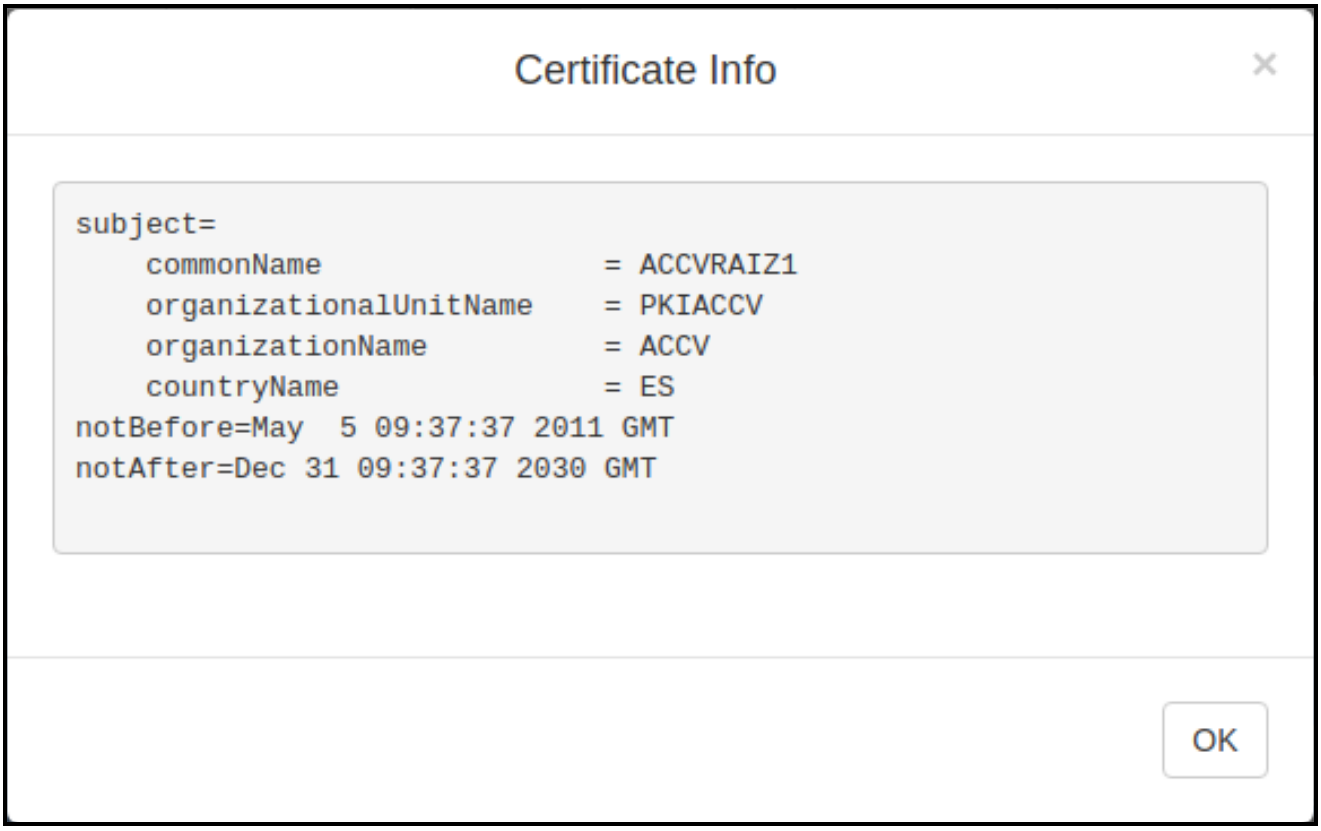
Table 2-9. SSL Configuration Parameters (continued)

Web Page Item	Description
Info	Provides details of the certificate. After clicking on this button, the **Certificate Info Window** appears. See Section 2.5.7.1, "Certificate Info Window".
Remove	Removes this certificate from the list of trusted certificates. After clicking on this button, the **Remove Server Certificate Window** appears. See Section 2.5.7.2, "Remove Server Certificate Window".

2.5.7.1 Certificate Info Window

The **Certificate Info Window** provides details of the certificate. This window appears after clicking on the **Info** button. See Figure 2-19.

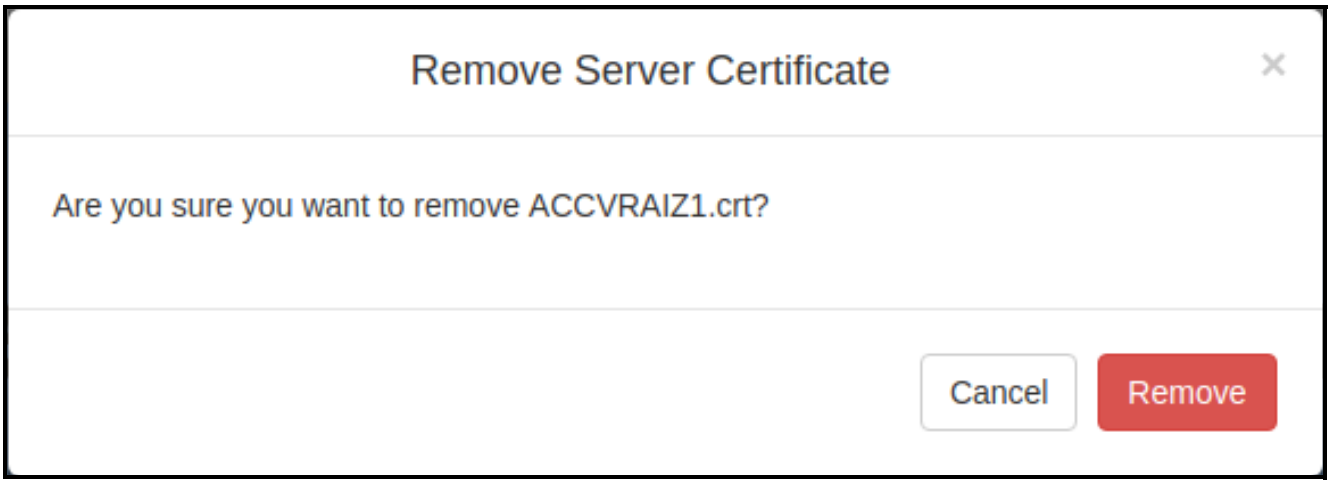
Figure 2-19. Certificate Info Window



2.5.7.2 Remove Server Certificate Window

The **Remove Server Certificate Window** will ask if the user wants to remove a certificate from the list of trusted certificates. This window appears after clicking on the **Remove** button. See Figure 2-20.

Figure 2-20. Remove Server Certificate Window



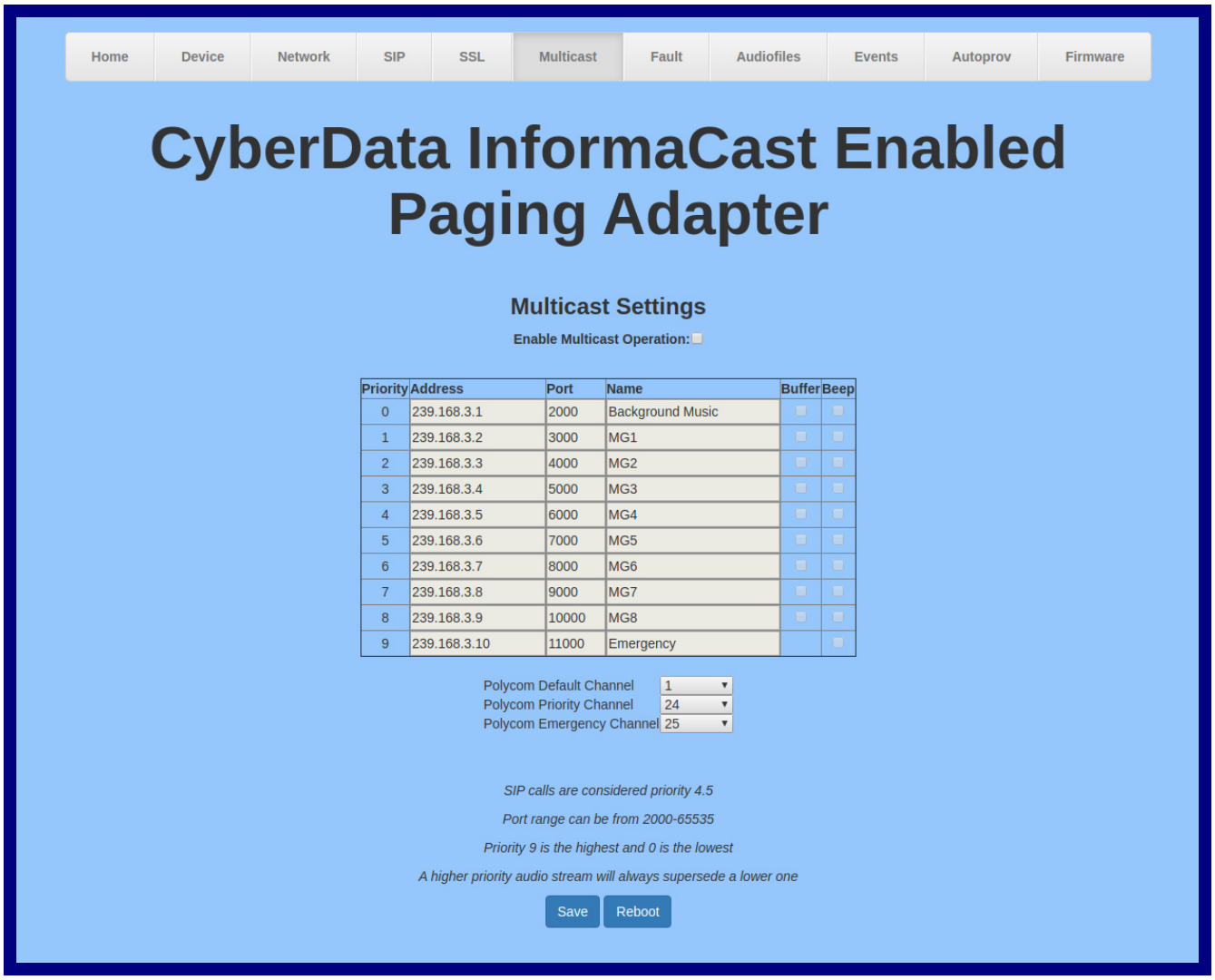
2.5.8 Configure the Multicast Parameters

Multicast groups use multicasting to create public address paging zones. Multicasting is based on the concept of a group. Multicast addresses specify an arbitrary group of IP hosts that have joined the group and want to receive traffic sent to the group. Group members send IGMP messages to their local multicast routers, allowing the group traffic traversal from the source.

The **Multicast Configuration** page allows the device to join up to 10 paging zones for receiving ulaw/alaw, G722, or G729 RTP audio streams. A paging zone can consist of one or many CyberData multicast group-enabled products. There is no limit to how many devices 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 three. The device supports simultaneous SIP and Multicast.

1. Click on the **Multicast** button to open the **Multicast** page. See Figure 2-21.

Figure 2-21. Multicast Page



2. On the **Multicast** page, enter values for the parameters indicated in Table 2-10.

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-10. Multicast Configuration Parameters

Web Page Item	Description
Enable Multicast Operation	Enables or disables multicast operation.
Priority	Indicates the priority for the multicast group. Priority **9** is the highest (emergency streams). **0** is the lowest (background music). SIP calls are considered priority **4.5**. See Section 2.5.8.1, "Assigning Priority" for more details.
Address	Enter the multicast IP Address for this multicast group (15 character limit).
Port	Enter the port number for this multicast group (5 character limit [range can be from 2000 to 65535]). **Note**: The multicast ports have to be even values. The webpage will enforce this restriction.
Name	Assign a descriptive name for this multicast group (25 character limit).
Buffer	Device will buffer up to four minutes of audio and then play back the recording after the multicast stream finishes or after the buffer is full.
Beep	When selected, the device will play a beep before multicast audio is sent.
Polycom Default Channel	When a default Polycom channel/group number is selected, the SIP Paging Adapter will subscribe to the default channel for one-way group pages. Group Numbers 1-25 are supported. Or, select **Disabled** to disable this channel.
Polycom Priority Channel	When a priority Polycom channel/group number is selected, the SIP Paging Adapter will subscribe to the priority channel for one-way group pages. Group Numbers 1-25 are supported. Or, select **Disabled** to disable this channel.
Polycom Emergency Channel	When an emergency Polycom channel/group number is selected, the SIP Paging Adapter will subscribe to the default channel for one-way group pages. Group Numbers 1-25 are supported. Or, select **Disabled** to disable this channel.
Save	Click the **Save** button to save your configuration settings.
Reboot	Click on the **Reboot** button to reboot the system.

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

2.5.8.1 Assigning Priority

When playing multicast streams, audio on different streams will preempt each other according to their priority in the list. An audio stream with a higher priority will interrupt a stream with a lower priority.

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**.

Note SIP calls, multicast streams, ring tones, ringback tones, and nightring tones are all prioritized.

Ringtones and Nightringtones

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.

2.5.8.2 Polycom Paging

Page your entire paging infrastructure, including legacy analog paging systems, using Polycom IP phones and a CyberData SIP Paging Adapter. Simultaneously paging your IP phones and overhead speakers can be as simple as pressing the Paging soft key on a Polycom IP phone.

The Polycom Paging feature is supported on Polycom IP phones using UC Software 4.0.0 and higher. The Polycom paging feature operates in two modes: Push-to-Talk (PTT) and Group Paging. Only Group Paging mode pages are supported by the SIP Paging Adapter.

Polycom phones use the same multicast IP address and port number for both PTT and Group Paging multicasts. Make sure to note the Polycom multicast IP address and port number before configuring the CyberData SIP Paging Adapter. Polycom phones use a default multicast IP address of 224.0.1.116 and odd-numbered port 5001.

While the same multicast IP address and port number is used for all Polycom pages in both modes, Polycom uses numbered "groups" or "channels" to differentiate between each paging group. Each "group" or "channel" is numbered 1 through 25.

The SIP Paging Adapter can subscribe to Group Numbers 1 through 25 for Group Paging one-way audio pages. You may configure up to three group numbers or "channels", which are labeled **Polycom Default Channel**, **Polycom Priority Channel**, and **Polycom Emergency Channel** on the **Multicast Page**. Each of the three available channels can be disabled.

It is important to note the SIP Paging Adapter assigns a priority to each multicast group, as referenced in Section 2.5.8.2, "Polycom Paging". Polycom priority assignments by channel are ignored.

When configuring Polycom phones for their Group Paging feature, be sure the following settings are configured:

- Payload Size = 20 ms (milliseconds)
- Codec = G.711Mu

The SIP Paging Adapter supports Polycom Group Paging multicasts that are G.711Mu encoded with a payload size of 20 ms.

Use the following steps to configure Polycom Group Paging on the SIP Paging Adapter:

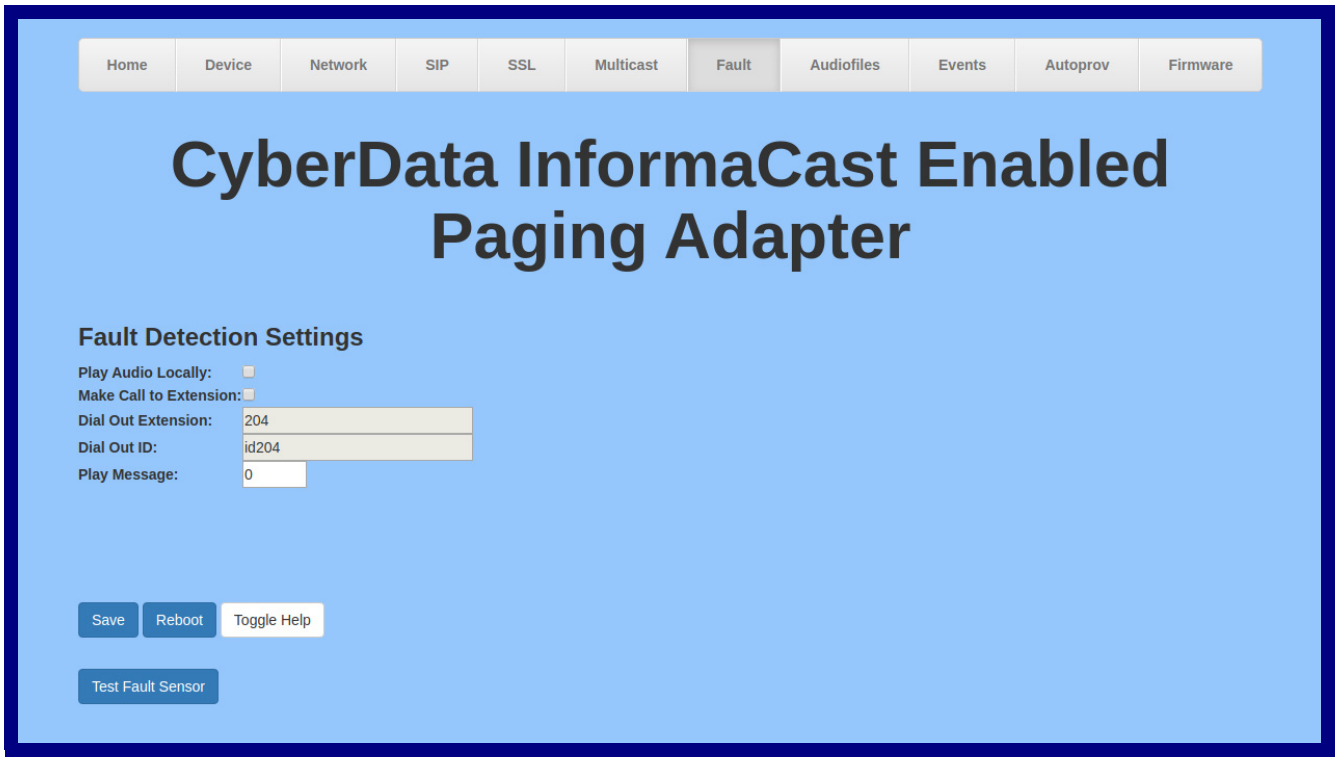
1. Identify the Polycom multicast IP address and port number used by the Polycom phones.

2. Check the box to **Enable Multicast Operation** on the **Multicast Page**.
3. Choose a priority group and enter the Polycom IP address and port number into the **Priority**, **Address**, and **Port** fields on the **Multicast Page**.
4. Select up to three channel/group numbers for Group Paging subscriptions at the bottom of the **Multicast Page**.
5. Save and reboot to store changes.

2.5.9 Configure the Fault Detection Parameters

1. Click on the **Fault** button to open the **Fault** page. See Figure 2-22.

Figure 2-22. Fault Page



2. On the **Fault Detection** page, enter values for the parameters indicated in Table 2-11.

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-11. Fault Detection Configuration Parameters

Web Page Item	Description
Triggered Settings	
Play Stored Audio Locally ?	When selected, the device will play the user defined “sensor triggered” audio file when the fault detection is triggered.
Make Call to Extension ?	When selected, the device will call an extension when fault detection is triggered. Use the **Dial Out Extension** field to specify the extension the device will call.
Dial Out Extension ?	Specify the extension the device will call when fault detection is triggered. Enter up to 64 alphanumeric characters.
Dial Out ID ?	An additional Caller identification string added to outbound calls. Enter up to 64 alphanumeric characters.
Repeat Message ?	The number of times to repeat the audio message through the local speaker or to the remote endpoint. A value of 0 will repeat forever. Enter a value from 0-65536.
Test Fault Detection	Click on the **Test Fault Detection** button to test the fault detection feature.
Save	Click the **Save** button to save your configuration settings.
Reboot	Click on the **Reboot** button to reboot the system.
Toggle Help	Click on the **Toggle Help** button to see a short description of some of the web page items. First click on the **Toggle Help** button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

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

2.5.10 Configure the Audio Parameters

Click on the **Audiofiles** button to open the **Audiofiles** page. See Figure 2-23. 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 2-23. Audiofiles Page

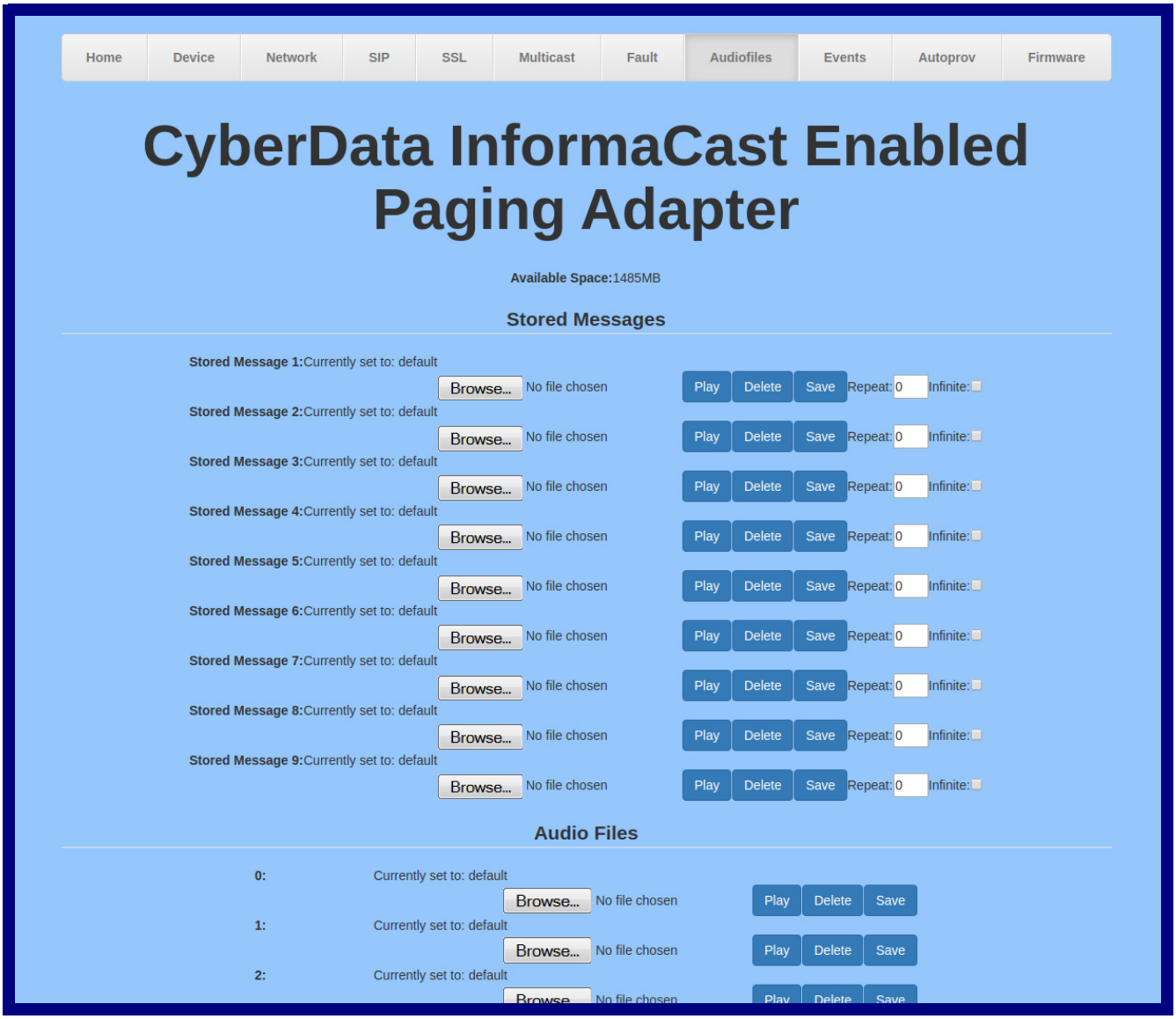


Figure 2-24. Audiofiles Page

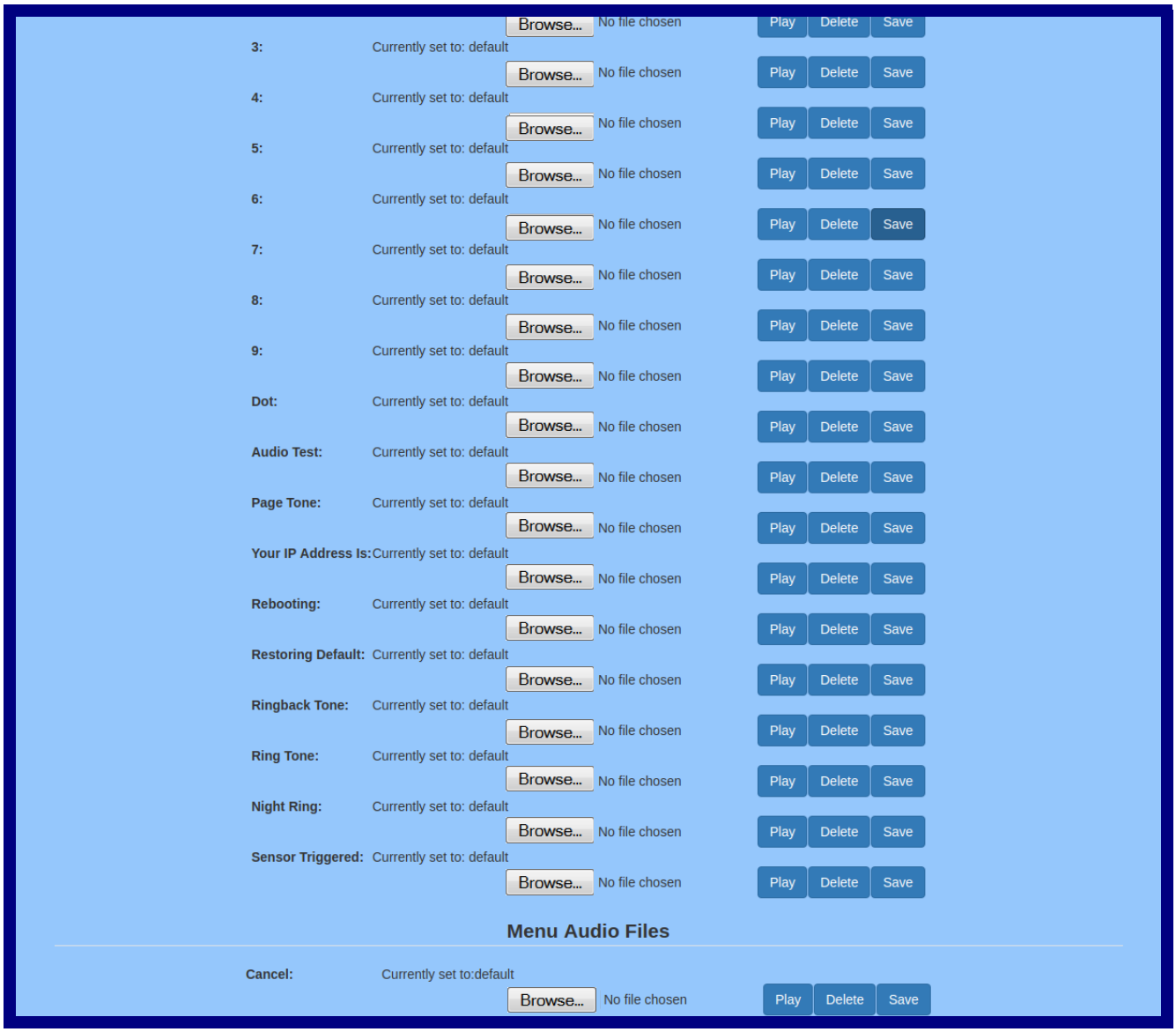


Figure 2-25. Audiofiles Page

On the **Audiofiles** page, enter values for the parameters indicated in Table 2-12.

Note Each entry on the **Audiofiles** page replaces one of the stock audio files on the board. When the input box displays the word **default**, the InformaCast Enabled Paging Adapter is using the stock audio file. If that file is replaced with a user file, it will display the uploaded filename.

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-12. Audiofiles Configuration Parameters

Web Page Item	Description
Stored Messages	
Stored Message 1 through 9	**Stored Message 1** corresponds to the message played after pressing **1** on a phone keypad. **Stored Message 2** corresponds to the message played after pressing **2** on a phone keypad. **Stored Message 3** corresponds to the message played after pressing **3** on a phone keypad. **Stored Message 4** corresponds to the message played after pressing **4** on a phone keypad. **Stored Message 5** corresponds to the message played after pressing **5** on a phone keypad. **Stored Message 6** corresponds to the message played after pressing **6** on a phone keypad. **Stored Message 7** corresponds to the message played after pressing **7** on a phone keypad. **Stored Message 8** corresponds to the message played after pressing **8** on a phone keypad. **Stored Message 9** corresponds to the message played after pressing **9** on a phone keypad.
Repeat	Type the number of times that you want the specific **Stored Message** to repeat. A value of **0** means the message will play once (no repeat). A value of **1** means the message will play twice (one repeat).
Infinite	When selected, the specific **Stored Message** will repeat indefinitely after pressing the specific number key on a phone keypad. **Note**: The repeatedly playing audio can be canceled by calling, selecting the message, and pressing the **#** key.
Audio Files	
0-9	The name of the audio configuration option is the same as the spoken audio that plays on the board (24 character limit). '0' corresponds to the spoken word “zero.” '1' corresponds to the spoken word “one.” '2' corresponds to the spoken word “two.” '3' corresponds to the spoken word “three.” '4' corresponds to the spoken word “four.” '5' corresponds to the spoken word “five.” '6' corresponds to the spoken word “six.” '7' corresponds to the spoken word “seven.” '8' corresponds to the spoken word “eight.” '9' corresponds to the spoken word “nine.”
Dot	Corresponds to the spoken word “dot.” (24 character limit).
Audio Test	Corresponds to the message “This is the CyberData IP speaker test message...” (24 character limit).
Enter Code	Corresponds to the message “Enter Code” (24 character limit).

Table 2-12. Audiofiles Configuration Parameters (continued)

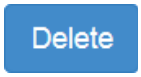
Web Page Item	Description
Invalid Code	Corresponds to the message “Invalid Code” (24 character limit).
Page Tone	Corresponds to a simple tone that is unused by default (24 character limit).
Your IP Address is	Corresponds to the message “Your IP address is...” (24 character limit).
Rebooting	Corresponds to the spoken word “Rebooting” (24 character limit).
Restoring Default	Corresponds to the message “Restoring default” (24 character limit).
Sensor Triggered	Corresponds to the message “Sensor Triggered” (24 character limit).
Night Ring	Specifies the ringtone for nightring. By default this parameter uses the same audio file that is selected for the **Ring Tone** parameter.
Menu Audio Files	**Menu Audio Files** are user-uploadable messages that create the audio menu played to the caller.
Cancel	Corresponds to the word "Cancel" used in the audio menu played to the caller. (24 character limit).
Currently Playing	Corresponds to the words "Currently Playing" used in the audio menu played to the caller. (24 character limit).
Fault Detection Message	Corresponds to the words "Fault Detection Message" used in the audio menu played to the caller. (24 character limit).
Invalid Entry	Corresponds to the words "Invalid Entry" used in the audio menu played to the caller. (24 character limit).
Page	Corresponds to the word "Page" used in the audio menu played to the caller. (24 character limit).
Play Stored Message	Corresponds to the words "Play Stored Message" used in the audio menu played to the caller. (24 character limit).
Pound (#)	Corresponds to whatever word or phrase the user wishes to call the pound key in the audio menu played to the caller (24 character limit).
Press	Corresponds to the word "Press" used in the audio menu played to the caller. (24 character limit).
Stored Message	Corresponds to the words "Stored Message" used in the audio menu played to the caller. (24 character limit).
Through	Corresponds to the word "Through" used in the audio menu played to the caller. (24 character limit).
To	Corresponds to the word "To" used in the audio menu played to the caller. (24 character limit).
Enter Zone	Corresponds to the words "Enter Zone" used in the audio menu played to the caller. (24 character limit).
	The **Browse** button will allow you to navigate to and select an audio file.
	The **Play** button will play that audio file.
	The **Delete** button will delete any user uploaded audio and restore the stock audio file.
	The **Save** button will download a new user audio file to the board once you've selected the file by using the **Browse** button. The **Save** button will delete any pre-existing user-uploaded audio files.
	Click the **Save** button to save your configuration settings.

Table 2-12. Audiofiles Configuration Parameters (continued)

Web Page Item	Description
Reboot	Click on the **Reboot** button to reboot the system.

2.5.10.1 User-created Audio Files

User-created audio files must be saved in one of the following formats:

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

Note These audio format restrictions are enforced by the webpage.

You can use the free utility *Audacity* to convert audio files into this format. See Figure 2-26 through Figure 2-28.

Figure 2-26. Audacity 1

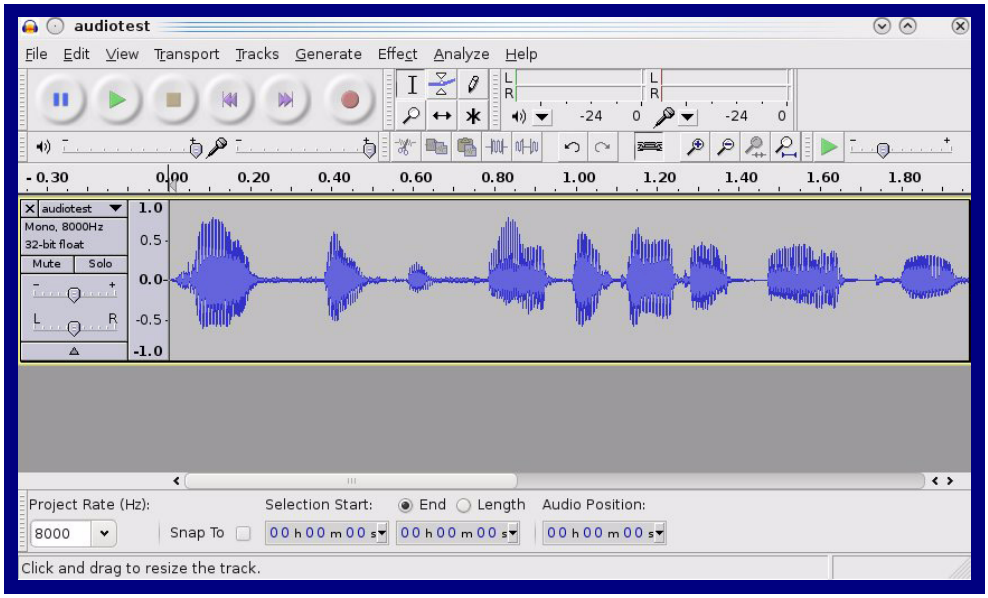
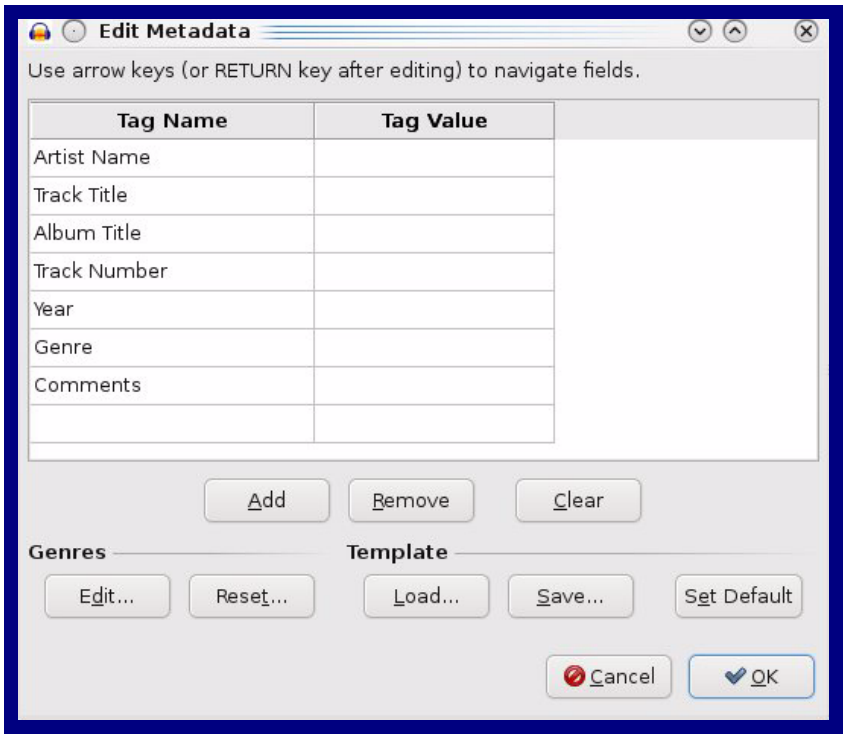


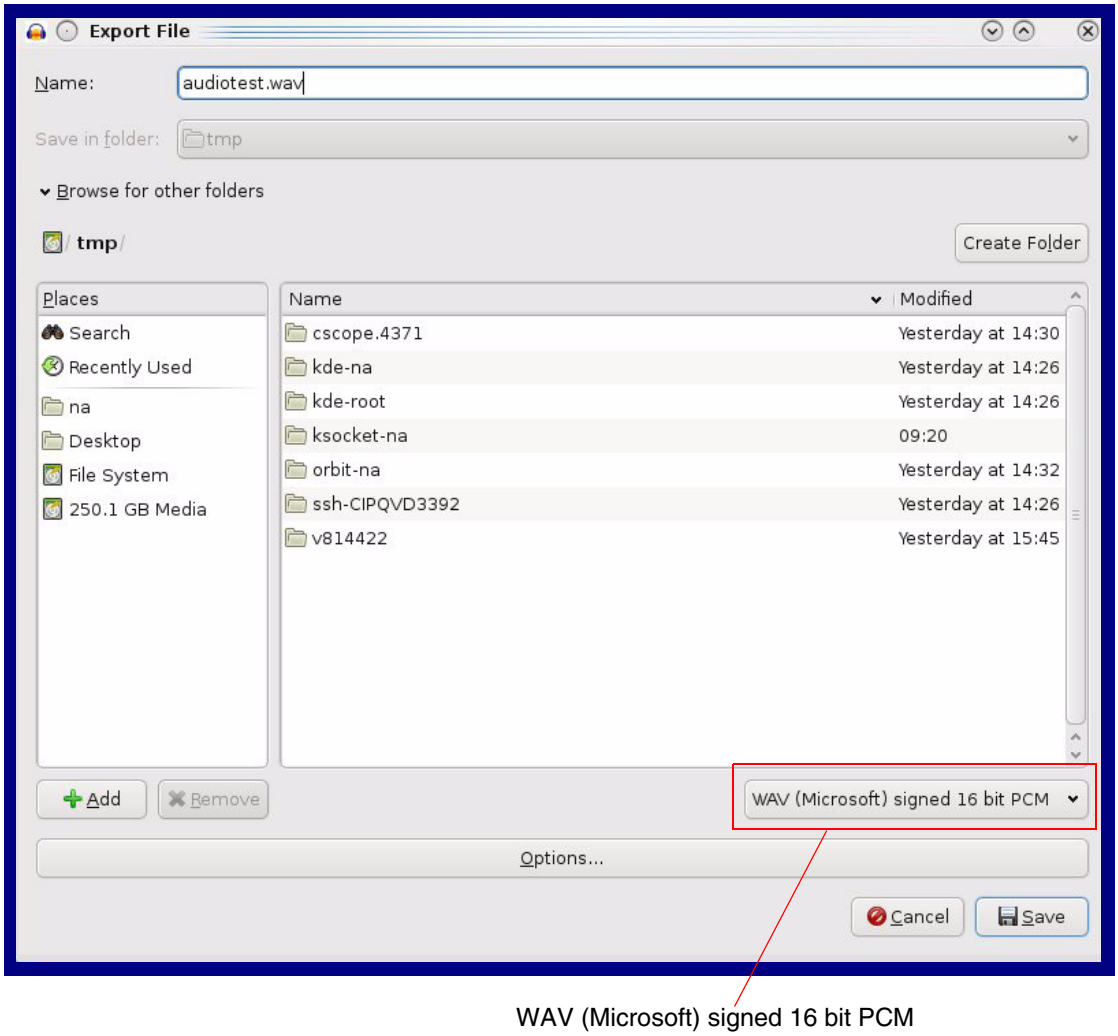
Figure 2-27. Audacity 2



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

- **WAV (Microsoft) signed 16 bit PCM**.

Figure 2-28. WAV (Microsoft) signed 16 bit PCM



2.5.11 Configure the Event Parameters

Click on the **Events** button to open the **Events** page (Figure 2-29). The **Events** page specifies a remote server that can be used to receive HTTP POST events when actions take place on the board.

Figure 2-29. Events Page

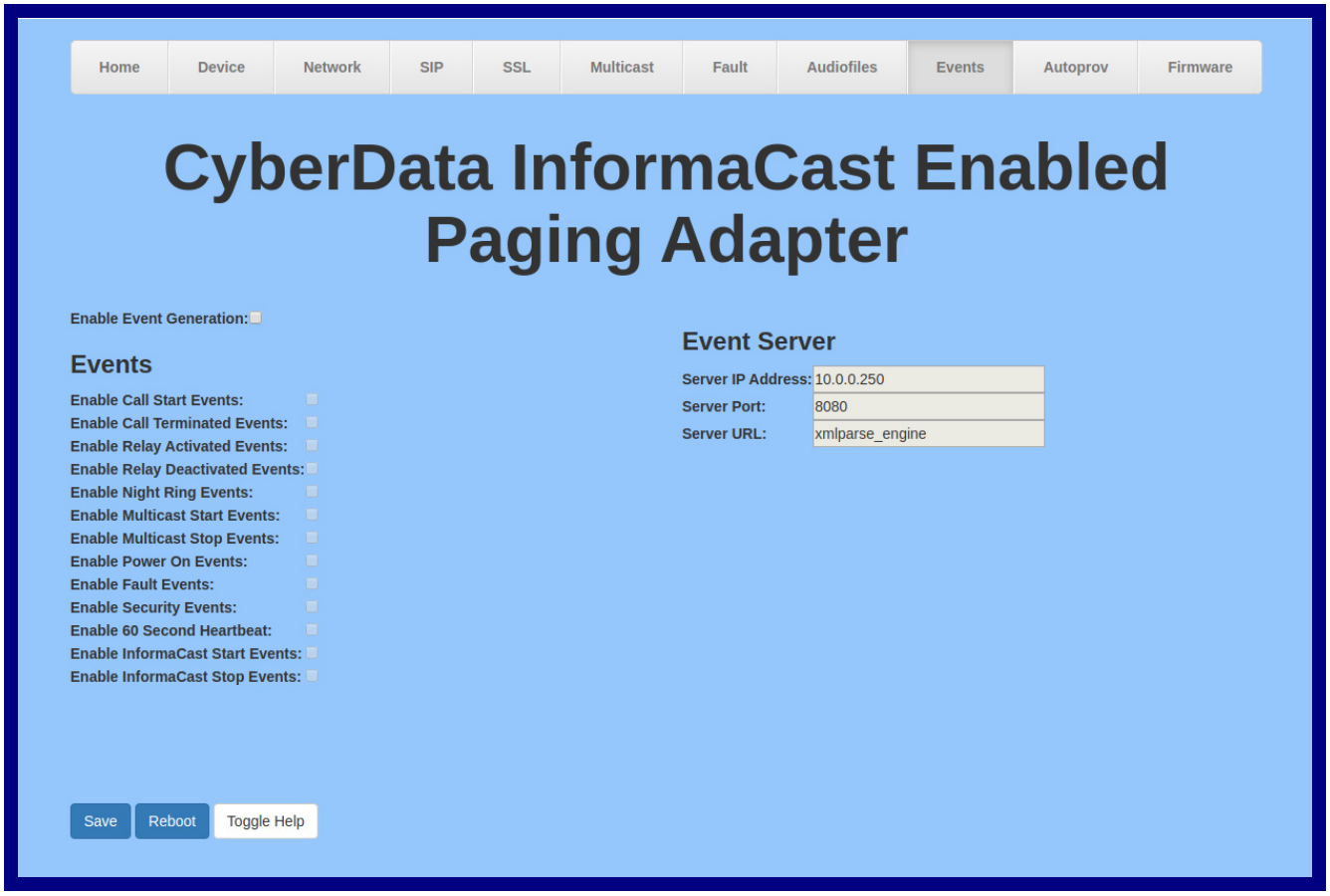


Table 2-13 shows the web page items on the **Events** page.

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-13. Events Configuration

Web Page Item	Description
Enable Event Generation ?	The device will send HTTP POST events to the specified remote server and port number whenever a certain action takes place. Select an event type below to generate an HTTP POST event. See Section 2.5.11.1, "Example Packets for Events" for sample packets.
Events	
Enable Call Start Events ?	When selected, the device will report the start of a SIP call.
Enable Call Terminated Events ?	When selected, the device will report the end of a SIP call.
Enable Relay Activated Events ?	When selected, the device will report relay activation.
Enable Relay Deactivated Events ?	When selected, the device will report relay deactivation.
Enable Night Ring Events ?	When selected, the device will report when it starts ringing upon an incoming SIP call to the Nightringer extension. As a reminder, the Nightringer extension always rings upon an incoming SIP call and it is not possible to alter this behavior.
Enable Power On Events ?	When selected, the device will report when it boots.
Enable Fault Events ?	When selected, the device will report when the on-board fault detection is activated.
Enable 60 Second Heartbeat ?	When enabled, the device will report a Heartbeat event every 60 seconds. SIP registration is not required to generate Heartbeat events.
Enable Informacast Start Events ?	When selected, the device will report when a Start event has been received from the Singlewire server.
Enable Informacast Stop Events ?	When selected, the device will report when a Stop event has been received from the Singlewire server.
Event Server	
Server IP Address ?	The IPv4 address of the event server in dotted decimal notation.
Server Port ?	Specify the event server port number. The supported range is 0-65536. Enter up to 5 digits.
Server URL ?	Generally, the destination URL is the name of the application that receives the events and the string in the HTTP POST command. It can be a script used to parse and process the HTTP POST events. Enter up to 127 characters.
Check All	Click on **Check All** to select all of the events on the page.
Uncheck All	Click on **Uncheck All** to de-select all of the events on the page.
Save	Click the **Save** button to save your configuration settings.
Reboot	Click on the **Reboot** button to reboot the system.

Table 2-13. Events Configuration (continued)

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

Note You must click on the **Save** button for the changes to take effect, and then the **Reboot** button if you are specifying a server.

2.5.11.1 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>
```

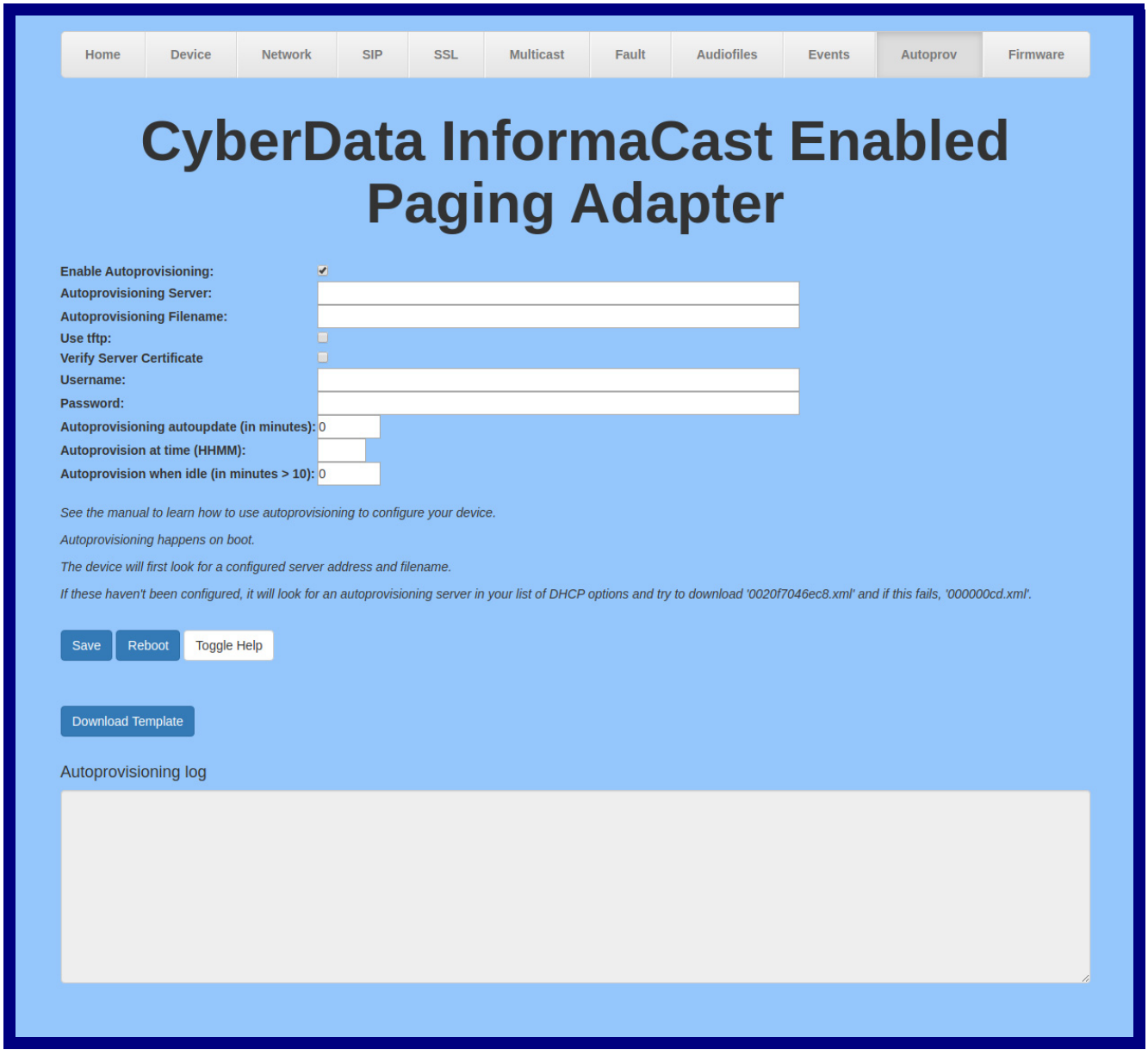
2.5.12 Configure the Autoprovisioning Parameters

Autoprovisioning can be used to automatically configure your device. The autoprovisioning file is an xml file with the device configuration. Values found in this file will override values stored in on-board memory.

Note By default, the device will try to set up its configuration with autoprovisioning.

1. Click the **Autoprov** menu button to open the **Autoprovisioning** page. See Figure 2-30.

Figure 2-30. Autoprovisioning Page



2. On the **Autoprovisioning** page, you may enter values for the parameters indicated in Table 2-14.

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-14. Autoprovisioning Configuration Parameters

Web Page Item	Description
Disable Autoprovisioning ?	Prevent the device from automatically trying to download a configuration file. See Section 2.5.12.1, "Autoprovisioning" for more information.
Autoprovisioning Server ?	Enter the address of the provisioning server as a fqdn or IPv4 address in dotted decimal notation.
Autoprovisioning Filename ?	The name of the configuration file. The default autoprovisioning filename is in the format of **<mac address>.xml**. Supported filename extensions are ".txt", and ".xml." The current filename is denoted by an asterisk at the bottom of the **Autoprovisioning Page**. Enter up to 256 characters. A file may have any name with an xml extension. If a file name is entered, the device will look for the specified file name, and only that file.
Use tftp ?	The device will use TFTP (instead of http) to download autoprovisioning files.
Username ?	The username used to authenticate with an autoprovisioning server. Leave this field blank to disable authentication.
Password ?	The password used to authenticate with an autoprovisioning server. Leave this field blank to disable authentication.
Autoprovisioning autoupdate (in minutes) ?	The reoccurring time (in minutes) the device will wait before checking for new autoprovisioning files. Enter up to 6 digits. A value of 0 will disable this option. **Note**: To use the auto update options, enable the **Enable NTP** setting on the **Device Page** page (see Table 2-6).
Autoprovision at time (HHMMSS) ?	The time of day the device will check for a new autoprovisioning file. The time must be 6 characters in length and in HHMMSS format. An empty value will disable this option. **Note**: To use the auto update options, enable the **Enable NTP** setting on the **Device Page** page (see Table 2-6).
Autoprovision when idle (in minutes > 10) ?	The idle time (in minutes greater than 10) after which the device will check for a new autoprovisioning file. Enter up to 6 digits. A value of 0 will disable this option. **Note**: To use the auto update options, enable the **Enable NTP** setting on the **Device Page** page (see Table 2-6).
Save	Click the **Save** button to save your configuration settings.
Reboot	Click on the **Reboot** button to reboot the system.
Toggle Help	Click on the **Toggle Help** button to see a short description of some of the web page items. First click on the **Toggle Help** button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

Table 2-14. Autoprovisioning Configuration Parameters (continued)

Web Page Item	Description
Download Template	Press the **Download Template** button to create an autoprovisioning file for the device. See Section 2.5.12.3, "Get Autoprovisioning Template Button"
Autoprovisioning log	The autoprovisioning log provides information about the latest autoprovisioning attempt (i.e. dhcp options and server accessed and files parsed or not found).

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

2.5.12.1 Autoprovisioning

On boot, the device will look for an autoprovisioning server configured on the Autoprovisioning Page or specified as a DHCP option. When it finds a server, it will try to download the following (in order of preference):

1. The file configured on the autoprovisioning page.
2. A file named according to it's mac address (for example: 0020f7350058.xml).
3. The file 000000cd.xml

The file can be hosted using a standard web server (like apache, IIS, or nginx), and the device can download over SSL. The file server can be an ipv4 address in dotted decimal notation or a fully qualified domain name.

By default, the device will get its autoprovisioning server from the DHCP options. See Section 2.5.12.2, "Sample dhcpd.conf" for an example of how to configure dhcpd to offer autoprovisioning server addresses. If multiple options are set, the device will attempt to download autoprovisioning files from every server.

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

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

You can download an autoprovisioning template file from the Autoprovisioning Page using the **Download Template** button (see Table 2-14). This file contains every configuration option that can be set on the board.

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

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

```
    <MiscSettings>
        <DeviceName>CyberData VoIP Intercom</DeviceName>
<!--    <AutoprovFile>common.xml</AutoprovFile>-->
<!--    <AutoprovFile>sip_reg[macaddress].xml</AutoprovFile>-->
<!--    <AutoprovFile>audio[macaddress]</AutoprovFile>-->
```

```
<!--    <AutoprovFile>device[macaddress].xml</AutoprovFile>-->
    </MiscSettings>
```

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

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

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

The file 0020f7123456.xml contains:

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

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

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

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

Checking for New Autoprovisioning Files after Boot

The device will always check for an autoprovisioning files on boot but it can be configured to also check after a periodic delay, when idle, or at a specified time. When one of these options is set, the device will download its autoprovisioning files again, and if it finds any differences from the files it downloaded on boot, it will force a reboot and reconfigure.

The Autoprovisioning Filename

The autoprovisioning filename can contain a file, a file path, or a directory.

Table 2-15. Autoprovisioning File Name

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

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

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

For example:

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

The autoprovisioning filename is set to "cyberdata/"

On boot, the device will try to download:

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

...and if this fails:

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

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

Autoprovisioning Firmware Updates

```
<FirmwareSettings>
  <FirmwareFile>505-uImage-ceilingspeaker</FirmwareFile>
  <FirmwareServer>10.0.1.3</FirmwareServer>
  <OutdoorIntercom30>firmware_file_v9.3.0</OutdoorIntercom30>
  <OutdoorIntercom31>firmware_file_v10.3.0</OutdoorIntercom31>
  <CallButton31>firmware_file_v10.3.0</CallButton31>
</FirmwareSettings>
```

In the <FirmwareSettings> section, the <FirmwareServer> element can be used to specify a different server for hosting firmware files. When this element is not available, the device will try to download the file from the autoprovisioning server.

The device will use the filename to determine when to autoprovision firmware updates. The default configuration is blank, so the first time you set a value in your autoprovisioning file, it may force a firmware update even if the firmware version has not changed.

The <FirmwareFile> name can contain path elements (i.e. /path/to/firmware/10.3.0-uImage-[device_file_name]).

The device also supports product strings for downloading firmware. If the <FirmwareFile> option is not set, the device will look for its particular product string for a firmware filename. In this way, a generic autoprovisioning file can specify unique firmware for a range of products.

The list of valid product strings:

```
<ProductString>CallButton31</ProductString>
<ProductString>EmergencyIntercom31</ProductString>
<ProductString>EmergencyIntercom31SW</ProductString>
<ProductString>IndoorIntercom31</ProductString>
<ProductString>IndoorIntercom31SW</ProductString>
<ProductString>IndoorKeypad31</ProductString>
<ProductString>IndoorKeypad31SW</ProductString>
<ProductString>OfficeRinger31</ProductString>
<ProductString>OfficeRinger31SW</ProductString>
<ProductString>OutdoorIntercom31</ProductString>
<ProductString>OutdoorIntercom31SW</ProductString>
<ProductString>OutdoorKeypad31</ProductString>
<ProductString>OutdoorKeypad31SW</ProductString>
<ProductString>Strobe31</ProductString>
<ProductString>Strobe31SW</ProductString>
```

Autoprovisioning Example 1

Here's a simple example using four autoprovisioning files to configure two devices:

We boot up two devices with mac addresses **00:20:f7:02:00:01** and **00:20:f7:02:00:02** (Device1 and Device2).

The devices are set to use DHCP and that server provides an autoprovisioning server address with option 43. The address is “https://autoprovtest.server.net.” The files on this server are as follows:

000000cd.xml

```
<MiscSettings>
<DeviceName>CyberData Autoprovisioned</DeviceName>
<AutoprovFile>sip_common.xml</AutoprovFile>
<AutoprovFile>sip_[macaddress].xml</AutoprovFile>
</MiscSettings>
```

sip_common.xml

```
<SIPSettings>
<SIPServer>10.0.0.253</SIPServer>
<RemoteSIPPort>5060</RemoteSIPPort>
</SIPSettings>
```

sip_0020f7020001.xml

```
<SIPSettings>
<SIPUserID>198</SIPUserID>
<SIPAuthPassword>ext198</SIPAuthPassword>
<DialoutExtension0>204</DialoutExtension0>
</SIPSettings>
```

sip_0020f7020002.xml

```
<SIPSettings>
<SIPUserID>500</SIPUserID>
<SIPAuthPassword>ext500</SIPAuthPassword>
<DialoutExtension0>555</DialoutExtension0>
</SIPSettings>
```

On boot, Device1 tries to fetch the file **0020f7023614.xml** from “https://autoprovtest.server.net”. This file is not available, so device1 then tries to fetch the file **000000cd.xml**. This file exists, and Device1 parses the three elements.

1. Device1 changes its device name to **CyberData Autoprovisioned**.
2. Device1 finds an AutoprovFile element containing the filename **sip_common.xml**. The device downloads **sip_common.xml** from “https://autoprovtest.server.net,” and imports this configuration, setting the sip server to **10.0.0.253** and the remote port to **5060.3**.
3. Device1 finds another AutoprovFile element containing the filename **sip_[macaddress].xml**. The device replaces the **[macaddress]** with its own mac address value creating **sip_0020f7020001.xml**, downloads this file from “https://autoprovtest.server.net,” and imports this configuration. This sets the user ID to **198**, the password to **ext198**, and the dialout extension to **204**. Device1 is now finished with autoprovisioning.

Device2 goes through the same steps by setting its device name to **CyberData Autoprovisioned**, its SIP server to **10.0.0.253**, and its port to **5060**. When Device2 "sees" **sip_[macaddress].xml**, Device2 replaces it with its own mac address and downloads **sip_0020f7020002.xml** from "https://autoprovtest.server.net." Device2 sets the SIP User ID to **500**, the password to **ext500**, and the dialout extension to **555**.

Autoprovisioning Example 2

Here is another example of setting up your autoprovisioning files:

We boot up two devices with mac addresses **00:20:f7:02:00:01** and **00:20:f7:02:00:02** (Device1 and Device2) and boot them on a network with a DHCP server configured with an autoprovisioning server at **10.0.1.3** on option **150**. Our TFTP server has three files:

0020f7020001.xml

```
<MiscSettings>
<AutoprovFile>common_settings.xml</AutoprovFile>
</MiscSettings>
<SIPSettings>
<SIPUserID>198</SIPUserID>
<SIPAuthPassword>ext198</SIPAuthPassword>
<DialoutExtension0>204</DialoutExtension0>
</SIPSettings>
```

0020f7020002.xml

```
<MiscSettings>
<AutoprovFile>common_settings.xml</AutoprovFile>
</MiscSettings>
<SIPSettings>
<SIPUserID>500</SIPUserID>
<SIPAuthPassword>ext500</SIPAuthPassword>
<DialoutExtension0>555</DialoutExtension0>
</SIPSettings>
```

common_settings.xml

```
<MiscSettings>
<DeviceName>CyberData Autoprovisioned</DeviceName>
</MiscSettings>
<SIPSettings> <SIPServer>10.0.0.253</SIPServer>
<RemoteSIPPort>5060</RemoteSIPPort>
</SIPSettings>
```

1. On boot, Device1 downloads **0020f7020001.xml** from **10.0.1.3** and imports these values. The SIP User ID is **198**, the password is **ext198**, and the dialout extension is **204**.

2. Device1 then gets the filename **common_settings.xml** from the AutoprovFile element and downloads this file from the TFTP server at **10.0.1.3**. and imports these settings. The device name is set to **CyberData Autoprovisioned**, the SIP server is set to **10.0.0.253**, and the port is set to **5060**.

Device2 does the same except it downloads **0020f7020002.xml** on boot and imports these values instead. The Sip User ID is **500**, password is **ext500**, and dialout extension is **555**. Device2 then downloads the **common_settings.xml** file and imports those values. The device name is set to **CyberData Autoprovisioned**, the SIP server is set to **10.0.0.253**, and the port is set to **5060**.

XML Files

XML files can contain <AutoprovFile> elements. If multiple DHCP options are specified, the device will try to download autoprovisioning files from each in turn. The device will only look for <AutoprovFile> elements in the first file downloaded from each server. You can specify up to 20 <AutoprovFile> elements in the first autoprovisioning file.

There are numerous ways to change an element of the **configuration(xml)** file. Using **sip ext** as an example, the extension can be changed:

Within the device-specific xml, i.e. **[macaddress].xml**, via the AutoprovFile element:<SIPSettings>/<SIPExt>

From the device specific xml, a pointer to a sip_common file

From the device specific xml, a pointer to the device specific sip_[macaddress].xml

From the common file, a pointer to sip_common.xml

From the common file, a pointer to the device specific (sip_[macaddress].xml)

Autoprovisioned Audio Files

Audio files are stored in non-volatile memory and an autoprovisioned audio file will only have to be downloaded once for each device. Loading many audio files to the device from the web page could cause it to appear unresponsive. If this happens, wait until the transfer is complete and then refresh the page.

The device uses the file name to determine when to download a new audio file. This means that if you used autoprovisioning to upload a file and then changed the contents of this file at the TFTP server, the device will not recognize that the file has changed (because the file name is the same).

Since audio files are stored in non-volatile memory, if autoprovisioning is disabled after they have been loaded to the board, the audio file settings will not change. You can force a change to the audio files on the board by clicking **Restore Default** on the **Audio Configuration** page or by changing the autoprovisioning file with “**default**” set as the file name.

2.5.12.2 Sample dhcpd.conf

```
#
# Sample configuration file for ISC dhcpd for Debian
#

ddns-update-style none;

option domain-name "voiplab";
option domain-name-servers 10.0.0.252;
option option-150 code 150 = ip-address;
option ntp-servers north-america.pool.ntp.org;
option space VendorInfo;
option VendorInfo.text code 10 = { text };
authoritative;
log-facility local7;

subnet 10.0.0.0 netmask 255.0.0.0 {
    max-lease-time 3600;
    default-lease-time 3600;

    option routers                  10.0.0.1;
    option subnet-mask              255.0.0.0;

    option domain-name              "voiplab";
    option domain-name-servers      10.0.0.252;

    option time-offset              -8;             # Pacific Standard Time

#     option www-server               99.99.99.99;                    # OPTION 72

#     option tftp-server-name          "10.0.1.52";                   # OPTION 66
#     option tftp-server-name          "http://test.cyberdata.net";   # OPTION 66

#     option option-150                10.0.0.252;                    # OPTION 150

# These two lines are needed for option 43
#     vendor-option-space VendorInfo;                                 # OPTION 43
#     option VendorInfo.text "http://test.cyberdata.net";             # OPTION 43

    range 10.10.0.1 10.10.2.1; }
```

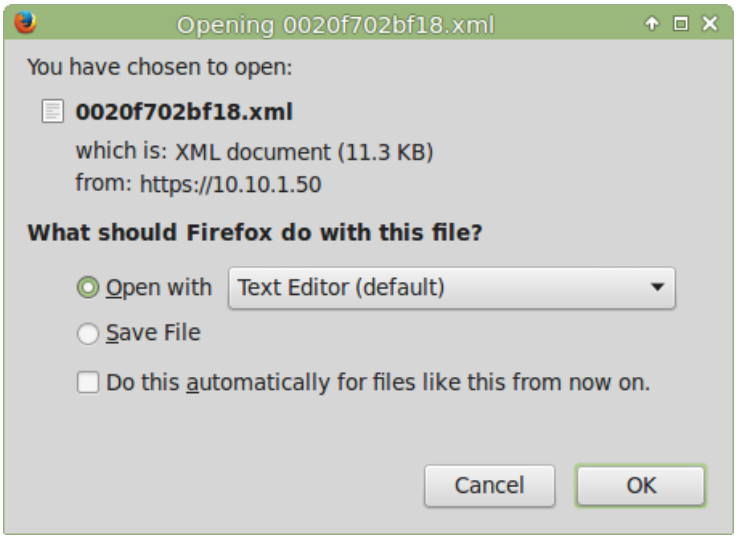
2.5.12.3 Get Autoprovisioning Template Button

The **Get Autoprovisioning Template** button allows the user to generate, download, edit, and then store an autoprovisioning template on the server that serves the autoprovisioning files for devices.

To generate an autoprovisioning template directly from the device, complete the following steps:

1. On the **Autoprovisioning** page, click on the **Get Autoprovisioning Template** button.
2. You will see a window prompting you to save a configuration file (**.xml**) to a location on your computer (Figure 2-31). The configuration file is the basis for the default configuration settings for your unit).
3. Choose a location to save the configuration file and click on **OK**. See Figure 2-31.

Figure 2-31. Configuration File



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

2.6 Upgrade the Firmware

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

To upgrade the firmware of your device:

1. Download the latest firmware file from the **Downloads** tab at the following webpage:

   https://www.cyberdata.net/products/011230

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

- Firmware file
- Release notes
- Autoprovisioning template

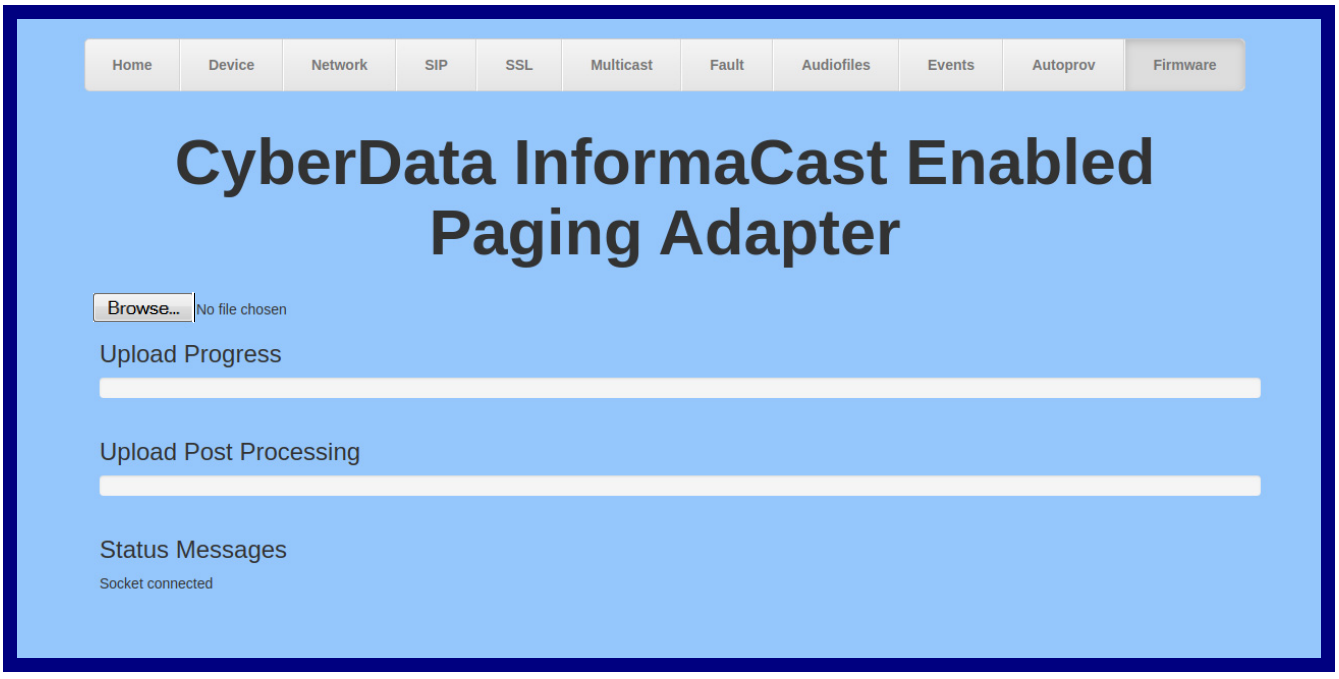
3. Log in to the **Home** page as instructed in Section 2.5.3, "Log in to the Configuration GUI".

4. Click on the **Firmware** menu button to open the **Firmware** page (Figure 2-32).

Caution

Equipment Hazard: CyberData strongly recommends that you first reboot the device before attempting to upgrade the firmware of the device. See Section 2.6, "Upgrade the Firmware".

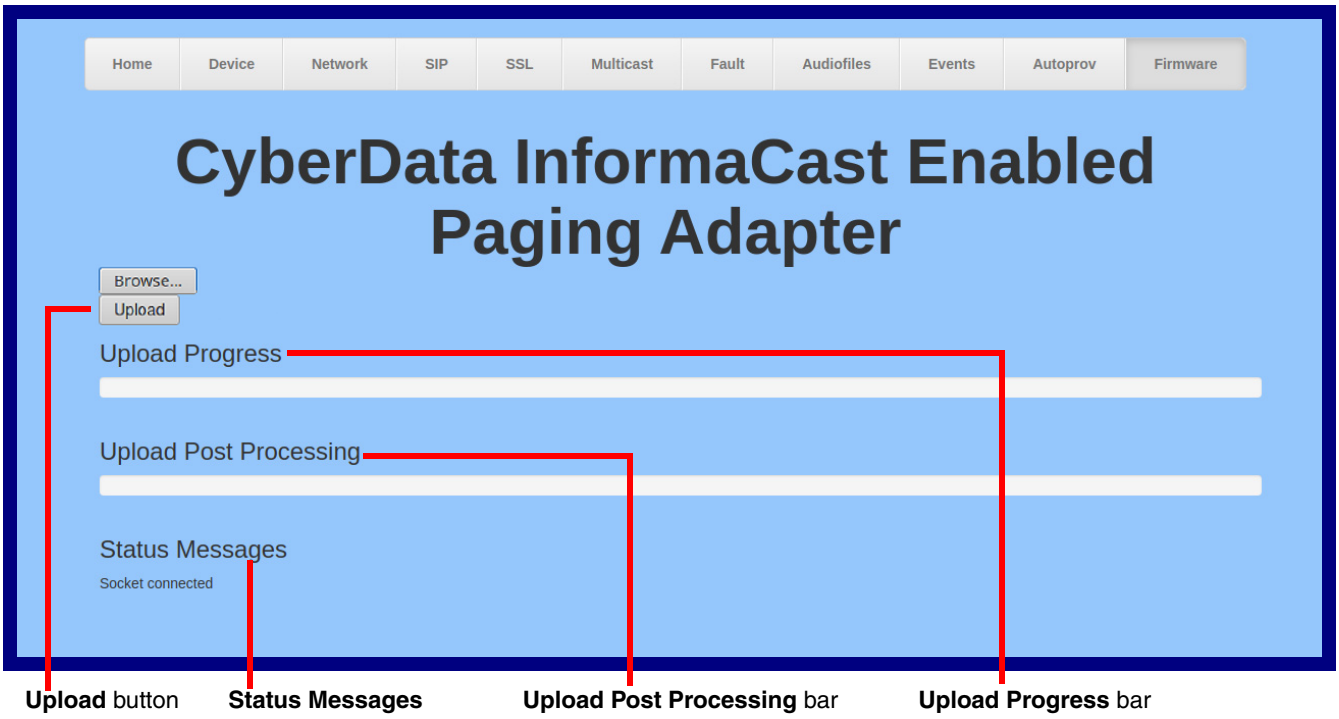
Figure 2-32. Firmware Page



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

6. Select the firmware file. This reveals the **Upload** button (Figure 2-33).

Figure 2-33. Upload Button



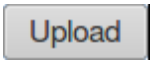
7. Click on the **Upload** button. After selecting the **Upload** button, you will see the progress of the upload in the **Upload Progress** bar.
8. When the upload is complete, you will see the words **Upload finished** under **Status Messages**.
9. At this point, you will see the progress of the upload's post processing in the **Upload Post Processing** bar.

Note Do not reboot the device before the upgrading process is complete.

10. When the process is complete, you will see the words **SWUPDATE Successful** under **Status Messages**.
11. The device will reboot automatically.
12. The **Home** page will display the version number of the firmware and indicate which boot partition is active.

Table 2-16 shows the web page items on the **Firmware** page.

Table 2-16. Firmware Page Parameters

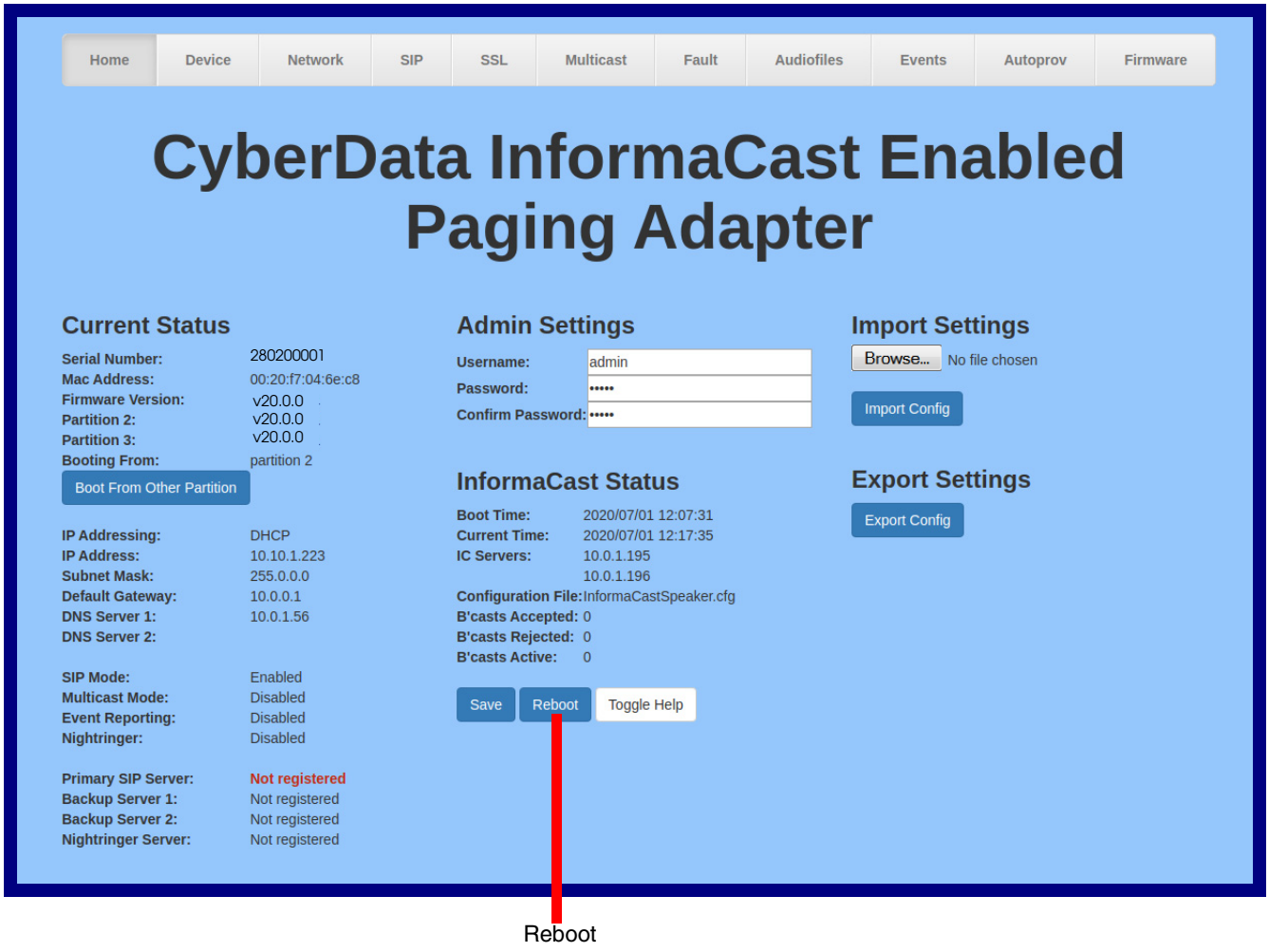
Web Page Item	Description
	Use the **Browse** button to navigate to the location of the firmware file that you want to upload.
	Click on the **Upload** button to automatically upload the selected firmware and reboot the system. **Note**: This button only appears after the user has selected a firmware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

2.6.1 Reboot the InformaCast Enabled Paging Adapter

To reboot a InformaCast Enabled Paging Adapter, log in to the web page as instructed in Section 2.5.3, "Log in to the Configuration GUI".

1. Click **Reboot** (Figure 2-34). A normal restart will occur.

Figure 2-34. Home Page



2.7 Command Interface

Some functions on the device can be activated using simple POST commands to the web interface. The examples in Table 2-17 use the free unix utility, **wget commands**. However, any program that can send HTTP POST commands to the device should work.

2.7.1 Command Interface Post Commands

The commands in Table 2-17 require an authenticated session (a valid username and password to work).

Table 2-17. 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.

2.8 Identifying and Testing a Device when Using InformaCast 4.0 or Later

This section describes the basic process for identifying and testing the CyberData device when using Singlewire's InformaCast software version 4.0 or later.

Note If you have questions or need help, please consult your InformaCast documentation and or contact the CyberData support team.

Note CyberData's support is limited to IP endpoint functionality when used with an InformaCast system.

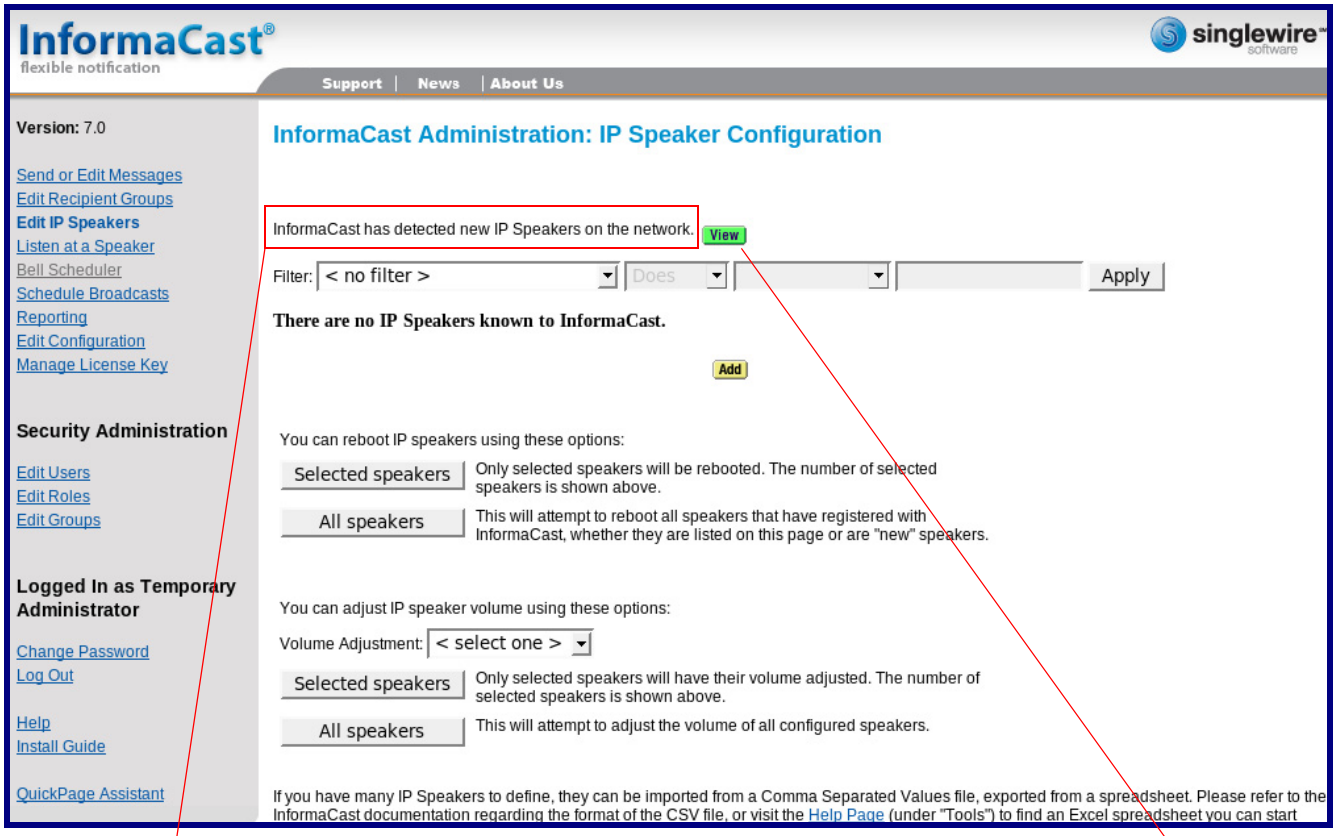
To add the InformaCast Enabled Paging Adapter to the InformaCast server:

1. Click **Edit IP Speakers** on the **Main Screen** of the **Singlewire Informacast Server Web Interface**.

Figure 2-35. Main Screen of the Singlewire InformaCast Server Web Interface

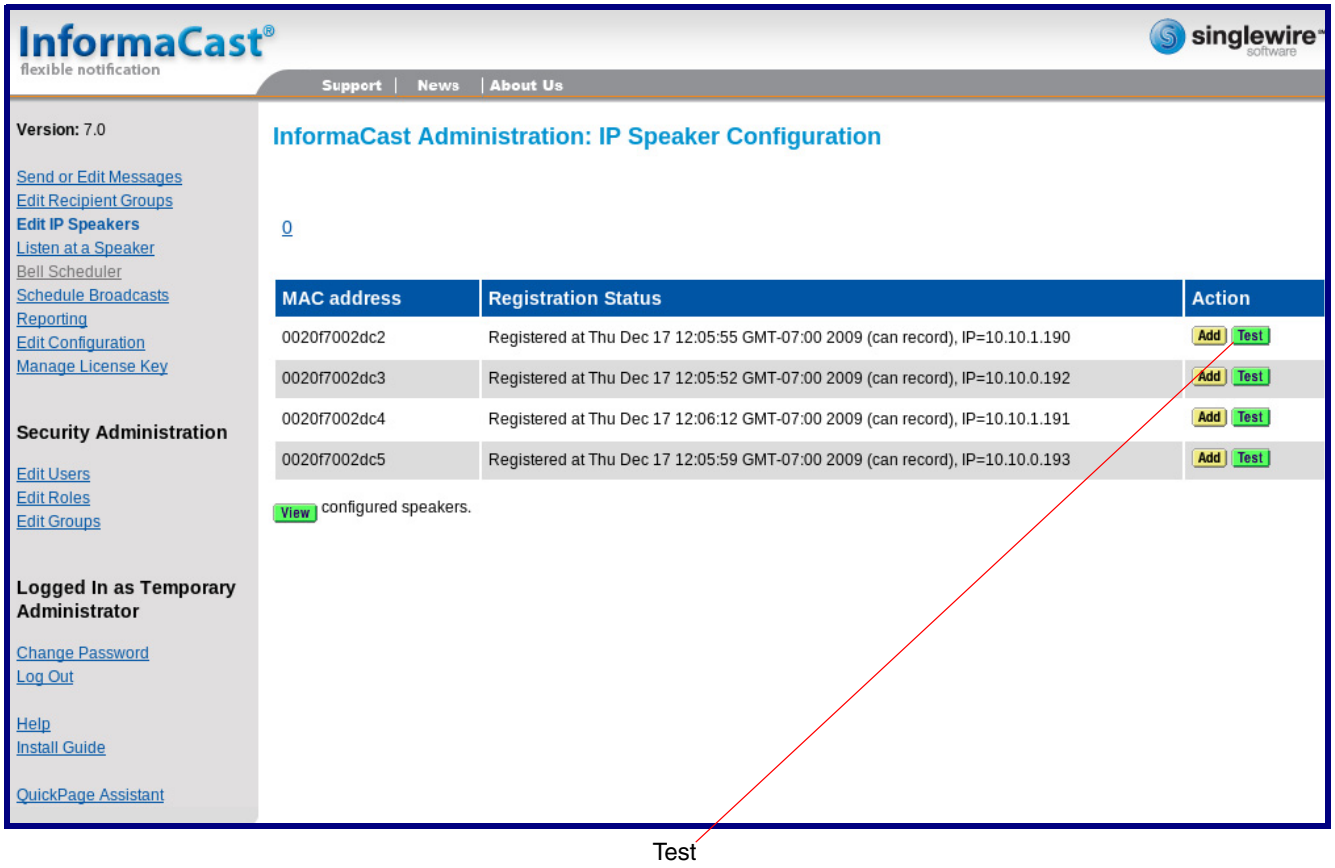
2. On the **IP Speaker Configuration** page, InformaCast will indicate that it has detected new speakers. Click **View**.

Figure 2-36. IP Speaker Configuration Page



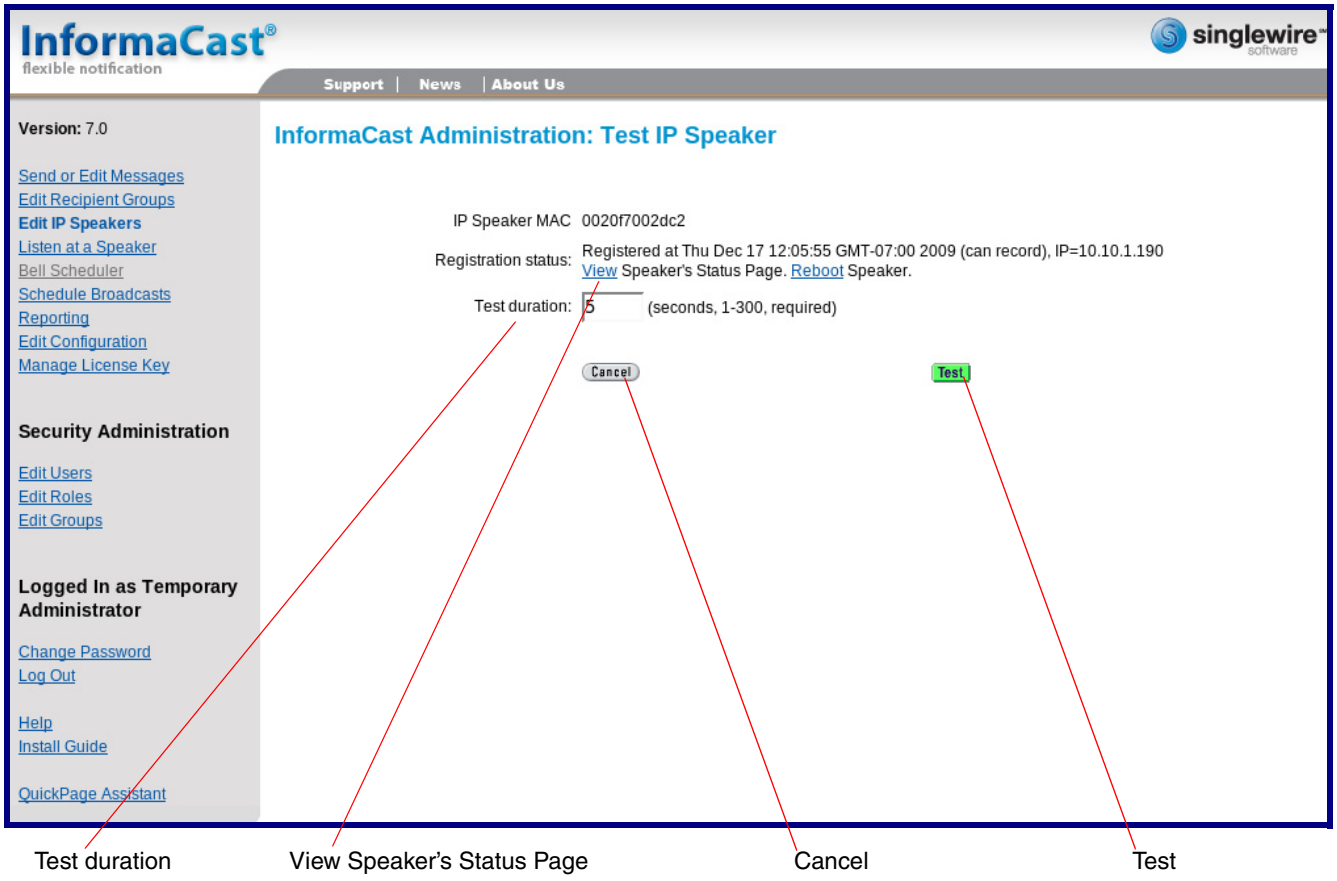
3. The **IP Speaker Configuration** page will show four newly detected speakers. Click **Test**.

Figure 2-37. IP Speaker Configuration Page



4. On the **Test IP Speaker** page, Enter a number into the **Test duration** field.
5. Click **Test**.
6. You will hear a tone from the speaker being testing.
7. After the test, click **Cancel** to return to the **IP Configuration** page.

Figure 2-38. Test IP Speaker Page



Note When viewing the device's status page via Informacast, Informacast links to the wrong port and path.

Informacast expects our device's status page to be at:

http://<ipaddr>:10004/status.

The status page is actually at:

http://<ipaddr>/ (port 80)

Therefore, if a user clicks the link to view the status page and is directed to:

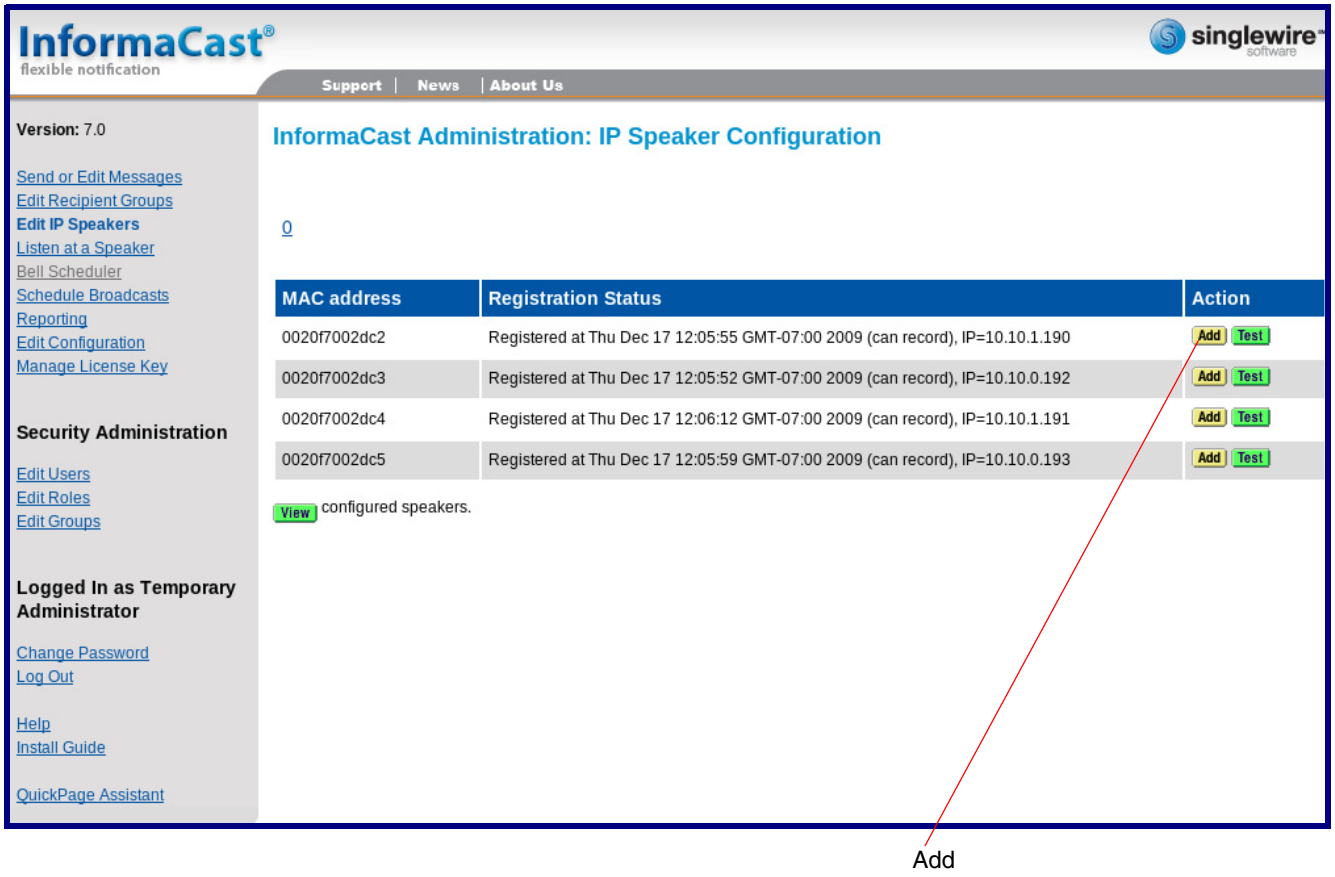
http://10.10.10.10:1004/status

The user will need to edit the url in the address bar to:

http://10.10.10.10/

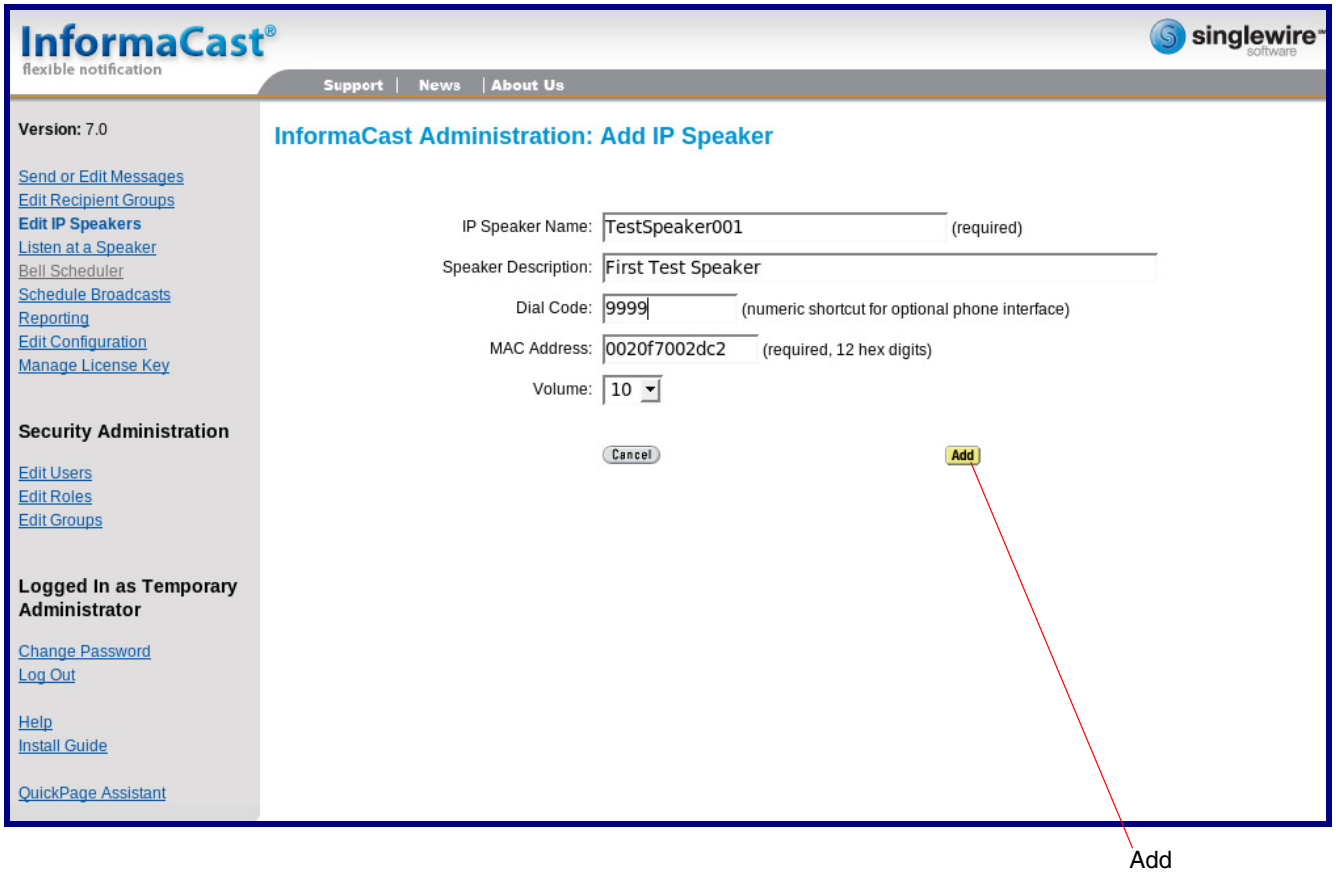
8. On the **IP Speaker Configuration** page, Click **Add** to add a speaker to the InformaCast server.

Figure 2-39. IP Configuration Page



9. On the **Add IP Speaker** page, Fill out appropriate fields and click **Add**.

Figure 2-40. Add IP Speaker Page



Your device is now registered to the InformaCast server. You now can configure this device as part of the InformaCast system setup as required.

Appendix A: Setting up a TFTP Server

A.1 In a LINUX Environment

To set up a TFTP server on LINUX:

1. Create a directory dedicated to the TFTP server, and move the files to be uploaded to that directory.
2. Run the following command where `/tftpboot/` is the path to the directory you created in Step 1: the directory that contains the files to be uploaded. For example:

   ```
   in.tftpd -l -s /tftpboot/your_directory_name
   ```

A.2 In a Windows Environment

You can find several options online for setting up a Windows TFTP server. This example explains how to use the Solarwinds freeware TFTP server, which you can download at:

http://www.cyberdata.net/support/voip/solarwinds.html

To set up a TFTP server on Windows:

1. Install and start the software.
2. Select **File**/**Configure**/**Security** tab/**Transmit Only**.
3. Make a note of the default directory name, and then move the firmware files to be uploaded to that directory.

Appendix B: Troubleshooting/Technical Support

B.1 Frequently Asked Questions (FAQ)

To see a list of frequently asked questions for your product, click on the **FAQs** tab at the following webpage:

https://www.cyberdata.net/products/011280

B.2 Documentation

The documentation for this product is released in an English language version only.

To download PDF copies of CyberData product documentation, click on the **Downloads** tab at the following webpage:

https://www.cyberdata.net/products/011280

B.3 Contact Information

Contact

CyberData Corporation
3 Justin Court
Monterey, CA 93940 USA
www.CyberData.net
Phone: 800-CYBERDATA (800-292-3732)
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:

http://support.cyberdata.net/

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

Phone: (831) 373-2601, Extension 333

B.4 Warranty and RMA Information

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

http://support.cyberdata.net/

Index

Symbols

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W