CyberData
The IP Endpoint Company

SIP Paging Zone Controller with 4-Port Audio Out Operations Guide

Part #*011171*

Document Part #*931216C*
for Firmware Version *11.6.1*

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

Operations Guide 931216C
SiP Compliant 011171

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 History

Revision 931216C, which corresponds to firmware version 11.6.1, was released on January 2, 2020, and has the following changes:

- Updates Section 1.2, “Product Features”
- Updates Section 1.4, “Specifications”

Contents

Chapter 1 Product Overview 1

1.1 How to Identify this Product 1
1.2 Product Features 2
1.3 Supported Protocols 2
1.4 Specifications 3

Chapter 2 Implementing the SIP Paging Zone Controller with 4-Port Audio Out 4

2.1 Parts List 4
2.2 Typical Installation 5
2.3 Setting up the SIP Paging Zone Controller 6
2.3.1 Cables Used for Connecting to Legacy Analog Amplifiers 6
2.3.2 Connect to the Power Source 6
Poe 6
Non-Poe 6
Chassis Ground 6
2.3.3 Connect to the Network 7
2.3.4 Confirm that the SIP Paging Zone Controller is Up and Running 8
Confirm Power on, Network Connectivity, and Connection Speed 8
2.3.5 Restore the Factory Default Settings as Required 9
2.4 Configuring the SIP Paging Zone Controller 10
2.4.1 Gather the Required Configuration Information 10
Static or DHCP Addressing? 10
Username and Password for Configuration GUI 10
SIP Settings 10
2.4.2 SIP Paging Zone Controller Web Page Navigation 11
2.4.3 Using the Toggle Help Button 12
2.4.4 Log in to the Configuration Home Page 14
2.4.5 Configure the Device Parameters 18
Time Zone Strings 21
2.4.6 Configure the Network Parameters 24
2.4.7 Configure the SIP Parameters 27
Point-to-Point Configuration 32
2.4.8 Configure the Zone Parameters 33
Operating the SIP Paging Zone Controller 34
Configuring the Multicast Parameters 35
2.4.9 Configure the Audio Parameters 36
User-created Audio Files 41
2.4.10 Configure the Event Parameters 44
Example Packets for Events 46
2.4.11 Configure the Autoprovisioning Parameters 49
Autoprovisioning 51
Sample dhcpd.conf 59
Get Autoprovisioning Template Button 60
2.5 Upgrading the Firmware 61
2.5.1 Upgrade the Firmware 61
2.5.2 Reboot the Device 63

Mounting the SIP Paging Zone Controller 64

A.1 Mount the SIP Paging Zone Controller 64

A.1.1 Mounting Components 64
A.1.2 Mounting Procedure 65

Appendix A Setting Up a TFTP Server 66
A.1 Set up a TFTP Server 66
A.1.1 In a LINUX Environment 66
A.1.2 In a Windows Environment 66

Appendix B Troubleshooting/Technical Support 67
B.1 Frequently Asked Questions (FAQ) 67
B.2 Documentation 67
B.3 Contact Information 68
B.4 Warranty and RMA Information 68

Index 69

1 Product Overview

The CyberData SIP Paging Zone Controller with 4-Port Audio Out with Audio-Out enables access to existing paging speakers through a VoIP phone system. The interface is designed to use a standard paging amplifier with audio inputs and supports paging up to 15 zone groups from a VoIP phone.

The SIP Paging Zone Controller is a PoE-enabled, single SIP-endpoint, enabling user-defined paging zones through RCA line level output connections to legacy analog amplifiers to existing legacy analog speakers.

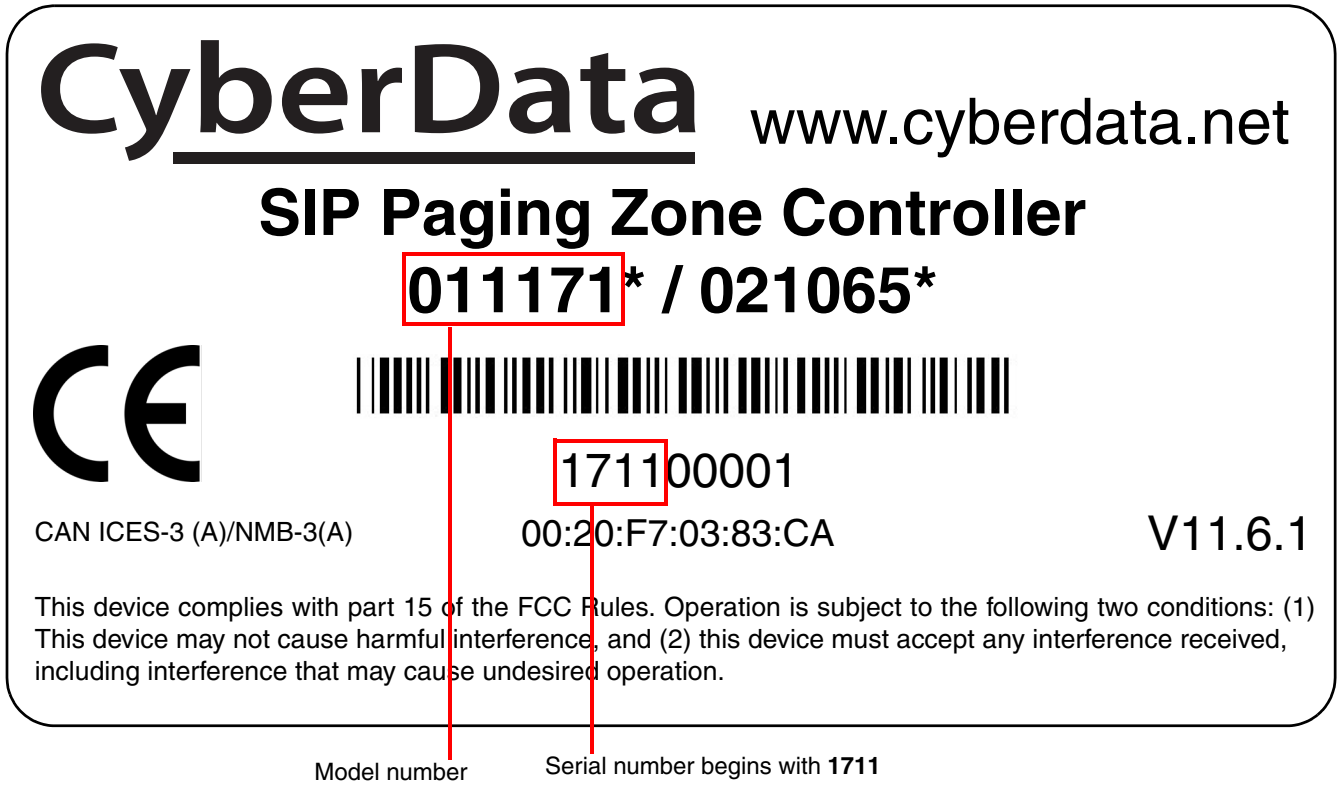
SIP compliant IP-PBX's can now interface with existing legacy analog paging speaker installations.

1.1 How to Identify this Product

To identify the SIP Paging Zone Controller, 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 **011171**.
- The serial number on the label should begin with **1711**.

Figure 1-1. Model Number Label



1.2 Product Features

- Can launch one of 9 uploadable audio messages
- Delayed paging
- Loud ringer - second SIP extension
- 4 Paging zones
- 15 Paging zone groups
- Page all
- Web-based configuration
- Web-based firmware upgradeable
- Connector for external power supply
- Small footprint
- Rack mountable

1.3 Supported Protocols

- HTTP Web-based configuration
- Provides an intuitive GUI for easy system configuration and verification of speaker operations.
- DHCP Client
- TFTP Client
- Audio Codec
- G.711
- DTMF detection

1.4 Specifications

Table 1-1. Specifications

Specifications	
Ethernet I/F	10/100 Mbps
Protocol	SIP RFC 3261 Compatible
Power Input	PoE 802.3af or 48 VDC (not included)
Line Out:	
Output Signal Amplitudes	2.0 VPP maximum
Output Level	+2dBm nominal
Total Harmonic Distortion	0.5% maximum
Output Impedance	10k Ohm
Payload Types	G.711 a-law, G.711µ-law
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]	6.2 inches [157.48 mm] Length
	4.5 inches [114.30 mm] Width
	1.22 inches [30.98 mm] Height
Weight	1.08 lbs. [0.49 kg]
Boxed Weight	1.37 lbs. [0.62 kg]
Warranty	2 Years Limited
Part Number	011171

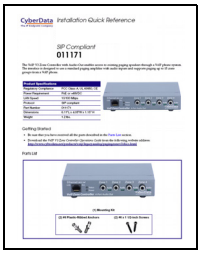
a. Dimensions are measured from the perspective of the product being upright with the front of the product facing you.

2 Implementing the SIP Paging Zone Controller with 4-Port Audio Out

2.1 Parts List

The packaging for the SIP Paging Zone Controller includes the parts in this illustration.

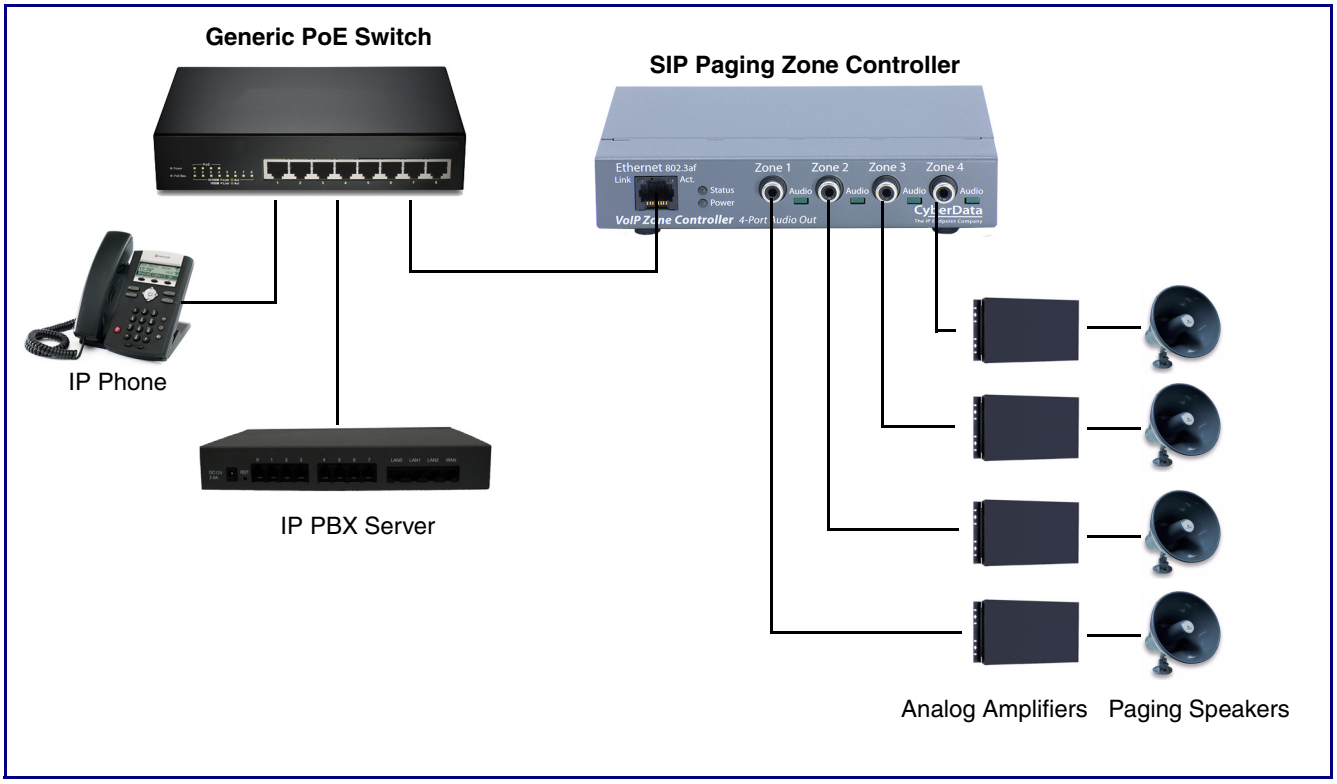
Table 2-2. Parts List

Quantity	Part Name	Illustration
1	SIP Paging Zone Controller with 4-Port Audio Out	
1	Installation Quick Reference Guide	
1	Mounting Kit	

2.2 Typical Installation

Figure 2-1 illustrates how the SIP Paging Zone Controller is normally installed as part of a paging system.

Figure 2-1. Typical Installation



2.3 Setting up the SIP Paging Zone Controller

Before you set up the SIP Paging Zone Controller, be sure that you have received all the parts described in Section 2.1, "Parts List".

2.3.1 Cables Used for Connecting to Legacy Analog Amplifiers

The VoIP Zone Controller connects to zones through RCA line level output connections to legacy analog amplifiers to existing legacy analog speakers.

2.3.2 Connect to the Power Source

Figure 2-2. Connecting to the Power Source

PoE

Non PoE (with 48 VDC power supply)

Chassis Ground

Chassis Ground

To set up the SIP Paging Zone Controller, connect the device to your network:

Poe

- For **PoE**, plug one end of an 802.3af Ethernet cable into the SIP Paging Zone Controller 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 SIP Paging Zone Controller to a **48VDC power supply**. See the figure on the left.

Chassis Ground

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

2.3.3 Connect to the Network

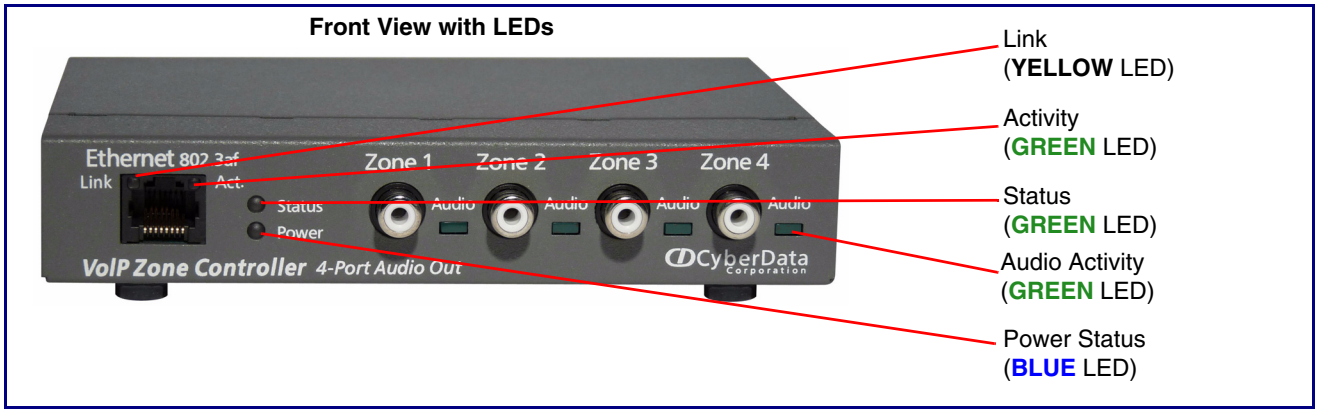
Plug one end of a standard Ethernet cable into the SIP Paging Zone Controller **Ethernet** port. Plug the other end into your network.

Figure 2-3. Connecting to the Network

2.3.4 Confirm that the SIP Paging Zone Controller is Up and Running

The indicator LEDs on the front of the SIP Paging Zone Controller verify the unit's operations.

Figure 2-4. SIP Paging Zone Controller Indicator LEDs



2.3.4.1 Confirm Power on, Network Connectivity, and Connection Speed

When you plug in the Ethernet cable or power supply:

- The round, **BLUE Power Status** LED on the front of the SIP Paging Zone Controller comes on indicating that the power is on.
- The square, **YELLOW Link** LED above the Ethernet port indicates that the network connection has been established. The **Link** LED changes color to confirm the auto-negotiated connection speed:
  - This LED is **YELLOW** at 10 Mbps.
  - This LED is **ORANGE** at 100 Mbps.
- The square, **GREEN Activity** LED above the Ethernet port blinks when there is network activity.
- The round, **GREEN Status** LED comes on after the device is booted and initialized. This LED blinks when the unit is operational.
- The square, **GREEN Audio Activity** LEDs turn on solid when a Zone is being paged.

2.3.5 Restore the Factory Default Settings as Required

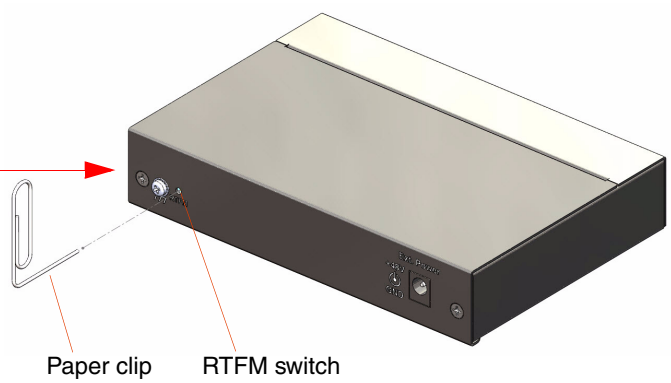
The SIP Paging Zone Controller is delivered with factory set default values for the following parameters. Use the **RTFM** switch (see Figure 2-5) on the back of the unit to restore these parameters to the factory default settings.

Figure 2-5. RTFM Switch

Back View with RTFM Switch

To restore the SIP Paging Zone Controller's factory default settings:

1. Use a paper clip to press and hold the **RTFM** switch while all of the indicator LEDs turn off. See the picture on the right.
2. Continue to press the RTFM switch until after the indicator LEDs turn back on.
3. Release the RTFM switch. All of the SIP Paging Zone Controller settings will be restored to the factory default settings.
4. You will hear the "Restoring defaults..." audio message play through all ports before the device reboots.



Note When you perform the RTFM procedure in Figure 2-5, 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.

2.4 Configuring the SIP Paging Zone Controller

Use this section to configure the SIP Paging Zone Controller.

2.4.1 Gather the Required Configuration Information

Have the following information available before you configure the SIP Paging Zone Controller.

2.4.1.1 Static or DHCP Addressing?

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

- IP Address
- Subnet Mask
- Default Gateway

2.4.1.2 Username and Password for Configuration GUI

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

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

2.4.1.3 SIP Settings

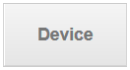
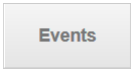
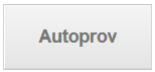
To configure the SIP parameters, determine whether you want to register the SIP Paging Zone Controller. If you do, determine the number of minutes the registration lease remains valid, and whether you want to automatically unregister when you reboot. To configure the SIP parameters, you also need to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

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

2.4.2 SIP Paging Zone Controller Web Page Navigation

Table 2-4 shows the navigation buttons that you will see on every SIP Paging Zone Controller web page.

Table 2-4. Web Page Navigation

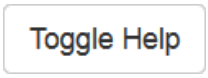
Web Page Item	Description
	Link to the **Home** page.
	Link to the **Device** page.
	Link to the **Network** page.
	Link to go to the **SIP** page.
	Link to the **Zone** page.
	Link to the **Audiofiles** page.
	Link to the **Events** page.
	Link to the **Autoprovisioning** page.
	Link to the **Firmware**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

2.4.3 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:

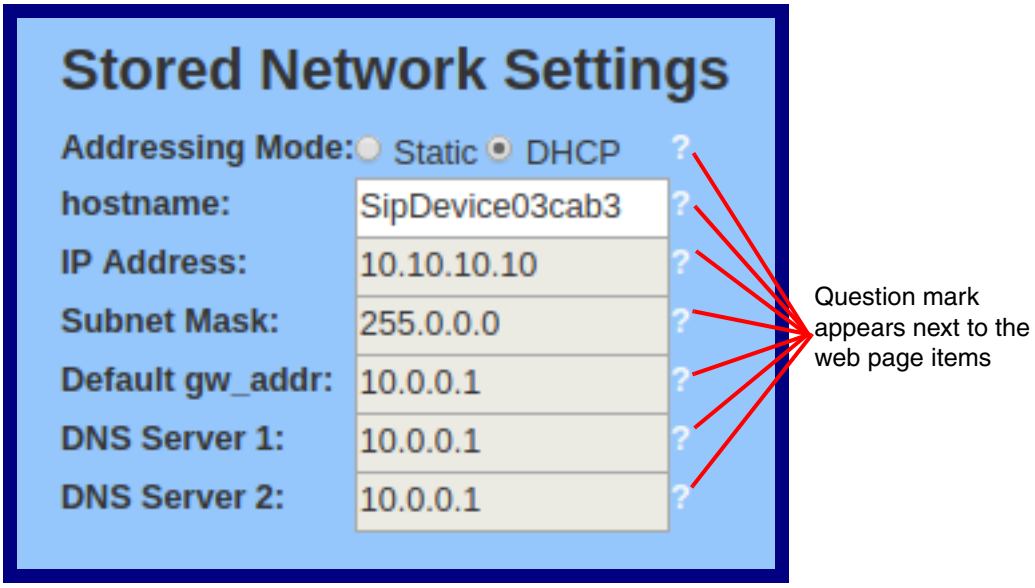
1. Click on the **Toggle Help** button that is on the UI webpage. See Figure 2-6 and Figure 2-7.

Figure 2-6. Toggle/Help Button



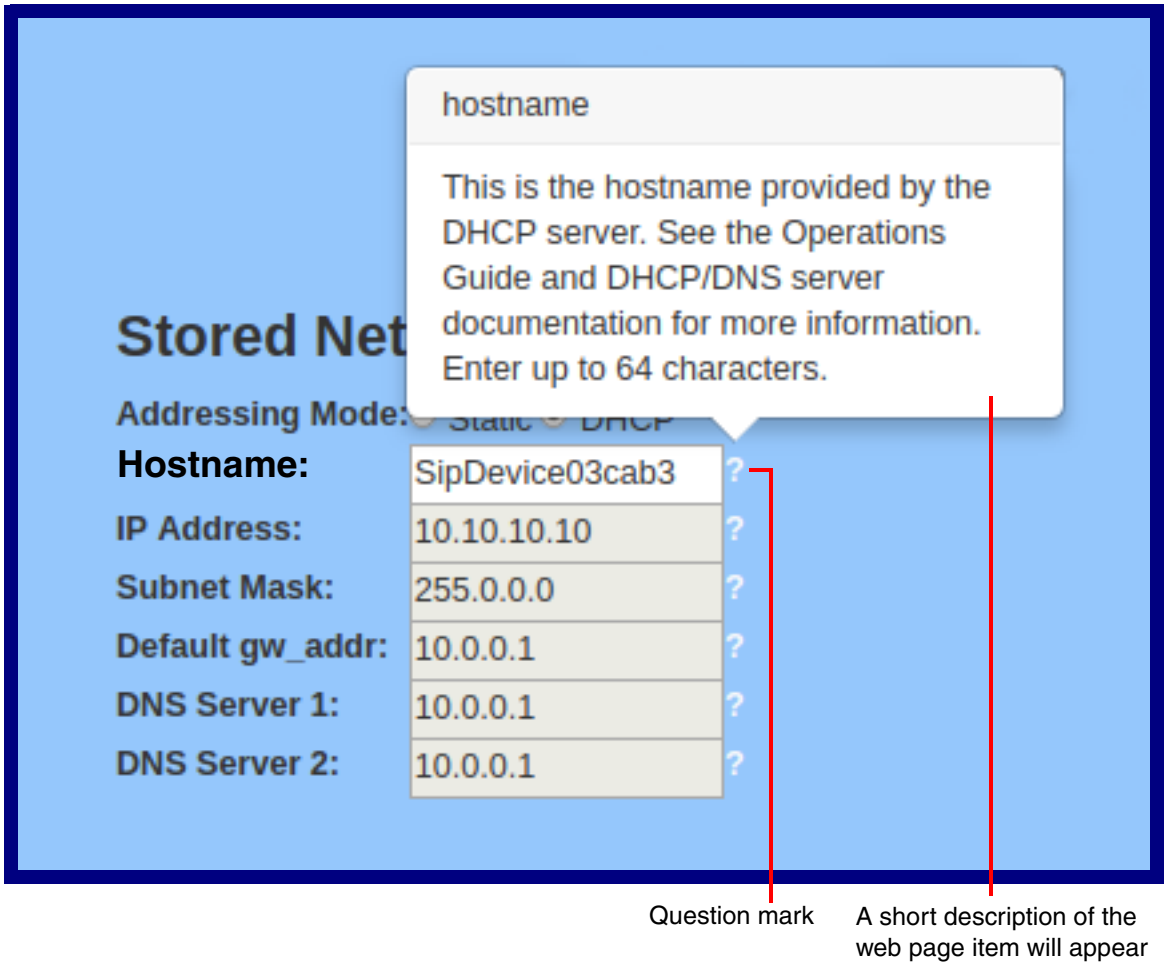
2. You will see a question mark (?) appear next to each web page item that has been provided with a short description by the Help feature. See Figure 2-7.

Figure 2-7. 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 2-8.

Figure 2-8. Short Description Provided by the Help Feature



2.4.4 Log in to the Configuration Home Page

1. Open your browser to the SIP Paging Zone Controller 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 SIP Paging Zone Controller.

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 **Downloads** tab on the following webpage:

https://www.cyberdata.net/products/011171

Note 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 SIP Paging Zone Controller configuration *after* the initial configuration, log in using the IP address you assign to the device. Section 2.4.6, "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 20 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 2-9. Home Page

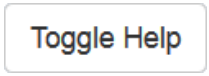
4. On the **Home Page**, review the setup details and navigation buttons described in Table 2-5

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.
Import Settings	
Choose File	Use this button to select a configuration file to import.
Import Config	After selecting a configuration file, click Import to import the configuration from the selected file. Then, click Save and Reboot to store changes.
Export Settings	
Export Config	Click Export to export the current configuration to a file.
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.

Table 2-5. Home Page Overview (continued)

Web Page Item	Description
	Click on the **Reboot** button to reboot the system.
	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 and then the **Reboot** button for the changes to take effect.

At this point you can:

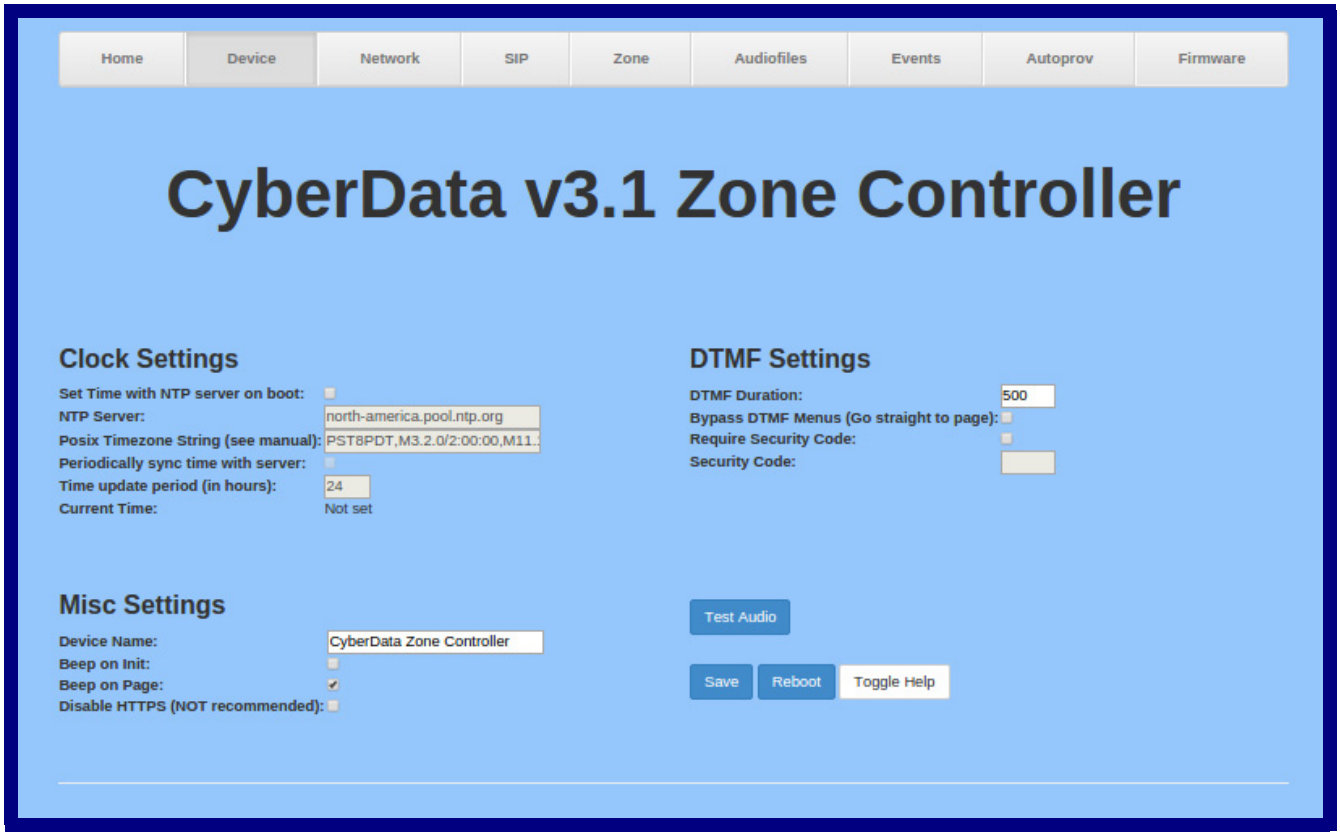
- Review the SIP Paging Zone Controller's **Current Settings**. Use the RTFM switch to restore the factory default settings. See Section 2.3.5, "Restore the Factory Default Settings as Required".
- Configure the device parameters. Click on the **Device** button and see Section 2.4.5, "Configure the Device Parameters" for instructions.
- Configure the network parameters. Click on the **Network** button and see Section 2.4.6, "Configure the Network Parameters" for instructions.
- Configure the SIP parameters. Click on the **SIP** button and see Section 2.4.7, "Configure the SIP Parameters" for instructions.
- Configure the PGROUPS parameters. Click on the **Zone** button and see Section 2.4.8, "Configure the Zone Parameters" for instructions.
- Configure the audio parameters. Click on the **Audiofiles** button and see Section 2.4.9, "Configure the Audio Parameters" for instructions.
- Configure the event parameters. Click on the **Events** button and see Section 2.4.10, "Configure the Event Parameters" for instructions.
- Configure the autoprovisioning parameters. Click on the **Autoprov** button and see Section 2.4.11, "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 2.5, "Upgrading the Firmware" for instructions.

2.4.5 Configure the Device Parameters

1. Click the **Device** button to open the **Device** page. See Figure 2-10.

Figure 2-10. 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
Clock Settings	
Set Time with NTP Server on boot ?	When selected, the time is set with an external NTP server when the device restarts.
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.
Posix Timezone String ?	See Section 2.4.5.1, "Time Zone Strings" for information about how to use the Posix Timezone String to specify time zone and daylight savings time where applicable. Enter up to 63 characters.
Periodically sync time with server ?	When selected, the time is periodically updated with the NTP server at the configured interval below.
Time update period (in hours) ?	The time interval after which the device will contact the NTP server to update the time. Enter up to 4 digits.
Current Time	Allows you to input the current time. (6 character limit)
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.
DTMF Settings	
DTMF Duration ?	The duration, in milliseconds, of DTMF tones played out of the device's analog audio ports (0-65535).
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).
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.
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.

Table 2-6. Device Configuration Parameters (continued)

Web Page Item	Description
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 and then the **Reboot** button for the changes to take effect.

2.4.5.1 Time Zone Strings

The posix time zone string tells the internal date and time utilities how to handle daylight savings time for different time zones. The following table shows some common strings.

Table 2-7. Common Time Zone Strings

Time Zone	Time Zone String
US Pacific time	PST8PDT,M3.2.0/2:00:00,M11.1.0/2:00:00
US Mountain time	MST7MDT,M3.2.0/2:00:00,M11.1.0/2:00:00
US Eastern Time	EST5EDT,M3.2.0/2:00:00,M11.1.0/2:00:00
Phoenix Arizona[a]	MST7
US Central Time	CST6DST,M3.2.0/2:00:00,M11.1.0/2:00:00

a.Phoenix, Arizona does not use daylight savings time.

The following table shows a breakdown of the parts that constitute the following time zone string:

- ***CST6DST,M3.2.0/2:00:00,M11.1.0/2:00:00***

Table 2-8. Time Zone String Parts

Time Zone String Part	Meaning
CST6CDT	The time zone offset from GMT and three character identifiers for the time zone.
CST	Central Standard Time
6	The (hour) offset from GMT/UTC
CDT	Central Daylight Time
M3.2.0/2:00:00	The date and time when daylight savings begins.
M3	The third month (March)
.2	The 2nd occurrence of the day (next item) in the month
.0	Sunday
/2:00:00	Time of day to change
M11.1.0/2:00:00	The date and time when daylight savings ends.
M11	The eleventh month (November)
.1	The 1st occurrence of the day (next item) in the month
.0	Sunday
/2:00:00	Time of day to change

Time Zone String Examples

The following table has some more examples of time zone strings.

Table 2-9. Time Zone String Examples

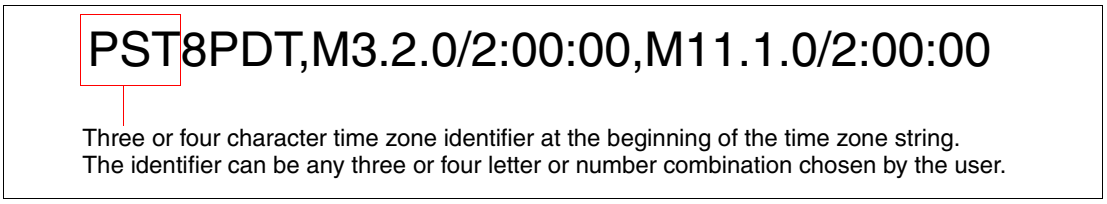
Time Zone	Time Zone String
Tokyo[a]	IST-9
Berlin[b]	CET-1MET,M3.5.0/1:00,M10.5.0/1:00

a.Tokyo does not use daylight savings time.
b.For Berlin, daylight savings time starts on the last Sunday in March at 01:00 UTC, and ends on the last Sunday in October at 01:00 UTC, and is one hour ahead of UTC.

Time Zone Identifier

A user-definable three or four character time zone identifier (such as PST, EDT, IST, MUT, etc) is needed at the beginning of the posix time zone string to properly set the time. However, the specific letters or numbers used for the time zone identifier are not important and can be any three or four letter or number combination that is chosen by the user. However, the time zone identifier cannot be blank.

Figure 2-11. Three or Four Character Time Zone Identifier



You can also use the following URL when a certain time zone applies daylight savings time:

http://www.timeanddate.com/time/dst/2011.html

World GMT Table

The following table has information about the GMT time in various time zones.

Table 2-10. World GMT Table

Time Zone	City or Area Zone Crosses
GMT-12	Eniwetok
GMT-11	Samoa
GMT-10	Hawaii
GMT-9	Alaska
GMT-8	PST, Pacific US
GMT-7	MST, Mountain US
GMT-6	CST, Central US
GMT-5	EST, Eastern US
GMT-4	Atlantic, Canada
GMT-3	Brazilia, Buenos Aries
GMT-2	Mid-Atlantic
GMT-1	Cape Verdes
GMT	Greenwich Mean Time, Dublin

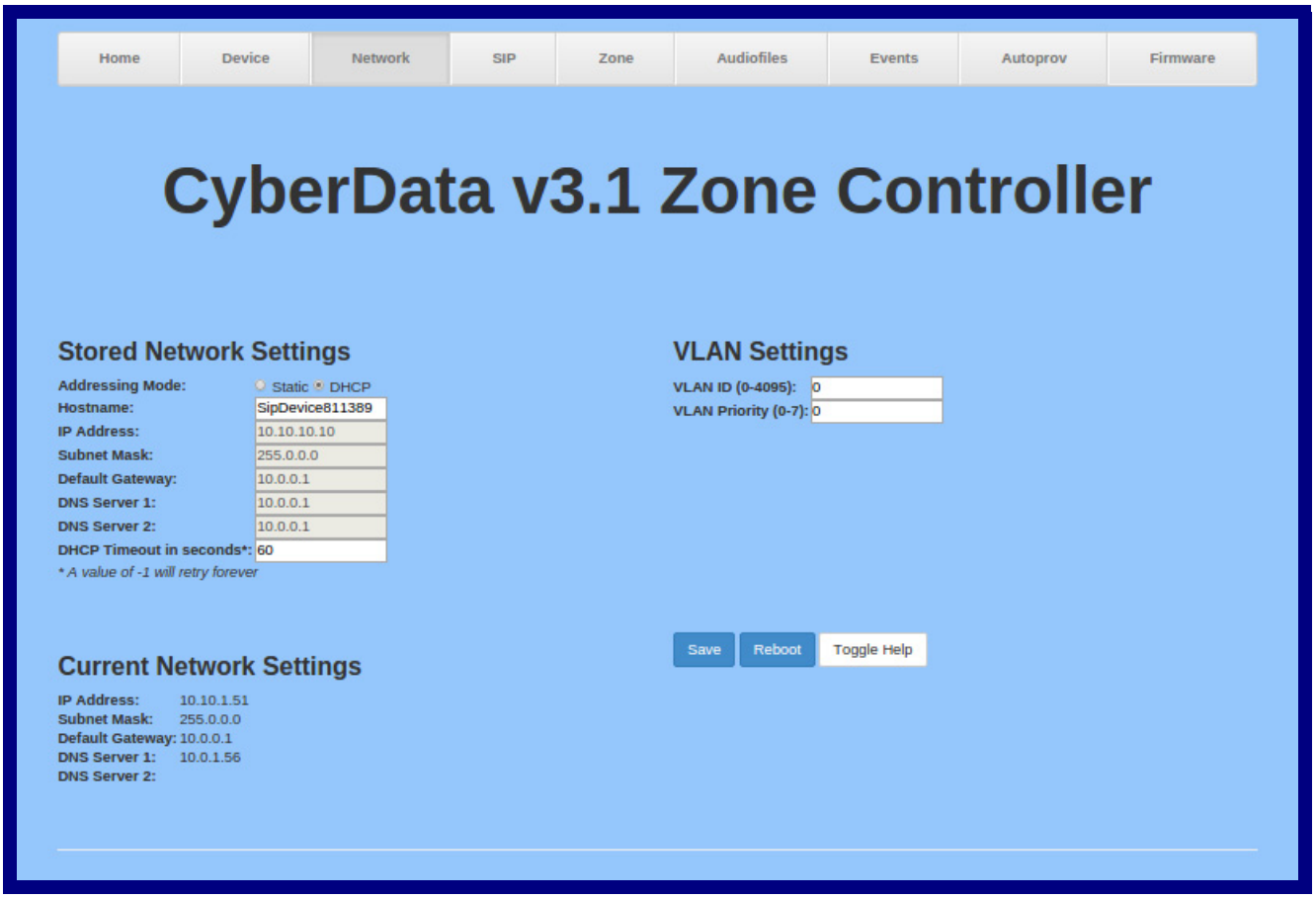
Table 2-10. World GMT Table (continued)

Time Zone	City or Area Zone Crosses
GMT+1	Berlin, Rome
GMT+2	Israel, Cairo
GMT+3	Moscow, Kuwait
GMT+4	Abu Dhabi, Muscat
GMT+5	Islamabad, Karachi
GMT+6	Almaty, Dhaka
GMT+7	Bangkok, Jakarta
GMT+8	Hong Kong, Beijing
GMT+9	Tokyo, Osaka
GMT+10	Sydney, Melbourne, Guam
GMT+11	Magadan, Soloman Is.
GMT+12	Fiji, Wellington, Auckland

2.4.6 Configure the Network Parameters

Configuring the network parameters enables your network to recognize the SIP Paging Zone Controller and communicate with it. Click on the **Network** button on the Home page to open the **Network** page.

Figure 2-12. Network Page



On the **Network** 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. 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 2.3.5, "Restore the Factory Default Settings as Required" 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.
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.
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.

Table 2-11. Network Configuration Parameters (continued)

Web Page Item	Description
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
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 SIP Paging Zone Controller's **IP Address**: The SIP Paging Zone Controller 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.

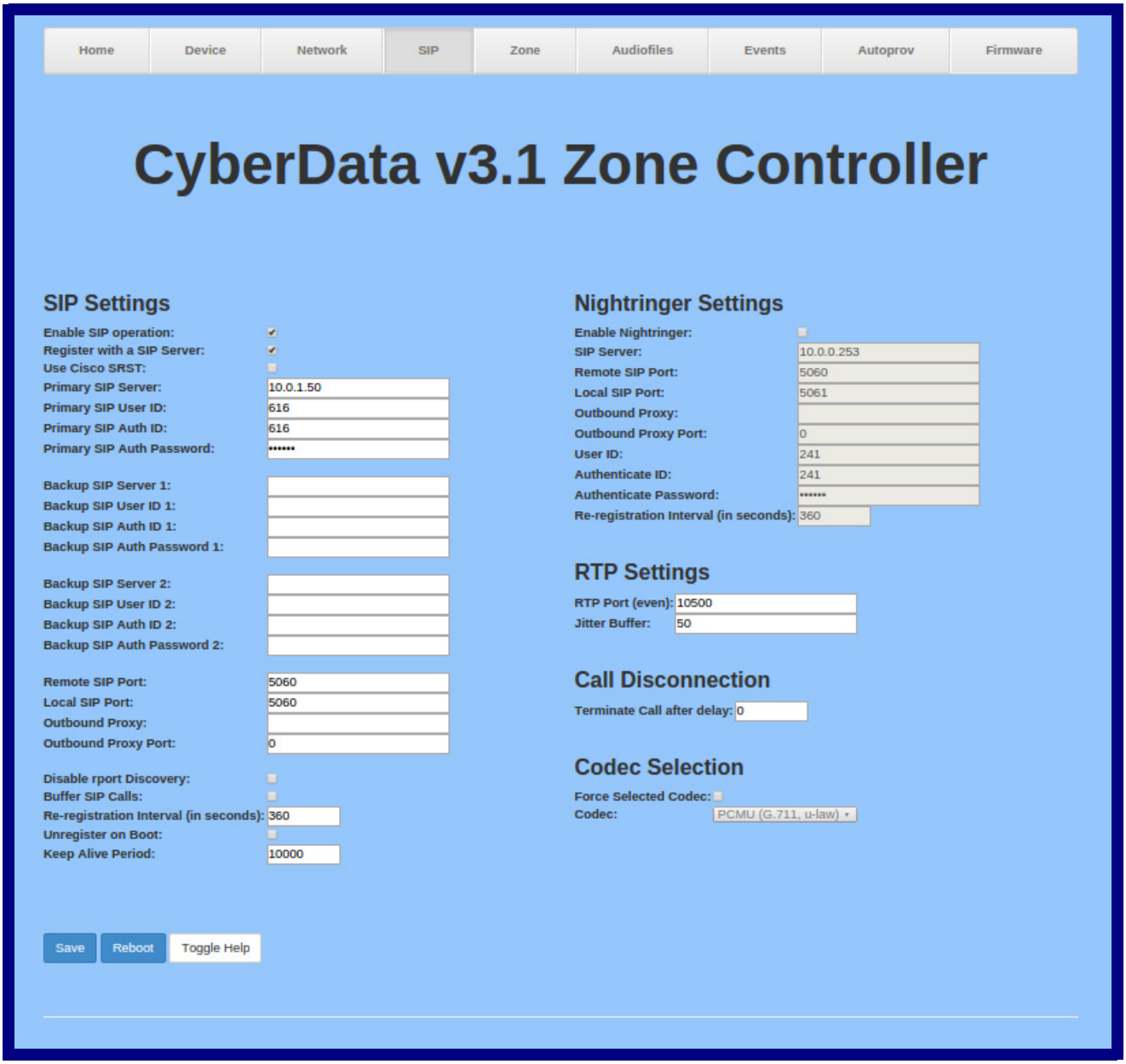
2.4.7 Configure the SIP Parameters

The SIP parameters enable the SIP Paging Zone Controller to contact and register with the SIP server. On the Home page, click on the **SIP** button to open the **SIP** page.

Caution

Nightringer requires SIP Registration. Nightringer cannot be used in peer to peer mode.

Figure 2-13. SIP Page



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

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. 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.
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 2.4.7.1, "Point-to-Point 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.
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.

Table 2-12. SIP Configuration Parameters (continued)

Web Page Item	Description
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.
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.
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.

Table 2-12. SIP Configuration Parameters (continued)

Web Page Item	Description
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.
Relay rings to multicast	When selected, the device will play ring tones to the specified multicast address and port.
Multicast Address	The multicast address used for nightring audio.
Multicast Port	The multicast port used for nightring audio.
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.
Jitter Buffer	Specify the size of the jitter buffer (in milliseconds) used for SIP calls. Valid values are 50-1000.
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), or G.722]. Otherwise, the device will perform codec negotiation using the default list of supported codecs.
Codec	Select desired codec (only one may be chosen).

Table 2-12. SIP Configuration Parameters (continued)

Web Page Item	Description
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
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 and then the **Reboot** 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 SIP Paging Zone Controller when you reboot it.
   b. Select **No** to keep the SIP Paging Zone Controller registered when you reboot it.
6. In the **Register Expiration** field, enter the number of seconds the SIP Paging Zone Controller registration lease remains valid with the SIP Server. The SIP Paging Zone Controller automatically re-registers with the SIP server before the lease expiration timeout.

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

2.4.7.1 Point-to-Point Configuration

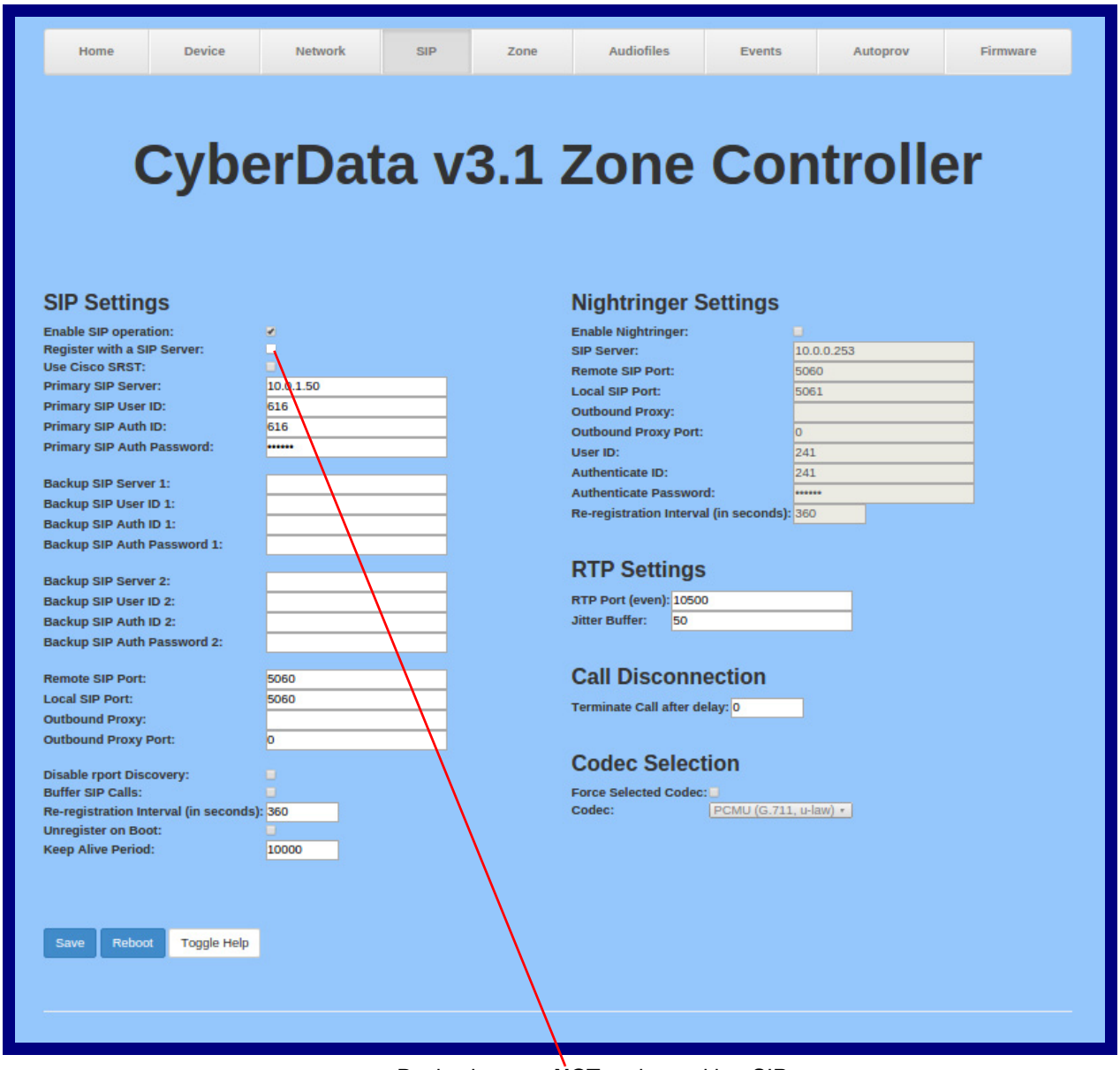
When the board is set to not register with a SIP server, it's possible to set the device to dial out to a single endpoint. To do this, do the following:

1. On the **SIP Configuration** page (Figure 2-14), 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 The delayed DTMF functionality is available in the Point-to-Point Mode.

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

Figure 2-14. SIP Configuration Page Set to Point-to-Point Mode

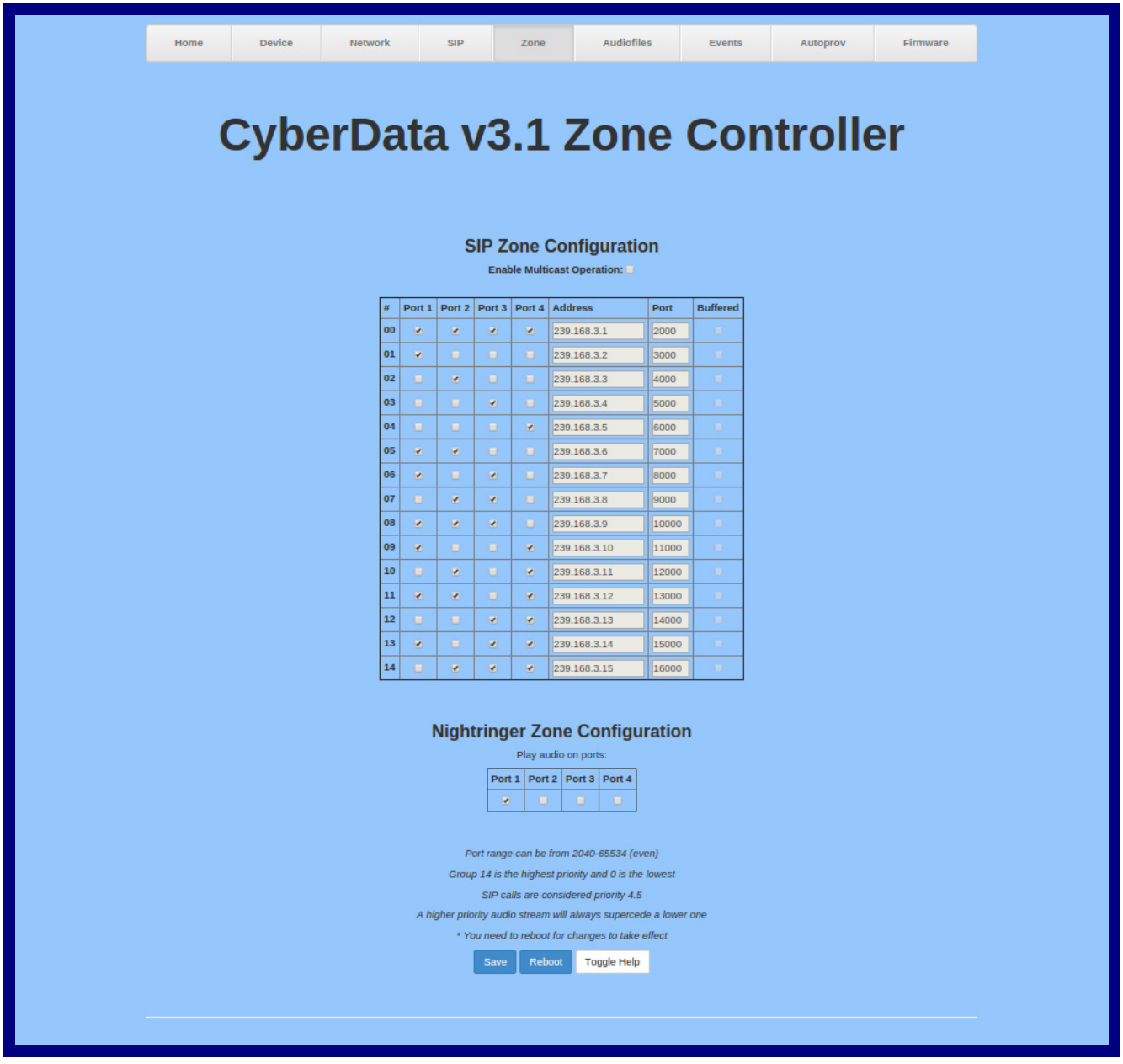


2.4.8 Configure the Zone Parameters

- Each audio output jack on the VoIP Zone Controller represents a port.
- A Zone is comprised of a combination of one or more ports.
- You will need to plug any ports that are used on the VoIP Zone Controller into an analog amplifier. Any speakers attached to the amplifier will be present in the port.

1. Click on the **Zone Config** button to open the **Zone Configuration** page. See Figure 2-15.

Figure 2-15. Zone Configuration Setup



2. On the **Zone Configuration** page, enter values for the parameters indicated in Table 2-13.

Table 2-13. Zone Configuration Parameters

Web Page Item	Description
SIP Zone Configuration	
Enable Multicast Operation	Enables or disables multicast operation. See Section 2.4.8.2, "Configuring the Multicast Parameters"
Zone Number (00 through 14)	Zones are prioritized; multicasts to higher priority zones supercede multicasts to lower priority zones.00 is the lowest priority and 14 is the highest.
Port 1 through **Port 4** Checkboxes	Check the box for the port(s) that comprise the zone.
Address	The IP address at which each zone will listen for a multicast.
Port	The port number at which each zone will listen for a multicast. The port number must be even.
Buffered	Also referred to as delayed paging. When this is enabled, multicast pages to the device will be stored in memory and will play when either the page is terminated or the buffer is full. The receive buffer is 2MB in size, or roughly four minutes of ulaw encoded audio.
Nightringer Zone Configuration	
Play audio on ports **Port 1** through **Port 4** Checkboxes	Check the box for the port(s) that comprise the zone.
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
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.

3. After changing the parameters, click on the **Save** button.
4. Click **Reboot** for the new settings to take effect.

2.4.8.1 Operating the SIP Paging Zone Controller

To operate the SIP Paging Zone Controller:

1. Call to make a page. The SIP Paging Zone Controller will generate a tone over the phone.
2. When you hear this tone, enter the two-digit code for the group that you want to page.
3. If the zone is valid, the SIP Paging Zone Controller will play the user-defined "good zone" sound. Go to Step 4.

Note If the zone is invalid, the SIP Paging Zone Controller will play the user-defined "bad zone" sound. Repeat Step 2.

4. When you hear the "good zone" tone, you can begin speaking.

2.4.8.2 Configuring the Multicast Parameters

The **Multicast** configuration parameters allows the Zone Controller to join up to one paging zone for receiving a ulaw/alaw encoded RTP audio stream. 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. A 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.

2.4.9 Configure the Audio Parameters

Click on the **Audiofiles** button to open the **Audiofiles** page. See Figure 2-16. 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 2-16. Audiofiles Page

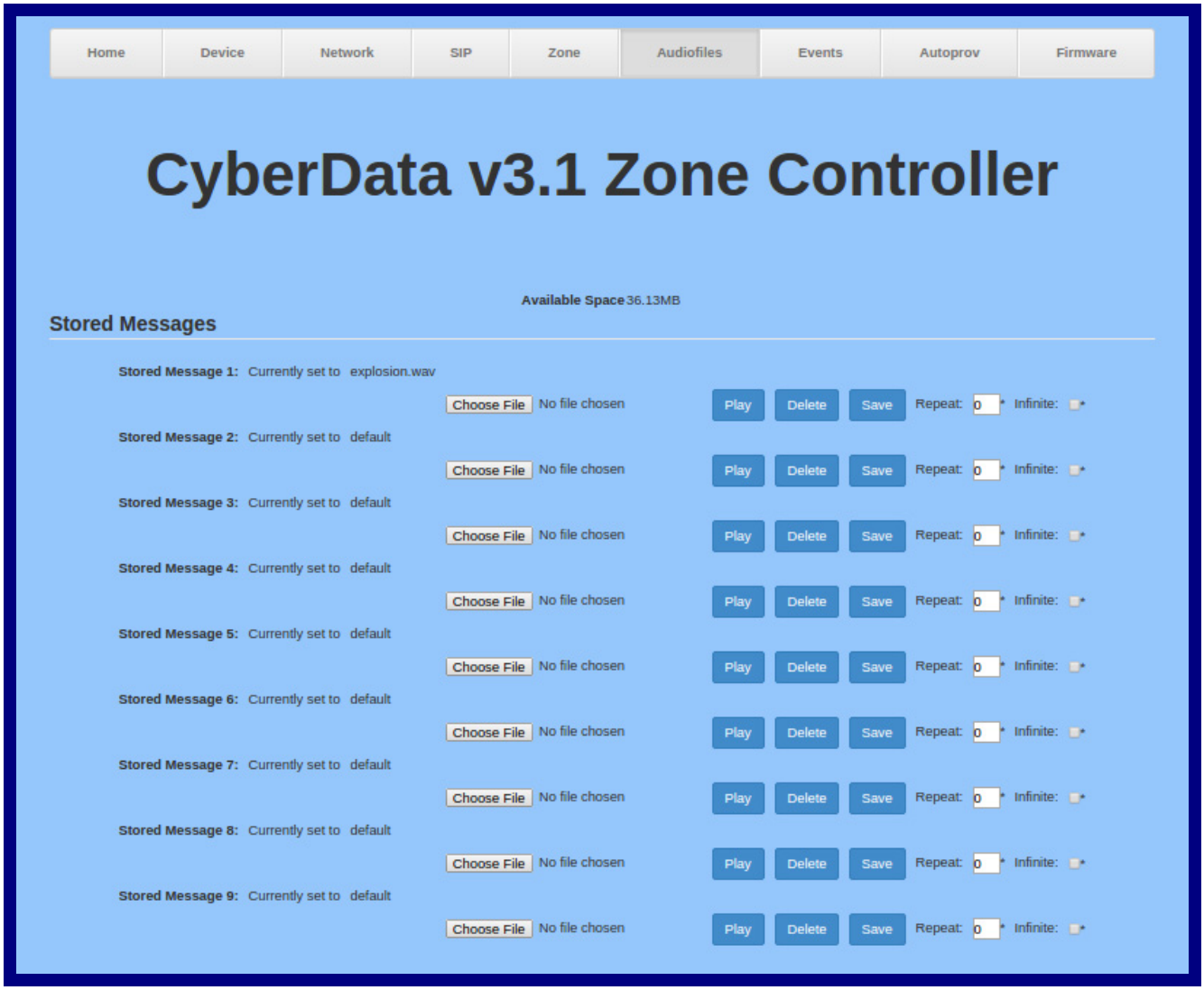


Figure 2-17. Audiofiles Page

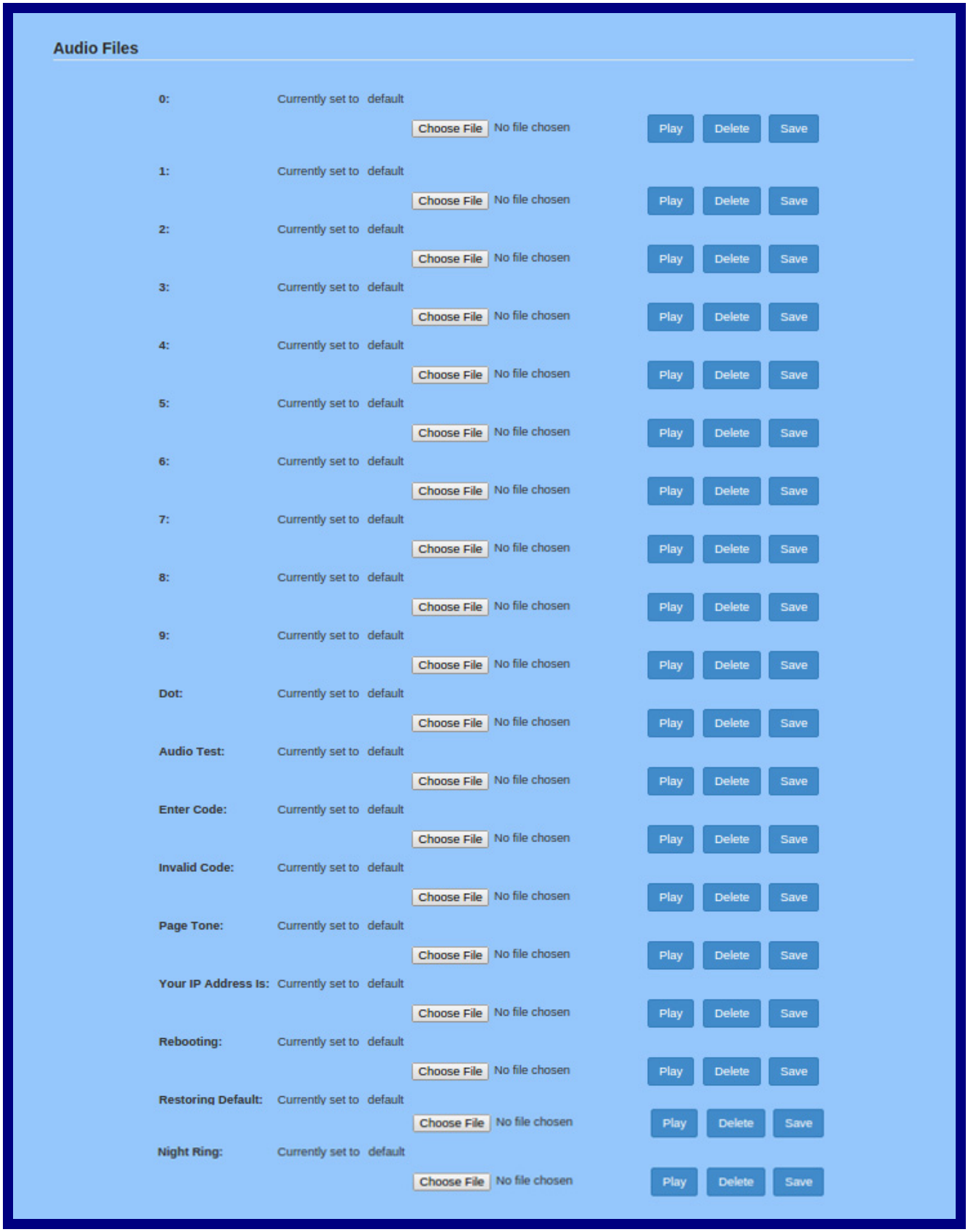


Figure 2-18. Audiofiles Page

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

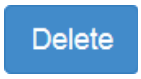
Note Each entry on the **Audiofiles** page replaces one of the stock audio files on the board. When the input box displays the word **default**, the SIP Paging Zone Controller is using the stock audio file. If that file is replaced with a user file, it will display the uploaded filename.

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 2-14. 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 paging zone, 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 2-14. 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).
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).
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).
	Use this button 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 **Choose File** or **Browse** button. The **Save** button will delete any pre-existing user-uploaded audio files.

2.4.9.1 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 2-19 through Figure 2-21.

Figure 2-19. Audacity 1

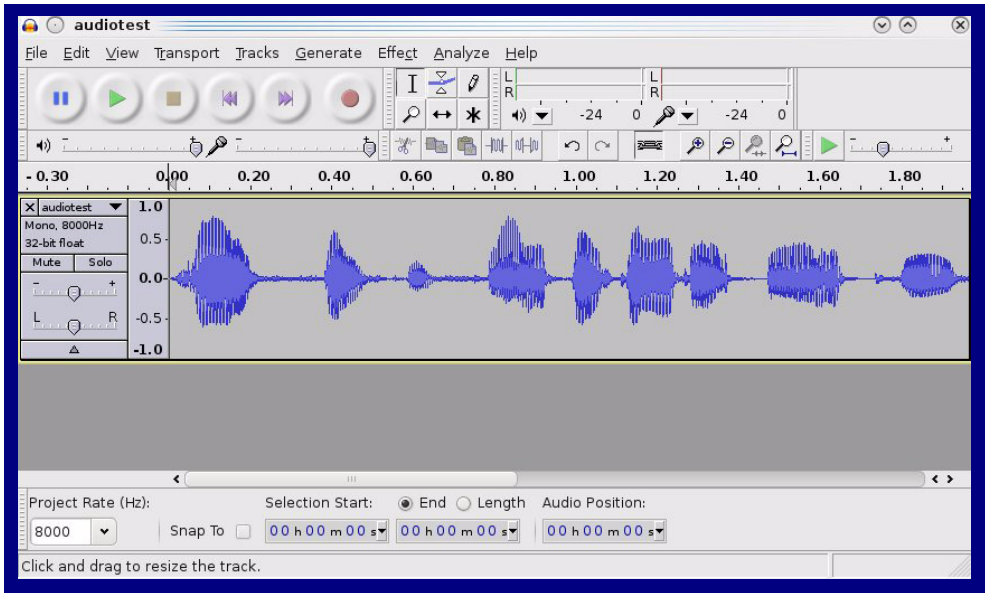
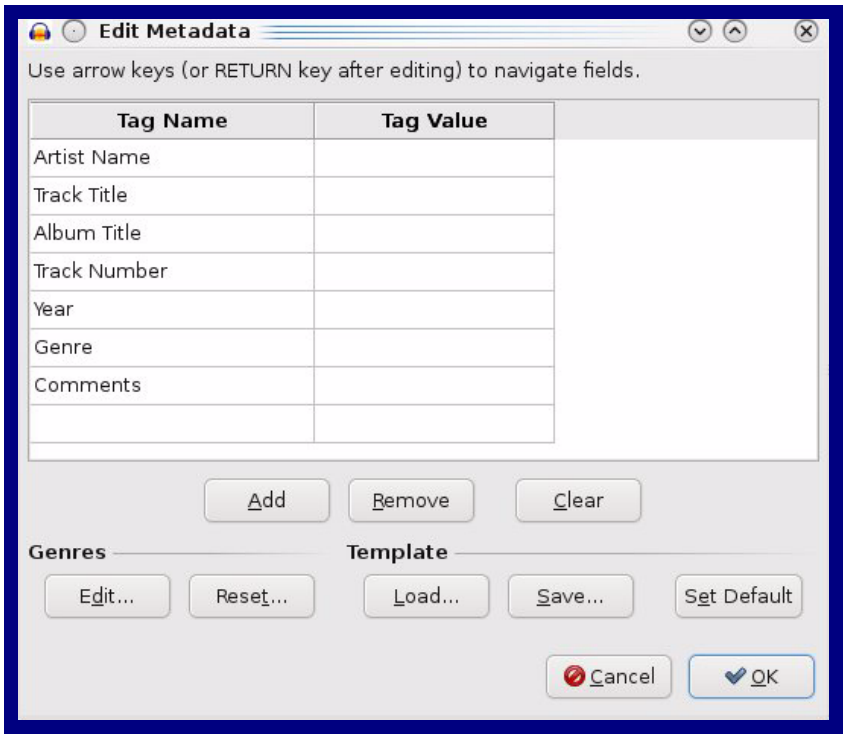


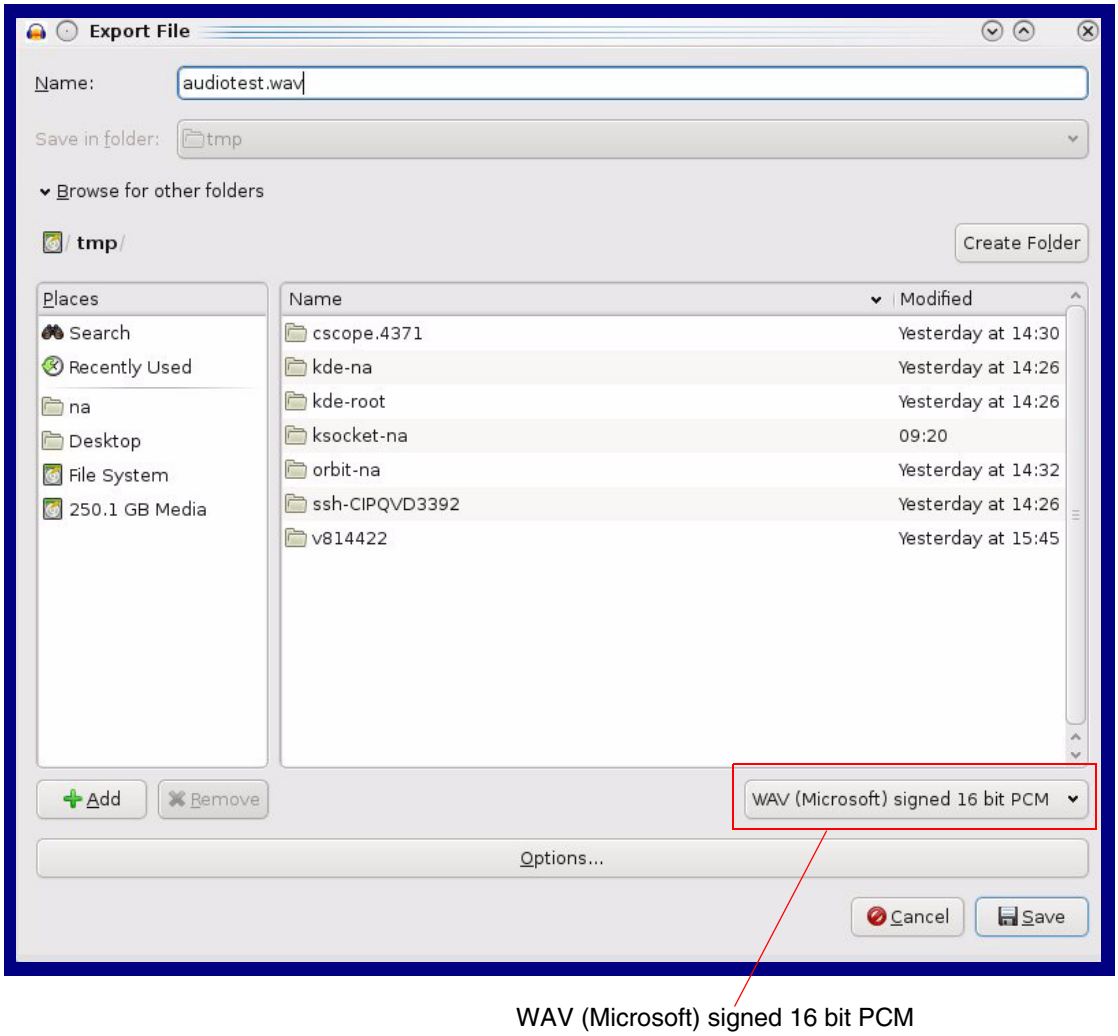
Figure 2-20. Audacity 2



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

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

Figure 2-21. WAV (Microsoft) signed 16 bit PCM



2.4.10 Configure the Event Parameters

Click on the **Events** button to open the **Events** page (Figure 2-22). The **Events** page specifies a remote server that can be used to receive HTTP POST events when actions take place on the board.

Figure 2-22. Events Page

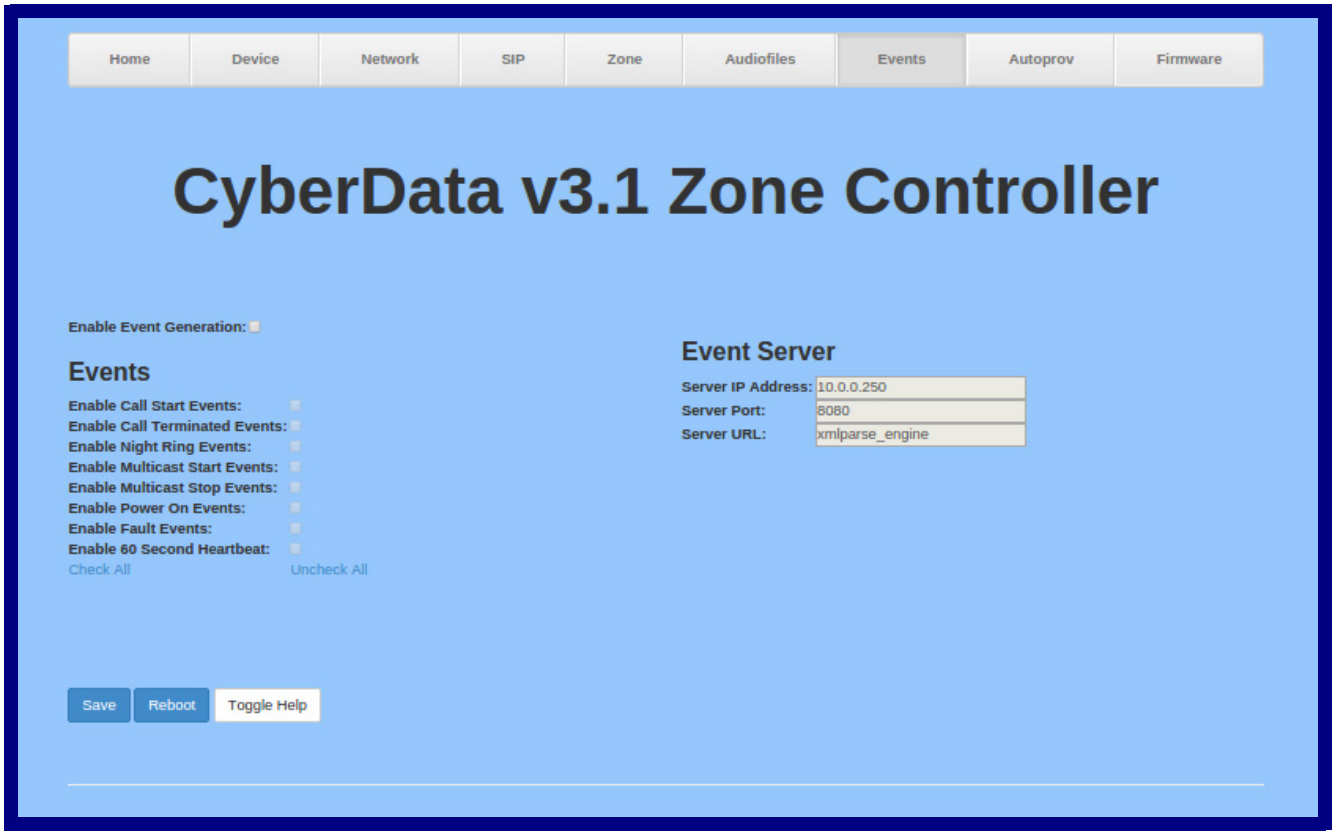


Table 2-15 shows the web page items on the **Events** page.

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 2-15. 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 2.4.10.1, "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 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 Multicast Start Events ?	When selected, the device will report when the device starts playing a multicast audio stream.
Enable Multicast Stop Events ?	When selected, the device will report when the device stops playing a multicast audio stream.
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.
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.
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.
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
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 and then the **Reboot** button for the changes to take effect.

2.4.10.1 Example Packets for Events

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

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

Here are example packets for every event:

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

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


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

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


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

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

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

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData VoIP Device' MAC='0020f70015b6'>
<event>CALL_ACTIVE</event>
</cyberdata>
POST xmlparse_engine HTTP/1.1
```

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

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


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

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


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

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

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

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

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

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

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>
```

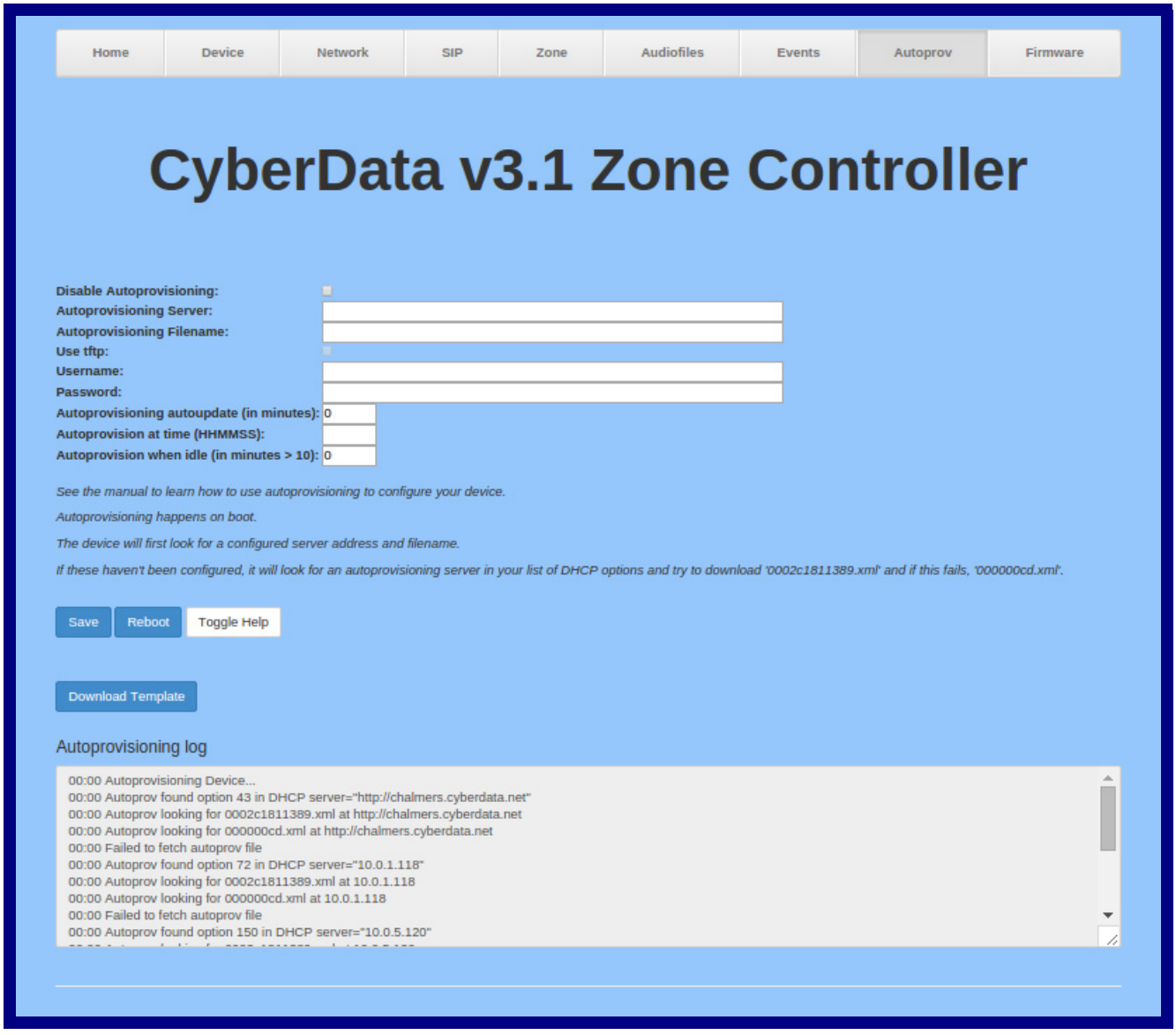
2.4.11 Configure the Autoprovisioning Parameters

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 2-23.

Figure 2-23. Autoprovisioning Page



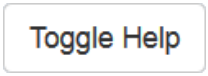
2. On the **Autoprovisioning** page, you may enter values for the parameters indicated in Table 2-16.

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 2-16. Autoprovisioning Configuration Parameters

Web Page Item	Description
Disable Autoprovisioning ?	Prevent the device from automatically trying to download a configuration file. See Section 2.4.11.1, "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 **Set Time with NTP Server on boot** 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 **Set Time with NTP Server on boot** 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 **Set Time with NTP Server on boot** setting on the **Device Page** page (see Table 2-6).
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.

Table 2-16. Autoprovisioning Configuration Parameters (continued)

Web Page Item	Description
	Click on the **Reboot** button to reboot the system.
	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.
	Press the **Download Template** button to create an autoprovisioning file for the device. See Section 2.4.11.3, "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 and then the **Reboot** button for the changes to take effect.

2.4.11.1 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 2.4.11.2, "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 2-16). 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 2-17. 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.

2.4.11.2 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; }
```

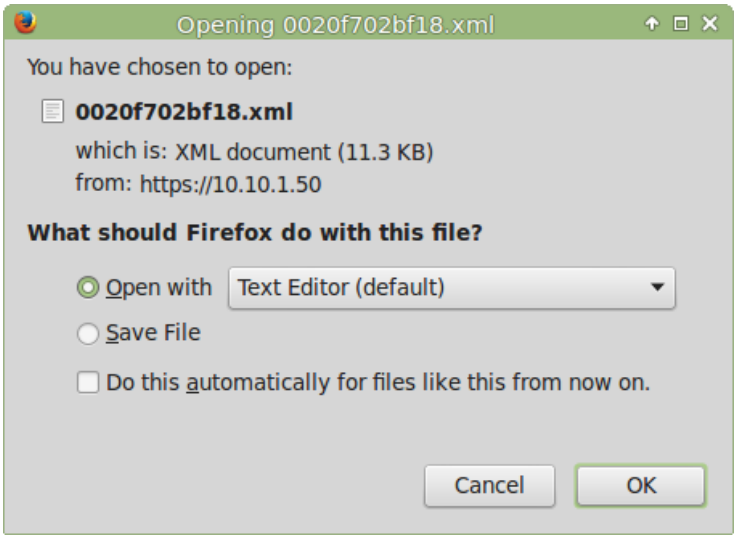
2.4.11.3 Get Autoprovisioning Template Button

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 2-24). 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 2-24.

Figure 2-24. 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.

2.5 Upgrading the Firmware

Caution

Equipment Hazard: Devices with a serial number that begins with 1711xxxxx can only run firmware versions 11.0.0 or later.

2.5.1 Upgrade the Firmware

To upload the firmware from your computer:

1. Retrieve the latest SIP Paging Zone Controller firmware by clicking on the **Downloads** tab at the following webpage:

   https://www.cyberdata.net/products/011171

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

- Firmware file
- Release notes

3. Log in to the SIP Paging Zone Controller home page as instructed in Section 2.4.4, "Log in to the Configuration Home Page".

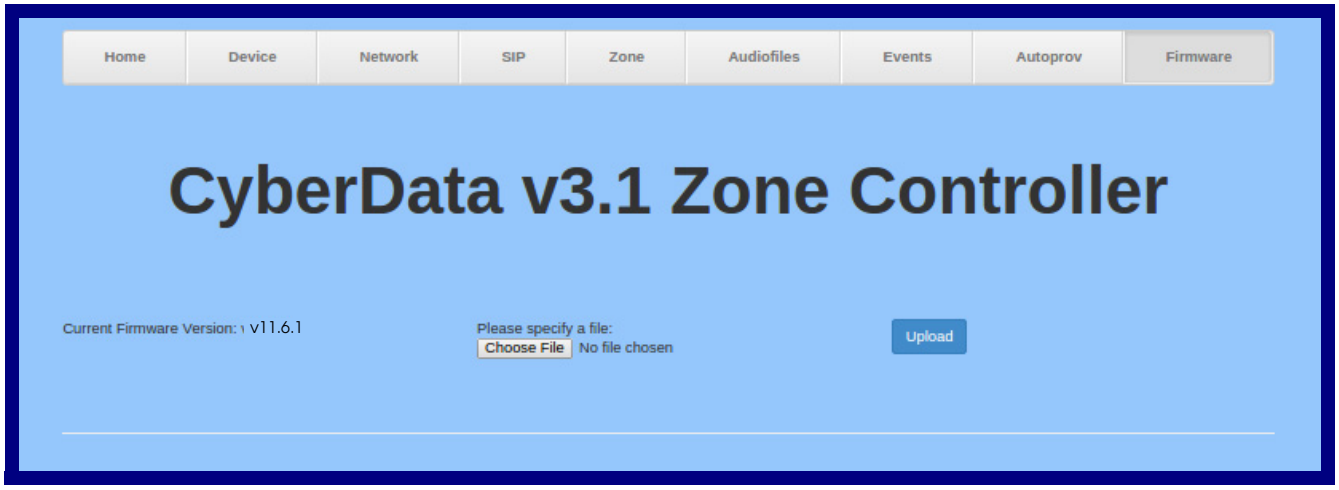
4. Click on the **Firmware** menu button to open the **Firmware** page. See Figure 2-25.

GENERAL ALERT

Caution

Equipment Hazard: CyberData strongly recommends that you first reboot the device before attempting to upgrade the firmware of the device. See Section 2.5.2, "Reboot the Device".

Figure 2-25. Firmware Page



5. Click on the **Choose File** or **Browse** button, and then navigate to the location of the firmware file.
6. Select the firmware file.
7. Click on the **Upload** button.

Note Do not reboot the device after clicking on the **Upload** button.

Note This starts the upgrade process. Once the SIP Paging Zone Controller has uploaded the file, the **Uploading Firmware** countdown page appears, indicating that the firmware is being written to flash. The SIP Paging Zone Controller will automatically reboot when the upload is complete. When the countdown finishes, the **Firmware** page will refresh. The uploaded firmware filename should be displayed in the system configuration (indicating a successful upload and reboot).

8. Table 2-18 shows the web page items on the **Firmware** page.

Table 2-18. Firmware Parameters

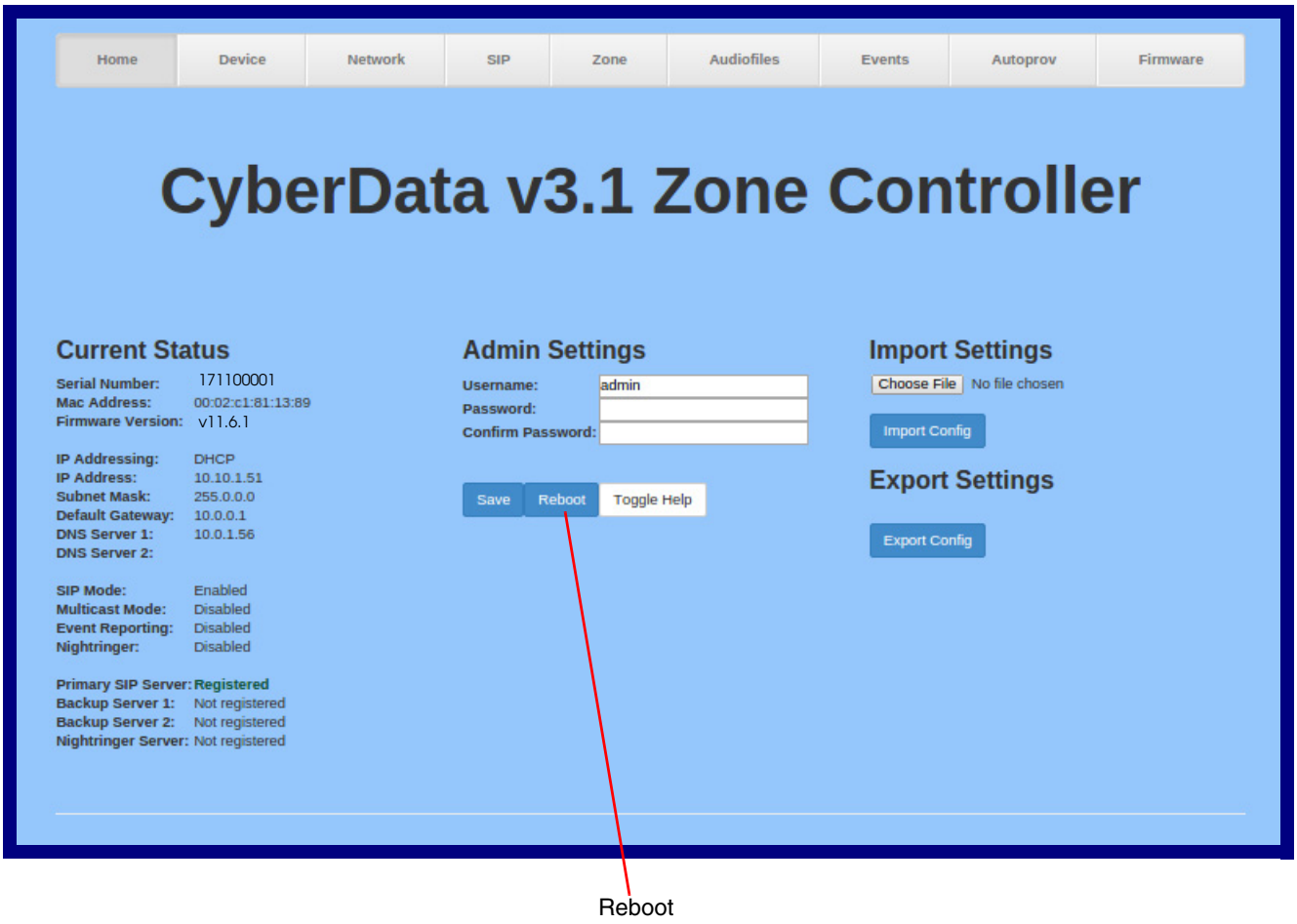
Web Page Item	Description
Current Firmware Version	Shows the current firmware version.
Choose File	Use this button to navigate to and select a firmware file.
Upload	Click on the **Upload** button to automatically upload the selected firmware and reboot the system.

2.5.2 Reboot the Device

To reboot a SIP Paging Zone Controller, log in to the web page as instructed in Section 2.4.4, "Log in to the Configuration Home Page".

1. Click **Reboot** (Figure 2-26). A normal restart will occur.

Figure 2-26. Home Page



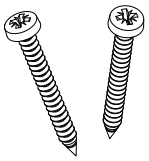
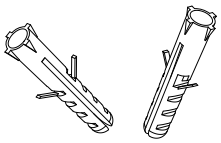
Appendix A: Mounting the SIP Paging Zone Controller

A.1 Mount the SIP Paging Zone Controller

A.1.1 Mounting Components

Before you mount the SIP Paging Zone Controller, make sure that you have received all of the parts for each SIP Paging Zone Controller. Refer to Table A-1.

Table A-1. Wall Mounting Components (Part of the Accessory Kit)

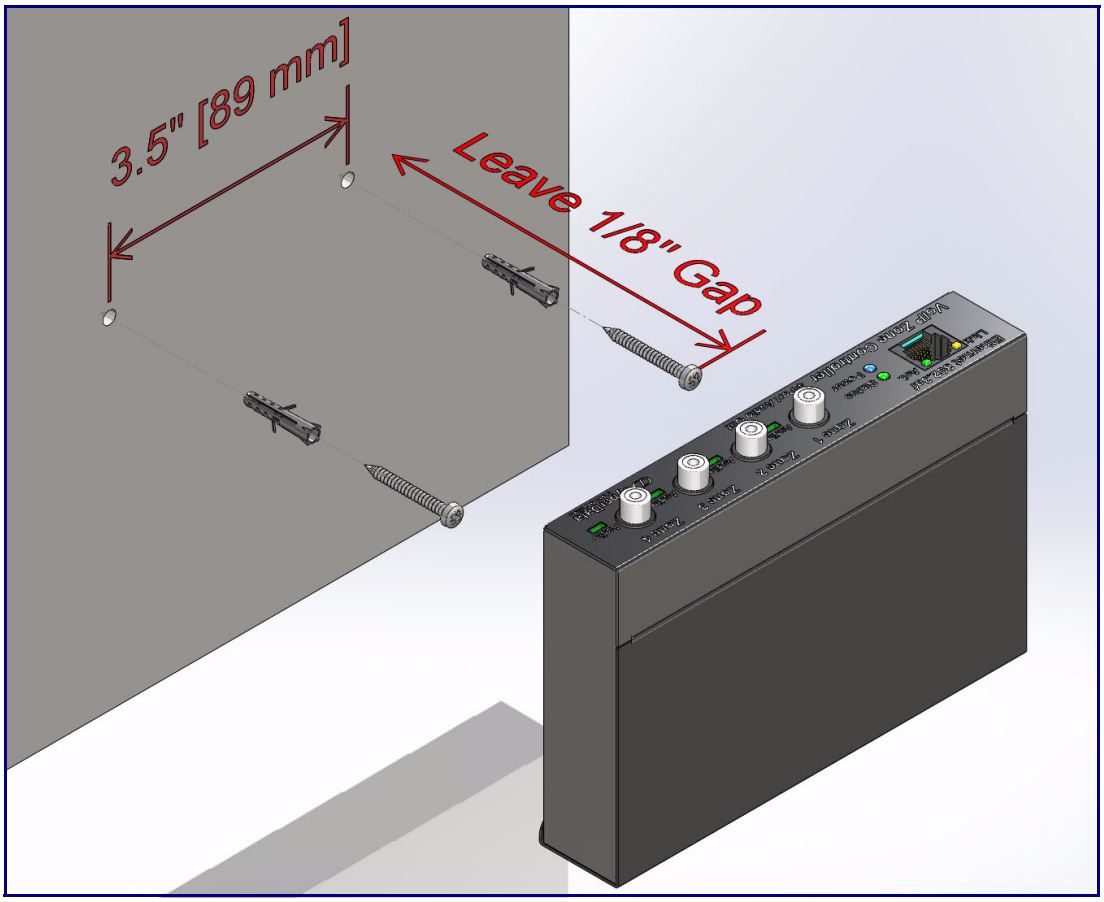
Quantity	Part Name	Illustration
2	#6 x 1 1/2-inch Screws	
2	#6 Plastic-Ribbed Anchors	

A.1.2 Mounting Procedure

To mount the SIP Paging Zone Controller:

1. On the mounting location, mark and then drill two 3/16-inch (0.1875-inch) holes 3.5 inches apart from and parallel to each other for the plastic-ribbed anchors and screws. See Figure A-1.
2. Insert the plastic-ribbed anchors into the prepared holes. See Figure A-1.
3. Install the #6 screws into the plastic-ribbed anchors and leave approximately 1/8-inch gap from the screw head to the wall. See Figure A-1.
4. Determine which sides of the SIP Paging Zone Controller will be facing up, and then slide the SIP Paging Zone Controller down over the screws to latch onto the screws.

Figure A-1. Mounting



Appendix A: Setting Up a TFTP Server

A.1 Set up a TFTP Server

Autoprovisioning requires a TFTP server for hosting the configuration file.

A.1.1 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.1.2 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/011171

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/011171

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, Ext. 333
Email: support@cyberdata.net

B.4 Warranty and RMA Information

The most recent warranty and RMA information is available by clicking on **Warranty & RMA** on the following webpage:

http://support.cyberdata.net/

Index

Numerics

100 Mbps indicator LED 8

A

act LED 8
activity LED 8
address, configuration login 14
addressing
  DHCP 10, 26
  static 10, 26
admin username and password 14
amplifier connections
  cables used 1, 6
audio activity LED 8
audio configuration 36
  night ring tone parameter 40
audio configuration page 36
authenticate ID and password for SIP server registration 31
autoprovision at time (HHMMSS) 50
autoprovision when idle (in minutes > 10) 50
autoprovisioning 51
  download template button 51
autoprovisioning autoupdate (in minutes) 50
autoprovisioning configuration 49, 50
autoprovisioning filename 50
autoprovisioning server (IP Address) 50

B

backup SIP server 1 28
backup SIP server 2 28
backup SIP servers, SIP server
  backups 28
blue status LED 8

C

cables used to connect the paging device to the legacy analog amplifiers 1, 6
changing
  the web access password 18
changing default username and password for configuration GUI 14
Cisco SRST 28
configurable parameters 19, 25, 28
configuration information 10
configuration page
  configurable parameters 19, 25
connection speed
  10 Mbps 8
  100 Mbps 8
connection speeds 8
connections
  cables used 1, 6
contact information 68
contact information for CyberData 68
current network settings 25
current settings, reviewing 17
CyberData contact information 68

D

default
  gateway 9
  IP address 9
  subnet mask 9
  username and password 9
default gateway 9, 25
default gateway for static addressing 26
default login address 14
default password for configuration GUI 14
default settings, restoring 9
default username and password for configuration GUI 14
device configuration 18
  device configuration parameters 50
  the device configuration page 49
device configuration page 18
device configuration parameters 19
device configuration password
  changing for web configuration access 18
DHCP addressing 10, 26
dimensions 3
discovery utility program 14
DNS server 25
door sensor 39, 40
download autoprovisioning template button 51

E

enable night ring events 45
ethernet I/F 3

event configuration
enable night ring events 45
expiration time for SIP server lease 29, 30, 31
export settings 16

F

features 2
firmware
where to get the latest firmware 61
firmware, upgrade 61

G

get autoprovisioning template 51
GMT table 22
GMT time 22
GUI username and password 14

I

identifier names (PST, EDT, IST, MUT) 22
identifying your product 1
illustration of device mounting process 64
import settings 16
import/export settings 16
intercom configuration page
configurable parameters 28
IP address 9, 25
SIP server 31
IP addressing
default
IP addressing setting 9

L

lease, SIP server expiration time 29, 30, 31
link LED 8
Linux, setting up a TFTP server on 66
local SIP port 29, 31
log in address 14
logging in to configuration GUI 14

M

mounting procedure 65
mounting the device 64
multicast configuration 32
Multicast IP Address 34

N

navigation (web page) 11
navigation table 11
network configuration page 24
network parameters, configuring 24
network setup button 24
network, connecting to 7
Nightringer 27, 60
Nightringer in peer to peer mode (cannot be used) 27
nightringer settings 29
Nightringer, SIP registration required 27
NTP server 19

O

operating the zone controller 34
output connections 1, 6

P

paging LED 8
part number 3
parts list 4
password
configuration GUI 10, 14
for SIP server login 28
restoring the default 9
SIP server authentication 31
payload types 3
point-to-point configuration 32
port
local SIP 29, 31
remote SIP 29, 31
posix timezone string
timezone string 19
power
connecting to 6
power input 3
power status LED 8
product
mounting 64
product overview 1
product specifications 3
product specifications 3
protocol 3

R

reboot 62, 63
    unregistering from SIP server during 31
registration and expiration, SIP server
    lease expiration 31
remote SIP port 29, 31
required configuration for web access username and password 10, 14
resetting the IP address to the default 64, 67
restoring factory default settings 9
rport discovery setting, disabling 29
RTFM switch 9

S

sales 68
server
    TFTP 66
server address, SIP 28
service 68
set time with external NTP server on boot 19
SIP
    enable SIP operation 28
    local SIP port 29
    user ID 28
SIP configuration page 27
SIP configuration parameters
    outbound proxy 29, 30
    registration and expiration, SIP server lease 29, 30
    unregister on reboot 29
    user ID, SIP 28
SIP registration 28
SIP remote SIP port 29
SIP server 28
    password for login 28
    unregister from 29
    user ID for login 28
SIP server configuration 28
SIP server parameters, configuring 10
SIP setup button 27
specifications 3
SRST 28
static addressing 10, 26
status LED 8
subnet mask 9, 25
subnet mask static addressing 26
supported protocols 2

T

tech support 68
technical support, contact information 68
TFTP server 66
time zone string examples 22

U

unregister from SIP server 31
upgrade firmware 61
user ID
    for SIP server login 28
user ID for SIP server registration 31
username
    changing for web configuration access 18
    restoring the default 9
username for configuration GUI 10, 14

V

VLAN ID 25
VLAN Priority 25
VLAN tagging support 25
VLAN tags 25

W

warranty policy at CyberData 68
web access password 9
web access username 9
web configuration log in address 14
web page
    navigation 11
web page navigation 11
Windows, setting up a TFTP server on 66

Z

zone controller
    configuration 10
zone controller operation 34