VoIP Telephones

HDE Setup & Configuration

HDE-11-VoIP

HDE-1100-VoIP

HDE-12-VoIP

HDE-1200-VoIP

P007451 Rev. B 130313 3/13/2013 2:50 PM

7552 - 10th Street N.E. Calgary, Alberta, Canada T2E 8W1
Ph: 403.258.3100 \ email:info@guardiantelecom.com \ www.guardiantelecom.com

VoIP Setup & Configuration P007451 Rev. B (applicable to firmware V0.0.62)

Toll-free 1-800-363-8010

Guardian Telecom Inc.

Phone (403) 258-3100
Fax. (403) 253-4967
www.guardiantelecom.com
E-mail: sales@guardiantelecom.com

IMPORTANT Installation Step

It is important to register this VoIP product with Guardian Telecom to ensure it has the most current version of software and to receive notification of software updates.

Registering Your VoIP Product

To register your VoIP product send an email to info@guardiantelecom.com.
Be sure to include "Guardian VoIP Registration" in the subject field of your email.

Include the following information:

- **Company Name of End User (Req'd)**
- **Address of End User (Optional)**
- **Device Model (Req'd)**
- **Serial Number - Found on the Exterior Label (Req'd)**
- **Date of purchase (Req'd)**
- **Name of Supplier (Req'd)**
- **Prime Contact name and e-mail (Req'd)**
- **Secondary Contact name and e-mail (Optional)**
- **Phone Info: (Optional)**

It is very important that we receive e-mail contact information of the person responsible for maintaining the installed Guardian Equipment, in order to ensure optimum performance of the device.

Contact information will remain confidential and will not be used for third-party marketing purposes.

Important Safety Instructions

1. Read these instructions.
2. Keep these instructions.
3. Heed all warnings.
4. Follow all instructions.
5. Install in accordance with the manufacturer's instructions.
6. Do not install near any heat sources such as radiators, heat registers, stoves, or other apparatus (including amplifiers) that produce heat.
7. Only use attachments/accessories specified by the manufacturer.
8. Refer all servicing to qualified service personnel.
9. Prior to installation, consult local building and electrical code requirements.

GENERAL ALERT	Warning *Electrical Hazard:* This product should be installed by a licensed electrician according to all local electrical and building codes.
GENERAL ALERT	Warning *Electrical Hazard:* To prevent injury, this apparatus must be securely attached to the floor/wall in accordance with the installation instructions.

Table of Contents

Figures

Tables

Acronyms

DHCP Server	Dynamic Host Configuration Protocol
DHCPD	Dynamic Host Configuration Protocol Daemon
DTMF	Dual-tone Multi-frequency
HTTP	Hypertext Transfer Protocol
IP Address	Internet Protocol Address
LAN	Local Area Network
LINUX	Unix-like computer operating system
PBX	Private Branch Exchange
PC	Personal Computer
PCM	Pulse-Code Modulation
PCMA	Paired Carrier Multiple Access
PCMU	Pulse Code Modulation mu-law
PoE	Power over Ethernet
POST	Power On Self Test
RIFF	A short, repeated musical phrase
RTP	Real-time Transport Protocol
RTP Port	Real-time Transport Protocol port
AVP	Audio Video Profile
SIP	Session Initiation Protocol
TFTP	Trivial File Transfer Protocol
URL	Uniform Resource Locator
VoIP	Voice Over Internet Protocol
WAV	Waveform Audio File Format
WAVE	Waveform Audio File Format
XML File	Extensible Markup Language

1. Typical System Installation

The Voice-over-IP (VoIP) Telephone is a Power-over-Ethernet (PoE 802.3af) and Voice-over-IP (VoIP) two-way communications device that easily connects into existing local area networks (LANs) with a single cable connection. The telephone is compatible with most SIP-based IP PBX servers that comply with SIP RFC 3261.
Figure 1 illustrates how VoIP Telephones can be installed as part of a VoIP phone system.

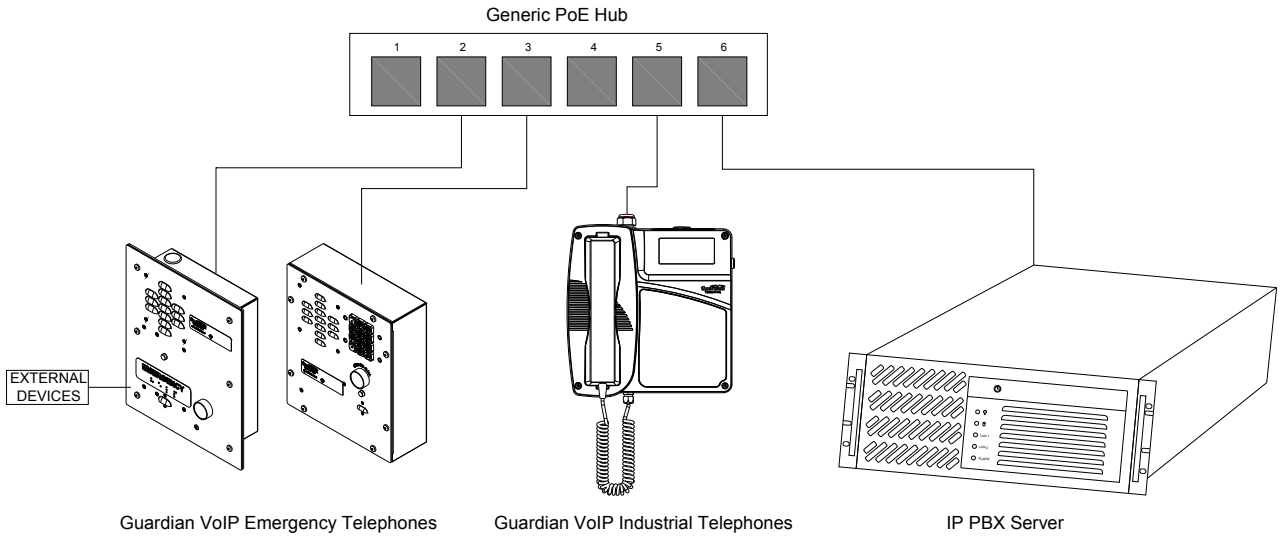

Figure 1 - Typical Installation

2. Operation

Once your VoIP Telephone has been properly installed and energized, operation is identical to most other single line telephones.

3. Supported Protocols

The VoIP Telephone with Keypad supports:

- SIP (Session Initiation Protocol)
- HTTP Web-based configuration
  Provides an intuitive user interface for easy system configuration and verification of a VoIP Telephone.
- DHCP Client
  Dynamically assigns IP addresses in addition to the option to use static addressing.
- TFTP Client
  Facilitates hosting for the Autoprovisioning configuration file.
- RTP
  Facilitates autoprovisioning configuration values on boot
- Audio Encodings
  PCMU (G.711 mu-law)
  PCMA (G.711 A-law)
  Packet Time 20 ms

4. Supported SIP Servers

As a SIP device, this product will operate with most IP PBX servers.

5. Getting Started

The Installation manual for the telephone provides information on installing and connecting the device to the server.
This manual describes the steps required to customize the telephone to suit the individual's preferences.
The Discovery Utility is available on Guardian's website and needs to be installed manually.

To access a VoIP phone for programming:

- Install the Guardian Discovery Utility onto the network server or SIP server.
- Start the Utility by double clicking the icon.
- Click on "Refresh List".
- Click on the device to be programmed to highlight it.
- Click on "Launch Browser".

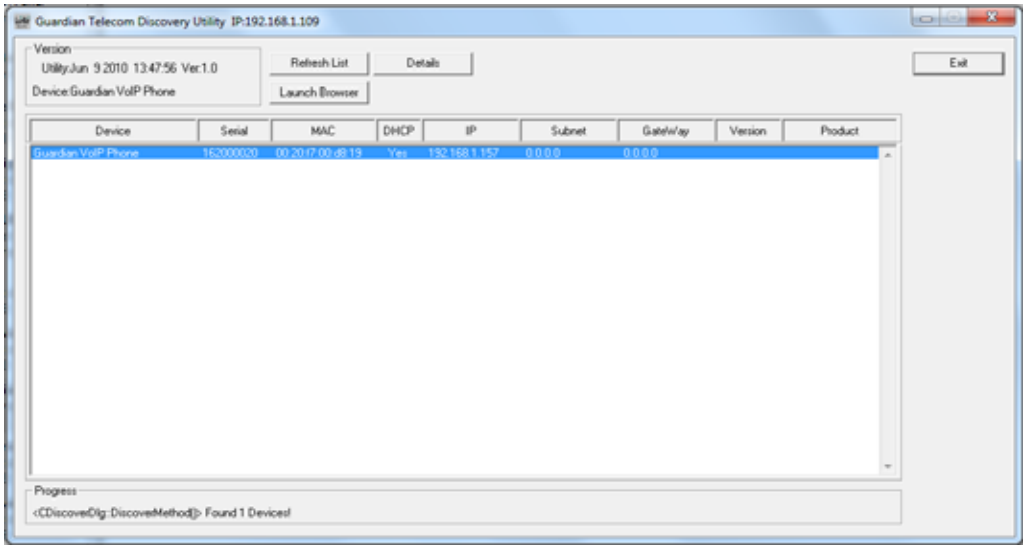

Figure 2 - Startup Screen

6. Configure the Telephone Parameters

To configure the Telephone online use a standard web browser.
All Telephones are initially configured with the following default IP 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

Table 1 - Factory Default Settings

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

When configuring more than one Telephone attach the Telephones to the network and configure one at a time to avoid IP address conflicts.

6.1. Telephone Web Page Navigation

Table 2 shows the navigation buttons that you will see on every Telephone web page.

Web Page Item	Description
Home	Link to the **Home** page.
Device Config	Link to the Device Configuration page.
Networking	Link to the **Networking** page.
SIP Config	Link to the SIP Configuration page.
Nightringer	Link to the Nightringer Configuration page.
Audio Config	Link to the Audio Configuration page.
Event Config	Link to the Event Configuration page.
Autoprovisioning	Link to the Autoprovisioning Configuration page.
Update Firmware	Link to the **Update Firmware** page.

Table 2 - Telephone Web Page Navigation

6.2. Log in to the Configuration Home Page

1. Open your browser to the Telephone's IP address. If you do not know the IP address, you can use the "Discovery Utility" to detect all VoIP devices on the network. When opened the Discovery Utility scans the network for VoIP devices, specifically Guardian VoIP devices. Individually select the device and launch the browser. Another method to obtain the IP address is to press the RESET switch for approximately one second. The phone will announce the address through the speaker. The physical location of a telephone can be determined by comparing the MAC Address, IP Address or Serial Number shown on the Discovery Utility screen with the information on the unit.

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 Telephone.

2. When prompted, use the following default **Web Access Username** and **Web Access Password** to access the **Home Page** (Figure 3):

Web Access Username: **admin**

Web Access Password: **admin (lower case)**

3. On the **Home Page**, review the setup details and navigation buttons described inTable 3.

Note: **The Screen Captures shown are only examples; refer to the tables for definitions.**

Figure 3 - Home Page

Web Page Item	Description
Device Settings	
Device Name:	Shows the device name.
Change Username:	Type in this field to change the username.
Change Password:	Type in this field to change the password.
Re-enter Password:	Type the password again in this field to confirm the new password.
Current Settings	
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.
Speaker Volume:	Shows the current speaker volume level.
Microphone Gain:	Shows the current microphone gain level.
SIP Mode is:	Shows the current SIP Mode status.
Event Reporting is:	Shows the current Event Reporting status.
Nightringer is:	Ringtone broadcast when enabled and extension is called.
Primary SIP Server:	Primary SIP Server
Backup Server 1:	Redundant SIP Server “1”
Backup Server 2:	Redundant SIP Server “2”
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 device.

Table 3 - Home Page Overview

6.3. Configure the Device Parameters

1. Click the **Device Configuration** button to open the **Device Configuration** page. See Figure 4.

Figure 4 - Device Configuration Page

2. On the **Device Configuration** page, you may enter values for the parameters indicated in Table 4.
3. After changing the parameters, click the **Save** button.

Web Page Item	Description
Volume Settings	The volume settings describe the volume set on reboot. The user can change the volume by using the up and down arrows, but this change is temporary and the volume will be reset when the device is rebooted.
Hands Free Speaker Volume:	The speaker volume sets the initial volume of the device on boot. Valid values are 0-9. Test the speaker volume using the 'Test Audio' button below. Saving changes to the speaker volume will take effect immediately (it does not require a restart).
Hands Free Microphone Gain:	The microphone gain sets the initial input gain of the on board microphone. Valid values are 0-9. Test the speaker volume using the 'Test Microphone' button below. Saving changes to the speaker volume will take effect immediately (it does not require a restart).
Relay Settings	
Activate Relay with DTMF Code:	When this option is enabled, the device will activate the relay when it receives a DTMF code (rfc2833).
DTMF Activation Code:	This 25 character field can be used to set a DTMF code used to activate the relay.
DTMF Activation Duration (in seconds):	When the relay is activated with a DTMF code, it will remain active for this duration in seconds. Valid values are 1-9. **NOTE**: A DTMF activation of **0** will toggle the relay indefinitely or until the activation code is sent again.
Activate Relay During Ring**:**	When this option is enabled, the relay will activate when the device has received a call and is playing a ringtone.
Activate Relay During Night Ring**:**	When this option is enabled, the relay will activate when the device has received a call to the night ring extension.
Pulse Relay when Ringing:	When a "ring" is present the relay will pulse with a cadence of 2 seconds on, 3 seconds off.
Pulse Buzzer when Ringing:	When a "ring" is present the internal ringer will pulse with a cadence of 2 seconds on, 3 seconds off.
Activate Relay While Call Active**:**	When this option is enabled, the relay will activate when a call is established with another SIP device. It will remain active for the duration of the call.
Miscellaneous Settings	
Call Termination Lockout:	The Call Termination Lockout feature is applicable only to the RED button switch. When the Call Termination Lockout is enabled the RED button can initiate an autodialing action; however subsequently pressing the RED button will not terminate the call.
Auto-Answer Incoming Calls**:**	When this option is enabled, the device will automatically answer incoming calls.
Test Audio	This button will play an audio test message and can be used to test the volume level.
Test Microphone	When this button is pressed the device will record 3 seconds of audio, beep, and then play back the recorded audio. This can be used to test the microphone gain level.
Test Relay	This button will activate the relay for the DTMF activation Duration (in seconds).
Start Button Test	When this button is toggled, it will put the device into button test mode. In this mode, the speaker will play an audio file when a button is pressed on the device. For normal keypad input (keys 0-9) it will speak the associated file from the audio configuration page. For the other keypad keys, (*, #, any other function keys) it will play a DTMF tone while the button is depressed. The button press mode will time out after 60 seconds.
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 device.

Table 4 - Device Configuration Parameters

6.4. Configure the Network Parameters

1. Click the **Networking** button to open the **Network Configuration** page (Figure 5).

Figure 5 - Network Configuration Page

2. On the **Network Configuration** page, enter values for the parameters indicated in Table 5.

3. After changing the parameters, click **Save** to store the settings before going to the other configuration pages. If no other changes are required beyond this state, click **Reboot** to reset the device for other changes to take effect.
The new settings will not take effect if **Reboot** is clicked without saving first.

4. Connect the Telephone to the target network.

5. From a computer on the same network as the Telephone, open a browser with the new IP address of the Telephone.

Web Page Item	Description
Stored Network Settings	Shows the settings stored in non-volatile memory.
IP Addressing:	This setting is used to configure the device to use the static IP address configured below or to fetch its address from a DHCP server on the network. When the device is plugged into a network without a DHCP server, it will request an address 12 times over the course of 60 seconds before it will fall back on the last known good DHCP address, or if it has never had a DHCP address, to the stored static IP address (by default 10.10.10.10).
IP Address:	The IPV4 static IP address in standard dotted decimal notation.
Subnet Mask:	The IPV4 routing prefix in standard dotted decimal notation.
Default Gateway:	This is the node to go to when an IP address doesn't match any routes in the routing table. This requires standard quad-dotted decimal notation.
DNS Server 1: DNS Server 2:	The DNS server configuration is used to setup the primary and secondary name servers for the network. These use standard dotted decimal notation.
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.
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 device.

Table 5 - Network Configuration Parameters

6.5. Configure the SIP Parameters

1. Click **SIP Config** to open the **SIP Configuration** page (Figure 6).

   Note: Guardian VoIP telephones are compatible with most SIP servers.

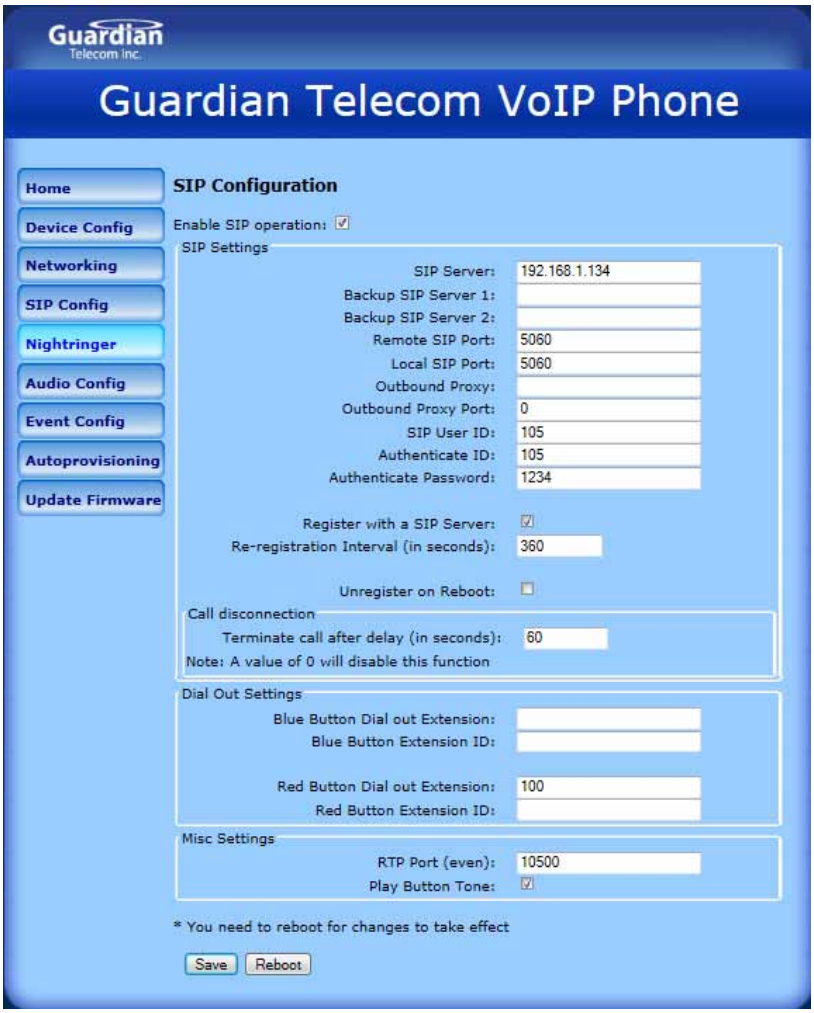

Figure 6 - SIP Configuration Page

2. On the **SIP Configuration** page, enter values for the parameters indicated in Table 6.
3. After changing the parameters, click **Save Settings**

Table 6 - SIP Configuration Parameters

Web Page Item	Description
Enable SIP Operation:	When this option is enabled, the device will initialize the SIP engine and try to register with a SIP server or listen for incoming SIP connections.
SIP Settings	
SIP Server	The SIP server is used to set the address (in dotted decimal notation or as a canonical name) of the SIP registrar. This field can accept canonical names of up to 255 characters in length.
Backup SIP Server 1:	The SIP server is used to set the address (in dotted decimal notation or as a canonical name) of the SIP registrar. This field can accept canonical names of up to 255 characters in length.
Backup SIP Server 2:	The SIP server is used to set the address (in dotted decimal notation or as a canonical name) of the SIP registrar. This field can accept canonical names of up to 255 characters in length.
Remote SIP Port:	The Remote SIP Port is used to set the port number that the SIP registrar uses for SIP traffic.
Local SIP Port:	The Local SIP Port is used to set the port number this device will use to listen for and transmit SIP traffic.
Outbound Proxy:	The Outbound Proxy Port is an optional field only filled in if a Proxy server is used for SIP communications. It is used to set the port number of the Proxy Server.
Outbound Proxy Port:	Type the Outbound Proxy Port number (8 character limit).
SIP User ID:	The SIP User ID is the user part of a SIP address; generally this is the extension number of the device.
Authenticate ID:	The Authenticate ID is the ID used for authentication by the SIP server. If authentication is not configured on the SIP server, this field should be blank.
Authenticate Password:	The Authenticate Password is the password used for authentication by the SIP server. If authentication is not configured on the SIP server, this field should be blank.
Register with a SIP Server:	When this option is enabled, the device will try to register with the SIP server and credentials (given above) on boot. When the device has successfully registered with a SIP server, it will show its status at the top of the page. When this option is disabled, the device will operate in point to point (P2P) mode. In this mode, the device can connect to other SIP devices without using a SIP server as an intermediary. This option only exists when using the speed dial option on the button configuration page. Instead of putting an extension in these fields, use an IP address. **Note:** Some phones do not support placing or receiving calls to a device rather than a SIP server.
Re-registration Interval (in seconds):	The re-registration interval determines how often the device will attempt to re-register with the SIP server. Valid values are 100-3600 seconds. Some SIP servers may request a device register more or less often than the value configured here.
Unregister on Reboot:	If Unregister on Reboot is checked, this device will attempt to send a remove all register(s) request to the SIP server upon booting. Please note that if the SIP server does not support this unregister request, it may cause some problems.

Call disconnection	
Terminate call after delay (in seconds):	Enter number in seconds. Call will terminate once time has expired. **Note: A value of 0 will disable this function**
ID:	Password for Keypad AD extension. If authentication is not configured on the SIP server, this field should be blank.
Dial Out Settings	
Blue Button Dial out Extension:	Enter the speed dial extension that is to be used when the user presses the Blue button. If the field is left blank pressing the blue button will result in a dial tone, allowing the user to dial out without restriction.
Blue Button Extension ID:	Password for Ringdown extension. If authentication is not configured on the SIP server, this field should be blank.
Red Button Dial out Extension:	Enter the speed dial extension that is to be used when the user presses the Red button.
Red Button Extension ID:	Password for Ringdown extension. If authentication is not configured on the SIP server, this field should be blank.
Misc Settings	
RTP Port (even) :	The RTP Port field is used to set the port pair that this device will use for listening for and transmitting RTP and RTCP traffic. This field sets the RTP port. This field +1 sets the RTCP port. Per the RFCS55O specification, the RTP port should be even, but an odd port number is allowed.
Play Button Tone:	When selected, you will hear a button tone when a keypad button is pressed.
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 device.

THIS PAGE INTENTIONALLY LEFT BLANK

6.6. Configure the Nightringer Page

Click the **Nightringer** button to open the **Nightringer Configuration** page (Figure 7).

On the **Nightringer Configuration** page you may enter values for the parameters indicated in Table 7.

Figure 7 - Nightringer Configuration Page

Web Page Item	Description
Enable Nightringer:	When the 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.
Nightringer Settings	
SIP Server:	Type the SIP server represented as a numeric IP address in dotted decimal notation.
Remote SIP Port:	Type the Remote SIP Port number (default 5060) (8 character limit).
Local SIP Port:	Type the Local SIP Port number (default 5060) (8 character limit). Note: This value cannot be the same as the **Local SIP Port** found on the **SIP Configuration Page.**
User ID:	Type the **User ID** (up to 64 alphanumeric characters).
Authenticate ID:	Type the **Authenticate ID** (up to 64 alphanumeric characters).
Authenticate Password:	Type the **Authenticate Password** (up to 64 alphanumeric characters).
Re-registration Interval (in seconds):	Type the SIP Registration lease time in minutes (default is 60 minutes) (8 character limit). Re-registration Interval (in seconds).
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 device.

Table 7 - Nightringer Configuration Parameters

6.7. Configure the Audio Parameters

1. Click **Audio Config** to open the **Audio Configuration** page (Figure 8).

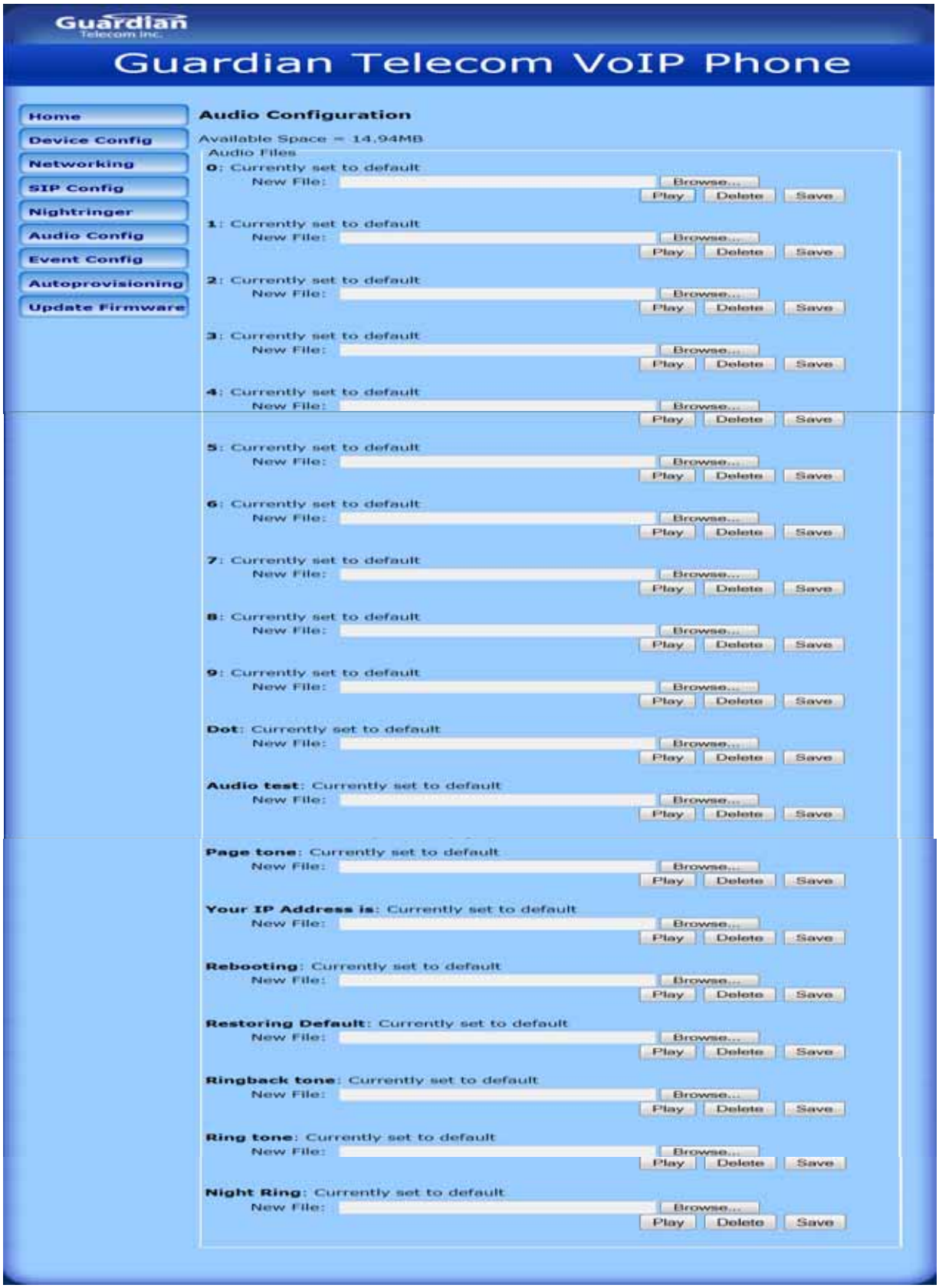

Figure 8 - Audio Configuration Page

The **Audio Configuration** page is used to add custom audio to the board. User uploaded audio will take precedence over the audio files shipped with the Telephone.

2. On the **Audio Configuration** page, enter values for the parameters indicated in Table 8.

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

The character limits relate to the file names, not the contents of the file.

Web Page Item	Description
Audio Files	
0-9:	The name of the audio configuration option is the same as the spoken audio that plays on the board. '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 Guardian IP telephone test message...” (200 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).
Ringback Tone:	This is the ringback tone that plays when calling a remote extension (24 character limit).
Ring tone:	Tone that plays when the device is ringing.
Night Ring:	When the 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.
Browse...	Click the Browse button to search for files.
Play	Click the Play button to hear the current message.
Delete	Click the Delete button to empty the box.
Save	Click the **Save** button to save your settings.

Table 8 - Audio Configuration Parameters

6.7.1. User-created Audio Files

User created audio files should be saved in the following format:

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

You can use the free utility *Audacity* to convert audio files into this format, see Figure 9 through Figure 11.

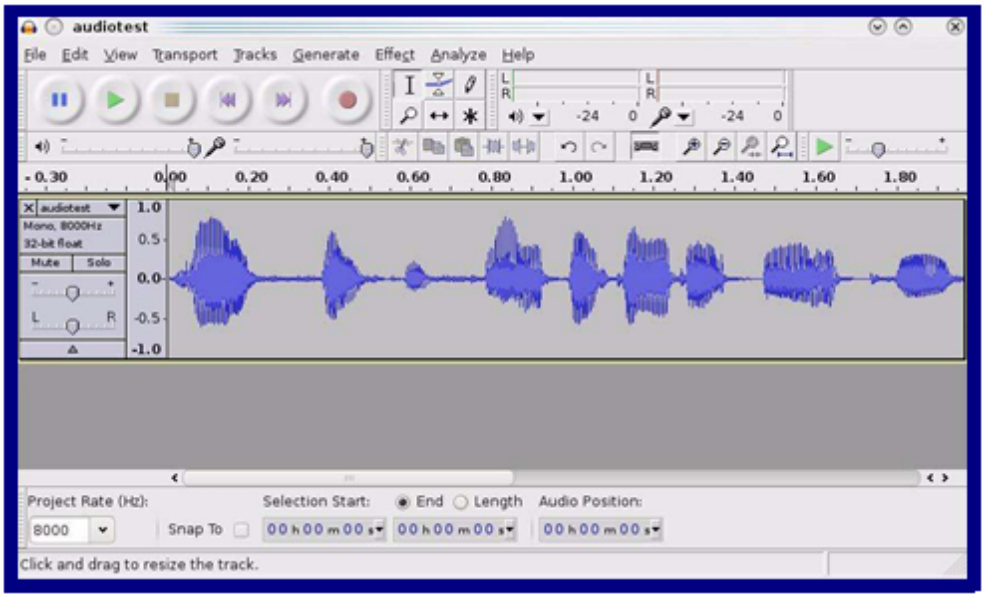

Figure 9 - Audacity 1

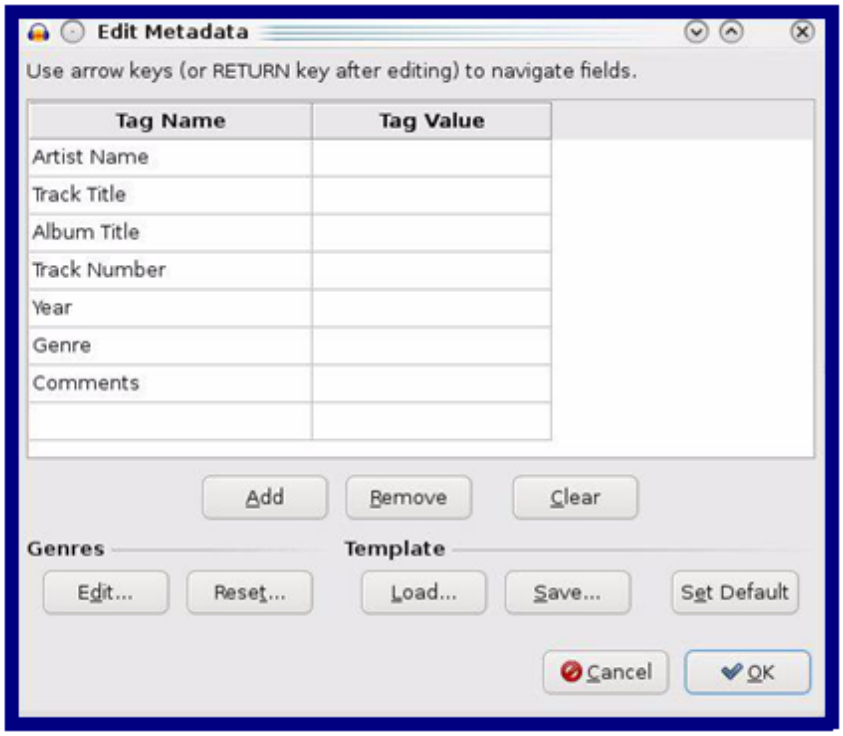

Figure 10 - Audacity 2

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

- WAV (Microsoft) signed 16 bit PCM.

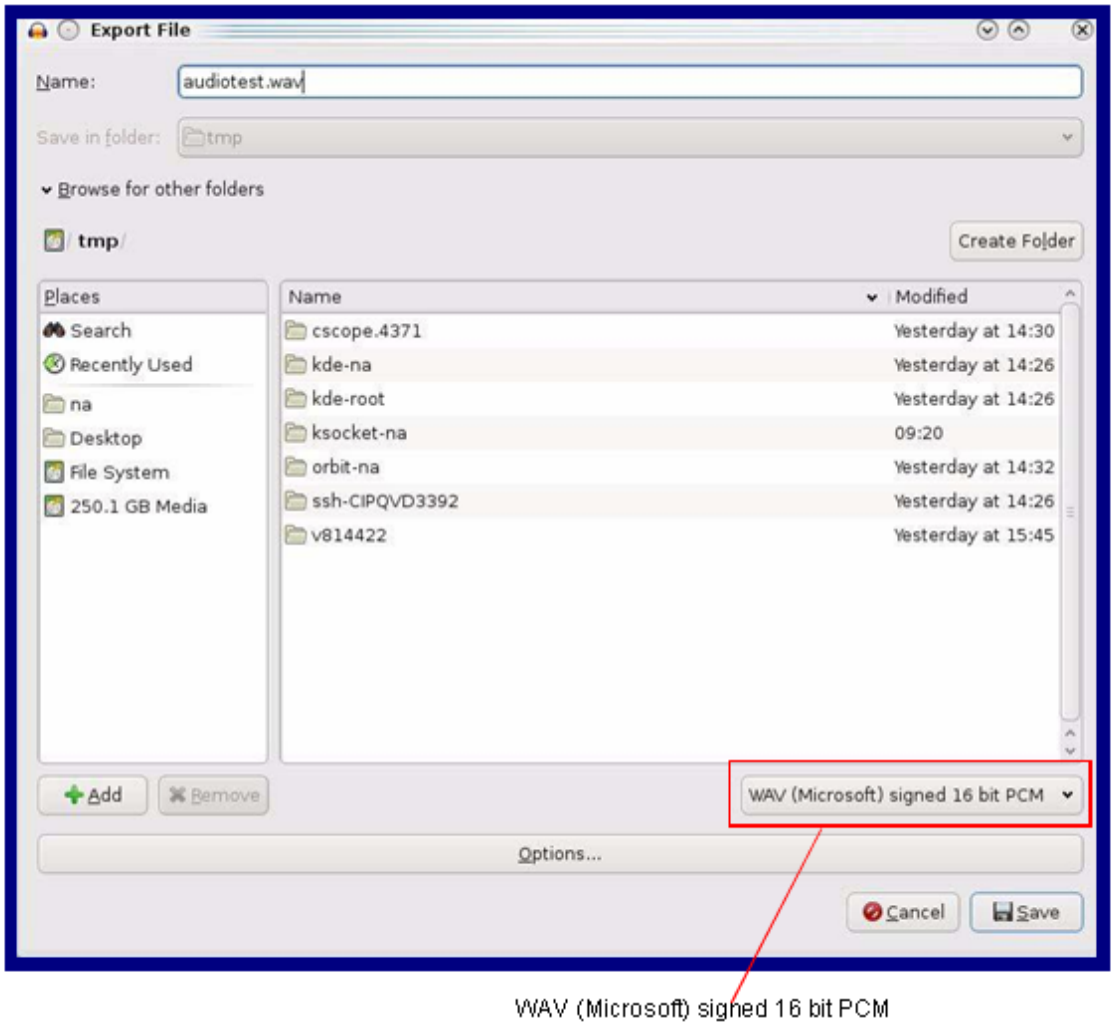

Figure 11 - WAV (Microsoft) signed 16 bit PCM

6.8. Configure the Event Parameters

Click the Event Config button to open the Event Configuration page (Figure 12).

The Event Configuration page specifies a remote server that can be used to receive HTTP POST events when actions take place on the board.

Figure 12 - Event Configuration Page

Table 9 shows the web page items on the **Event Configuration** page.

Table 9 - Event Configuration

Web Page Item	**Description**
Enable Event Generation:	When this option is selected the device will initialize the event generation engine. This mechanism can be used to send xml formatted http POST packets to an external server in response to triggers in the operation of the device.
Remote Event Server	
Remote Event Server IP:	This is the address of the remote TCP server for receiving POST events. This field can accept addresses in dotted decimal notation or canonical names of up to 64 characters in length.
Remote Event Server Port:	The Remote Event Server Port is used to set the port number that the remote server is listening on.
Remote Event Server URL:	POST requests have to be sent to a target script at the given IP address. This field defaults to 'xml_engine' and can accept up to 127 characters.
Events	**Examples**
Enable Button Events:	When this option is enabled an event will be sent to the remote server every time a button is pressed. 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='GuardianVoIP Device' MAC='0020f70015b6'> <event>BUTTON</event> </cyberdata>
Enable Call Active Events:	When this option is enabled an event will be sent to the remote server when a call becomes active. 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='Guardian VoIP Device' MAC='0020f70015b6'> <event>CALL_ACTIVE</event> </cyberdata>
Enable Call Terminated Events:	When this option is enabled an event will be sent to the remote server when a call is terminated. 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='Guardian VoIP Device' MAC='0020f70015b6'> <event>CALL_TERMINATED</event> </cyberdata>

Enable Relay Activated Events:	When this option is enabled an event will be sent to the remote server when the relay is activated. 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='Guardian VoIP Device' MAC='0020f70015b6'> <event>RELAY_ACTIVATED</event> </cyberdata>
Enable Relay Deactivated Events:	When this option is enabled an event will be sent to the remote server when the relay is deactivated. 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='Guardian VoIP Device' MAC='0020f70015b6'> <event>RELAY_DEACTIVATED</event> </cyberdata>
Enable Ring Events:	When this option is enabled an event will be sent to the remote server when the device starts playing a ringtone. 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='Guardian VoIP Device' MAC='0020f70015b6'> <event>RINGING</event> </cyberdata>
Enable Night Ring Events:	When selected, there is a notification when the device receives a night ring. 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= 'Guardian VOIP Device' MAC='002 0f70015b6'> <event>NIGHTRINGING</event> </cyberdata>
Enable Power On Events:	When this option is enabled an event will be sent to the remote server when the device powers up. 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='Guardian VoIP Device' MAC='0020f70015b6'> <event>P0WER ON</event> </cyberdata>

Enable General Purpose Input 1:	When this option is enabled an event will be generated when a change is seen on the one of the opto-isolated input lines. 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='Guardian VoIP Device' MAC='0020f70015b6'> <event>INPUT1</event> </cyberdata>
Enable General Purpose Input 2:	When this option is enabled an event will be generated when a change is seen on the one of the opto-isolated input lines. 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='Guardian VoIP Device' MAC='0020f70015b6'> <event>INPUT2</event> </cyberdata>
Enable General Purpose Input 3:	When this option is enabled an event will be generated when a change is seen on the one of the opto-isolated input lines. 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='Guardian VoIP Device' MAC='0020f70015b6'> <event>INPUT3</event> </cyberdata>
Enable General Purpose Input 4:	When this option is enabled an event will be generated when a change is seen on the one of the opto-isolated input lines. 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='Guardian VoIP Device' MAC='0020f70015b6'> <event>INPUT4</event> </cyberdata>
Enable 60 Second Heartbeat Events:	When this option is enabled an event will be sent to the remote server every 60 seconds. 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='Guardian VoIP Device' MAC='0020f70015b6'> <event>HEARTBEAT</event> </cyberdata>
Save	Click the **Save** button to save your configuration settings. **Note**: You need to reboot for changes to take effect.
Test Event	Click Test Event to test the event.
Reboot	Click on the **Reboot** button to reboot the device.

6.9. Configure the Autoprovisioning Parameters

1. Click the Autoprovisioning button to open the Autoprovisioning Configuration page (Figure 13).

Figure 13 - Autoprovisioning Configuration Page

2. On the **Autoprovisioning Configuration** page, you may enter values for the parameters indicated in Table 10.

Auto-Provisioning:

Every phone that needs auto-provisioning has to have its auto-provisioning file set up.

The auto-provisioning of a HDE-VoIP phone is done as follows:

1. Copy an auto-provision template of the phone from Guardian's website. **Make sure that the template is for the HDE-VoIP emergency phone.**
2. Open and edit the template to change the features of the phone.
3. Save and rename the file using its MAC address with a file extension of .config.

For instance: The phone has a MAC address of 00:20:f7:01:0f:22.

The auto-provisioning file of this particular device/phone must be saved as 0020f7010f22.config.

Follow the instructions in the Guardian Discovery tool program to complete the auto-provisioning of a VoIP phone.

The Autoprovisioning Template may be downloaded from Guardian's website at www.guardiantelecom.com - APTemplate.xml

Web Page Item	Description
Autoprovisioning	
Enable Autoprovisioning:	When this option is enabled, the device will try to fetch an autoprovisioning file from a remote server.
Get Autoprovisioning from DHCP:	When this option is enabled, the device will fetch its autoprovisioning file from the server specified from the DHCP server.
Autoprovisioning Server (IP Address):	If the option to get autoprovisioning from DHCP is not enabled, the device will try to fetch its autoconfiguration file from this configured address. The field accepts a standard ipv4 address in dotted decimal notation.
Autoprovisioning Autoupdate (in minutes):	This field accepts numbers from 0-999999. If this field is set to 0, the autoprovisioning autoupdate is disabled. If this field contains anything other than 0 it will re-download its autoprovisioning file after the configured number of minutes and force the board to reboot if the new autoprovisioning file differs from the current file.
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 device.

Table 10 - Autoprovisioning Configuration Parameters

Figure 14 - Update Firmware Page

Web Page Item	Description
File Upload	
Firmware Version:	Shows the current firmware version.
Browse…	Select a firmware file on your system to load to the device.
Submit	Click on the **Submit** button to automatically upload the selected firmware, the device will automatically reboot.

Table 11 - Firmware Update Parameters

THIS PAGE INTENTIONALLY LEFT BLANK

6.10. Advanced Configuration (Debug) Page

In addition to the visible webpages (web based utility) there is a hidden page for advanced features and troubleshooting. This page is reached by manually changing the URL.

For example, to view the firmware update page the URL could show:

http://10.0.3.78/cgi-bin/upgrade.cgi (example)

Change the word **upgrade to debug:**

http://10.0.3.78/cgi-bin/debug.cgi (example)

Figure 15 - Advanced Configuration

Web Page Item	Description
Misc Config	
Debug Level (0-9, 9 = more verbose):	This changes the verbosity of the logging application status as it runs. Boards ship at level 3, though for troubleshooting problems tech support may ask you to set this at 9. A value of 0 will turn off all logging.
Disable Watchdog Timer:	When this option is enabled the internal watchdog timer responsible for resetting the board when the main application becomes unresponsive is disabled.
CS6422 Config	This section contains the programmable registers of the on board echo cancellation circuit. Do not touch these unless you know what you are doing.
Register (0 - 5):	Use these parameters to set up the six registers in the echo cancellation circuit.
Restore Defaults	This button restores the echo cancellation parameters to their factory default values.
Upgrade LCD/Keypad	
Select a file (and use Save to upload):	Navigate to the location of the file that you want to upload.
Browse…	Use the Browse button to navigate to the location of the file that you want to upload.
Upgrade	This button will let the user upgrade the LCD.
Logfiles	
Write logfile to RAM:	By default the device will keep a circular logfile in RAM.
Write logfile to Flash:	This option will allow you to write the logfile to serial flash for troubleshooting problems that reboot the board.
Available Space =	14.95mb
Get Application Log Button	This button will let the user download the current logfile.
Get Autoprovision File Button	This button will allow the user to download the autoprovisioning file downloaded by the device.
Remove Debug File Button	This button will erase the current logfile.
Restore Factory Defaults	
Restore Factory Defaults Button	This button will restore the factory default configuration (same as if the user pressed the RESET button on the PCB).
Erase Audio files Button	This button will restore all audio files to the factory default condition.
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 device.

Table 12 - Advanced Configuration

6.10.1. Reboot the Telephone

After a firmware download, the telephone will automatically initiate a reboot.
To manually reboot a Telephone, log in to the web page as instructed in Section 6.2, "Log in to the Configuration Home Page". Click on reboot on any of the active pages which provide that function.

7. Setting up a TFTP Server

Autoprovisioning requires a TFTP server for hosting the configuration file.

7.1. 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*

7.2. 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.

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.

8. Discovery Process

Apart from the main application, the device runs a process in the background that listens to discovery requests and can make changes to the network settings when requested by the client application.

8.1. Accessing webpage functionality without a browser

In addition to the web pages hosted by the internal web server, there is a headless HTML command interface. This command.cgi interface is meant to be used via scripting and can do things like trigger the relay, reboot the board, or start and stop calls.

The examples below use the free Unix utility wget but any program that can send authenticated http POST commands should work.

Device Action	HTTP Post Command
To trigger the relay (for the configured delay)	wget --user admin --password admin --post-data "test_relay=yes" "http://10.0.3.78/cgi-bin/command.cgi" > /dev/null
To cause the Device to place a call to extension 130	wget --user admin --password admin --post-data "call=130" "http://10.0.3.78/cgi-bin/command.cgi" > /dev/null
To terminate an active call	wget --user admin --password admin --post-data "terminate=yes" "http://10.0.3.78/cgi-bin/command.cgi" > /dev/null
To force the Device to reboot	wget --user admin --password admin --post-data "reboot=yes" "http://10.0.3.78/cgi-bin/command.cgi" > /dev/null
To play the test audio file	wget --user admin --password admin --post-data "test_audio=yes" "http://10.0.3.78/cgi-bin/command.cgi" > /dev/null
To cause the Device to speak it's IP address	wget --user admin --password admin --post-data "speak_ip_address=yes" "http://10.0.3.78/cgi-bin/command.cgi" > /dev/null

Table 13 - Command Interface Post Commands

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

8.2. RESET Switch

- The RESET switch is used to get the IP address of the device or reset to factory defaults.
- Press and release the RESET switch within a *5* second window and it will speak the IP address through the on board speaker.
- Press and hold the RESET switch for *5* seconds and it will indicate that it is restoring defaults and rebooting the board.

8.3. Testing the hardware

The hardware can be tested using a utility started manually in the debug console. This is called the **t test** because it is initiated by pressing the **t** button at the console.

The **t test** will show a menu that will change when the user presses buttons or activates inputs.

```
Testing Device with Keypad
Check LEDs and Relay are toggling
RESET switch:
Isolated input 1:
Isolated input 2:
Isolated input 3:
Isolated input 4:
Keypad:
On Hook
Press SPACE to quit
```

An example when the user **lifts the handset receiver:**

```
Testing Device with Keypad
Check LED5 and Relay are toggling
RESET switch:
Isolated input 1:
Isolated input 2:
Isolated input 3:
Isolated input 4:
Keypad:
Off Hook
Press SPACE to quit
```

When the user presses **key 2**:

```
Testing Device with Keypad
Check LEDS and Relay are toggling
RESET switch:
Isolated input 1:
Isolated input 2:
Isolated input 3:
Isolated input 4:
Keypad: 2
On Hook
Press SPACE to quit
```

- Every time the input changes, the output lines will toggle. So when the user presses the RESET switch, in addition to the change shown on the screen, the relay will trigger, the two optoisolated outputs will be driven, the LCD will be activated, the LCD will display a change, and the ringer will activate.
- In addition to the general IO, when the t test is started, the audio input and output are looped together.
- When the audio is looped back it replays anything picked up by the microphone out the on board speaker after a short delay.

9. Frequently Asked Questions

1. How do I update my firmware?

Extract the firmware file from Guardian's website at www.guardiantelecom.com.

2. For additional support or answers to questions not covered on this page, who should I contact?

Contact Guardian Telecom VoIP Technical Support.

3. When dialling the three-digit DTMF tone on the IP phone, I can hear the DTMF-tones coming out of the speaker of the VoIP device but there is no relay action. The relay works when using the relay test-button on the configuration software. How do I fix this?

Since the relay test button is working, it seems like the problem results from interfacing with the IP phone where the DTMF tone is generated. To resolve this problem verify that the DTMF tone on the phone is set to out-of-band.

4. I was able to register your device with our SIP server, but when I tried to enter a DTMF tone there was no function.

Make sure your SIP phone is set to 101 for the DTMF payload type (Out of Band RFC2833).

5. After a period of time, my device stops working or is unreachable.

This is a common problem when the re-registration time value is not set correctly.

On a Guardian VoIP device, you need to make sure that the re-registration time value (in minutes) is **less than** that is set on the IP-PBX server.

6. On an Asterisk-based VoIP SIP PBX system, the Guardian SIP Device status is "Busy" or "Unreachable". I have set up both the Guardian VoIP SIP device and the PBX extension information for the device. I can see the device on the network, am able to PING it, and can bring up the device web page with a browser. However, when I try to call it from a phone extension, I see the word "Busy" or "Unreachable" in the Asterisk log.

In the PBX setup page for the extension of the Guardian device, find the **Qualify=** value and change it to **NO**. If the **Qualify=** value requires a numeric value, then change it to **0**.

Note that on some Asterisk systems (such as **Intuitive Voice**) this value is called the **Heartbeat=** value. Set the **Heartbeat=** value to **NO**, and then save the settings.

Also, on the product's **SIP Setup** page, make sure that the **Register Expiration (minutes)** setting is set to less than **6** minutes (**5** minutes is good) because it needs to be a value less than the Asterisk default value of 6 minutes. Save the settings after changing the **Register Expiration (minutes)** setting.

7. What type of audio files can be uploaded into the device?

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

You can use the free utility 'Audacity' (http://audacity.sourceforge.net/) to convert audio files into a format the device can recognize.

When you export an audio file with this program, you can save the output as "WAV (Microsoft) signed 16 bit PCM."

8. On the V2 products, what happens during a firmware upload if the process gets corrupted?

To guard against failed firmware upgrades, units shipped from Guardian Telecom with V.0.0.29 feature a built-in "fail safe" mechanism.

The Device will store the "TFTP Server IP" and "New Filename" entered on the "Update Firmware" web page. If, during the boot process, the Device is unable to boot the firmware, it will attempt to download the stored image from the stored TFTP server.

9. I see in the electrical connection diagram in the users guide that there is a High PIV Ultra Fast switching diode. Do I need it and if so do you have a source?

This High PIV Ultra Fast switching diode prevents CEMF kick back from an intermediary relay coil when power is cut and the coil field collapses. You could use an On-Semi MUR105 diode or an IN4007, which is readily available.

Specifications Datasheet	
Digi-Key Part Ordering	Ordering Page

10. We have the Cisco 3550 switch and it looks like the unit is not able to negotiate the power with the switch. It keeps cycling over and over.

This happens because with default settings, the switch port is resetting power too quickly. Therefore, on the 3550 switch, on the switch port that the unit is attached to, please try adding the following CLI command:

power inline delay shutdown 20 initial 300

That should keep power supplied until the unit can boot up all the way.

11. The Guardian device connected to a Dell Powerconnect 3524P or 3548P port did not stay linked up. The device comes up, and then it goes down, and then it comes up cycling.

If connected to a Linksys SRW208MP switch, the Guardian device stays up.

Pantel, Cisco, or Linksys PoE endpoints all work on the Dell Powerconnect 3524P.

A user tried hard coding the switch speed/duplex and tried four different Dell Powerconnect 3524P switches. --- Check to make sure the Dell Powerconnect 3524P has flow control enabled on the port for the Guardian device to power up properly.

According to Dell:

Flow Control Support (IEEE 802.3X): Flow control enables lower speed devices to communicate with higher speed devices by requesting that the higher speed device refrains from sending packets. Transmissions are temporarily halted to prevent buffer overflows. For information on configuring Flow Control for ports or LAGs, see "**Defining Port Configuration**" or "**Defining LAG Parameters**" in the **Dell™ PowerConnect™ 35xx Systems User's Guide**.

12. I am unable to connect with the unit when it is plugged into a Cisco SLM 224P switch.

The cables or switch ports that you are connecting to are set in **switch** or **hub mode** instead of **endpoint stations**. The **MDIX** setting needs to be changed to **MDI** since Guardian VoIP products are end stations.

From the Cisco SLM 224P User Guide:

Change to MDI:

MDI / MDIX Displays the Media Dependent Interface (MDI) / Media Dependent Interface with Crossover (MDIX) status on the port. Hubs and switches are deliberately wired the opposite of the way end stations are wired, so that when a hub or switch is connected to an end station, a straight through Ethernet cable can be used, and the pairs are matched up properly. When two hubs or switches are connected to each other, or two end stations are connected to each other, a crossover cable is used to ensure that the correct pairs are connected. The possible field values are: - **MDIX** Use for hubs and switches. - **MDI** Use for end stations.

13. I have a Cisco 6513 switch. When I plug in a Guardian VoIP device, the device constantly reboots and will not register to the SIP server.

Adjust the switch power selection to **Power inline static**, as opposed to **Power inline dynamic**. This will allow the device to continuously receive 15.4W of power.

14. We have registered the device on Cisco Call Manager but are unable to register the device's Nightringer using the device's MAC address. How do I configure two extensions on Call Manager for the device?

Create a second directory number and user for the Nightringer extension. You may need to fudge a digit of the MAC Address so that Call Manager allows you to associate it to the new user. Be sure this MAC address does not match any other Guardian devices on your network.

10. Product Specifications

Category	
Ethernet I/F	10/100 MBPS
Protocol	SIP RFC 3261 Compatible
Power Input	802.3AF Compliant or 12-24Volts at 500mA PoE
Payload Types	G711, A-law and µ-law

Notes:

Model No.
Part No.
Serial No.
Date of Purchase

THIS PAGE INTENTIONALLY LEFT BLANK

Guardian Telecom Inc.
7552 - 10th Street N.E.
Calgary, Alberta, Canada T2E 8W1
Toll-free 1-800-363-8010
Phone (403) 258-3100
Fax. (403) 253-4967
www.guardiantelecom.com
E-mail: sales@guardiantelecom.com
(Click to open message box)

Industrial Communications Worldwide