KNG Series Trunked Radio Programming Guide

1 Table of Contents

2 RELM/BK P25 Trunked radio subscriber units and options.

RELM/BK Radio KNG Series Project 25 radios are available in all public safety and government frequency bands for land mobile radio use. KNG Series radios meet FCC and NTIA requirements for narrowband operation. Offering a rich feature set including analog conventional, P25 digital conventional, and P25 trunked. Encryption options are available for secure tactical communications.

	Frequency Range	Full Keypad	Limited Keypad	Mobile Radio	Base Station
VHF	136-174 MHz	KNG-P150	KNG-P150T2	KNG-M150	KNG-B150
UHF Range 1	380-470 MHz	KNG-P400	KNG-P400T2	KNG-M400	KNG-B400
UHF Range 2	440-520 MHz	KNG-P500	KNG-P500T2	KNG-M500	KNG-B500
700/800 MHz	763-870 MHz	KNG-P800	KNG-P800T2	KNG-M800	KNG-B800
Portable Radio Options					
KZA0558	Intrinsically Safe				
KZA0577	DES OFB / AES Encryption Includes FIPS-140-2 Approved Hardware				
KZA0570	Project 25 Over the Air-Rekey (OTAR)				
KZA0579	Project 25 9600 Baud Trunking – 2048 Channel				
KZA0581	Multi-Cast Vote Scan Plus				
KZA0582	Over the Air Reprogramming				
KZA0591	GPS Option for KNG Portables				
KZA0593	Project 25 Phase II-TDMA Trunking				
KZA 0595	Project 25 Link Layer Authentication (Radio Authentication)				
Mobile Radio Options					
KZA0154	Option, High Power, 110W KNG-M150 Only				
KAA0660	Remote Control Head Plug & Play KNG Mobiles				
KAA0670	Handheld Control Head				
KZA0569	P25 9600 Baud Trunking				
KZA0576	DES OFB / AES Encryption Includes FIPS-140-2 Approved Hardware				
KZA0580	P25 Over the Air Rekeying (OTAR)				
KZA0581	Multi-Cast Vote Scan Plus				
KZA0589	GPS Option for KNG Mobiles				
KZA0592	Over the Air Reprogramming				
KZA0594	Project 25 Phase II-TDMA Trunking				
KZA0596	Project 25 Link Layer Authentication (Radio Authentication)				
KAA0261	External Speaker 20W, 4 Ohm, W/ Mounting Bracket				
KAA0276	Standard Handheld Microphone KNG-M				
KAA0290	Handheld Programming Microphone				

3 Capabilities of RELM/BK P25 Trunked Radios

Vocoder	DVSI IMBE/AMBE+2 Enhanced Dual Rate Vocoder Selectable Automatic Gain Control (AGC) Selectable Background Noise Reduction	Version 1.80
Systems	Conventional or Trunked Radio Systems	16
Channels/Groups	Total number of Channels or Talk Groups	2048
Channel ID Table	Channel Plan for VHF/ UHF Trunked Systems	16 / System
Radio ID List	Preprogrammed Radio ID Alias	1024 / System
Control Channels	Channel used to transmit and receive channel assignment data or other commands	256 / System
Sites	Fixed infrastructure Aliases	512 / System
Dynamic Site Array	Internal list of adjacent sites used for roaming	32
Encryption Keys	AES (256 bit) , DES and 40 bit RSA	64
Key Sets	Groups of Keys usually used in OTAR	2
Packet Data	Ability to receive voice and data on the same channel.	Integrated Voice and Data
Receiver Mode	Ability to receive standard P25 signals (C4FM) and simulcast (LSM) modulation	C4FM/CQPSK
Phase 1/Phase 2	Project 25 Phase 1 FDMA or Phase 2 TDMA	Phase 1:C4FM/CQPSK Phase 2:H-CPM/H-DQPSK
Over The Air Rekey	Ability to securely update encryption Keys	P25 OTAR
Authentication	Project 25 Link Layer Authentication for registration	AES-128
Over the Air Reprogramming	P25 Packet Data System can be utilized to read or write subscriber radio programming	P25 Compatible
System Redundancy	Ability for subscriber radios to continue operation during system failure	Site Trunking, Failsoft and Direct
System Coverage	Ability to limit P25 trunking operation on a single RF site or for automatic roaming across multiple RF sites to include multiple zones or systems	Single Site or Wide Area
Advanced Trunking Features	Busy Queuing, Inhibit/Uninhibit, Radio Check, Continuous Assignment Updating, Dynamic Regrouping, Talk Group/Super Group Patch, Site Search, Site Lock, Radio Monitor/Radio Trace, Status Query/Messaging	

4 Programming Software Installation

4.1 RNDIS Driver Installation:

NeoVision uses the RNDIS driver to communicate with the KNG radio. RNDIS is a general-purpose driver, developed by Microsoft and used to connect a wide variety of intelligent devices (such as smartphones) to a Windows-based computer over a USB interface. RNDIS creates a TCP/IP network connection between the computer and the radio and therefore may be affected by firewalls and other network constraints.

Like most plug-and-play devices, the RNDIS driver should install automatically when the KNG radio is attached to an Internet-connected computer and turned on. Since the RNDIS interface is generic, Windows should transparently navigate through the differences in operating system (Windows XP vs. Windows 7) and install the correct version. By default, the user should allow the computer to install the driver automatically.

4.2 Manual Driver Installation

In certain cases, the automatic installation might fail, or the computer might be disconnected from the Internet as a policy. In these cases, the user can install the driver manually. To install the RELM RNDIS driver, do the following:

1. With the radio turned on and plugged in open the Device Manager
   Start | Control Panel | Hardware and Sound | Device Manager
2. Under Other Devices right click RNDIS/Ethernet Gadget
3. Choose Update Driver Software
4. Select "Browse my computer for driver software"
5. (64-bit) Point to a folder that has the file RNDIS.Ethernet.x64.inf and select.
6. (32-bit) Point to a folder that has the file RNDIS.Ethernet.x86.inf and select.

4.3 NeoVision Problems / FAQs

4.3.1 Windows Vista/Windows 7

"Error reported during network adapter setup: 2147749891".

This issue is related to the Win7 OS User Account Control feature preventing proper IP configuration between NeoVision and the radio. To correct this issue, take the following steps:

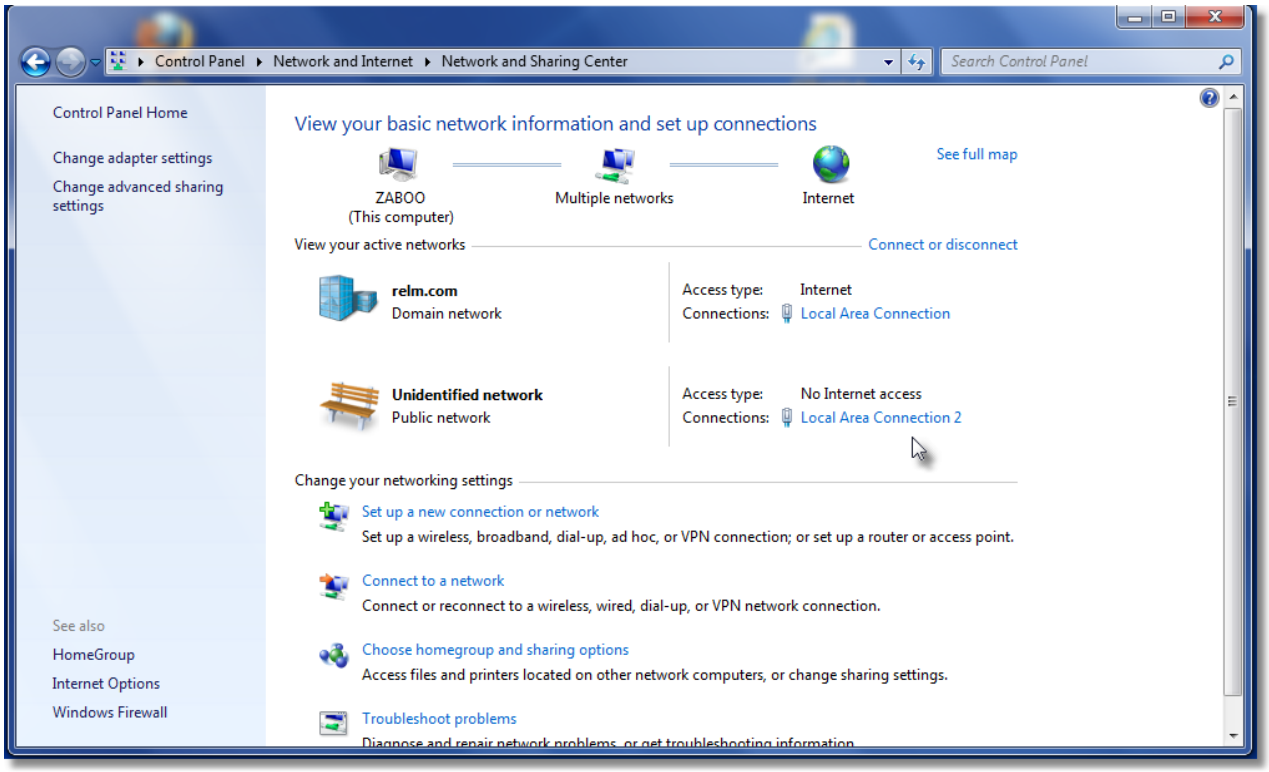
- Locate the NeoVision "exe" file. The default installation directory is: C:Program Files(x86)/Relm Wireless Corp/NeoVision. The NeoVision exe can also be accessed via the Start menu. (The file type is Application).
- Hold down the "Shift" key and right click on NeoVision.exe.
- Select "Run as administrator" and click Yes when prompted.
- This will only have to be done the first time the software is executed.

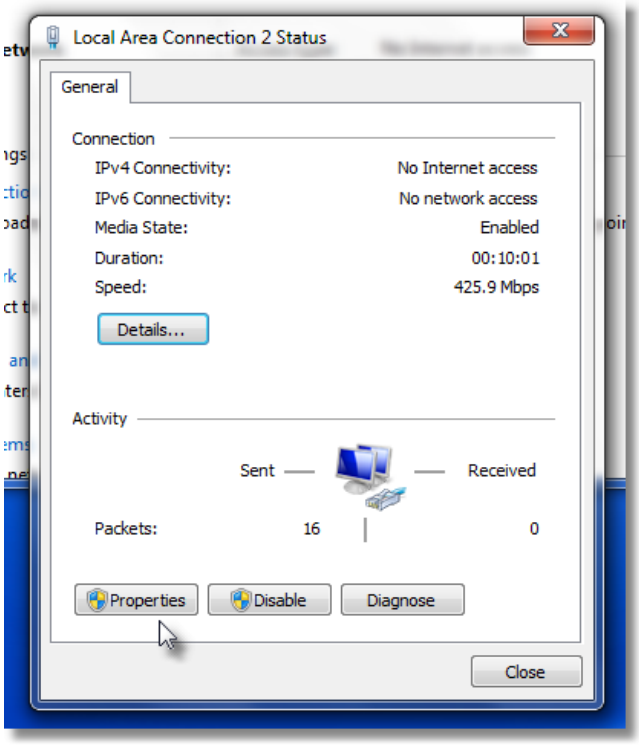
4.3.2 IP Address Mismatch

The RNDIS driver sees other devices as network computers, each with its own unique IP address. The KNG radio expects to see the computer hosting NeoVision at IP address 10.250.46.5. During NeoVision installation, this address is loaded into the driver. However, the process occasionally fails, and the user must load the address manually.

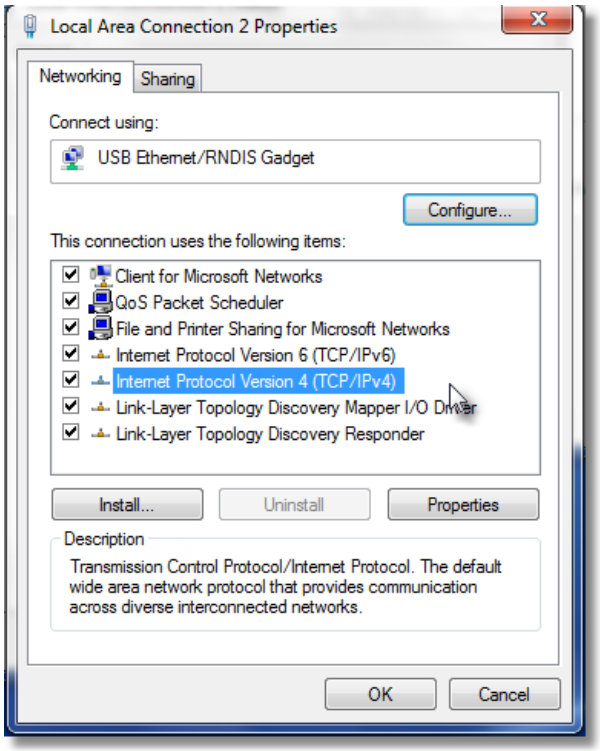
Steps:

- Open Control Panel.
- Navigate through: Network and Internet|Network and Sharing Center|View Basic Network Information.
- (In lower-right corner of window), click “Local Area Connection 2”.

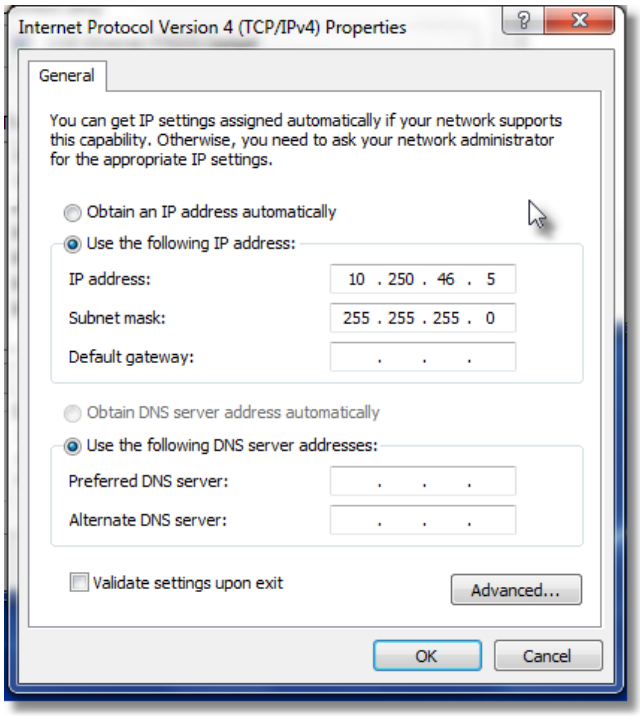




- Click “Properties”.
- Click “Internet Protocol Version 4 (IPV4)”.



- Click “Properties”.



- IP Address should be 10.250.46.5. Correct if wrong.
- Subset Mask should be 255.255.255.0. Correct if wrong.

4.4 Bad Driver Install

If the NeoVision driver has been improperly installed, you will need to reinstall it with the Internet disconnected:

- Ensure that the proper driver is downloaded or available on the CD.
- Disconnect the PC from the Internet.
- In Control Panel, navigate to Device Manager.
- Connect the radio to the PC and turn the radio on.
- Right-click on the radio driver icon. It will be found either in Network Adaptors as “USB Ethernet/RNDIS Gadget” or in Universal Serial Bus Controllers as “Unknown Device”. Click “Update Driver” and browse to the proper file location. Click the checkbox “Erase driver software”—this will erase the cached copy of the incorrect driver.

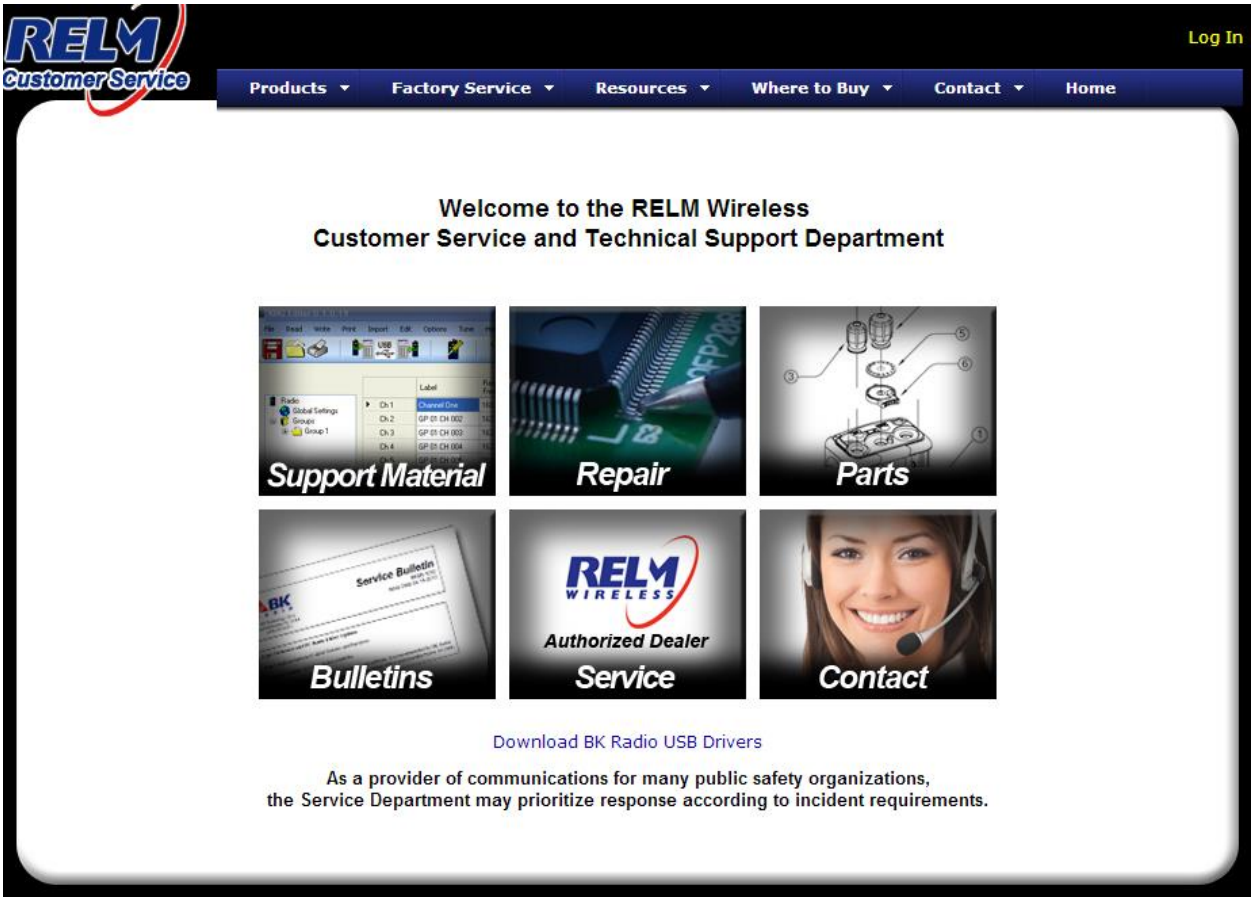
You should now be able to reinstall the driver as detailed in Section 4.2.

5 KNG Series Firmware Updates

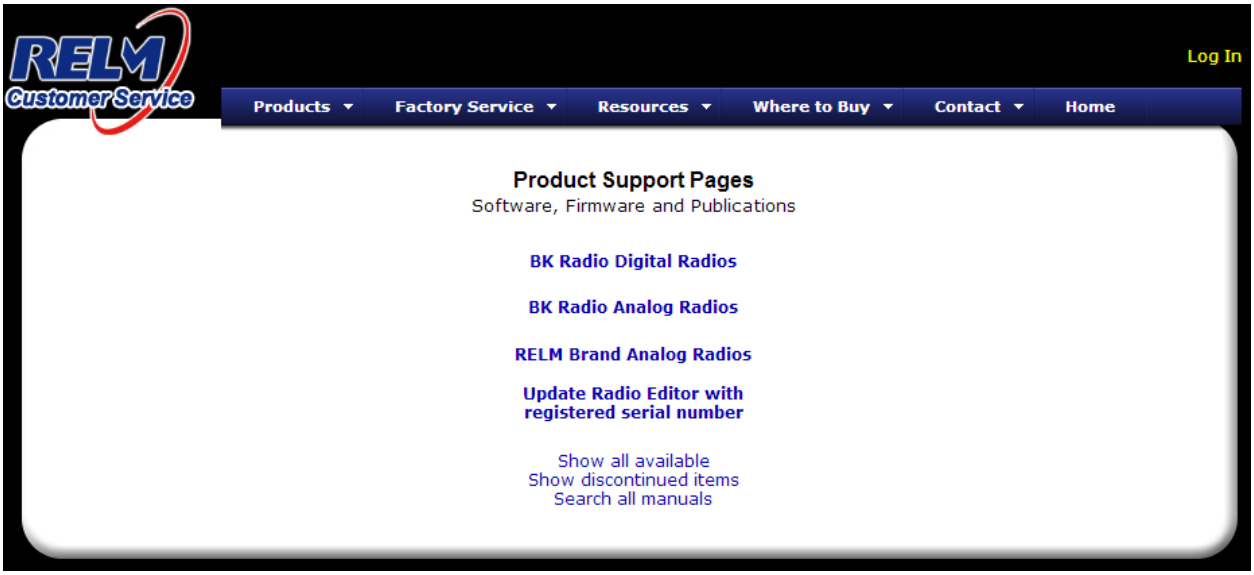
RELM Maintains radio firmware updates on the RELM Service Web Portal. This section provides instructions for downloading firmware revisions and installing them in KNG series radios. RELM firmware updates are available at no cost to the end user.

5.1 RELM Service Website

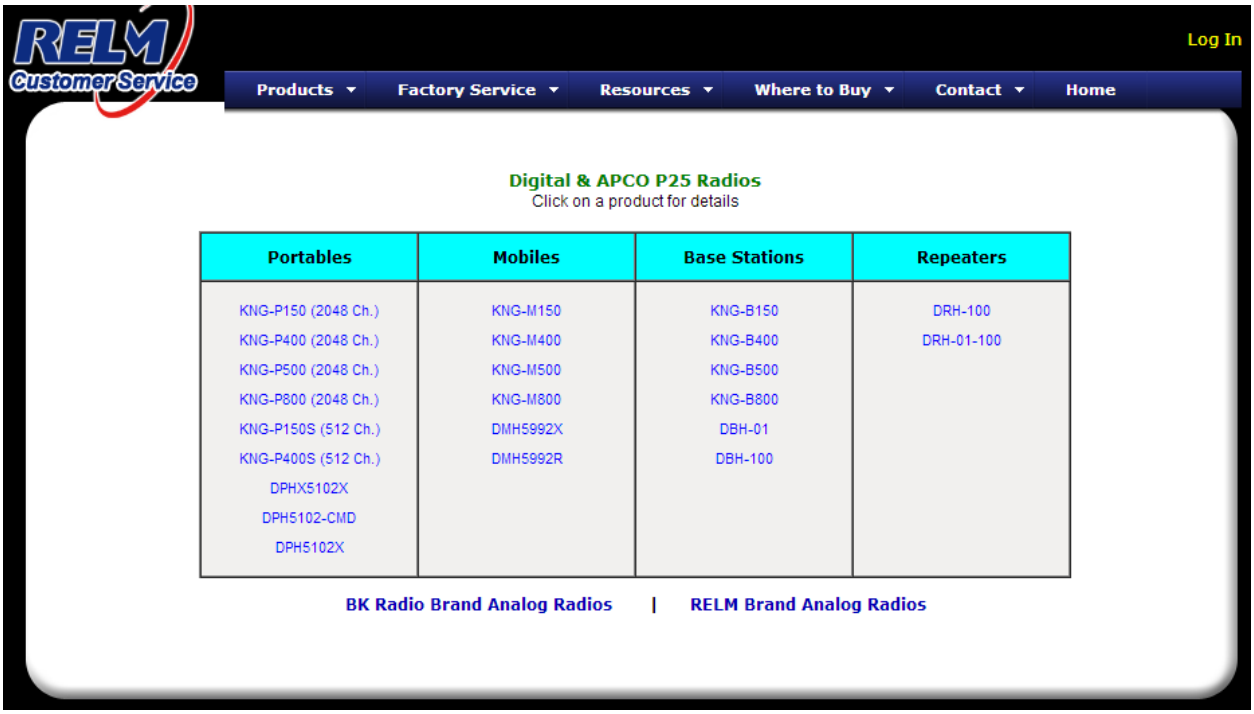
The RELM service website can be found at http://www.relmservice.com/ . From this website you can access the many services RELM customers are offered. To obtain the latest radio Firmware and drivers select the Support Material hub.



Then select the radio type (typically it is BK Radio Digital Radios).

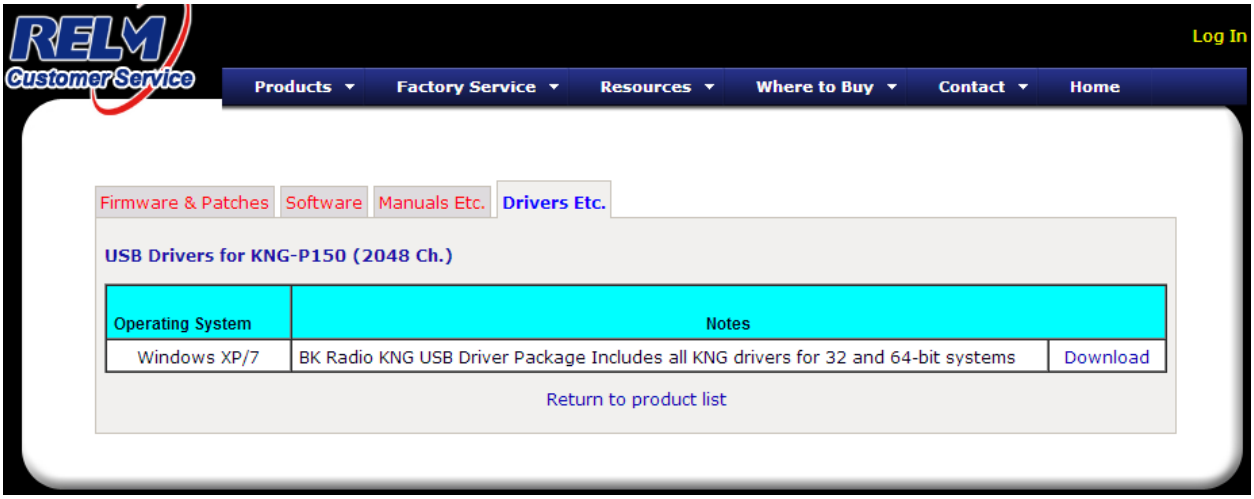


From here you can select whether you need a Mobile or Portable and the banding.



5.2 Firmware Driver Installation

The firmware drivers are the same for the Portable, Mobile, and Remote Control Head (RCH) and only need to be installed once. The download for the driver can be found on the service website after you select a radio, in the last tab.

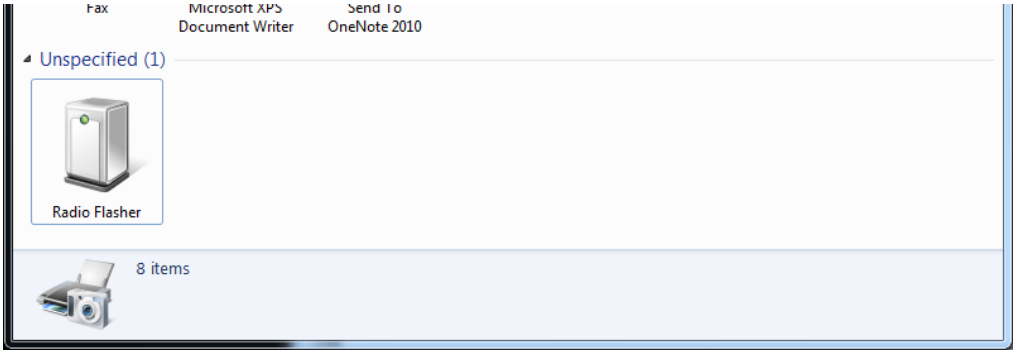


After you have downloaded the zip file, extract it to a folder you can find easily (the desktop works best).

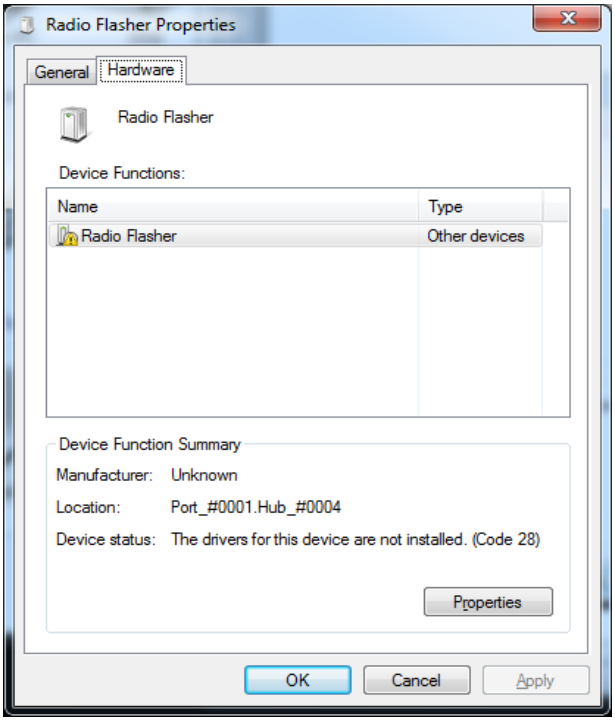
1. With radio turned off, connect the radio to the PC via USB cable (use KNG side-port adapter for portables)
2. While holding the radio push-to-talk, turn on radio power
3. When the top LED flashes blue, release the push-to-talk button

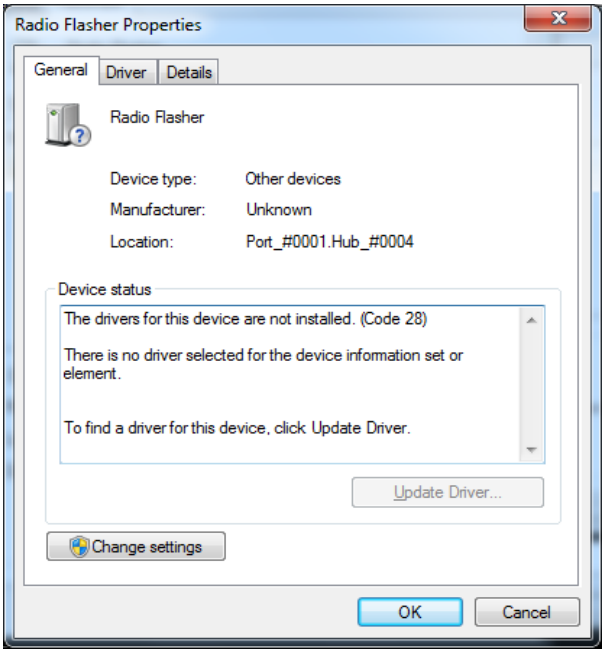
Windows will attempt to automatically install the drivers or prompt for driver installation. If prompted, select the option for selecting the location of the drivers. Then select the folder you extracted from the download.

If not prompted to install drivers you will have to select the device and do it manually. On Windows, select the start menu and devices and printers. The radio is listed as Radio Flasher.

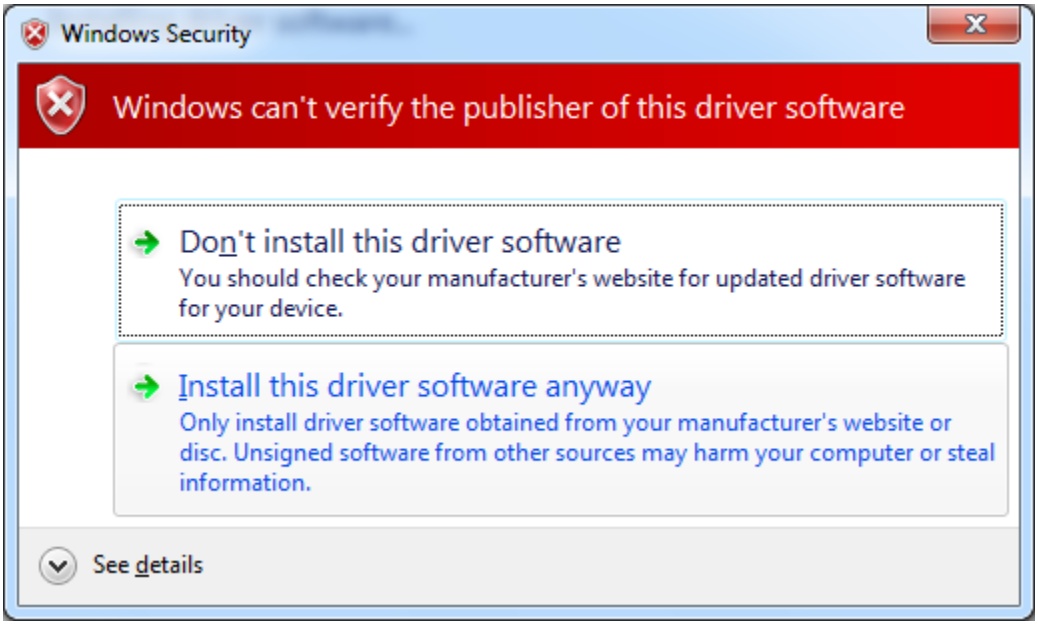


Double click the icon and select the Hardware Tab. Select Properties and then Change settings.





From here select Update Driver and when prompted select Browse my computer for driver software. Then select the folder you created from the downloaded zip file. If Windows Security cannot verify the publisher of the driver, select Install this driver software anyway.



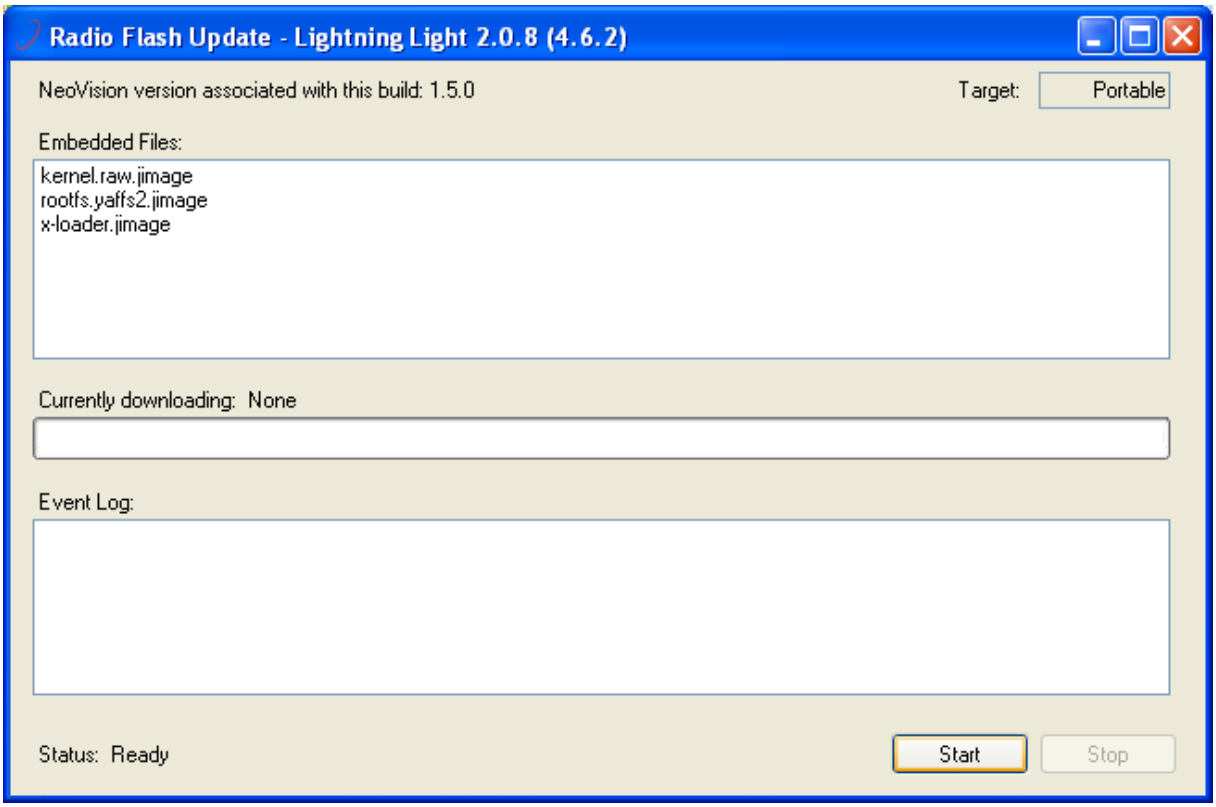
5.3 Firmware Upgrade

5.3.1 Portables

The latest released firmware can be found on the service website. After you have selected the band your radio is in you can download the firmware by selecting the download link. You can also view the release notes for each version of firmware for a list of new features and bug fixes. After downloading the zipped file, unzip the file into a folder that is easy to find. Then run the install file. If flashing radios right away insure the Run Lightning Light is selected. Once the software launches you are ready to upgrade.

1. With the radio powered off, connect the radio to the PC via the USB cable (use KNG side-port adapter for portables)
2. While holding the radios push-to-talk, turn on radio power.
3. When the LED flashes blue, release the push-to-talk button

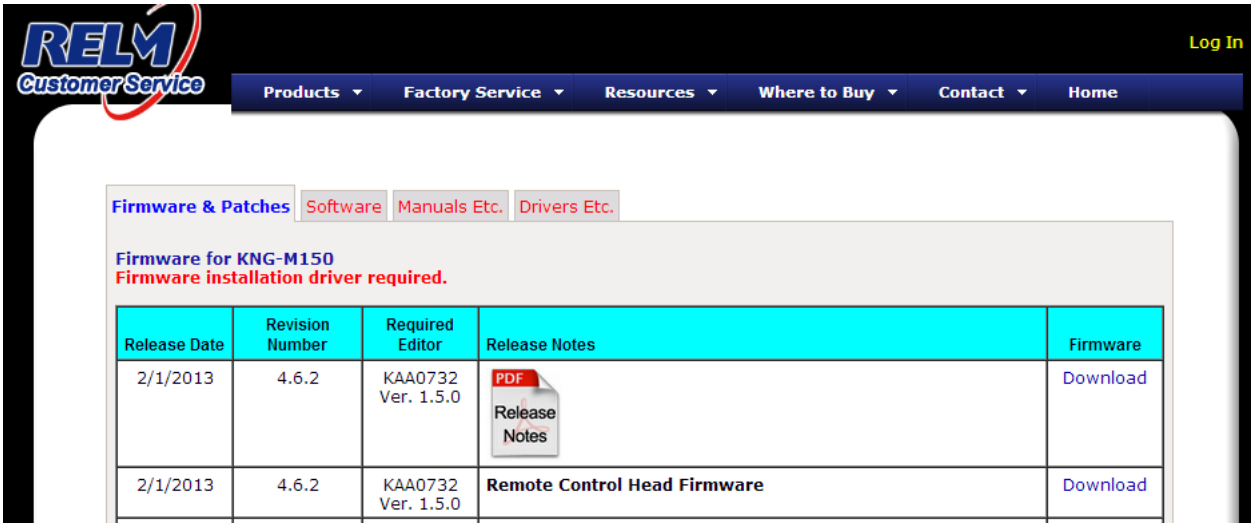
4. Double check that the software target matches the radio you are flashing (Here the target is a portable and the radio connected to the PC is a portable). If there is a mismatch the radio could be inoperable after it is flashed..



5. Click the Start button to begin. A status bar will indicate the progress. Wait for the radio to reboot before disconnecting from the PC. If you are finished click the exit button. If there are more radios to be done repeat from step 1.

5.3.2 Mobiles and Remote Control Head (RCH)

The mobile and RCH firmware can be found both at the same page on the service website. The steps for updating the firmware are the same as the portable.



6 Advanced System Key Generation and Use

6.1 Introduction

This section provides a brief description of the Advanced System Key (ASK) mechanism for the KNG radio. ASK is used to restrict programming access of the KNG radios to authorized users only.

6.2 Advanced System Key Components

The ASK consists of two hardware devices and two software components: the Master Key and the Child Key.

6.2.1 Master Key

The Master Key is a USB device, configured and supplied by RELM, which allows the user organization to create child keys with the Child Key Maker software.

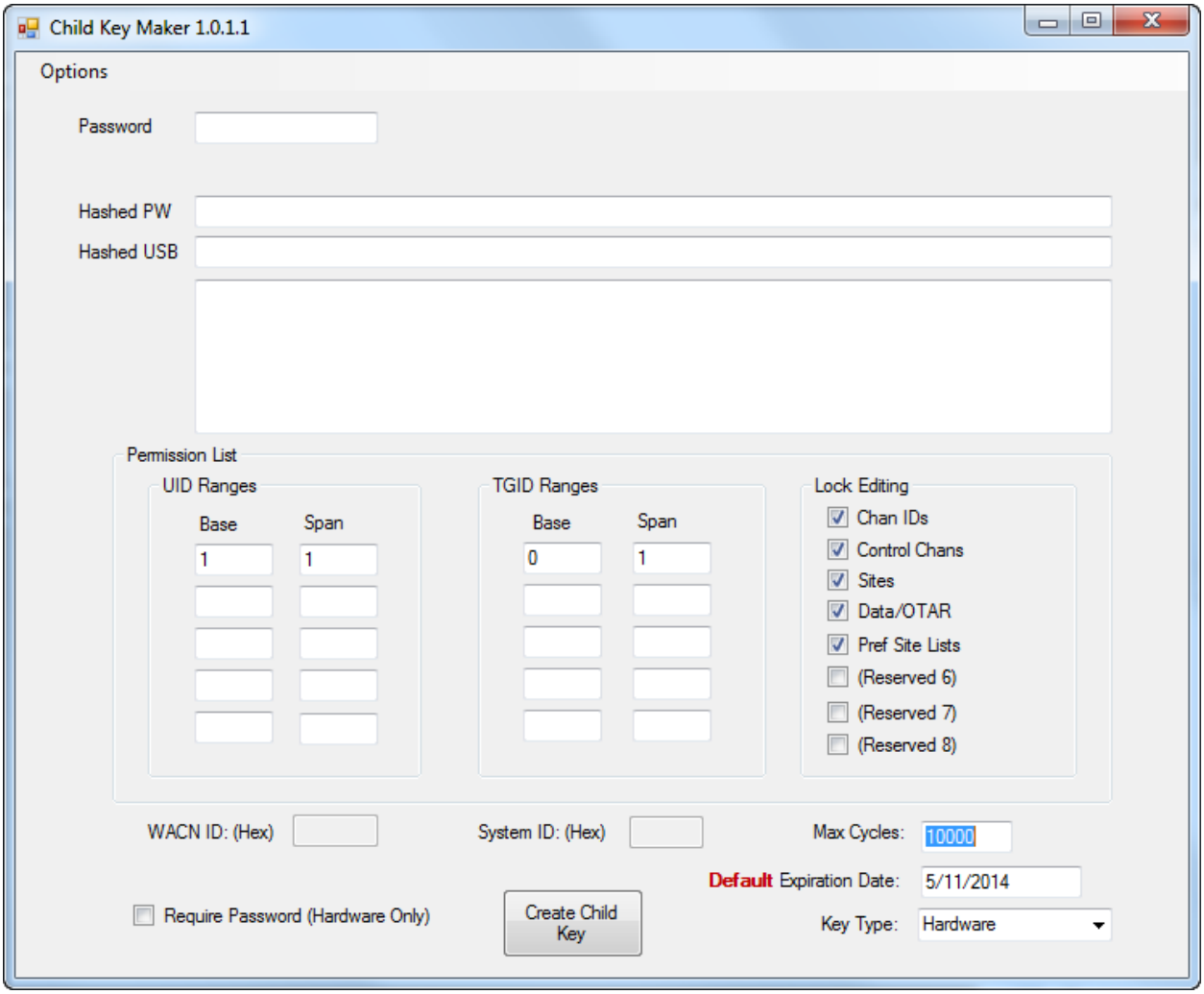
6.2.2 Child Key

The Child Key is the core of the ASK scheme. It is a cryptographic based key which contains both the access list for various programming parameters and the authentication information which allows only authorized users the permission to read, modify, and write configuration information to the radio. It is created and configured with Child Key Maker. Principally a USB Hardware based key, with provisions for creating a software key.

6.2.2.1 Child Key Generation

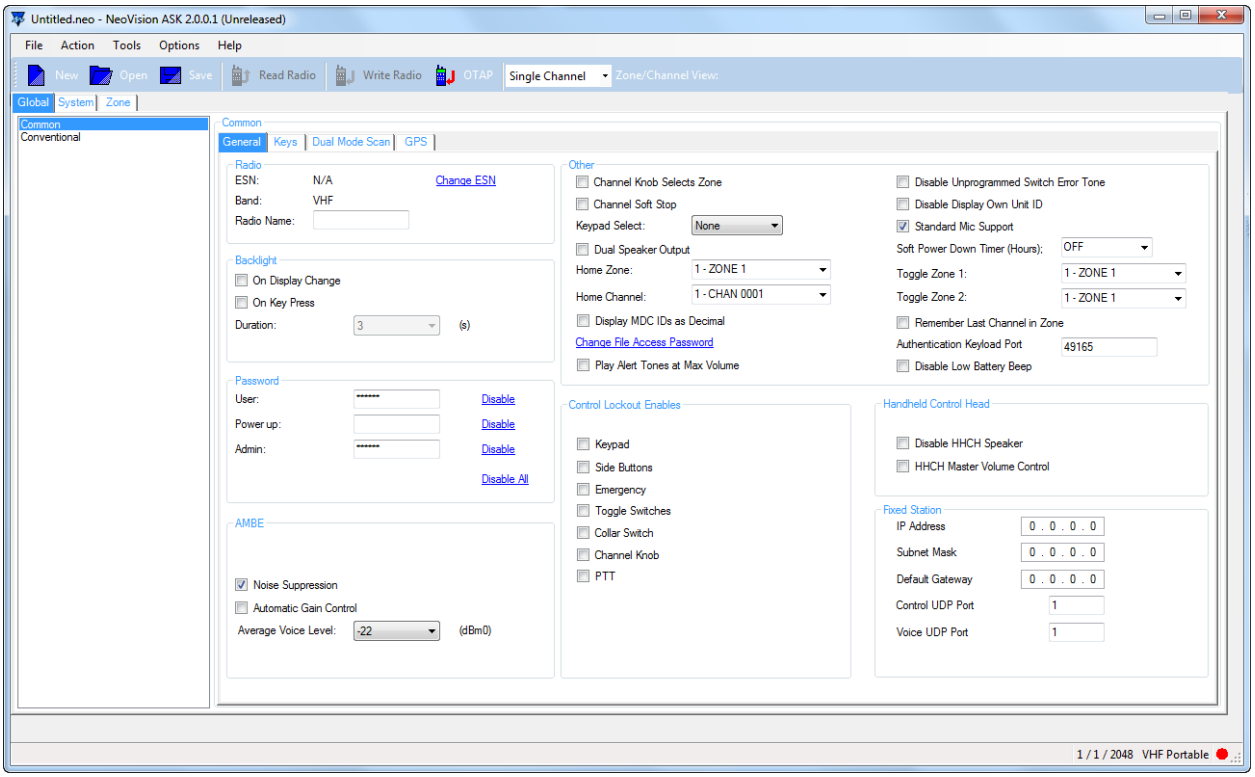
The Windows program “Child Key Maker” (CKM) creates the child (user) keys. CKM can customize the permission list by setting:

a. Ranges of values for UID/TGID
b. Permission list for modification of various parameters
c. Maximum number of programming cycles
d. Expiration date for the key

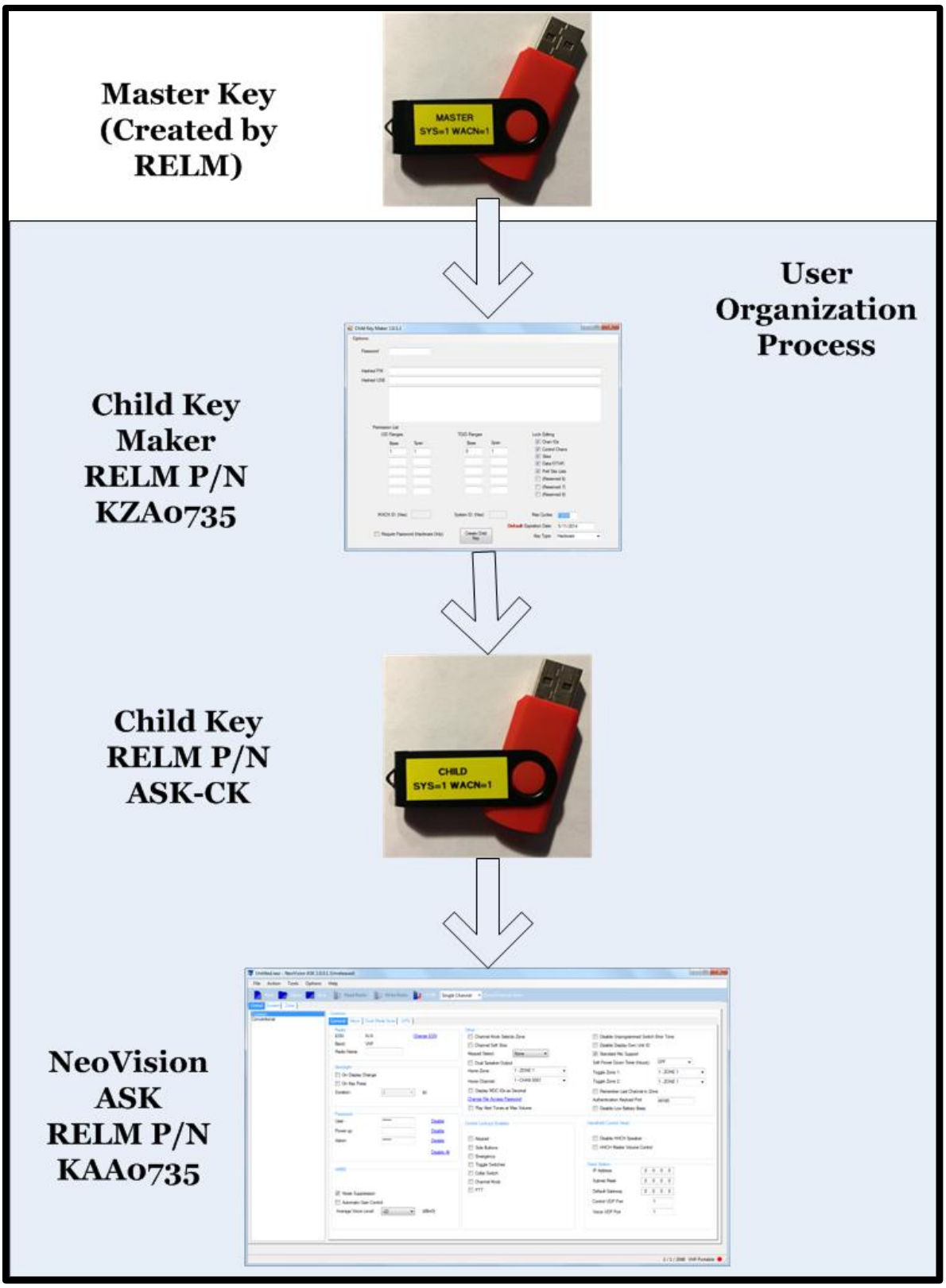


6.2.2.2 NeoVision Advanced System Key (ASK)

NeoVision ASK is the Windows-based software used to configure software settings for KNG radios. The ASK scheme works by restricting access to NeoVision capabilities, based on the child key.



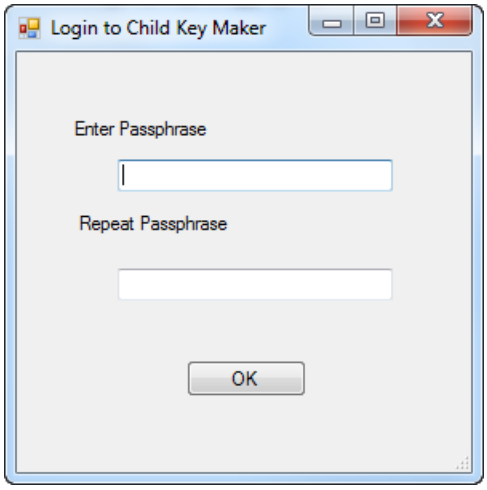
6.2.2.3 Advanced System Key Overview

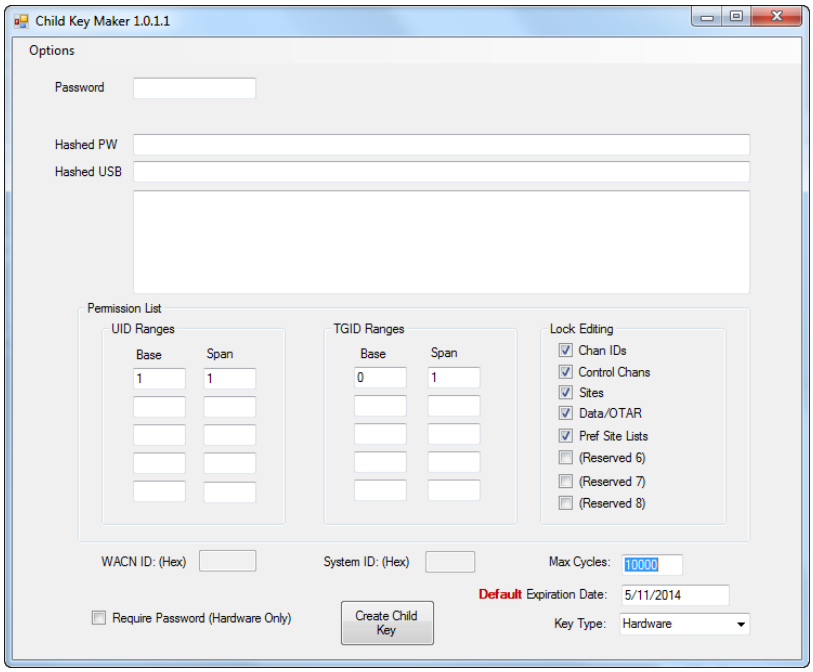


6.3 ASK Operation

6.3.1 Create the Child Key

a. Insert the Master Key (supplied by RELM) into a USB port of the computer.
b. Start Child Key Maker.exe.
c. If required (by the master key), enter the passphrase in each required box to log in.
   Note: If a passphrase is required, the user must enter a phrase the first time Child Key Maker is used. This phrase will be used for subsequent access.

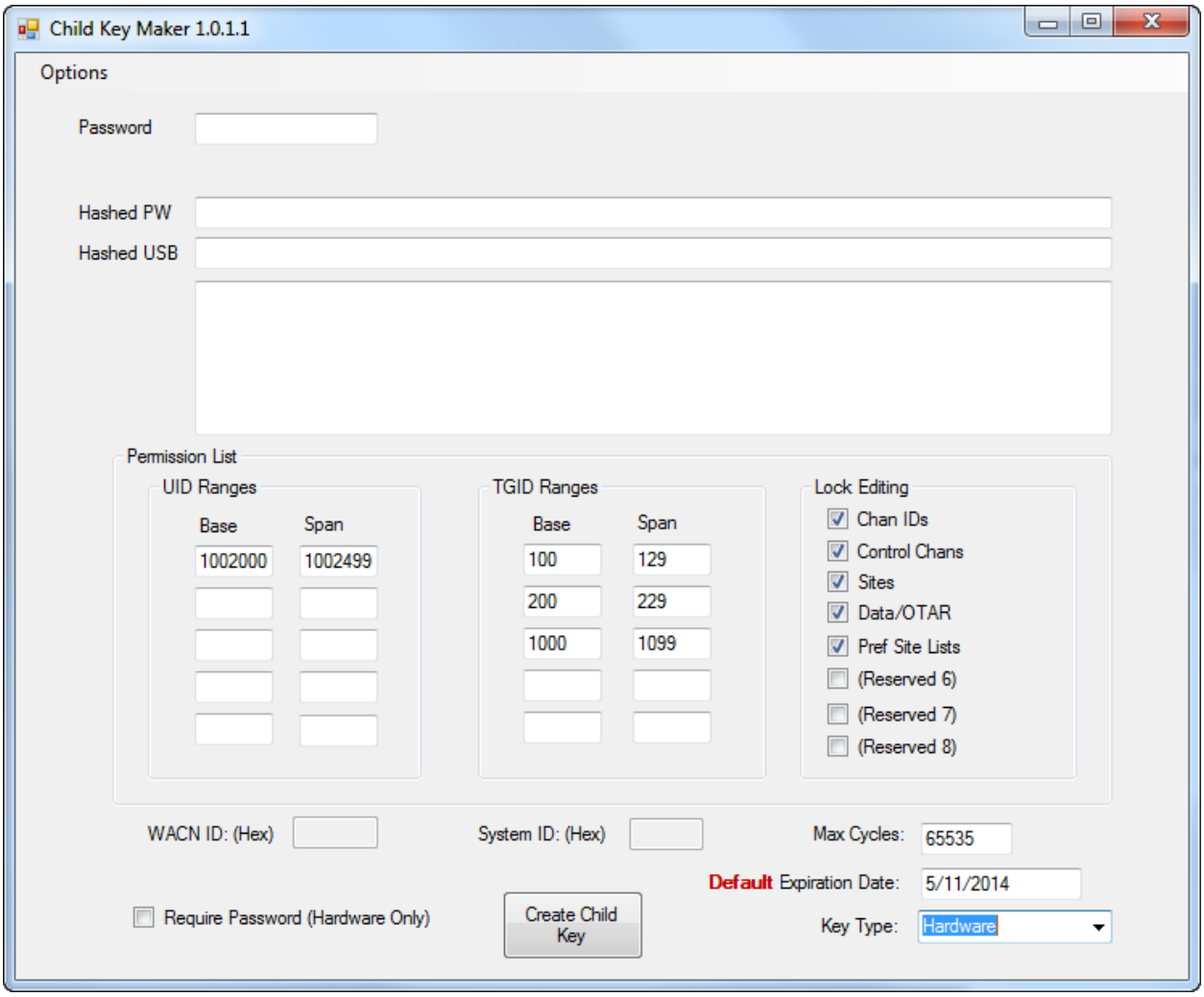




6.3.1.1 Define Limits of the Child Key

a. Set the ranges of allowed Unit IDs (up to 5 ranges are allowed). Leave these fields blank to allow all values.

b. Set the ranges of allowed Talk Group IDs (up to 5 ranges are allowed). Leave these fields blank to allow all values.



c. Set the other parameter permissions, as desired.

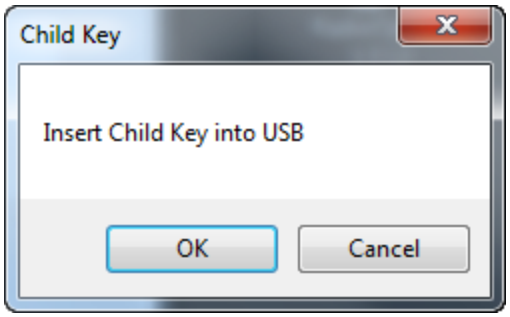
d. Set the maximum number of write cycles permitted. Maximum Value is 65535.

e. Set the expiration date (default is 6 months from the current day).

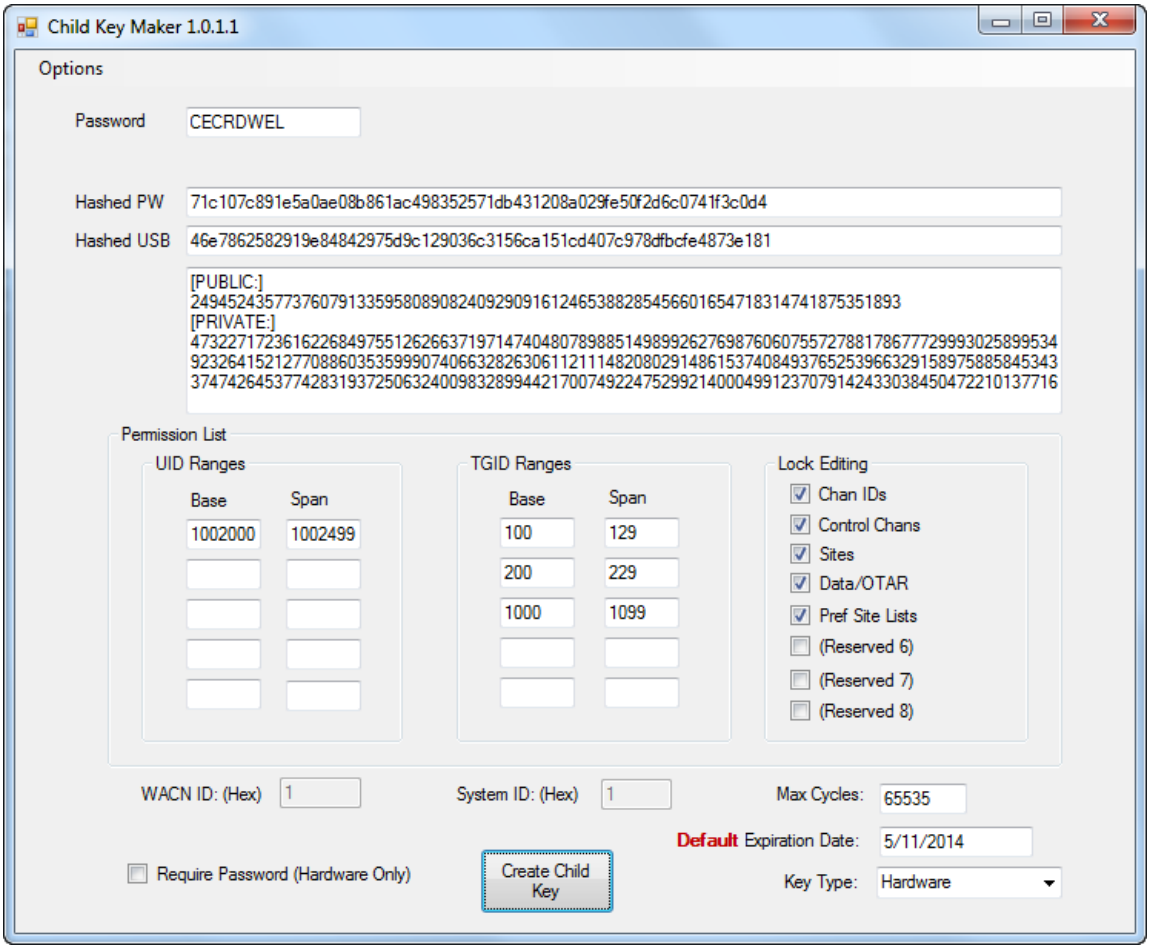
f. If only a software key is desired, select “Key Type: Software” and select a folder to save the access key. This file may be distributed to the end-user’s computer in any typical manner (flash drive, network transfer, etc.).

g. If desired, check the box “Require Password” (hardware key type only). This option will require the NeoVision ASK user to enter an 8-character randomly-generated password.

h. Click “Create Child Key” button to create the key. The permissions, as well as authentication data, will be saved to the key.



i. Insert a new USB Child Key device in a USB slot of computer and click OK.



j. Record the password generated by Child Key Maker. If the box “Require Password” is checked, NeoVision will prompt for it before starting.

k. Repeat steps (a)-(k) for each child key.

7 Radio Firmware Upgrades

KNG

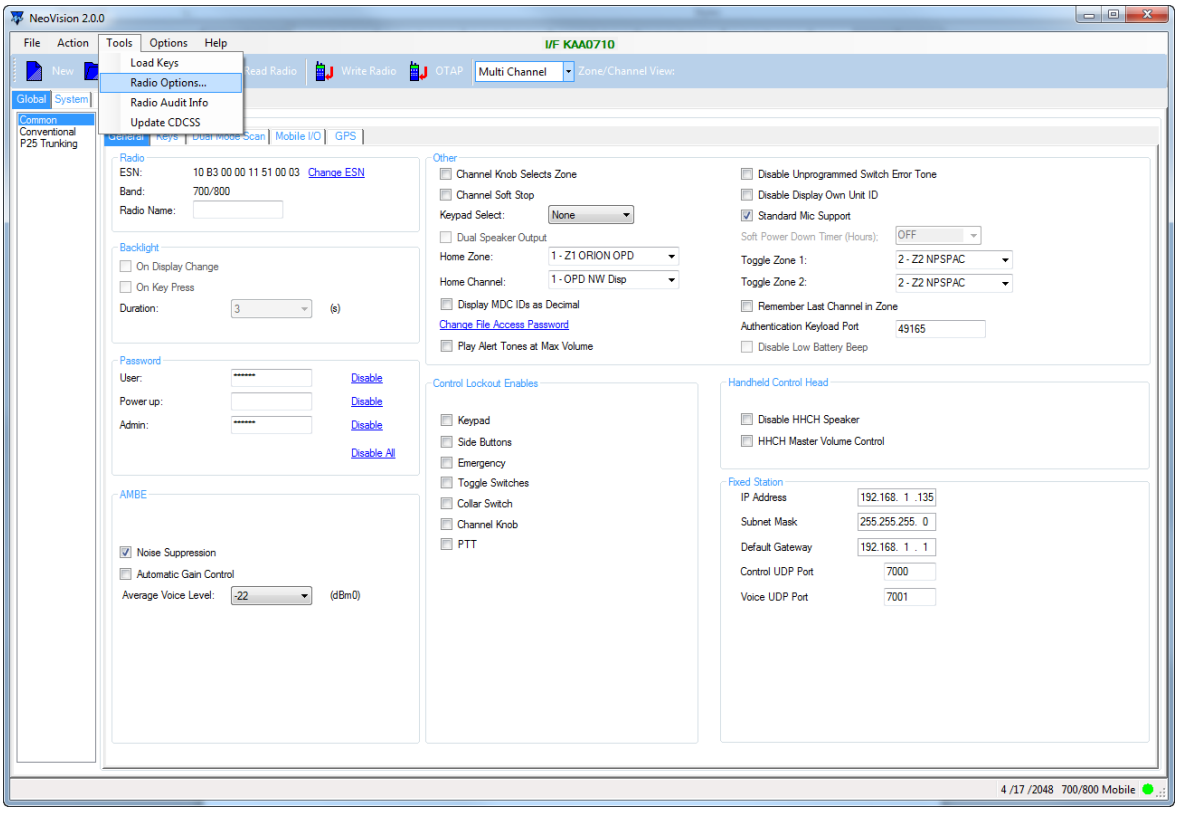
8 Radio Options Upgrades

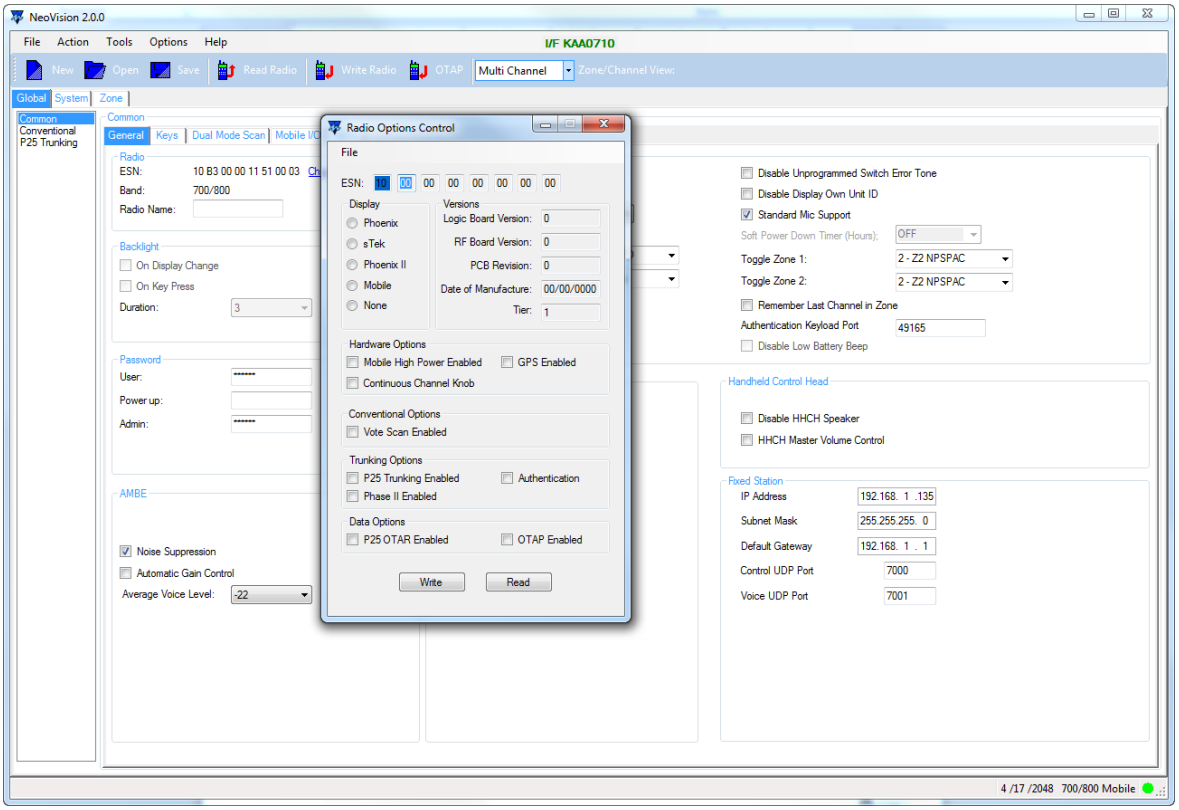
KNG Series radios support upgrading radio features via NeoVision programming software.

8.1 Radio Options Files

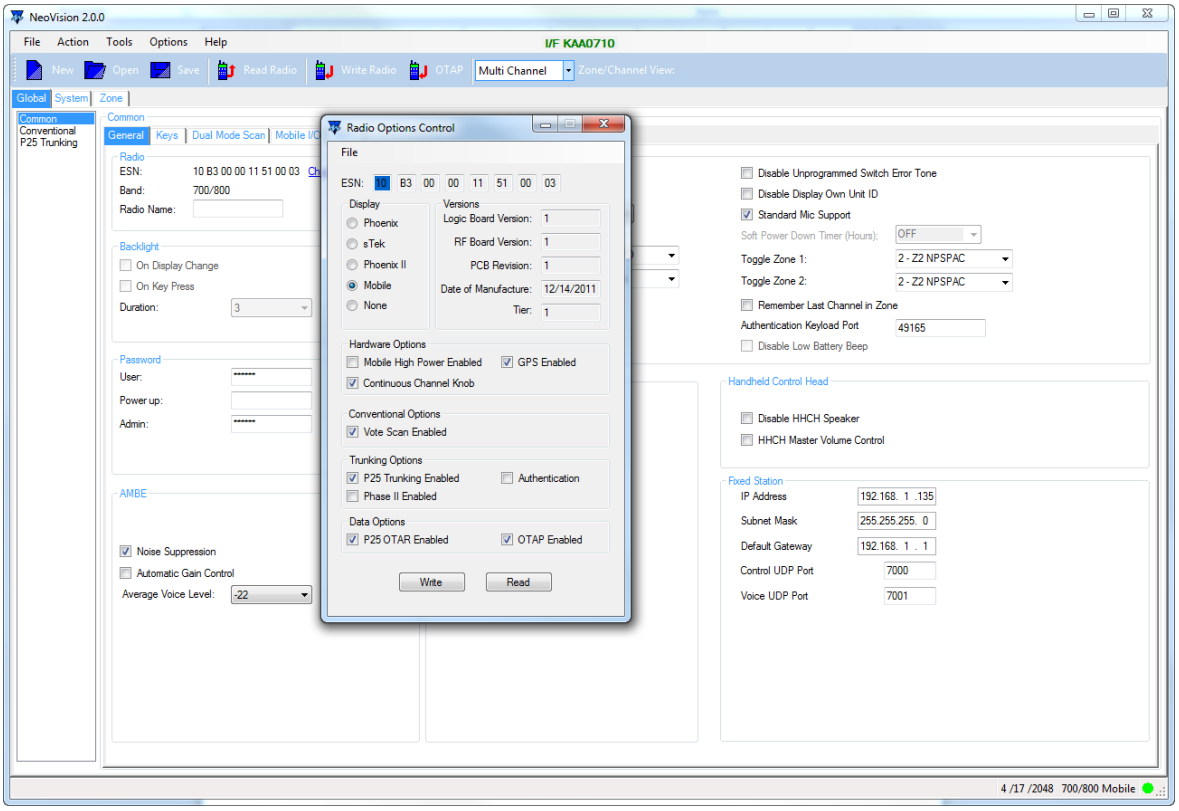
The KNG radio feature set is contained in an encrypted options file. NeoVision programming software can read the current radio options file and save this file. The radio options file is bound to a specific radio by the embedded ESN. The options file can only be loaded into a radio if the ESN matches that stored on the radio.

Use the tools menu to read the current radio options file

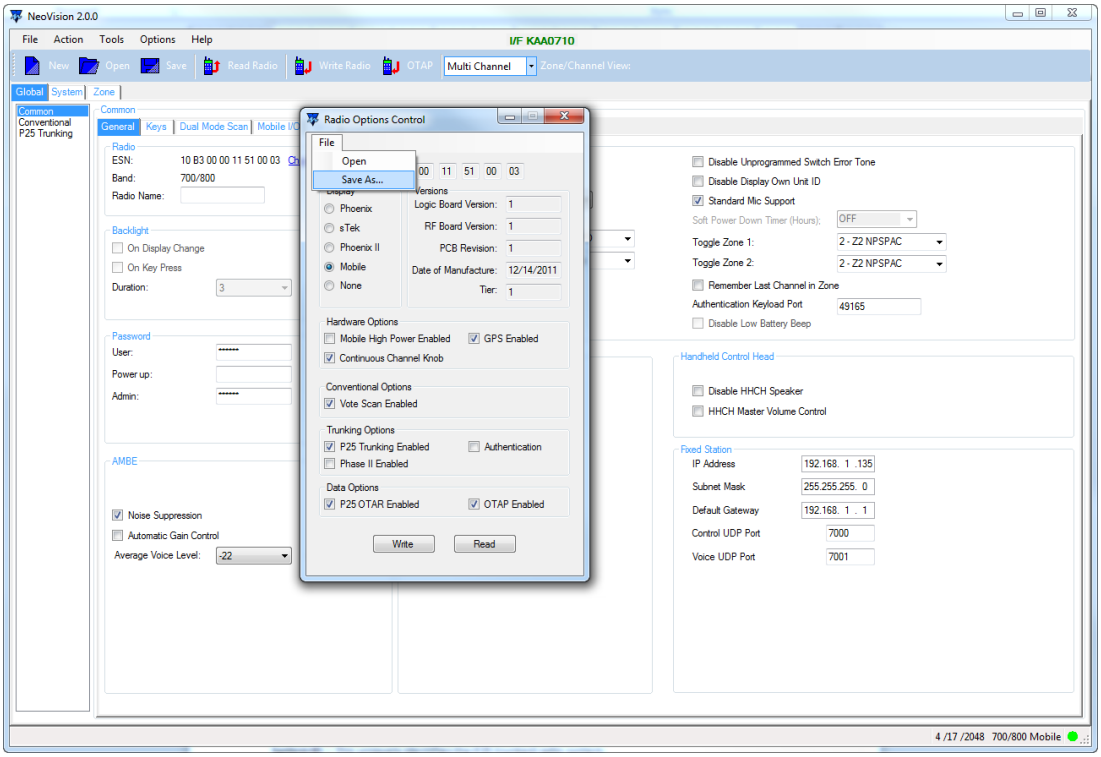




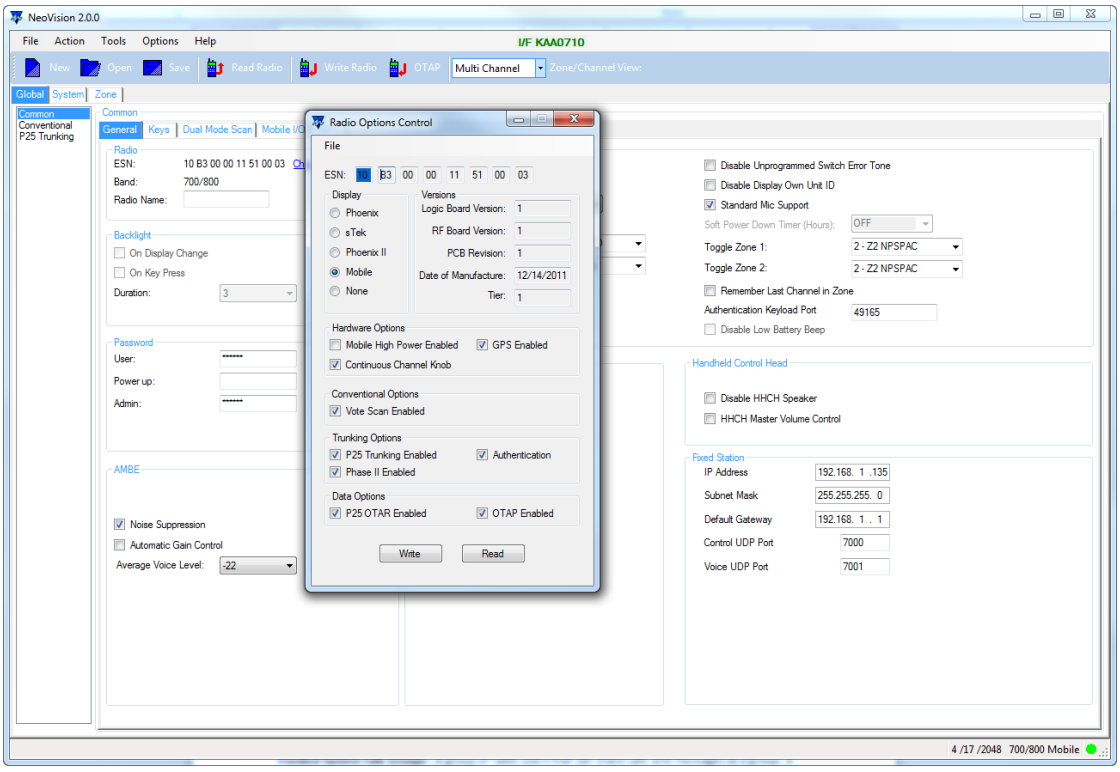
Click Read to upload the current radio options



Use the file/save as command to save the current radio options. The default filename is 'radio ESN.opt'.



Once saved, the options file can be e-mailed to RELM customer service and new options enabled. The updated options file is then written back to the radio by the end user or service tech.



9 Programming KNG Series Radios for Trunked Operation:

Programming Trunked System Parameters Requires a Valid System Key

See Section 10 for additional information on System Keys

To program KNG Series radios for trunked operation on a P25 trunking system, the following information is required:

Radio Unit ID – This uniquely identifies a radio unit on the system.

System ID – This uniquely identifies the P25 trunked radio system.

WACN ID - Wide Area Communication Network is composed of a collection of one or more P25 Systems uniquely identified by a 20-bit WACN ID.

Trunked System Channel Identifier Tables – These tables are used by the subscriber radios to convert channel numbers sent by the trunking system to the appropriate transmit and receive frequency. P25 radio systems typically broadcast the channel identifier tables which allows the KNG radios to dynamically update this information and correct any changes in system programming.

Trunked System Control Channels - Communication channel(s) implemented by a base station or repeater used to transmit and receive channel assignment data or process other control commands from the system. KNG Series radios will initially search pre-programmed system control channels during initial system acquisition. In the event that the designated system is not found, KNG series radios will institute a full spectrum control channel search. This allows new radio sites to be added without reprogramming KNG series radios.

Trunked System Talk Groups - A group of radio users that can share calls and messages as a group. A talk group comprises a group of users who have a need to communicate with each other.

In addition to the required information above, the following optional information can also be programmed.

Trunked System Unit Calls – KNG Series radios allow programming of a unit ID list. This is essentially a phone book which links radio unit IDs to an alias or name. When the radio displays unit ID information and this ID is in the Unit Call list, the radio will automatically display the alias instead of the number.

Trunked System Announcement Groups – Announcement groups are a collection of two or more talk groups. These are also sometimes referred to as multigroups.

Trunked System Sites – KNG Series radios allow radio systems sites to be programmed. If the radio user activates a function that displays site information, the KNG radio will automatically substitute the site alias instead of reporting the site ID.

9.1 NeoVision ASK - Customer Programming Software

KNG Trunked radios are programmed using RELM/BK Radio's NeoVision ASK programming software (KAA0735). A valid system key (either hardware or software) is required to open NeoVision ASK. Only trunking systems for which a valid system key is present can be programmed using NeoVision ASK.

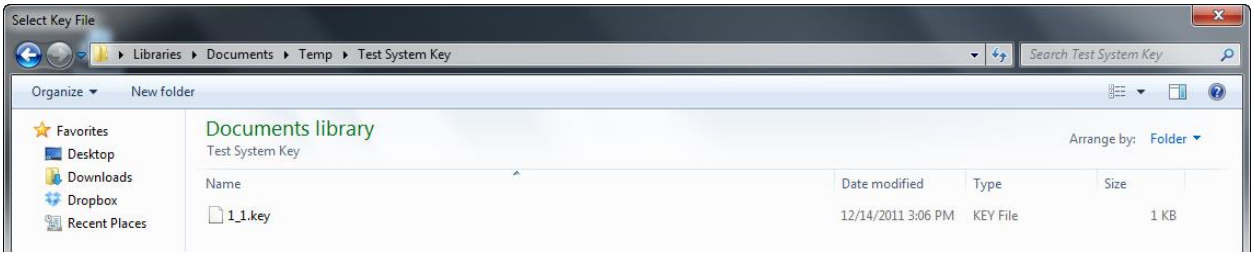
9.1.1 NeoVision ASK

Ensure that the child key is inserted in a USB slot of the computer (hardware key option), or that the key file resides on the computer (software key option).

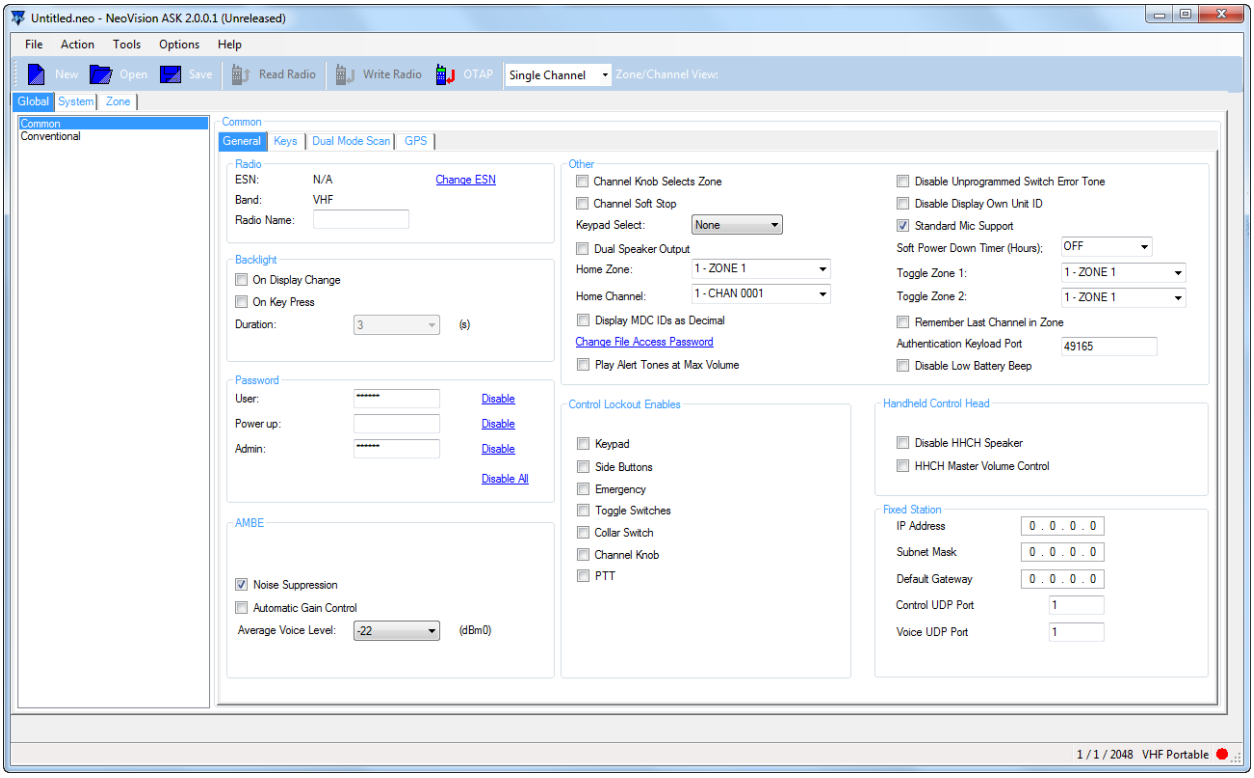
Start NeoVision ASK.

(Hardware key): If prompted, enter the password associated with the key.

(Software key): Select the folder in which the software key resides.



NeoVision ASK can now be used to create or edit an existing radio codeplug.



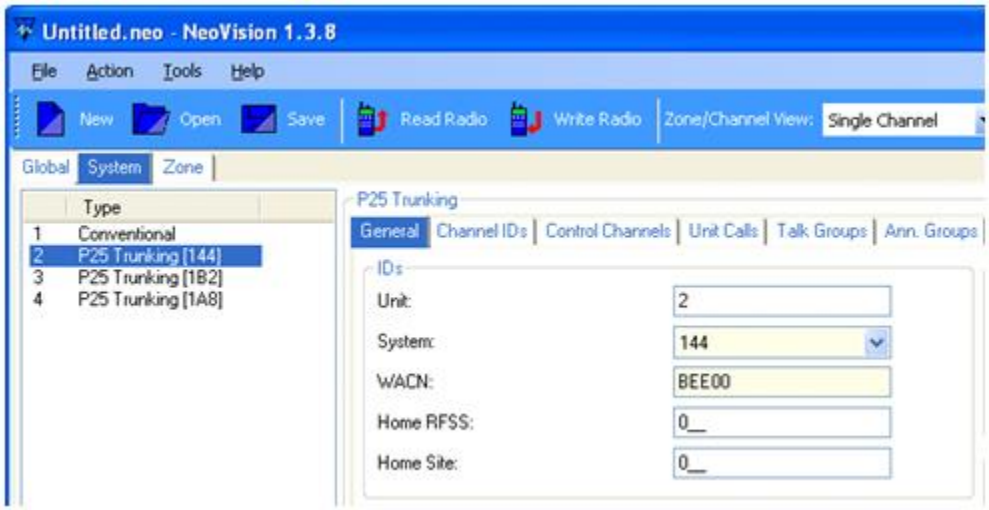
NeoVision ASK will enforce the restrictions programmed on the child key and will allow the user to edit only the permitted parameters and enter only valid UIDs and TGIDs.

NeoVision is now ready to program the remaining trunked system parameters as described below.

9.2 Programming Unit ID, System ID and WACN

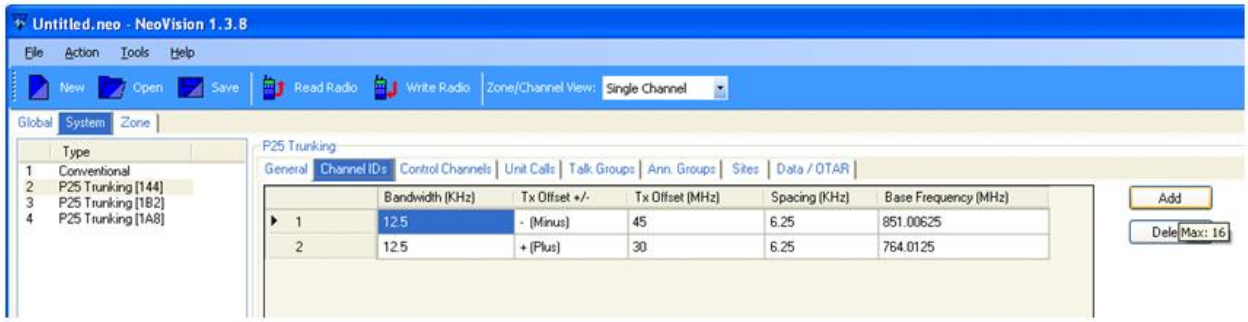
Unit ID, System ID and WACN ID are all programmed on the General Tab of the appropriate trunked system page.

Throughout the programming software, items in yellow shaded boxes are entered in hexadecimal.



9.3 Programming Channel Identifier Tables

The Channel Identifier Tables are programmed on the Channel ID's Tab of the appropriate trunked system page.



Parameters for the channel identifier table should be provided by the radio infrastructure vendor. Channel identifiers for VHF and UHF are dependent on the frequencies that have been liscensed by the radio system operator. Channel plans for 700 and 800 MHz are well defined and usually do not vary.

Bandwidth (KHz): Specifies the channel bandwidth in KHz., usually 12.5 KHz.

TX Offset +/-: Specifies whether the TX frequency is offset positively or negatively from the RX frequency.

TX Offset (MHz): Offset from the RX frequency used to derive the TX frequency

Spacing (KHz): Specifies the channel spacing in KHz. Does not have to match the channel bandwidth.

Base Frequency (MHz): Specifies the base frequency used to determine all channel calculations for this channel split.

P25 standards limit the number of channel identifier tables to 16.

Typical Channel Identifiers for 700/800 MHz Systems

	Bandwidth (KHz)	TX Offset	TX Offset (MHz)	Spacing(KHz)	Base Frequency (MHz)
1	12.5	- (Minus)	45	6.25	851.00625
2	12.5	+ (Plus)	30	6.25	762.00625

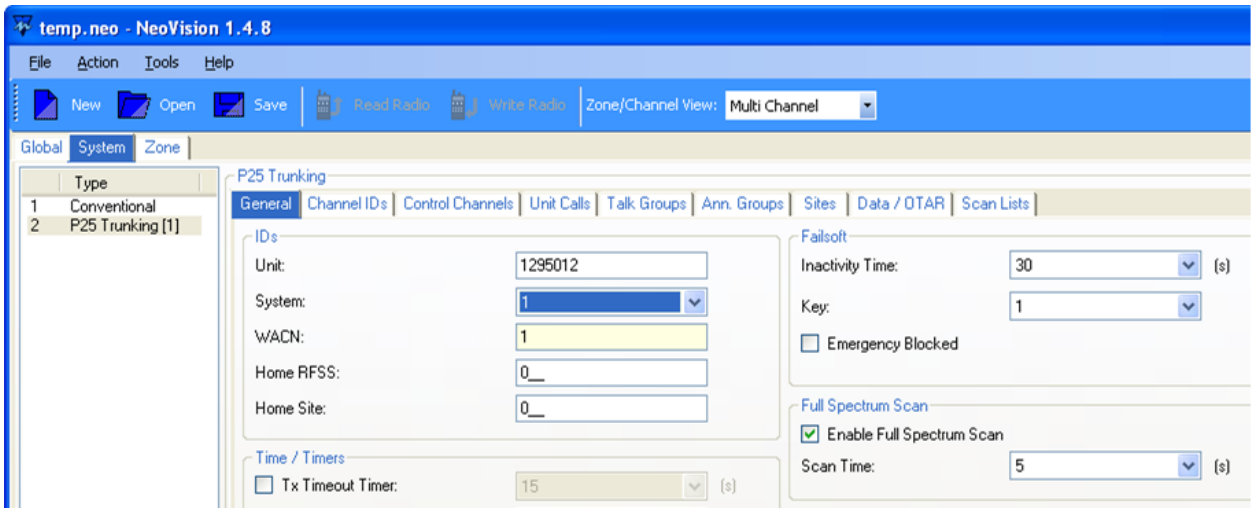
9.4 Programming Control Channel Frequencies

The Control Channel Frequencies are programmed on the Control Channel's Tab of the appropriate trunked system page.

Transmit and Receive frequencies are entered for the control channel at each site. It is permissible to enter alternate control channels. Up to 256 control channels can be entered. While 256 is an upper limit, in practice this will not prevent a radio from operating on a system with more than 256 control channels.

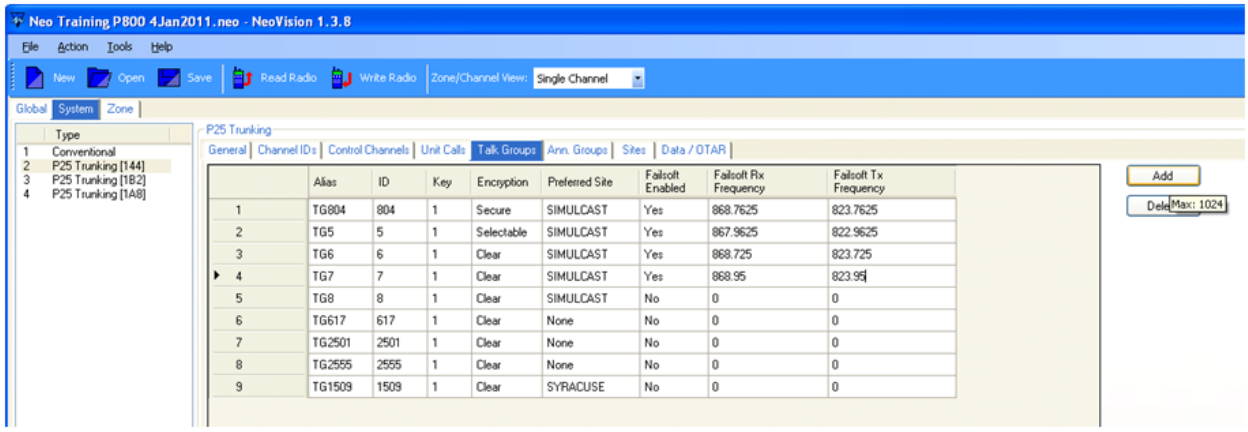
The control channel frequency pairs in this chart are shown from the subscriber viewpoint. When referencing control channel frequencies from the system view point, the transmit and receive frequencies are reversed.

RELM radios will enter full spectrum control channel scan if a valid control channel is not found in the pre-programmed list and the full spectrum scan option is enabled. This will allow the KNG radio to acquire radio sites that have not been preprogrammed in the control channel list.



9.5 Programming trunked talk groups

The Talk Groups are enabled on the Talk Group Tab of the appropriate trunked system page.



Talk Group Table: Talk groups enabled for assignment to specific channel locations are entered in this table. Once populated, these talk groups will appear in the Talk Group drop down menu on each trunking channel page.

Alias: The Alias assigned to the specific talk group id.

ID: Actual talk group id (decimal)

Key: The SLN location of the encryption key assigned to this talk group.

Encryption Strapping: Determines the encryption strapping assigned to this talk group. The options are Clear, Secure or Selectable via the menu or a function button.

Preferred Site: Allows a site preference to be assigned to this talk group from the "Site" table.

Failsoft Enabled: The radio will be able to operate under a system Failsoft condition when enabled.

Failsoft Rx Frequency: The receive frequency used for this TG in failsoft mode.

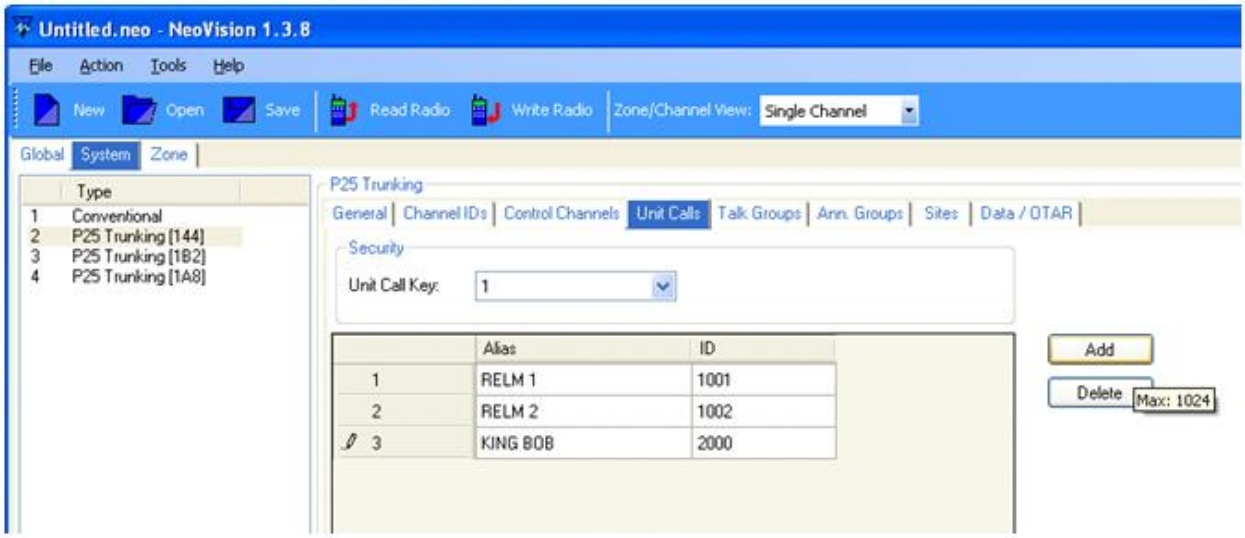
Failsoft Tx Frequency: The transmit frequency used for this TG in failsoft mode.

Failsoft Key: Sets the encryption key SLN location to use during Failsoft.

Talk Groups are assigned to a zone and channel position in the Zone Page

9.6 Programming for Individual Calls

The Unit ID Alias table is entered on the Unit Calls Tab of the appropriate trunked system page.



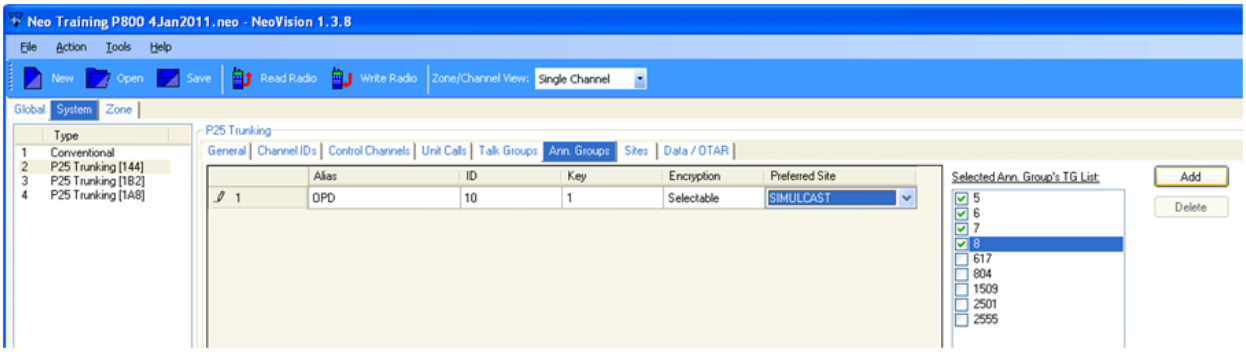
Unit Call Table: Entries in this table will be assigned to the Unit Call list and be accessible to the user via the Unit Call menu or function button.

Rx ID and Unit Calls received from id's populated on this table will then be displayed as the assigned alias instead of the actual unit id number.

The Unit Call Key selects the SLN used to encrypt Unit-to-Unit calls.

9.7 Programming Announcement Talk Groups

Announcement groups consist of two or more standard talk groups. This allows a user to communicate with multiple talk groups at the same time. The Trunked System Announcement Groups are entered on the Ann. Groups Tab of the appropriate trunked system page.



Announcement groups enabled for assignment to specific channel locations are entered in this table. Once populated, these announcement groups will appear in the Announcement Group drop down menu on each trunking channel page.

Alias: The Alias assigned to a specific announcement group id.

ID: Actual announcement group id (decimal)

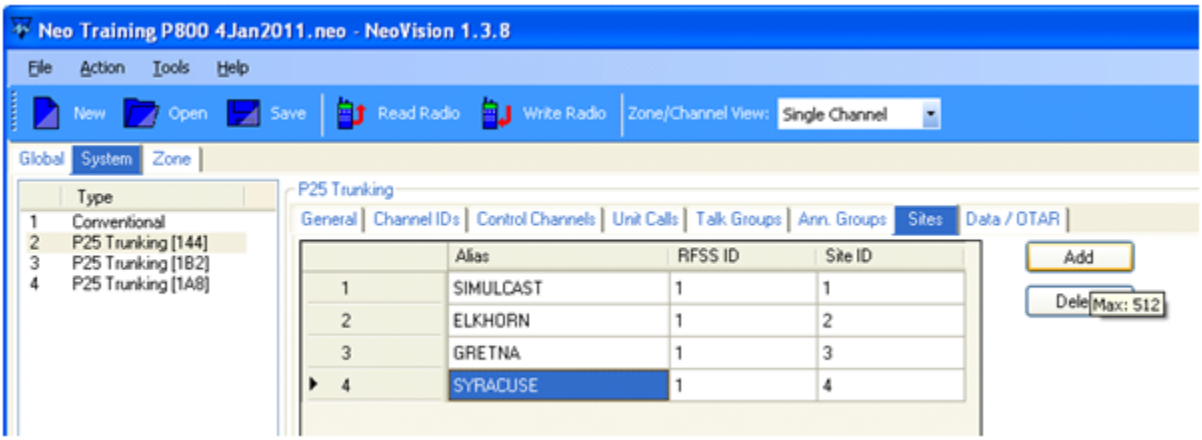
Key: The SLN location of the encryption key assigned to this announcement group.

Encryption Strapping: Determines the encryption strapping assigned to this announcement group. Options are: Clear, Secure or Selectable via the menu or a function button.

Select the talk groups to include in the announcement group using check box in the Selected Ann. Group's TG List.

9.8 Programming site aliases

The Trunked System Site aliases are entered on the Sites Tab of the appropriate trunked system page.



Sites entered into this table can be assigned aliases and can also be assigned as preferred sites to talk and announcement groups. Site aliases will also be visible when making selections from the Site Display, Site Search and Site Lock menu or function button items.

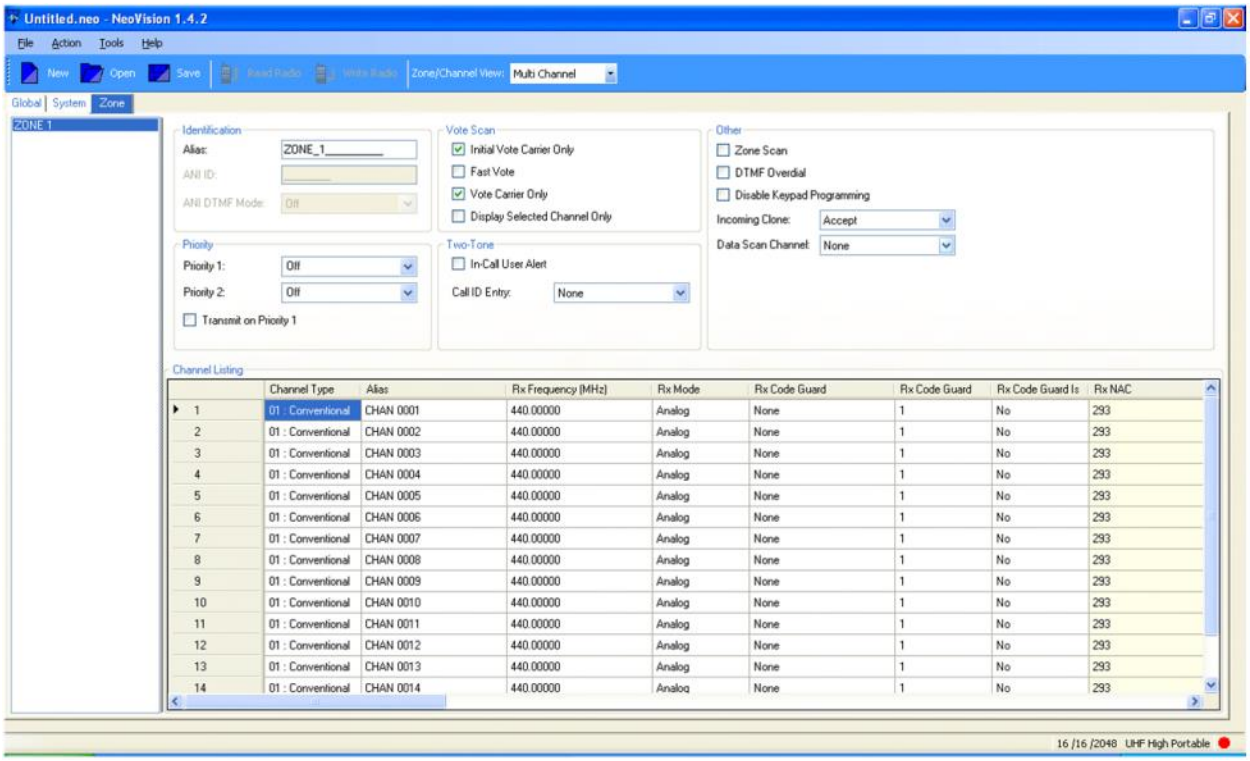
Alias: The alias assigned to a specific site id.

RFSS ID: The Radio Frequency Sub System to which the specified site is assigned.

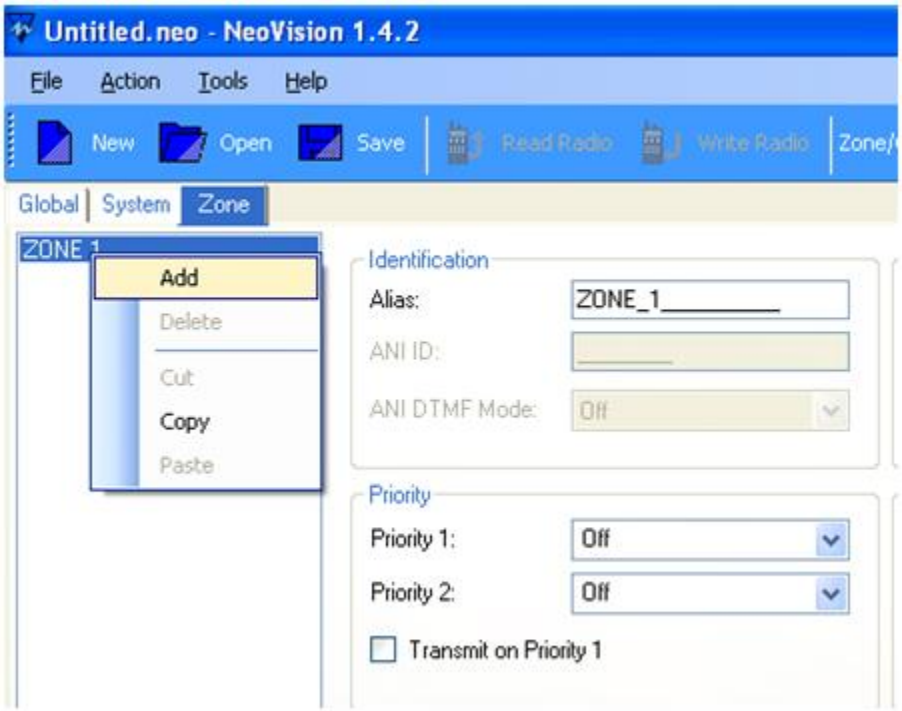
Site ID: Actual site id.

RFSS ID and Site ID are determined by the infrastructure provider.

9.9 Zone and Channel Programming.

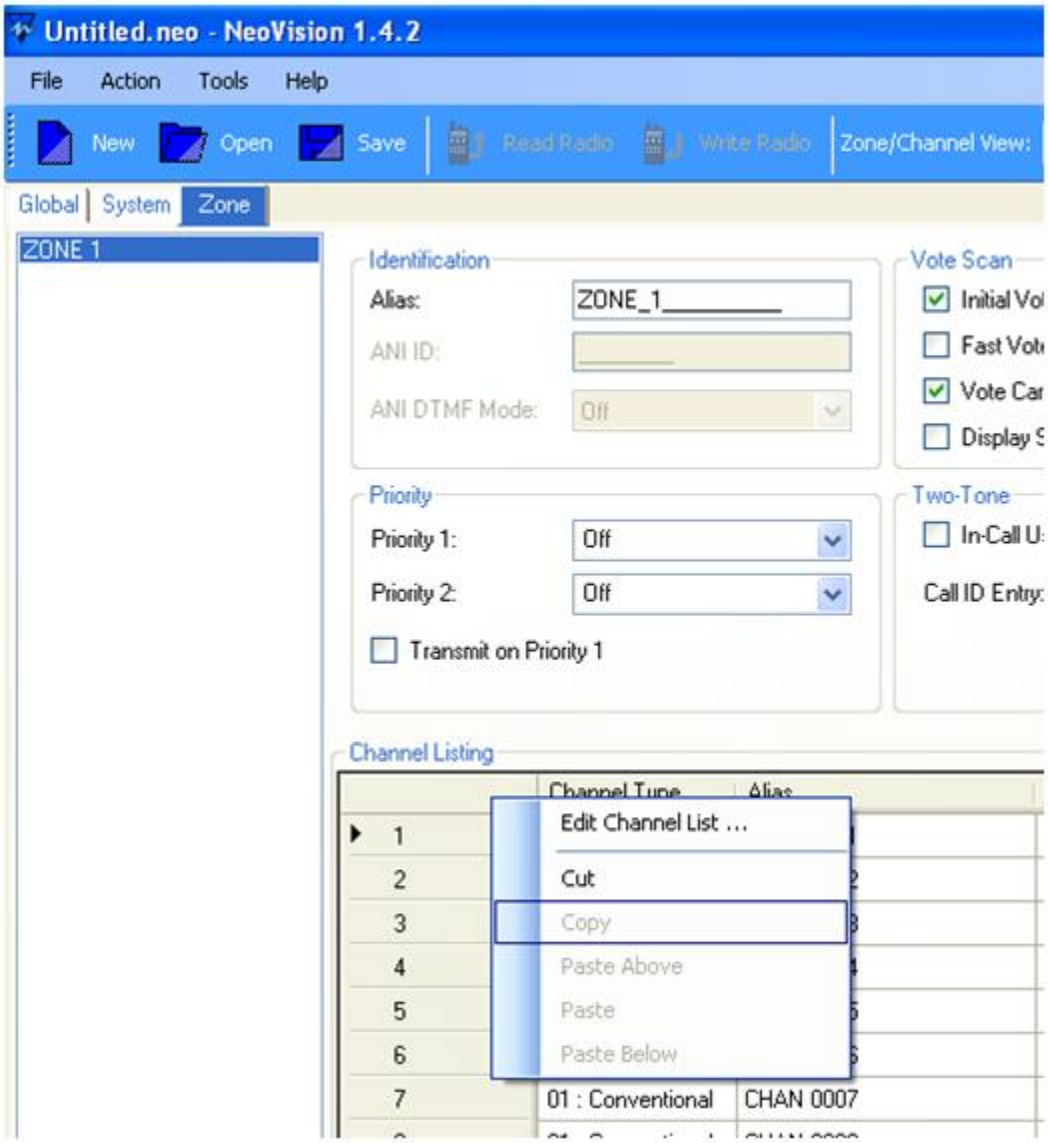


Zone Settings Screen: Selecting the Zone tab will display the zone General page. The left pane shows the active zones. A right mouse click in the left pane will bring up a drop down menu. Options for this menu are: Add Zone, Delete, Cut, Copy and Paste.



The right pane displays the General parameters to be programmed for the zone highlighted in the left pane. The selected zone alias is also detailed directly above the Channel Listing pane.

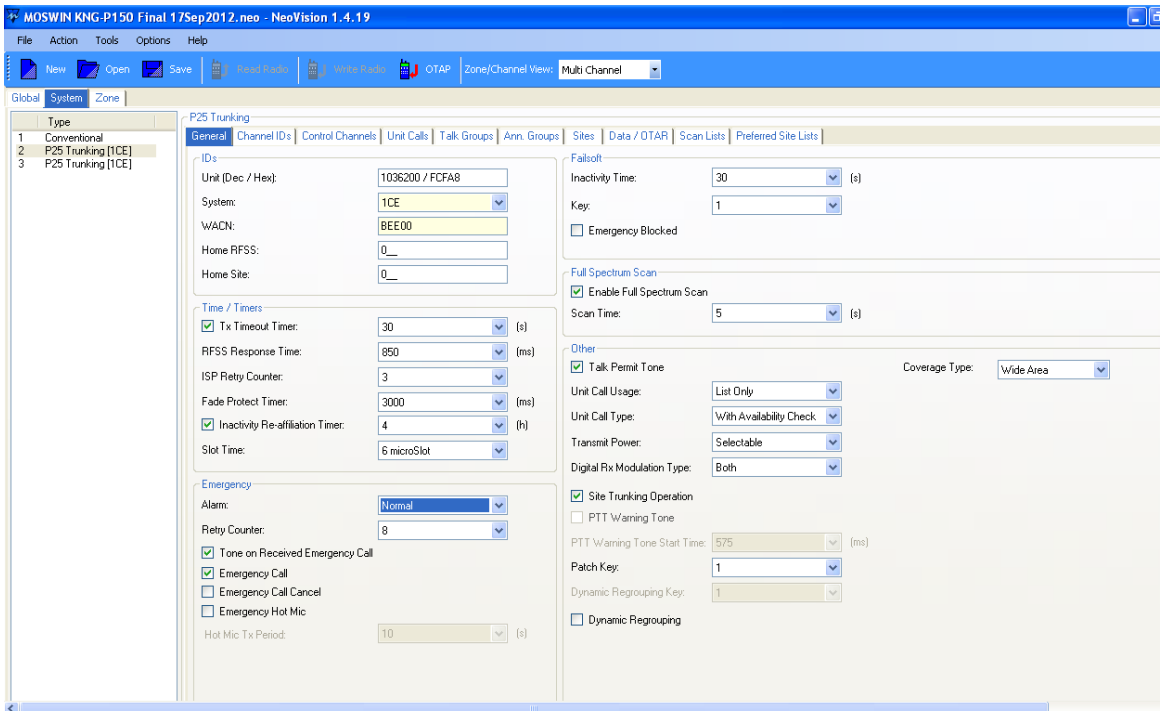
The Channel Listing pane controls which channels are enabled and their functional parameters. The highlighted channel location and alias will then be displayed above the Channel Listing pane. A right click in the Channel pane will display a drop down menu which will enable the channels to be assigned to the highlighted zone. Select the Edit Channel List option.



The channel locations can be enabled separately but selecting the check box. Right clicking in the channel pane will display all possible channel locations within the highlighted zone. Checking the box will activate that channel location.

9.10 Programming Emergency Operation

Emergency operation is programmed using the Emergency pane from the General tab for the selected trunking system.



9.10.1 Emergency Alarm

Enabling emergency alarm will cause the radio to send the emergency alarm message once the emergency has been activated (Press and hold emergency function key for approximately two seconds). Supported options are 1) None, Normal and Silent. The retry counter setting is the number of times the radio will repeat the alarm message to the infrastructure until it is acknowledged. Once the radio receives an acknowledge from the system, the radio will indicate the emergency alarm has been acknowledged.

9.10.2 Tone on Received Emergency Call

If enabled, the radio will indicate an audible tone upon receipt of radio traffic which includes an active emergency signal. The radio will also display Emergency and the unit ID or alias of the radio initiating the emergency.

9.10.3 Emergency Call

If enabled, when the emergency condition has been activated, the radio will send all voice traffic with the emergency condition asserted. This will allow other radios and dispatch consoles to display a visual indicator and generate an audible tone (if tone on receive emergency call is enabled).

9.10.4 Emergency Call Cancel

For infrastructure systems that permit the subscriber radio to cancel the emergency call select this option. This option is not supported on Motorola systems.

9.10.5 Emergency Talk Group Selection

KNG Series radios support programming for tactical emergency or emergency revert. The Zone channel assignment page provides a drop down box for programming the Emergency Group to be used for emergency alarms and emergency calls. When the emergency mode has been activated, the radio will transmit and receive on the designated Emergency Group..

9.11 Programming and Configuring Trunked OTAR

9.11.1 Required Information

NeoVision will require the following KMF information to compile a code plug for OTAR operation on the designated system: KMF IP Address, KMF UDP Port, Subscriber UDP Port, Rx Security Level and the Tx Security level settings.

9.11.2 KMF Programming Requirements.

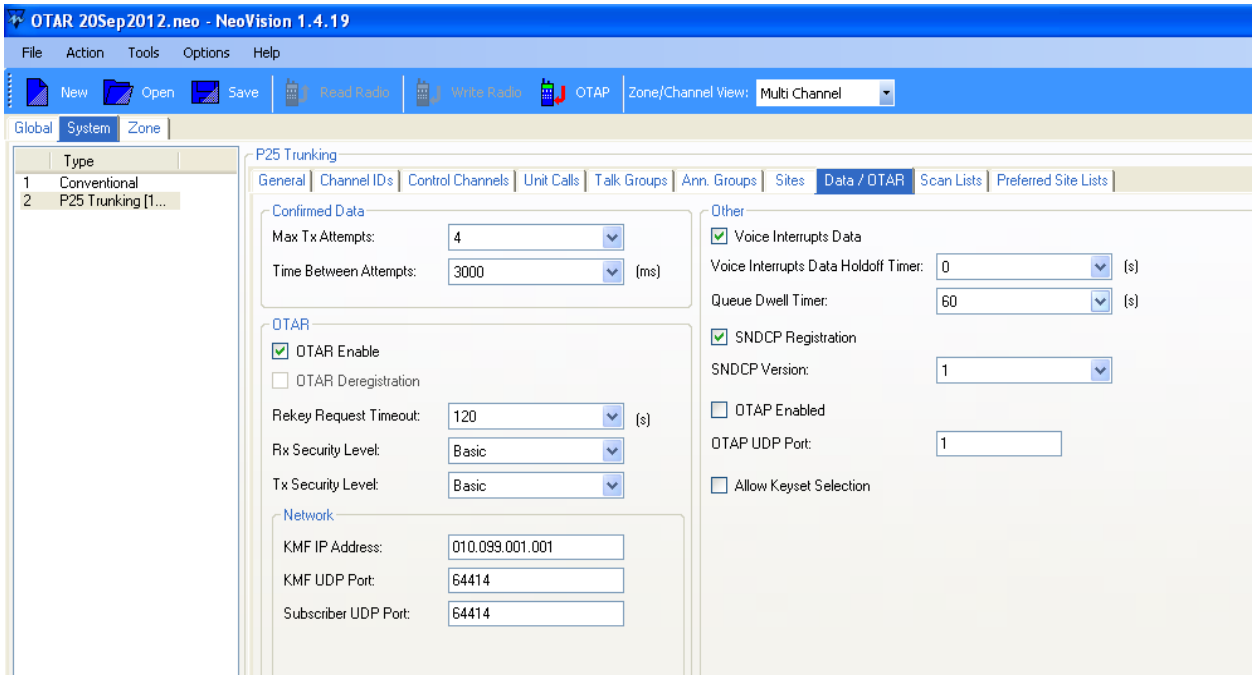
Each subscriber will have to be enabled and detailed in the KMF data base before any re-keying activity can take place.

9.11.3 Subscriber Keyload Requirements.

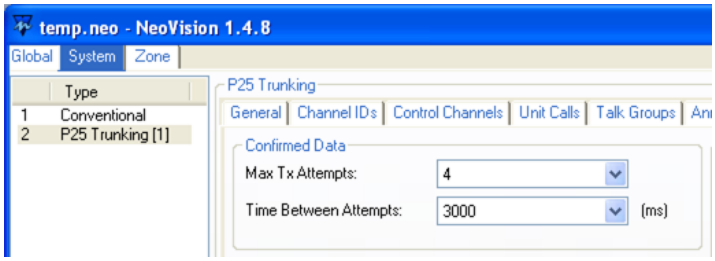
Each subscriber will require a UKEK and an RSI be loaded using an appropriate keyloader before being re-keyed via the OTAR system..

9.11.4 P25 Trunking OTAR Programming.

The Data/OTAR tab of the NeoVision P25 Trunking system page is located under the main “System” tab. Select the desired P25 Trunking system under the “Type” column. The “Data/OTAR” sub page contains the programmable OTAR features for the selected trunking system.



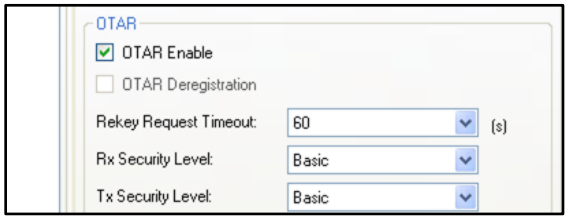
9.11.5 Confirmed Data



Max Tx Attempts: Specifies the number of times the radio attempts to send confirmed data before the attempt is considered a failure and ends (non-registrations).

Time Between Attempts: Specifies the approximate time that the radio waits before attempting to resend a confirmed data packet.

9.11.6 OTAR



The Network and Security Level settings are specific to the KMF in use. Contact the system administrator to determine the proper settings.

OTAR Enable: Select to enable Over the Air Rekeying (OTAR) of encryption keys on theP25 Trunking system

OTAR De-Registration: When enabled the radio will deregister from the KMF Server and trunked data system when powering off or switching to other trunked radio systems.

Rekey Request Timeout: When rekeying is initiated by the radio (Rekey Request message) this setting determines the maximum length of time the radio will wait for the Rekey Request procedure to complete before reporting a time out. Times of 15 to 240 seconds can be programmed. Default is 60 seconds.

Rx Security Level: Two settings are possible for this feature:

Enhanced: The radio accepts only encrypted and authenticated KMM's from the KMF.

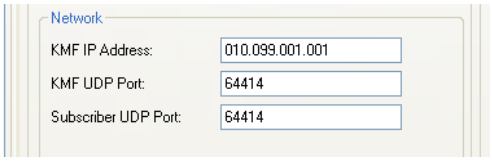
Basic: The radio accepts any KMM that is in a format allowed by the OTAR standard.

Tx Security Level: Two settings are possible for this feature:

Enhanced: All OTAR procedures originating from the radio are encrypted and authenticated. If they cannot be encrypted and authenticated, the radio does not send the KMM.

Basic: The radio will send unencrypted KMMs if the OTAR standard allows them to be unencrypted and unauthenticated.

9.11.7 Network

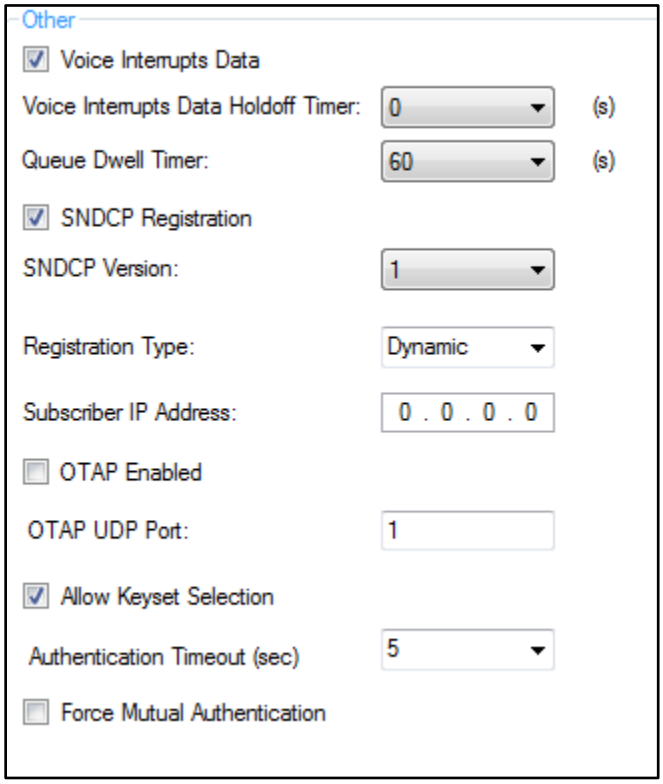


KMF IP Address: The KMF's IP address. Consult system administrator for this value.

KMF UDP Port: The UDP port the radio uses when it sends KMMs to the KMF. The default value is 64414. Consult system administrator for this value.

Subscriber UDP Port: The UDP port the radio expects KMMs from the KMF. The default value is 64414. Consult system administrator for this value.

9.11.8 Other Data Settings



Voice Interrupts Data: When enabled, a voice call will interrupt the data activity, including OTAR. For mission critical voice systems this should be enabled.

Voice interrupts Data Holdoff Timer: The setting determines the amount of time the radio will remain on the voice channel before attempting to return to the data channel after voice traffic had interrupted an active OTAR event.

Queue Dwell Timer: Specifies the amount of time data can stay in the SNDCP output queue. Settings are from 15 to 120 seconds. Default setting is 60 seconds.

SNDCP Registration: SNDCP registration should be enabled for proper OTAR operation. This allows the radio to register with and receive an IP address from the system.

SNDCP Version: The SNDCP protocol version used by the radio when communicating with the system.

Registration Type: If the radio subscriber has been configured in the radio system manager for static IP addressing, select static IP addressing**.** Note even if the infrastructure is configured for static IP addressing, some systems will properly provide the subscriber IP address if the radio requests dynamic registration. In these cases, it is possible to leave this field set to dynamic and avoid having to change the IP address for each subscriber. However, if OTAP operation is desired, static IP addressing is suggested.

Subscriber IP Address: Enter the radio's static IP address here.

OTAP Enabled: If the OTAP option has been purchased for the subscriber radio, check this box for over the air programming operation.

OTAP UDP Port: This is the UDP port the OTAP application uses to send programming information to. In general, the value of this port can be set to any unused UDP port value. P25 defines available UDP ports 49200-49213 as available UDP ports for P25 applications.

Allow Keyset Selection: Enabling this checkbox allows the radio user to designate which keyset is the active keyset. A keyset is a group of keys that will be used within a subscriber unit for the same algorithm and cryptoperiod. This allows the group of keys to be managed as a single entity (i.e., they can be rekeyed, updated and deleted at the same time with a single command).

Authentication Timeout: The period of time allowed before the subscriber unit determines that the authentication process (if enabled) has failed.

Force Mutual Authentication: Basic link layer authentication requires the infrastructure to authenticate a subscriber unit. In mutual authentication the subscriber radio will also authenticate the infrastructure. Select this checkbox if the infrastructure supports mutual authentication.

Radio Operator Selectable Features

KNG Series radios allow the following features to be selected from the radio menu, or assigned to a radio function key.

Rekey Request: Selecting this function will initiate a rekey request to the KMF.
Keyset Select: Allows the operator to switch from one internal keyset to the other. This must also be enabled on the Data/OTAR page.
Zeroize Keys: Selecting this function will zeroize all keys in the radio (TEKs and KEKs).
Radio Info: This function displays the current radio unit ID, radio IP address, OTAR registration status and Authentication status.

9.11.9 KMF Programming

This section will detail KMF programming requirements. Contact the KMF system administrator to verify the status of these items.

All radios must have a defined “Radio Record” within the KMF data base to use secure voice and OTAR services.

The Radio Record will detail radio specific items such as the Radio Group, RSI and the designated UKEK.

There are additional “Radio Details” that control radio capabilities and status, such as Locked Out and Inhibit/Enabled conditions.

Once the Radio Record is entered using the KMF Client and the UKEK and RSI have been loaded into the radio via the KVL, the KMF operator must mark the radio as being ready for OTAR communications by invoking the “Mark as Provisioned” operation for the given Radio Record. This step must be done before the KMF can communicate with the radio.

9.11.10 Subscriber Radio Keyloading Requirements for OTAR Operation

There are several different steps that must be taken before any OTAR activity can take place. The following items should be configured using a keyloader device at radio setup.

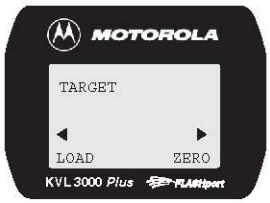
*** Important Note: The “Update” command on the KVL should NOT be used to provision a radio. Instead, the UKEK should be loaded manually using the “Target -> Load -> Keys command. ***

9.11.10.1 Initializing the encryption module and deleting all Keys

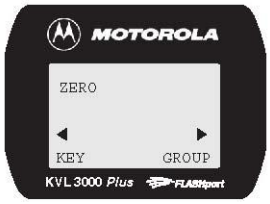
For initial radio setup, all keys should be deleted from the radio. This will reset the encryption module and prepare it for proper operation. To Zeroize or delete all keys:

1. Turn on the KVL and the target radio, and then connect them using the appropriate cable.

2. Use the ▭ key to select **TARGET** from the Main Menu. The following screen is displayed.



3. Use the ▭ key to select **ZERO**. The following screen is displayed.



4. Use the ◄ or ► keys to display **ALL**, then use the • key to select it. The following screen is displayed (typical screen shown).

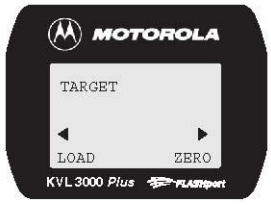
5. Use the • key to select **YES**. The following screen is displayed while the keys are being zeroized:

6. When finished, the following screen is displayed to confirm that all of the keys in the target device were zeroized. Use the • key to select **OK**.

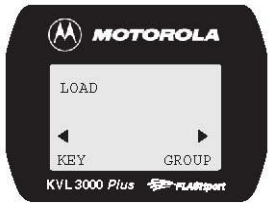
9.11.10.2 Loading the Unique Key Encryption Key (UKEK)

UKEK: The Unique Key Encryption Key will be used to decode KMMs from the KMF. This will allow the TEK keysets to be sent to the radio via the OTAR process.

1. Turn on the KVL and the target radio, then connect them using the appropriate cable.
2. Use the • key to select **TARGET** from the Main Menu. The following screen is displayed.



3. Use the • key to select **LOAD**. The following screen is displayed.



4. Use the • key to select **KEY**. The following screen is displayed (typical screen shown).

5. Use the ◄ or ► keys to select the key you wish to load to the target radio or use the keypad to directly enter the CKR, then press **Enter**.
6. Use the • key to select **LOAD**. The following screen is displayed while the key is being loaded:

7. When finished, the following screen is displayed to confirm that the key was loaded into the target radio. Use the • key to select **OK**.

9.11.10.3 Loading the Target RSI, KMFRSI and MNP

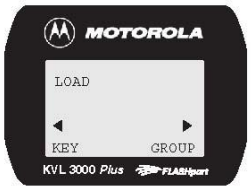
TGTRSI: The Individual RSI for the given radio must be loaded into the radio before OTAR activity can take place. Note: Because this step resets the Message Number for the given RSI, this RSI loading step should take place whenever a Radio Record is created for the given radio, even if the radio already happens to have the given RSI loaded.

KMFRSI: The proper KMFRSI value should be loaded into the radio. The default value for KMFRSI is 9999999. Consult system administrator for this value.

MNP: The correct Message Number Period should be loaded into the radio. This value should match the MNP value being used by the KMF. Message Number validation can be disabled by entering 65535. Consult system administrator for this value.

Connect the KVL to a target device and load a TGTRSI, KMFRSI, or MNP into the device.
1. Turn on the KVL and the target device.
2. Connect them using the appropriate cable.
3. Use the • key to select **TARGET** from the Main Menu. The following screen is displayed.

4. Press ▪ to select **LOAD**. The following screen is displayed.



5. Use the ◄ or ► keys to navigate to **TGTRSI**, **KMFRSI**, or **MNP** (as desired), then press ▪ to select the desired parameter. The following screen is displayed (TGTRSI shown):

6. Enter the desired TGTRSI (or KMFRSI or MNP), then press ▪ to select **LOAD**. The KVL loads the entered parameter into the target device. Messages are displayed to indicate the status of the process. If you select:

- **TGTRSI**, the **LOAD** selection does not appear until you have entered the first digit of the RSI
- **KMFRSI** or **MNP**, the KMFRSI or MNP currently stored in the KVL is displayed. You may edit this number as desired.

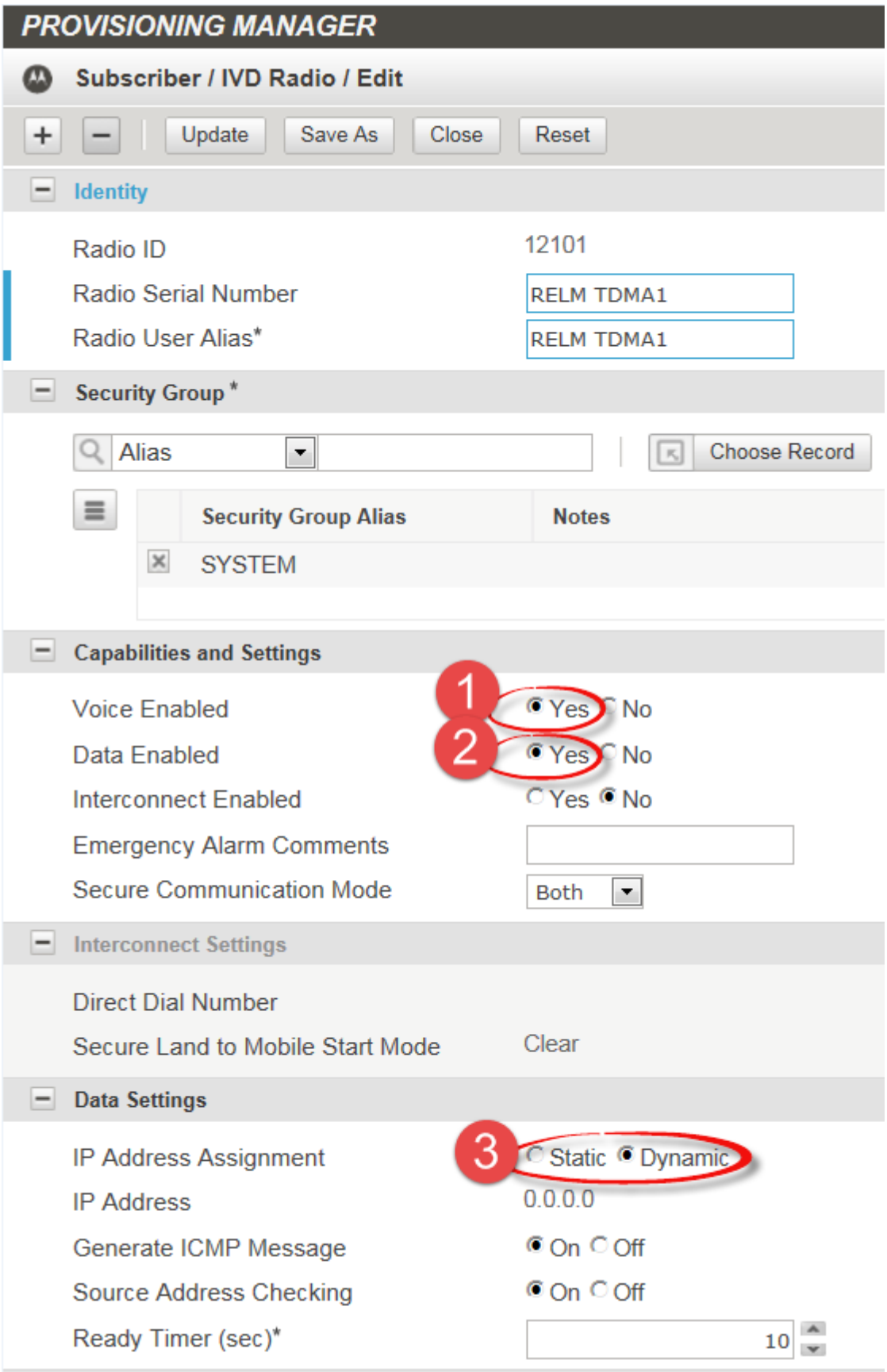
9.11.11 OTAR Trouble Shooting

Proper OTAR operation first requires that the radio be configured for voice and data operation. This requires the subscriber radio to be properly configured in the radio system as well as configured using NeoVision programming software for data operation.

9.11.11.1 Motorola Radio System Configuration

Verify that the subscriber ID is configured for voice and data operation. Appropriate settings for Motorola radio systems are as follows:

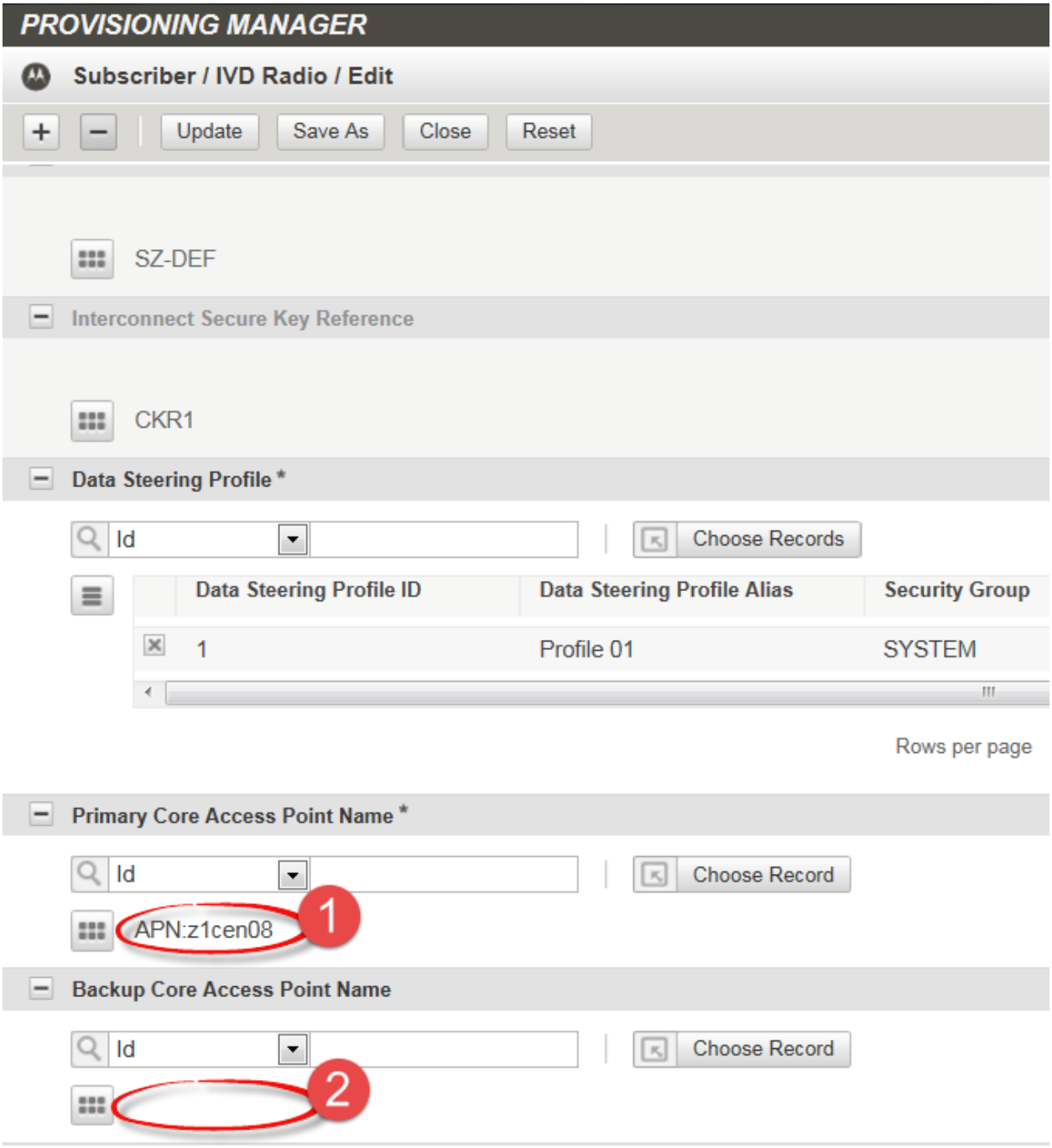
1) Voice Enabled: Yes
2) Data Enabled: Yes
3) IP Address Assignment: Static or Dynamic is Acceptable


PROVISIONING MANAGER
Subscriber / IVD Radio / Edit
Update
Save As
Close
Reset
Identity
Radio ID
12101
Radio Serial Number
RELM TDMA1
Radio User Alias*
RELM TDMA1
Security Group *
Alias
Choose Record
Security Group Alias
Notes
SYSTEM
Capabilities and Settings
1
Voice Enabled
Yes
No
2
Data Enabled
Yes
No
Interconnect Enabled
Yes
No
Emergency Alarm Comments
Secure Communication Mode
Both
Interconnect Settings
Direct Dial Number
Secure Land to Mobile Start Mode
Clear
Data Settings
3
IP Address Assignment
Static
Dynamic
IP Address
0.0.0.0
Generate ICMP Message
On
Off
Source Address Checking
On
Off
Ready Timer (sec)*
10

Additional System Settings:

1) Verify the Primary Core Access Point is set.

2) If the system is configured for a Backup Core Access Point, verify this is set. In some instances, this should be set to the same as the Primary Core Access Point.



9.11.11.2 Harris Radio System Configurations

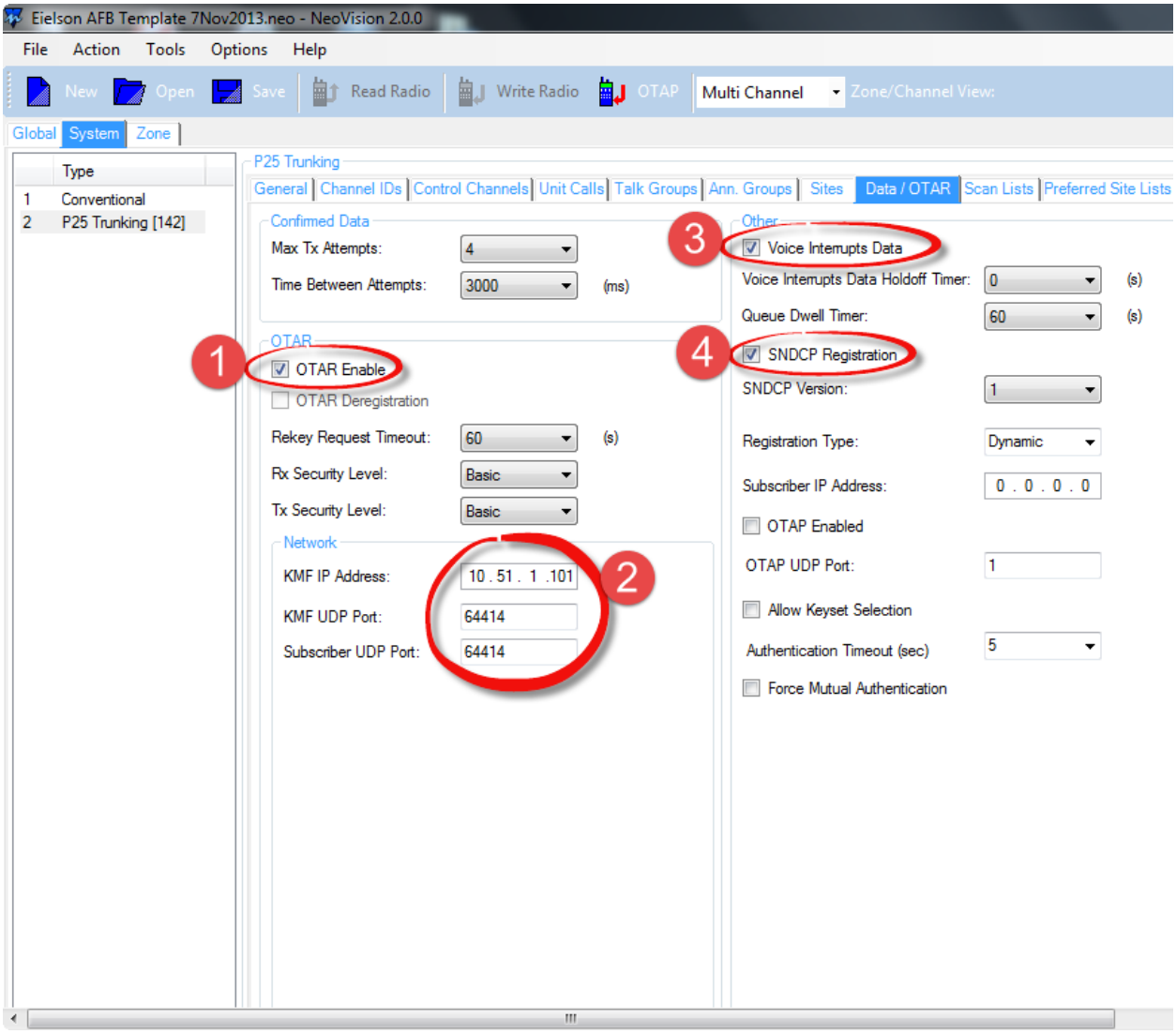
9.11.11.3 Subscriber Configuration

1) Verify that OTAR is enabled

2) Verify that the Correct KMF IP Address, KMF UDP Port and Subscriber UDP Port are entered.

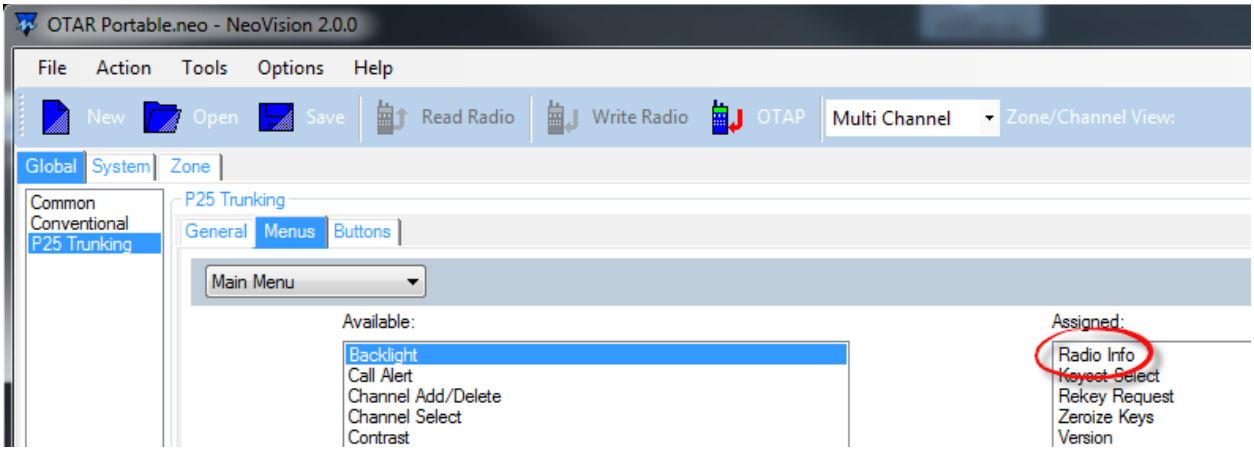
3) Select voice interrupts data

4) Enable SNDCP Registration, Version 1.



9.11.11.4 Verifying Radio Status

Assign the Radio Info function to the trunking menu items. This will allow verification of unit ID, IP Address, OTAR registration and authentication.



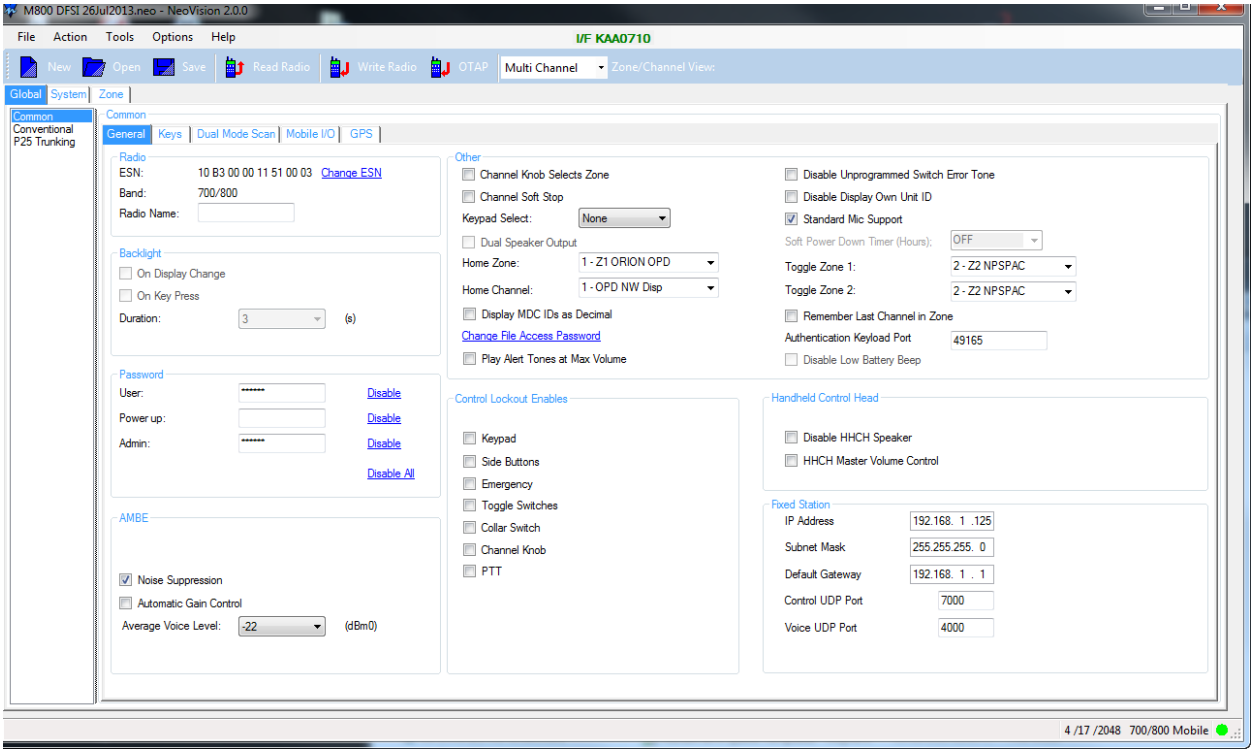
Radio Info display.

10 Digital Fixed Station Interface (DFSI)

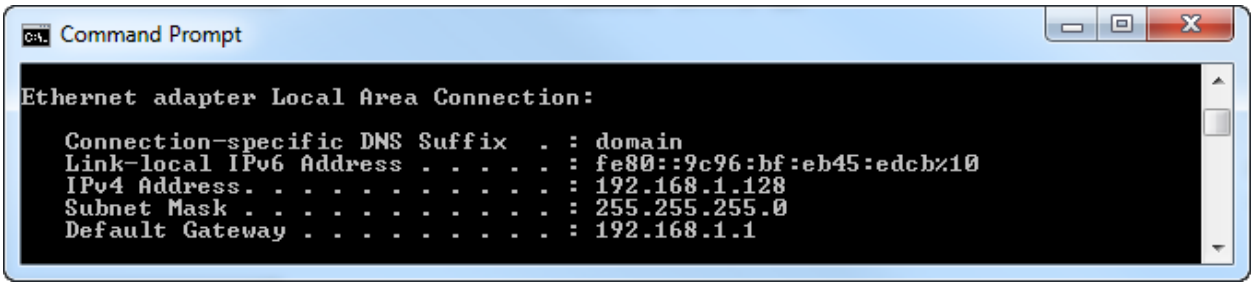
RELM KNG Series mobile radios can be configured to use the P25 DFSI. This allows connection via IP networks for voice and control operation. A PC based interface application is available from RELM, or a third party DFSI complaint console can be used. The feature requires use of radio firmware 5.0.0 and above, NeoVision 2.0.0 and above.

10.1 Programming the KNG Mobile for DFSI Operation

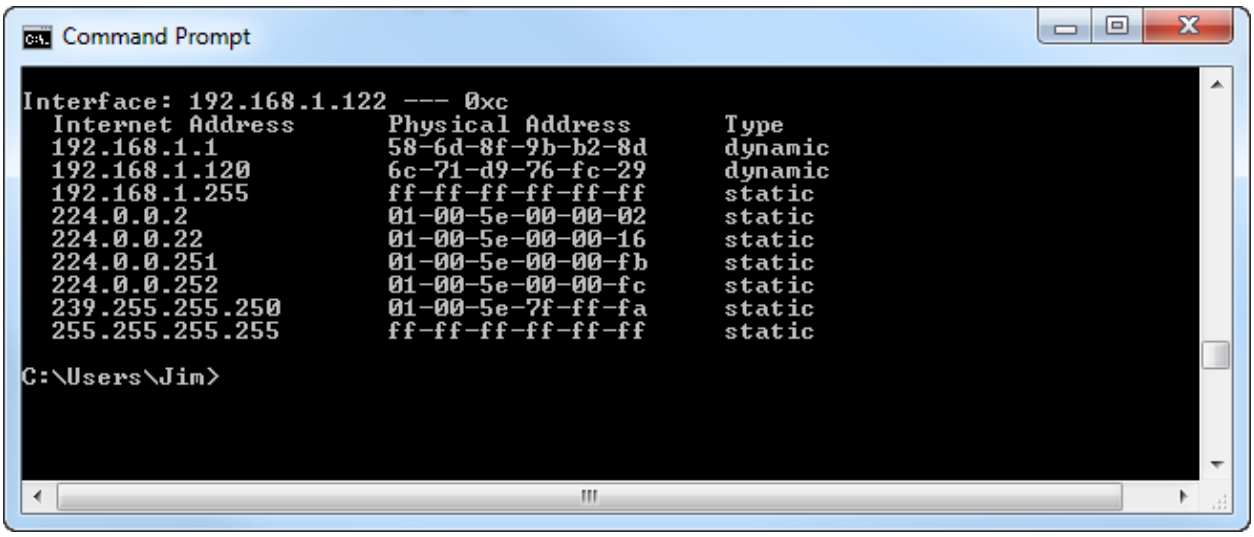
The DFSI interface is configured via the Fixed Station window which is found on the Global/Common/General page of NeoVision programming software.



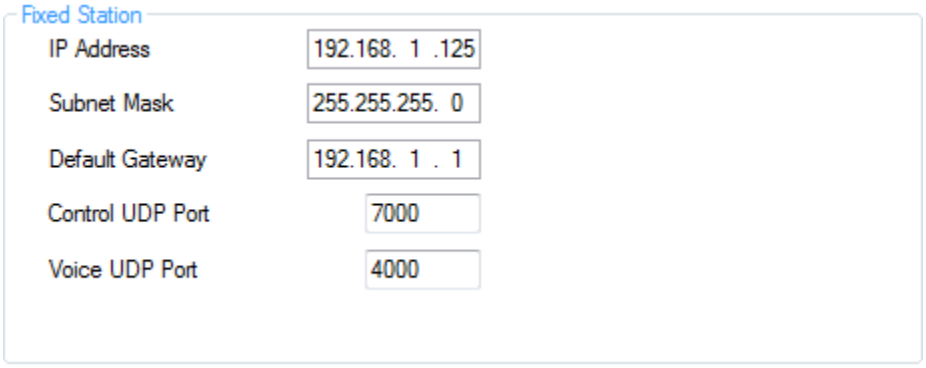
Enter an appropriate IP Address, Subnet Mask and Default Gateway for your IP Network. If you are unsure of appropriate values, from a computer connected to the network, open a command prompt and type ipconfig. The utility will return the IP address, Subnet Mask and Default Gateway of the computer's Ethernet adapter.



To determine which IP addresses are currently in use, type arp –a from the command prompt. You can then select an IP address which is currently not in use.

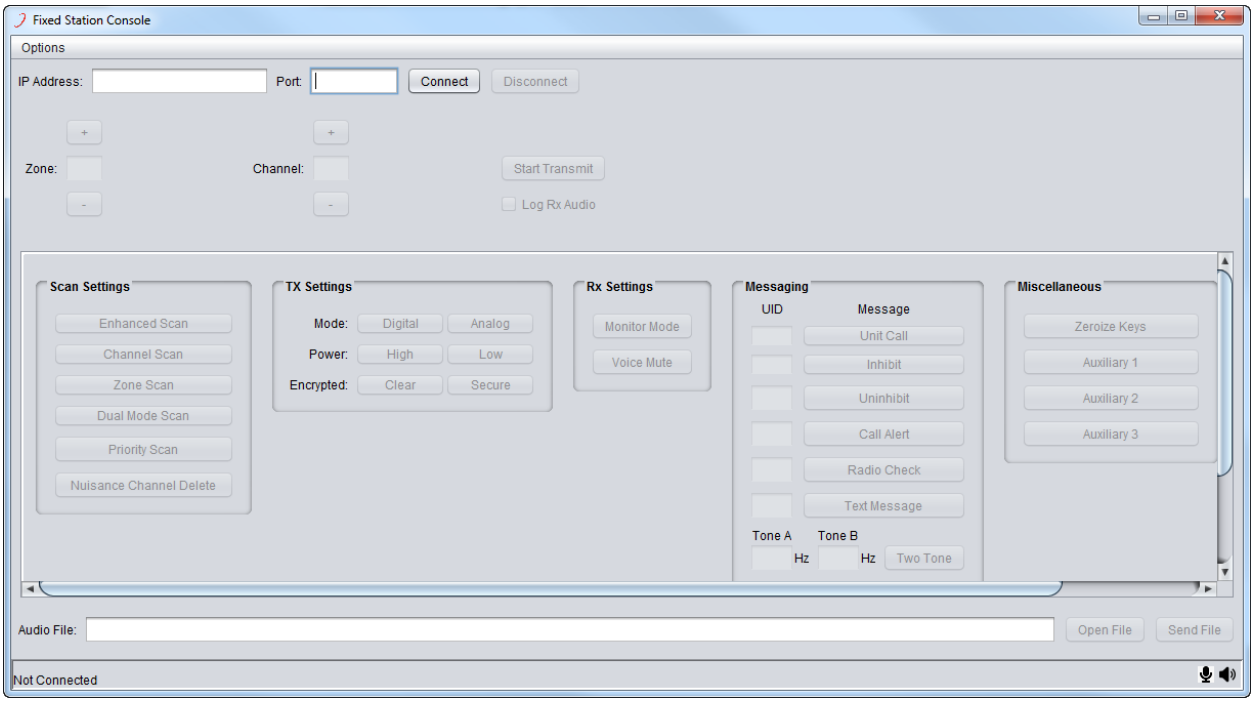


In NeoVision, configure the Fixed Station to use an IP address that is currently not in use. Enter the Subnet Mask and Default Gateway as provided. The P25 DFSI Standard identifies UDP port 7000 as the default control port. No default port is identified for the Voice UDP Port.

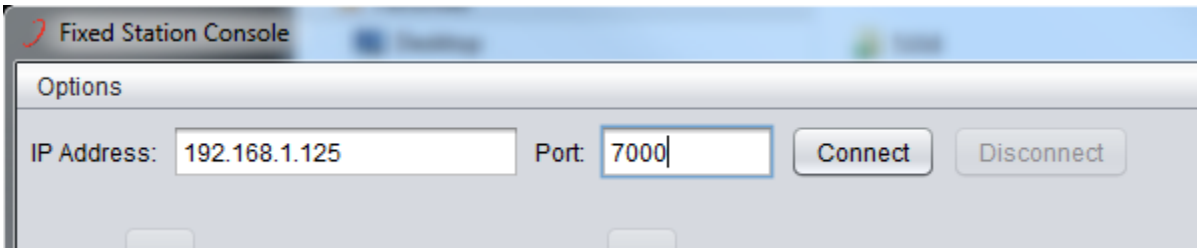


10.2 Configure and Use of the FSI Console Application

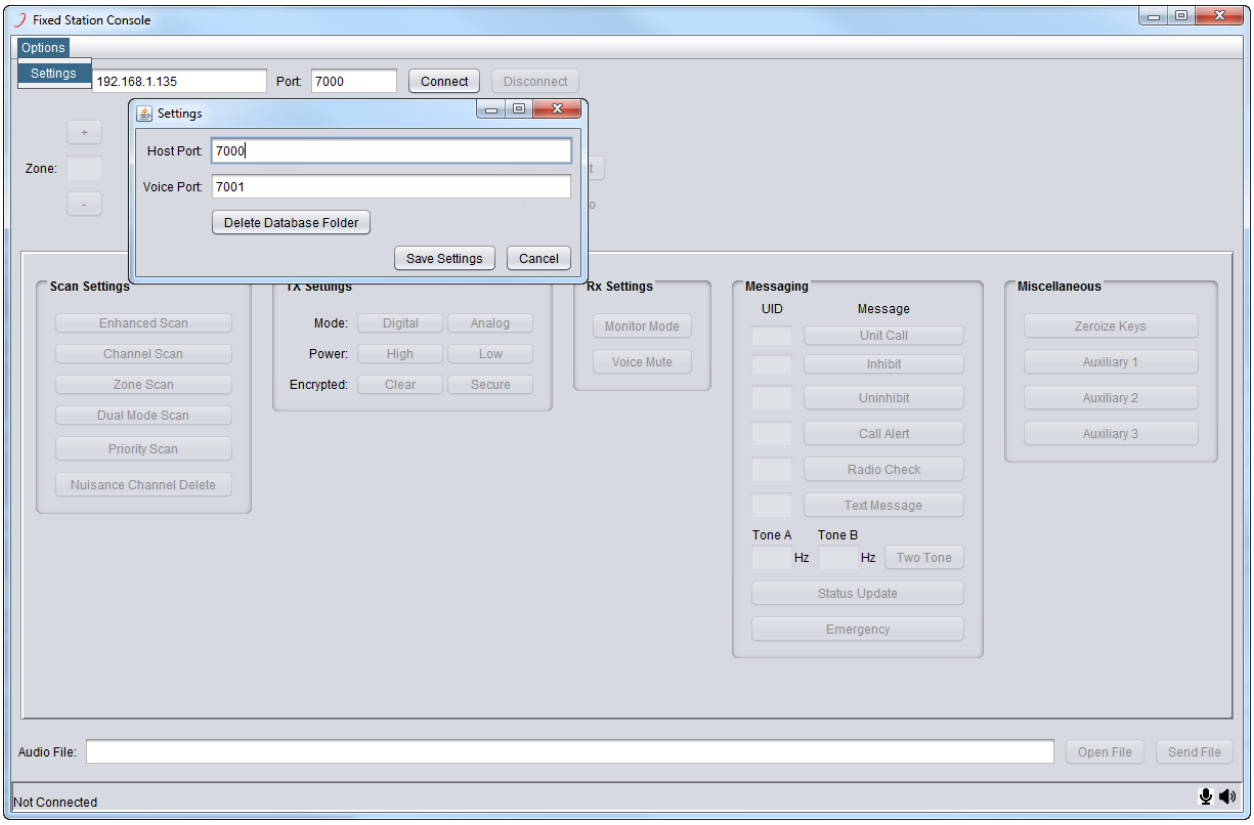
Double click on the file FSIConsole .exe, or send this file to the desktop as a shortcut and double click to open.



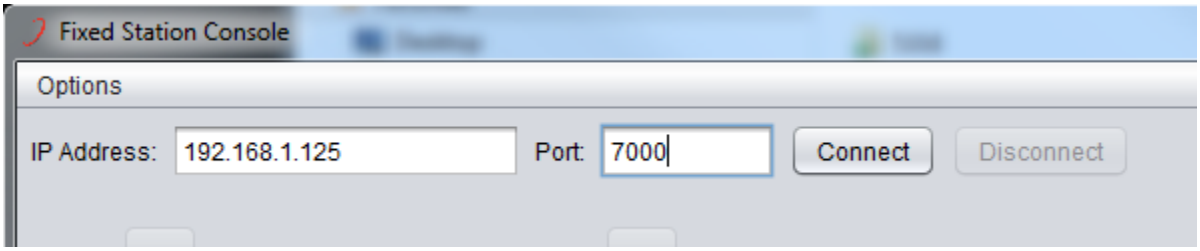
Enter the IP address of the target radio and the UDP Control Port. This is configured via NeoVision as shown in Section 10.1.



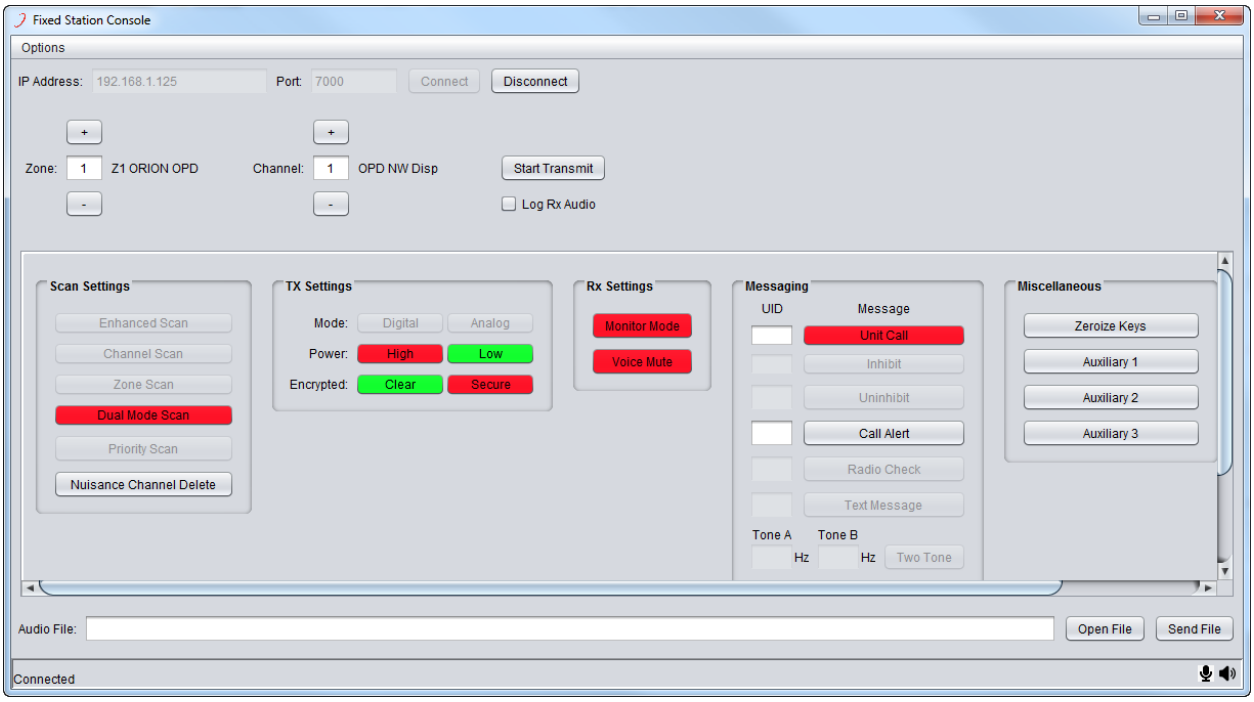
If it is necessary to set the UDP voice port, select Options, then Settings. Enter the UDP Control Port and Voice Port. Click Save Settings.



Once the IP Address and port address are set, click connect.



The display on the KNG radio will now be blanked out, and the radio will be controlled by FSIConsole operation.



A red control box indicates that the option is available. A green control box indicates the option has been selected or activated.

Click the Disconnect button to return control of the KNG mobile to the local control head.

11 System Keys:

RELM KNG series radio programming software requires a system key to enable programming for a given trunked radio system. RELM has implemented a procedure to generate the system key and to restrict distribution of the key per the radio system owner's written instructions.

RELM's Policy for generating and distributing trunked radio system keys is documented on the following pages.

Date: 21 October, 2010

Author: Jim Holthaus

Subject: System Key Generation Procedure

Purpose: This document describes the procedure that is used to create and distribute a "Trunked Radio System Key".

Background: System Keys are used to protect trunked radio systems from unauthorized access. The System Key is a cryptographically encoded file derived from the Trunked Radio System ID. RELM trunked radio programming software (NeoVision) requires that the System Key be available before trunked radio parameters can be programmed into a RELM radio.

Procedure:

1. The System Key Authorization form will be completed by the designated representative of the trunked radio system.
2. The authorization form will be sent to the identified RELM representative and a System Key will be generated and distributed to the individual authorized. Distribution of the key can be via electronic means or shipped (CD) per the authorized system agent's instructions.
3. A copy of the System Key will not be maintained by RELM.

RELM Wireless
7100 Technology Drive
West Melbourne, FL 32904
Trunking System Authorization

RELM Wireless utilizes this form to identify a trunked radio system owner and to provide the customer with a "System Key". This "System Key" is unique to RELM BK Radios and is required to programtrunked radio system parameters.

System Owner Information	
Customer/Agency Name:	
Customer Point of Contact:	
Title	
Street Address:	
City, State Zip:	
Phone:	
E-Mail Address	

System Information	
System ID:	WACN ID:

Authorized System Key Recipient	☐ CD ☐ WEB Distribution
Recipient:	
Agency:	
Title	
Street Address:	
City, State Zip:	
Phone:	
E-Mail Address	

RELM Contact Information	
Name	Jim Holthaus
Title	Director - Product Marketing
E-Mail Address	jholthaus@relm.com
Phone:	402-990-1551
FAX	800-753-0942

Authorization Start Date:		End Date:	

System Owner Signature _____ Date: _____

I certify that I am authorized to provide System ID information to RELM/BK Radio.
I authorize RELM to produce the System Key and to provide the Key to the recipient noted above.