Designed, Manufactured and Supported in the USA

VIKING
SECURITY & COMMUNICATION

PRODUCT MANUAL

E-32T Series
IP Intercoms with Secure SIP and Web UI
April 2, 2024

IP Intercoms with Secure SIP and Web UI

The **E-32T Series** of IP Intercoms are designed to provide reliable and secure voice communication for SIP VoIP phone systems. SIP over TLS and full SIPS provide a higher level of security and compatibility with SIP providers. The built-in Web User Interface allows for programming and configuration from any operating system with a web browser.

The **E-32T-SS-IP** intercoms can dial programmable numbers and be programmed remotely via a built-in Web UI. On-board 2 Amp relay contacts are provided for activating door strikes or gate controllers. The **E-32T-SS-IP** intercoms will flash the blue LED during dialing and automatically light the LED when the call is answered. All units are PoE class 2 powered.

For outdoor installations where the unit is exposed to precipitation or condensation, the **E-32T-SS-IP** intercoms are available with Enhanced Weather Protection (EWP). EWP products are designed to meet IP66 standards and may feature foam rubber gaskets, sealed connections, gel-filled butt connectors, as well as potted circuit boards. For more information on EWP, see DOD 859.

E-32T-SS-IP or
E-32T-SS-IP-EWP
Brushed Stainless Steel

E-32T-SS-IP or
E-32T-SS-IP-EWP
Shown in Optional VE-5x5 Surface Mount Box

Installation requires a Network Administrator / IT Technician

Features

- SIP compliant (see compatible IP-PBX Phone Systems / Service Providers)
- SIP Transport over TLS
- Plays user uploaded wave files for voice announcement or alert tone
- Remotely programmable via Web UI
- Optional Network Relay for Remote Relay Control (**RC-4A**)
- 2 Amp relay contacts for door/gate or optional **SL-2** strobe light (DOD 242)
- Blue backlit 316 stainless steel push button switch
- PoE powered (class 2, < 6.5 Watts)
- Network downloadable firmware
- T-10 Torx security screws for added security
- Handsfree operation
- Vandal resistant stainless steel prevents corrosion
- Laser etched graphics
- Cycles through backup phone numbers on busy or no-answer
- Optional Enhanced Weather Protection (EWP), EWP products are designed to meet IP66 Ingress Protection Rating (DOD 859)
- Optional SIPS (SIP Secure)
- Extended temperature range of -40° F to 140° F
- Available finishes: stainless steel
- Volume adjustments for microphone and speaker
- Flush mounts in a standard double gang electrical box (not included), or may be surface mounted using an optional **VE-5x5** Surface Mount Box (DOD 424)
- Diagnostics for testing microphone, speaker, and relay

Applications

- Gate Entrance
- Parking ramps/lots
- ATM machines
- Medical centers
- Lobbies
- Entryways
- Stadiums
- Convention centers
- Public access areas

www.VikingElectronics.com
Information: 715-386-8861

Specifications

Power: PoE class 2 (< 6.5 Watts)
Maximum Sound Pressure: 90 dB SPL @ 1m
Dimensions: 5" x 5" x 2.25" (127 mm x 127 mm x 57 mm)
Operating Temperature: -40° F to 140° F (-40° C to 60° C)
Humidity - Standard Products: 5% to 95% non-condensing
Humidity - EWP Products: Up to 100%
Audio Codecs: G711u, G711a, G722
Network Compliance: IEEE 802.3 af PoE, SIP 2.0 RFC3261, 1000BASE-T with auto cross over
Connections: (1) RJ45 100/1000 Base-T, (3) gel-filled butt connectors

(See page 5 for additional Specifications)

Table of Contents

1 - VoIP Compatibility

VoIP Compatibility List

On-Premise SIP Servers
3CX
FreePBX-Sangoma*
Freeswitch*
Grandstream 6104*
Grandstream 6202*
Mitel 3300
Kamailio
SIPStation
TekSIP

Cloud Based SIP Providers
Callcentric
FreePBX-Sangoma
Ring Central* (Kamailio 5.2)
sip.myviking.com (Viking Cloud SIP Server)
Voip.ms
Nextiva

SIP Endpoints for Video Calls
Linphone-Android
Linphone-Desktop
MicroSIP
Yealink Video Desk Phones
Zoiper Pro

Important: *Exclusion from this list means only that compatibility has not been verified, **it does not mean incompatibility**. If you have questions, please call Viking Electronics at 715-386-8861.*

2 - Definitions

Bitrate : The amount of video bits transferred per second. Higher values make for better video definition, but more bandwidth is consumed. Some systems may limit the maximum video bitrate.

Client: A computer or device that makes use of a server. As an example, the client might request a particular file from the server.

Codec (audio encoder/decoder): SIP audio Codecs convert the analog audio to/from digital audio that is sent in the SIP call. The Codec format that is used should be supported by the SIP server and all SIP devices involved in the VoIP call.

DHCP: Dynamic Host Configuration Protocol. In this procedure the network server or router takes note of a client's MAC address and assigns an IP address to allow the client to communicate with other devices on the network.

DNS Server: A DNS (Domain Name System) server translates domain names (ie: www.vikingelectronics.com) into an IP address.

Ethernet: Ethernet is the most commonly used LAN technology. An Ethernet Local Area Network typically uses twisted pair wires to achieve transmission speeds up to 1Gbps.

FPS : Frames Per Second. The number of video frames transmitted per second.

H.264: Video compression for high-definition digital video. Also known as MPEG -4 Part 10 or Advanced Video Coding (MPEG-4 AVC), H.264 is defined as a block-oriented, compensation based video compression standard the defines multiple profiles (tools) and levels (max bitrates and resolutions).

Host: A computer or device connected to a network.

Host Name: A host name is a label assigned to a device connected to a computer network that is used to identify the device in various forms of network communication.

Hosts File: A file stored in a computer that lists host names and their corresponding IP addresses with the purpose of mapping addresses to hosts or vice versa.

Internet: A worldwide system of computer networks running on IP protocol which can be accessed by individual computers or networks.

IP: Internet Protocol is the set of communications conventions that govern the way computers communicate on networks and on the Internet.

IP Address: This is the address that uniquely identifies a host on a network.

LAN: Local Area Network. A LAN is a network connecting computers and other devices within an office or building.

Lease: The amount of time a DHCP server reserves an address it has assigned. If the address isn't used by the host for a period of time, the lease can expire and the address can be assigned to another host.

MAC Address: MAC stands for Media Access Control. A MAC address, also called a hardware address or physical address, is a unique address assigned to a device at the factory. It resides in the device's memory and is used by routers to send network traffic to the correct IP address. You can find the MAC address of your **E-10/20/30/32-IP** phone printed on a white label on the top surface of the PoE LAN port.

MJPEG (Motion JPEG): A video encoding format in which each video frame or interlaced field of a digital video sequence is compressed separately as a JPEG image.

Multicast : This can refer to RTP Multicasting (audio only), or to RTSP (audio and video). One device is broadcasting a stream to multiple listening devices. A specific IP address and port are used.

Router: A device that forwards data from one network to another. In order to send information to the right location, routers look at IP Address, MAC Address and Subnet Mask.

RTP: Real-Time Transport Protocol is an Internet protocol standard that specifies a way for programs to manage the real-time transmission of multimedia data over either unicast or multicast network services.

RTSP (Real-Time-Streaming-Protocol): Application level network communication system that transfers real-time data from multimedia to an endpoint device by communicating directly with the server streaming the data.

Server: A computer or device that fulfills requests from a client. This could involve the server sending a particular file requested by the client.

Session Initiation Protocol (SIP): Is a signaling communications protocol, widely used for controlling multimedia communication sessions such as voice and video calls over Internet Protocol (IP) networks. The protocol defines the messages that are sent between endpoints, which govern establishment, termination and other essential elements of a call.

Static IP Address: A static IP Address has been assigned manually and is permanent until it is manually removed. It is not subject to the Lease limitations of a Dynamic IP Address assigned by the DHCP Server. The default static IP Address is: **192.168.154.1**

Subnet: A portion of a network that shares a common address component. On TCP/IP networks, subnets are defined as all devices whose IP addresses have the same prefix. For example, all devices with IP addresses that start with 100.100.100. would be part of the same subnet. Dividing a network into subnets is useful for both security and performance reasons. IP networks are divided using a subnet mask.

TCP/IP: Transmission Control Protocol/Internet Protocol is the suite of communications protocols used to connect hosts on the Internet. TCP/IP uses several protocols, the two main ones being TCP and IP. TCP/IP is built into the UNIX operating system and is used by the Internet, making it the de facto standard for transmitting data over networks.

TISP: Telephone Internet Service Provider

Video Payload: An integer between 96 and 127. This is used for the SDP (Session Description Protocol) to indicate the RTP Payload Type. H.264 and MJPEG video calls fall under the "Dynamic" payload type.

WAN: Wide Area Network. A WAN is a network comprising a large geographical area like a state or country. The largest WAN is the Internet.

Wireless Access Point (AP): A device that allows wireless devices to connect to a wired network using Wi-Fi, or related standards. The AP usually connects to a router (via a wired network) as a standalone device, but it can also be an integral component of the router itself.

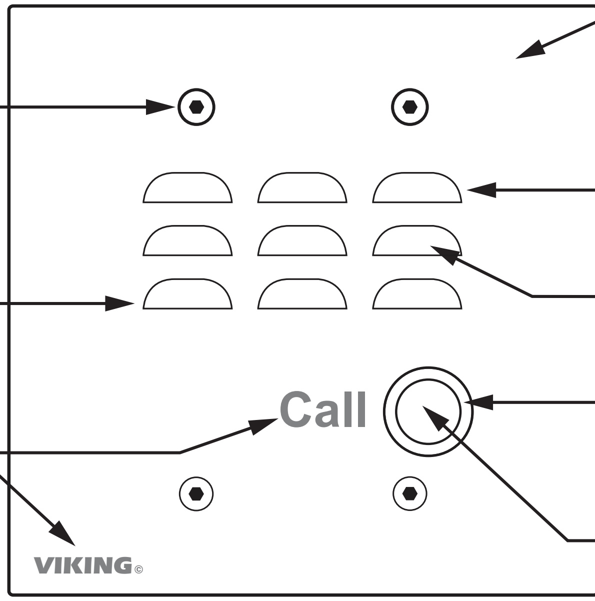
Wireless Repeater (Wireless Range Extender): takes an existing signal from a wireless router or access point and rebroadcasts it to create a second network. When two or more hosts have to be connected with one another over the IEEE 802.11 protocol and the distance is too long for a direct connection to be established, a wireless repeater is used to bridge the gap.

Front View of the E-32T

Mounting Screws: (4) 6-32 x 3/4" marine grade 316 stainless steel, flat head, T-10 Torx security screws and drive bit (included)

Speaker: Mylar speaker with rubber gasket to maintain water-tight seal and eliminate water deterioration.

Laser Etched Graphics: For long lasting easy to read graphics.



Faceplate: SS model is 18 gauge 316 stainless steel with a #4 brushed finish. BK and BN models are 14 gauge 304 stainless steel with a durable powder painted finish.

Microphone: Omni-directional microphone with protective water-resistant cloth.

Speaker Screen: Speaker screen with 0.018" wide slots to prevent punctures from paperclips, etc.

Blue LED: Lights steady to help locate the button in low light, flashes during dialing, then lights steady when answered.

Push Button Switch: Push to initiate call, push again to disconnect. Solid 316 stainless steel internally sealed per IP67.

Rear (PCB) View of E-32T

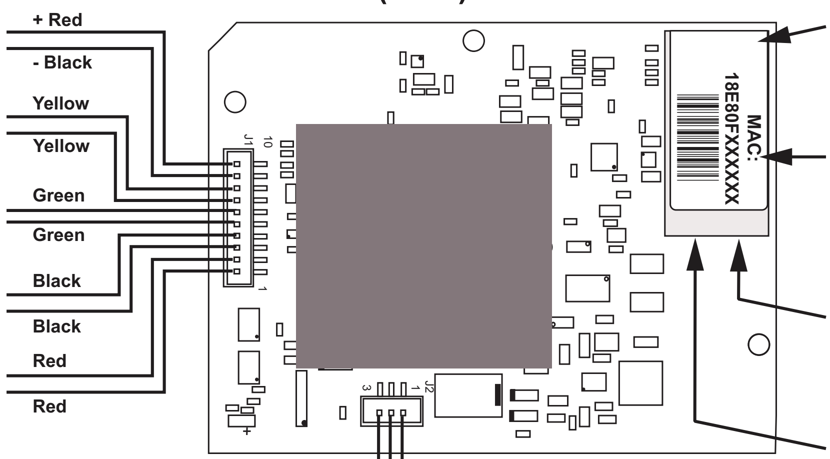
Microphone

Speaker

Request for Exit (REX Input)

Help Switch

LED



PoE LAN Port 10/100, PoE Class 2 (<6.5 Watts): Connect to your LAN via RJ45 plug and CAT5 or greater twisted pair wire.

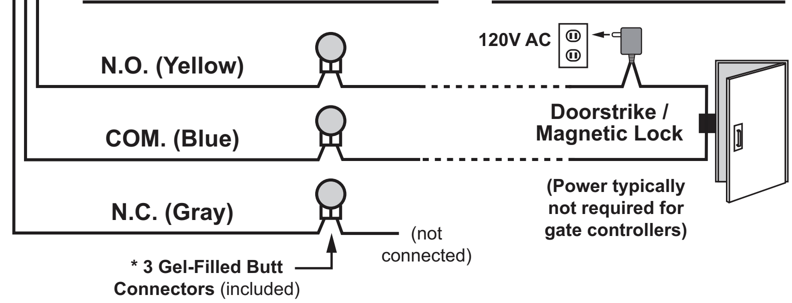
MAC Address Label: The MAC address is a unique 12 digit number used by routers to send network traffic to the correct IP address.

Yellow Network Status LED: Lights steady to indicate power and data link. Blinks to indicate network activity.

Green Unit Status LED

On-Board 2 Amp Relay Output Contacts
(2A@30VDC/ 250VAC maximum)

Connect to Optional Doorstrike, Mag Lock, Gate Controller, etc.



***Note:** The gel-filled (water-tight) butt connectors are designed for insulation displacement on 19-26 gauge wire with a maximum insulation of 0.082 inches. Cut off stripped wire ends before terminating.*

4 - Specifications

Intercom Specifications

Dimensions: 5” x 5” x 2.25” (127 mm x 127 mm x 57 mm)

Shipping Weight: XX lbs (XX kg)

E-32T-IP-SS Faceplate: 14 gauge 316 stainless steel with #4 brushed finish

Blue LED: Call connected LED lights steady to help locate the button in low light, flashes during dialing, then lights steady when answered.

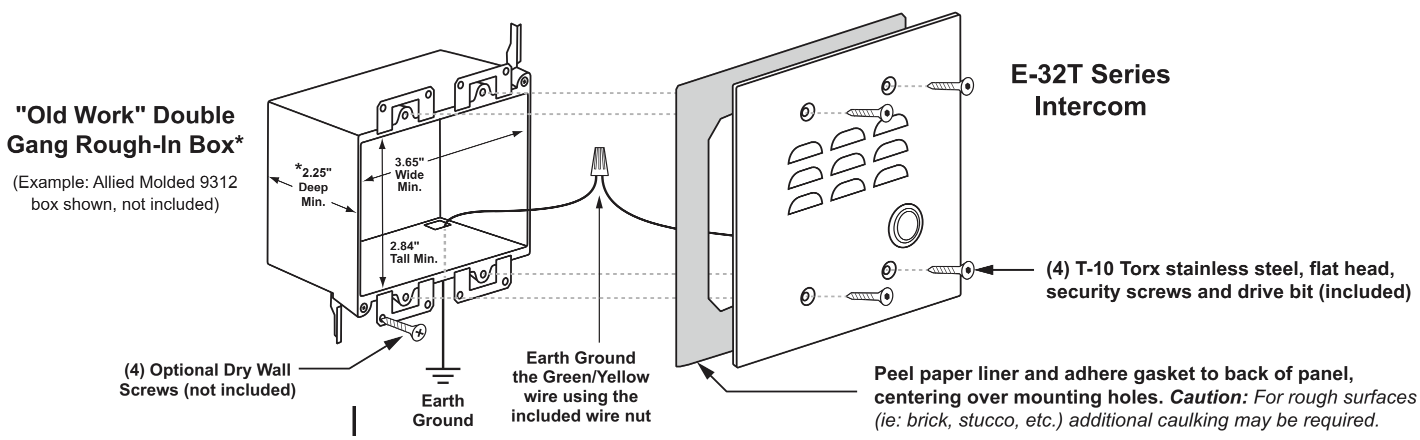
Mounting with Rough-In Box (not included): Flush mount to a standard double gang electrical box (recommended minimum internal dimensions: 3.65”W x 2.84”H x 2.25”D).

Mounting with Optional VE-5x5: Surface mount to walls, single gang boxes, double gang boxes, posts, or to a Viking **VE-GNP** Gooseneck pedestal.

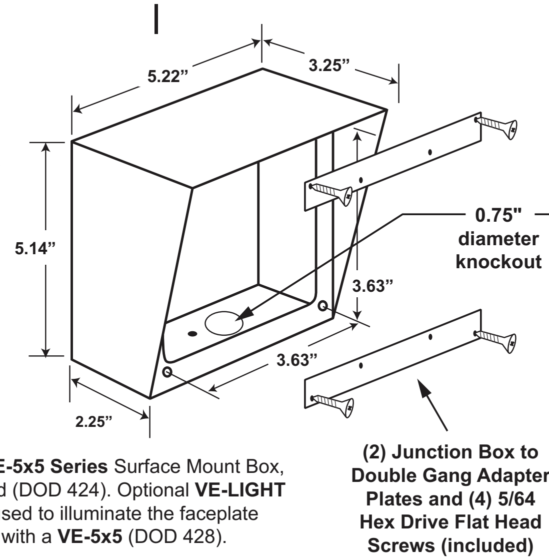
Optional Enhanced Weather Protection (EWP) Available: EWP products are designed to meet IP66 standards and may feature foam rubber gaskets, sealed connections, gel-filled butt connectors, as well as potted circuit boards with internally sealed, field-adjustable trim pots and DIP switches for easy onsite programming. For more information on EWP, see DOD 859.

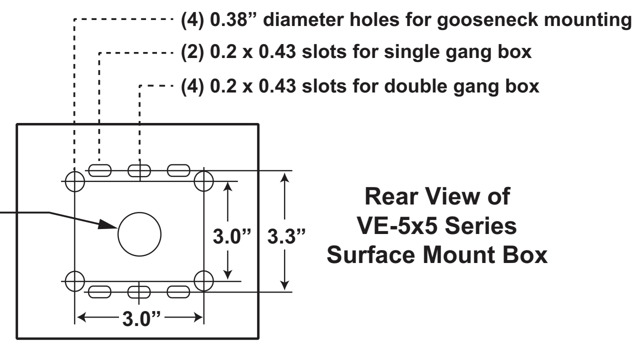
Note: *When mounting outside to rough or uneven surfaces (ie: brick, stucco, etc.) apply a bead of clear silicone caulking around the top edge and sides of faceplate.*

5 - Mounting



OR





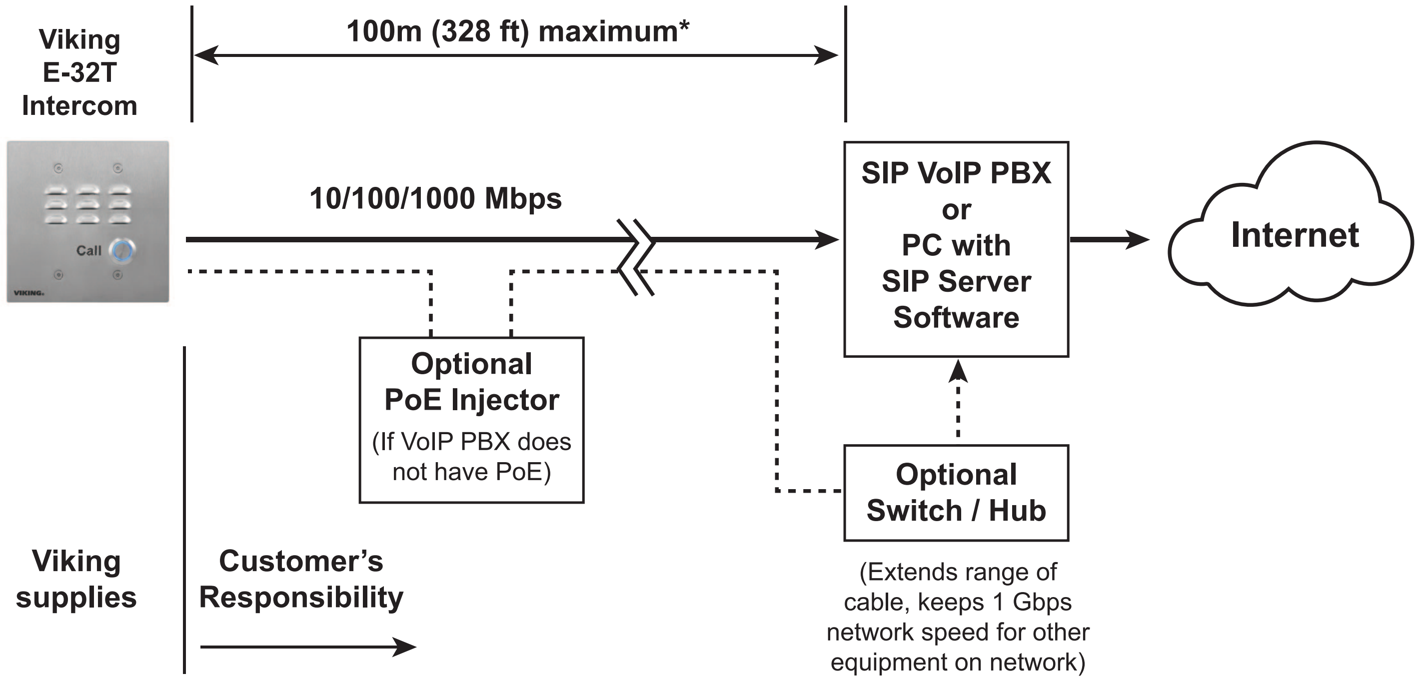
Optional **VE-5x5 Series** Surface Mount Box, not included (DOD 424). Optional **VE-LIGHT** kit can be used to illuminate the faceplate when used with a **VE-5x5** (DOD 428).

WARNING: Do NOT use a wet location box.

The optional **VE-5x5 Series** Surface Mount Boxes are designed to be surface mounted to a single gang box, double gang box, or **VE-GNP** Gooseneck Pedestal. For more information on the **VE-5x5 Series** and **VE-GNP**, see DOD 424.

*** CAUTION:** Excessive wire length and/or using a rough-in box with inadequate depth can apply force to the circuit board causing physical damage. Recommended minimum internal dimensions for rough-in box: 3.65”W x 2.84”H x 2.25”D.

6 - Typical Installation on SIP Based VoIP Phone System



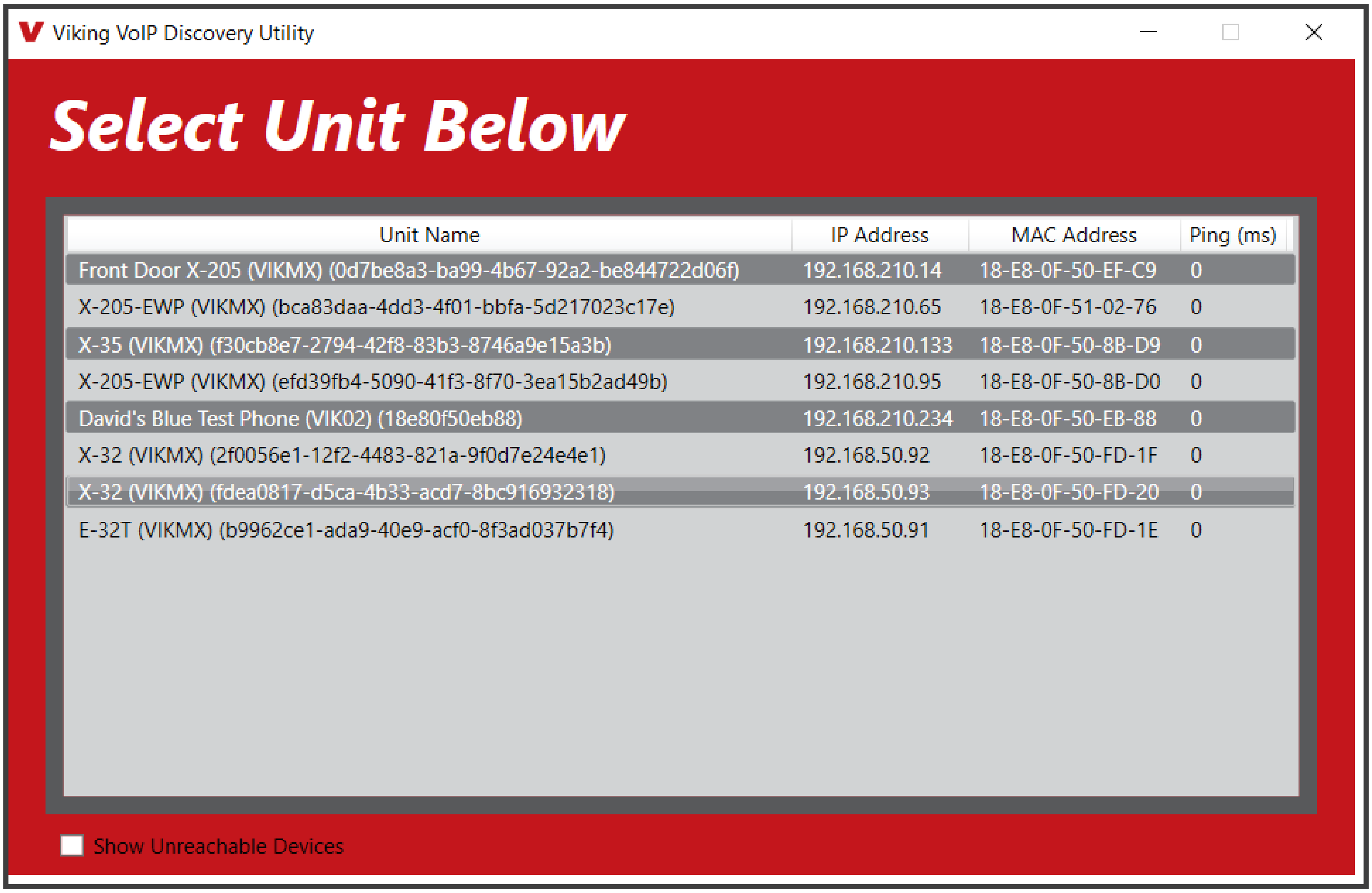
*** Note:** *A PoE extender can be used for an additional 100 meters per extender. For longer runs (up to 2 km / 1.2 miles) an ethernet to fiber media converter can be used.*

7 - Network Infrastrusture Requirements

- 10/100 or 1 Gbps network connection with PoE (Class 2)
- Ethernet Cable: Cat 5e or greater
- Browser for accessing the X-35 Web UI for Programming. Supported browsers: Chrome, Firefox, Opera, and Konquerer
- Computer with X-Series Discovery Utility (to find the unit's IP address for UI access).
- Viking VoIP Discovery Utility Software
  Download here: https://vikingupgradeserver.com/_install/X-Discovery.zip

8 - Initial Set-up

Install and run the **Viking VoIP Discovery Utility** software. **E-32T-SS-IP** units on the same LAN will show up with their IP addresses. Double-click on a unit to open the Web UI in your default browser. Once your IP address is known, you can open the Web UI in a smartphone browser.



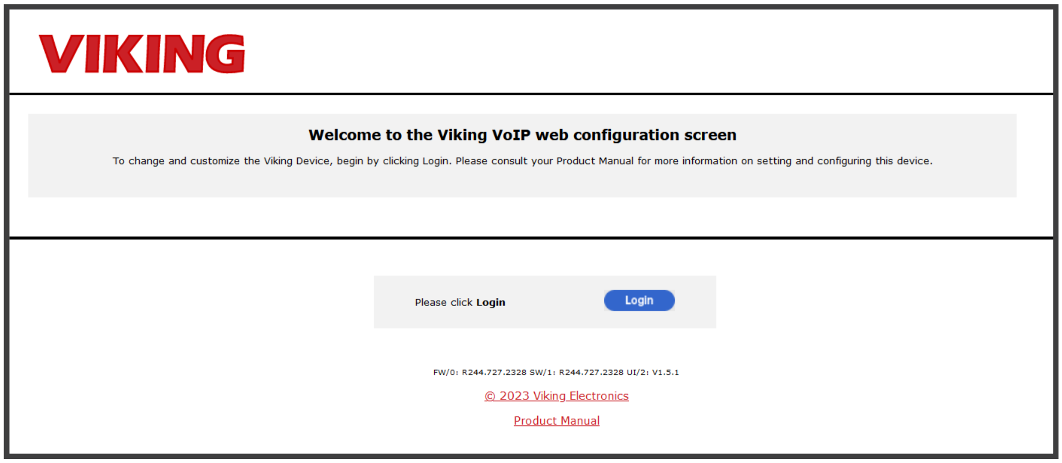
STEP 1	Install the unit using Cat 5e (or greater) Ethernet cable. The **E-32T-SS-IP** is PoE powered (class 2). We suggest a managed PoE switch, but it is not required. A PoE injector is acceptable.
STEP 2	After the unit is powered, it will boot up (30 to 45 seconds). The unit will then listen to discovery messages from the **Viking VoIP Discovery Utility**
STEP 3	Download and run the **Viking VoIP Discovery Utility**. Any **E-32T-IP** devices on your LAN should be displayed. Simply double-click on the unit's name/address in the Discovery window to open the Web UI. Alternatively, if the IP address of the **E-32T-SS-IP** is known, type it in the address bar of your browser to access it (defaults to https://E32's IPADDRESS).
STEP 4	If you do not want to install/run the **Viking VoIP Discovery Utility**, the Web UI can also be accessed via IP address or "Hostname".local on your LAN. The default Hostname is the unit's MAC address without the ":" separators (e.g. HTTPS://18e80f508bda.local).
STEP 5	If a unit cannot be accessed (example: set to a Static IP that is not available), a hard reset can be performed to reset all settings to defaults (unit will start out as DHCP).
STEP 6	To reset the unit, hold down the call button on the front panel while cycling power. The unit will beep 2 times, then flash the LED for about 10 seconds and then beep four times. Release the button within 3 seconds of the 4 beeps. The unit will reboot itself and come back up with factory defaults settings. Note that this reboot takes 30-60 seconds.

9 - Web UI

To open the UI, enter the **E-32T-SS-IP**'s IP address in the address bar of your browser. HTTPS is default. If your browser shows an insecure connection, click on the "Lock" icon near the address bar. View the CA certificate and add it to the Certificate Store on the computer that will be used for access.

If the **Viking VoIP Discovery Utility** is used, double-clicking on the unit will attempt to login with the default password.

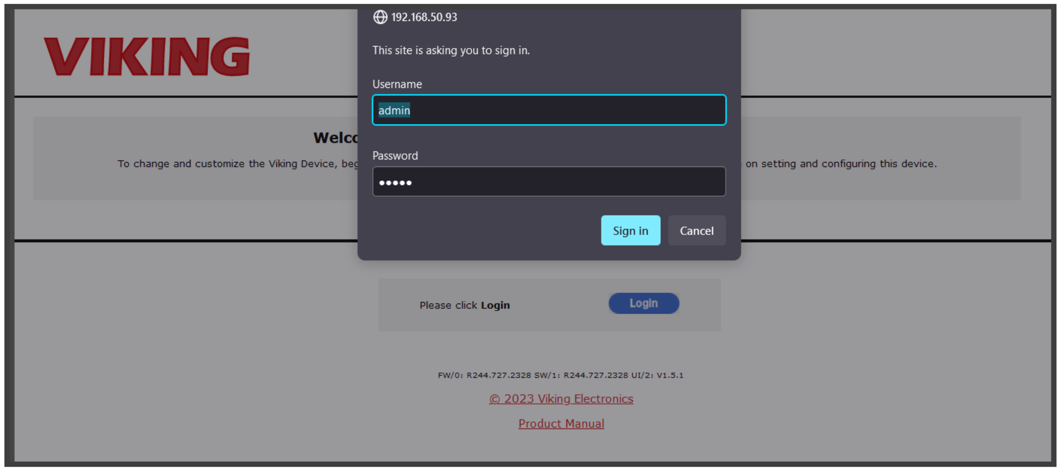
Click on **Login**.



For the first login, sign in as:

Username: admin
Password: admin

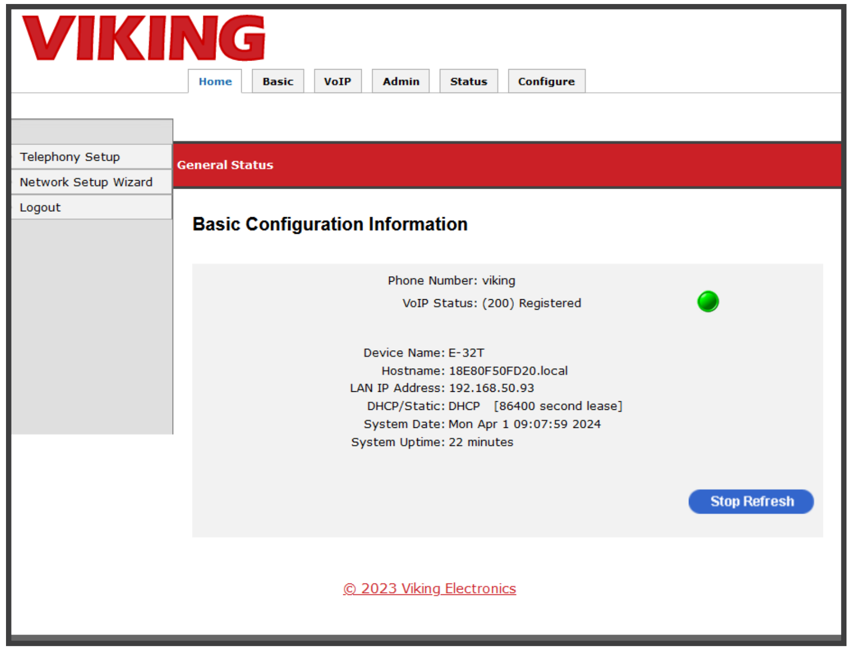
You will be prompted to change to a non-default password for security.



Home Tab

The Home tab opens and displays Basic Configuration Information about the unit, including registration status.

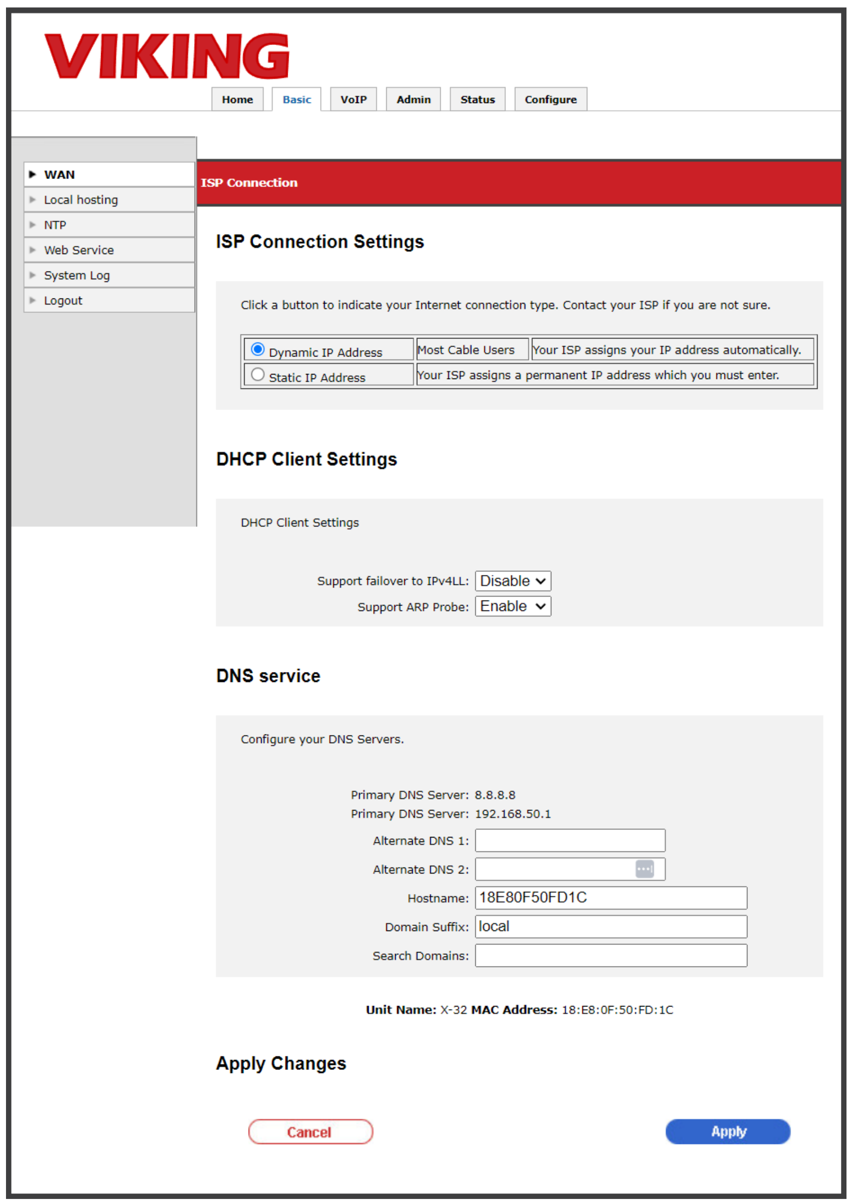
A green dot indicates the unit is registered and the network is OK. A yellow dot would indicate an error with SIP registration or the network.



Basic Tab

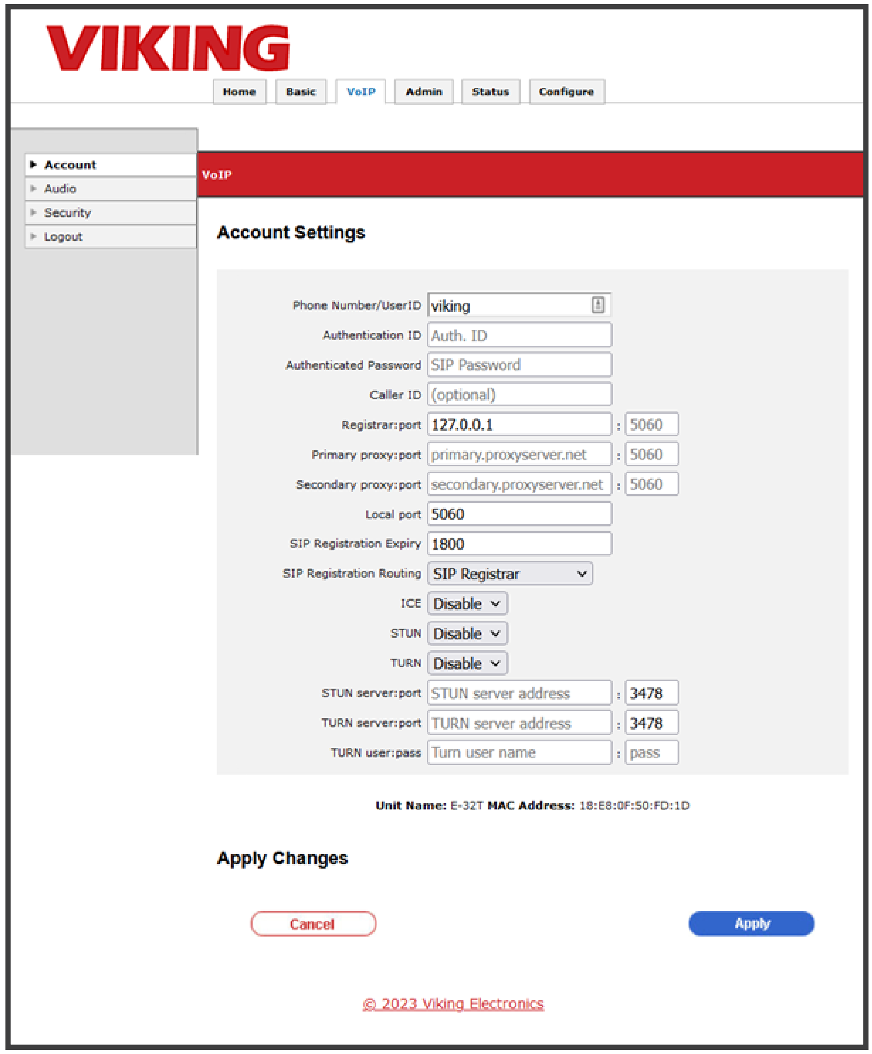
The Basic tab contains many of the initial IP/Network settings such as DHCP or static IP.

The unit will default to DHCP, making it easier to initially configure. Once an IP address is reserved, it can be used as the unit's static IP, which is easier to find the IP address of the unit for Web UI configuration.



VoIP Tab

The VoIP tab is used for SIP settings. Enter your SIP credentials here. The **E-32T-SS-IP** will attempt to register after the “Apply” button is clicked.

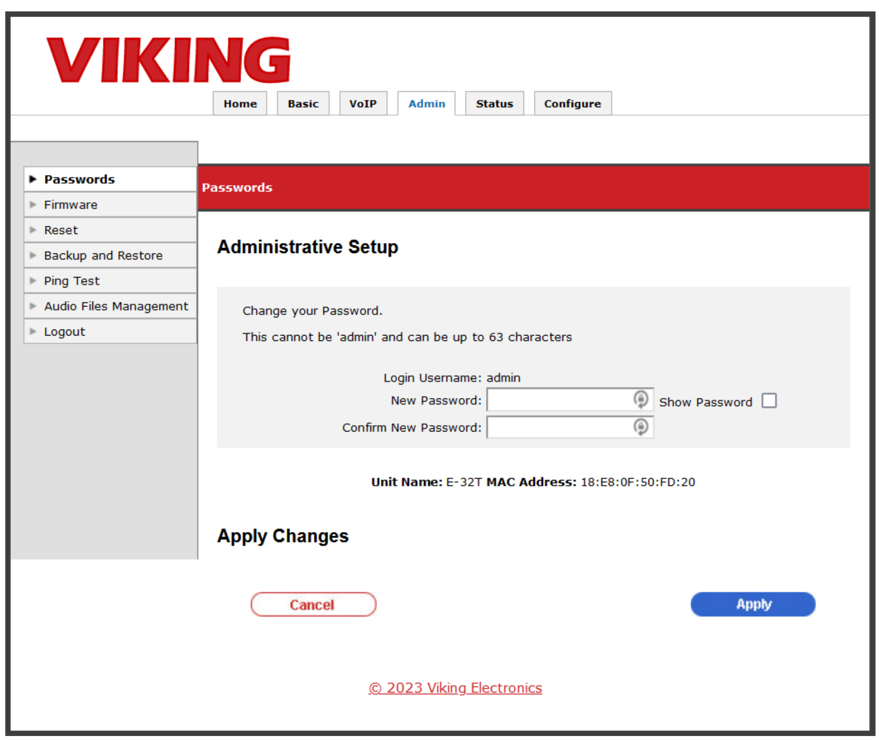


Admin Tab

The Admin tab is used for advanced settings such as changing the unit’s password, or updating firmware.

Use the Backup and Restore feature to save all settings for future use, or for provisioning multiple units.

When a configuration is downloaded, it creates a file named “x-series-backup.xml” in your downloads directory.

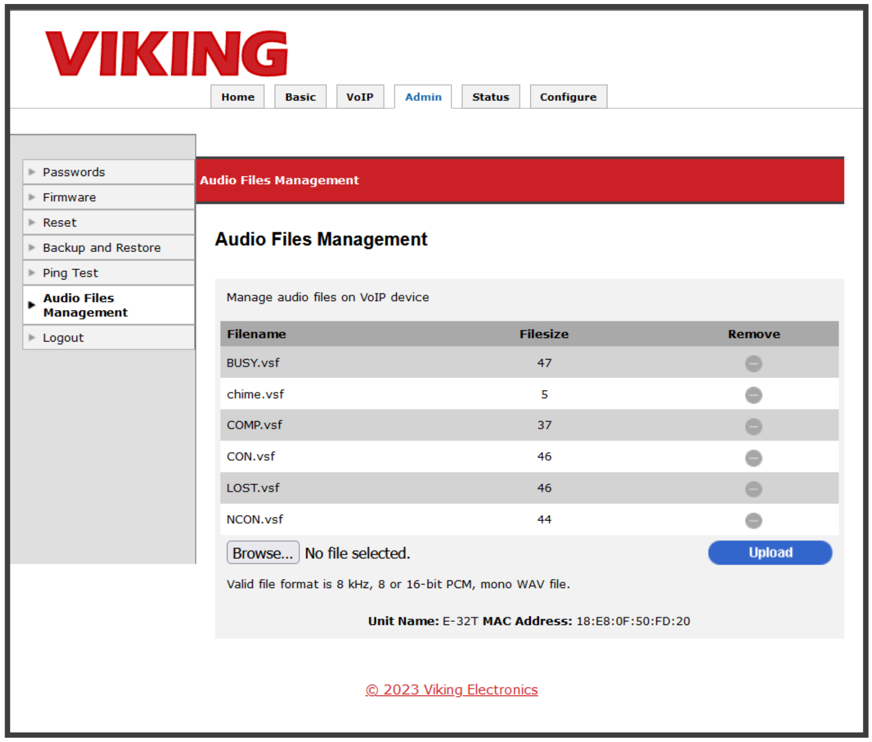


Admin Tab

Audio Files Management

The Audio Files Management page is used to upload WAV files. Click on the Browse button and select your WAV file. Then click on Upload to send the file. The format should be 8 kHz, 8 or 16-bit PCM, mono WAV file. A stereo file can be uploaded, and it will be automatically converted to mono before it is uploaded.

When enabled, the Announcement is played on outbound SIP calls once the call is connected. This audio is heard from the speaker and sent to the connected device, see page 16.

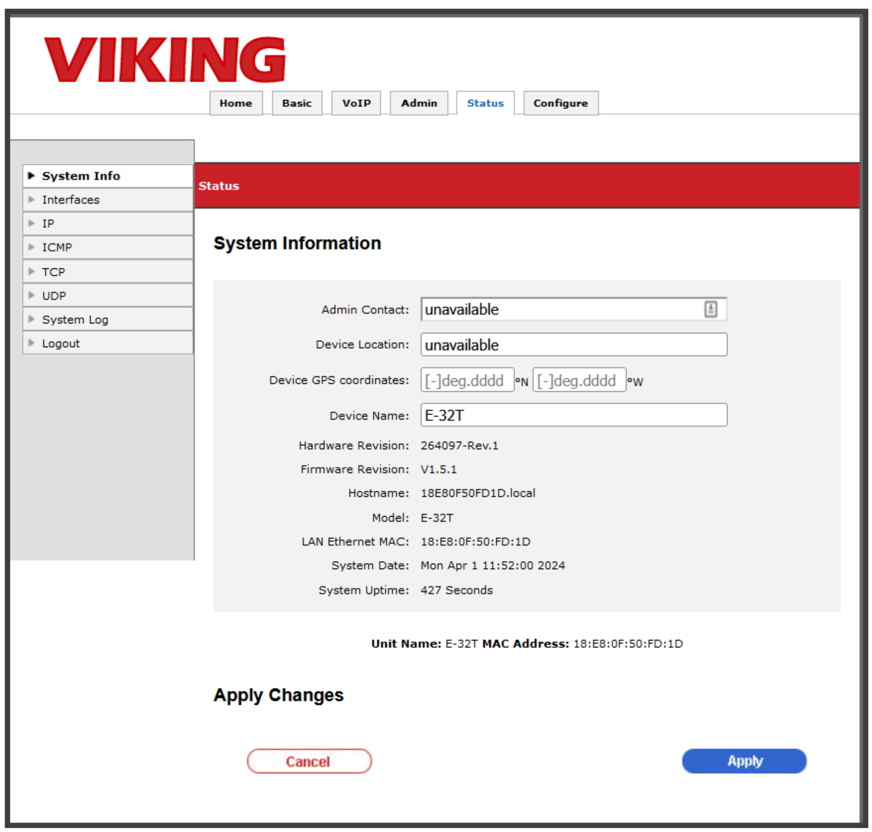


Status Tab

The Status tab includes system and Network Packet information.

Use this page to set your “Device Name”. This is the name that will be broadcast to the network for discovery.

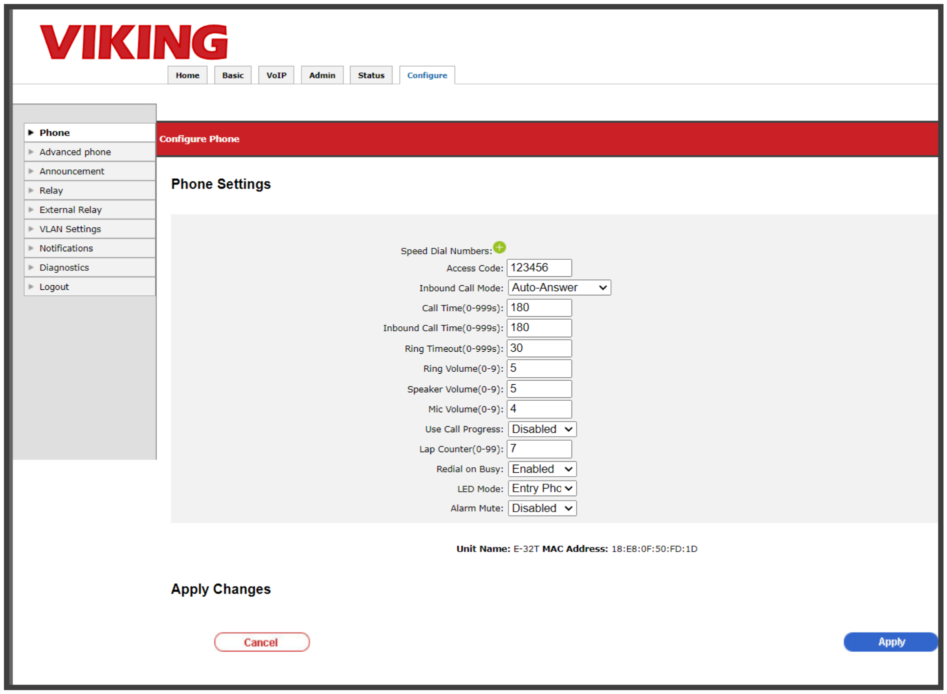
There are separate monitors for different IP protocols such as monitoring TCP connections to the unit.



Configure Tab

Phone Settings

Speed dial numbers, call/dialing options and volume levels are set on the Phone Settings Tab. These settings are used to control how the device acts during inbound and outbound SIP calls.



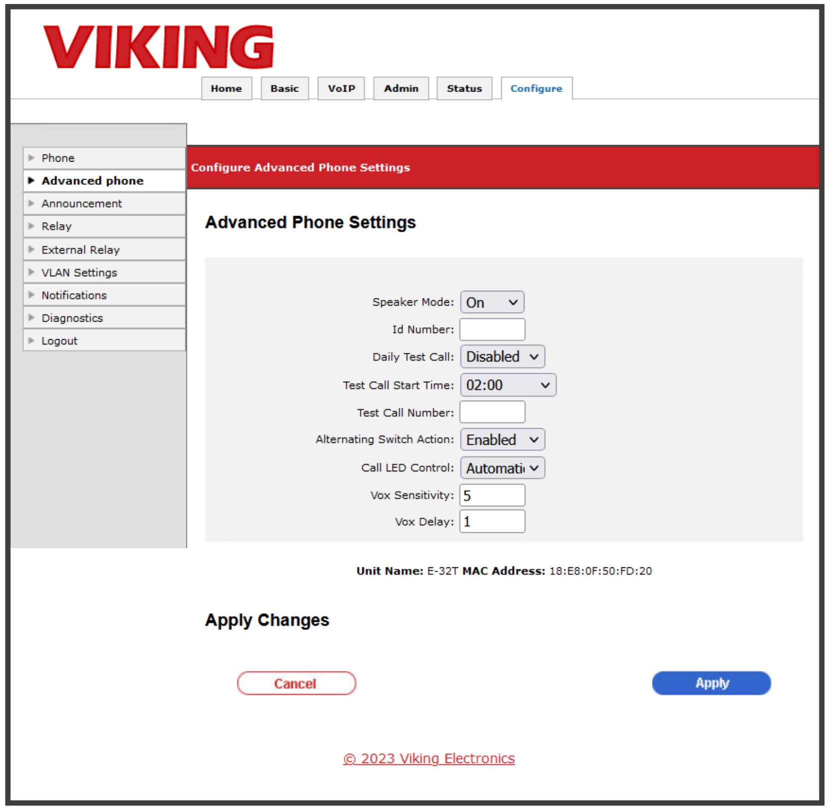
Setting	Description	Factory Default
Speed Dial Numbers	These are the phone numbers/extensions the **E-32T-SS-IP** will dial after pressing the Call button. The numbers are dialed top to bottom in order, once a call is answered the dialing sequence is ended.	n/a
Access Code	1-6 digits. This code must be entered by a caller before the relay can be controlled. This only applies to calls inbound to the **E-32T-SS-IP**. A long access code makes the unit more secure, but keep in mind it will likely be manually dialed by a caller from their SIP device. **Note:** In-band DTMF detection is not supported at this time.	123456
Inbound Call Mode	**Disabled:** All inbound calls are rejected. **Auto Answer:** Inbound calls are auto answered with video and audio. Relays can be controlled after the Acess Code is entered (if programmed). **Auto Answer Secured:** Inbound calls are auto answered without video or audio. The caller has 10 seconds to dial the Access Code to establish video and audio or the call will be ended. Relays can be controlled after the Access Code is entered (if programmed to Door Strike Mode).	Auto Answer
Call Time	Affects outbound calls made by the **E-32T-SS-IP**. Set to 0 to disable the timer. Resolution is in seconds, 1-999.	180 (3 minutes)
Inbound Call Time	Affects inbound ringing calls made to the **E-32T-SS-IP**. Set to 0 to disable the timer. Resolution is in seconds, 1-999.	180 (3 minutes)
Ring Timeout	This value is how many seconds the **E-32T-SS-IP** will try to call the “Numbers”. Once a call is answered this timer stops and the Call timer is in control. This only affects outbound calls from the **E-32T-SS-IP**.	30
Ring Volume	Changes the volume of Loud Ringing.	6
Speaker Volume	0-9. Changes the level of the audio produced by the **E-32T-SS-IP** speaker.	3
Mic Volume	0-9. Changes the level of the audio from the **E-32T-SS-IP** microphone.	5
Use Call Progress	Enabled/Disabled. Set this to enable when the **E-32T-SS-IP** is calling outside of the building and analog audio detection is required.	Disabled
Lap Counter	The number of times the group of programmed numbers is dialed. 0 = continuous dialing. Example: 5 numbers are programmed, Lap Counter is set to 3. The unit will dial 15 times (3 laps of 5 numbers).	7

<table>
<tr><th>Setting</th><th>Description</th><th>Factory Default</th></tr>
<tr><td>Redial on Busy</td><td>Enabled/Disabled. When enabled the unit will dial again after a call fails or busy signal is heard. When disabled the unit hangs up after a failed/rejected call.</td><td>Enabled</td></tr>
<tr><td>LED Mode</td><td>This setting determines how the LED on the E-32T-SS-IP will act when idle and during calls.
<table>
<tr><th>LED Mode</th><th>Description</th></tr>
<tr><td>Entry Phone</td><td>The LED will remain ON in the idle state, turn off while button is pressed, blink during dialing, light steady when the call is answered, then turn OFF momentarily when the call is completed.</td></tr>
<tr><td>Emergency Phone</td><td>The LED will remain OFF in the idle state, blink during dialing, light steady when the call is connected, then turn OFF when the call is completed.</td></tr>
<tr><td>Emergency Phone Outbound Only</td><td>On outbound calls, the LED will remain OFF in the idle state, blink during dialing, light steady when the call is connected, then turn OFF when the call is completed. On inbound calls, the LED will remain off. This is useful for silent monitoring on inbound calls.</td></tr>
<tr><td>Off</td><td>Stays off when idle and during connected calls. Flashes on boot up, during dialing, and when the unit has a Network/Registration error.</td></tr>
</table></td><td>Entry Phone</td></tr>
<tr><td>Alarm Mute</td><td>When the SIP/Network Alarm is active (unit is not registered, or a network error) the E-32T-SS-IP will beep 3 times every 30 seconds. The LED on the button will also flash. When Alarm Mute is set to enabled, the LED will still flash but no beeps are produced for the Alarm.</td><td>Disabled</td></tr>
<tr><td></td><td></td><td></td></tr>
</table>

Configure Tab

Advanced Phone Settings

The advanced phone settings page contains additional phone features from legacy Viking products. These settings are used before and during SIP video calls.

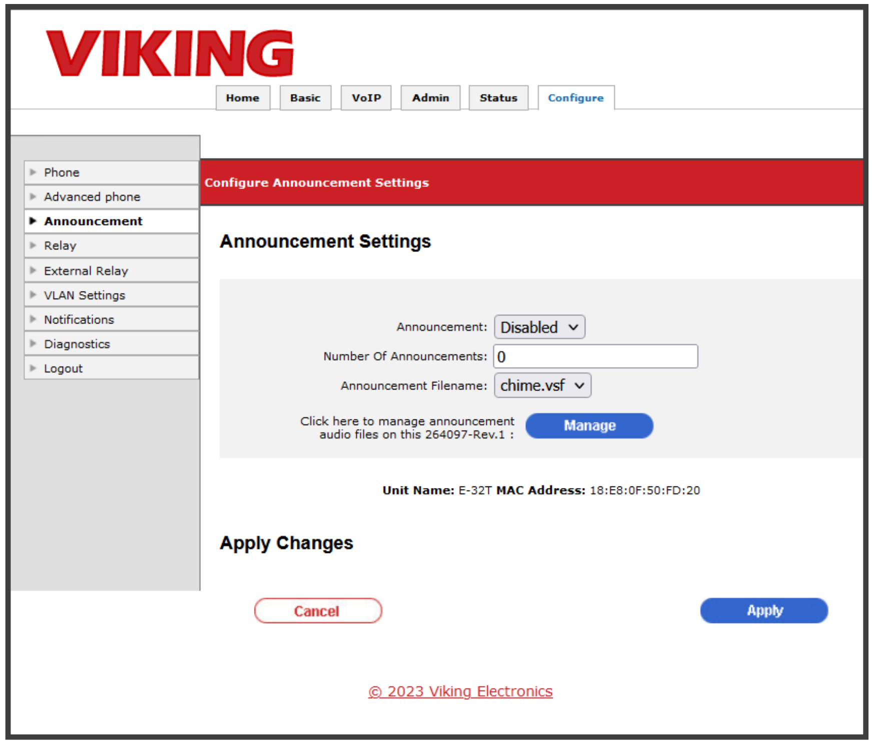


<table>
<tr><th>Setting</th><th>Description</th><th>Factory Default</th></tr>
<tr><td>Speaker Mode</td><td>This setting determines how the speaker on the E-32T-SS-IP will function.
<table>
<tr><th>Speaker Mode</th><th>Description</th></tr>
<tr><td>On</td><td>The speaker is active during inbound and outbound calls.</td></tr>
<tr><td>Silent Monitor</td><td>The speaker is will be muted during inbound and outbound calls.</td></tr>
<tr><td>Off Until Answered</td><td>The speaker will remain off until an outbound SIP call is connected. On inbound calls the speaker will function normally.</td></tr>
</table></td><td>On</td></tr>
<tr><td>Id Number</td><td>The Id Number is an In-band or RFC 2833 DTMF string sent to the calling party after a “*” is dialed. Leave blank to disable this feature.</td><td>Blank - disabled</td></tr>
<tr><td>Daily Test Call</td><td>When set to Enabled, the device will make a SIP call once a day at a programmable hour.</td><td>Disabled</td></tr>
<tr><td>Test Call Start Time</td><td>The time of day the unit will make the Daily Test Call.</td><td>02:00 AM</td></tr>
<tr><td>Alternating Switch Action</td><td>When enabled, a VoIP call can be ended with the button. When disabled, calls can only be started with the button.</td><td>Enabled</td></tr>
<tr><td>Call Led Control</td><td>During outbound calls, the LED can turn on when the call is connected, or wait until a “*” is received.</td><td>Automatic</td></tr>
<tr><td>Vox Sensitivity</td><td>1-10. Higher values make the unit more sensitive to audio from the called party.</td><td>5</td></tr>
<tr><td>Vox Delay</td><td>1-10 (100 mS to 1 S). The amount of switching time to switch between talk and listen modes.</td><td>5 (0.5 seconds)</td></tr>
</table>

Configure Tab

Announcement Settings

When enabled, the Announcement is played on outbound SIP calls once the call is connected. This audio is heard from the speaker and sent to the connected device. The Announcement will also play on inbound calls if the Access Code and a "*" are dialed. The Number Of Announcements setting controls how many times the audio file will automatically play (8 seconds between plays). Select your uploaded file from the Announcement Filename drop down (your file will have a ".vsf" file extension). If you have not uploaded a file yet, click on the Manage button to open Audio Files Management.



Configure Tab

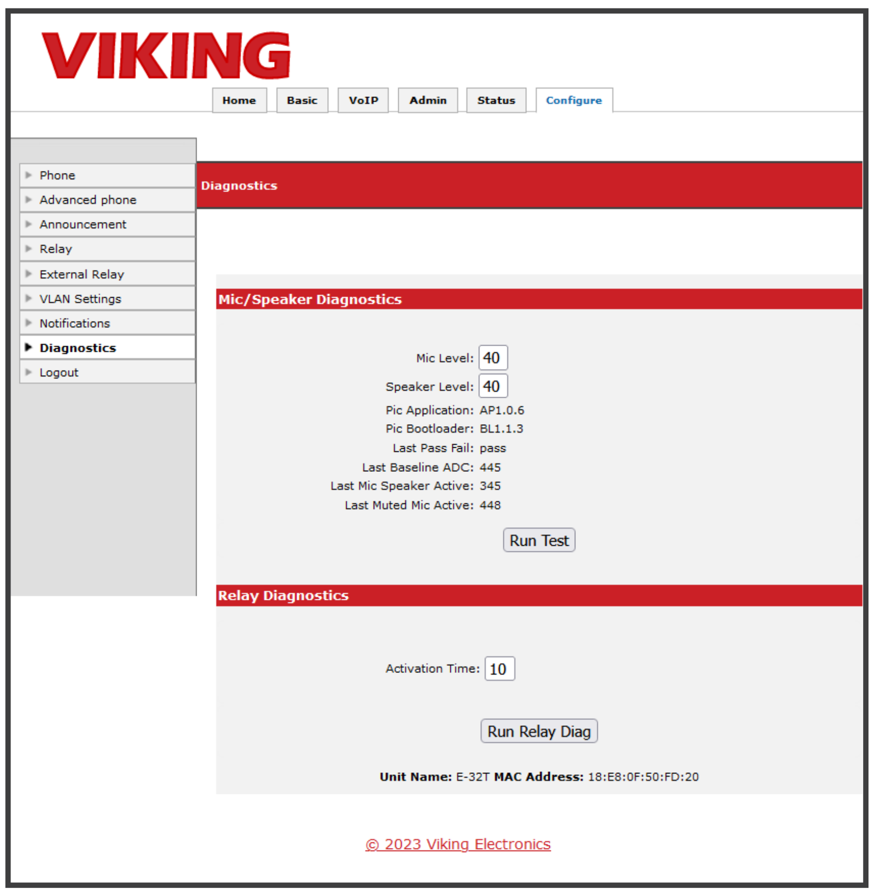
Diagnostics

Mic/Speaker Diagnostics:

The microphone and speaker are tested at the same time when the Run Test button is clicked. A tone will play from the speaker, and the microphone will listen. Background noise can affect this, so there are configurable values for audio levels (Mic Level, Speaker Level). In quiet areas, these can be lowered, in louder areas they may have to be increased.

Relay Diagnostics:

The Relay Diagnostic allows you to test your relay contact wiring without making a SIP call. Enter the Activation Time you would like the relay to stay on for and click on Run Relay Diagnostic. The button in the UI will turn Green for the duration of the closure.

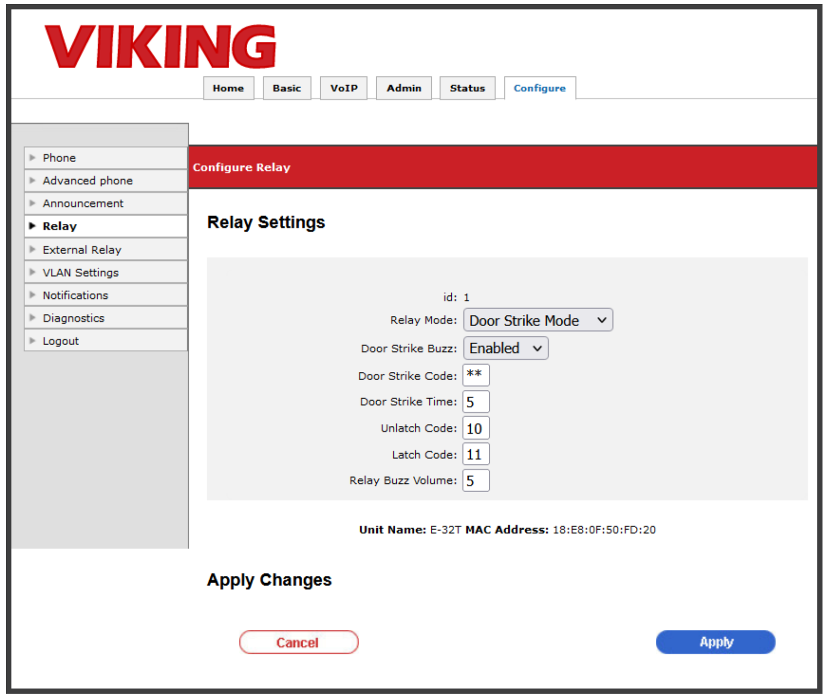


Configure Tab

Relay Settings

The relay settings are set here. Select the relay mode (or disable it) and set your DTMF codes for controlling the relay.

Note: Relay must be set to “Door Strike Mode” to use DTMF to control the relay.



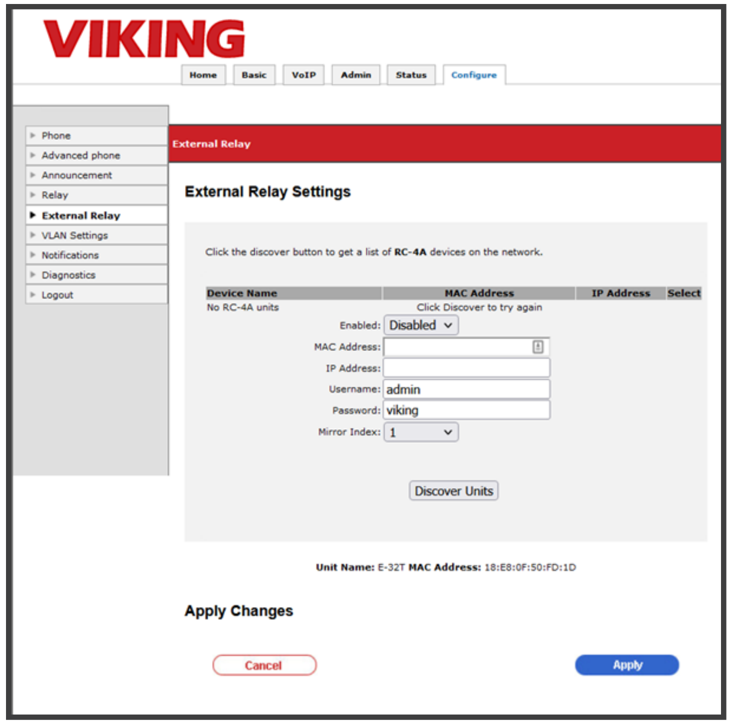
<table>
<tr><th>Setting</th><th>Description</th><th>Factory Default</th></tr>
<tr><td>Relay Mode</td><td>Select the mode you would like the relay to operate.
<table>
<tr><th>Relay Mode</th><th>Description</th></tr>
<tr><td>Disabled</td><td>The relay is disabled at all times.</td></tr>
<tr><td>Door Strike Mode</td><td>The relay can be controlled with Touch tones received by the E-32T-SS-IP. The Door Strike Code, Off Code and On Code can be entered during a call. The REX Input can also be used to control the relay.</td></tr>
<tr><td>Outbound Call</td><td>The relay will activate while outbound calls from the E-32T-SS-IP are connected.</td></tr>
<tr><td>Inbound/Outbound Call</td><td>The relay will activate when calls to/from the E-32T-SS-IP are connected.</td></tr>
<tr><td>Doorbell</td><td>The relay will activate for the programmable Door Strike Time at the beginning of an outbound call.</td></tr>
<tr><td>Alarm</td><td>The relay will activate continuously while the E-32T-SS-IP is registered to a SIP server. When the SIP/Network Alarm activates the Relay will de-energize.</td></tr>
<tr><td>Ring</td><td>The relay will activate continuously while the E-32T-SS-IP’s extension is ringing, and the “Loud Ring” feature on the E-32T-SS-IP is enabled.</td></tr>
<tr><td>Ring Flash</td><td>The relay will activate in a 400mS on/off pattern while the E-32T-SS-IP’s extension is ringing, and the “Loud Ring” feature on the E-32T-SS-IP is enabled.</td></tr>
</table></td><td>Door Strike Mode</td></tr>
<tr><td>Door Strike Buzz</td><td>Enabled or Disabled. When enabled, a buzz will be heard after a valid Door Strike Code is dialed. This buzz should match the Door Strike time up to 5 seconds. The volume of this Door Strike Buzz matches the Speaker volume setting.</td><td>Enabled</td></tr>
<tr><td>Door Strike Code</td><td>When this code is dialed, the relay will turn on for the length of the Door Strike Time.</td><td>**</td></tr>
<tr><td>Door Strike Time</td><td>The length of time (in seconds) that the relay will activate for (after Door Strike Code or REX input). 0.5-99 seconds (enter 0 for 0.5 second closure).</td><td>5 seconds</td></tr>
<tr><td>Off Code</td><td>When this code is dialed the relay will latch off (1 beep is heard from the E-32T-SS-IP speaker).</td><td>10</td></tr>
<tr><td>On Code</td><td>When this code is dialed the relay will latch on (2 beeps are heard from the E-32T-SS-IP speaker).</td><td>11</td></tr>
<tr><td>Relay Buzz Volume</td><td>0-10. Level of the buzz heard after a momentary relay activation.</td><td>5</td></tr>
</table>

***NOTE:** “Off” and “On” codes are also referred to as latching commands. These can be disabled by deleting them. This will prevent the relay from being stuck in an open position.*

Configure Tab

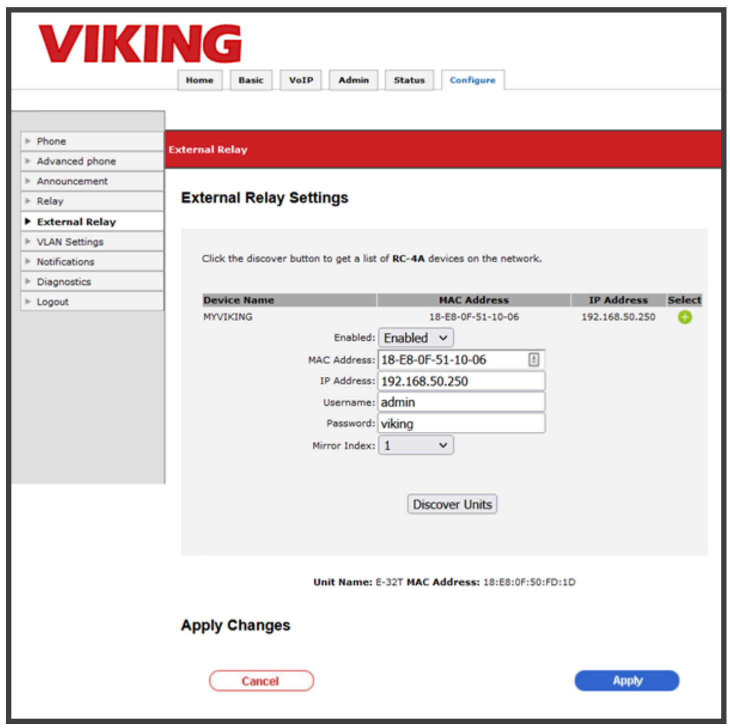
RC-4A Network Relay Control

The External Relay page will show you a list of RC-4A devices on your network. In order to connect an X-Series Device to one of them, click on the '+' button near under the Select column.



The RC-4A's IP address and MAC address will be copied into the text boxes. Enter your RC-4A user name and password (the RC-4A defaults are admin:viking). Click 'Apply' to save the changes. Any relay activations will trigger the RC-4A relay matching the 'Mirror Index'.

If no RC-4A units are discovered, check your connections, and make sure the RC-4A is on the same LAN as the X-Series device.

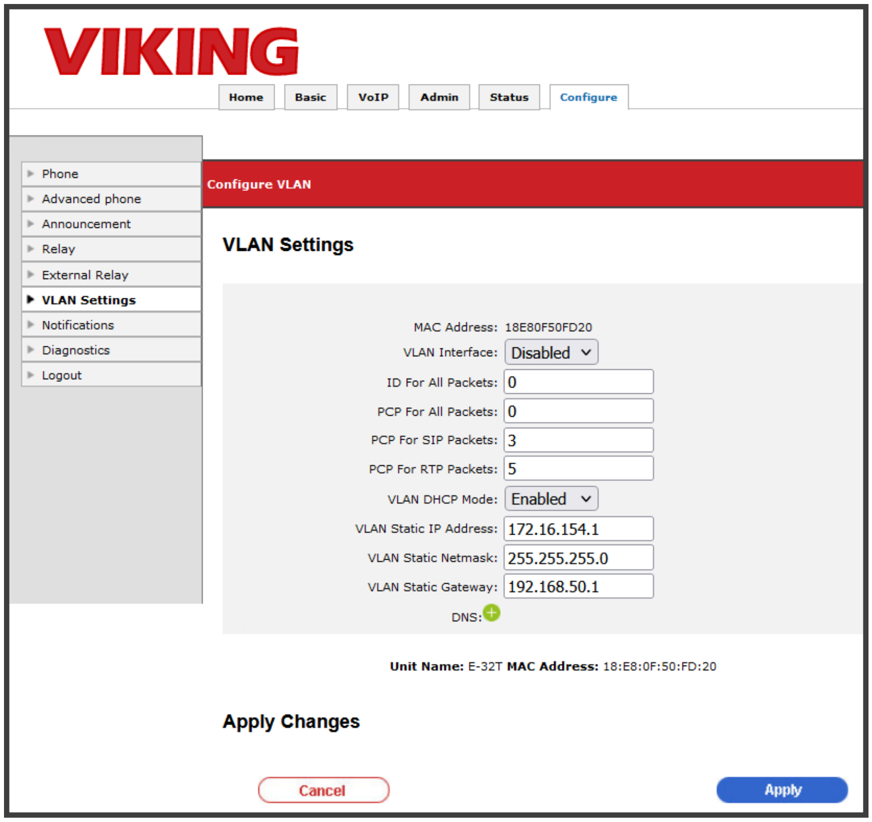


Setting	Description	Factory Default
Enabled	Turns Network Relay Interaction on or off.	Disabled
MAC Address	The MAC address of the RC-4A. Use the '+' button to copy this value into the field.	Blank
IP Address	The IP Address of the RC-4A.	Blank
RC-4A user name	The user name used to authenticate with the RC-4A.	admin
RC-4A password	The password used to authenticate with the RC-4A.	viking
Mirror Index	The relay on the RC-4A you would like to control (1-4).	1

Configure Tab

VLAN Settings

Advanced network settings are found on this page. Configure your VLAN settings as well as an alternate DNS list. Using this page, when Apply is clicked a pop-up warning will be seen, when confirmed the unit will reboot. If the IP address is changed, use the new address to connect to the unit once it reboots (about 45 seconds).



Setting	Description	Factory Default
VLAN Interface	Enabled or Disabled (Factory set to Disabled). When set to enabled (and changes are applied) the **E-32T-SS-IP** will reboot using the VLAN interface. Be sure all other VLAN settings are properly configured before applying changes.	Disabled
ID For All Packets	VLAN Identifier. Set to “0” by default to make sure if you enable VLAN by accident, but do not select the proper tag, The VLAN setting will not take effect (“0” is reserved and cannot be used as a VLAN ID). Change this to the proper tag for your VLAN.	0
PCP For All Packets	Priority code point for all traffic. This includes TCP, TLS, and all other packets to and from the **E-32T-SS-IP** on the VLAN. This is set to “0” by default (highest priority), this is the best option for NVR streaming. This can be changed if your network infrastructure requires it.	0
PCP For All SIP Packets	Priority code point for all SIP traffic. This is set to “3” by default. It is set lower than the All Packets PCP, but higher than the RTP PCP which should prevent SIP calls from being dropped due to network congestion.	3
PCP For All RTP Packets	Priority code point for all RTP traffic. This is set to “5” by default. This is a lower priority than SIP traffic to prevent SIP calls from being dropped due to network congestion.	5
VLAN DHCP Mode	Enabled or Disabled	Enabled
VLAN Static IP Address	IP address that should be reserved before enabling VLAN.	172.16.154.1
VLAN Static Netmask	Netmask for the VLAN Interface.	255.255.255.0
VLAN Static Gateway	Gateway for the VLAN Interface.	n/a

VLAN Operation

When set to Enabled, the **E-32T-SS-IP** will create a new network interface and receive/send packets that have the selected “ID For All Packets”. You can also set the PCP separately for SIP or RTP.

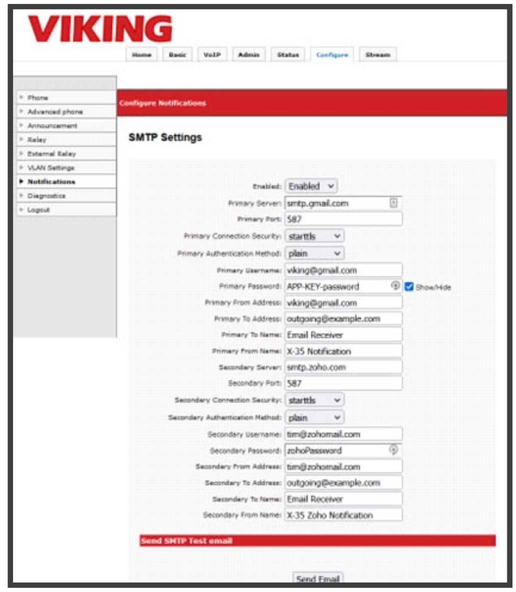
The VLAN interface can be set to use a DHCP address (default) or a Static IP. If a static IP is used, be sure your DNS is setup properly. Multiple DNS servers can be added with the green button, if one fails the next one will be tried.

Once VLAN is enabled and the unit is rebooted (happens automatically after changing network settings), the device will come up with it’s new IP address. If there is an issue trying to access the Web UI of the **E-32T-SS-IP** after enabling VLAN tagging, there is a backup address for access. Use https://<mac_Address>.local replacing <mac_Address> with your device’s mac (all lower case, no special characters).

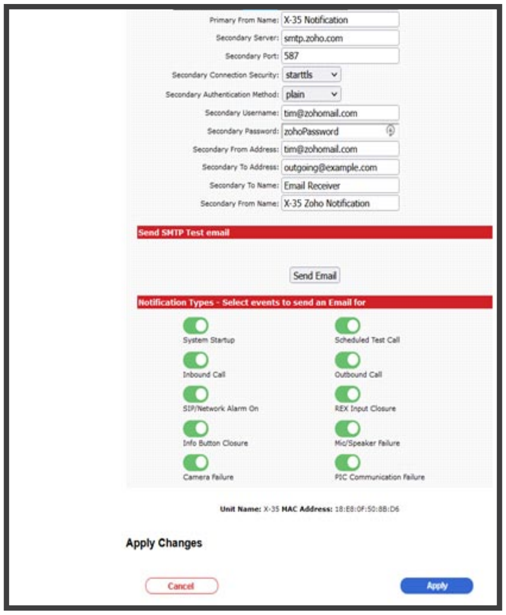
Configure Tab

SMTP Notifications

Two different email senders can be used by entering a Primary and a Secondary account. If only one account is entered it will be retried on failure. If a secondary account is used our SMTP server will bounce between primary and secondary retrying until it is successful. In the case the network is unreachable an email will be sent when our device detects the network is working again.



Setting	Description	Factory Default
SMTP Enabled	Turn SMTP Notifications on or off.	Disabled
Primary/Secondary Server	SMTP address of the email sending account	Blank
Primary/Secondary Port	587(TLS) or 465(SSL). See the settings in your SMTP sender account.	Blank
Primary/Secondary Connection Security	StartTLS or TLS security type	startTLS
Primary/Secondary Authentication Method	Choose the auth method used by your email sender as ‘none’, ‘plain’, ‘hmac-md5’, or ‘login’.	Plain
Primary/Secondary Username	Username for your SMTP sender account (for Gmail this is your Gmail address).	Blank
Primary/Secondary Password	Password for SMTP auth (for Gmail you must create an App Password for your Gmail Account).	Blank
Primary/Secondary ‘From’ Address	This will likely match your Username and is the email address SMTP is sent from.	Blank
Primary/Secondary ‘To’ Address	The email address of the recipient.	Blank
Primary/Secondary ‘To’ Name	The name that appears in the Recipient field of the email.	Blank
Primary/Secondary ‘From’ Name	The name that appears in the Sender field of the email.	Blank



Test Email:

Click the Send Email button to try a test email using the saved settings (you must apply changes before testing).
The Primary SMTP account will be tested first, if it fails the Secondary account will be tested.

Notification Types:

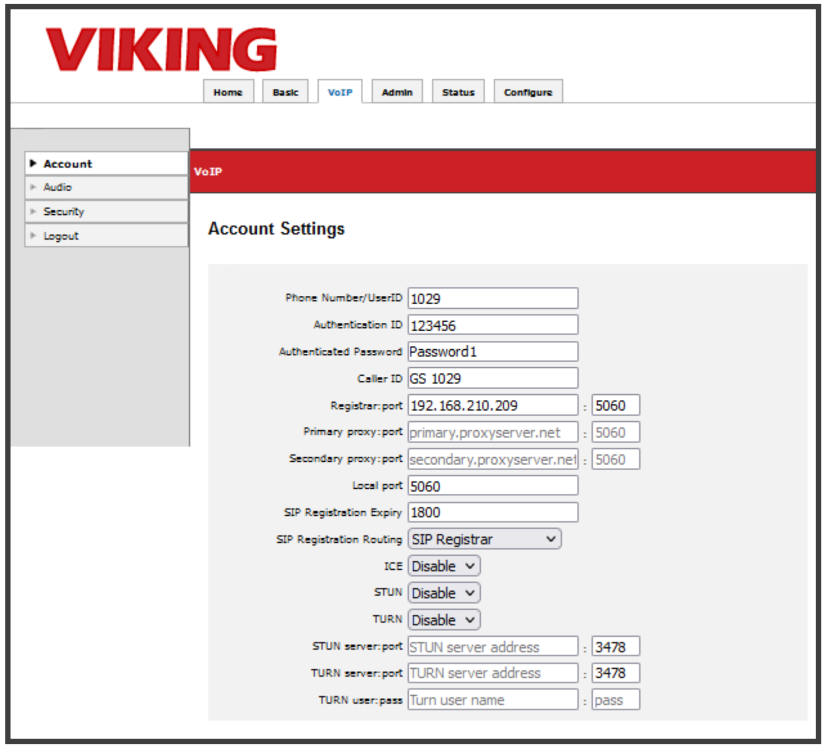
Check the button for any events you would like to send emails for. The body of the email will include a description of the event type.

Notification Type	Event Type
System Startup	An email will be sent when the device is power cycled, rebooted, or after a firmware upgrade.
Scheduled Test Call	When the Test Call is set up (see Reverse Polling) an email at the same time as the Test Call is scheduled for.
Inbound Call	An email will be sent when a SIP call is sent to the X-Series device. This is sent regardless of the Inbound Call Mode.
Outbound call	An email will be sent when a SIP call is made with the Call button.
SIP / Network Alarm On	When the SIP/Network Alarm activates, and email is sent. This occurs when SIP registration is lost, or the network becomes unreachable (email is sent when network returns indicating the error occurred).
REX Input Closure	An Email is sent when the relay activates from a closure of the REX Input (green wire pair).
Info Button Closure	An Email is sent when a SIP call is triggered by the Info button (model specific).
MIC / Speaker Failure	When the MIC/Speaker Diagnostic fails an email is sent.
Camera Failure	If the camera module fails an email is sent.
PIC Comm. Failure	An email is sent if there is a major hardware issue on the device.

SIP Server/SIP Provider

To configure an **E-32T-SS-IP** device to register to a SIP Server or SIP Provider, enter the Phone Number (or SIP extension name), SIP Password, Authentication ID (if required), and the IP Address/URL of the SIP Server. Enter the SIP port that will be used, if this is blank port 5060 will be used.

The default SIP protocol is UDP, if TLS or Secure RTP is to be used, change this setting on the VoIP-Security page.

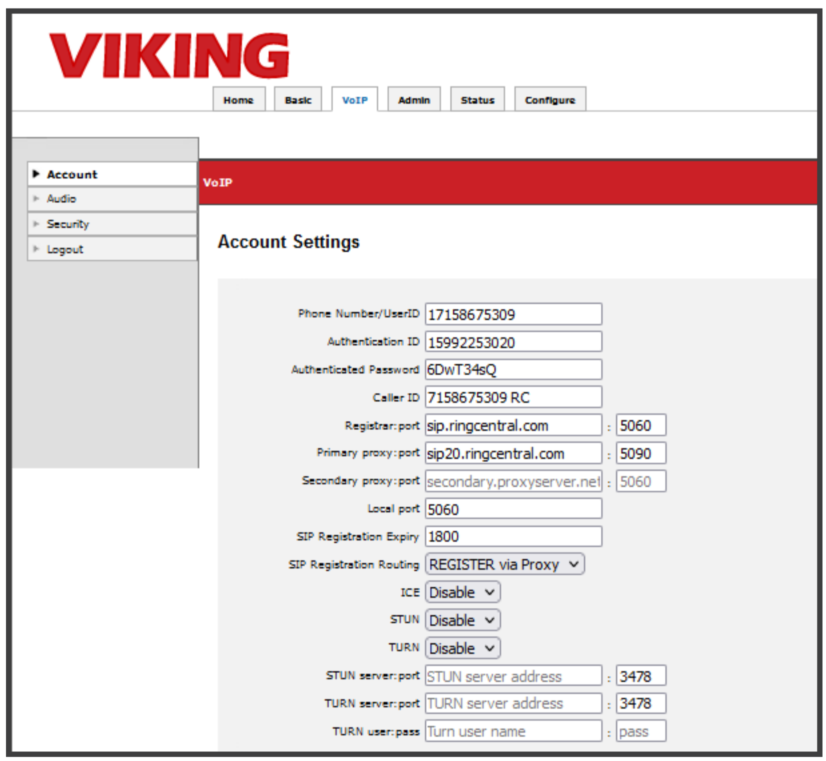


Outbound Proxy Settings

Registering via an Outbound Proxy

To register an **E-32T-SS-IP** device to a SIP Server or SIP Provider with an Outbound Proxy, follow the steps below.

STEP 1	Change the drop down for “SIP Registration Routing” to “REGISTER via Proxy”.
STEP 2	Enter the Phone Number (or SIP extension name), SIP Password, Authentication ID (if required), and the IP Address/URL of the SIP Server.
STEP 3	Enter the Outbound Proxy IP Address/URL.
STEP 4	Enter the SIP port that will be used (this port could differ between the SIP Domain and Outbound Proxy), if this is blank port 5060 will be used.
STEP 5	The default SIP protocol is UDP, if TLS or Secure RTP is to be used, change this setting on the VoIP-Security page.



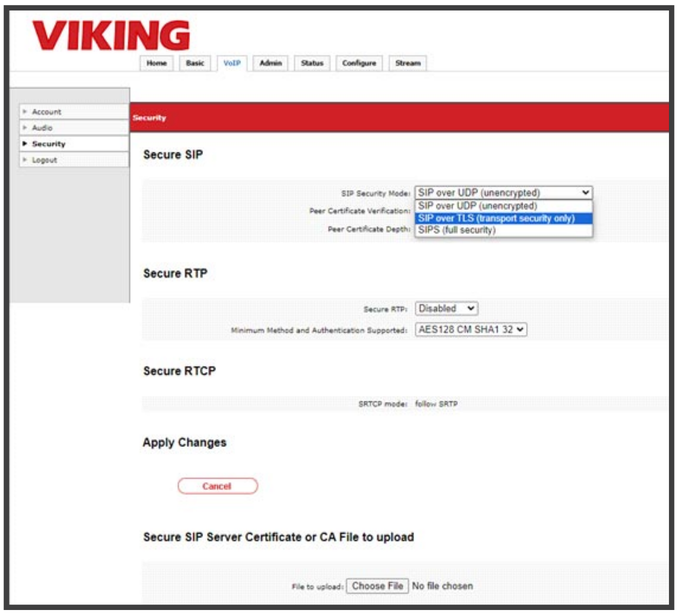
VoIP Security

SIP Transport

By default, SIP transport is sent over UDP. For TLS transport select the 'SIP over TLS' option. This only encrypts the SIP control traffic. For fully encrypted calls select the SIPS option and enable secure RTP below.
NOTE: SIP over TLS and SIPS will use a different port with the SIP Server/Provider, ensure this is set correctly on the VoIP Account page.

Secure RTP:

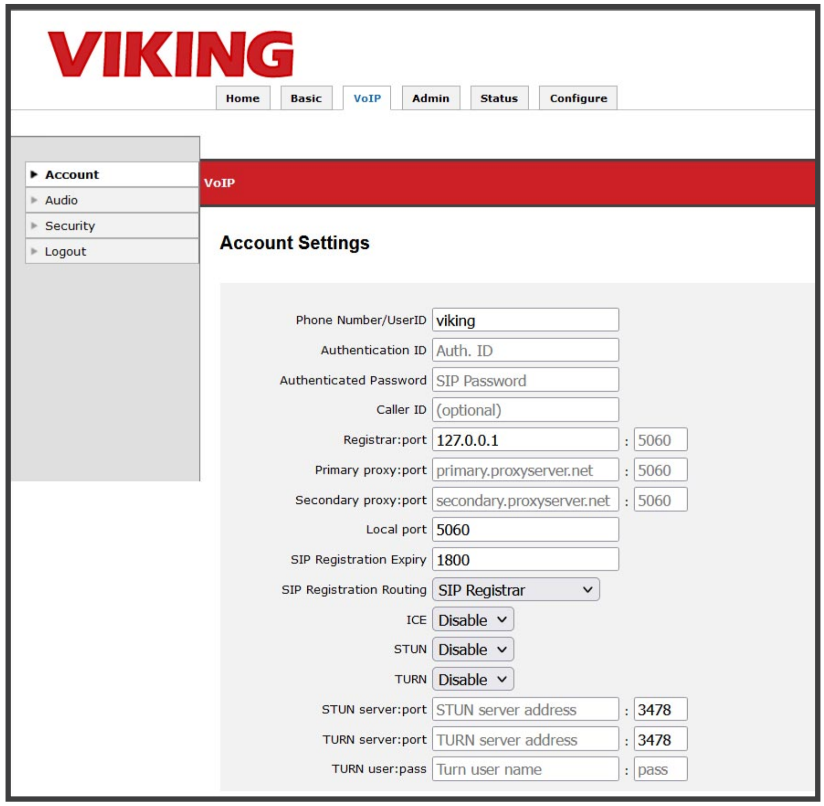
Select an option for audio encryption. By default, the audio is sent via unencrypted RTP.
Disabled: Audio is sent as unencrypted RTP.
Optional: Encrypted audio is offered when a call is set up. If the negotiation is successful VoIP audio will be sent using encrypted RTP.
Mandatory: Encrypted audio is offered when a call is set up, if the negotiation is successful the call is set up using encrypted RTP. If not, the VoIP call is ended.



11 - Configuring Peer to Peer (Self-Registration)

The **E-32T-SS-IP** can be set up to make SIP calls without a SIP Server. To enable this feature enter “127.0.0.1” as the “Registrar” and set a “Phone Number/User ID” (this can be any letter/digit combination). This string must be dialed along with the IP Address of the **E-32T-SS-IP** device to make an Inbound call.

For example, to call the **E-32T-SS-IP** devices shown right, a SIP endpoint would dial “x32@192.168.0.11” where “192.168.0.11” is the IP Address of the X-Series device.

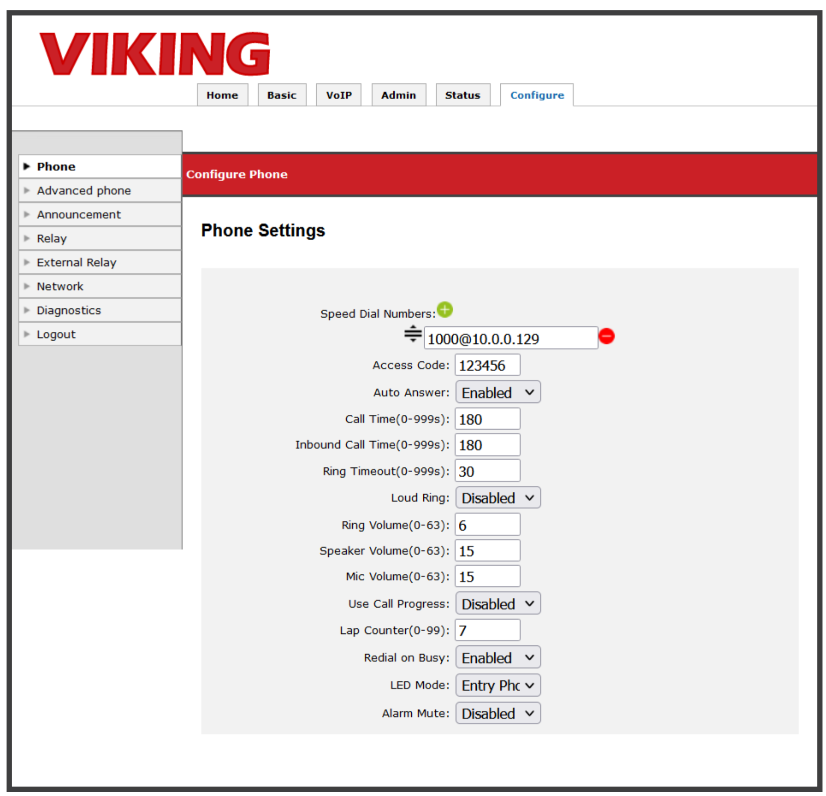


Peer to Peer Speed Dial Numbers

Outbound Peer to Peer calls are made by dialing directly to the IP Address of an endpoint using the “Phone Number” or “Extension Name”.

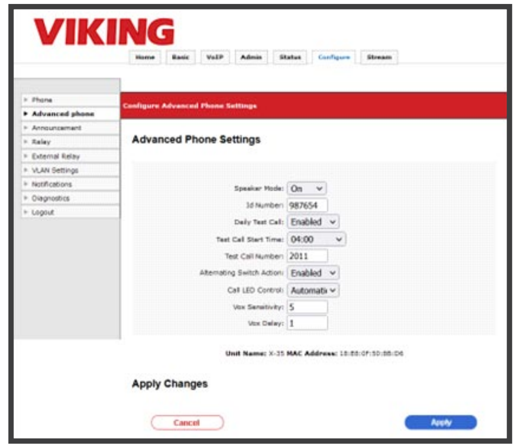
See the screenshot to the right as an example.

The Extension Name is ”1000” and the IP Address of the SIP Endpoint to be called is “192.168.0.10”.



Reverse Polling

To set up scheduled daily test calls (Reverse Polling) visit the Advanced Phone page. The settings depicted below show a Test Call set to call the extension ‘2011’ at 4 AM daily. If an Announcement is uploaded and the setting is enabled, it will play when the call is answered. If the answering party dials a ‘*’ the ID Number will be sent from the X-Series Device (RFC/SIP INFO Dialing).
The test call number can be up to 36 characters. Format the number to match the format of the Speed Dial Numbers. For example, if your Sped Dial Numbers are calling a POTS line use the format ‘95558675309’. The image below is using a SIP Extension (2011).



13 - Operation

A. Making a Call

When the Call button is pressed, the **E-32T-SS-IP** dials the first number in its list. If the call fails (busy, rejected or other SIP call failure) and redial on busy is enabled, the next number will be dialed. If redial on busy is disabled, the **E-32T-SS-IP** will hang up and go into its idle state.

Outbound calls will ring until the ring timeout is met, or the call is answered.

When the call is answered, two-way voice is established. The call timer starts. The called device can enter the relay commands if door strike mode is enabled. Door strike code starts a momentary relay closure, and the latching commands (on code/off code) will latch the relay. The call can be ended with the call button, a DTMF "#" or remotely with a call ended signal. Otherwise the call timer ends the call when its value is met.

B. Incoming Calls

The **E-32T-SS-IP** will handle incoming calls based on the Inbound Call Mode Setting:

Setting	Description
Disabled	All inbound calls are rejected.
Auto Answer	Inbound calls are auto answered with the Microphone and Speaker enabled. If an Access Code is set, it must be entered to control the relay with DTMF code.
Auto-Answer-Secure	Inbound calls are auto answered with the Microphone and Speaker enabled. The Access Code must be usedto enable communication and DTMF relay control.
Loud Ringing	A Loud Ringing signal is emitted from the speaker on inbound calls. The call can be answered by pressing the 'Call' button on the panel

14 - Troubleshooting

A. SIP / Network Alarm

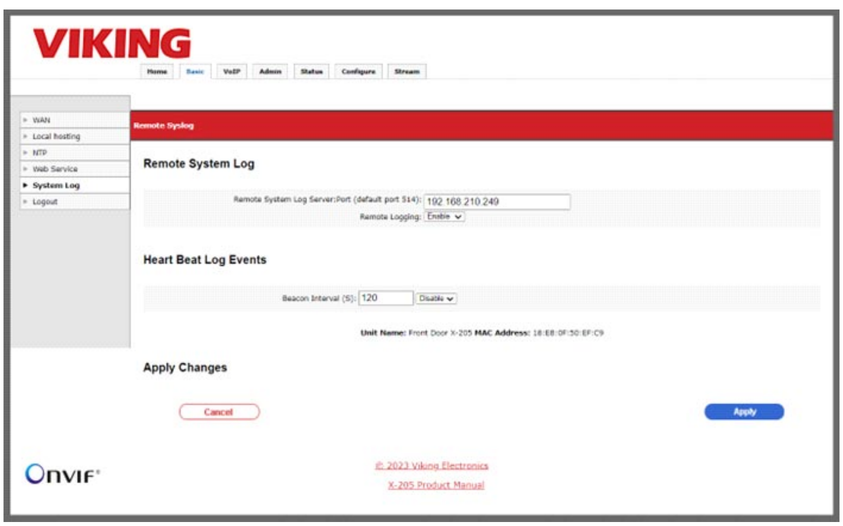
If there is a network error or the unit cannot register to the SIP Server/Provider the blue LED on the button will blink on and off every 2 seconds, and three error beeps will be heard every 30 seconds until the problem is resolved. This is to alert users to a potential problem that may prevent the X-Series device from making an outbound call.

B. Muting the SIP / Network Alarm

These beeps can be temporarily or permanently disabled. To mute the Alarm press and hold the button for at least 5 seconds (2 beeps will be heard indicating when to release it). This mutes the beeps until the next reboot, power cycle, or a change in registration/network status. The beeps can be permanently disabled on the Configure Tab under "Phone Settings". Set the Alarm Mute setting to "Disabled" and the beeps will be disabled for all "Alarm" conditions. The LED will continue flash when the unit's "Alarm" is active even if the beeps are muted.

C. Syslog

The Viking VoIP device can output status messages and errors to a syslog server. A PC that is running syslog listening software can store and display this log. Enter the IP address of the syslog server in the Web UI under Basic->System Log. Set this to Enabled and optionally enable 'Heart Beat Log Events' for monitoring. These messages are sent using UDP protocol on port 514. To use a non-default port enter it along with the IP Address with the following format 'IPADDRESS:PORT'.



15 - Open Source Licenses

Our VoIP firmware contains code from open-source packages which have been published under various licenses.

PACKAGE-VERSION	LICENSE TYPE	CHANGED	X-SERIES (BETA)	X-SERIES (V1.0)
curl v7.69.1-DEV	MIT-curl		x	
ffmpeg	LGLP 2.1		x	
glib v2.0	LGLP 2.1		x	
gSOAP v2.8	LGLP v2	x	x	
GStreamer v1.20	LPGL		x	
Kernel v4.9.88	GPL		x	
libatopology	LGLP 2.1+		x	
libfdk aac	GPL		x	
libffi	MIT-GNU-GPL		x	
libgcrypt	LGLP 2.1+		x	
libgmp v6.1	LGLP 2/3		x	
libgnuutils	LGLP 2.1+		x	
libgpg-error	LGLP 2.1		x	
libhogweed v6.0	LGLP 2		x	
libjpeg v62.2.0	jpeg license		x	
libjson-glib v1.0	LGLP 2.1		x	
libmicrodns v0.1.0			x	
libmp3lame v0.0	LPGL		x	
libnettle v8.0-nettle_3.6	LGPL 2+/3		x	
libnice v10.9	LGLP 2.1		x	
libpcre-16	BSD		x	
libpcre-32	BSD		x	
libpcreposix v0.0.7	BSD		x	
libturbojpeg v0.1	BSD		x	
libvpu v.4	LGLP 2.1		x	
libxml2 v2.9.12	MIT		x	
OpenSSL v1.0.2u	OpenSSL		x	
U-Boot v	GPL v2	x	x	
zlib v.1.2.11	GPL		x	

libjpeg license:

LICENSE TERMS (ships as a part of the libjpeg package in the README file)
=============

1. We don't promise that this software works. (But if you find any bugs, please let us know!)
2. You can use this software for whatever you want. You don't have to pay us.
3. You may not pretend that you wrote this software. If you use it in a program, you must acknowledge somewhere in your documentation that you've used the IJG code.

In legalese:

The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided "AS IS", and you, its user, assume the entire risk as to its quality and accuracy.

This software is copyright (C) 1991-2016, Thomas G. Lane, Guido Vollbeding. All Rights Reserved except as specified below.

Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

(1) If any part of the source code for this software is distributed, then this README file must be included, with this copyright and no-warranty notice unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation.
(2) If only executable code is distributed, then the accompanying documentation must state that "this software is based in part on the work of the Independent JPEG Group".
(3) Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code, not just to the unmodified library. If you use our work, you ought to acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company name in advertising or publicity relating to this software or products derived from it. This software may be referred to only as "the Independent JPEG Group's software".

We specifically permit and encourage the use of this software as the basis of commercial products, provided that all warranty or liability claims are assumed by the product vendor.

Curl license:

COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1996 - 2022, Daniel Stenberg, daniel@haxx.se, and many contributors, see the THANKS file.

All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

OpenSSL:
dual OpenSSL and SSLeay license:

OpenSSL License

 ===

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:
   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:
   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ''AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
==

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).
This product includes software written by Tim Hudson (tjh@cryptsoft.com)

Original SSLeay License

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).
The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.
If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.
This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

Warranty

IF YOU HAVE A PROBLEM WITH A VIKING PRODUCT, CONTACT VIKING TECHNICAL SUPPORT: 715-386-8666

Our Technical Support Department is available for assistance Monday through Friday 8:00am to 5:00pm central time. Before you call, please:

1. Know the model number, the serial number and what software version you have (see serial label).
2. Have the Product Manual in front of you.
3. It is best if you are on site.

RETURNING PRODUCT FOR REPAIR

The following procedure is for equipment that needs repair:

1. Customer must contact Viking's Technical Support Department at 715-386-8666 to obtain a Return Authorization (RA) number. The customer MUST have a complete description of the problem, with all pertinent information regarding the defect, such as options set, conditions, symptoms, methods to duplicate problem, frequency of failure, etc.
2. Packing: Return equipment in original box or in proper packing so that damage will not occur while in transit. The original product boxes are not designed for shipping - an overpack box is required to prevent damage in transit. Static sensitive equipment such as a circuit board should be in an anti-static bag, sandwiched between foam and individually boxed. All equipment should be wrapped to avoid packing material lodging in or sticking to the equipment. Include ALL parts of the equipment. C.O.D. or freight collect shipments cannot be accepted. Ship cartons prepaid to: **VIKING ELECTRONICS**
1531 INDUSTRIAL STREET
HUDSON, WI 54016
3. Return shipping address: Be sure to include your return shipping address inside the box. We cannot ship to a PO Box.
4. RA number on carton: In large printing, write the RA number on the outside of each carton being returned.

RETURNING PRODUCT FOR EXCHANGE

The following procedure is for equipment that has failed out-of-box (<u>within 10 days of purchase</u>):

1. Customer must contact Viking's Technical Support at 715-386-8666 to determine possible causes for the problem. The customer MUST be able to step through recommended tests for diagnosis.
2. If the Technical Support Product Specialist determines that the equipment is defective based on the customer's input and troubleshooting, a Return Authorization (RA) number will be issued. <u>This number is valid for fourteen (14) calendar days from the date of issue</u>.
3. After obtaining the RA number, return the approved equipment to your distributor. Please reference the RA number on the paperwork being shipped back with the unit(s), and also the outside of the shipping box. The original product boxes are not designed for shipping - an overpack box is required to prevent damage in transit. Once your distributor receives the package, they will replace the product over the counter at no charge. The distributor will then return the product to Viking using the same RA number.
4. **The distributor will NOT exchange this product without first obtaining the RA number from you. If you haven't followed the steps listed in 1, 2 and 3, be aware that you will have to pay a restocking charge.**

TWO YEAR LIMITED WARRANTY

Viking warrants its products to be free from defects in the workmanship or materials, under normal use and service, for a period of two years from the date of purchase from any authorized Viking distributor. If at any time during the warranty period, the product is deemed defective or malfunctions, return the product to Viking Electronics, Inc., 1531 Industrial Street, Hudson, WI., 54016. Customer must contact Viking's Technical Support Department at 715-386-8666 to obtain a Return Authorization (R.A.) number.

This warranty does not cover any damage to the product due to lightning, over voltage, under age, accident, misuse, abuse, negligence or any damage caused by use of the product by the purchaser or others. This warranty does not cover non-EWP products that have been exposed to wet or corrosive environments. This warranty does not cover stainless steel surfaces that have not been properly maintained.

<u>NO OTHER WARRANTIES</u>. VIKING MAKES NO WARRANTIES RELATING TO ITS PRODUCTS OTHER THAN AS DESCRIBED ABOVE AND DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTIES OR MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE.

<u>EXCLUSION OF CONSEQUENTIAL DAMAGES</u>. VIKING SHALL NOT, UNDER ANY CIRCUMSTANCES, BE LIABLE TO PURCHASER, OR ANY OTHER PARTY, FOR CONSEQUENTIAL, INCIDENTAL, SPECIAL OR EXEMPLARY DAMAGES ARISING OUT OF OR RELATED TO THE SALE OR USE OF THE PRODUCT SOLD HEREUNDER.

<u>EXCLUSIVE REMEDY AND LIMITATION OF LIABILITY</u>. WHETHER IN AN ACTION BASED ON CONTRACT, TORT (INCLUDING NEGLIGENCE OR STRICT LIABILITY) OR ANY OTHER LEGAL THEORY, ANY LIABILITY OF VIKING SHALL BE LIMITED TO REPAIR OR REPLACEMENT OF THE PRODUCT, OR AT VIKING'S OPTION, REFUND OF THE PURCHASE PRICE AS THE EXCLUSIVE REMEDY AND ANY LIABILITY OF VIKING SHALL BE SO LIMITED.

IT IS EXPRESSLY UNDERSTOOD AND AGREED THAT EACH AND EVERY PROVISION OF THIS AGREEMENT WHICH PROVIDES FOR DISCLAIMER OF WARRANTIES, EXCLUSION OF CONSEQUENTIAL DAMAGES, AND EXCLUSIVE REMEDY AND LIMITATION OF LIABILITY, ARE SEVERABLE FROM ANY OTHER PROVISION AND EACH PROVISION IS A SEPARABLE AND INDEPENDENT ELEMENT OF RISK ALLOCATION AND IS INTENDED TO BE ENFORCED AS SUCH.

If trouble is experienced with the **E-32T-SS-IP**, for repair or warranty information, please contact:
Viking Electronics, Inc., 1531 Industrial Street, Hudson, WI 54016 Phone: 715-386-8666

WHEN PROGRAMMING EMERGENCY NUMBERS AND (OR) MAKING TEST CALLS TO EMERGENCY NUMBERS:

Remain on the line and briefly explain to the dispatcher the reason for the call. Perform such tests in off-peak hours, such as early morning or late evenings.

PART 15 LIMITATIONS

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

CANADA

This class A digital apparatus complies with Canadian ICES-003. Cet appareil numerique de la classe A est conforme a la norme NMB-003 du Canada.

Product Support: 715-386-8666