



a division of Circa Enterprises Inc.

tough. trusted. true.



VoIP Telephones

HDE Setup & Configuration



APPLICABLE FOR FIRMWARE VERSION V3.9.2 OR LATER

P007451 Rev. K 211208 12/8/2021 11:54 AM

Ph: 403.258.3100 \ email:info@guardiantelecom.com \ www.guardiantelecom.com



VoIP Setup & Configuration P007451 Rev. K (applicable to firmware V3.9.2 Only!)**COPYRIGHT NOTICE:**

© 2021 Circa Enterprises Inc.
ALL RIGHTS RESERVED

This manual and the related materials are the copyrighted property of Circa Enterprises. No part of this manual or related materials may be reproduced or transmitted, in any form or by any means (except for internal use by licensed customers), without prior express written permission of Circa Enterprises. This manual, and the products, software, firmware, and/or hardware described in this manual are the property of Circa Enterprises provided under the terms of an agreement between Circa Enterprises and the recipient of this manual, and their use is subject to that agreement and its terms.

DISCLAIMER: Except as expressly and specifically stated in a written agreement executed by Circa Enterprises Circa Enterprises makes no representation or warranty, express or implied, including any warranty or merchantability or fitness for any purpose, with respect to this manual or the products, software, firmware, and/or hardware described herein. Circa Enterprises assumes no liability for damages or claims resulting from any use of this manual or such products, software, firmware, and/or hardware. Circa Enterprises reserves the right to make changes, without notice, to this manual and to any such product, software, firmware, and/or hardware.

OPEN SOURCE STATEMENT: Certain software components included in Guardian products are subject to the GNU General Public License (GPL) and Lesser GNU General Public License (LGPL) "open source" or "free software" licenses. Some of this Open Source Software may be owned by third parties. Open Source Software is not subject to the terms and conditions of the Circa Enterprises COPYRIGHT NOTICE or software licenses. Your right to copy, modify, and distribute any Open Source Software is determined by the terms of the GPL, LGPL, or third party, according to who licenses that software.

Software or firmware provided by Circa Enterprises that is unrelated to Open Source Software is copyrighted by Circa Enterprises, subject to the terms of Circa Enterprises licenses, and may not be copied, modified, reverse-engineered, or otherwise altered without explicit written permission from Circa Enterprises.

TRADEMARK NOTICE: Guardian Telecom and the Guardian Telecom logos are trademarks of Circa Enterprises, other product names, trademarks, and service marks may be the trademarks or registered trademarks of their respective owners.

Updating Your VoIP Product

Please review www.guardiantelecom.com support pages to obtain the latest F/W or contact Guardian Telecom Support at <mailto:rmateststation@guardiantelecom.com>

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
ALERTE GÉNÉRALE

Warning

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

Avertissement

De danger électrique : Ce produit doit être installé par un électricien agréé selon tous les codes électriques et du bâtiment.

Table of Contents

1.	Typical System Installation	6
2.	Supported Protocols	6
3.	Supported SIP Servers	6
4.	Features	7
5.	Getting Started	8
6.	Back-Up Server Modes	8
6.1.	Normal Operation (SRST/MITEL) Disabled	8
6.2.	Cisco SRST	8
6.3.	Mitel Resiliency	9
7.	RESET Switch	9
8.	Configure the Telephone Parameters	9
8.1.	Telephone Web Page Navigation	10
8.2.	Log in to the Configuration Home Page	11
8.3.	Configure the Device Parameters	13
8.4.	Configure the SIP Parameters	18
8.5.	Configure the Audio Parameters	23
8.5.1.	User-created Audio Files	25
8.6.	Configure the Event Parameters	27
8.7.	Configure the Autoprovisioning Parameters	30
8.8.	Configure Update Firmware	32
8.8.1.	Reboot the Telephone	32
9.	Setting up a TFTP Server	33
9.1.	In a LINUX Environment	33
9.2.	In a Windows Environment	33
10.	Frequently Asked Questions	34
11.	Product Specifications	36
12.	Appendix A Time Zone Settings	37

Figures

Figure 1 - Typical Installation	6
Figure 2 - Startup Screen	8
Figure 3 - Home Page	11
Figure 4 - Device Configuration Page	13
Figure 5 - Network Configuration Page	16
Figure 6 - SIP Configuration Page	18
Figure 7 - Audio Configuration Page	23
Figure 8 - Audacity 1	25
Figure 9 - Audacity 2	25
Figure 10 - WAV (Microsoft) signed 16 bit PCM	26
Figure 11 - Event Configuration Page	27
Figure 12 - Autoprovisioning Configuration Page	30
Figure 13 - Update Firmware Page	32

Tables

Table 1 - Factory Default Settings	9
Table 2 - Telephone Web Page Navigation.....	10
Table 3 - Home Page Overview	12
Table 4 - Device Configuration Parameters	15
Table 5 - Network Configuration Parameters	17
Table 6 - SIP Configuration Parameters.....	22
Table 7 - Audio Configuration Parameters	24
Table 8 - Event Configuration.....	29
Table 9 - Autoprovisioning Configuration Parameters	31
Table 10 - Firmware Update Parameters	32

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 all SIP Compliant hardware or cloud based servers.

Figure 1 illustrates how VoIP Telephones can be installed as part of a VoIP phone system.

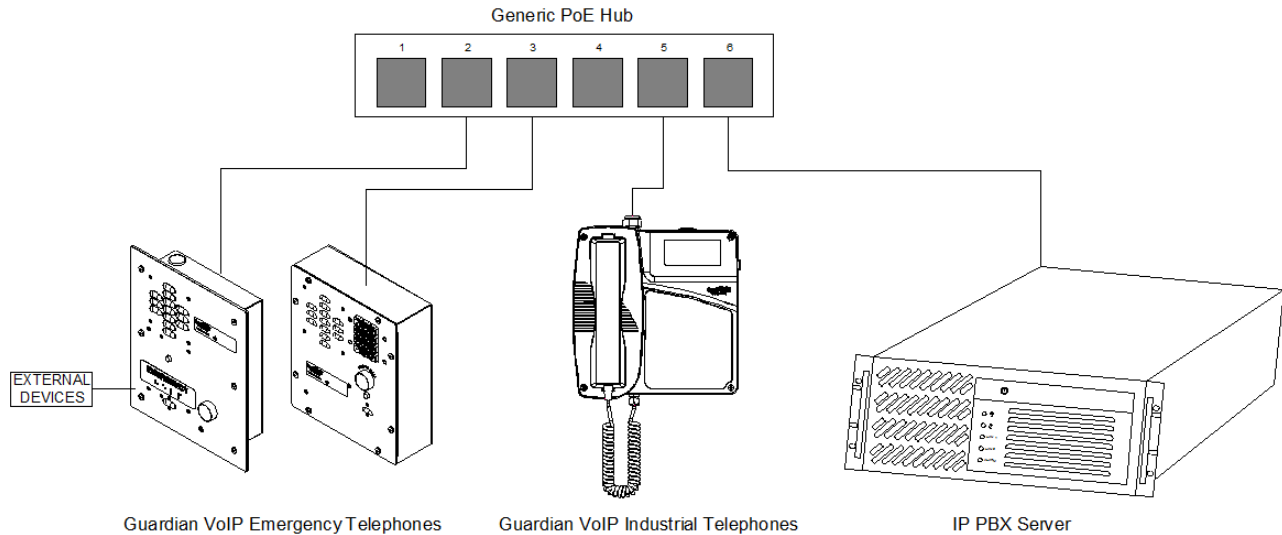


Figure 1 - Typical Installation

2. 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)
 - G.722.1 (SIREN 7)
 - G.722.2 (ANR-WB)
 - g.729 (729J & 729EV)

3. Supported SIP Servers

As a SIP device, this product will operate with all SIP Compliant hardware or cloud based servers. Contact Guardian Sales or Support on any interoperability questions. A list of formally tested compliant servers is available on the Guardian Website.

4. Features

Standard Features on All Models

- PoE 802.3af enabled (Power-over-Ethernet) or alternate power source.
- Control Relay – network configurable auxiliary relay.
- Compatible with SIP-based IP-PBX servers that comply with SIP RFC 3261.
- Network web management.
- Device Configuration Manager allows a significant operational list of features concerning the Auxiliary relay, LED functions, Audio setup and others.
- Guardian Discovery Utility makes it easy to detect, locate and launch the web based configuration screens.
- Product self-diagnostic testing available through web interface.
- Network adjustable volume and microphone sensitivity.
- Network downloadable firmware.
- Remote programming provides network management from a central location.
- Night ringer mode.

Single Button Units:

- Calls may be initiated from the phone or answered from the monitoring station.
- Can be used for Emergency or Information type applications.
- Single Push Button – depressing once automatically rings designated number to summon help. Use the Red Button Register in the SIP configuration to store the auto-dialed number.
- Integrated LED – provides visual confirmation of call status and connection, or can be configured alternatively through the Device Configuration.
- Doubles as a Paging Speaker when Auto-Answer is enabled.
- Auxiliary Relay can be programmed using several modes as required (*Note: Power limits*).
- Night ringer mode available.

Dual Button Units with / without Telephone keypad:

- Calls may be initiated from the phone or answered from the monitoring station.
- Can be used for Emergency AND Information type applications with a single unit.
- Separate button to designate for emergency and one for Information or to activate keypad (if equipped).
- Emergency Push Button – depressing once automatically rings designated number to summon help. Use the Red Button Register in the SIP configuration to store the auto-dialed number.
- Information Button – Depressing once to call an information operator. Use Blue button register in the SIP configuration to store this number.
- Keypad – If installed, leave Blue button register BLANK. Then if pushed, a dial tone will be heard and user can direct dial via the keypad.
- Integrated LED's (Qty. 2) – provides visual confirmation of call status and connection or can be configured alternatively through the Device Configuration.
- Doubles as a Paging Speaker when Auto-Answer is enabled.
- Auxiliary Relay can be programmed using several modes as required (*Note: Power limits*).
- Night ringer mode available.

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 at <https://www.guardiantelecom.com/resources/voip-support/> and needs to be installed manually by copying the executable file to a local drive.

To access a VoIP phone for programming:

- Copy 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".

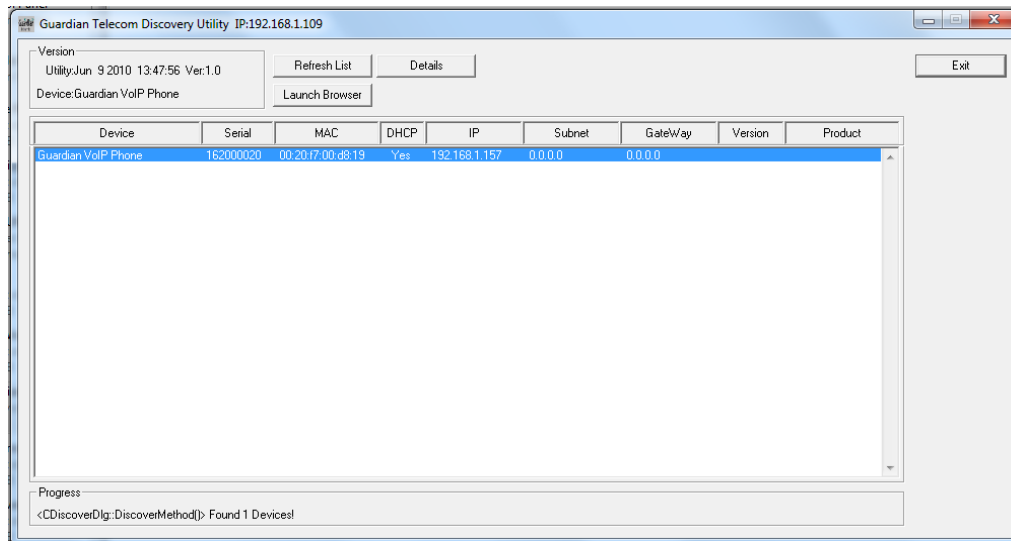


Figure 2 - Startup Screen

6. Back-Up Server Modes

6.1. Normal Operation (SRST/MITEL) Disabled

Guardian Normal Backup Process:

If the primary server fails, the phone will attempt to register automatically with backup #2, if that fails, it will try with backup #3. It will cycle through the servers until it registers or it will remain unregistered (if all servers off-line). Once the phone establishes a link to the back up, it will remain on that server until a forced reset occurs or the server it is on, kicks it out (reset or unregistration). Then the phone will re-attempt registration starting with the primary server.

If any of the above events occur and phone is not registered within 60 seconds of drop, and if the event mode is enabled for heartbeat the phone will issue out a XML notification.

6.2. Cisco SRST

Cisco Unified SRST functions in the remote-location router to automatically detect a failure in the network, initiate a process to provide call-processing backup redundancy for the IP phones in that location, and help ensure that the telephony capabilities stay operational. Upon restoration of WAN connectivity, the system intelligently and automatically shifts call processing back to the primary Cisco Unified Communications Manager cluster.

6.3. Mitel Resiliency

The Mitel Resiliency filter allows for seamless failover between two Mitel SIP servers without user intervention.

The device supports two levels of resiliency: Bronze and Silver.

Bronze:

The device supports multiple DNS records for a single FQDN. If the device fails to register with one server via an IP address associated with the FQDN's DNS record, it will try other IP addresses given. Alternatively, the DNS server can provide a single IP address for an FQDN if it is aware of the servers' statuses.

Silver:

While idle, the device will attempt to register with the primary Mitel SIP server ("Primary SIP Server" in the device's configuration). If the device fails to register with this primary server at any point, it will register with the secondary Mitel SIP server ("Backup SIP Server 1" in the device's configuration). The device will maintain registration with the secondary server, but will indefinitely attempt to re-register with the primary server. When the primary server comes back online, the device will unregister with the secondary server and go back to registering with the primary server. On first boot (or first registration), the time it takes for the device to failover to the secondary server is based on timers in the SIP RFC. Once the device has successfully registered with a (any) server, the time it takes for the device to failover to another server is based on the same timers as well as the SIP Re-registration Interval specified in the device's configuration. The device attempts to re-register with its SIP server at about 66% of the specified interval, which should result in downtime of no more than 75% of the specified interval.

When the device sends a SIP INVITE request, the device will start a timer ("Invite Timeout" in the device's configuration). If the SIP INVITE exchange is not successfully completed before this timer expires, the call will be aborted and the device will failover to the next server. The user will need to attempt the call again.

7. 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 more than 10 seconds until it indicates that it is restoring defaults and rebooting the board.

8. 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.

8.1. Telephone Web Page Navigation

Table 2 shows the navigation buttons that will be seen 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.
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

8.2. 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, the "Discovery Utility" can be used to detect all Guardian VoIP devices on the network. When opened refresh the Discovery Utility list to trigger the application to scan the network for 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 to five seconds, then release. 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.

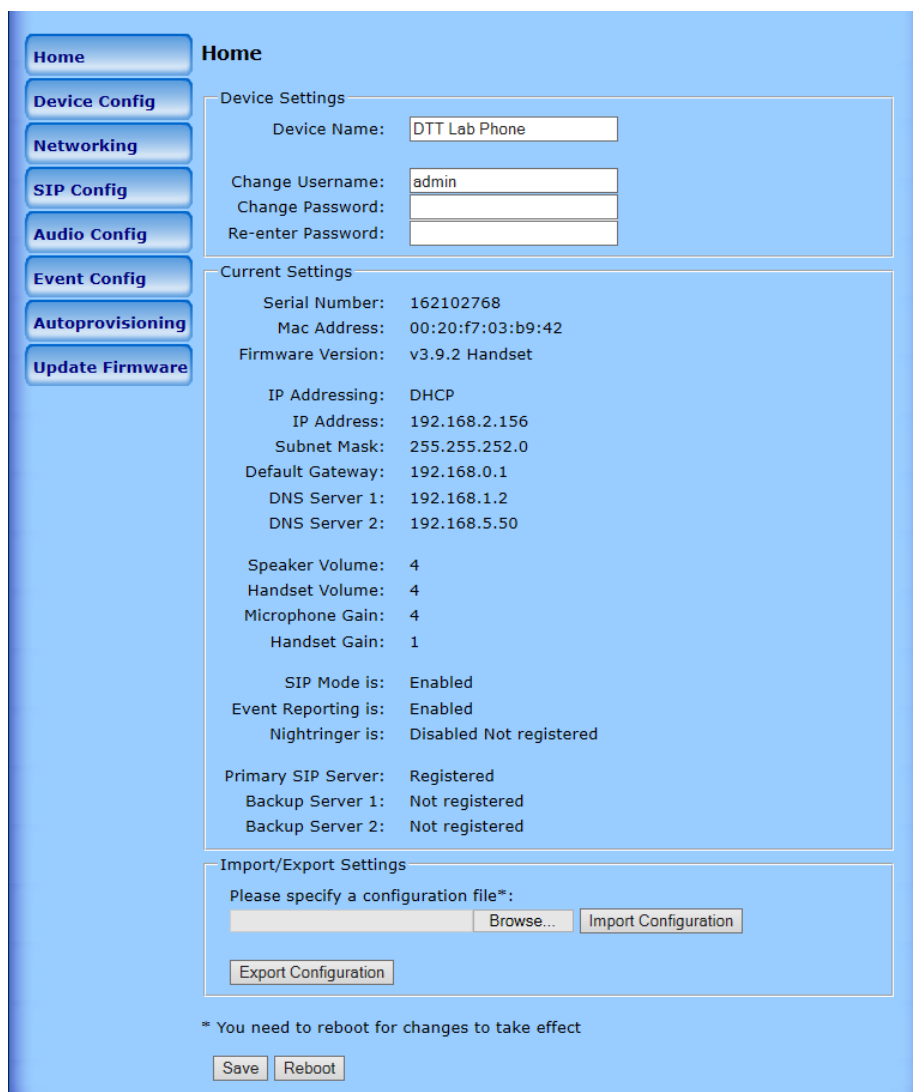
2. When prompted, use the following default **Web Access Username** and **Web Access Password** to access the **Home Page** (Figure 3):

Web Access Username: **admin**

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

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

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



Home

Device Settings

Device Name:

Change Username:

Change Password:

Re-enter Password:

Current Settings

Serial Number: 162102768

Mac Address: 00:20:f7:03:b9:42

Firmware Version: v3.9.2 Handset

IP Addressing: DHCP

IP Address: 192.168.2.156

Subnet Mask: 255.255.252.0

Default Gateway: 192.168.0.1

DNS Server 1: 192.168.1.2

DNS Server 2: 192.168.5.50

Speaker Volume: 4

Handset Volume: 4

Microphone Gain: 4

Handset Gain: 1

SIP Mode is: Enabled

Event Reporting is: Enabled

Nightringer is: Disabled Not registered

Primary SIP Server: Registered

Backup Server 1: Not registered

Backup Server 2: Not registered

Import/Export Settings

Please specify a configuration file*:

* You need to reboot for changes to take effect

Figure 3 - Home Page


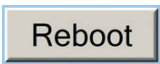
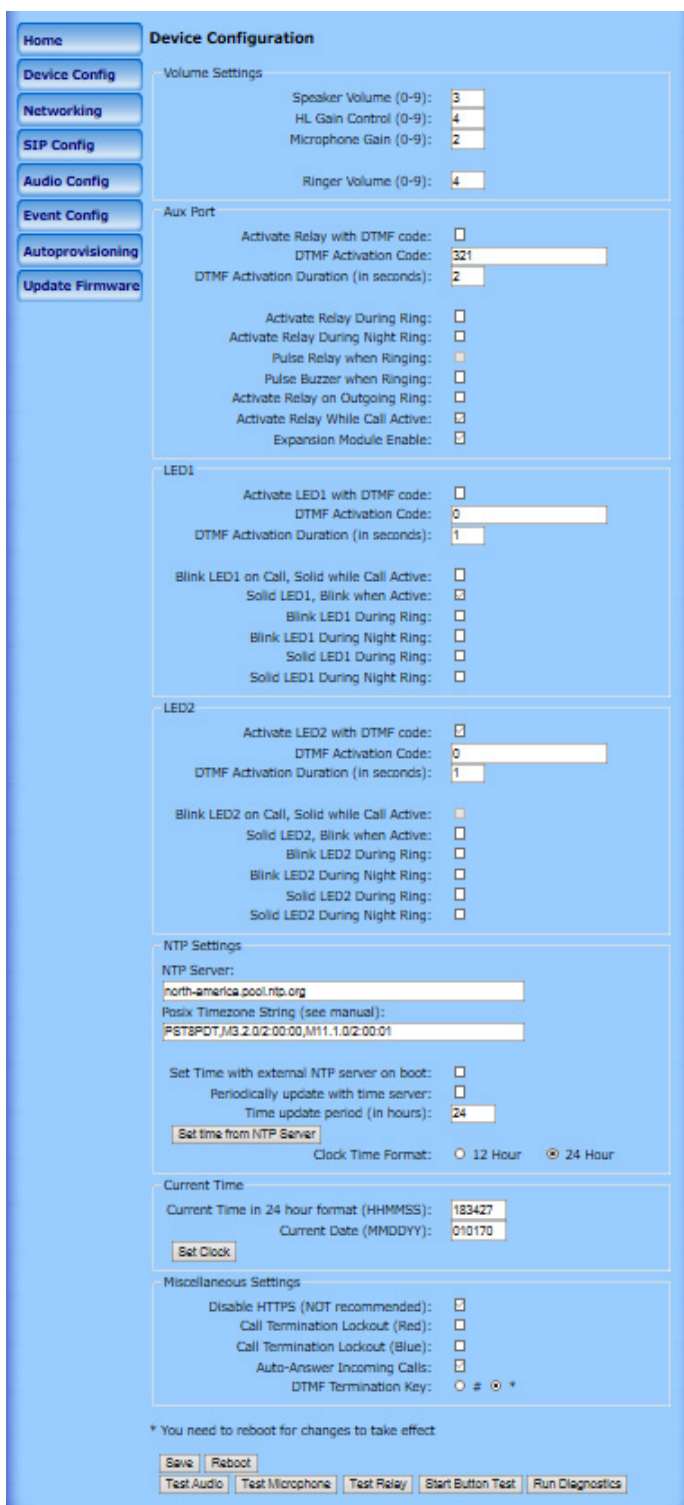
Web Page Item	Description
Device Settings	
Device Name:	Change the device name as required.
Change Username:	Type in this field to change the username.
Change Password:	Type in this field to change the password. <i>(Passwords can be up to 25 characters and can NOT contain the following special characters ; < > ' " % & special characters allowed include ! @ # \$ ^ * _ -)</i>
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"
LED1 / LED2 State:	This will indicate if LED is "Active" (on) or "Inactive" (off) – Useful when using toggle Mode (i.e.: DTMF enabled with timer set to "0" Zero seconds).
Import/Export Settings	
Choose File	Select a configuration file to import to the device.
Import Configuration	Click to import the selected configuration file. The configuration file allows the user to set up a custom default configuration for the VoIP products and import into multiple devices to save time.
Export Configuration	Click to export the current configuration to a file. The export file can then be used to confirm, share or modify and re-import back into the VoIP devices.
	Click the Save button to save the configuration settings. Note: You need to reboot for changes to take effect.
	Click on the Reboot button to reboot the device.

Table 3 - Home Page Overview

8.3. Configure the Device Parameters

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



Device Configuration

Volume Settings

Speaker Volume (0-9):

HL Gain Control (0-9):

Microphone Gain (0-9):

Ringer Volume (0-9):

Aux Port

Activate Relay with DTMF code: ☐

DTMF Activation Code:

DTMF Activation Duration (in seconds):

Activate Relay During Ring: ☐

Activate Relay During Night Ring: ☐

Pulse Relay when Ringing: ☐

Pulse Buzzer when Ringing: ☐

Activate Relay on Outgoing Ring: ☐

Activate Relay While Call Active: ☐

Expansion Module Enable: ☐

LED1

Activate LED1 with DTMF code: ☐

DTMF Activation Code:

DTMF Activation Duration (in seconds):

Blink LED1 on Call, Solid while Call Active: ☐

Solid LED1, Blink when Active: ☐

Blink LED1 During Ring: ☐

Blink LED1 During Night Ring: ☐

Solid LED1 During Ring: ☐

Solid LED1 During Night Ring: ☐

LED2

Activate LED2 with DTMF code: ☐

DTMF Activation Code:

DTMF Activation Duration (in seconds):

Blink LED2 on Call, Solid while Call Active: ☐

Solid LED2, Blink when Active: ☐

Blink LED2 During Ring: ☐

Blink LED2 During Night Ring: ☐

Solid LED2 During Ring: ☐

Solid LED2 During Night Ring: ☐

NTP Settings

NTP Server:

Posix Timezone String (see manual):

Set Time with external NTP server on boot: ☐

Periodically update with time server: ☐

Time update period (in hours):

Clock Time Format: ☐ 12 Hour ☒ 24 Hour

Current Time

Current Time in 24 hour format (HHMMSS):

Current Date (MMDDYY):

Miscellaneous Settings

Disable HTTPS (NOT recommended): ☐

Call Termination Lockout (Red): ☐

Call Termination Lockout (Blue): ☐

Auto-Answer Incoming Calls: ☐

DTMF Termination Key: ☐ # ☐ * ☐ *

* You need to reboot for changes to take effect

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 followed by **Reboot** to complete.

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.
Speaker Volume (0-9):	The speaker volume sets the default volume of the device on boot. Valid values are 0-9. Test the speaker volume using the 'Test Audio' button below.
HL Gain Control (0-9)	This is used in conjunction with the optional VoIP Extender Module w/Hearing Aid Loop amplifier. Only for units which are equipped with a Hearing Aid T-Coil Antenna.
Microphone Gain (0-9):	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.
Ringer Volume (0-9):	The ringing volume that is heard on the speaker of the phone. Valid values are 0-9. This setting is for units that use the speaker as a ringer. It will not affect units with a fixed buzzer.
Aux Port	
Activate Relay with DTMF Code:	When this option is enabled, the device will activate the relay when it receives a DTMF code (SIP or rfc2833).
DTMF Activation Code:	This 25-character field (Digits 0-9 only) can be used to set a DTMF code used to activate the relay. NOTE: the operator must press the "#" or "*" key after entering the code for it to be accepted.
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:	On in-coming calls...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 on Outgoing Ring	When enabled, once a push button is pressed, the relay will activate and remain activated until the call is answered. Then it will deactivate unless the "Activate Relay While Call Active" is also enabled.
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.
Expansion Module Enable	Check this feature when used with the Guardian Telecom VoIP Expansion Module. This activates the extended relay management features and hearing loop function when installed.
LED1 & LED 2 Control Setup	(LED1 shown, LED2 similar, "n" can stand for 1 or 2)
Activate LED1 with DTMF Code:	When this option is enabled, the device will activate Output Port 1 (Generally wired to the Emergency Button respective LED) when it receives a DTMF code (SIP or rfc2833).
Activate LED2 with DTMF Code:	When this option is enabled, the device will activate Output Port 2 (Generally wired to the Information or General Call Button respective LED) when it receives a DTMF code (SIP or rfc2833).
DTMF Activation Code:	This 25-character field (Digits 0-9 only) can be used to set a DTMF code used to activate the LED. NOTE: the operator must press the "#" or "*"key after entering the code for it to be accepted.
DTMF Activation Duration (in seconds):	When the LED 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 LED state indefinitely until the activation code is sent again.
Blink LEDn on Call, Solid while Call Active:	Active button – LED will flash on/off during call progress and remain on once call link is established.
Solid LEDn, Blink during ring & call	LED always on, blinks when button pressed and for duration of call.

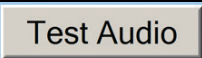

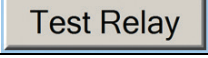

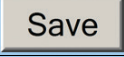
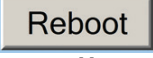
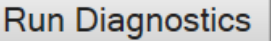
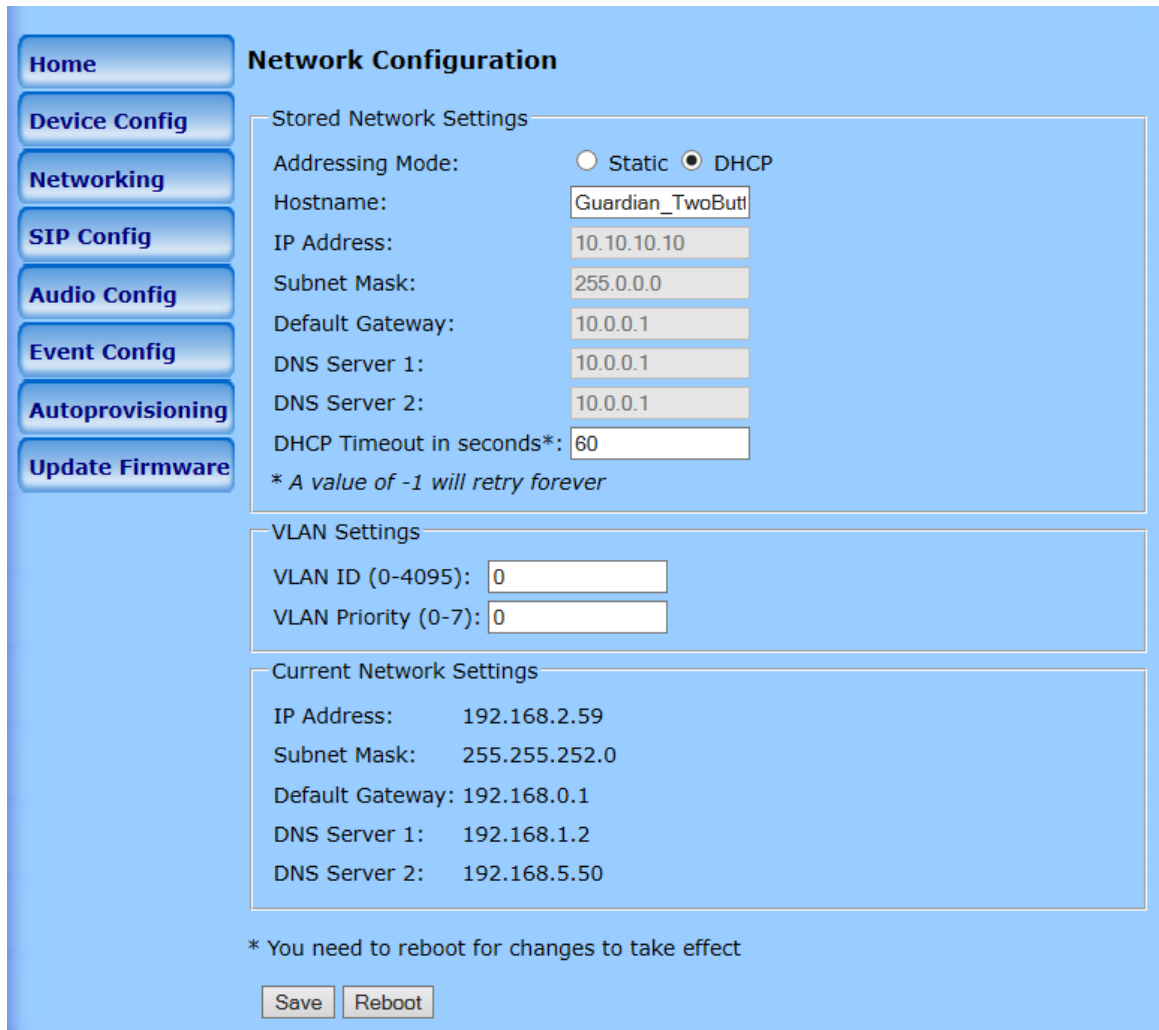
Blink LEDn During Ring:	LED for respective button will flash on receipt of call during device ringing.
Blink LEDn During Night Ring	When this option is enabled, the LED will activate and flash when the device has received a call and is playing a ringtone.
Solid LEDn During Ring:	LED activated during receipt of call and in ring mode.
Solid LEDn During Night Ring:	LED activated during receipt of call and in night ring mode.
NTP Settings	
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	Allows the device to access a local network based timeserver or a global internet server to allow the device to auto set/update the device clock. See Appendix A.
Set Time with external NTP server on Boot	When selected, the time is set with an external the NTP server when the device restarts.
Periodically update with time 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.
Set time from NTP Server	Clicking on this button will immediately set the time.
Current Time	
Current Time in 24 hour format (HHMMSS):	Allows you to input the current time manually. (6 character limit)
Current Date (MMDDYY):	Allows you to input the current date manually. (6 character limit)
Set Clock	Clicking on this button will immediately set the clock format.
Miscellaneous Settings	
Disable HTTPS (NOT recommended):	Disables the encrypted connection to the webpage. Depending on network security enable / disable as required.
Call Termination Lockout*:	When this option is enabled, a call cannot be terminated using the Emergency Call button.
Auto-Answer Incoming Calls	When selected, the device will automatically answer incoming calls. When Auto-Answer Incoming Calls is disabled, the device will play a ring tone (corresponds to Ring Tone on the Audiofiles page) out of the speaker, or the buzzer will sound until someone presses the Call button to answer the call or the caller disconnects before the call can be answered.
DTMF Termination Key	Key can be * or # as user chooses.
	This button will play an audio test message and can be used to test the volume level.
	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.
	This button will activate the relay for the DTMF activation Duration (in seconds).
	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.
	Click the Save button to save your configuration settings. Note: You need to reboot for changes to take effect.
	Click on the Reboot button to reboot the device.
<ul style="list-style-type: none"> You need to reboot for changes to take effect *Call termination lock out only applies to red button calls 	
	Click on this to run the new advanced diagnostics manually.

Table 4 - Device Configuration Parameters

Configure the Network Parameters

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



Network Configuration

Stored Network Settings

Addressing Mode: ☐ Static ☒ DHCP

Hostname:

IP Address:

Subnet Mask:

Default Gateway:

DNS Server 1:

DNS Server 2:

DHCP Timeout in seconds*:

* A value of -1 will retry forever

VLAN Settings

VLAN ID (0-4095):

VLAN Priority (0-7):

Current Network Settings

IP Address: 192.168.2.59

Subnet Mask: 255.255.252.0

Default Gateway: 192.168.0.1

DNS Server 1: 192.168.1.2

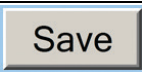

DNS Server 2: 192.168.5.50

* You need to reboot for changes to take effect

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.

Note: If changing from DHCP to STATIC Only: Once the reboot button has been selected, the webpage will show a countdown timer. The timer will hit zero and will reset and continue with countdown. At this point the web page can be shutdown and re-started. The web page will not automatically restart when switching from DHCP to STATIC.

Web Page Item	Description
Stored Network Settings	Shows the settings stored in non-volatile memory.
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 Table 1 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:	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 does not 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.
DHCP Timeout in seconds*: *A value of -1 will retry forever	Specify the desired time-out duration (in seconds) that the device will wait for a response from the DHCP server before reverting back to the stored static IP address. The stored static IP address may be the last known IP address or the factory default address if no prior DHCP lease was established. Enter up to 8 characters. A value of -1 will retry forever.
VLAN Settings	Shows the current VLAN settings.
VLAN ID (0-4095):	Specify the IEEE 802.1Q VLAN ID number. Enter up to 4 digits. Note: The device supports 802.1Q VLAN tagging support. The switch port connected to the device will need to be in "trunking mode" for the VLAN tags to propagate.
VLAN Priority (0-7):	Specify the IEEE 802.1p VLAN priority level. Enter 1 digit. A value of 0 may cause the VLAN ID tag to be ignored.
Current Network Settings	Shows the current network settings.
IP Address:	Shows the current Static IP address.
Subnet Mask:	Shows the current Subnet Mask address.
Default Gateway:	Shows the current Default Gateway address.
DNS Server 1:	Shows the current DNS Server 1 address.
DNS Server 2:	Shows the current DNS Server 2 address.
	Click the Save button to save your configuration settings. Note: You need to reboot for changes to take effect.
	Click on the Reboot button to reboot the device.

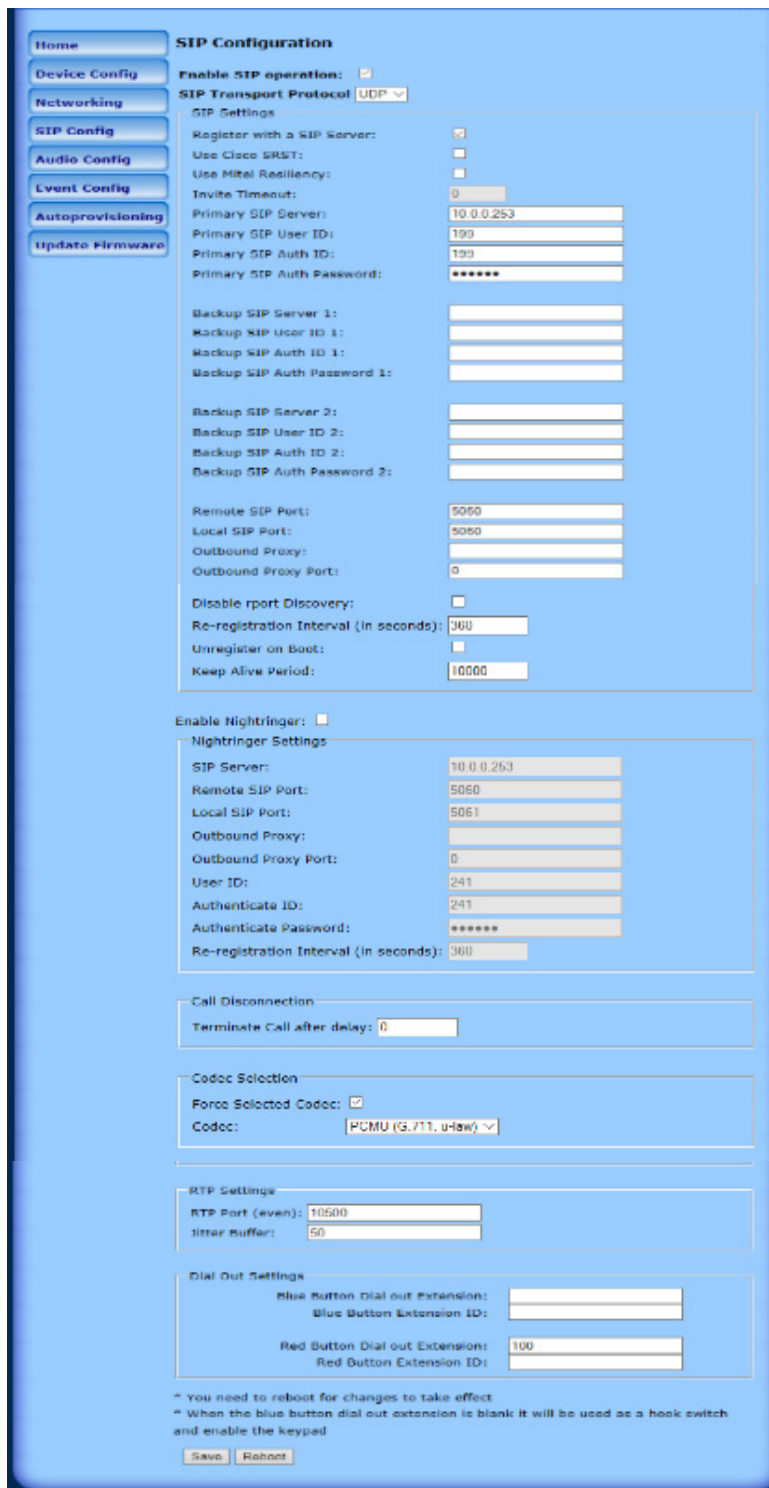
- You need to reboot for changes to take effect

Table 5 - Network Configuration Parameters

8.4. 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.



The screenshot displays the 'SIP Configuration' page with a sidebar menu on the left containing links: Home, Device Config, Networking, SIP Config (highlighted), Audio Config, Event Config, Autoprovisioning, and Update Firmware.

SIP Configuration

Enable SIP operation: ☒

SIP Transport Protocol: UDP ▾

SIP Settings

Register with a SIP Server: ☒

Use Cisco SRST: ☐

Use Mitel Resiliency: ☐

Invite Timeout: 0

Primary SIP Server: 10.0.0.253

Primary SIP User ID: 199

Primary SIP Auth ID: 199

Primary SIP Auth Password: *****

Backup SIP Server 1:

Backup SIP User ID 1:

Backup SIP Auth ID 1:

Backup SIP Auth Password 1:

Backup SIP Server 2:

Backup SIP User ID 2:

Backup SIP Auth ID 2:

Backup SIP Auth Password 2:

Remote SIP Port: 5060

Local SIP Port: 5060

Outbound Proxy:

Outbound Proxy Port: 0

Disable rport Discovery: ☐

Re-registration Interval (in seconds): 360

Unregister on Boot: ☐

Keep Alive Period: 10000

Enable Nightringer: ☐

Nightringer Settings

SIP Server: 10.0.0.253

Remote SIP Port: 5060

Local SIP Port: 5060

Outbound Proxy:

Outbound Proxy Port: 0

User ID: 241

Authenticate ID: 241

Authenticate Password: *****

Re-registration Interval (in seconds): 360

Call Disconnection

Terminate Call after delay: 0

Codec Selection

Force Selected Codec: ☒

Codec: PCMU (G.711, u-law) ▾

RTP Settings

RTP Port (even): 10500

Jitter Buffer: 50

Dial Out Settings

Blue Button Dial out Extension:

Blue Button Extension ID:

Red Button Dial out Extension: 100

Red Button Extension ID:

* You need to reboot for changes to take effect
 * When the blue button dial out extension is blank it will be used as a hook switch and enable the keypad

Save Reboot

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**

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 Transport Protocol	Allows user to select between SIP TCP or UDP mode.
SIP Settings	
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 .
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.
Use Mitel Resiliency:	When used with MITEL PBX with Mitel proprietary redundancy, this enables compliance operating mode for compatibility.
Invite Timeout:	When Mitel Resiliency is enabled, the device will use the "Invite timeout" value for outbound calls. The device will send an invite and if it does not get a response from the SIP server in <value> seconds, it will presume the server is down, cancel the call, and failover to the next server.
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.
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 report Discovery:	Disabling report 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.
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.
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.
Nightringer Settings	
SIP Server:	Enter the SIP server address as an IPv4 address in dotted decimal notation or a fully qualified domain name. This parameter also becomes the host portion of the SIP-URI for the device's Nightringer extension on the SIP server. This field can accept entries of up to 255 characters in length.

Remote SIP Port:	The Remote SIP Port is the port number the device will use as the destination port when sending SIP messages for the Nightringer extension. The default Remote SIP Port is 5060. The supported range is 0-65536. Enter up to 5 digits.
Local SIP Port:	The Local SIP Port is the port number the device will use to receive SIP messages for the Nightringer extension. This value cannot be the same as the Local SIP Port for the primary extension. The default Local SIP Port is 5061. The supported range is 0-65536. Enter up to 5 digits.
Outbound Proxy:	Enter the Outbound Proxy address as an IPv4 address in dotted decimal notation or a fully qualified domain name (FQDN). When an IP address is configured, the device will send all SIP messages to this IP address for the Nightringer extension. When an FQDN is configured, the device will run DNS NAPTR, SRV, and A queries on the FQDN to resolve an IP address to which it will send all SIP messages for the Nightringer extension. This field can accept entries of up to 255 characters in length.
Outbound Proxy Port:	The Outbound Proxy Port is port number used as the destination port when sending SIP messages to the outbound proxy for the Nightringer extension. A value of 0 will default to 5060. The supported range is 0- 65536. Enter up to 5 digits.
User ID:	Specify the SIP User ID for the SIP server. This parameter becomes the user portion of the SIP-URI for the device's Nightringer extension. Enter up to 64 alphanumeric characters.
Authenticate ID:	Specify the Authenticate ID for the SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters.
Authenticate Password:	Specify the Authenticate Password for the SIP Server. This parameter is required for SIP registration authentication. Enter up to 64 alphanumeric characters. Re-registration Interval (in seconds).
Re-registration Interval (in seconds):	The SIP Re-registration Interval (in seconds) is the SIP Registration lease time, also known as the expiry. The supported range is 30-3600 seconds. Enter up to 4 digits.
Call Disconnection	
Terminate Call after delay:	Automatically terminate an active call after a given delay in seconds. A value of 0 will disable this function. Enter up to 8 digits.
Codec Selection	
Force Selected Codec:	When selected, 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 a desired Codec in the drop-down list.
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.
Dial Out Settings	
Blue Button Dial out Extension:	Specify the extension the device will call when someone presses the blue Call button. Enter up to 64 alphanumeric characters.
Blue Button Extension ID:	A Caller identification string added to outbound calls. Enter up to 64 alphanumeric characters.



Red Button Dial out Extension:	Specify the extension the device will call when someone presses the red Emergency Call button. Enter up to 64 alphanumeric characters.
Red Button Extension ID:	A Caller identification string added to outbound calls. Enter up to 64 alphanumeric characters.
	Click the Save button to save your configuration settings. Note: You need to reboot for changes to take effect.
	Click on the Reboot button to reboot the device.
<ul style="list-style-type: none"> • You need to reboot for changes to take effect • When the blue button dial-out extension is blank, it will be used as a hook switch and enable the keypad. 	

Table 6 - SIP Configuration Parameters

8.5. Configure the Audio Parameters

1. Click **Audio Config** to open the **Audio Configuration** page (Figure 7).

Audio Configuration

Available Space = 36.19MB

Audio Files

01: Currently set to default
New File: Browse...
Play Delete Save

1: Currently set to default
New File: Browse...
Play Delete Save

2: Currently set to default
New File: Browse...
Play Delete Save

3: Currently set to default
New File: Browse...
Play Delete Save

4: Currently set to default
New File: Browse...
Play Delete Save

5: Currently set to default
New File: Browse...
Play Delete Save

6: Currently set to default
New File: Browse...
Play Delete Save

7: Currently set to default
New File: Browse...
Play Delete Save

8: Currently set to default
New File: Browse...
Play Delete Save

9: Currently set to default
New File: Browse...
Play Delete Save

Dot: Currently set to default
New File: Browse...
Play Delete Save

Audio test: Currently set to default
New File: Browse...
Play Delete Save

Page tone: Currently set to default
New File: Browse...
Play Delete Save

Your IP Address is: Currently set to default
New File: Browse...
Play Delete Save

Rebooting: Currently set to default
New File: Browse...
Play Delete Save

Restoring Default: Currently set to default
New File: Browse...
Play Delete Save

Ringback tone: Currently set to default
New File: Browse...
Play Delete Save

Ring tone: Currently set to default
New File: Browse...
Play Delete Save

Night Ring: Currently set to default
New File: Browse...
Play Delete Save

Figure 7 - 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 7.

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.

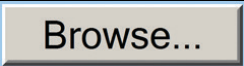
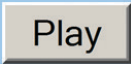
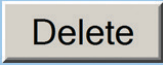
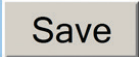
Web Page Item	Description
Audio Files	
0-9:	The name of the audio configuration option is the same as the spoken audio that plays on the board. '0' corresponds to the spoken word "zero." '1' corresponds to the spoken word "one." '2' corresponds to the spoken word "two." '3' corresponds to the spoken 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 "Guardian_Audio.wav 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.
	Click the Browse button to search for files.
	Click the Play button to hear the current message.
	Click the Delete button to empty the box.
	Click the Save button to save your settings.

Table 7 - Audio Configuration Parameters

8.5.1. 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 8 through Figure 10.

You may download the application at <https://creativecommons.org/licenses/by/3.0/>.

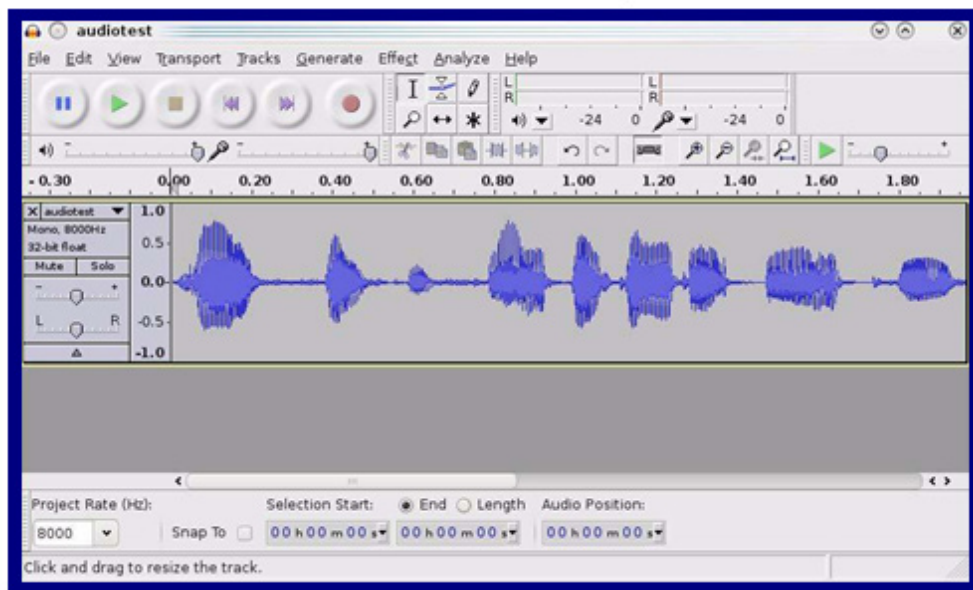


Figure 8 - Audacity 1

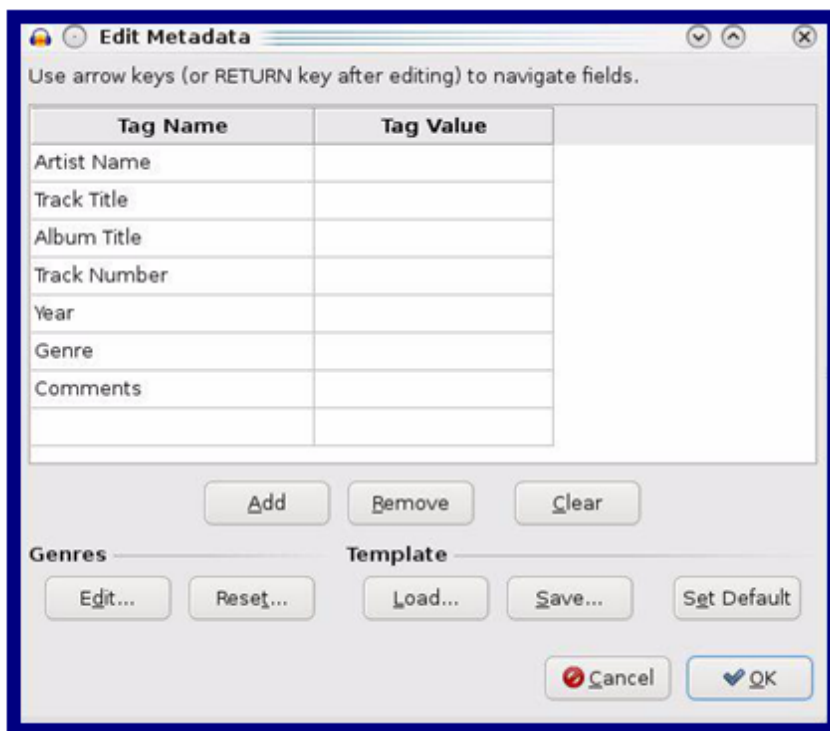
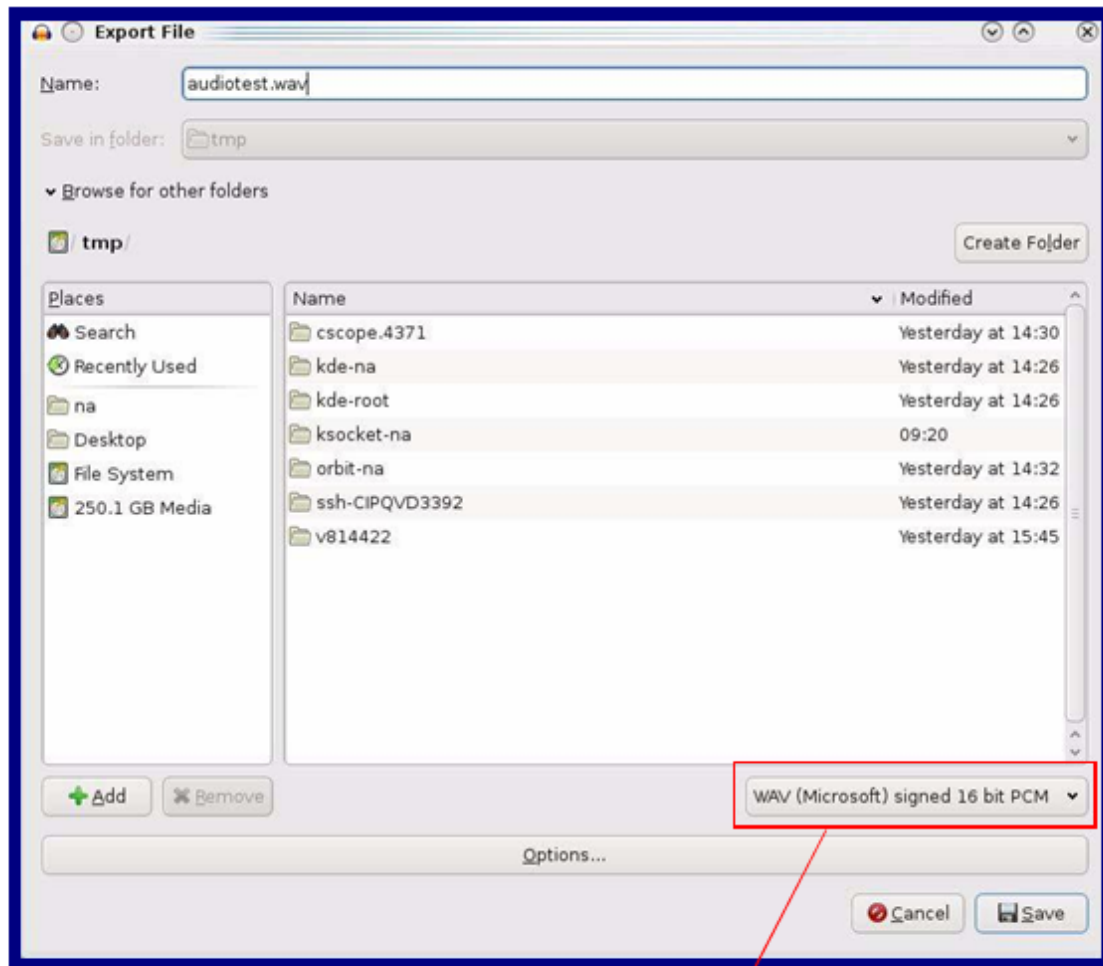


Figure 9 - Audacity 2

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

- WAV (Microsoft) signed 16 bit PCM.



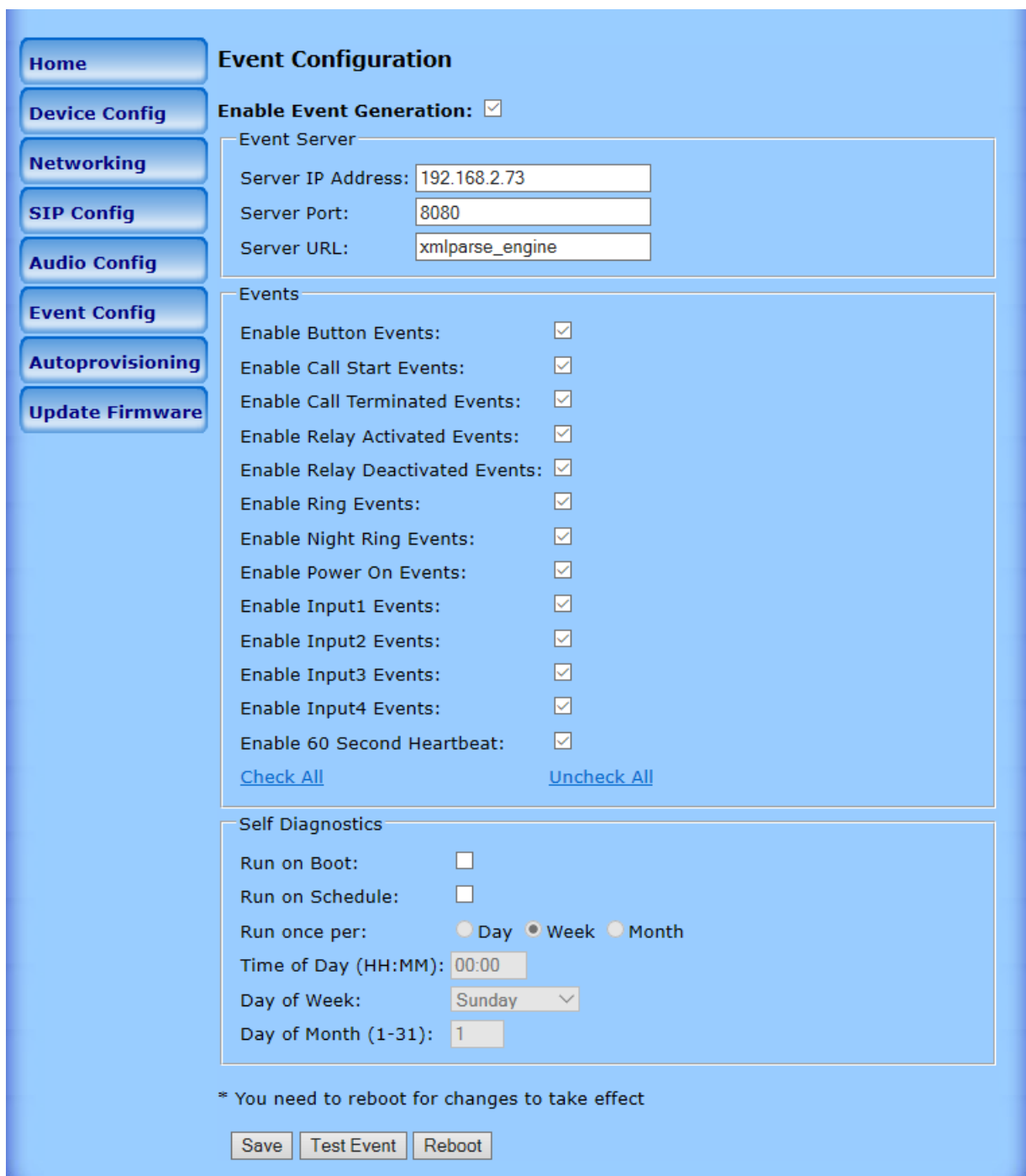
WAV (Microsoft) signed 16 bit PCM

Figure 10 - WAV (Microsoft) signed 16 bit PCM

8.6. Configure the Event Parameters

Click the Event Config button to open the Event Configuration page (Figure 11).

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



Event Configuration

Enable Event Generation: ☒

Event Server

Server IP Address:

Server Port:

Server URL:

Events

Enable Button Events: ☒

Enable Call Start Events: ☒

Enable Call Terminated Events: ☒

Enable Relay Activated Events: ☒

Enable Relay Deactivated Events: ☒

Enable Ring Events: ☒

Enable Night Ring Events: ☒

Enable Power On Events: ☒

Enable Input1 Events: ☒

Enable Input2 Events: ☒

Enable Input3 Events: ☒

Enable Input4 Events: ☒

Enable 60 Second Heartbeat: ☒

[Check All](#) [Uncheck All](#)

Self Diagnostics

Run on Boot: ☐

Run on Schedule: ☐

Run once per: ☐ Day ☒ Week ☐ Month

Time of Day (HH:MM):

Day of Week:



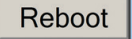
Day of Month (1-31):

* You need to reboot for changes to take effect

Figure 11 - Event Configuration Page

Table 8 shows the web page items on the **Event Configuration** page.

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.
Event Server	
Server IP Address:	This is the address of the iGuard Gateway if a custom developed monitor is used then this will reflect the IP 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.
Server Port:	The Remote Event Server Port is used to set the port number that the remote server is listening on.
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	Description (Note: For actual XML Messaging, contact Guardian Telecom)
Enable Button Events:	Check this box to trigger notification when a button is pressed.
Enable Call Start Events:	Triggered when the phone call processing is complete and a call is active.
Enable Call Terminated Events:	Triggered when the phone call is ended by placing the phone back on hook or when the receiving party terminates the call.
Enable Relay Activated Events:	This will trigger if an operator remotely activates the Aux Relay.
Enable Relay Deactivated Events:	Notification Trigger if the activated Aux Relay is cleared / Disabled.
Enable Ring Events:	Triggers when an incoming call is received.
Enable Night Ring Events:	If phone is in Night Ring mode a receiving call will trigger this event.
Enable Power On Events:	IF the phone is powered up for the first time or on each power cycle, on boot up of the operating system, the phone will initiate a Power On event notification.
Enable Sensor Events:	There are 4 input sensors that are optically coupled to accept input from devices such as intrusion switches, temp alarms, etc. For each of these should an event occur the appropriate notification will be sent out.
Enable 60 Second Heartbeat:	This will request the phone to send out a status of the phone heartbeat AND also indicate if the phone is still registered with the SIP Server.
Self-Diagnostics	Setup of Enhanced Diagnostics - Note results are verbally annunciated from the device speaker as well as transmitted as an XML if event monitoring is enabled.
Run on Boot:	If enabled, the diagnostics will automatically run every time the phone is rebooted. This is a useful setting for installers to verify operation.
Run On Schedule	If enabled, diagnostics can be setup to run automatically per the following:
Run Once Per:	Day, Week or Month can be setup as a period between auto run of diagnostics.
Time of Day:	Set the time diagnostics should run (Note input is 24Hr time)
Day of Week:	If set weekly period use this to set the desired day (will be grayed out if not enabled).

Day of Month:	Set the date of each month. Note if set to 31 and month has only 30 days, then test will run on 30 th .
	Click the Save button to save your configuration settings. Note: You need to reboot for changes to take effect.
	Click Test Event to test the event.
	Click on the Reboot button to reboot the device.

- You need to reboot for changes to take effect.

Table 8 - Event Configuration

8.7. Configure the Autoprovisioning Parameters

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. Create an auto-provision template of the phone.
 - Go to Import/Export Settings near the bottom of the page on the Home Page.
 - Select Export Configuration; the device will prompt with Save options.
 - Using an appropriate editor such as WordPad or XML modify the parameters of the file.
2. Open and edit the template to change the features of the phone.
3. Save and rename the file as desired with a file extension of .xml or .txt. For example, if the phone has a MAC address of 00:20:f7:01:0f:22 the auto-provisioning file of this particular device/phone could be saved as 0020f7010f22.xml.
4. Click the Autoprovisioning button to open the Autoprovisioning Configuration page (Figure 12).



Figure 12 - Autoprovisioning Configuration Page

On the **Autoprovisioning Configuration** page, you may enter values for the parameters indicated in Table 9.

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


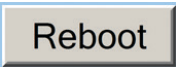
Web Page Item	Description
Autoprovisioning	
Disable Autoprovisioning:	When this option is enabled, the device will try to fetch an autoprovisioning file from a remote server.
Autoprovisioning Server:	When this option is enabled, the device will fetch its autoprovisioning file from the server specified from the DHCP server.
Autoprovisioning Filename:	Enter the Autoprovision file name that was generated with the Setup parameters.
Use tftp:	If using TFTP (instead of http) to download autoprovisioning files click the box.
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):	<p>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.</p> <p>Note: To use the auto update options, enable the Set Time with NTP Server on boot setting on the Device Configuration Page.</p>
Autoprovision at time (HHMMSS):	<p>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.</p> <p>Note: To use the auto update options, enable the Set Time with NTP Server on boot setting on the Device Configuration Page.</p>
Autoprovision when idle (in minutes > 10):	<p>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.</p> <p>Note: To use the auto update options, enable the Set Time with NTP Server on boot setting on the Device Configuration Page.</p>
Infinite Retries (Not Recommended):	Selected will try to get the AutoProvisioning file from provisioning server until the file is loaded.
	Click the Save button to save your configuration settings. Note: You need to reboot for changes to take effect.
	Click on the Reboot button to reboot the device.

Table 9 - Autoprovisioning Configuration Parameters

8.8. Configure Update Firmware

Click the Update Firmware button to open the Update Firmware page (Figure 13).

NOTE: IF UPDATING FROM PRE V3.9.0 REVIEW THE SUPPLIED FIRMWARE INSTALLATION DOCUMENT FIRST!!!

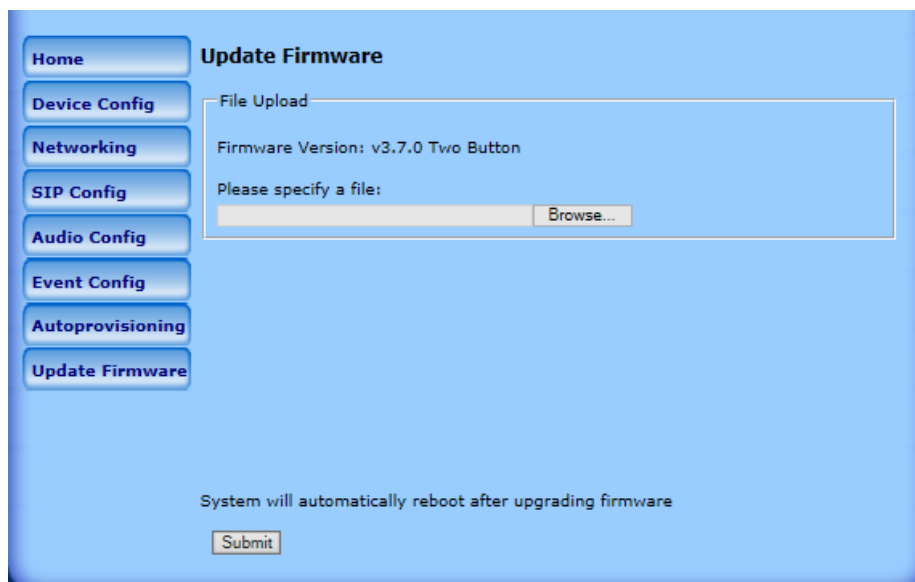


Figure 13 - Update Firmware Page

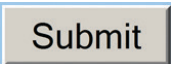
Web Page Item	Description
File Upload	
Firmware Version:	Shows the current firmware version.
Please specify a file	Select a firmware file on your system to load to the device.
	Click on the Submit button to automatically upload the selected firmware, the device will automatically reboot.

Table 10 - Firmware Update Parameters

8.8.1. 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 7.2, "Log in to the Configuration Home Page". Click on reboot on any of the active pages that provide that function.

9. Setting up a TFTP Server

Autoprovisioning requires a TFTP server for hosting the configuration file.

9.1. 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
```

9.2. 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.

10. Frequently Asked Questions

1. When I set my device network mode to “Static”, after I save and reboot the unit, the count down time continuously recycles and never exits.

Once the IP address is physically changed to static mode, the webscreen does not know to change addresses and will attempt to re-connect to the original IP address. The solution is to monitor the timer and after it hits 0:00 on the first cycle close the browser and use the discovery or open a new browser to the new IP address.

2. I have plugged my device into the network and it can be discovered but the web interface will not open up?

In some instances, when the device is initially plugged in, some of the registers may not be configured automatically with the correct data. Press and hold the device reset button for >10sec until the device announces that it is restoring factory settings. Wait approximately 1 min for the device to complete the reboot cycle and then retry.

3. I have plugged in my device to my network but the Discovery tool does not see the device.

There are several possibilities:

- Verify the device is powered up. You should see the Data/Ack LED's on the LAN connector on steady or blinking.
- Ensure that you wait approx. 45 secs for the boot up sequence to complete.
- Confirm your IP address – Press and hold reset button for approx. 2 seconds then release. The IP address will be announced through the hands free speaker or the handset earpiece.
- If IP address is returned as 10.10.10.10 then the device failed to reach the DHCP server and it reset the IP to factory default. – Verify network settings.
- Ensure multiple new devices were not added to network without pre-configuring the network settings – Static Network only!

4. How do I update my firmware?

1. Contact Guardian support at sales@guardiantelecom.com or at 1-800-363-8010 to obtain the most recent firmware version.
2. Extract the ulmage file to the computer that will be used to perform the update on the device.
3. With the HDE active on the network, open the web interface to the device you wish to update.
4. Go to the Update Firmware update page.
5. Browse for the new ulmage file.
6. Click Select to initiate the update process. The web timer will be displayed. Once the update is completed, the unit will return to the web interface.
7. Confirm version displayed on the web interface.

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

Contact Guardian Telecom VoIP Technical Support.

6. 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.

7. 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).

8. 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.

- 9. 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.

- 10. 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."


- 11. 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.

- 12. I see in the electrical connection diagram in the user's 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

- 13. 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.

- 14. 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 refrain 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**.

15. 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.

16. 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.

17. 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.

11. Product Specifications

Category	
Ethernet I/F	10/100 MBPS
Protocol	SIP RFC 3261 Compatible
Power Input	802.3AF Compliant or 24VDC @ 1A
Codecs Supported	G711, A-LAW and μ -LAW G722.1 (SIREN7) G722.2 (AMR-WB) G729.1 (G729J and G729EV)

12. Appendix A Time Zone Settings

The posix time zone string tells the internal date and time utilities how to handle daylight savings time for different time zones. Shown below are some common strings.

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.

Shown below is a breakdown of the parts that constitute the following time zone string:

- **CST6XXX,M3.2.0/2:00:00,M11.1.0/2:00:00**

Time Zone String Parts

Time Zone String	Meaning
Part	
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
XXX	Any three letters
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

More examples of time zone strings.

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, 1ST, 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.

Three or Four Character Time Zone Identifier

PST8PDT,M3.2.0/2:00:00,M11.1.0/2:00:00

Three or four character time zone identifier at the beginning of the time zone string.
 The identifier can be any three or four letters or number combination chosen by the user.

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

<http://www.timeanddate.com/time/dst>

More information about the GMT time in various time zones.

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	Brasília, Buenos Aries
GMT-2	Mid-Atlantic
GMT-1	Cape Verdes
GMT	Greenwich Mean Time
GMT+1	Berlin, Rome
GMT+3	Israel, Cairo
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

[illegible]



© Circa Enterprises 2021