Security Escort

SE3000 Series

en Technical Reference Manual

Table of contents

1 Copyright and warranty

1.1 Trademarks

Microsoft® and Windows® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

1.2 Software license agreement

Security Escort's Central Control software for Microsoft® Windows®.

Notice!
This software relates to security. Access should be limited to authorized individuals. This software contains provisions for setting security passwords. Appropriate security levels should be established and passwords should be set before allowing operating personnel access to this software. The original disk should be safeguarded against unauthorized use. In addition, security/fire controls contain passwords to prevent unauthorized access; these passwords must also be set and their identity carefully safeguarded.

Please read the following license agreement prior to installing and operating the software. Do not install this software unless you agree to the following terms:

You MAY

- Use the Security Escort program only on a single Security Escort system, with a single master computer, a single optional slave computer, and only the number of workstations originally factory programmed into the software key.
- This program can be used without a software key only for demo purposes. In no case can this program be used on a live system without an authorized software key.
- Copy the program into another computer only for backup purposes in support of your use of the program on one Security Escort system.

You may NOT

- Transfer this program or license to any other party without the express written approval of Bosch Security Systems.

1.3 Limited warranty

Bosch Security Systems warrants that the program will substantially conform to the published specifications and documentation, provided that it is used on the computer hardware and with the operating system for which it was designed. Bosch Security Systems also warrants that the magnetic media on which the program is distributed and the documentation are free of defects in materials and workmanship. No Bosch Security Systems dealer, distributor, agent, or employee is authorized to make any modification or addition to this warranty, oral, or written. Except as specifically provided above, Bosch Security Systems makes no warranty or representation, either express or implied, with respect to this program or documentation, including their quality, performance, merchantability, or fitness for a particular purpose.

1.4 Remedy

Bosch Security Systems will replace defective media or documentation, or correct substantial program errors at no charge, provided you return the item with proof of purchase to Bosch Security Systems within 90 days of the date of delivery. If Bosch Security Systems is unable to replace defective media or documentation, or correct substantial program errors, Bosch Security Systems will refund the license fee. These are your sole remedies for any breach of warranty.

Because programs are inherently complex and may not be completely free of errors, you are advised to verify your work. In no event will Bosch Security Systems be liable for direct, indirect, incidental, or consequential damages arising out of the use of or inability to use the program or documentation, even if advised of the possibility of such damages. Specifically, Bosch Security Systems is not responsible for any costs including, but not limited to, those incurred as a result of lost profits or revenue, loss of use of the computer programs or data, the cost of any substitute program, claims by third parties, or for other similar costs. Bosch Security Systems does not represent that the licensed programs may not be compromised or circumvented. In no case shall Bosch Security Systems liability exceed the amount of the license.
Some states do not allow the exclusion or limitation of implied warranties, or limitation of liability for incidental or consequential damages, so the above limitation or exclusion may not apply to you.
Bosch Security Systems retains all rights not expressly granted. Nothing in this license constitutes a waiver of Bosch Security Systems rights under the U.S. Copyright laws or any other Federal or state law.
Should you have any questions concerning this license, write to:

Robert Bosch Security Solutions Pte Ltd
11 Bishan Street 21
Singapore 573943

1.5 Use latest software

Before operating the device for the first time, make sure that you install the latest applicable release of your software version. For consistent functionality, compatibility, performance, and security, regularly update the software throughout the operational life of the device. Follow the instructions in the product documentation regarding software updates.

For more information, refer to the Security Escort release notes and manuals from the Bosch online product catalog.

The following links provide more information:
– General information: https://www.boschsecurity.com/xc/en/support/product-security/
– Security advisories, that is a list of identified vulnerabilities and proposed solutions: https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html

Bosch assumes no liability whatsoever for any damage caused by operating its products with outdated software components.

2 System overview

Notice!
The following sections will mostly cover the Security Escort new hardware (SE coordinator and SE receiver) only. For information on the installation and configuration of old hardware (e.g. EA500 transponder, EA102 receiver, EA120 alert unit, Moxa and Lantronix interface, and others), please refer to the Security Escort 2.18 manuals.

2.1 What is Security Escort?

- Unique multiple user help call and asset tracking system
- Identifies user information and location, by floor, above or below ground
- Small, easy to carry transmitters
- Indoor/outdoor protection for 60,000+ users and assets as well as multiple buildings
- Man-down alarm, officer tracking & guard tour
- Post-alarm tracking and alarm map recall
- System capabilities perfect for campus and community environments

2.2 Emphasis on reliability

- Supported by a multi million dollar company
- Extensive field testing under maximum abuse conditions, from -20°F to +120°F
- Supervised system communication
- Low battery user and system operator notification
- Archived retrieval of system activity
- Patented technology
- Post alarm transmitter tracking
- System-wide backup power feature

2.3 System applications

- Student Safety
- Officer Tracking
- Guard Tour
- Employee/Faculty Security
- VIP Protection
- Executive Protection
- Man-Down
- Asset Tracking

2.4 Some example installations

Educational Facilities:
- Florida Southern, FL
- Oswego State, NY
- Nazareth College, NY

Healthcare Facilities:
- New Hanover Medical Center, NC
- Provo Psychiatric Hospital, Utah
- Fairport Retirement Home, NY

Correctional Facilities:
- Westchester County D.O.C., Valhalla, NY
- Immigration & Naturalization Facility, TX

– US Naval Brig, SC

Other:
– Diamond Mines, South Africa
– Amusement Park, FL
– International Art Museum, NY

2.5 Other system applications

– Hotels & Casinos
– Amusement Parks
– Commercial Complexes
  – Buildings
  – Parking Lots/Garages
– Museums
– Financial Institutions
– Child Care Facilities

2.6 Security Escort features

The Security Escort System is engineered to provide reliability and user ease of operation. Our patented feature set allows for customization and integration in any installation. These features ensure system integrity and the comfort that when assistance is needed, help is just a click away.

User Self Test
– Assures you that your transmitter is working
– Battery condition sent with every transmission
– Each test verifies system integrity
– Logs each test performed for easy access and reporting
– Can be performed indoors and outdoors
– Ensures user acceptance and peace of mind

Asset Tracking
– Location of assets
– Protection against removal
– Wireless sensing
– No re-cabling for asset relocation
– Auto tracking and location identification

Fixed Point Identification
– Allows for identification of any fixed point
– Simple system integration
– Expands over all system capability and functionality

2.7 System components description

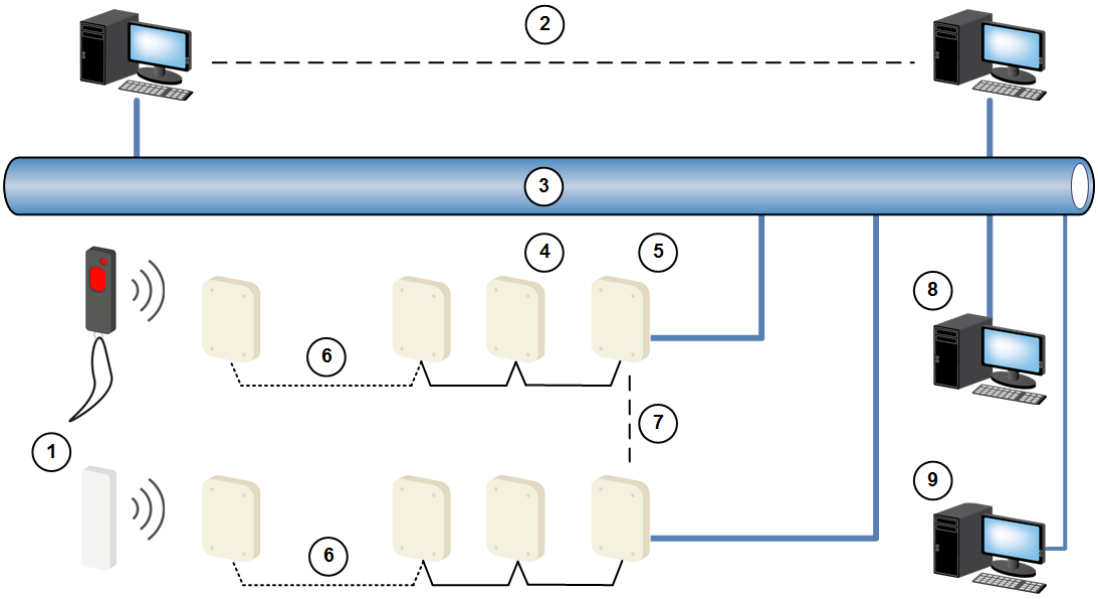


Figure 2.1: System Block Diagram

1	SE transmitters	6	Up to 15 SE receivers
2	Up to 8 workstations	7	Up to 1024 SE coordinators
3	LAN	8	Slave workstation
4	SE receivers	9	Master workstation
5	SE coordinator		

The Security Escort System consists of four basic components: SE transmitters, SE receivers, SE coordinators, and the Central Console.
The **SE transmitter** is a miniature, hand-held radio transmitter used to transmit either a distress or a test signal. The **SE receivers** are located throughout the protected area and detect the radio transmissions from SE transmitters. **SE coordinators** are devices that control groups of SE receivers, connected to them by wire. Each SE coordinator relays alarm and test signals from its SE receivers to the Central Console.
In addition, the SE coordinator tests for device and wiring faults, and transmits problem conditions to the Central Console. The **Central Console** consists of a computer (plus an optional backup and up to 8 optional workstations) which receives alarm and trouble signals from the SE coordinators, analyzes the signals, activates strobes and sirens, and produces a display for the Security dispatcher. Each of these system elements is described more fully in the sections that follow.

2.8 Compatible parts

The following table indicates the new parts available for inclusion in a Security Escort system.

Part Name	Description
Electronics, Components	
SE-COR-433	Electronics for coordinator

SE-RCV-433	Electronics for indoor or outdoor receiver
SE-TRM-433T01	Personnel transmitter
SEC-3402-433	Point tracking transmitter
SEC-RFPB60M-433	Pendant transmitter
Software	
SE2005	System software for up to 500 users
SE2010	System software for up to 1,000 users
SE2050	System software for up to 5,000 users

Contact Bosch Security Systems Customer Service or refer to website for the latest transmitter models.

The following table indicates the existing parts that are compatible with the new parts of the Security Escort system.

Part Name	Description
Enclosures and Housings	
AE3	Large enclosure, 51.5 cm x 37.5 cm (20.25 in x 14.75 in)
AE1	Small enclosure, 36.8 cm x 31.8 cm (14.5 in x 12.5 in)
AE_100	Indoor receiver enclosure
AE_101	Outdoor receiver enclosure

Contact Bosch Security Systems Customer Service or refer to website for up-to-date model numbers.

3 System components and specifications

3.1 Central Console

Description

The Central Console consists of one or two computers (and up to 8 additional workstations) running the Security Escort software within the Microsoft Windows environment. One computer serves as the master controller for the entire Security Escort system and the second slave computer serves as a back-up. The slave computer can be used for administrative functions such as adding subscribers or performing routine system tests without interfering with the operation of the main computer. The workstations can perform all normal Security Escort functions with the exception of communicating with the SE coordinators.

Software overview

The Central Console contains all of the operating software and all of the databases required by the Security Escort system. The installation and maintenance portion of the Security Escort software is designed to facilitate set-up and modification of the system and to provide rapid diagnosis of system problems, usually with only one person being required. The system software also continually monitors the status of each SE coordinator to ensure it is functioning correctly.

Versions

There are several versions of the software available. The number of users the system will support defines each version. The following table lists the available models and number of supported users:

Model	User Base
SE2005	500
SE2010	1,000
SE2050	5,000

Notice!

For systems supporting more than 5,000 users, contact Bosch Security Systems Sales.

Minimum system requirements

As a minimum, each computer in the Central Console should be equipped with the following features and components:

- **Processor:** Intel i5 and above
- **Operating system:** Microsoft Windows 7® 32/64-bit, Windows 8/8.1® 32/64-bit, Windows 10® 32/64-bit, Windows Server 2008, Windows Server 2012, Windows Server 2016 R2
- **Virtual operating system:** VMware® Workstation 12 Player or newer
- **RAM:** Minimum 2 GB, due to .NET requirement
- **Hard disk space:** 1 GB of hard disk space should be available to allow collection of historical data
- **Backup:** External backup drive for backup and history storage
- **Video:** Color depth of 32 bit should be used
- **Modem:** Optional V.32bis (14.4), V.34 (33.8), or V.90 (56.6) modem for remote access and pager dial-out. If modem is external an additional serial port is required.
- **Printer:** Network printers

3.2 SE coordinator

Features

- Relays alarm and test signals from the SE receiver to the Central Console.
- Can support a combined total of 16 SE receivers (inclusive of the SE coordinator's receiver).
- AC powered with battery backup for all SE receivers.
- Can provide power to SE485 Interface and/or Spread Spectrum Radio.
- Available in a large or small indoor enclosure.
- Monitors SE receivers for alarms, tests, tamper notification, and power loss.

Description

The SE coordinator is a device controller for up to 15 SE receivers. Its primary function is to monitor the SE receivers and report conditions and events to the Central Console via Ethernet communication. It also provides power output to certain devices.

Installation

The SE coordinator can be mounted in one of two different sized enclosures. It is always mounted indoors. The devices are connected to the SE coordinator by means of a multi-drop RS-485 twisted pair wire. Each bus is capable of supporting up to 15 SE receivers (excluding the SE coordinator). A Security Escort system supports up to 1024 SE coordinators.

Configuration

Each SE receiver is identified to the SE coordinator by an address which is set during system installation using the dip switch on the SE receiver circuit board. SE coordinators communicate on the data bus with individual devices by issuing commands, which contain the SE receiver's address.

Setup and testing

Each SE coordinator and the devices connected to it are set up and can be tested remotely from the Central Console. Also, each SE coordinator reports any problems, such as low battery, immediately upon detecting them.

Function during an alarm

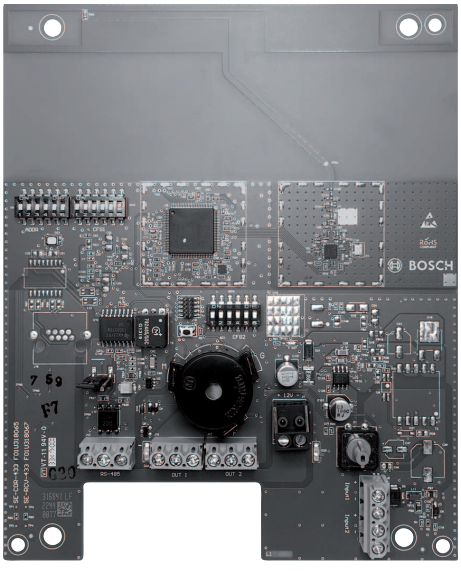
When a SE receiver detects an alarm, it goes into an "Off Normal" state. To quickly locate any devices which might be in the "Off Normal" state, the SE coordinator issues global commands (which are interpreted simultaneously by all of its devices) approximately 10 times per

second. These global commands are followed by commands to specific devices to determine the nature of the “Off Normal” condition and, in the case of an alarm (or test), to obtain the SE transmitter Identification Number, SE transmitter battery condition, and received signal strength. This information is then sent to the Central Console, by Ethernet wire, where it is used to display the identity of the subscriber transmitting the alarm and determine the subscriber’s location graphically.

Compatible Enclosures	AE_100 indoor enclosure AE_101 outdoor enclosure
Temperature Range	-30°C to +65°C (-22°F to +149°F)
Primary Power Source	Power over Ethernet (PoE)
Secondary Power Source	24 VDC in
Input	2 analog inputs (4 state supervised monitoring)
Output	2 relay outputs (relay dry contact, 1A @ 30 VDC)
Antenna Type	Internal
Sensitivity Adjustments	-100 dB minimum
Communication Interface	Ethernet 10/100 BaseT (Central Console) RS-485 (SE receivers)
Frequency	433.42 MHz

Notice!
The SE coordinator, SE receiver and SE transmitters are only compatible with other equipment using the same radio frequency band.

3.3 SE receiver



Features

– Receives SE transmitter alarms and tests, and relays the information to the SE coordinator.

- Built-in self testing through Buddy Check feature.
- Indoor and outdoor security enclosures available.
- Indoor enclosure provides confirmation of successful SE transmitter test (outdoor enclosures use other type of signaling device, such as a horn/strobe).
- Indoor SE receivers provide local sounders in alarm events.

Description

The SE receivers are located throughout the protected area, including building interiors. Each SE receiver contains a radio receiver to detect the transmissions from SE transmitters, and a microcomputer to decode and interpret the received test and alarm messages. In addition, the microcomputer monitors tampering and other problems, and reports such conditions to the SE coordinator.

Each SE receiver contains an internal self-contained sounder. These sounders are optionally activated if the SE receiver has detected an alarm transmission.

Indoor SE receivers are typically mounted on inside walls and are housed in small beige, rectangular units. Indoor SE receivers have one red and one green light. The green light is used to indicate a successful test of an SE transmitter; the red light is only illuminated during certain system tests and during alarms.

Outdoor SE receivers are contained in small weatherproof enclosures typically mounted on the sides of buildings and on light posts. Outdoor SE receivers do not have the visible red and green LEDs. Outdoors, the strobe lights connected to the SE receivers flash to acknowledge a successful test.

Function during an alarm

In the event of an alarm, the SE receivers detect an alarm signal from an SE transmitter and send this information to the SE coordinator. The SE coordinator forwards this information the Central Console where, using the reported information from all the SE receivers that detected the signal, the location of the transmission is graphically displayed on the Alarm Map.

Buddy check

In addition to its radio receiver, each SE receiver also contains a transmitter functionally similar to the hand held SE transmitters. This transmitter can be commanded by the Central Console to transmit a test message to other nearby SE receivers. This Buddy Checking is performed periodically to verify that the SE receivers are functioning satisfactorily. Results of the Buddy Check are compared with the results of earlier Buddy Checks, and any changes in an SE receiver's sensitivity are reported to the Central Console where this information is stored in a system database.

Compatible Enclosures	AE_100 indoor enclosure AE_101 outdoor enclosure
Temperature Range	-30°C to +65°C (-22°F to +149°F)
Power	24 VDC in
Input	2 analog inputs (4 state supervised monitoring)
Output	2 relay outputs (relay dry contact, 1A @ 30 VDC)
Antenna Type	Internal
Sensitivity Adjustments	-100 dB minimum
Communication Interface	RS-485 (SE coordinator/SE receivers)
Frequency	433.42 MHz

3.4 SE transmitters

The SE transmitters contain a unique code which is associated with the user at the time the transmitter is assigned. When the transmitter generates an alarm, this code is sent to the Central Console. The Central Console displays the transmitter location graphically on a map along with the user's picture, and his/her name, and any other necessary information.

3.4.1 SE personnel transmitter

Features

- Personal duress alarm transmitter.
- Man-down alarm.
- Lanyard pull alarm (optional).
- Allows user to test from anywhere within the protected area.
- Notifies Central Console of user's name and location immediately on alarm.
- Post-alarm and supervision tracking, alarm map recall, and more.
- Internal antenna.
- User replaceable battery with four-year life.
- Belt clip attachment.
- Optional silent manual alarm.
- Low battery indication.
- Optional holster for common security belt sizes.

Description

The SE personnel transmitter contains a unique code which is associated with the user at the time the transmitter is assigned. When the user generates an alarm, this code is sent to the Central Console. The Central Console displays the user's location graphically on a map along with the user's picture, and his/her name, and any other necessary information.

Transmitting an alarm

There are three ways in which an alarm may be generated, depending on the features enabled on the SE transmitter. The types of alarms are as follows:

- **Manual Duress Alarm:** An alarm can be initiated by pressing the large button on the SE transmitter.
- **Man-Down Alarm:** The SE transmitter will transmit an alarm to the Central Console if it is tipped 60° from upright.

– **Lanyard Pull:** A cord connected to the pin, inserted in the base of the SE transmitter can be looped around a utility belt. If the pin is removed from the SE transmitter (such as when the SE transmitter is pulled away from the belt), the SE transmitter will immediately go into alarm.

Auto-tracking feature

During an alarm, the SE transmitter automatically resends the alarm signal every few seconds constantly updating the Central Console of the user's location.

Supervision tracking

With "Supervision Tracking" enabled, the SE transmitter will send a tracking signal to the Central Console constantly updating the user's location.

Testing

The "Test" mode allows users to test their SE transmitter anywhere in the protected area. When the user is located indoors in sight of an indoor SE receiver, or outdoors in sight of a strobe wired to the output of an outdoor SE receiver, pressing the manual test button performs a test. If the test is successful, a small green light will flash on the indoor SE receiver, or the strobe will flash briefly. There will be no response at all if the test fails. If the test fails, the user should contact the Security Office as soon as possible.
When the SE transmitter is tested, a special "low battery" message is included in the transmission to Central Console if the SE transmitter's battery is in need of replacing. Every successful test is recorded in the **Subscriber Database** in the Central Console Software and optionally printed on the hardcopy printer. The **Subscriber Database** contains all of the information related to each subscriber, including the date and time of the most recent test transmission. It is possible to search the **Subscriber Database** for individuals who have not performed tests for a specified period of time.

Temperature Range	-20°C to 65°C (-4°F to 149°F)
Battery	3V Lithium CR2 or equivalent
Communication Interface	Wireless radio frequency (SE coordinator/SE receiver)
Frequency	433.42 MHz

Notice!
The SE personnel transmitter is only compatible with other equipment using the same radio frequency band.

3.4.2 Point tracking transmitter

Features

- Supervision.
- Manual duress alarm.
- Low battery indication.
- Flexible mounting options.

Description

The Point Tracking Transmitter contains a unique code that is associated with the item attached to the transmitter. During an alarm, the transmitter sends this code to the Central Console. The Central Console software displays the item's photograph, location on a map, and any relevant information.

Supervision

The transmitter can send a tracking signal to the Central Console every 60 minutes (user configurable), updating the transmitter's location. During periods of inactivity, the transmitter sends one status and location report to the Central Console every hour. To reset the transmitter, restore all device conditions such as tamper, loop, and magnet, to normal.

Manual Duress Alarm

During an alarm, the transmitter automatically continues to transmit every 7 seconds, providing the most current location information.

Low Battery Indication

At test mode, when the transmitter’s battery needs replacement, a low battery message appears on the Central Console.

Reed Switch or External Input

The transmitter has the capacity to monitor magnetic and/or dry external contacts. External Normally Closed (NC) or external Normally Open (NO) contacts can be monitored.

Temperature Range	-20°C to 65°C (-4°F to 150°F)
Battery	3V Lithium or equivalent
Communication Interface	Wireless radio frequency (SE coordinator/SE receiver)
Frequency	433.42 MHz

Notice!
The point tracking transmitter is only compatible with other equipment using the same radio frequency band.

3.4.3 Pendant transmitter

Features
- Supervision
- Auto-tracking
- Water and dust resistant
- Up to 3 years battery life
- Low battery indication

Description
The pendant transmitter is designed to work with the Security Escort system. When an alarm is initiated, a signal identifying the transmitter and its location is sent to the Central Console at regular intervals. The Central Console software displays the item's photograph, location on a map, and any relevant information.

Supervision
To identify the last known location, the transmitter sends a tracking signal to the central console every 60 minutes.

Manual duress alarm
When help is needed, pressing both buttons simultaneously will generate a duress alarm. During this alarm, the transmitter continues to transmit automatically every 10 seconds for a duration of 10 minutes.

Test alarm
Initiate a test alarm whenever required to conduct a health check functionally, to verify the transmission of the radio frequency signal, and also its battery level measurement.

Low battery indication
If the transmitter’s battery needs replacing, a low battery message is sent to the central console whenever a test alarm is initiated.

Temperature Range	-10 °C to +49 °C (+14 °F to +120 °F)
Battery	CR2032 lithium coin cell battery, 3 VDC
Communication Interface	Wireless radio frequency (SE coordinator/SE receiver)
Frequency	433.42 MHz

Notice!
The pendant transmitter is only compatible with other equipment using the same radio frequency band.

4 Equipment estimation

A Security Escort system installation consists of three major steps:

1. the initial equipment estimate,
2. the pre-installation coverage verification, and
3. the post installation after survey.

The SE receivers work effectively in a wide variety of installations and can be placed with confidence provided these installation requirements are met. Therefore, It is acceptable to estimate the initial required equipment. To ensure proper coverage after proposal acceptance, potential SE receiver locations can be verified using a standard SE receiver in test mode or the portable test SE receiver before installation begins.

4.1 Location accuracy

The Security Escort system provides quick response to a duress call. Its intent is to dispatch a responding individual to an area without additional delay to their response to that duress call. The Security Escort system uses radio frequency (RF) for alarm transmissions. This is significant because it prevents normal construction from blocking the signal and helps to eliminate dead spots where the alarm could not be heard. The fact that RF energy passes through normal construction prevents Security Escort from locating an alarm with 100% certainty to a specific side of a wall. Alarms originating at or near building walls will typically be indicated within 7.5 m (25 ft) of the actual location. However, there may be times when the computed location may appear to be on the other side of the wall.
The Security Escort system was designed to provide a computed alarm location typically within 7.5 m (25 ft) of the actual location when indoors, and a computed alarm location typically within 15 m (50 ft) of the actual location outdoors. Any deviation from the following installation guidelines will degrade the computed location accuracy. Therefore, to achieve accuracy, the following installation guidelines must be adhered to.

4.2 Initial equipment estimate

4.2.1 Number of indoor SE receivers

To estimate the number of indoor SE receivers, read the *Indoor SE receiver installation (Summary), page 27* first. Assume the SE receivers are placed on a grid with a maximum spacing of 25 m (80 ft) between SE receivers for standard construction. In multi-floor applications, the SE receivers on each floor must be placed directly above the SE receivers on the floor below (this is required for proper floor-to-floor location).
For example, to determine the number of SE receivers required to protect a building of standard construction of 60 m x 30 m (200 ft x 100 ft) and four floors:

1. To determine the number of SE receivers in each direction, divide each dimension of the building by 25 m (80 ft), drop the remainder, and add 1. For example:
   - 60 m/25 m = 2.4, becomes 2, add 1 = 3
     (200 ft/80 ft = 2.5, becomes 2, add 1 = 3)
   - 30 m/25 m =1.2, becomes 1, add 1 = 2
     (100 ft/80 ft =1.25, becomes 1, add 1 = 2)
2. To determine the number of SE receivers required per floor, multiply the number of SE receivers in one direction by the number of SE receivers in the other direction.
   Number of receivers per side x number of sides
   - 3 x 2 -= 6
   6 SE receivers per floor.

3. To determine the total number of SE receivers, multiply the number of SE receivers per floor by the number of floors.
   Number of receivers per floor x number of floors
   - 6 x 4 = 24
   24 SE receivers for the building

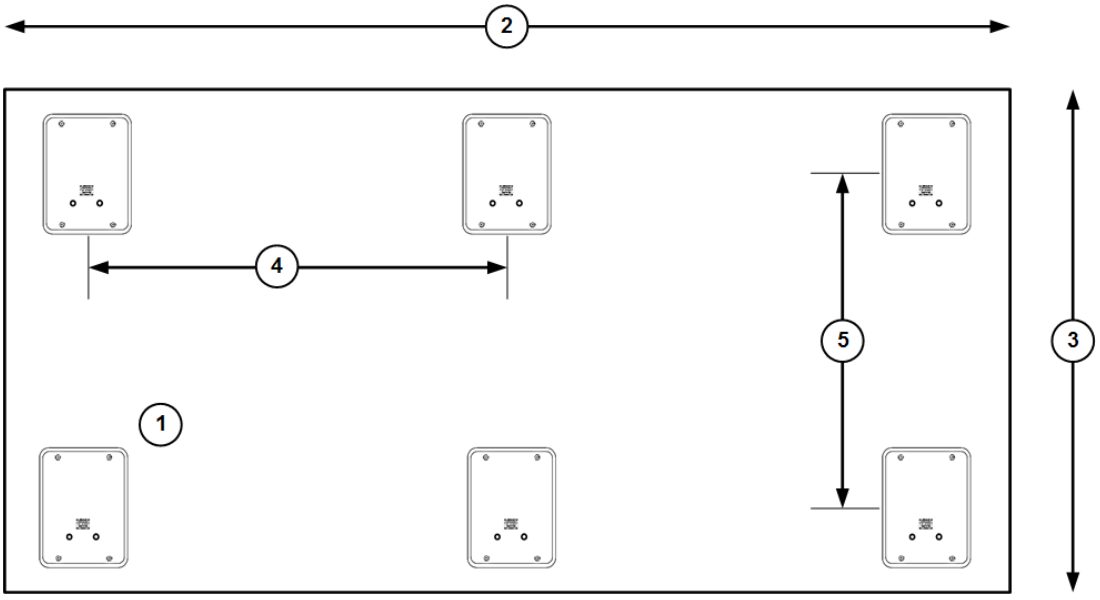


Figure 4.1: Determining the Number of Indoor SE receivers Required

1	SE receivers (6 units)	4	25 m (80 ft)
2	60 m (200 ft)	5	25 m (80 ft)
3	30 m (100 ft)		

For the best location accuracy, consistent SE receiver spacing is important. Do not place SE receivers significantly closer in one section of a building than another section.

4.2.2 Number of outdoor SE receivers

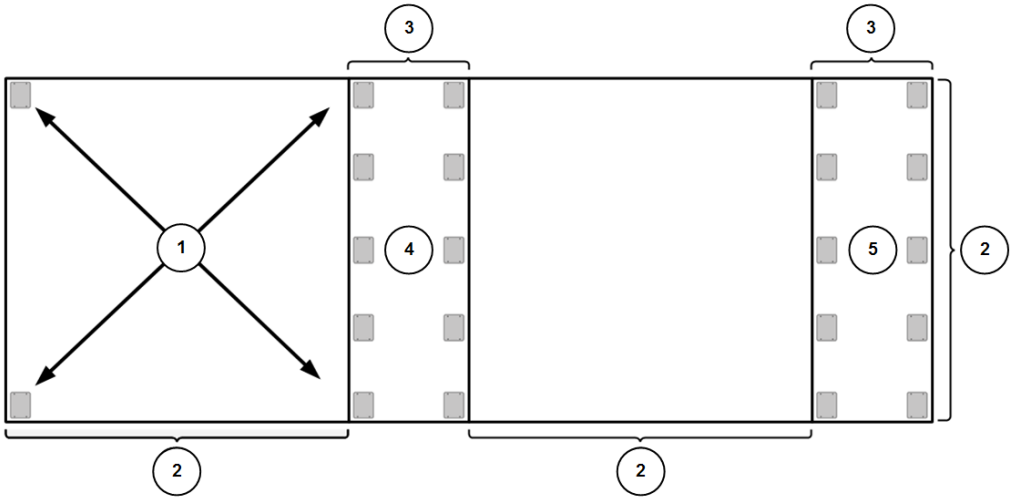


Figure 4.2: Number of outdoor SE receivers

1	SE receivers	2	90 m (300 ft)
3	30 m (100 ft)	4	Building 1
5	Building 2		

To estimate the number of SE receivers, read the Outdoor SE receiver installation first.
Assume a maximum SE receiver spacing of 90 m (300 ft) between SE receivers, in both directions, for SE receivers that are not within 30 m (100 ft) of a building with inside coverage. SE receivers within 30 m (100 ft) of a building should be spaced the same as SE receivers in the building (spacing the outside SE receivers at a somewhat larger spacing is acceptable in most cases).
An outside area directly between two buildings with inside protection will need no additional SE receivers if the buildings are 90 m (300 ft) or less apart. If the buildings are more than 90 m (300 ft) apart the outside SE receivers should be evenly spaced between the buildings.

Notice!
Make sure the standard 90 m (300 ft) spacing is not exceeded. For spacing outside adjacent to a covered building, start the 90 m (300 ft) spacing at the building wall.

4.2.3 Allowance for special coverage requirements

The number of SE receivers estimated above should be raised by 5% to allow for special coverage considerations and RF problem areas.

4.2.4 Number of SE coordinators and SE receivers

Assume that one SE coordinator will be installed per building for indoor installations. If wiring can be run from other buildings or from outdoor SE receivers, they may be connected to that SE coordinator. All outside wiring must be under ground, or in metal conduit.
Each SE coordinator can handle 15 SE receivers only. However, it is a good idea to leave some addresses available on each connection to allow for future expansion.

Bus wire
The recommended wiring for RS-485 communication is 24-AWG Cat5e or better, using 4-conductors, with unshielded twisted pair for indoor installations, and shielded twisted pair for outdoor.

4.3 Pre-installation coverage verification

The pre-installation coverage verification is performed before construction begins. It is done to determine the location of each SE receiver. Each SE receiver location should be checked using a standard SE receiver in the test mode.

4.3.1 Verify each potential SE receiver location

Using an SE receiver with ”receiver spacing” mode
”Receiver spacing” mode is enabled by setting switch number 1 of dip switch CFG2 on the SE receiver (see the Security Escort Coordinator & Receiver Installation Manual).
This mode is exactly the same as the “test” mode, except that the sounder is triggered for transmissions with an adequate receive margin. This indicates the maximum acceptable spacing of SE receivers. Use the following procedure to test the spacing of SE receivers:

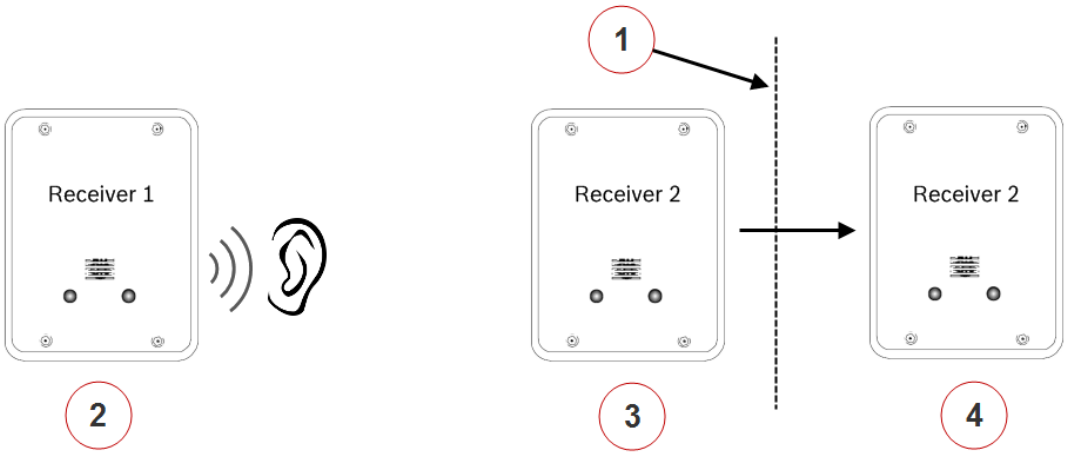


Figure 4.3: SE receiver Spacing

1	SE receiver 1 stops sounding the test beeps when SE receiver 2 is moved past this point	3	SE receiver 2 at maximum range
2	SE receiver 1	4	SE receiver 2 beyond maximum range

1. Mount the first SE receiver (SE receiver 1). Set switch number 1 of dip switch CFG2 to the ON position. Power the SE receiver from a 12 VDC source.
2. Take the second SE receiver (SE receiver 2) and an SE transmitter a distance away from the first SE receiver (SE receiver 1).
3. Activate the SE transmitter.
4. If SE receiver 1 sounds the test beep, SE receiver 2 is within range. Repeat this test until SE receiver 1 no longer sounds the test beeps. Move back to the last location where SE receiver 1 received the test beeps. This location marks the maximum spacing between the SE receivers. The distance between the SE receivers should not exceed 25 m (80 ft) indoors and 90 m (300 ft) outdoors. Mount SE receiver 2 at this location or closer to SE receiver 1.

Using an SE coordinator, SE receivers and laptop computer to determine SE receiver location.

Notice!
System software and area map must be installed on laptop computer to use this method.

Before the SE receivers are mounted, an SE coordinator with long RS-485 wires connected to the SE receivers can be used to see actual alarm location. Place the SE receivers in the proposed locations wired back to the SE coordinator. Program the SE receivers with their locations in the **Transponder Database**.
Using the maintenance SE transmitter and the maintenance alarm database, activate alarm transmissions within the area surrounded by the temporarily placed SE receivers. Verify that the location accuracy is acceptable at all points of concern. If not acceptable, move the SE receivers, update the SE receiver location in the **Transponder Database** and retest.
Do not test outside of the last SE receiver in any direction, as this will give incorrect locations. Repeat this test in all areas of different construction and concerns at the site.

4.3.2 Indoor SE receiver installation (Summary)

- Indoor SE receivers must be mounted in a evenly spaced grid no more than 25 m (80 ft) apart.
- Indoor SE receivers must be mounted 1.5 m to 1.8 m (5 ft to 6 ft) above the floor. This is true even if this is a single story building. Do not mount SE receivers above the ceiling or in roof rafters.
- In multistory buildings, the SE receivers must be mounted directly above the SE receivers on the floor below. The same number of SE receivers must be used on each floor level. If you meet all of the indoor installation guidelines, you can expect the computed location to indicate the correct floor about 95% of the time.
- SE receivers must not be mounted within 30 cm (1 ft) of any metal object, including wire mesh, metal foil, metal pipe and HVAC ducting in walls.
- Take care that large metal objects do not shield an SE receiver from a protected area. For example metal staircases, metal food serving lines, metal walls, lead lined walls, metal roofs, wire mesh in walls, walk-in freezers and refrigerators.

For the best indoor and outdoor location or an indoor only system

- Mount the indoor SE receivers on the recommended 25 m (80 ft) grid, with the last row of indoor SE receivers on the outside wall of the building. Do this even if the building is less than 25 m (80 ft) wide or long.
- There should be an SE receiver at each outside corner of a building.

Handling two protected buildings sharing a common wall with floor levels that do not match

- Ask the customer which building has areas of greater concern and favor the recommended mounting heights in that building.
- The recommended 25 m (80 ft) maximum indoor spacing grid should be maintained throughout both buildings as if the wall in question was not there. Mounting heights only for those SE receivers at or near (within 6 m [20 ft]) the wall in question should be affected. Mounting heights for all other SE receivers in the buildings must follow the indoor recommendation. Mark the recommended mounting height for SE receivers on the higher floor level and also mark the recommended mounting height for SE receivers on the lower floor level. Mount the SE receiver at its normal grid location midway between these two heights, but not above the ceiling level of the lower floor.

4.3.3 Outdoor SE receiver installation (Summary)

- Outdoor SE receivers must be mounted in a evenly spaced grid no more than 90 m (300 ft) apart.
- Outdoor SE receivers must be mounted 3 m (10 ft) above the ground.
- SE receivers must not be mounted within 30 cm (1 ft) of any metal object, including fences, metal walls and walls with wire mesh. If an SE receiver is mounted on a metal fence, that fence should be grounded (not floating or insulated from ground) and the SE receiver should be spaced 30 cm (1 ft) from the fence and 3 m (10 ft) above the ground.
- Take care that large metal objects do not shield an SE receiver from a protected area. For example; metal fences, metal staircases, metal buildings, power transformers and metal roofs.
- SE receiver locations should be below building overhangs and eaves as these can shield the areas below them.

– SE receivers should have a clear line of sight of the protected area. Therefore, take care where the ground is hilly or uneven, that there are no areas and low spots where several receivers can't hear the signal.

Transition areas between indoor and outdoor areas

– An outside area directly between two buildings with complete indoor protection will need no additional SE receivers between the buildings, if they are 90 m (300 ft) or less apart.
– When protecting an outside area directly between two buildings with complete indoor protection, and they are more than 90 m (300 ft) apart, place a row of outside SE receivers evenly spaced between the buildings. Make sure the SE receiver row does not exceed the standard 90 m (300 ft) spacing from the buildings. The spacing between SE receivers in that row should be about the same as the spacing for the SE receivers in the buildings.
– However, if a building is adjacent to an outdoor area, that building will have a greater density of SE receivers and, therefore, has a tendency to pull the computed location towards it. To counteract the building tendency to pull the location, consider the following special cases:
  – If the outdoor area adjacent to the building is wide open and the customer is not concerned about reduced location accuracy in this area, then nothing special needs to be done. Follow the normal indoor and outdoor recommendations.
  – The building is near the boundary of the protected area, with or without a fence at the boundary. The SE receivers at the boundary of the protected area near the building should be spaced about the same as those in the building, approximating the same grid as used in the building.
  – The building is adjacent to a large protected outdoor area that extends for more than 90 m (300 ft) from the building. The SE receivers in the large protected outdoor area should be placed on the normal 90 m (300 ft) grid except for the first row of SE receivers adjacent to the building. This first row of outdoor SE receivers in the transition area should "split the difference" between the indoor and outdoor spacing at about 60 m (200 ft).

Boundary areas at the outer edge of the protected area

The system cannot locate an alarm past the last SE receiver at the boundary of the protected area. Therefore, the last row of SE receivers must be at or past the end of the protected area.

4.4 Post installation after survey

4.4.1 Testing the location accuracy of an installation

Notice!

Before doing any of the following testing, it is important to verify that every SE receiver in the system is functioning correctly using the procedure described in the Security Escort Hardware Installation Manual and Software Installation Manual. Additionally, every SE receiver must be programmed in the **Transponder Database** with its actual physical location and floor level. **It is also important that SE receivers which are physically stacked directly above one another on floors of a building are also located at the same X and Y coordinates in the database**.

There are three methods that can be used to verify the location accuracy of an installed system, using a standard subscriber or maintenance SE transmitter. Repeat the chosen process throughout all protected areas. Ask the customer for the areas where they have special concerns and devote extra attention to those areas, since the customer is likely to be more critical in those areas.
Remember the intent of the Security Escort system is to dispatch a responding individual to an area that will not add additional delay to their response to that duress call. Therefore, the computed location should be considered to be in error only when it would add unacceptable additional time to the alarm response.
While testing, it is helpful to see which SE receivers are involved in the alarm response and the relative reception level they reported. To display the SE receivers, select menu **Utilities > Security Preferences**. Make sure the **No receiver icons** checkbox is not checked and click the **[Save]** button. Select menu **Setup > System Preferences.** If **Show test levels** and **Show maintenance levels** checkboxes are checked, the relative reception level is shown in the SE receiver icons; otherwise, the floor number will be shown.
When testing with any of the following methods, the SE transmitter must be used exactly as it would be used in normal operation. An SE transmitter designed to be belt mounted or used in a holster must be in its normal mounting attitude and be worn on the belt of the individual originating the test transmissions. Handheld SE transmitters must be held in the hand about waist high, never held above the head.

Using a standard subscriber SE transmitter

1. This method requires two people with radio contact between them. One person operates the computer running the Security Escort software, and the other takes the subscriber SE transmitter to the area to be tested.
2. Press the alarm on the SE transmitter and remain at the spot where you transmitted.
3. The computer operator acknowledges the alarm and accurately describes the computed location over the radio. The individual with the SE transmitter should confirm the reported location or describe over the radio the actual location. Either individual must record all discrepancies, including the actual and computed locations.
   We recommend using a map or floor plan and drawing an arrow from the actual alarm location to the reported location. It is also helpful if all successful alarm locations are marked with a **P** (passed), then the alarm can be reset from the computer screen.
4. For areas where there are alarm location problems, try facing in different directions in the same spot. Also generate additional alarms from different spots to fully understand the extent of the problem. You should generate alarms in areas adjacent to the area with the problem to see if they are also affected.

Using a maintenance SE transmitter with only one person

1. The Security Escort software retains the last 50 maintenance alarm locations. Make sure you are the only one using a maintenance SE transmitter on site, buddy check is off, and that you limit yourself to a maximum of 50 maintenance alarms per sequence.
2. Synchronize the time on your watch to the computer. Carry a detailed map or floor plan of the area to be tested that you can write on.
3. Take the maintenance SE transmitter to the area to be tested. Press the alarm on the SE transmitter and accurately mark the spot on the map where you transmitted with a “1” (for the first transmission). Also record the time of the first transmission only.

4. Continue to the next location, transmit and mark that spot on the map with a “2.” Repeat the process throughout the area to be tested, being sure not to exceed 50 alarm transmissions and making sure that at least 10-sec. elapse between transmissions.
5. When finished, return to the computer and select menu **File > Maintenance Alarm Database**. Scroll through the alarm list to find the alarm that matches the time of your first transmission. This is the maintenance alarm that you marked as “1” on your map.
6. Confirm that the actual location from the map matches the reported location.
7. If the actual location differs from the reported location, draw an arrow on the map from the actual location to the reported location. Press the up arrow once to go to the next alarm. Compare the locations, drawing an arrow to the reported location if they differ. Repeat this procedure for all points on your map, making sure that the points on the map stop when you run out of entries in the scrolling list on the computer screen. Otherwise, the points on the map and the screen are out of sync and the errors on your map are incorrect and misleading.
8. For areas where there were alarm location problems, you may want to repeat the above process facing in different directions from the same spot. This generates additional alarms from different spots in the problem areas to fully understand the extent of the problem.
9. You should also generate alarms in areas adjacent to the area with the problem to see if they are also affected.

Using a maintenance SE transmitter with two people

1. The two people must have radio contact between them. One person operates the computer running the Security Escort software and the other takes the maintenance SE transmitter to the area to be tested.
2. At the computer, select menu **File > Maintenance Alarm Database**. Make sure the top item in the scrolling list is selected.
3. Press the alarm on the SE transmitter and remain at the spot where you transmitted. At the computer, observe the alarm and accurately describe the computed location over the radio. The individual with the SE transmitter should confirm the reported location or describe the actual location over the radio. Either individual must record all discrepancies, including the actual and computed locations. We recommend using a map or floor plan and drawing an arrow from the actual alarm location to the reported location. It is also helpful if all successful alarm locations are marked with a **P** (passed).
4. For areas where there are alarm location problems, try facing in different directions from the same spot.
5. Generate additional alarms from different spots to fully understand the extent of the problem.
6. You should generate alarms in areas adjacent to the area with the problem to see if they are also affected.

Reviewing potential problem areas

Review the potential problem areas on the maps with the customer to see which areas cause them concerns, and which areas they consider acceptable. If the customer considers an area acceptable, it is typically not worth spending additional time trying to improve the location accuracy in those areas.

4.4.2 Improving the location accuracy of an installation

Once we have identified those areas that must be improved, what are the options to improve the computed location accuracy?

Notice!
All changes using the following steps could potentially change the computed locations for all alarms at or around the changed area. Therefore, after any change is made, the entire vicinity around the changed area must be verified.

- Typically the first thought is to add more SE receivers in the problem area. Generally this is a bad approach. If the system was properly designed using the recommended grid layout, adding extra SE receivers in any area of the grid will distort the response in adjacent areas and floors. While it may seem to fix the problem area, typically it will create more problems in adjacent areas. The exception is when an area is shielded by something such as wire mesh in the walls that prevent the RF transmitted signal from passing through. Therefore, additional SE receivers may have to be added in the shielded area to ensure that all alarm transmissions will be heard.
- Verify that the location of the SE receivers in the **Transponder Database** is accurate to their physical location, and the SE receivers are indicated to be at the correct floor level. It is also important that SE receivers that were physically stacked directly above one another on floors of a building are also located at the same X and Y coordinates in the database.
- Try changing the **Transponder Database** location of SE receivers (not the actual physical location) one at a time while testing the alarm location response, using one of the testing methods above. For example, if alarms are getting pulled outside a building in one area, move the closest SE receiver (in the **Transponder Database**) to that area a little further into the building and retest. If the area can be corrected using this method, verify the surrounding areas to make sure they were not adversely affected. It is generally better if the correction is done in small steps while verifying the adjacent areas, rather than trying to correct the entire error in one step.
- The Security Escort software allows individual SE receiver sensitivity to be set in the **Transponder Database**. SE receivers can be adjusted from 50% to 149% of their normal sensitivity. No physical SE receiver changes or upgrades are required. Try changing the **Transponder Database** sensitivity of SE receivers one at a time while testing the alarm location response, using one of the testing methods above. For example if alarms are being pulled towards a particular SE receiver, lower its sensitivity in 10% increments and retest. If the area can be corrected using this method, verify the surrounding areas to make sure they have not been adversely affected. **It is generally better if the correction is done in small steps while verifying the adjacent areas, rather than trying to correct the entire error in one step**.
- There are five different location algorithms that can be selected on an individual receiver basis in the **Transponder Database**. “Classic” (original Security Escort algorithm), “Linear”, “Low“ pull, “Medium” pull and “Strong” pull. By default, when an SE receiver is set for outside or tunnel, it will use the “Linear” algorithm and all other SE receivers will use the “Low” pull algorithm. The SE receiver that hears the alarm transmission the strongest will determine the algorithm used for this alarm. Changing the **Transponder Database** algorithm setting for an SE receiver only affects the location when the alarm is close to this SE receiver and it hears the alarm the strongest. Change the **Transponder Database** algorithm setting for an SE receiver and test in its area, using one of the testing

methods above. The stronger the pull the more the alarm will be pulled towards the SE receiver, with “Linear” having no extra pull. Verify the surrounding areas to make sure they have not been adversely affected.

– The five different location algorithms can individually limit how close other SE receivers must be to the level of the SE receiver hearing the alarm the best, before they will be included in the alarm. “Classic” (original Security Escort algorithm), “Linear”, “Low” pull, “Medium” pull and “Strong” pull each have a separate setting. By adjusting this setting you can control if distant SE receivers with low receive levels will be considered in the alarm calculation.
– You can add “Virtual” receivers in the **Transponder Database**. A “Virtual” receiver is added at one of the 15 points allowed per SE coordinator. However, there is no physical hardware used. The “Virtual” receiver is intended to compensate in cases where there is an SE receiver imbalance. For example if a building with a dense population of SE receivers is adjacent to a fence with few SE receivers and an alarm occurs between them; the alarm location may pull towards the building. The “Virtual” receiver references to other physical SE receivers that must be on the same SE coordinator. Only if both of the referenced SE receivers receive an alarm transmission, then the “Virtual” receiver will be added to the alarm as if was a physical SE receiver that heard the alarm at the average receive level of the two reference receivers.
  The “Virtual” receiver’s location and sensitivity may be adjusted the same as a physical SE receiver. After a “Virtual” receiver is added, verify the surrounding areas to make sure they have not been adversely affected. **In no event should a “Virtual” receiver be utilized as a cost savings measure to avoid the installation of an actual SE receiver**.

5 System wiring

5.1 General wiring guidelines

After the site survey (and special pre-installation verifications) has been completed, the wiring can be run between the proposed locations of the system components and the Central Console. See specific installation instructions accompanying each component for wiring details.

5.1.1 General wiring diagram

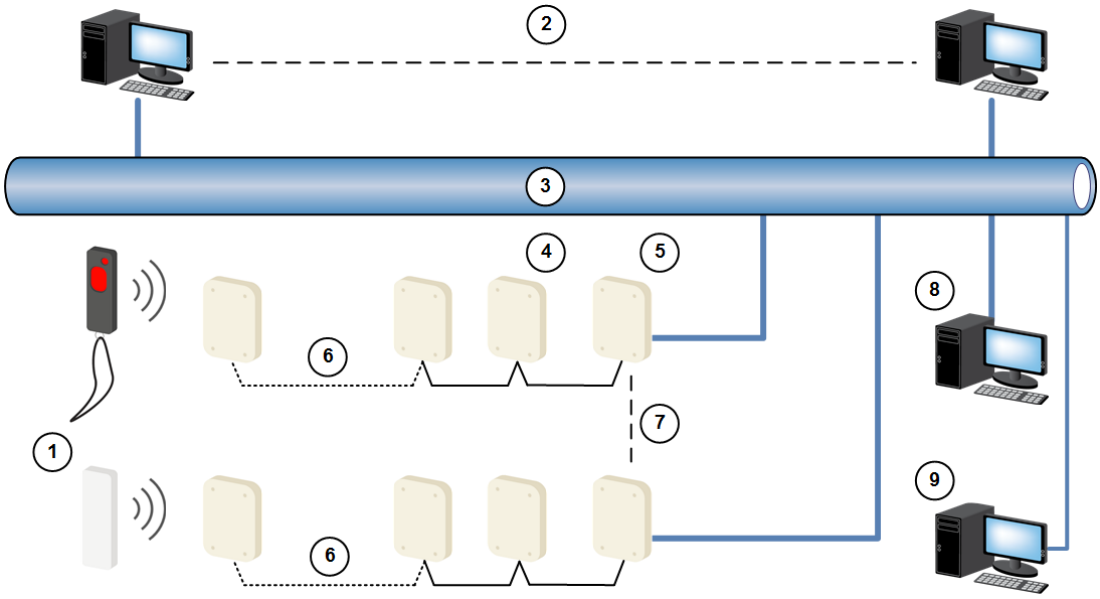


Figure 5.1: System Block Diagram

1	SE transmitters	6	Up to 15 SE receivers
2	Up to 8 workstations	7	Up to 1024 SE coordinators
3	LAN	8	Slave workstation
4	SE receivers	9	Master workstation
5	SE coordinator		

The Security Escort System consists of four basic components: SE transmitters, SE receivers, SE coordinators, and the Central Console.
The **SE transmitter** is a miniature, hand-held radio transmitter used to transmit either a distress or a test signal. The **SE receivers** are located throughout the protected area and detect the radio transmissions from SE transmitters. **SE coordinators** are devices that control groups of SE receivers, connected to them by wire. Each SE coordinator relays alarm and test signals from its SE receivers to the Central Console.
In addition, the SE coordinator tests for device and wiring faults, and transmits problem conditions to the Central Console. The **Central Console** consists of a computer (plus an optional backup and up to 8 optional workstations) which receives alarm and trouble signals from the SE coordinators, analyzes the signals, activates strobes and sirens, and produces a display for the Security dispatcher. Each of these system elements is described more fully in the sections that follow.
The following table indicates the specifications for the wiring:

From	To	Signal Type	Gauge	Max. Length	Remark
SE coordinator / SE receiver	SE receiver	RS-485	#24	1000 m per bus	Twisted pair Cat5e cable recommended. Shielded cable may be required for outdoor use.
	Power Supply	Power	#18	Please refer to the sections below for detailed specification.	
			#24		
	Input 1 or 2	I/O	#18	15 m	Solid, not twisted, not shielded
	Output 1 or 2	I/O	#18	15 m	Solid, not twisted, not shielded
SE coordinator	Host PC	Ethernet / PoE	Cat5e UTP	100 m	Shielded cable may be required for outdoor use

Table 5.1: Specifications for Wiring

5.2 Component wiring guidelines

5.2.1 Indoor wiring diagram with APS-PSU-60 using 18 AWG

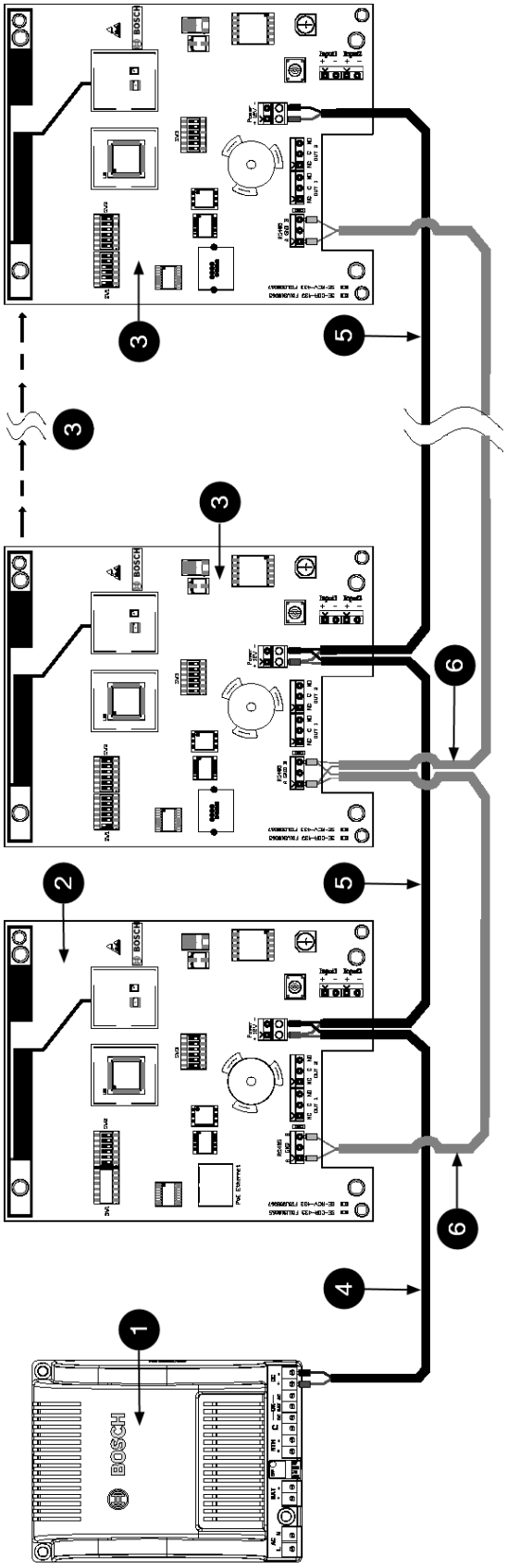


Figure 5.2: Wiring diagram example for indoor configuration using 18 AWG cable for input power

Item	Specification	Description	Quantity	Remarks
1	APS-PSU-60	Power supply	1	Output voltage set to 24V mode
2	SE-COR-433	SE coordinator board	1	
3	SE-RCV-433	SE receiver board	Up to 15	Maximum number of SE receivers that can be connected to the SE coordinator
4	18 AWG, 2 wires not twisted multi strands	15 m power cable from power supply to SE coordinator	1	Wire color: - red for (+) input - black for (-) input
5	18 AWG, 2 wires not twisted multi strands	24 m power cable from SE coordinator / SE receiver to SE receivers	Up to 15	Wire color: - red for (+) input - black for (-) input
6	4x2x24 AWG, Cat5e twisted multi strands	24 m twister pair RS-485 cable from SE coordinator / SE receiver to SE receivers	Up to 15	Wire color: - orange/white for RS-485 (A) - white/orange for RS-485 (B)

Notice!
Wire colors of Cat5e cable mentioned above may differ in other countries, depending on color coding standard.

Notice!
Please refer to the PSU-60 - AMC Power Supply Unit Quick Installation Guide for the configuration of APS-PSU-60.

5.2.2 Indoor wiring diagram with APS-PSU-60 using 24 AWG cable

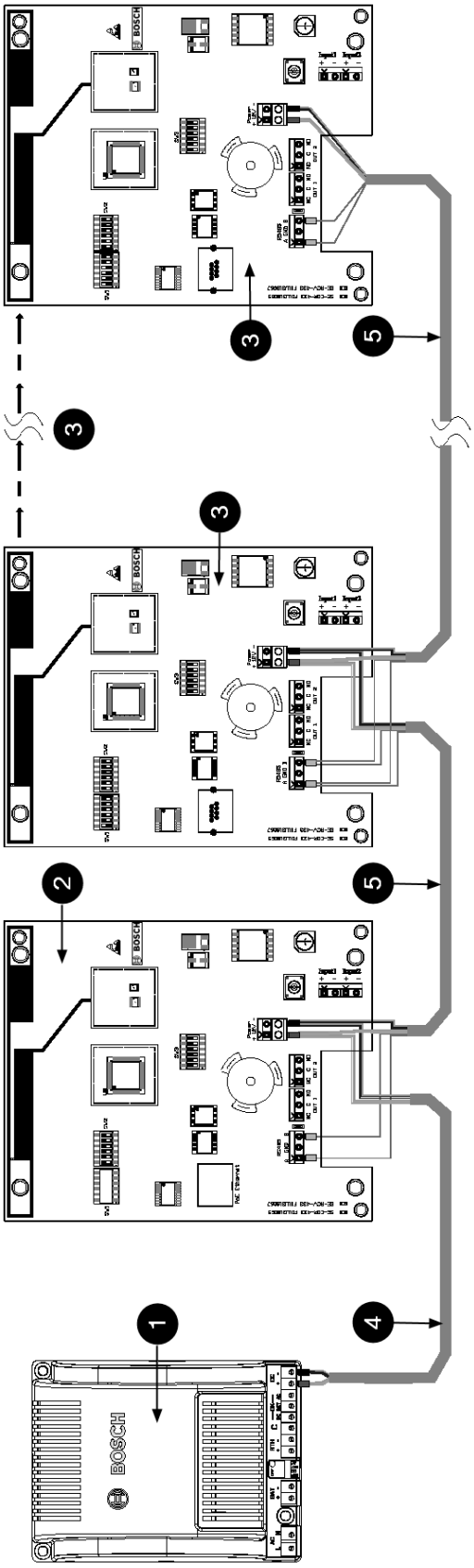


Figure 5.3: Wiring diagram example for indoor configuration using 24 AWG cable for input power

Item	Specification	Description	Quantity	Remarks
1	APS-PSU-60	Power supply	1	Output voltage set to 24V mode
2	SE-COR-433	SE coordinator board	1	
3	SE-RCV-433	SE receiver board	Up to 15	Maximum number of SE receivers that can be connected to the SE coordinator
4	4x2x24 AWG, Cat5e twisted multi strands	15 m power cable from power supply to SE coordinator (**use 3 pairs**)	1	Wire color: - brown/white and white/brown and green/white for (+) input - blue/white and white/blue and white/green for (-) input
5	4x2x24 AWG, Cat5e twisted multi strands	24 m power cable from SE coordinator / SE receiver to SE receivers (**use 3 pairs**) - 1 twisted pair for RS-485 communication	Up to 15	Wire color: - brown/white and white/brown and green/white for (+) input - blue/white and white/blue and white/green for (-) input - orange/white for RS-485 (A) - white/orange for RS-485 (B)

Notice!
Wire colors of Cat5e cable mentioned above may differ in other countries, depending on color coding standard.

Notice!
Please refer to the PSU-60 - AMC Power Supply Unit Quick Installation Guide for the configuration of APS-PSU-60.

5.2.3 SE coordinator/SE receiver wiring notes

Mounting

Normally, the enclosures are mounted first with the laying of cables and wires. Then, the electronics are mounted, wired, and tested. The enclosures come with their own mounting hardware (H500 Hardware Kit) for mounting the enclosure to a wall and mounting the circuit board to the enclosure.

– Mount the enclosure to the mounting surface.
– Mount the circuit board to the enclosure.

Leave at least 10 cm (4 in.) of wire hanging out of the unit. Do not leave extra wire inside the enclosure as this could impact the receiving antennas.

Wiring

The SE coordinator and SE receivers communicate with each other using the RS-485 interface. The communication connector is identified by their 3 terminal points, namely A, GND and B. The recommended data transmission speed is 19200 bps @ 1km (default) and 115 kbps @ 500m. Please refer to the table below for the full range of data transmission speeds:

Data transmission speed (bps)	Range (m)
19200	1000
38400	900
57600	800
115200	500

Table 5.2: Range of data transmission speeds

The recommended wiring for RS-485 communication is 24-AWG Cat5e using 4-conductors, with unshielded twisted pair for indoor installations, and shielded twisted pair for outdoor installations.

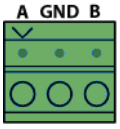


Figure 5.4: RS-485 Connector

The SE coordinator sends any received data from the SE receivers or SE transmitters to the Central Console Software via the Ethernet cable. The same Ethernet cable can also power the SE coordinator via Power over Ethernet (PoE) without needing an external DC input. The Ethernet connected is identified by the label PoE Ethernet on the SE coordinator. Connect the PoE using the standard Cat 5e Ethernet cable and above. PoE provides the maximum total power of 12.95 Watt to the SE coordinator, and complies with the IEEE802.3af class 0 standard.

Setting the loop address

Use the address dip switch ADDR to configure the RS-485 loop address of the SE receiver. Each SE coordinator/SE receiver on a loop must have its own unique address. Only addresses 0 through 15 are valid.

The SE coordinator always uses address 0. You do not need to set the address for the SE coordinator. Therefore, the dip switch ADDR is not available on the SE coordinator.

The SE receivers use addresses 1 to 15. Configure the four switches from the left, 1, 2, 3 and 4 of dip switch ADDR as the address of the device.

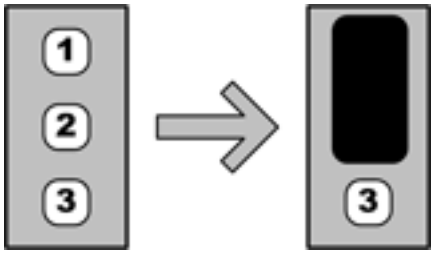
Address	Switch Number on Dip Switch ADDR			
	1	2	3	4
0 (used for coordinator only)	OFF	OFF	OFF	OFF
1 (default setting for receiver)	ON	OFF	OFF	OFF
2	OFF	ON	OFF	OFF
3	ON	ON	OFF	OFF
4	OFF	OFF	ON	OFF
5	ON	OFF	ON	OFF
6	OFF	ON	ON	OFF
7	ON	ON	ON	OFF
8	OFF	OFF	OFF	ON
9	ON	OFF	OFF	ON
10	OFF	ON	OFF	ON
11	ON	ON	OFF	ON
12	OFF	OFF	ON	ON
13	ON	OFF	ON	ON
14	OFF	ON	ON	ON
15	ON	ON	ON	ON

Table 5.3: Address settings on dip switch ADDR

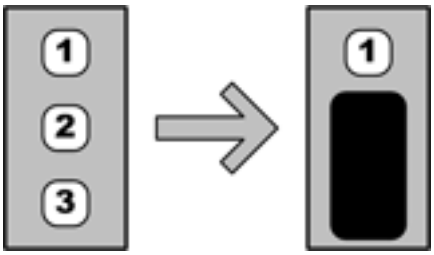
Setting the jumpers for RS-485

For RS-485 communication, it is necessary to include the end of line jumper settings on the last SE receiver to have a stable communication channel. Set the jumper for the SE coordinator and the SE receivers as of below:

1. For the SE coordinator and the last SE receiver only, locate the jumper block J5 and set the jumper over the jumper pins 1 and 2. This is the default factory setting on the SE coordinators/SE receivers.



2. For all SE receivers except the last SE receiver, locate the jumper block J5 and set the jumper over the jumper pins 2 and 3.



Testing SE receiver spacing

The spacing mode can be used to verify the maximum acceptable spacing of SE receivers. Enable or disable the spacing mode by setting switch number 1 on dip switch CFG2. Spacing mode is disabled by default, where switch number 1 is set to the OFF position. To enable the spacing mode, set switch number 1 on dip switch CFG2 to the ON position.

Enable/disable Spacing Mode	**Switch Number on Dip Switch CFG2**
	1
Disable Spacing Mode (default setting)	OFF
Enable Spacing Mode	ON

Table 5.4: Enable or disable the spacing mode on dip switch CFG2

To test the spacing of SE receivers:

1. Mount the first SE receiver (SE receiver 1). Set switch number 1 on dip switch CFG2 to the ON position. Power the SE receiver from a 24 VDC source.
2. Take the second SE receiver (SE receiver 2) and an SE transmitter a distance away from the first SE receiver.
3. Activate the SE transmitter.
4. If SE receiver 1 sounds the test beep, SE receiver 2 is within range. Repeat this test until SE receiver 1 no longer sounds the test beeps. Move back to the last location where SE receiver 1 received the test beeps. This location marks the maximum spacing between the SE receivers. The distance between the SE receivers should not exceed 25 m (80 ft.) indoors and 90 m (300 ft.) outdoors. Mount SE receiver 2 at this location or closer to SE receiver 1.

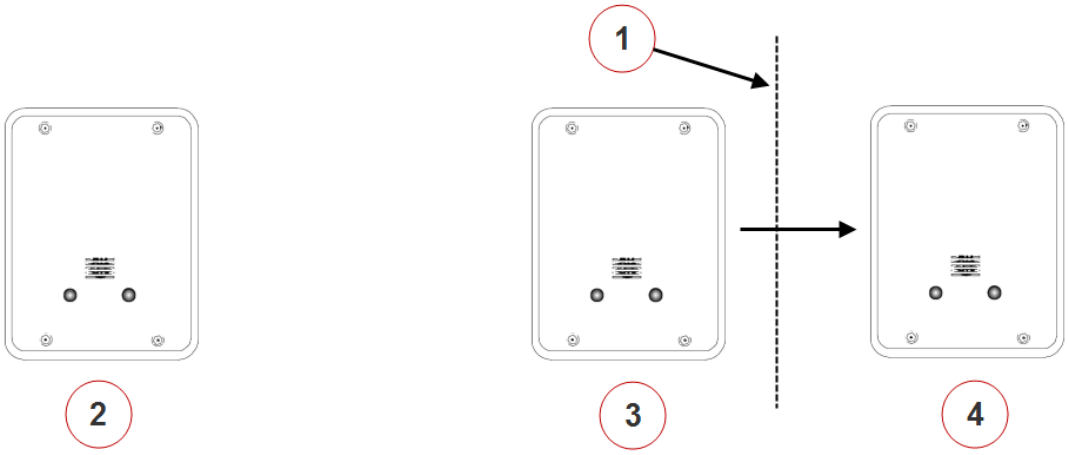


Figure 5.5: SE receiver Spacing

1	SE receiver 1 stops sounding the test beeps when SE receiver 2 is moved past this point	3	SE receiver 2 at maximum range
2	SE receiver 1	4	SE receiver 2 beyond maximum range

Pre-wired installations

When mounting the enclosure to a pre-wired electrical box, make sure that the electrical box has a 15.2 cm (6 in.) overhead clearance. The enclosure should be mounted as shown in figure below.

Notice!
The enclosure does not currently support octagonal electrical boxes.

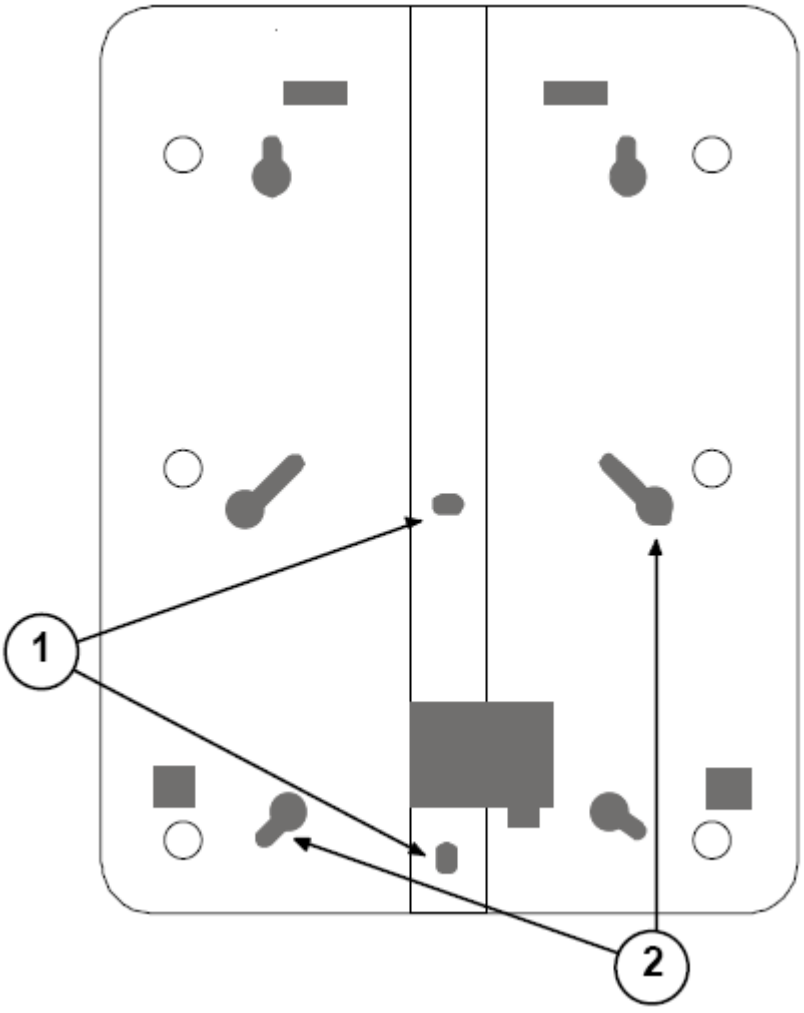


Figure 5.6: Back of indoor enclosure

1	Use with single-gang electrical boxes
2	Use with 8.9 cm (3½ in.) square electrical boxes

Drilling templates

Use the following templates for mounting the outdoor enclosure.

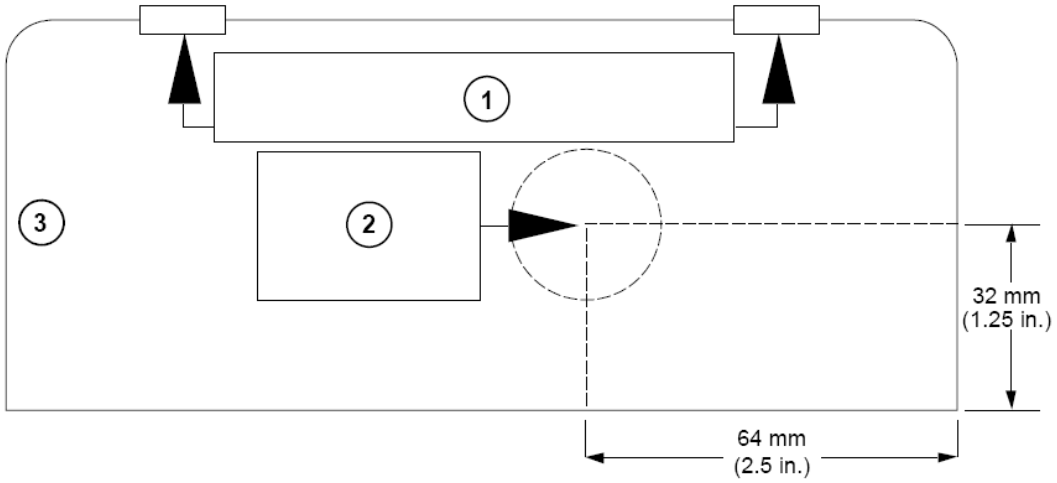


Figure 5.7: Drilling template bottom entry

1	Align template with mounting hole squares on box
2	Drill here, 25 mm (1 in.) diameter maximum; 19 mm (¾ in.) conduit.
3	Bottom entry

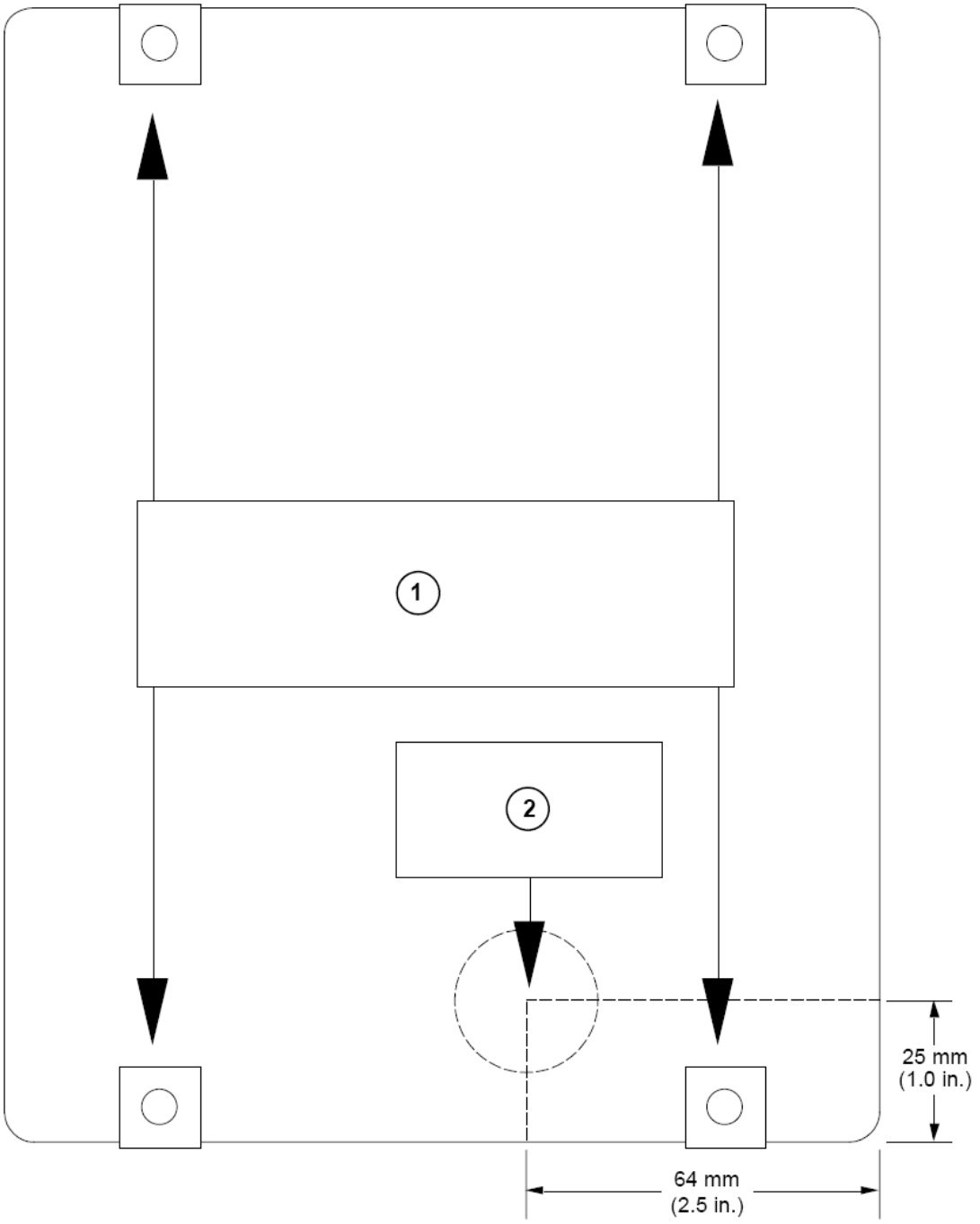


Figure 5.8: Drilling template rear entry

1	Align template with mounting holes on backside of box.
2	Drill here, 25 mm (1 in.) diameter maximum; 19 mm (¾ in.) conduit.

6 Installation options

6.1 Demo installations

When the software is used for demo purposes, there are limitations to the users and devices in the system. Users and devices are confined to these limits in the following table. If these limitations are observed, the system can be used with full functionality for demo purposes.

Components	Object	Limitations	Display in [About] dialog
Subscriber Database	Subscribers	30 records	30
Transponder Database	Transponders	1 record	1
	Receivers	Only any 24 receivers on Bus 0 to 2 are allowed	24
	SE coordinators	3 records	3
	SE receivers	Only 7 SE receivers from Points 1 to 7 of each SE coordinator are allowed	21
Workstations and Slave	Slave	1 computer	11
	Workstations	10 computers	

Table 6.5: Demo Limitations

In demo mode, communication is limited to 1 transponder and 3 SE coordinators even if the **Transponder Database** has more devices than above. All tests, supervisions and maintenance alarms will function normally; however only subscriber alarms from 24 receivers on bus 0 to 2 of the transponder, and 7 SE receivers from points 1 to 7 of each SE coordinator will function. If an alarm also includes other receivers or SE receivers, these alarms will be ignored. Therefore, actual Security Escort operations can be demonstrated using up to a total of 24 receivers on the transponder system and 21 SE receivers on the SE coordinator system.
A demo system can be used to directly connect to SE coordinators using the actual **Transponder Database** from the system to perform all functions except subscriber alarms. This is desirable to allow a laptop to be plugged directly into an SE coordinator to diagnose problems. In both of these modes the **Subscriber Database** must have 30 or less subscribers. Refer to *Installing the Security Escort software, page 48* section for the installation procedure. After the software has been installed, the demo installation is complete at this point and you do not have to refer to the rest of this document.

6.2 Non-network installations

If this system is not using the network to connect master, slave and workstation computers, refer to *Installing the Security Escort software, page 48* section to install the software. After the software has been installed, plug the software key into the USB port on the computer. A non-network installation is complete at this point and you do not have to refer to the rest of this document.

6.3 Network installations

The Security Escort software supports a single master computer, a single slave computer (optional) and a maximum of eight workstations. The master computer normally processes the real time communications to the SE coordinators and controls the system. The slave computer can assume the master's role by switching the SE coordinator communications to the slave computer.
This system redundancy feature is explained in further detail in *System redundancy, page 165* section.
The workstation computers allow other computers to respond to alarms, perform maintenance and edit the databases.

6.4 Installing the Security Escort software

6.4.1 Software installation procedure

Typically, the Security Escort program is delivered on a CD-ROM.

Notice!
Exit all other programs before inserting the CD-ROM.

An "autorun" feature should automatically start the installation program. If not, run SETUP.EXE using one of the following methods:

1. Double click the **Computer** icon on the desktop. Select the Compact Disc (X:), double-click the INSTALLER directory. Double-click the SETUP.EXE icon. X is the letter of the CD-ROM drive.
2. Go to **Start** > **Programs** > **Windows Explorer**. In Windows Explorer, select the Compact Disc (X:) and double-click the INSTALLER directory. Double-click the SETUP.EXE icon.
3. Click **Start** > **Run.** Type "X:\INSTALLER\SETUP.EXE" in the **Open** textbox and click the **[OK]** button. X is the drive letter for the CD-ROM drive.

Once SETUP.EXE is running, the following **Welcome** dialog appears.

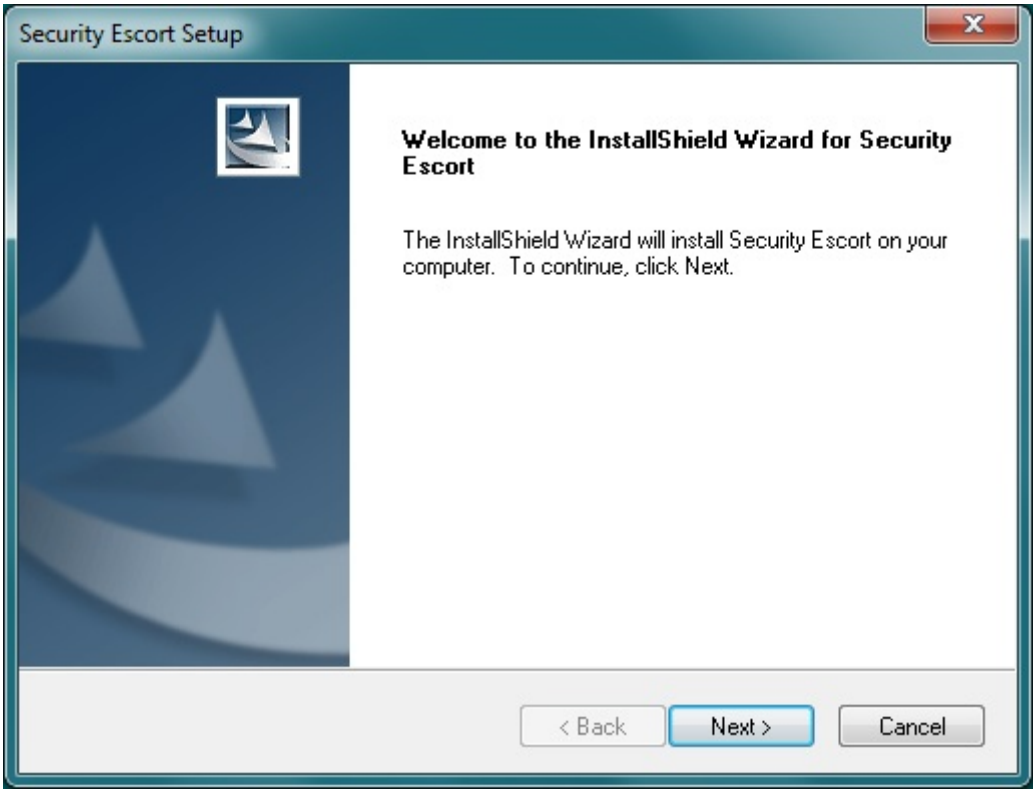


Figure 6.1: Security Escort Setup Welcome Dialog

You can click the **[Cancel]** button at any stage of installation to abort installation. The **Exit Setup** dialog will appear. Click the **[Yes]** button to abort installation.

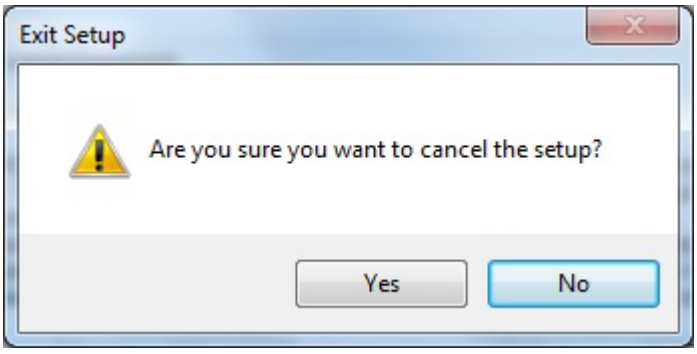


Figure 6.2: Exit Setup Dialog

Otherwise, click the **[Next >]** button. The **License Agreement** dialog appears.

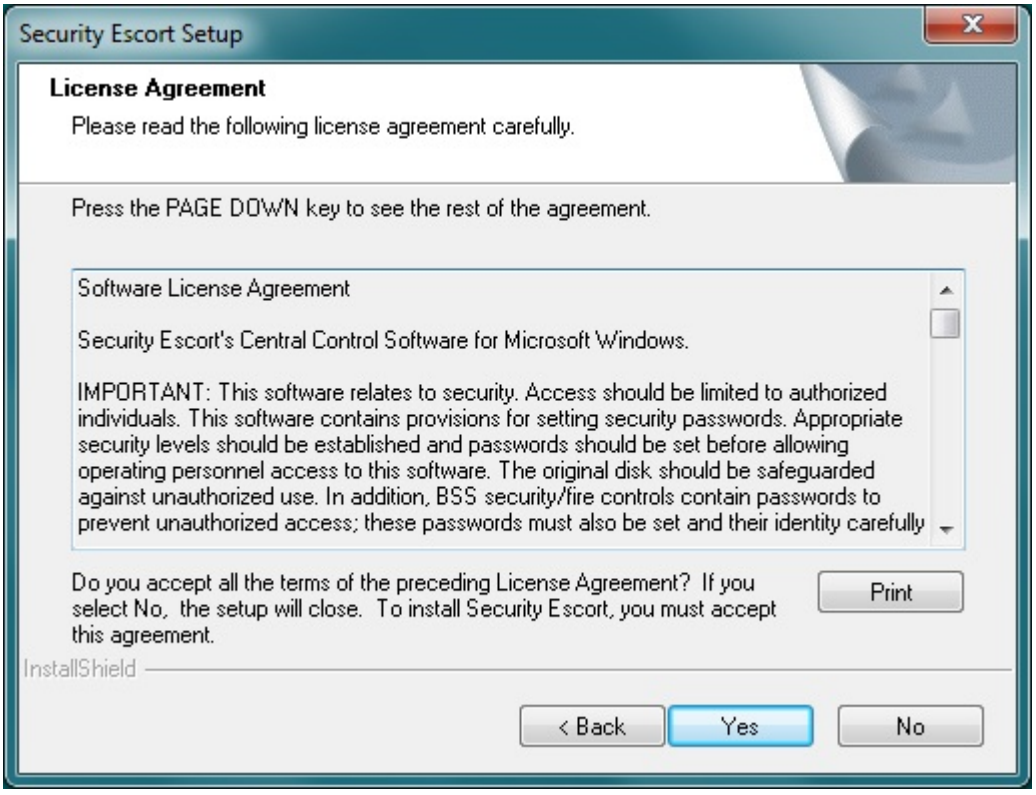


Figure 6.3: License Agreement Dialog

Click the **[Yes]** button to accept the License Agreement. The **Readme Information** dialog appears.

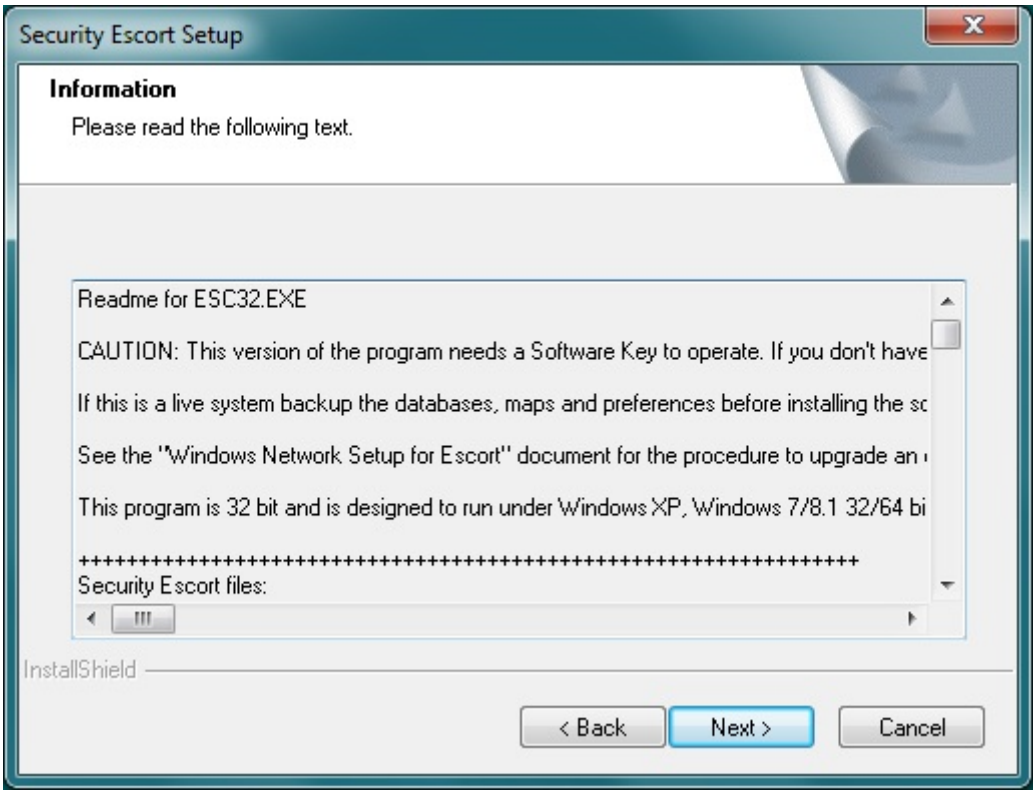


Figure 6.4: Readme Information Dialog

Read the entire file before proceeding (use the scroll bar on the right side to see the portion not currently displayed). Once done, click the **[Next >]** button. The **Choose Destination Location** dialog appears. Select the location on the hard disk drive to install the Security Escort program. Typically, the default location (“C:\ESCORT”) would be ideal.

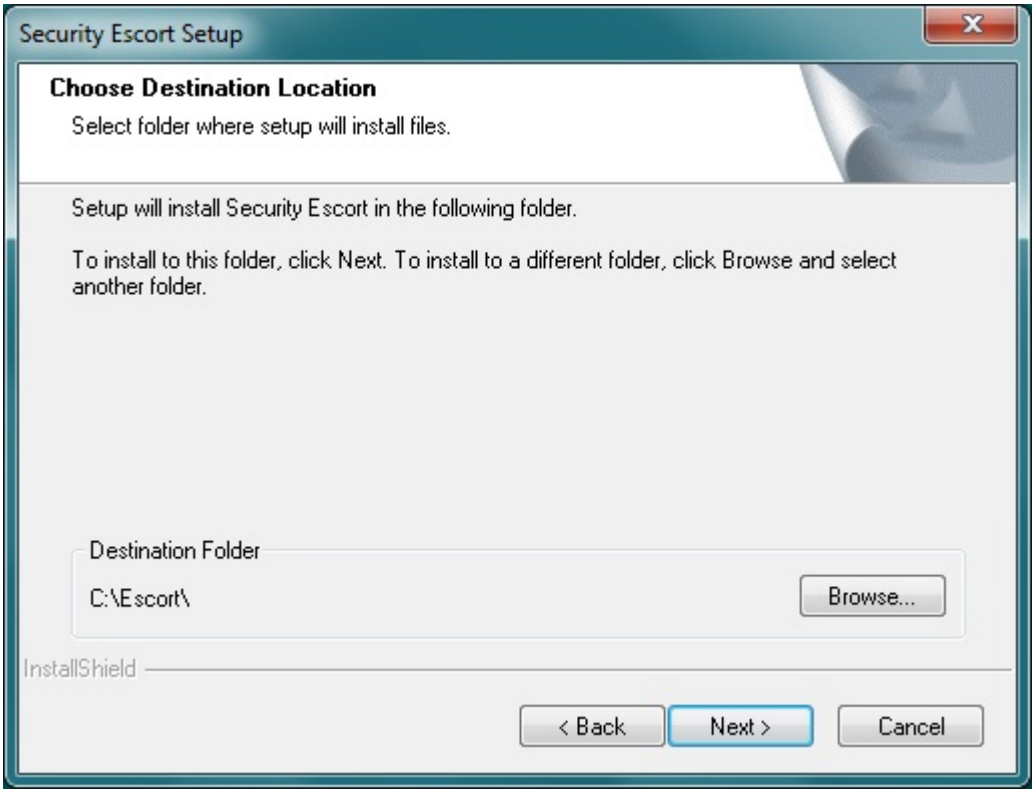


Figure 6.5: Choose Destination Location Dialog

If you wish to install the program in a different location, click the **[Browse]** button and the **Choose Folder** dialog appears. Select the desired folder and click the **[OK]** button. You will return to the **Choose Destination Folder** dialog.

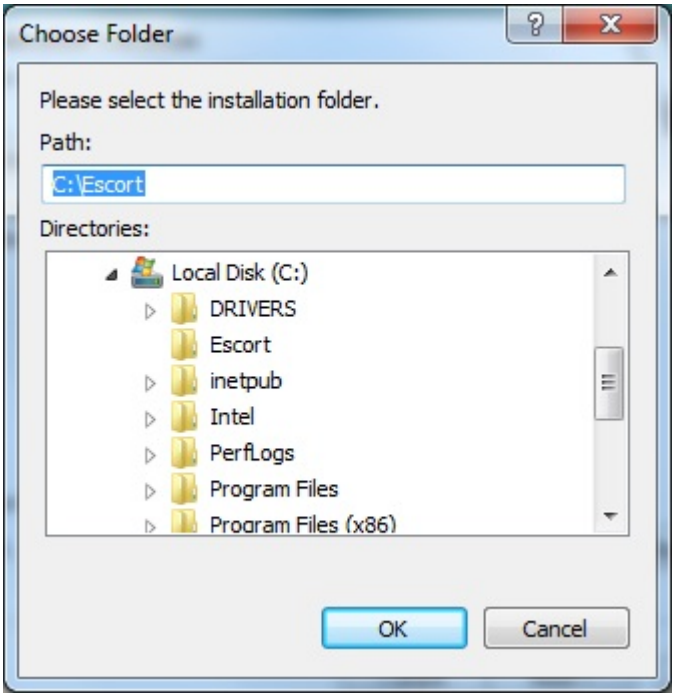


Figure 6.6: Choose Folder Dialog

Click the **[Next >]** button on the **Choose Destination Folder** dialog. The **Setup Type** dialog appears.

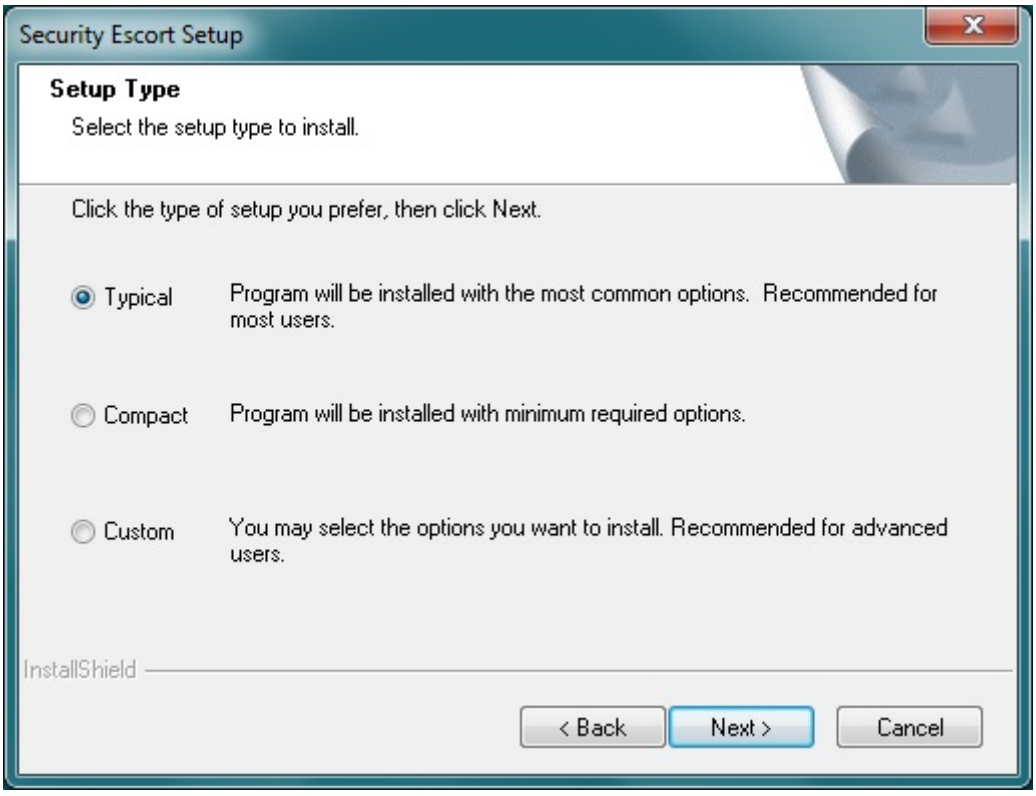


Figure 6.7: Setup Type Dialog

Select the type of installation you desire.

- **Typical** - For new installations, this is the option you should choose. It guarantees that all required components are installed and includes the installer for the software key. Use this selection for demo installations. Do not use this selection on existing installations; it replaces the databases and maps with the demo databases and maps.
- **Compact** - Only installs the application files. This selection can be used to update an existing installation. It does not write over the databases and map files. This selection cannot be used for new installations because it does not contain all required components, the installer for the software key, databases, and maps.
- **Custom** - This selection contains all systems components, databases, and maps. You may choose which to install.

Click the **[Next >]** button. The **Select Program Folder** dialog appears for you to place the Security Escort shortcuts in the selected program folder.

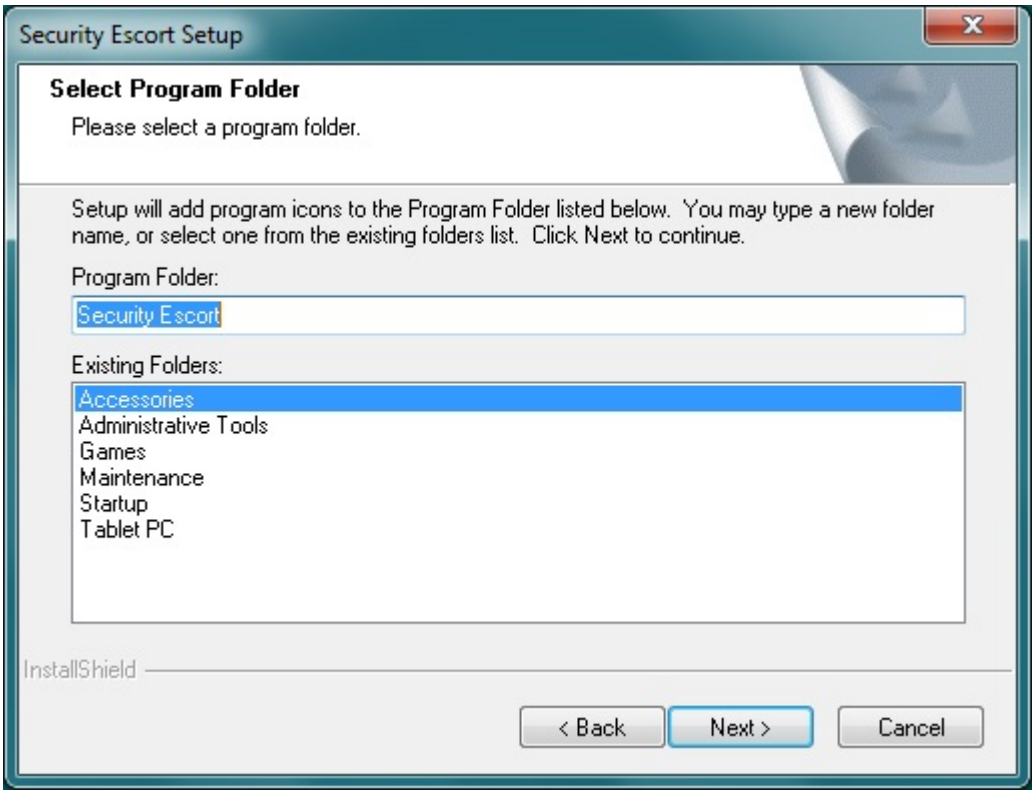


Figure 6.8: Select Program Folder Dialog

We are set to install the program. Click the **[Next >]** button. The installation starts, displaying the progress status.

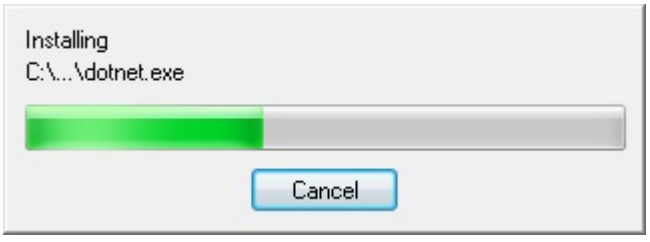


Figure 6.9: Installation Progress Dialog

Once installation has completed, the **Installation Complete** dialog appears, Click the **[Finish]** button to finish the installation.

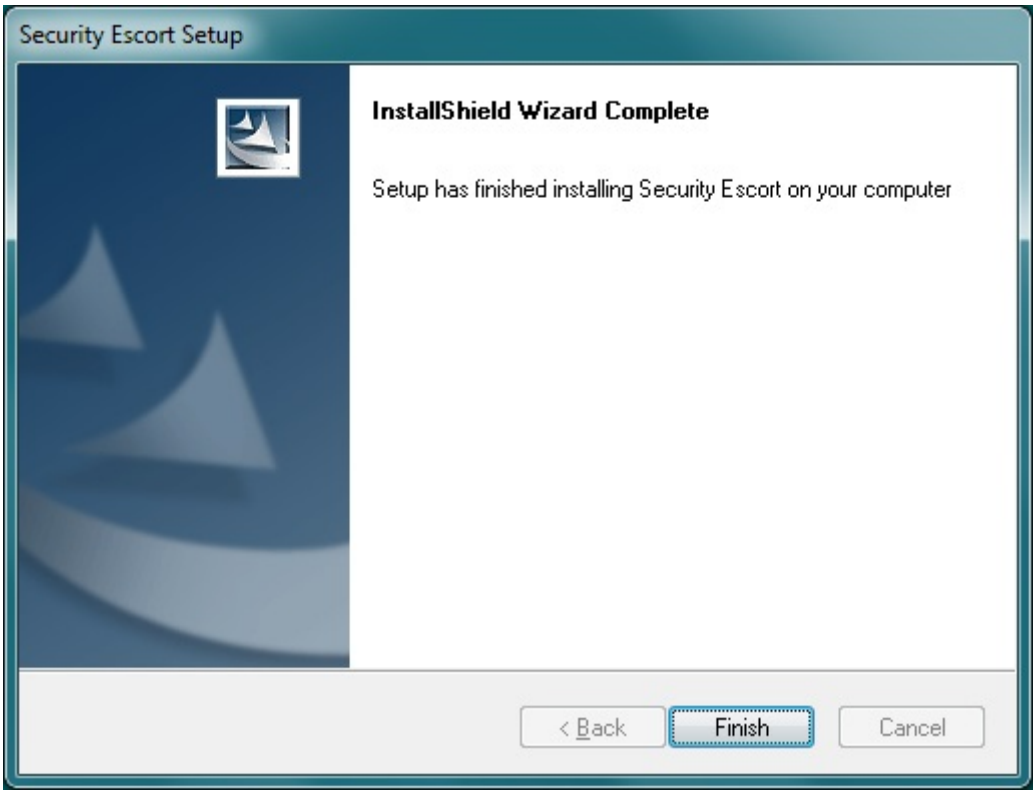


Figure 6.10: Installation Complete Dialog

To manually start the Security Escort program after installation, go to **Start > Programs > Security Escort**. In a live system, it is recommended that the Security Escort program be configured to automatically start. To auto start the program, place a shortcut to ESC32.EXE (the Security Escort program, typically located in “C:\ESCORT”) in the following path: **C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\Security Escort**

Turning on Microsoft .NET Framework feature

After installing the Security Escort software, you need to turn on the .NET feature in order for the software to work. Go to **Start > Control Panel > Programs and Features**.

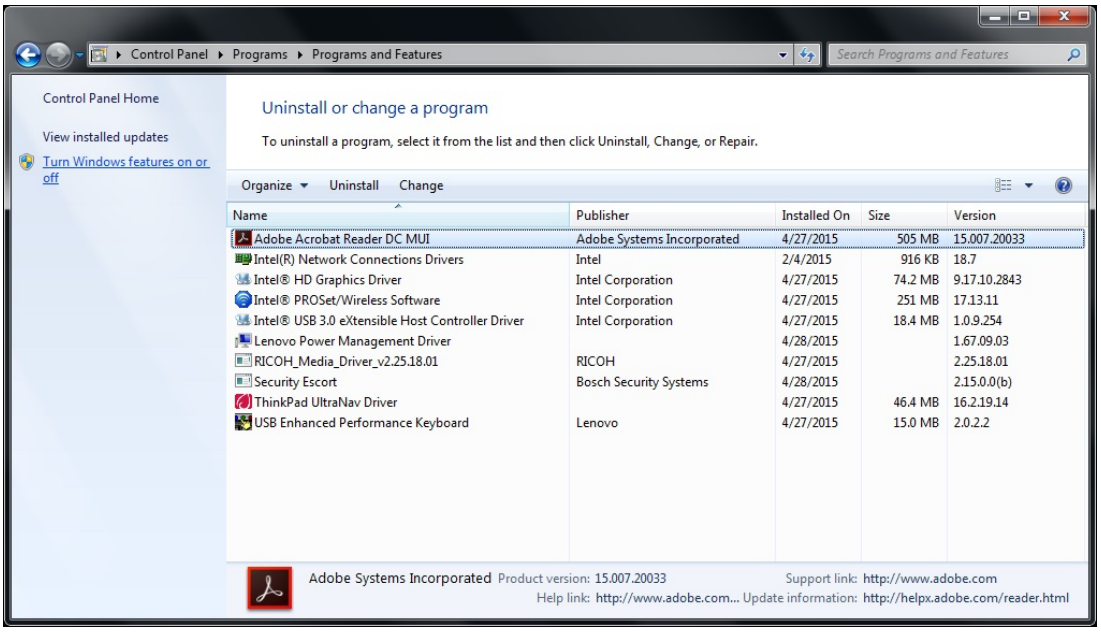


Figure 6.11: Control Panel

Click the **Turn Windows features on or off** link on the left of the window. The **Windows Features** dialog appears. Look for the **Microsoft .NET Framework 3.5.1** entry and ensure that the related checkboxes are selected.

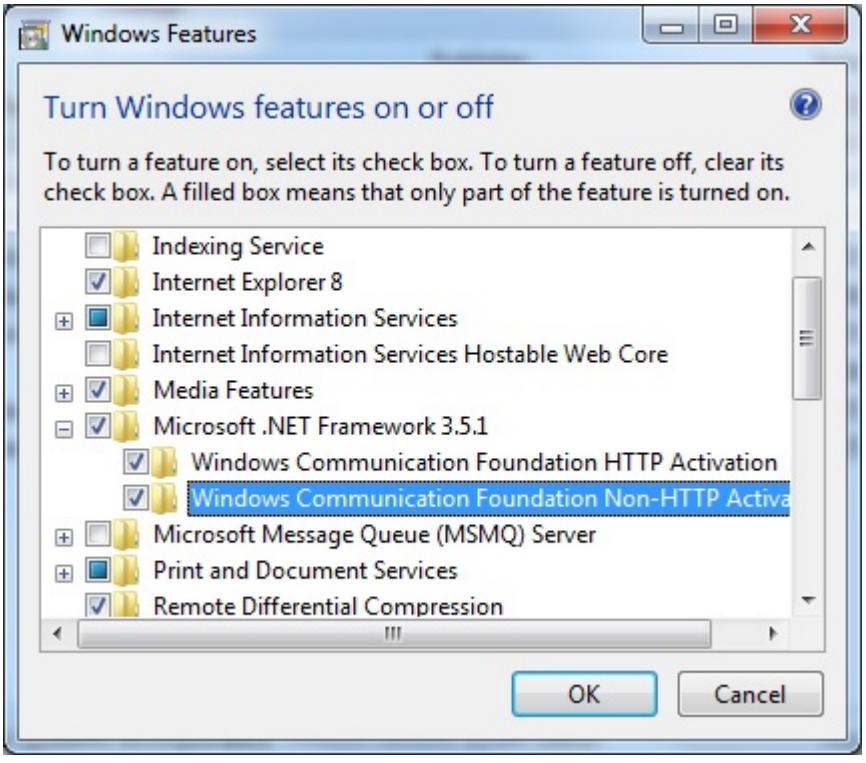


Figure 6.12: Windows Features Dialog

Click the **[OK]** button to turn on the Microsoft .NET Framework feature.

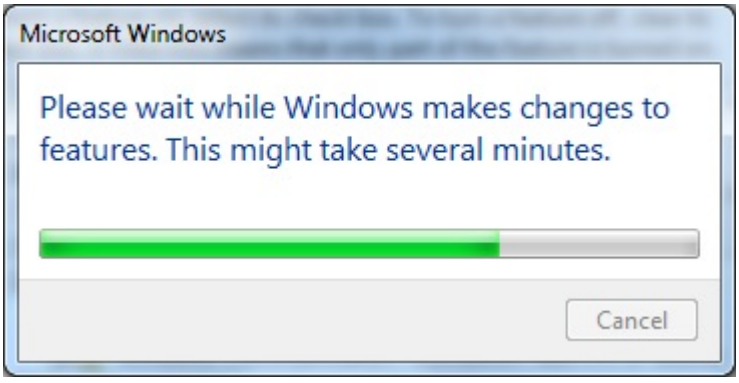


Figure 6.13: Change Progress Dialog

6.4.2 Initial login

When you first start the **Security Escort** software, you will be prompted to login to the system.

Figure 6.14: Login dialog box

The default operator ID is 4 and password is PPP.

Enter the operator ID, password and click **OK**. A dialog box appears where you are prompted to change this default password.

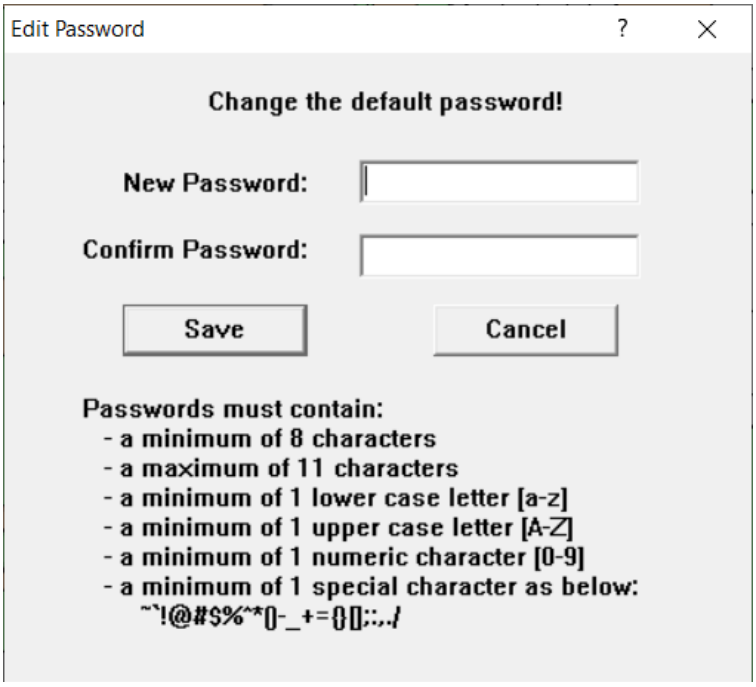


Figure 6.15: Change password dialog box

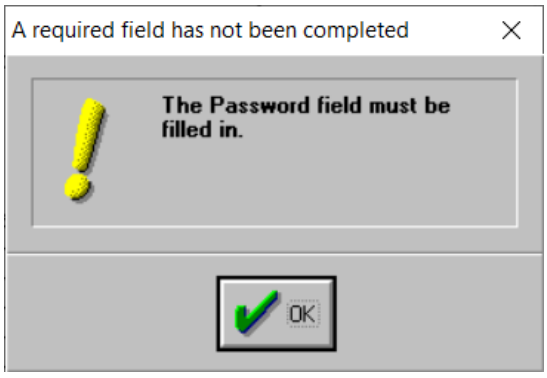
Follow the instructions accordingly to change the password. If you do not change the default password, you will not have access to the **Security Escort** software.

To change the default password:

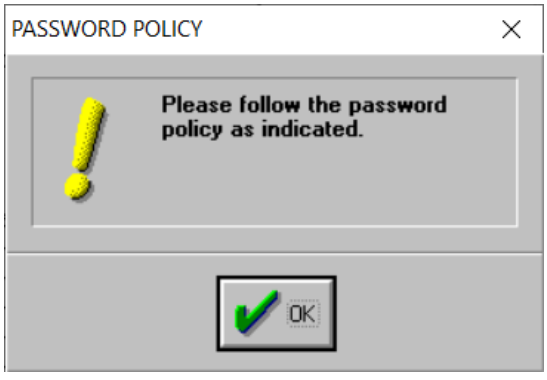
1. Enter the new password in the **New Password** text field.
2. Enter the same new password in the **Confirm Password** text field.
3. Click the **Cancel** command button to abort changing the password at any time. You will return to the login dialog box.
4. Click the **Save** command button once you have entered the **New Password** and **Confirm Password** text fields.
5. If the **New Password** and **Confirm Password** text fields match, the password has been changed successfully. You will return to the login dialog box where you can enter the operator ID and the new password to login.
6. If the **New Password** and **Confirm Password** fields do not match, a warning dialog box will appear. You will need to reenter the **New Password** and/or **Confirm Password** text fields.

Warning dialog boxes that you may encounter:

1. The following warning dialog box appears if you click the **Save** command button without entering the **New Password** text field.



2. The following warning dialog box appears if you click the **Save** command button and the **New Password** and/or **Confirm Password** text fields do not follow the password policy.



3. The following warning dialog box appears if you click the **Save** command button, and:
   - the **New Password** and **Confirm Password** text fields do not match, or
   - the **New Password** and/or **Confirm Password** text fields match but do not meet the minimum required characters.

For all these warning dialog boxes, click the **OK** command button to return to the change password dialog box.

6.4.3 Image files

Map file generation and scaling

The Security Escort maps are standard Windows bitmap files (.BMP). MAP0.EDB is the default map file, usually the ground floor in multiple map systems. The map must be saved in the Security Escort subdirectory (typically “C:\ESCORT”). These maps may be created from scratch using any Windows paint program, however it is best to scan in an existing site map. Commercial copy centers usually have scanners that can handle larger drawing sizes.
If an AutoCAD file is available, have AutoCAD export a bitmap for the best looking maps that require the least work to make presentable. If the scale of the exported map is too large or too small, re-export the map at the corrected scale rather than scaling the map in a graphic editor. Scaling a bitmap file directly will produce a file that will require a significant amount of manual effort to make presentable.
Save the scanned image as a Windows bitmap file (.BMP) with True Color (32 bit), but the file sizes will be much larger and the maps will be slower to load and may require more system RAM. It should be scaled so that the entire map file is at least 1024 by 768 pixels (covering the entire Windows screen). The Security Escort software auto scrolls the map; therefore it is not a problem if the map is larger than the screen. The map should not be too large. There should be enough area of the map on the screen when an alarm is shown, so there is no question where in the facility the alarm is located from a quick review of the map. A good rule-of-thumb is 100 pixels would represent 15 m (50 ft) or greater.

Multiple map files

For a multi-story building, the maps for each floor must have the same resolution. Each map must be vertically aligned with all the floors above and below it. Therefore the maps will have the same origin (0,0 = upper left corner). Typically, you would do the map for the ground floor, and then make the maps for the other floors by editing copies of the ground floor map.
Where the coordinators from multiple systems are reporting into the same computer, the map(s) for each system is separate and assigned unique map numbers, from the other maps on that same computer. The origin for the maps for each system is 0,0 = upper left corner. Therefore, the location of the receivers in the **Transponder Database** will only consider this system’s map without respect to the maps for any other systems being handled by the same computer.
The maps must be named MAP0.EDB, MAP1.EDB through MAP99.EDB, where MAP0.EDB is the default map file, usually the ground floor. The Security Escort software shows the default map if there are no other events being processed at a given time.
Assign the desired map number to an area or point in the **Transponder Database**. Assign the map for a fixed location transmitter by clicking the **[Advanced]** button when inserting a new or editing an existing record of the **Subscriber Database**.

Subscriber images

The images must be saved individually in JPG format. Please refer to *Subscriber images, page 128* for details on how to set the images in the **Subscriber Database**.

7 Central Console, computer setup and programming

7.1 Initial system configuration

The following is applicable upon initial login only. You will be asked to change to a new password after logging in for the first time. If you do not change this default password, you will not be able to access the **Security Escort** software.
The Master password, and other passwords for all system operators should be changed as well after gaining access to the **Security Escort** software.

- To change password after initial login, refer to *Initial login, page 57*.
- To generate the map file for the screen display, refer to *Image files, page 60*.
- To setup the system COMM ports, refer to *Remote comm port setup, page 61*.
- To set the function of the system COMM ports and setup remote access, see *Remote setup, page 63*.
- To program the system configuration, see *Transponder Database, page 66*.
- To program the system responses to an alarm, see *System Preferences, page 108*.
- To program the system responses to troubles, see *Popup trouble filter, page 187*.
- If this system has master and slave computers, set the Default Master Computer and Default Slave Computer. refer to *Remote setup, page 63*.
- If using pager access in this system, see *Pager setup, page 212*.
- If this computer runs other programs at the same time, Security Escort is running, set the **Not Always Top Window** field (see *Security Preferences, page 114*).
- To program the ID receiver to automatically enter the transmitter IDs, see *Security Preferences, page 114*.
- To set the names of the subscriber classes, see **System Default** dialog in the Security Escort Operations Guide.
- To program the transmitters into the **Subscriber Database**, refer to the Security Escort Operations Guide.

7.2 Remote comm port setup

This dialog connects the network, modem and system serial ports to the physical communication ports on the computer and sets their baud rate.

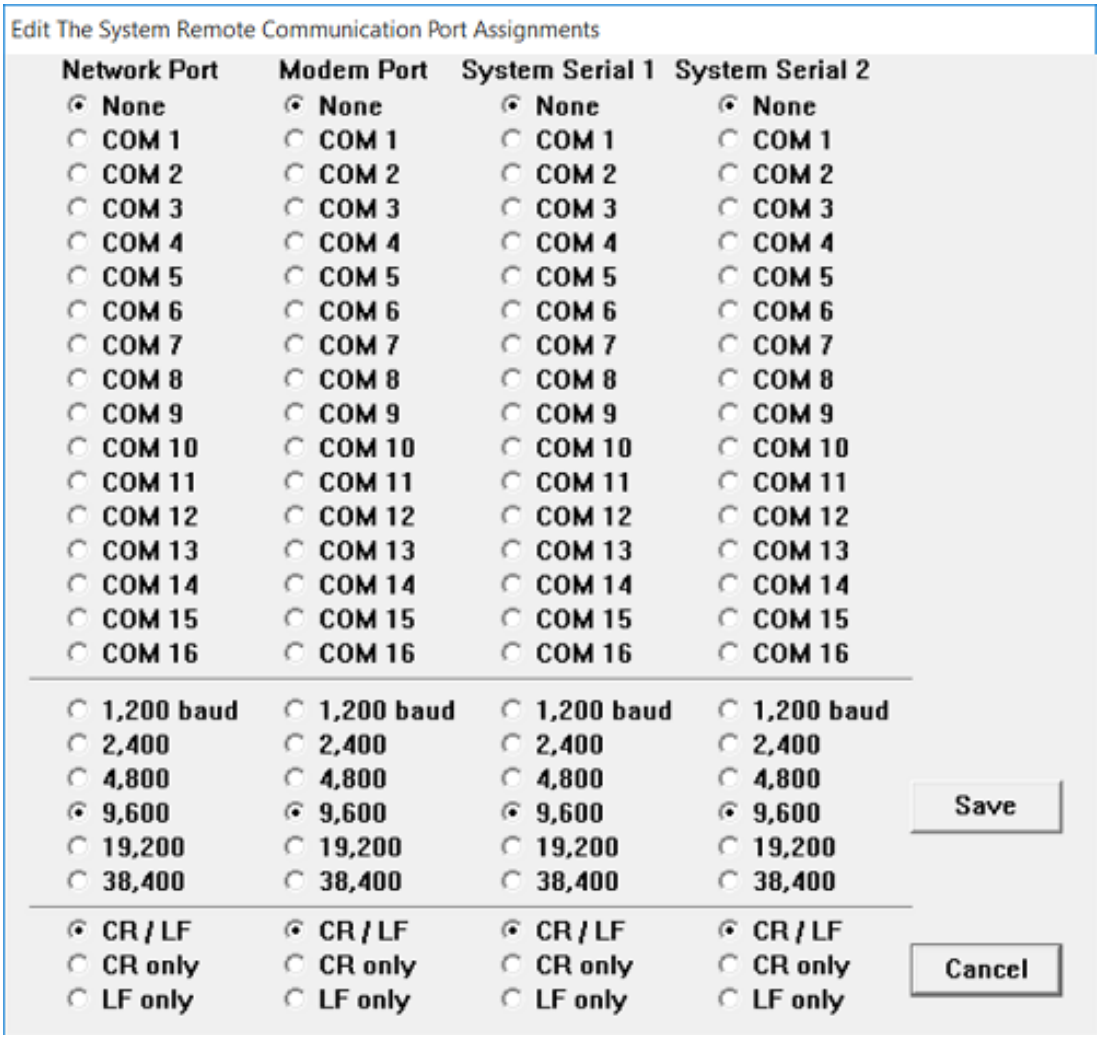


Figure 7.1: Remote comm port setup dialog

Element	Usage/Description
Network Port	This port connects the master and slave computers of the Security Escort System. If this system has only a single computer, this setting should be set to none.
Modem Port	This port typically connects to the modem for remote access and pager dial out. If set in the **Remote setup** dialog, use this port without a modem for direct connection to a computer that is always on line.
System Serial 1/2	This is a general-purpose serial port. Its function is set up in the **Remote setup** dialog.
COM	The actual physical communication port over which these communications are carried.
Baud	The speed at which characters are transmitted on this serial port. This setting must match the baud rate of the device connected at the other end of this serial connection. This setting should always be at the highest speed that both connected devices have in

Element	Usage/Description
	common. Modem connections are typically much more efficient, if the baud rate is set significantly faster than the modems rated speed (for a 28.8 modem, set the baud rate to 57600 or 115200). The default setting is 9600 baud.
CR/LF	Appends carriage return and line feed characters at the end of each string transmitted (default). Only functions with the system serial ports (ignored on the network and modem ports).
CR Only	Appends a carriage return character at the end of each string transmitted. Only functions with the system serial ports (ignored on the network and modem ports).
LF Only	Appends a line feed character at the end of each string transmitted. Only functions with the system serial ports (ignored on the network and modem ports).

7.3 Remote setup

This dialog sets up the remote access and system serial port parameters.

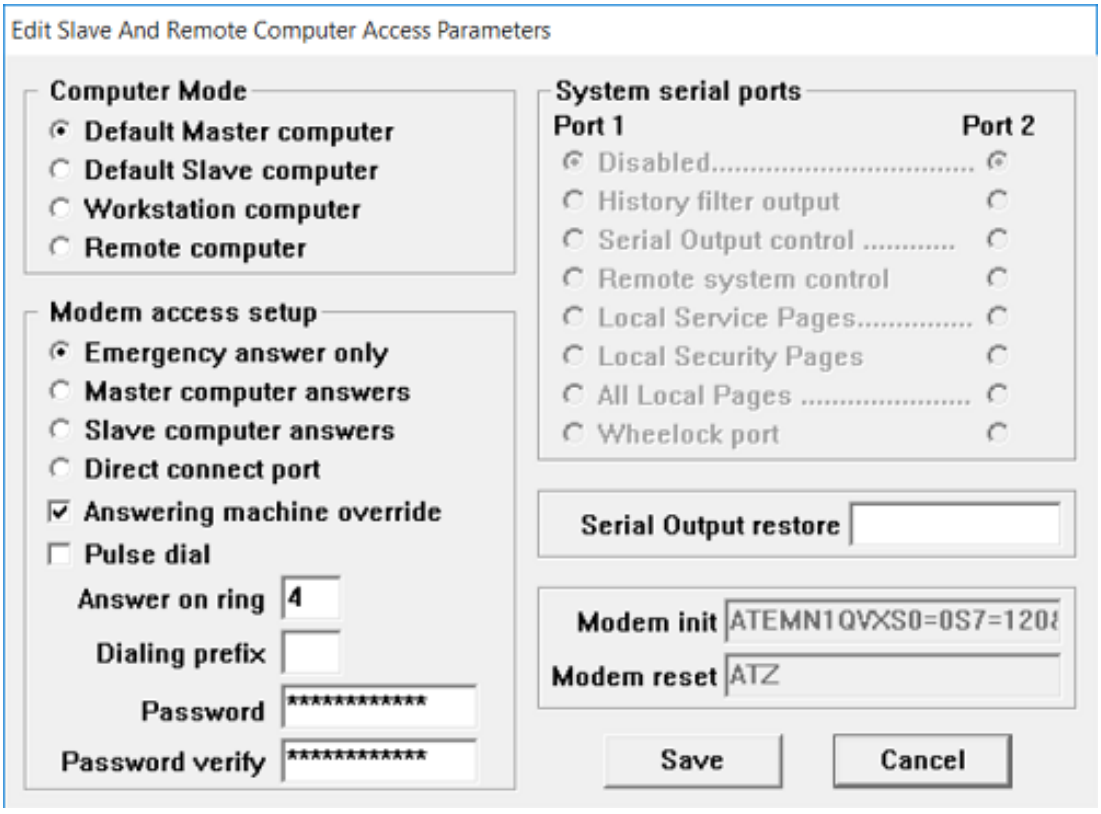


Figure 7.2: Remote setup dialog

Element	Usage/Description
Computer Mode group	
Default Master computer	This computer is either the only computer in the system, or on startup, this computer defaults to the Master computer in a live Security Escort System.
Default Slave computer	On startup, this computer defaults to the slave computer in a live Security Escort System.
Workstation computer	This computer is used in a live Security Escort System for all operator functions. It cannot control the system like the Master and Slave computers.
Remote computer	This computer is not in a live Security Escort System. It is used only for remote access. For this setting to be enabled, all transponder communication ports and the network port must be set to “None”.
Modem access setup group	
Emergency answer only	Allows the Master computer to answer a remote access only after 10 rings. If the Master does not answer, the Slave answers after 12 rings.
Master computer answers	Allows the Master computer to answer a remote access after the programmed number of rings. If the Master does not answer, the Slave will answer after the programmed number of rings plus 2.
Slave computer answers	Allows the Slave computer to answer a remote access after the programmed number of rings. If the Slave does not answer, the Master answers after the programmed number of rings plus 2. Generally, it is better to have the Master computer answer remote access calls.
Direct connect port	The modem port is not connected to a modem. This setting will allow a direct connection to another computer. This additional computer will not display alarms, but otherwise will behave like a Slave computer.
Answering machine override	If checked, an answering machine is connected to this phone line. If the answering machine answers a remote access call, hang up and redial. When another call is received within 1 min. of the last ring of a previous call, the Security Escort System will answer on the first ring, overriding the answering machine.
Pulse dial	If checked, use pulse dial on all outgoing calls. Otherwise, tone dialing (default) is used.
Answer on ring	Program the number of rings on which to answer. If there is an answering machine on this phone line, set the number of rings to at least 2 greater than the number of rings the answering machine answers. Also check the **Answering Machine Override** checkbox.
Dialing prefix	On outgoing calls, enter the dialing prefix, if any.

Element	Usage/Description
Password	This is the password that is used to gain remote access to the Security Escort System. If the first 5 characters of the password match the remote systems password, read only access will be allowed. If the first 8 characters match, you will be allowed to edit databases remotely (not currently implemented). If all 12 characters match, you will also be allowed to change system parameters remotely.
System serial ports group	
Password verify	For verification, reenter the same password as above.
Disabled	If selected, this system serial port is disabled (default).
History filter output	If selected, this system serial port sends out whatever items that are selected in the **History Filter** dialog.
Serial Output control	If selected, this system serial port sends out the strings programmed in the **Serial Output** field of the **Transponder Database Edit** dialog's **Area** data. Also see **Serial Output restore** field below.
Remote system control	If selected, this system is controlled by another system through a proprietary protocol. This setting can only be used when two systems are specifically designed to work together.
Local Service Pages	If selected, system will send service pages via the local port.
Local Security Pages	If selected, system will send security pages via the local port.
All Local Pages	If selected, system will send both service and security pages via the local port.
Wheelock port	If selected, system will send both service and security pages via the local port.
Others	
Serial Output restore	This string is transmitted on any system serial port programmed for **Serial Output control** when the alarm is cleared. This string is transmitted to the serial output to reset it to default. Up to 60 characters can be entered. Control characters can be entered as [^][A] for control A.
Modem init	This is the initialization string transmitted to the modem to set it up for all communications except paging. Normally, this setting does not need to change. To allow changes to this string, hold down the <Shift> + <Ctrl> keys when this dialog is first opened. This string is specific to each modem model. The default string should work with most modems.

Element	Usage/Description
Modem reset	This is the reset string transmitted to the modem. Normally, this setting does not need to change. To allow changes to this string, hold down the <Shift>+ <Ctrl> keys when this dialog is first opened. This string is specific to each modem model. The default string should work with most modems.
[Save]	Save the changes and close the dialog window.
[Cancel]	Cancel the changes and close the dialog window..

7.4 Transponder Database

The **Transponder Database** is established at system set-up and contains all necessary configuration data for each SE coordinator and SE receiver. It describes the basic structure of the installation, including all device names, locations, types, addresses, etc. This information is used by the Central Console to generate “Alarm” and “Test” displays on the console.
Start by filling out the setup of the SE coordinator and its SE receivers in the information sheet. Based on the information sheet, key in all the configuration details accordingly into the database using the **Transponder Database** dialog.

7.5 SE coordinator information sheet

SE coordinator ID:		**SE coordinator Location:**	
Transformer for SE coordinator Location:			
Breaker Panel Location:		**Breaker Number:**	
Siren/Strobe Output To:			
SE receiver Locations:			
Point #1:			
Point #2:			
Point #3:			
Point #4:			
Point #5:			
Point #6:			
Point #7:			
Point #8:			
Point #9:			
Point #10:			
Point #11:			
Point #12:			
Point #13:			
Point #14:			
Point #15:			
Location of Splices:			

7.6 Transponder Database dialog

From the **File** menu, select the **Transponder Database** menu item. This dialog allows you to check and enter all the configuration details of the SE coordinators and their corresponding SE receivers.

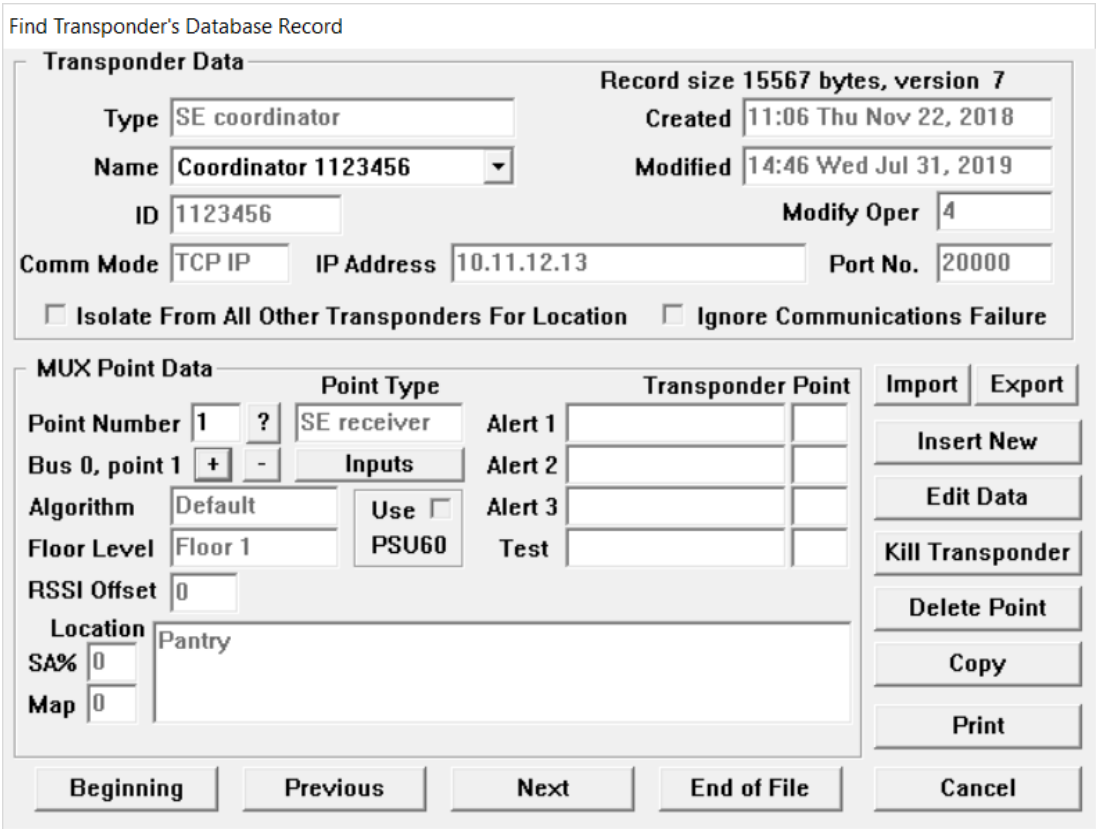


Figure 7.3: Find Transponder's Database Record dialog

Depending on the type of transponder record (transponder or SE coordinator), the elements of the screen may differ. The following table, applicable to SE coordinator only, describes the elements of the **Find Transponder's Database Record** dialog.

Element	Usage/Description
Type	This field indicates the type of transponder record that you are currently viewing. Currently, there are two types of transponders: transponder and SE coordinator.
Name	This drop-down list contains the names of the transponder record. Selecting the name of the SE coordinator in the drop-down list displays information of the SE coordinator record in the dialog window. The SE coordinator names are assigned during set-up and are used to indicate the physical location of the SE coordinator, or the region of the protected area covered by a particular SE coordinator.
Created **Modified** **Modify Oper**	The system software automatically creates these 3 fields to the right of the **Find Transponder's Database Record** window. They represent the date the SE coordinator was first entered into the

Element	Usage/Description
	Transponder Database, the date of the last change of any entry for this SE coordinator, and the identity of the operator making the last change.
ID	This is a number assigned to the SE coordinator at system set-up. It is the Radio ID found on the product label of the SE coordinator circuit board. This **ID** is used by the Central Console to identify the SE coordinator during all communications between the Central Console and the SE coordinator.
Comm Mode	This is the communication mode between the Central Console and the SE coordinator. Only TCP IP mode is applicable for SE coordinators.
IP Address	This field indicates the IP address assigned to the SE coordinator.
Port No.	This is the communications port that is used by the Central Console to communicate with the SE coordinator.
Isolate From All Other Transponders For Location	If this checkbox is selected, this SE coordinator is isolated from all other SE coordinators for location considerations. This should be used when distant SE coordinators sometimes hear an alarm and throw off the alarm location calculation. If this checkbox is selected, it indicates that this SE coordinator is protecting an area that is independent of all other SE coordinators in the system. When an alarm is reported, and the SE receivers on this SE coordinator have the best reception, only the SE receivers on this SE coordinator will be considered for the location of this alarm. If another SE coordinator has the best reception, then the SE receivers on this SE coordinator will be ignored for the location of this alarm.
Ignore Communications Failure	If this checkbox is selected, communication failures will be ignored for this SE coordinator. It is used during a new installation of SE coordinators that are not yet fully on line. During system maintenance, when an SE coordinator is out of service for a while, it is used so that the communication failure messages will not flash on the screen and distract the operator. **Selecting this checkbox causes the system to ignore communication failure. Therefore, if communication fails with this SE coordinator, the area that this SE coordinator protects will not be protected, and alarms from subscribers in that area will be missed without the operator's knowledge. This checkbox should not be selected in a live system.**
[Import]	Click this button to import the set of predefined **Transponder Database** information in XML file format into the **Transponder Database**.
[Export]	Click this button to export the **Transponder Database** information into a set of predefined XML file format.

Element	Usage/Description
[Insert New]	Click this button to enter a new SE coordinator to the database. The **Edit Transponder's Database Record** dialog window will appear.
[Edit Data]	Click this button to modify information of the current SE coordinator record.
[Kill Transponder]	Click this button to delete the current SE coordinator record. If the SE coordinator is "killed", its data is permanently deleted and cannot be recovered.
[Delete Point]	Click this button to delete the current point number from the current SE coordinator record. If the point is deleted, its data is permanently deleted and cannot be recovered. **Note: This button is not available for point number 0 of the current SE coordinator record. Point number 0 refers to the built-in SE receiver of the current SE coordinator, therefore it cannot be deleted.**
[Copy]	Click this button to copy the current SE coordinator record into a new SE coordinator record. This allows similarly configured SE coordinators to be copied into a new record. **Note: It is not possible to edit the SE coordinator ID itself. If this should be necessary, the [Copy] button can be used to produce another Transponder Database entry duplicating the first, but with the SE coordinator ID blank. The new SE coordinator ID can be entered, the new data saved by using the [Save] button, and the old SE coordinator entry can be deleted using the [Kill Transponder] button.**
[Print]	Click this button to print the current SE coordinator record in the database.
[Cancel]	Click this button to close the dialog window.
[Beginning]	Click this button to display the first SE coordinator record in the database.
[Previous]	Click this button to display the previous SE coordinator record in the database.
[Next]	Click this button to display the next SE coordinator record in the database.
[End of File]	Click this button to display the last SE coordinator record in the database.

7.6.1 MUX Point Data

The lower section of the **Find Transponder's Database Record** dialog provides information on the devices controlled by the selected SE coordinator record.
Two digits represent each SE receiver. The first digit is the bus on which the device is mounted. The bus is always 0 as all devices (SE receivers) are mounted on the same communication bus. The second digit is the point address assigned to the specific device. On

the bus, up to 15 devices may be installed, but each SE receiver device must be assigned a unique point address (1 to 15). This address is assigned by setting the dip switches on the SE receivers. The SE coordinator or its built-in SE receiver always use the point address 0.
These point address settings are also a part of the **Transponder Database**. The address shown in the **Transponder Database** and the address set on the device circuit board must be the same.

Notice!
It is a good idea to create an entry in the **Transponder Database** for each SE coordinator in the system before entering the data for each device, so that all SE coordinators appear in the drop-down menus.

7.7 Creating a new SE coordinator record

Creating and modifying the **Transponder Database** requires special authority levels usually assigned only to the installing company's personnel. Click the **[Insert New]** button to open the **Edit Transponder's Database Record** dialog window.
The System Design Layout Sheets prepared in advance by the installation manager should contain the necessary information for assigning the **Transponder Name** and **ID**, or the **Port No.**, as well as the names and multiplex addresses for all SE receivers connected to each SE coordinator. The layout sheets will also contain the text to be used to indicate the SE receiver locations.

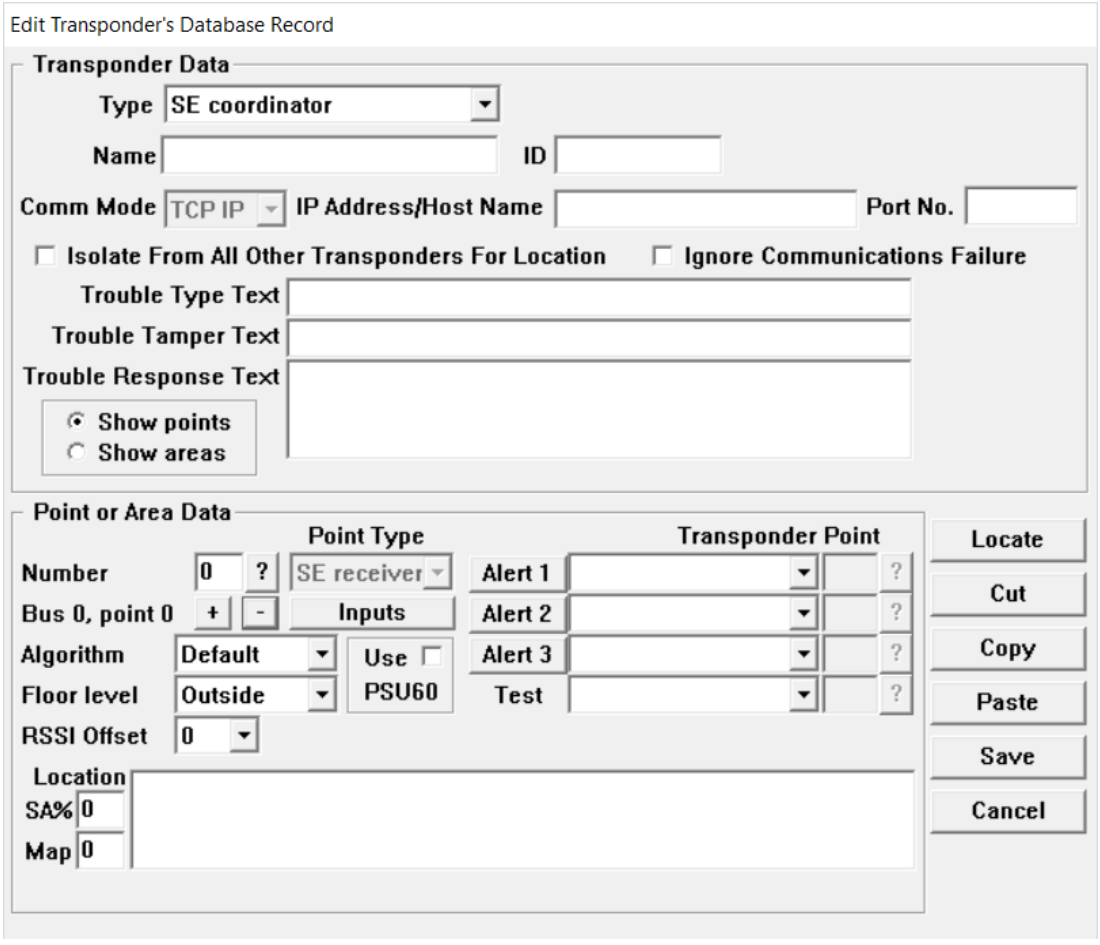


Figure 7.4: Edit Transponder's Database Record dialog after [Insert New]

The elements of the **Edit Transponder's Database Record** dialog are described as follows:

Element	Usage/Description
Type	Select the type of transponder record from the drop-down list box. There are two types of transponders, namely: "transponder" and "SE coordinator". Default is "SE coordinator".
Name	Key in the name of the SE coordinator.
ID	Key in the number that is assigned to the SE coordinator at system set-up. This is the Radio ID found on the product label of the SE coordinator circuit board. This **ID** is used by the Central Console to identify the SE coordinator during all communications between the Central Console and the SE coordinator.
Comm Mode	This field is disabled and defaulted as "TCP IP" if the **Type** selected is "SE coordinator". "TCP IP" is the only communication mode between the Central Console and the SE coordinator.
IP Address/Host Name	Key in the IP address or Host Name of the SE coordinator.
Port No.	Key in the communications port that is used by the Central Console to communicate with the SE coordinator. Valid port is between "1" and "65535".
Isolate From All Other Transponders For Location	Select this checkbox if this SE coordinator is isolated from all other SE coordinators for location considerations. This should be used when distant SE coordinators sometimes hear an alarm and throw off the alarm location calculation. If this checkbox is selected, it indicates that this SE coordinator is protecting an area that is independent of all other SE coordinators in the system. When an alarm is reported, and the SE receivers on this SE coordinator have the best reception, only the SE receivers on this SE coordinator will be considered for the location of this alarm. If another SE coordinator has the best reception, then the SE receivers on this SE coordinator will be ignored for the location of this alarm.
Ignore Communications Failure	Select this checkbox if communication failures is to be ignored for this SE coordinator. It is used during a new installation of SE coordinators that are not yet fully on line. During system maintenance, when an SE coordinator is out of service for a while, it is used so that the communication failure messages will not flash on the screen and distract the operator. **Selecting this checkbox causes the system to ignore communication failure. Therefore, if communication fails with this SE coordinator, the area that this SE coordinator protects will not be protected, and alarms from subscribers in that area will be missed without the operator's knowledge. This checkbox should not be selected in a live system.**
Trouble Type Text	This is the text that will be shown in the trouble dialog when the Remote Key input on the SE coordinator goes active (shorted).

Element	Usage/Description
Trouble Tamper Text	This is the text that will be shown in the trouble dialog when the Remote Key input on the SE coordinator goes into trouble (open).
Trouble Response Text	This is the text that will be shown in the trouble dialog as the action that the responding individual should take.
Show Points	Select this option to enter information of the point (“SE receiver”, “Virtual” or “None”).
Show Areas	Select this option to enter information of the alarm area.

Create or modify the SE receivers of the SE coordinator using the features of the **Point Data**. For configuring **Area Data**, refer to the *Configuring alarm area, page 80* section. The sections below explain the SE receiver point configuration in detail.

7.8 Modifying an existing SE coordinator entry

If the SE coordinator is already defined in the **Transponder Database**, the **[Edit Data]** button is used to modify the data. The information that can be modified is the same when creating a new SE coordinator entry (see *Creating a new SE coordinator record, page 71*).

7.9 Configuring SE receiver parameters

7.9.1 Setting the Point Number

Each SE receiver that is connected to the SE coordinator on its communication bus has a unique **Point Number** (address) assigned during the system design process. The **Point Number** ranges from 0 to 15. However, **Point Number** 0 is reserved for the built-in SE receiver of the SE coordinator. Therefore, SE receiver can only use the **Point Number** range from 1 to 15. As the devices are connected on the same bus, the **Bus Number** is always 0. Note that the **Point Number** (1 to 15) must correspond to the physical address of the actual SE receivers, which is configured using the dip switches on the SE receivers’ circuit board.
Clicking the **[?]** button to the right of the **Point Number** text box opens a dialog window displaying the **Point Numbers** in a grid format. The grid provides a quick way to select a **Point Number** by clicking the corresponding number button.

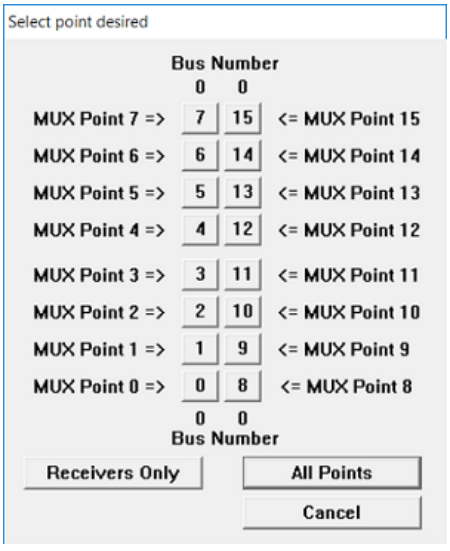


Figure 7.5: Select point desired dialog showing "All Points"

The buttons at the bottom of this dialog window allow the user to perform the following functions:

Element	Usage/Description
[All Points]	Display all possible point numbers regardless if a device has already been assigned to the SE coordinator.
[Receivers Only]	Display only the point numbers where a point type has been assigned.
[Cancel]	Closes the dialog window and return to the **Edit Transponder's Database Record** dialog.

As an example, clicking the **[Receivers Only]** button will display the grid with the point numbers of SE receivers only.

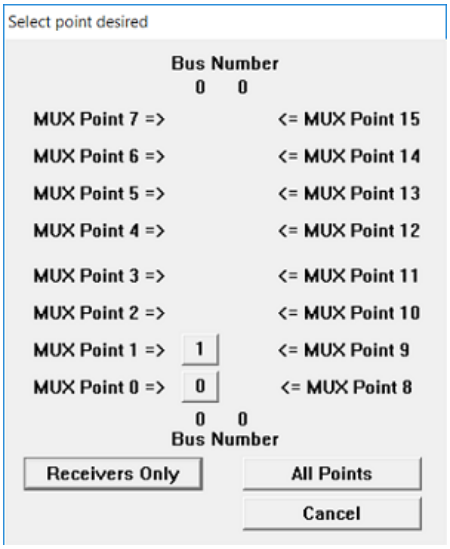


Figure 7.6: Example of Select point desired dialog showing "Receivers Only"

To configure the new SE receiver, click on the SE receiver's corresponding **Point Number** in the grid. This closes the window automatically and populates the number into the **Point Number** field on the **Edit Transponder's Database Record** dialog.
Alternatively, if you do not wish to use the grid, the **[+]** and **[-]** buttons, just below the **Point Number** lets you advance or retreat the device selection quickly by one location. This is useful when a task requires proceeding from device to device, as during system setup or check out.
The **[?]** button is used to display all devices to facilitate quick selection of a particular device. It is most useful when diagnosing a problem with a particular device.
Once the point you wish to configure is reflected in the **Point Number** field, you may proceed to enter the necessary information.

7.9.2 Selecting the Point Type

The **Point Type** drop-down list indicates the type of device that can be assigned to the selected **Point Number**. Click the drop-down list to change it to your desired **Point Type**.
The valid **Point Type** for SE coordinator are "SE receiver", "Virtual" (receiver), and "None".
The default **Point Type** is "None". Select the **Point Type** device accordingly when there is a physical device connected at this bus location.

Selecting "SE receiver" as the Point Type

Selecting "SE receiver" as the **Point Type** will populate the dialog window as shown below.

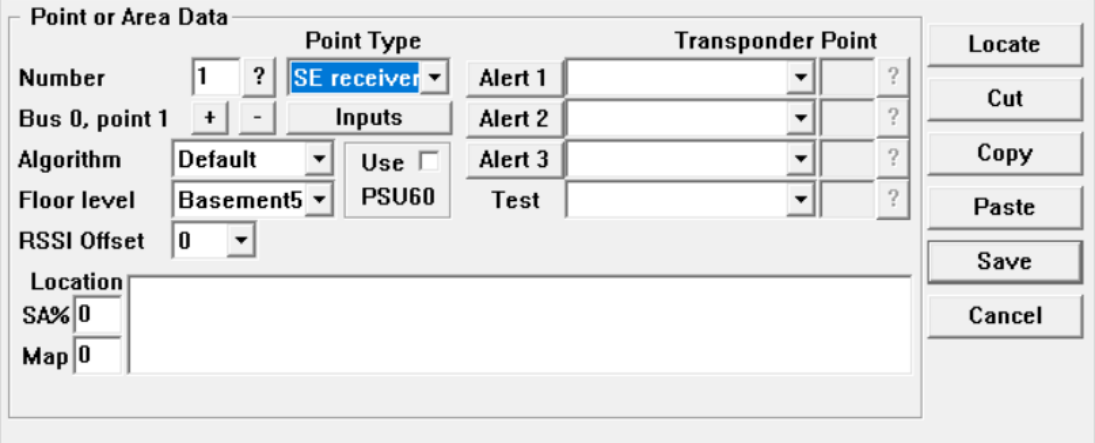


Figure 7.7: Data entry after selecting "SE receiver" as Point Type

If any SE receivers (including the SE coordinator, which is also SE receiver 0) is using the APS-PSU-60 power supply, select the **Use PSU60** checkbox. The power supply operation requires periodic and frequent auto switching from its battery to the direct current, and back.
The **Popup trouble filter** feature allows you to select the type of troubles (for example **AC loss / Input 1**) that is reported as a popup dialog. Normally, we will configure the system to monitor these troubles as they are important and may affect the entire operation.
Therefore, due to results of these internal APS-PSU-60 checks, the Central Console software may inadvertently report **AC loss / Input 1** trouble as popup trouble dialog windows. The frequency of these windows will cause unnecessary disruption to the normal SE operation.
Turning on the **Use PSU60** option will force the Central Console software to verify that actual **AC loss / Input 1** trouble was triggered before it displays the popup trouble dialog window.
Ensure that you select the **Use PSU60** checkbox if the SE receiver (0 to 15) is using the APS-PSU-60 power supply.

SE receiver has two analog inputs with four state supervised monitoring. Click the **[Inputs]** button to configure the input mapping of the device. **Input 1** and **Input 2** can be configured with their four states, namely **Short**, **Off**, **On** or **Broken**. Click the **[Save]** button to save the changes or **[Cancel]** button to abort the changes.

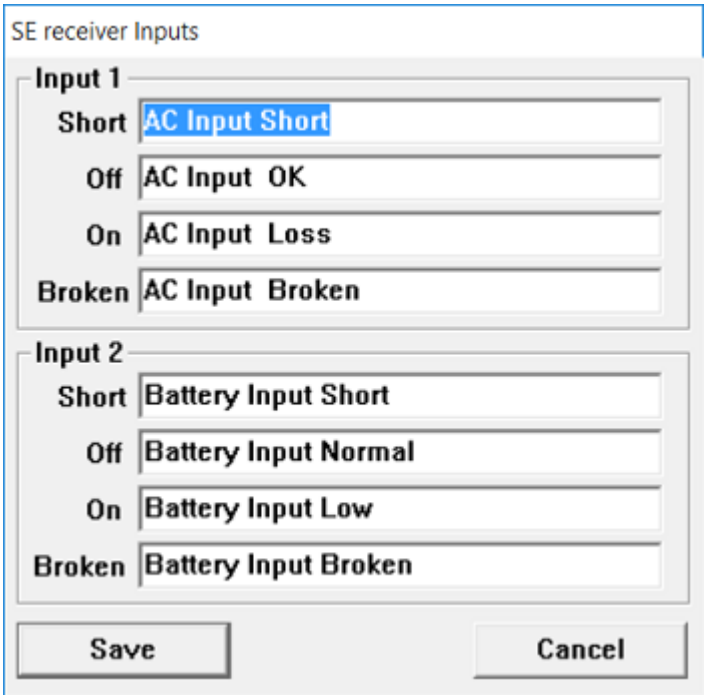


Figure 7.8: SE receiver Inputs dialog

Each SE receiver can be assigned with up to three alerts. When an “Alarm” event is reported by the SE receiver, these alerts will be activated. These alerts can be strobe/sirens (or any device) that is connected to the relay output of any SE receivers. These SE receivers need not be connected to the same SE coordinator.
Each SE receiver can also be assigned with one test device. Again, this test device can be strobes/sirens (or any device) that is connected to the relay output of any SE receivers. When performing “Test” transmissions for this SE receiver, this configured test device is triggered to provide a visual/sound indication of the transmission.

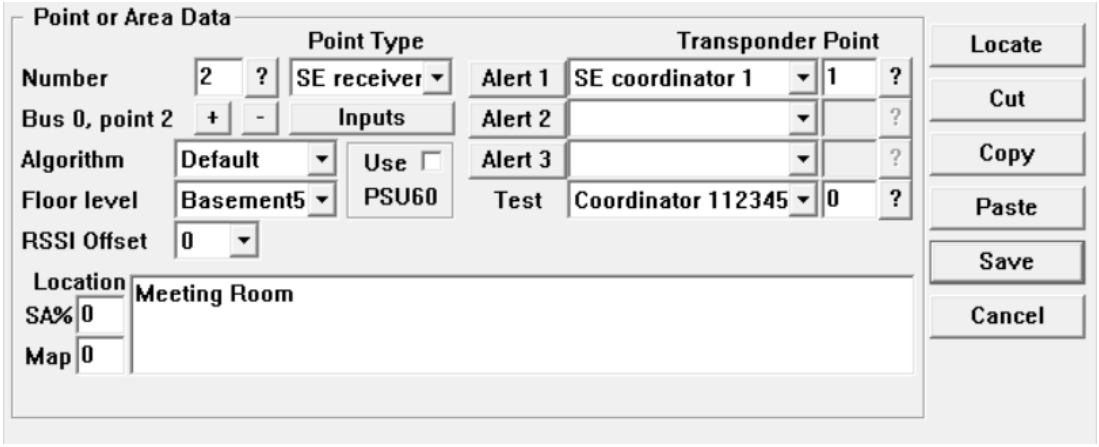


Figure 7.9: Assigning Alert or Test points to the SE receivers

Use the drop-down lists of **Alert 1**, **Alert 2**, **Alert 3** and **Test** to assign alerts/test to the SE receiver. Once the SE coordinator is selected from the items, key the point number into the **Point** text box. Alternatively, click the **[?]** button to select the point number from the grid. Click the SE receiver number on the grid to populate the point number into the **Point** text box.

Click the **[Alert 1]**, **[Alert 2]** or **[Alert 3]** button to change the alert points of all SE receivers of this SE coordinator to the current alert point. A **Change Alert On This Transponder** dialog window appears. Click the **[Change All]** button to affect the changes or **[Cancel]** button to abort the changes.

Selecting “Virtual” receiver as the Point Type

Use the “Virtual” item when there is no physical device connected at this bus location. A virtual receiver is added at one of the 15 points allowed for each SE coordinator. However, there is no physical hardware used.

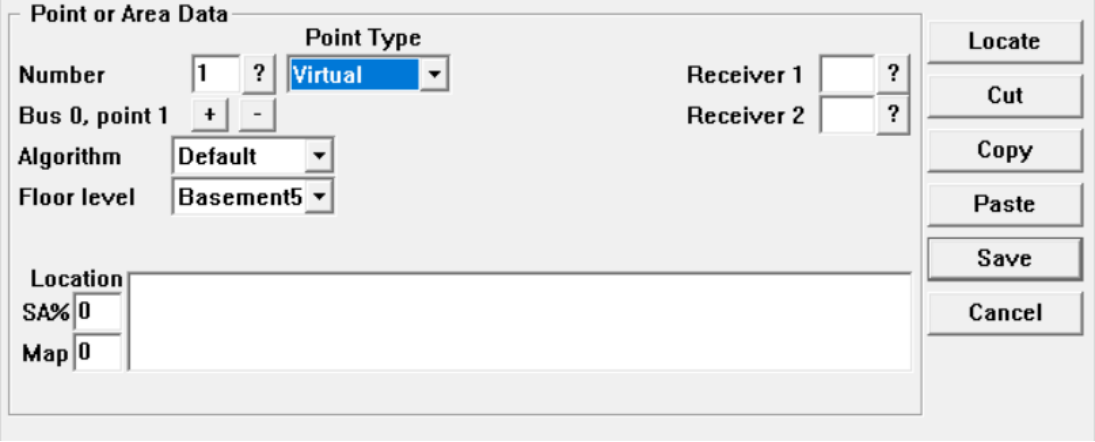


Figure 7.10: Data entry after selection of "Virtual" (receiver) Point Type

The Virtual receiver is intended to compensate in cases where there is an imbalance of SE receiver coverage. For example, if a building with a dense population of SE receivers is adjacent to a fence with few SE receivers, and an alarm occurs between them, the alarm location may be pulled towards the building. The Virtual receiver references two other **physical SE receivers** that must be on the same SE coordinator. Only if both the referenced SE receivers receive an alarm transmission, then the Virtual receiver will be added to the alarm as if it was a physical SE receiver that heard the alarm at the average receive level of the 2 referenced SE receivers.

Both the referenced SE receivers are configured in the **Receiver 1** and **Receiver 2** fields. These are the two SE receivers, on the same SE coordinator, where a Virtual receiver assumes the average of. Both SE receivers must receive a signal before the Virtual receiver reports it also received a signal that is the average of the other two SE receivers signals. The location algorithm and sensitivity adjust work the same for a Virtual receiver as for a physical SE receiver. Enter the Virtual receiver’s **Point Number** in the fields, or click the **[?]** button to select the Virtual receiver accordingly.

The Virtual receiver’s location and sensitivity may be adjusted the same as a physical SE receiver. After a Virtual receiver is added, verify the surrounding areas to make sure they have not been adversely affected.

Notice!

In no event should a Virtual receiver be utilized as a cost savings measure to avoid the installation of an actual SE receiver.

7.9.3 Selecting the Algorithm

There are 5 different location algorithms that can be selected for an individual SE receiver in the **Transponder Database**:

1. Classic (original Escort algorithm),

2. Linear,
3. Low pull,
4. Medium pull, and
5. Strong pull.

By default, when an SE receiver is set for outside or tunnel, it will use the linear algorithm and all other SE receivers will use the low pull algorithm. The SE receiver that hears the alarm transmission the strongest will determine the algorithm used for this alarm.
Changing the algorithm setting for an SE receiver only affects the location when the alarm is close to this SE receiver and it hears the alarm the strongest. The stronger the pull, the more the alarm will be pulled towards the SE receiver, with linear having no extra pull.
The algorithm setting will only be available if the **Enable algorithm tweaks** checkbox is selected in the **System Preferences** dialog. The Security Escort software also allows individual SE receiver's sensitivity to be set in the **Transponder Database**. SE receivers' sensitivity can be adjusted from 50% to 149% of their normal setting in the **SA%** text box.

7.9.4 Selecting the Floor Level

Use the **Floor level** drop-down list to assign the physical floor level where the SE receiver is mounted. The possible data range from "Basement5", "Basement4" to "Basement1", "Tunnel", "Basement", "Ground", "Outside", from "Floor 1", "Floor 2" to "Floor 99".

7.9.5 Setting the RSSI Offset

Use the **RSSI Offset** drop-down list to assign an offset to the RSSI value of the SE receiver in the **Transponder Database**. The **RSSI Offset** drop-down list allows the selection of "-70", "-60", "-50", "-40", "-30", "-20", "-10", "0", "+10", "+20", "+30", "+40", "+50", "+60" and "+70" values. The **RSSI Offset** field is set as "0" by default. Selecting other **RSSI Offset** values and saving it will mark the RSSI Offset field in yellow color in the **Transponder Database** dialog. This will offset the RSSI value by adding or subtracting to it, before the value reaches any calculation for SA% or Location. When RSSI value after offset is greater than 255, the result would be set as 255. When RSSI value after offset is less than or equal to 0, the result would be set as 1.
Note that the **RSSI Offset** is not applicable to virtual receivers.

7.9.6 Setting Location and Map

The **Location** field contains the text to be displayed on the Alarm Screen, if this SE receiver is closest to the alarm source. The location description is determined with the guidance of the security personnel who must respond to an alarm. It is vital that the description is clear and unambiguous to them.
To enter a location description, place the cursor in the **Location** text box, click the mouse, and begin typing. SE receiver location names are important because they are used for directing response to an alarm and aid service personnel in identifying the device in the event of a problem. The Problem Reports displayed on the Central Console and printed by the hardcopy printer contain the device location descriptions that are entered in the **Location** field.
The **Map** field defines which map to display for this SE receiver when an alarm is closest to it. The default map is 0, which corresponds to the bitmap file "MAP0.EDB" stored in the Security Escort sub-directory. Map 1 would correspond to the bitmap file "MAP1.EDB". Up to 100 maps (0 to 99) can be defined for each Security Escort system.

7.9.7 Adjusting the sensitivity (SA%)

Security Escort software allows individual SE receiver sensitivity to be set in the **Transponder Database**. SE receivers' sensitivity can be adjusted from 50% to 149% of their normal setting. No physical SE receiver changes or upgrades are required. This setting should only be changed if there are known location accuracy problems in the area of this SE receiver. Settings of 50 to 99 desensitize the SE receiver to 50% to 99% of the actual received signal strength. Settings of 1 to 49 increase the sensitivity to 101% to 149% of the actual received signal strength. Try changing the sensitivity of SE receivers one at a time while testing the alarm location response.

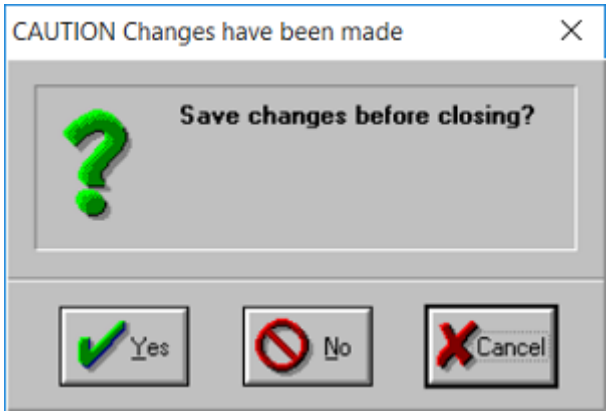
For example, if alarms are being pulled towards a particular SE receiver, lower its sensitivity in 10% increments and retest. If the area can be corrected using this method, verify the surrounding areas to make sure they have not been adversely affected. Generally, it is better if the correction is done in small steps while verifying the adjacent areas, rather than trying to correct the entire error in one step. The sensitivity adjustment option is only available if the **Enable algorithm tweaks** checkbox is selected in the **System Preferences** dialog.

In the **Transponder Database**, the **Algorithm** drop-down list also allows the selection of "Default", "Classic", "Linear", "Low", "Medium", or "Strong" pull location algorithms for each SE transmitter. The point reporting the best reception level determines the actual algorithm used for the location on any event. If programmed for "Default", the algorithm used is "Linear" for points programmed as outdoor or tunnel. All other points use "Low". If the point that reports the best reception level is not programmed with the "Default" algorithm, the location calculation uses the programmed algorithm.

7.9.8 Other miscellaneous command buttons

The functions of the other miscellaneous command buttons are described as of below:

Element	Usage/Description
[Locate]	Click this button to map the device on the map. The **Edit Transponder's Database Record** dialog disappears and the cursor changes to a cross hair. Moving the cursor to a point on the map and clicking the left mouse button scrolls the map so the point is at the center of the screen and all previously defined receivers and areas are shown with numerical labels. When the map is showing the location of the desired SE receiver, move the cross hair to the exact location of the SE receiver and click the right mouse button. The **Edit Transponder's Database Record** dialog reappears and the selected location is entered into the X and Y coordinates. If the cross hair cursor is displayed and you want to exit without changing any coordinate values, press the <Esc> key and the **Edit Transponder's Database Record** dialog reappears.
[Cut]	Click this button to copy the displayed point to a clipboard and returns all values to their defaults.
[Copy]	Click this button to copy the displayed point to a clipboard. Displayed values are not changed.
[Paste]	Click this button to copy the clipboard values to the displayed point. The values on the clipboard are not changed and can be copied to more points or areas.

Element	Usage/Description
[Save]	Click this button to save all changes to the database.
[Cancel]	Click this button to close the dialog window. If changes were made, the dialog window below appears, giving you another chance to save the changes by clicking the **[Yes]** button. 

7.10 Configuring alarm area

In the **Transponder Database** menu item under the **File** menu, select the SE coordinator where the alarm area is to be programmed in. Click the **[Edit Data]** button, followed by **Show areas** radio button and select the desired area.

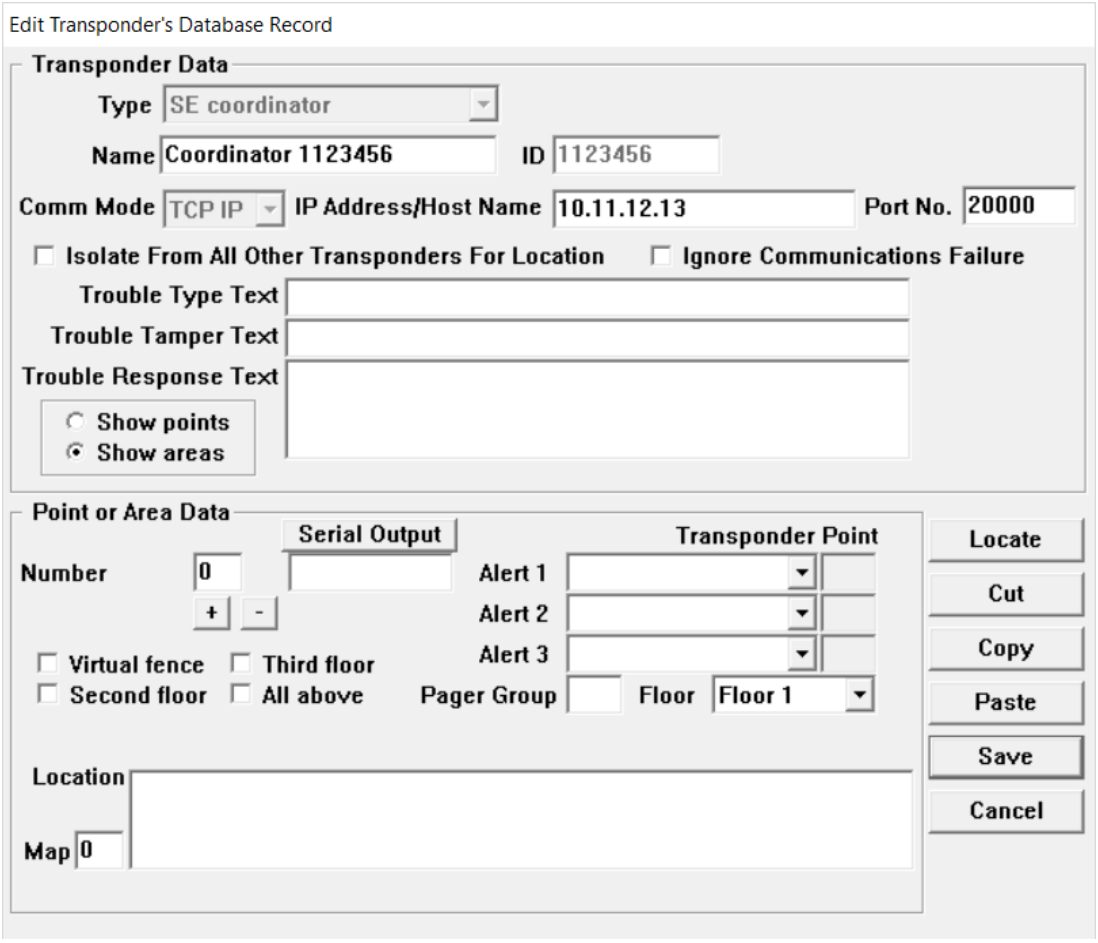
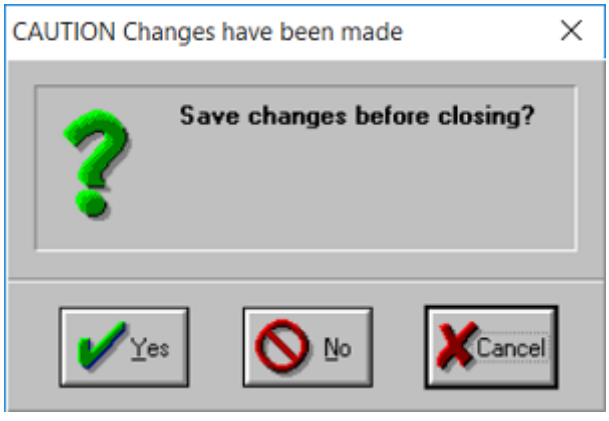


Figure 7.11: Configuring alarm area in the Edit Transponder's Database Record dialog

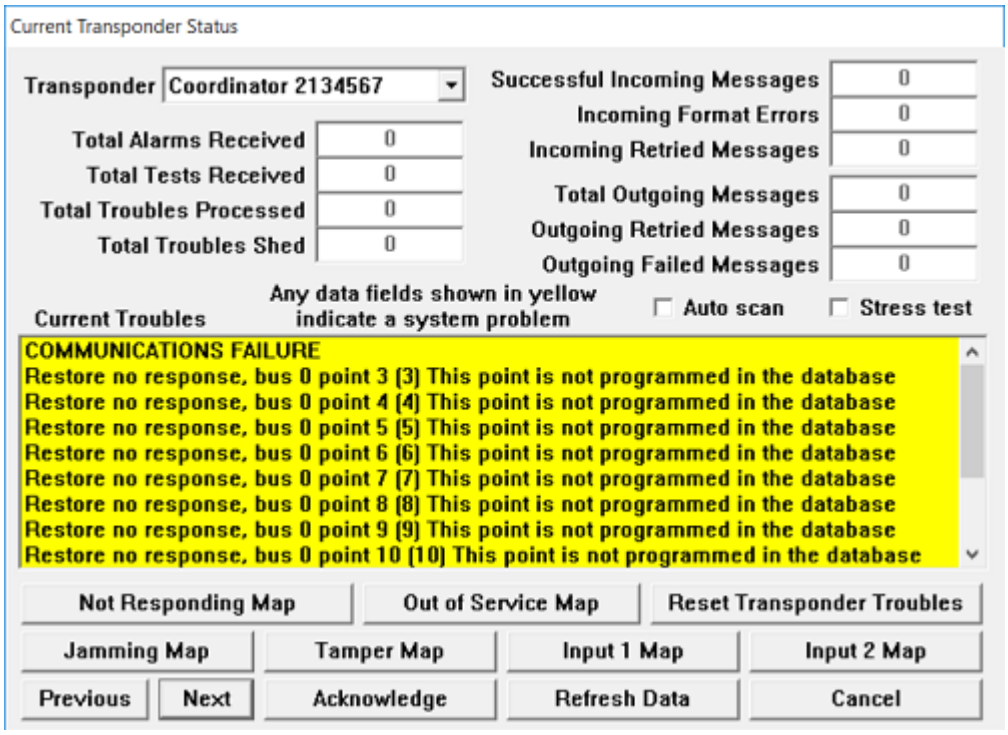
Element	Usage/Description
Number	Each SE coordinator can have up to 80 areas defined in them. This area number range from 0 to 79. Enter the area number directly or the **[+]** or **[-]** to advance or retreat an area number by 1 at a time. Use the **Locate** button to define the area graphically on the map.
Serial Output	The purpose is to send the string in the **Serial Output** text box automatically, where the alarm is most likely located, to the programmed serial port in the **Remote Setup** dialog. Up to 60 characters may be entered. Control characters may be entered as "^A" for control A. Clicking the **[Serial Output]** button sends the string to the serial port for testing purposes.
Pager Group	This **Pager Group** field may be programmed with a pager group that is paged if the alarm location is determined to be in this area. This pager group will be the first group paged to allow quick response by those individuals charged with responding to an alarm in this area. Each area may be assigned a pager group that can be the same or different from other alarm areas. The default alarm **Pager group** defined in the **Pager Setup** dialog will also be paged after the pager group is assigned to an area. If a pager group is not assigned to an area or the alarm location is not within a defined area, then only the default pager group will be paged.
Floor	Determines the floor number that this area is defined for. The areas on floors above and below this one may be defined differently. In order for an area to be selected when an alarm is received, the location determined by the Central Console must be located within the defined area, and it must be located on the designated floor.
Virtual fence **Second floor** **Third floor** **All above**	If this checkbox is selected, this area will not be used for normal alarm area location. This area will only be used to define a “Virtual” fence. Specific transmitters in the **Subscriber database** can reference this SE coordinator and area. When they reference this area, and the system locates the transmitter position outside the area, a Wandering (“Virtual” fence) Alarm will be generated. This alerts the operator and shows the position of the transmitter.
[Locate]	Click this button to define the alarm area on the map. The **Edit Transponder’s Database Record** dialog disappears and the cursor changes to a cross hair. Move the cross hair to the exact location of the first point of the polygon that describes the boundary of the area and right click. Move the cursor to the second point of the polygon and again right click. The computer draws a straight line between the first and second points. Repeat this process drawing all sides of the polygon to define the area. To close the polygon, place the last point on top of the first point.

Element	Usage/Description
	The polygon can have up to nineteen sides and no two lines of the polygon may cross each other. If you try to create more than nineteen sides, the computer automatically closes the polygon with the nineteenth side. When the polygon is closed, it can be crosshatched to make it more visible. After the polygon is complete, double click the left mouse button to return to the **Edit Transponder's Database Record** dialog. If the area being defined is a virtual monitor "fence" area for Wandering Alarms, the monitor fence (area boundary) should be drawn at least 7.62 m (25 ft.) past the area to be protected to reduce potential false alarms. This is due to the basic location accuracy of the Security Escort system. If the cross hair cursor is displayed and you want to exit without changing any coordinate values, press the <Esc> key and the **Edit Transponder's Database Record** dialog reappears.
[Cut]	Click this button to copy the area data to a clipboard and returns all values to their defaults.
[Copy]	Click this button to copy the displayed area data to a clipboard. Displayed values are not changed.
[Paste]	Click this button to copy the clipboard values to the displayed area data. The values on the clipboard are not changed and can be copied to more points or areas.
[Save]	Click this button to save all changes to the database.
[Cancel]	Click this button to close the dialog window. If changes were made, the dialog window below appears, giving you another chance to save the changes by clicking the **[Yes]** button. 

7.11 Powering up the system for the first time

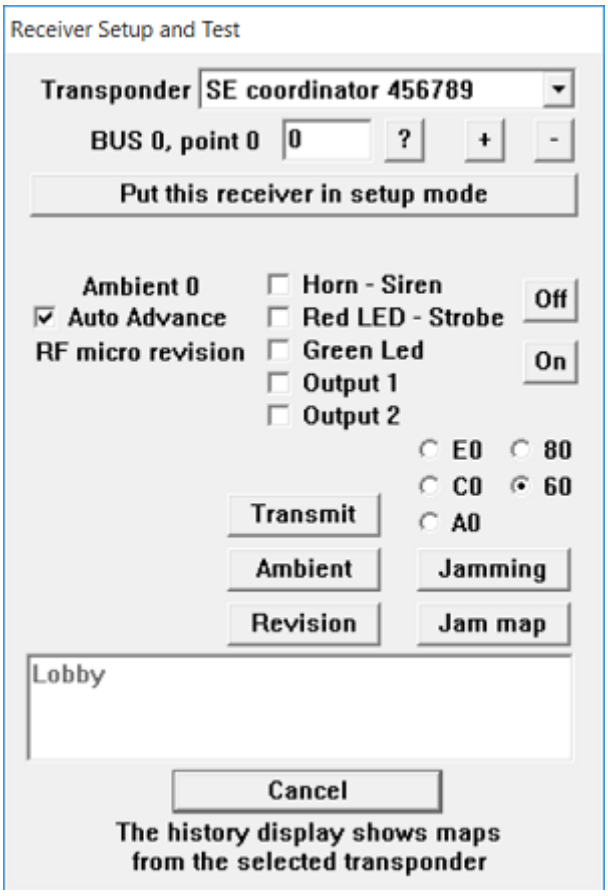
1. Ensure SE coordinator and receiver are powered up.

2. In the Security Escort Central Console software, select the menu **Setup > Transponder current status**. The following window appears:



3. Select the desired SE coordinator from the **Transponder** drop-down list box.
4. Click the **[Reset Transponder Troubles]** button. If the selected SE coordinator is communicating with the Central Console, the number “g1” will appear in the **Total Outgoing Messages** and **Successful Incoming Messages** fields. The SE coordinator is now communicating with the Central Console software. If the number “1” only appears in the **Total Outgoing Messages** field, there might be a problem between the Central Console and the SE coordinator (refer to the section Troubleshooting SE coordinators, points and SE receivers of this manual and locate the problem).
5. Check the **Stress test** checkbox. This tests the communications reliability by causing the Central Console software to send a continuous stream of messages to the selected SE coordinator. The values in the **Successful Incoming Messages** and **Total Outgoing Messages** fields should start counting up rapidly, with few, if any errors. It is normal to have slightly fewer **Total Outgoing Messages** than **Successful Incoming Messages**. If the errors are greater than 1% of the number of messages, then refer to the section Troubleshooting SE coordinators, points and SE receivers of this manual and locate the problem.
6. After the stress test runs, any current troubles are displayed. Correct any troubles at this time. Run the “Auto scan” process to sync with the actual status of the SE coordinators after resetting the troubles, or programming the SE coordinators in the Database.

7. To verify the RF reception, LED and sounder operation, and location of each SE receiver, select the menu **Setup > Receiver configuration**. The following dialog window appears:



8. Select the desired SE coordinator from the **Transponder** drop-down list box.
   - Click the **[?]** button next to the **point number** field. A grid of bus and point numbers appears showing the programmed SE receivers.
   - Click the lowest point number button. If the first SE receiver is MUX point zero (0), click the **[0]** button. If the first SE receiver is point one (1), click the **[1]** button. The point number is automatically entered.
   - Click the **[Put this receiver in setup mode]** button. The red and green LED light up for the selected SE receiver on the selected SE coordinator.
   - Take the maintenance SE transmitter and go to the selected SE receiver. The red and green LED should be lit when you arrive at the first SE receiver location.
   - Transmit an alarm from the maintenance SE transmitter. The SE receiver should activate by flashing the red LED and activate the sounder (if the sounder jumper is in place on the SE receiver). This confirms that the RF portion of the SE receiver is working and you are at the right location. The software then turns off the LEDs on the tested SE receiver. The SE receiver with the next higher point number is automatically selected and its red and green LED lights up.
   - Proceed to that SE receiver and perform the same operation with an alarm on the maintenance SE transmitter until the operation of all SE receivers is confirmed and all SE receivers are working and in their proper location on that SE coordinator. If the LED fails to light up, the LED jumpers may be missing on that SE receiver, the SE receiver may be set to the wrong address, or you may be at the wrong location. If the

LED are lit but the SE receiver fails to respond to the maintenance alarm, there may be a problem with the SE receiver board or another SE receiver is receiving a stronger signal.

9. Repeat the sequence above starting with step 1 for all other SE coordinators and SE receivers in the system.

8 Configuring equipment using Utility tool

Use the **Utility tool** to modify network information of the SE coordinators, scan and enroll SE receivers/SE transmitters to the SE coordinators, and upload firmware for SE coordinators, SE receivers and SE transmitters.
The operation of the **Utility tool** is recommended for configurators or administrators only as this involves the setup of the system hardware. The user must log in at “Reset Low Battery” **Authority Level** in order to access the **Utility tool**. The operations can be divided into three main sections, namely operations relating to SE coordinator, SE receivers and SE transmitters.
Operations relating to SE coordinator include changing the network name, modifying the IP address/Subnet Mask/Gateway/Port, and upgrading SE coordinator firmware.
Operations relating to SE receivers include scanning SE receivers that is connected (enrolled) to an SE coordinator, adding or removing SE receivers from an SE coordinator, upgrading SE receiver firmware, and so on.
The **Utility tool** also allows scanning of the SE transmitters, and upgrading of SE transmitter firmware.

8.1 Operations for the SE coordinator

8.1.1 Scanning SE coordinators

Opening the **Utility Tool** window will automatically scan all the SE coordinators of the Security Escort system. The SE coordinators that are connected to the Security Escort system are listed in the **SE Coordinators** grid view, together with their network details. To refresh the list of SE coordinators, click the **[Scan Coordinators]** button.

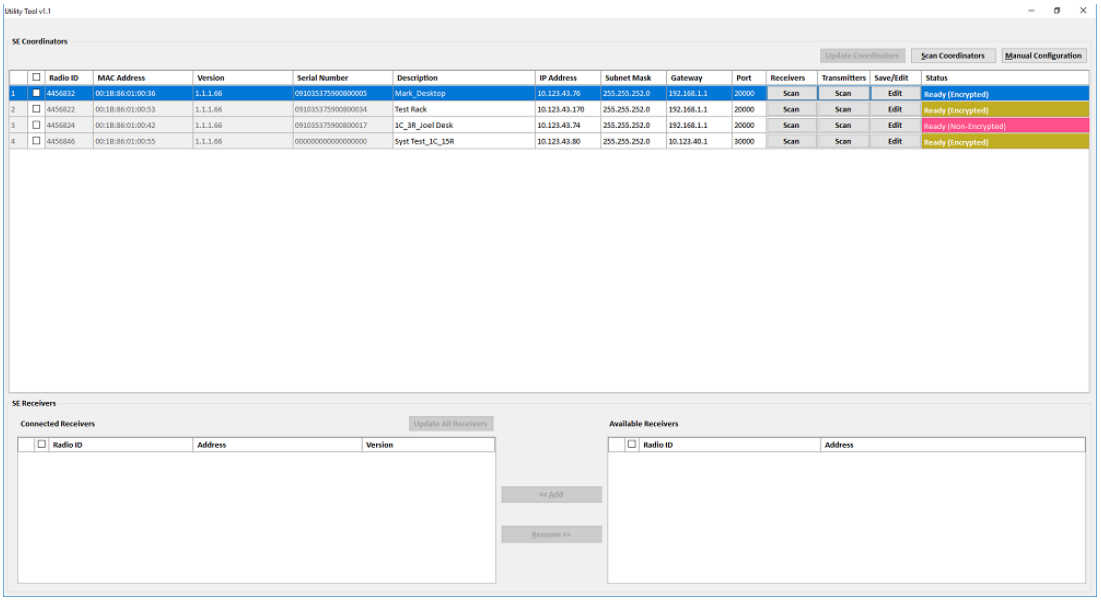


Figure 8.1: Utility tool dialog

Details of the SE coordinators are described as below:

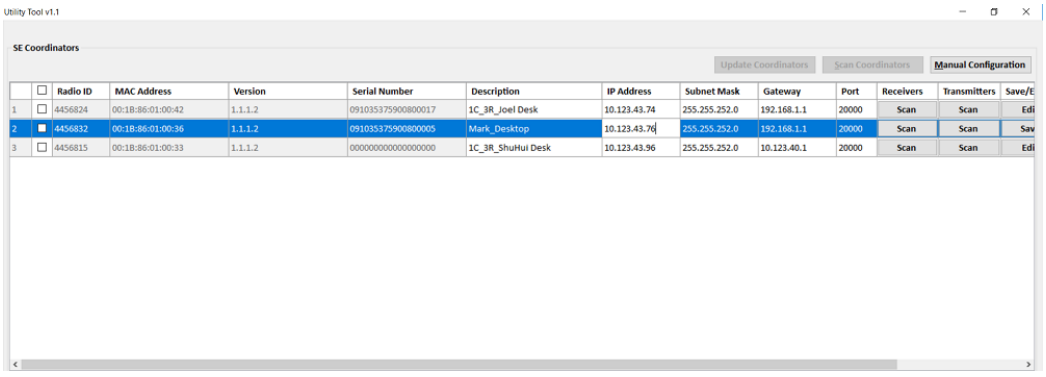
Element	Usage/Description
Radio ID	The radio ID of the SE coordinator. This radio ID is the same number as that is found on the back plate of the SE coordinator board. This information cannot be changed by the user.

Element	Usage/Description
MAC Address	MAC address of the SE coordinator. This information cannot be changed by the user.
Version	Firmware version of the SE coordinator.
Serial Number	Serial number of the SE coordinator.
Description	Description of the SE coordinator. Maximum length is 20 characters.
IP Address	IP address of the SE coordinator. A factory configured SE coordinator has the default IP address of 192.168.1.100. Valid IP addresses are from 1.0.0.0 to 255.255.255.255.
Subnet Mask	Subnet mask of the SE coordinator. A factory configured SE coordinator has the default subnet mask of 255.255.0.0. Valid subnet masks are from 1.0.0.0 to 255.255.255.255.
Gateway	Gateway of the SE coordinator. A factory configured SE coordinator has the default gateway of 192.168.1.1. Valid gateways are from 1.0.0.0 to 255.255.255.255.
Port	TCP/IP port of the SE coordinator. A factory configured SE coordinator has the default port of 20000. Valid ports are from 00001 to 65536.
Receivers	Click the **[Scan]** button to scan the SE receivers of the SE coordinator.
Transmitters	Click the **[Scan]** button to scan the SE transmitters of the SE coordinator.
Save/Edit	Click the **[Edit]** button to change the information of the SE coordinator. The **[Edit]** button changes to **[Save]** button. After making the necessary changes, click the **[Save]** button to affect the changes. The **[Save]** button changes to **[Edit]** button.
Status	Status of the communication with SE coordinator. The status shows if the communication is ready and encrypted: using color code schemes and status remarks in the column. The color code scheme represents the following: 1. Orange yellow color, with the "Encrypted" remark, shows an encrypted communication. 2. Red color, with the "Non-Encrypted" remark, shows an unencrypted communication. 3. Blue color, with either "Encrypted" or "Non-Encrypted" remark, shows the currently selected SE coordinator in the list. Status of the communication is represented by the following remarks in the column: – "Ready" shows that communication with the SE coordinator is working. – "Connection Failed" shows that communication with the SE coordinator has failed.

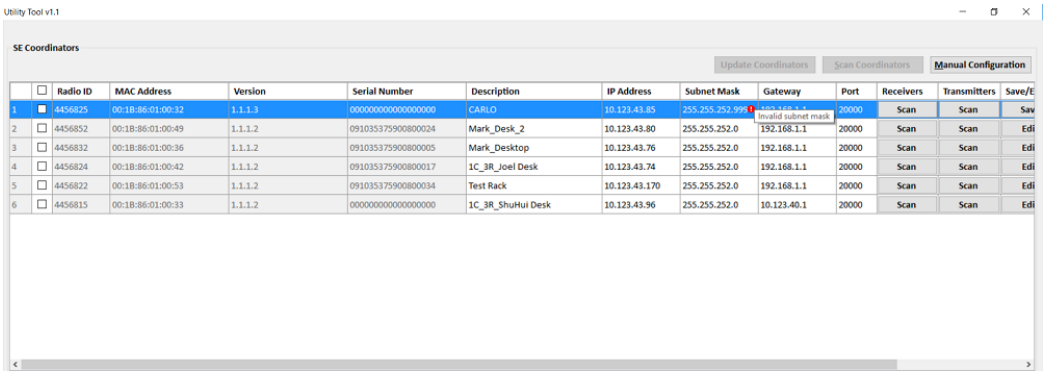
8.1.2 Modifying SE coordinator network settings

Follow the instructions below to change the network information of the SE coordinator. You can only change the data of one SE coordinator at any one time.

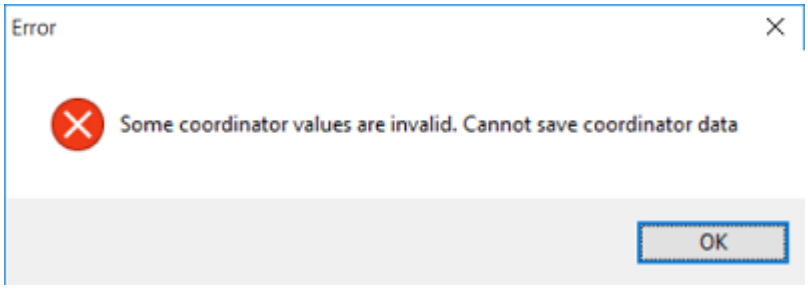
1. Click the **[Edit]** button under the **Save/Edit** column for the SE coordinator row entry that you wish to change. The **[Edit]** button changes to the **[Save]** button. Click once on the data that you wish to change. The field becomes enabled for data entry.
2. Alternatively, double-click on the data of the SE coordinator that you wish to change. The row entry will be highlighted, and the field becomes enabled for data entry. The **[Edit]** button changes to the **[Save]** button.



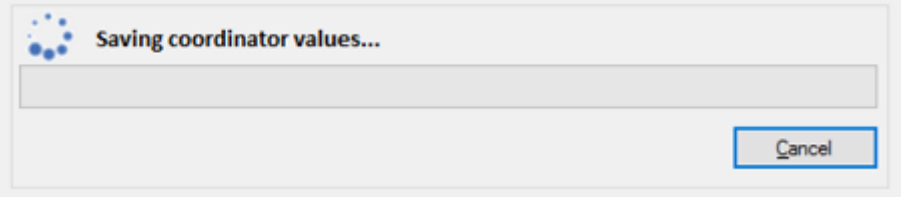
3. Enter the data that you wish to change. If the data entered is invalid, clicking on other data fields for the same SE coordinator will display a red exclamation point beside the incorrect new data. You can correct the data of the erroneous field at any point of time.



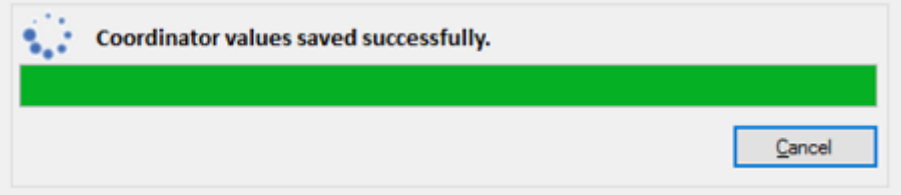
4. Click once on other data for the same SE coordinator that you wish to change, and make the changes.
5. To save the changes to the SE coordinator, click the **[Save]** button.
   – If the data entered is invalid, the red exclamation point will appear beside the incorrect data. An error dialog box appears. Click the **[OK]** button, re-enter the correct data and save the changes.



– If there are no errors, the data will be saved to the SE coordinator. An indicator bar appears on screen to display the progress. To abort the saving process, click the **[Cancel]** button.



If there are no errors, the indicator bar will show that the values are saved successfully.

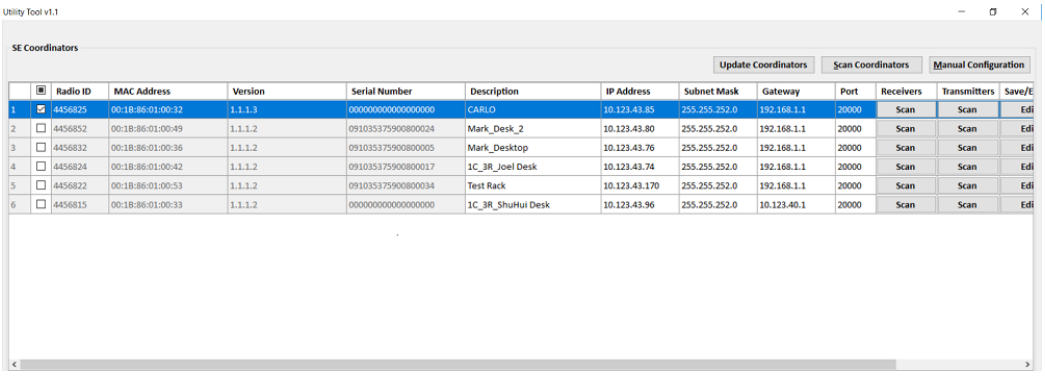


The **[Save]** button changes back to the **[Edit]** button.

8.1.3 Updating SE coordinator firmware

Follow the instructions below to update the SE coordinator firmware. You may update the firmware for selected SE coordinators or all of them at once.

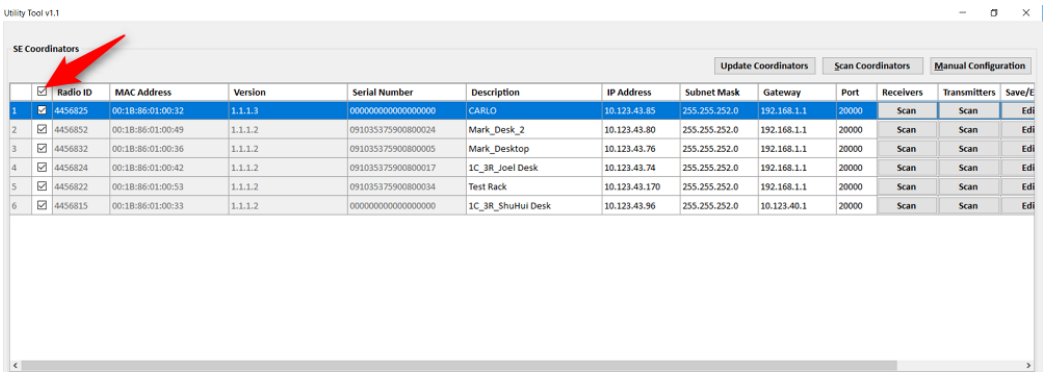
1. To update the firmware of the SE coordinator, select the checkbox beside the coordinator row entry. The **[Update Coordinators]** button is now enabled.



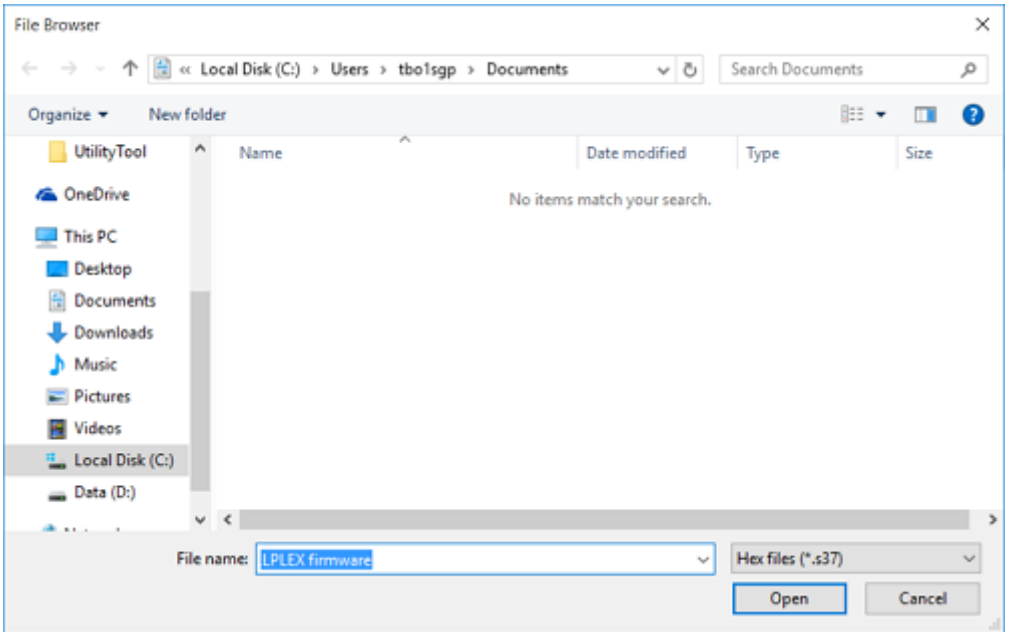
		Radio ID	MAC Address	Version	Serial Number	Description	IP Address	Subnet Mask	Gateway	Port	Receivers	Transmitters	Save/E
1	☑	4456825	00:1B:86:01:00:32	1.1.1.3	00000000000000000	CARLO	10.123.43.85	255.255.252.0	192.168.1.1	20000	Scan	Scan	Edi
2	☐	4456852	00:1B:86:01:00:49	1.1.1.2	091035375900800024	Mark_Desk_2	10.123.43.80	255.255.252.0	192.168.1.1	20000	Scan	Scan	Edi
3	☐	4456832	00:1B:86:01:00:36	1.1.1.2	091035375900800005	Mark_Desktop	10.123.43.76	255.255.252.0	192.168.1.1	20000	Scan	Scan	Edi
4	☐	4456824	00:1B:86:01:00:42	1.1.1.2	091035375900800017	1C_3R_Joel Desk	10.123.43.74	255.255.252.0	192.168.1.1	20000	Scan	Scan	Edi
5	☐	4456822	00:1B:86:01:00:53	1.1.1.2	091035375900800034	Test Rack	10.123.43.170	255.255.252.0	192.168.1.1	20000	Scan	Scan	Edi
6	☐	4456815	00:1B:86:01:00:33	1.1.1.2	00000000000000000	1C_3R_ShuHui Desk	10.123.43.96	255.255.252.0	10.123.40.1	20000	Scan	Scan	Edi

2. Repeat step 1 for other SE coordinators if you wish to update the same firmware for more than one SE coordinator.

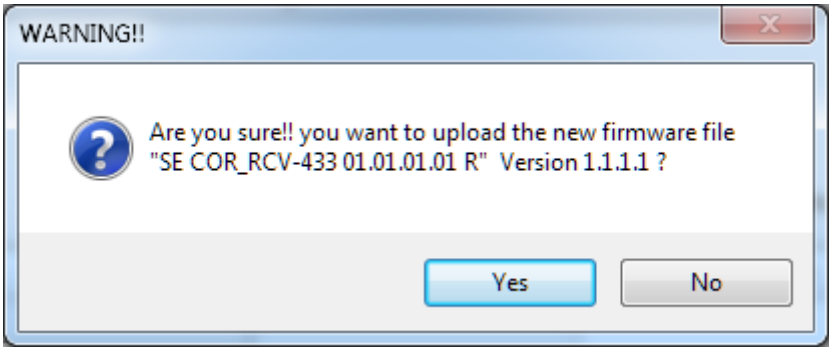
3. To update the firmware of all SE coordinators, select the checkbox on the row of the column names of the **SE Coordinators** grid view. All the checkboxes of the rows of SE coordinators are selected.



4. Click the **[Update Coordinators]** button, and a **File Browser** dialog appears.

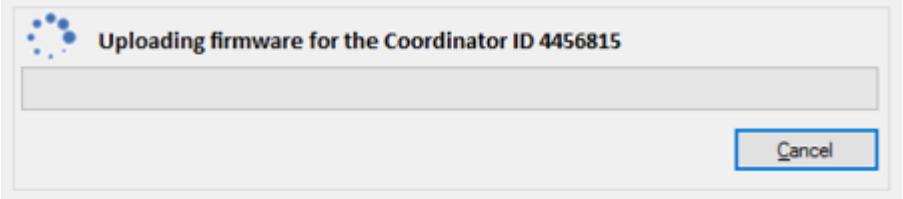


5. Browse and select the firmware file that you wish to update. Click the **[Open]** button.
6. A confirmation dialog box appears. Click the **[Yes]** button to proceed with the update, or the **[No]** button to abort.

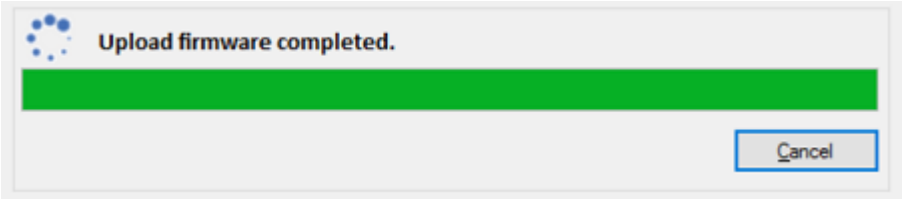


7. Upon clicking the **[Yes]** button, the firmware will be updated to the selected SE coordinators, one by one. An indicator bar appears on screen to display the progress for each SE coordinator's firmware update. The red and green LED of the selected SE

coordinators will blink continuously during the entire duration of update. To cancel the firmware update, click the **[Cancel]** button.



8. For each successful firmware update, the indicator bar shows the completed status. The red and green LED of the selected SE coordinators stops blinking and are turned off.



Notice!
Note that the **Status** column of the **SE Coordinators** grid view may show as **Connection Failed** for the successful firmware update. The latest status is not automatically refreshed in the list after the update. Click the **[Scan Coordinators]** button to refresh the list and status.

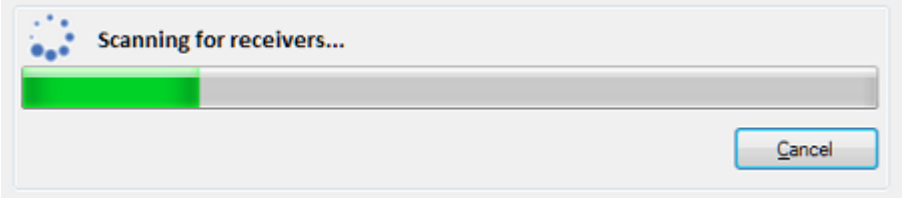
9. For each unsuccessful firmware update, an error message window appears.

8.2 Operations for the SE receiver

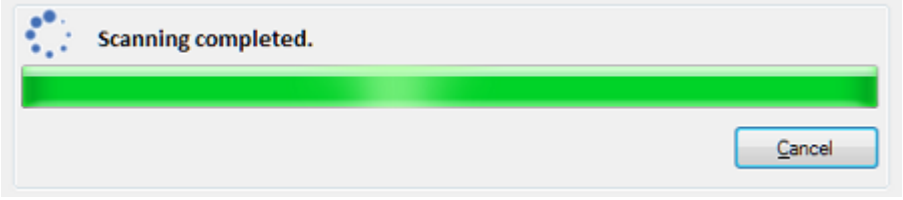
8.2.1 Scanning SE receivers

Follow the instructions below to list the SE receivers that are connected to the SE coordinator. **Connected Receivers** are SE receivers already connected (added) to an SE coordinator. **Available Receivers** are SE receivers on the same bus that are available to be added to the SE coordinator. You may scan the SE receivers for only one SE coordinator at any one time.

1. Click the **[Scan]** button under the **Receivers** column for the row entry of the SE coordinator from the **SE Coordinators** grid view.
2. The **Utility tool** scans for the SE receivers. An indicator bar appears on screen to display the scanning progress.



3. Upon completion of the scan, the indicator bar shows the completed status.



- SE receivers that are connected to the SE coordinator, appear in the **Connected Receivers** grid view.
- SE receivers that are available appear in the **Available Receivers** grid view.

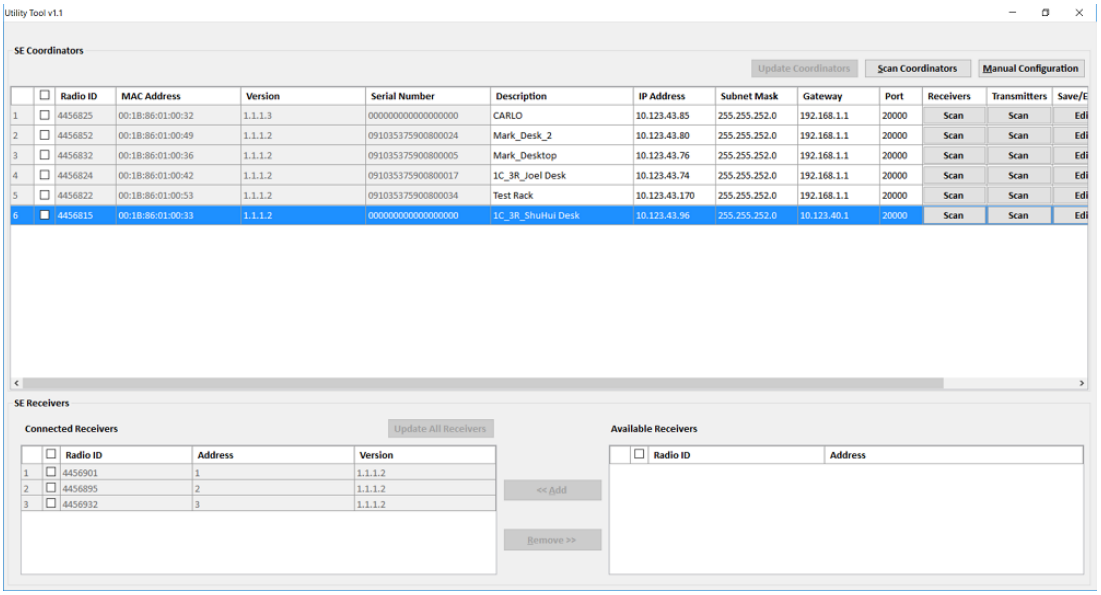


Figure 8.2: Scanning receivers

Details of the **Connected Receivers** are described as below:

Element	Usage/Description
Radio ID	The radio ID of the SE receiver. This radio ID is the same number as that is found on the back plate of the SE receiver board. This information cannot be changed by the user.
Address	Loop address of the SE receiver. The address is set via the dip switch on the SE receiver. This information cannot be changed by the user. Note: address 0 refers to the SE receiver that is built-in to the SE coordinator.
Version	Firmware version of the SE receiver.

Details of the **Available Receivers** are described as below:

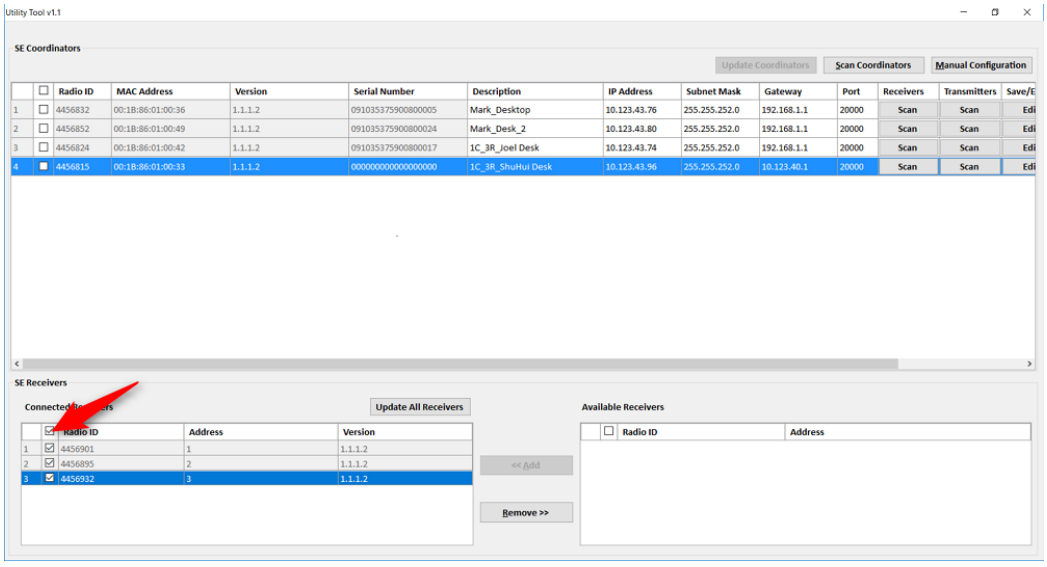
Element	Usage/Description
Radio ID	The radio ID of the SE receiver. This radio ID is the same number as that is found on the back plate of the SE receiver board. This information cannot be changed by the user.
Address	Loop address of the SE receiver. The address is set via the dip switch on the SE receiver. This information cannot be changed by the user. Note: address 0 refers to the SE receiver that is built-in to the SE coordinator.
Version	Firmware version of the SE receiver. The version will appear as 0.0.0.0 for the **Available Receivers**.

8.2.2 Updating SE receiver firmware

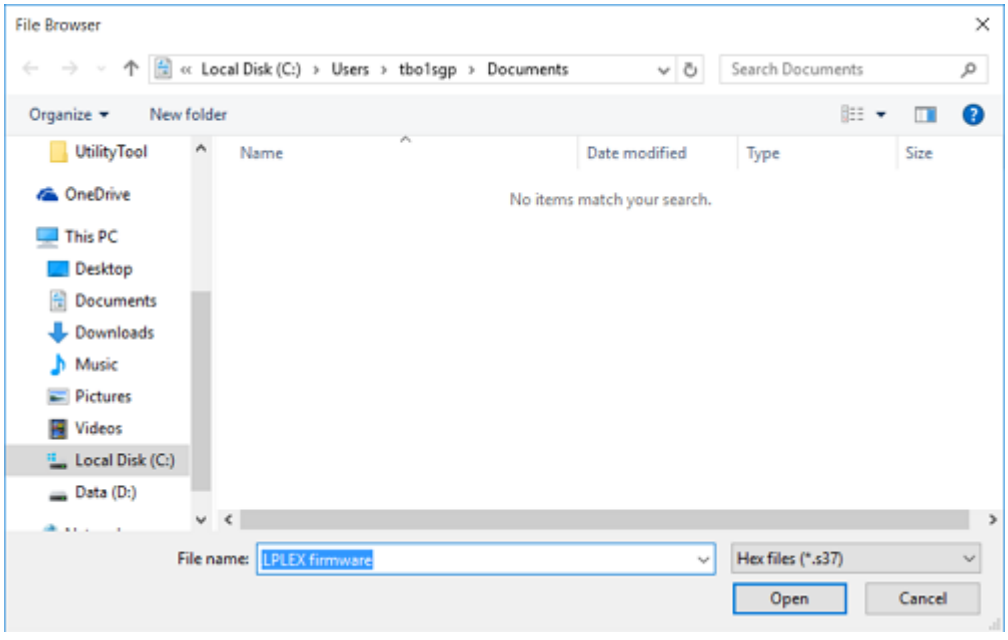
Follow the instructions below to update the firmware of all **Connected and Available Receivers**.

Notice!
Firmware update can only be performed on all connected receivers during a single session. You cannot update the firmware of any individual receiver independently in different separate sessions.

1. To update the firmware of all connected and available SE receivers, select all checkboxes beside every SE receiver row entry in the **Connected Receivers** grid view. Alternatively, select the checkbox on the row of the column names of the **Connected Receivers** grid view. All the checkboxes of the rows of connected SE receivers will be automatically selected. The **[Update All Receivers]** button is now enabled.

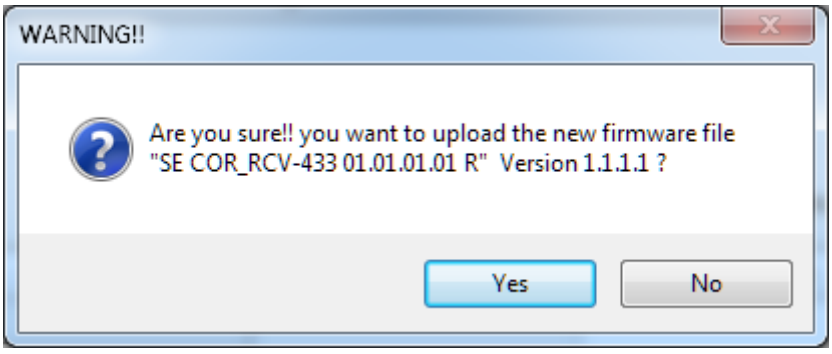


2. Click the **[Update All Receivers]** button, and a **File Browser** dialog appears.

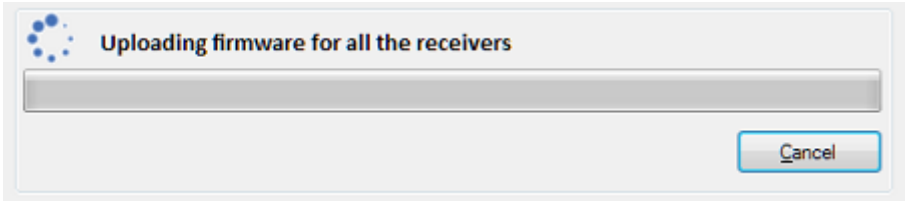


3. Browse and select the firmware file that you wish to update. Click the **[Open]** button.

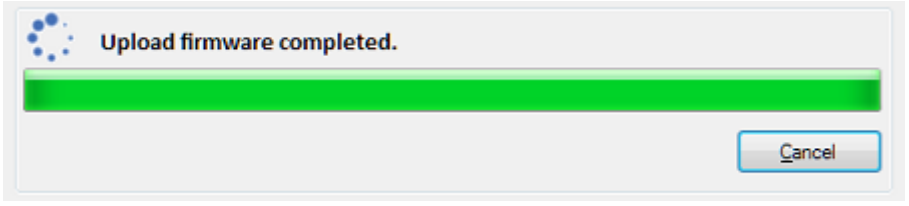
4. A confirmation dialog box appears. Click the **[Yes]** button to proceed with the update, or the **[No]** button to abort.



5. Upon clicking the **[Yes]** button, the firmware will be updated to all connected and available SE receivers. An indicator bar appears on screen to display the progress for the firmware update. The red and green LED of the SE coordinator will be turned on, while the red and green LED of all the SE receivers will blink continuously for the entire duration of update. To abort the update, click the **[Cancel]** button.



6. Upon successful firmware update, the indicator bar shows the completed status. The red and green LED of the SE coordinator and SE receivers will turn off once update is completed.



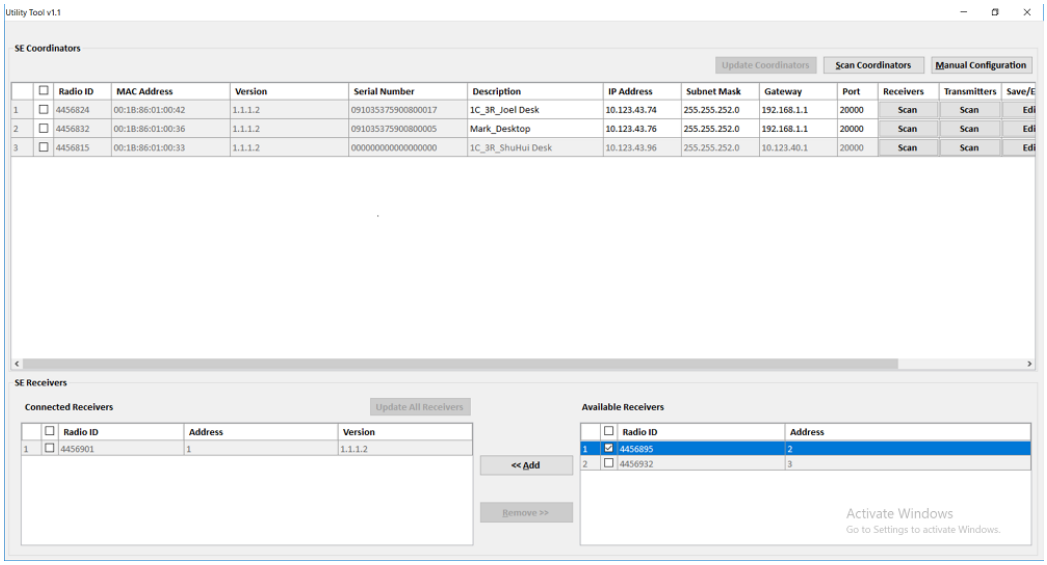
Notice!
Note that the **Version** column of the **Connected Receivers** grid view may still show the same firmware version for the SE receiver. The latest version number is not automatically refreshed in the grid after the firmware update. Click the **[Scan]** button under the **Receivers** column of the **SE Coordinators** grid view to refresh the list.

7. For each unsuccessful firmware update, an error message window appears.

8.2.3 Adding available SE receiver to the SE coordinator

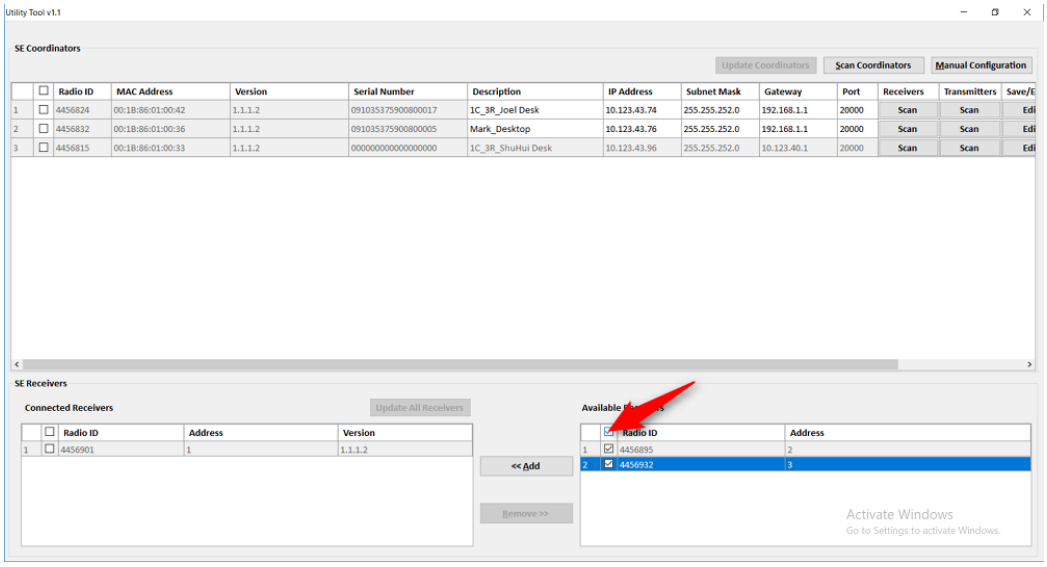
Follow the instructions below to add an SE receiver to an SE coordinator.

1. To add an available SE receiver, select the checkbox beside the SE receiver row entry in **Available Receivers** grid view. The **[Add]** button is enabled.



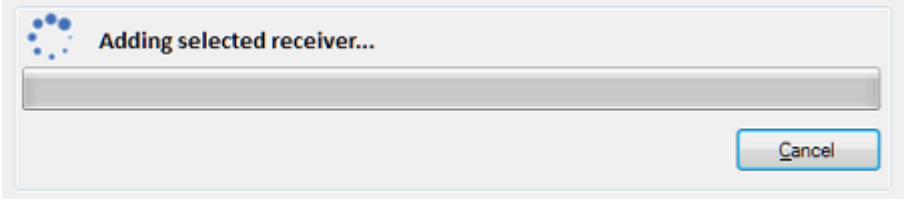
Notice!
Note that the version number of the available SE receivers are not displayed, and will show as 0.0.0.0 until it is added to an SE coordinator.

2. Repeat step 1 for other SE receivers if you wish to add more than one available SE receiver.
3. To add all available SE receivers, select the checkbox on the same row as the column names of the **Available Receivers** grid view. All the checkboxes of the SE receivers in the **Available Receivers** grid view are selected.

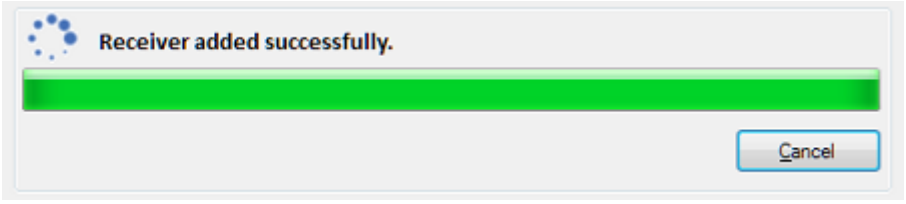


4. Click the **[Add]** button.

5. An indicator bar appears on screen to display the progress. To abort, click the **[Cancel]** button.



6. Once successfully added, the indicator bar shows the completed status.

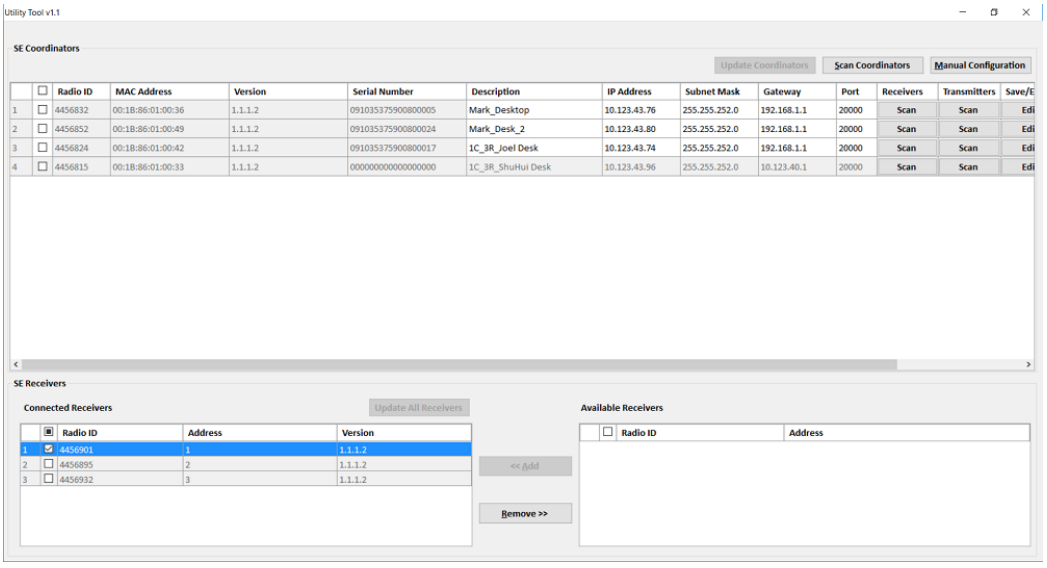


7. Receivers that are added successfully will be moved from the **Available Receivers** grid view to the **Connected Receivers** grid view. If the newly added receiver is showing 0.0.0.0 as its version, click the **[Scan]** button under the **Receivers** column of the coordinator row to refresh the **Connected Receivers** grid view.

8.2.4 Removing connected SE receiver from the SE coordinator

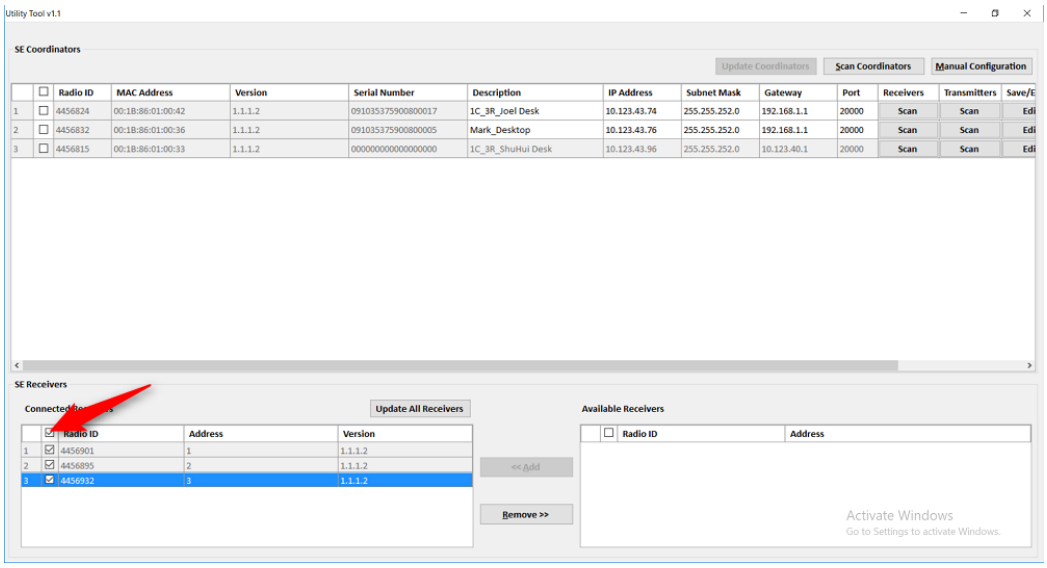
Follow the instructions below to remove a connected SE receiver from the SE coordinator.

1. To remove a connected SE receiver from the SE coordinator, select the checkbox beside the SE receiver row entry in the **Connected Receivers** grid view. The **[Remove]** button is enabled.

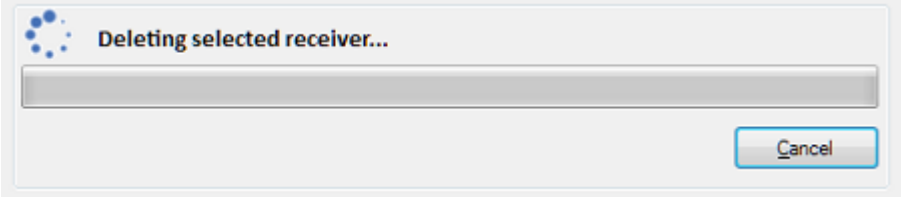


2. Repeat step 1 for other SE receivers if you wish to remove more than one connected SE receiver.

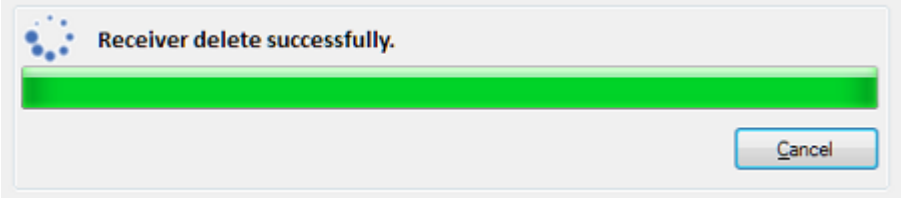
3. To remove all connected SE receivers, select the checkbox on the same row as the column names of the **Connected Receivers** grid view. All the checkboxes of the connected SE receivers are selected.



4. Click the **[Remove]** button.
5. An indicator bar appears on screen to display the progress. To abort, click the **[Cancel]** button.



6. Once successfully removed, the indicator bar shows the completed status.



7. If successful, the selected SE receivers will be moved from the **Connected Receivers** grid view to the **Available Receivers** grid view.

8.3 Operations for the SE transmitter

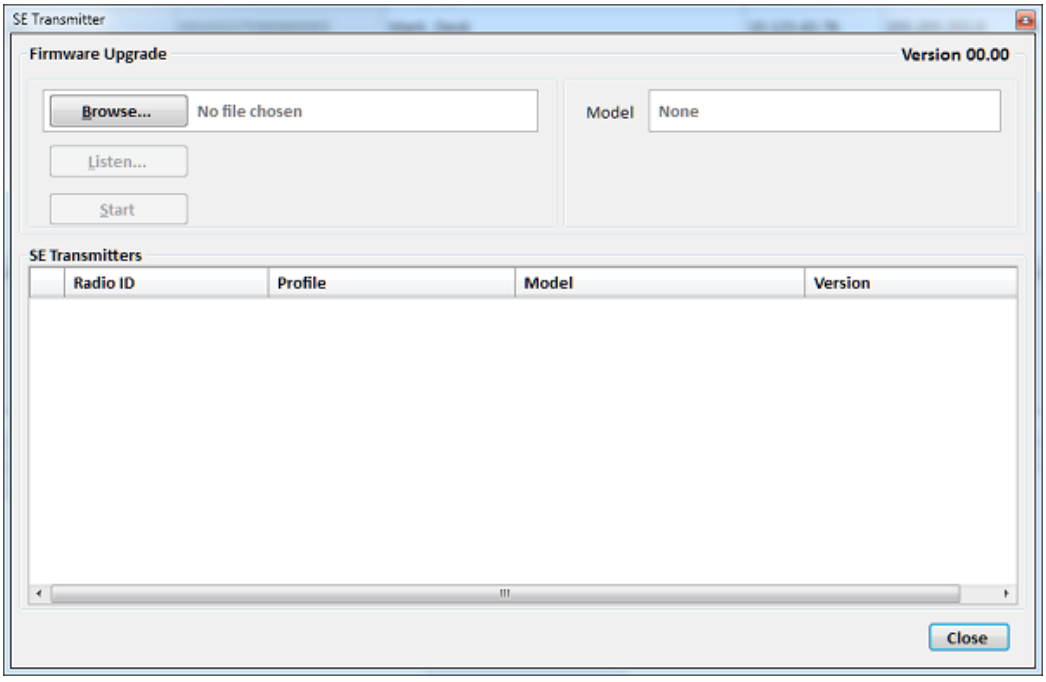
8.3.1 Scanning SE transmitters and upgrading firmware

Follow the instructions below to scan the SE transmitters that are within the RF communication range of the SE coordinator, from which the SE transmitter firmware can be uploaded. You may scan the SE transmitters for only one SE coordinator at any one time. The scanned SE transmitter will appear in the **SE Transmitters** grid view.

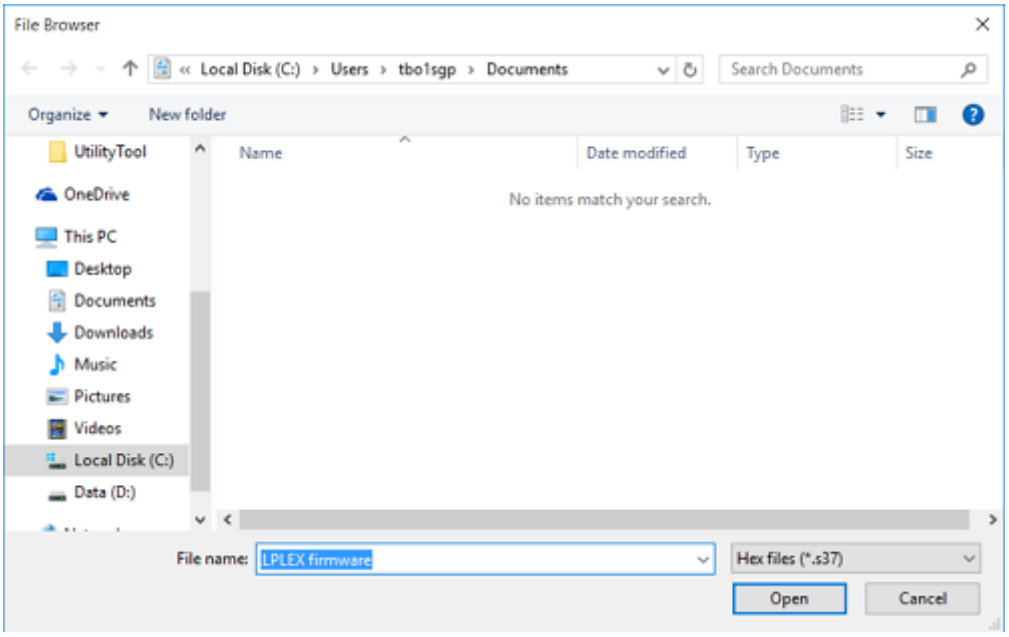
Details of the SE transmitters listed in the **SE Transmitters** grid view are described as below:

Element	Usage/Description
Radio ID	The radio ID of the SE transmitter. This radio ID is the same number as found on the back of the SE transmitter.
Profile	Profile of SE transmitter. The profile can be “User”, “Security” or “Maintenance”.
Model	Model of the SE transmitter.
Version	Firmware version of the SE transmitter.

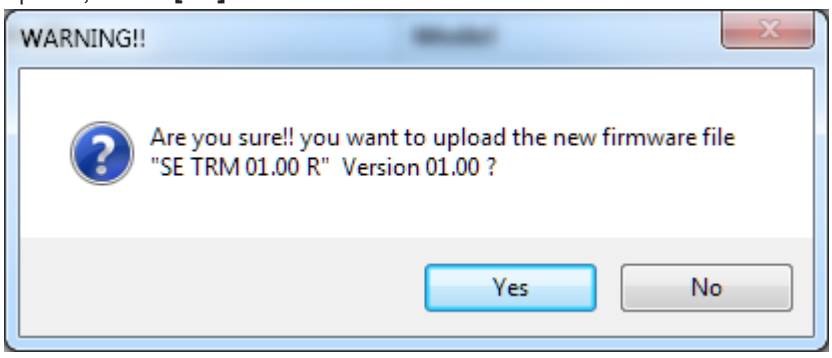
1. To scan the SE transmitters, click the **[Scan]** button under the **Transmitters** column for the row entry of the SE coordinator. The **SE Transmitter** dialog window appears.



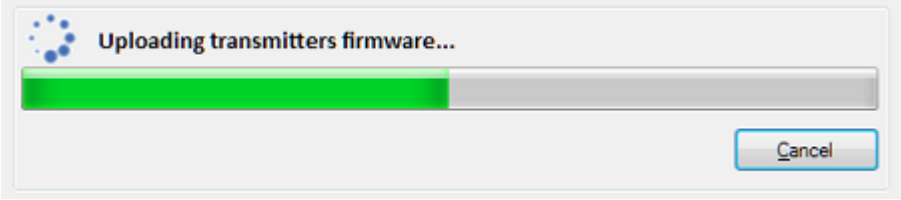
2. Click the **[Firmware Upload]** button, and a **File Browser** window appears.



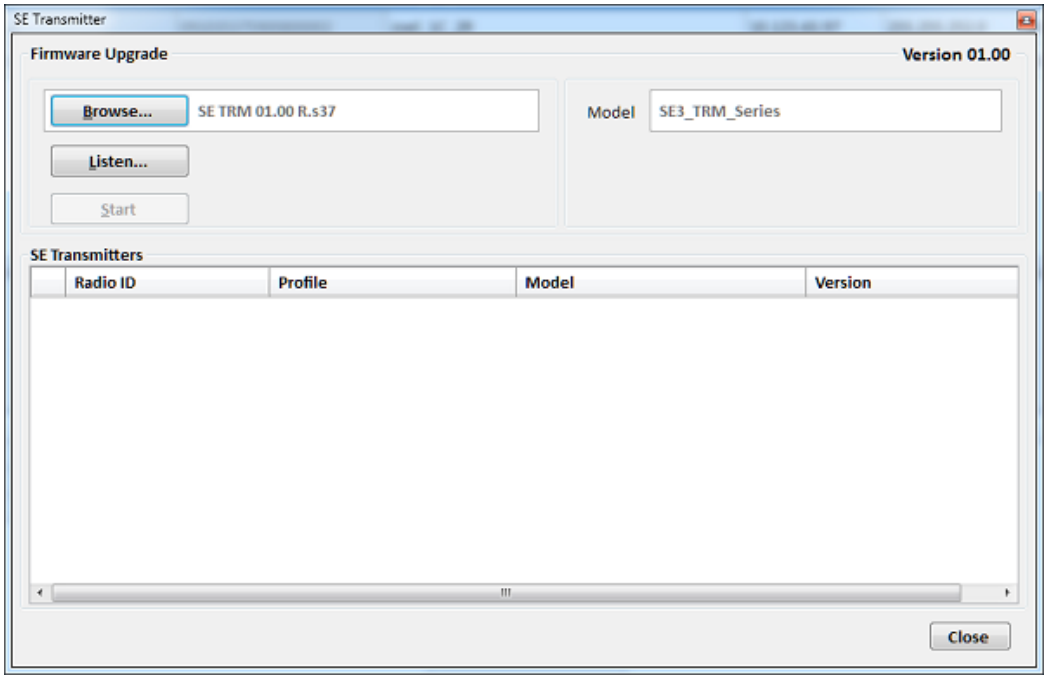
3. Browse and select the firmware file that you wish to upload. Click the **[Open]** button.
4. A confirmation dialog window appears. Click the **[Yes]** button to proceed with the upload, or the **[No]** button to abort.



5. Upon clicking the **[Yes]** button, the firmware will be uploaded. An indicator bar appears on screen to display the progress of the firmware upload. To abort the upload, click the **[Cancel]** button.

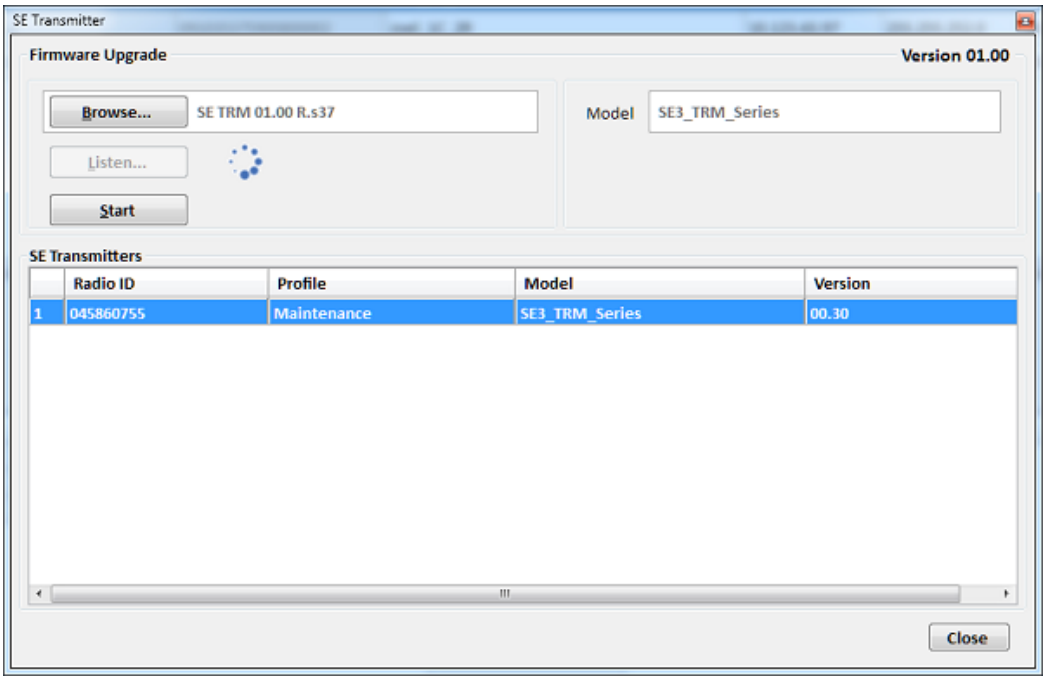


6. Upon completion of the firmware upload, the indicator bar will disappear. The version number is now updated, and the **[Listen]** button is enabled.

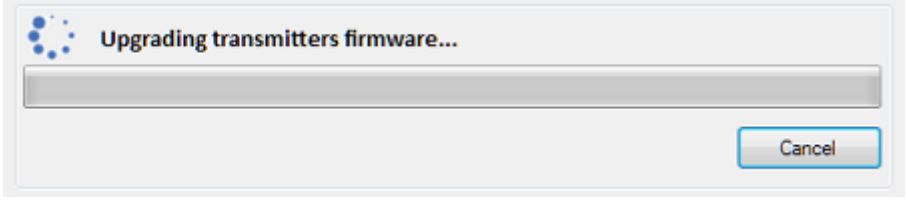


7. Click the **[Listen]** button to listen to transmissions from SE transmitters. The **[Listen]** button is now disabled.
8. Perform a transmitter test within sight of the SE coordinator. The SE transmitter will emit a series of beeping tones (1 short beep tone, with an interval, followed by 3 consecutive short beep tones) repeatedly. The SE transmitter information appears in the **SE Transmitters** grid view. If the version of the SE transmitter is the same as the version of

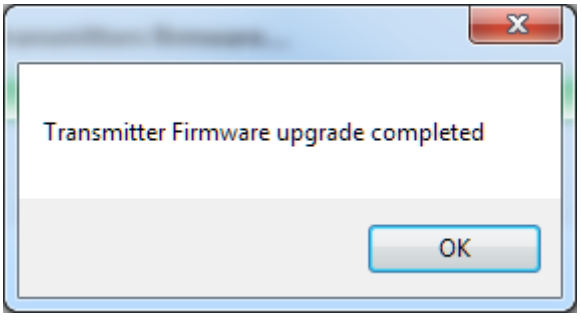
the firmware that is uploaded at the start, the SE transmitter row will be grayed out and disabled.



9. Repeat steps 8 for other SE transmitters if required.
10. To start upgrading the SE transmitter firmware, click the **[Start]** button. An indicator bar appears on screen to display the progress of the firmware upgrade. The beeping tone changes to continuous single beep tones. The red and green LED of the SE coordinator will be turned on for the entire duration of upload. To abort the upgrade, click the **[Cancel]** button.



11. Upon completion of the firmware upgrade, the SE transmitter emits a rapid succession of beeping tones for 1 second, indicating that the firmware upgrade is successful. A confirmation dialog message appears. The red and green LED of the SE coordinator will be turned off once upload has completed. Click the **[OK]** button to close the dialog message, and the indicator bar will disappear.



12. Perform the transmitter test again within sight of the SE coordinator. Confirm that the firmware version is correctly upgraded.

The firmware upgrade can be tweaked so that the process is optimized. The following parameters are available:

Element	Usage/Description
Version	Firmware version of the transmitter to be upgraded. This version is uploaded upon clicking the **[Firmware Upload]** button.

9 Troubleshooting coordinators, points and receivers

9.1 Troubleshooting reference

Symptoms	Probable Cause	Possible Solutions
SE coordinator not responding.	No power to SE coordinator.	If powered by Power over Ethernet (PoE), check that the Cat5e cable or the power sourcing equipment (for example, the network switch supplying the PoE) is not faulty.
		If powered by DC input, check power for 10.8V DC to 13.2V DC. If lower than 10 V or no voltage present, check wiring on power side of SE receiver, repair or replace cable.
	Defective SE coordinator.	If power is present and SE coordinator is not responding, replace SE coordinator.
SE coordinator intermittently not responding.	Moisture on circuit board.	Seal housing where moisture is entering enclosure. Replace SE coordinator until the old one dries out.
	Bad splice to SE coordinator.	Check all splices to make sure cables are tight and not loose causing high resistant open.
	Defective SE coordinator.	If power is present and SE coordinator is intermittently not responding, replace SE coordinator.
SE coordinator LEDs not working.	Defective SE coordinator.	Replace the SE coordinator.
SE coordinator LEDs all lighted up.	Incorrect address.	Check that addresses of SE coordinator and the SE receivers are correct. If addresses are correct, replace SE coordinator.

Table 9.6: SE coordinator issues

Symptoms	Probable Cause	Possible Solutions
Single SE receiver not responding in a connected bus network.	Incorrect address.	Check the address of SE receiver configured on the dip switch.
	No power to SE receiver.	Check power for 10.8 V DC to 13.2 V DC. If lower than 10 V or no voltage present, check wiring on power side of SE receiver, repair or replace cable.
	Defective SE receiver.	If power is present and address switch is configured correctly, replace SE receiver.
Single SE receiver intermittently not responding.	SE receiver is located past the 1000 m (3300 ft) maximum cable run.	Re-position the SE receiver within the recommended spacing.
	Moisture on circuit board.	Seal housing where moisture is entering enclosure. Replace SE receiver until the old one dries out.
	Bad splice to SE receiver.	Check all splices to make sure cables are tight and not loose causing high resistant open.
	Defective SE receiver.	If power is present and address switch is configured correctly, replace SE receiver.
SE receiver jamming.	Electrical equipment in area causing jamming on SE receiver.	Go to the software dialog **Setup** r**eceiver configuration**. Increase jamming threshold by one degree at a time until jamming stops and SE receiver returns to normal. If jamming persists after increasing level, relocate SE receiver or attempt to identify and minimize the jamming source.
SE receiver LEDs not working.	Defective SE receiver.	Replace the SE receiver.
SE receiver’s sounder not operating.	Switch 6 on dip switch CFG1 in “OFF” position on SE receiver.	Remove the cover, check dip switch CFG1 and make sure switch 6 is set to “ON”.

Symptoms	Probable Cause	Possible Solutions
	“Run Silent” is turned on in the Central Console software.	At the Central Console, select menu **Setup** > **Transponder Parameter** dialog and un-check the **Run Silent** checkbox.
	Defective SE receiver.	If the sounder still does not operate after performing the steps above, replace the SE receiver.

Table 9.7: SE receiver issues

9.2 Exporting and importing the Transponder Database

The following sections describe the steps to export and import data from and into the **Transponder Database**. Only users or operators who are assigned the minimum Authority Level of “Install” is able to view the **Transponder Database**. The file type supported is the XML file format.

Notice!
If extensions for known file types are enabled, this could affect the export and import operations of the database. These extensions should be hidden from view.
For Windows 7, open **Windows Explorer**. From the menu bar, click **Tools > Folder options** menu item. The **Folder Options** window appears. Click the **View** tab. Under the **Advanced settings** tree, look for the **Hide extensions for known file types** option. Ensure that the checkbox is **selected**.
For Windows 10, open **File Explorer** (This PC). From the menu bar, click **View** menu item to view the ribbon menu. Ensure that the checkbox of the **File name extensions** option is **not selected**.

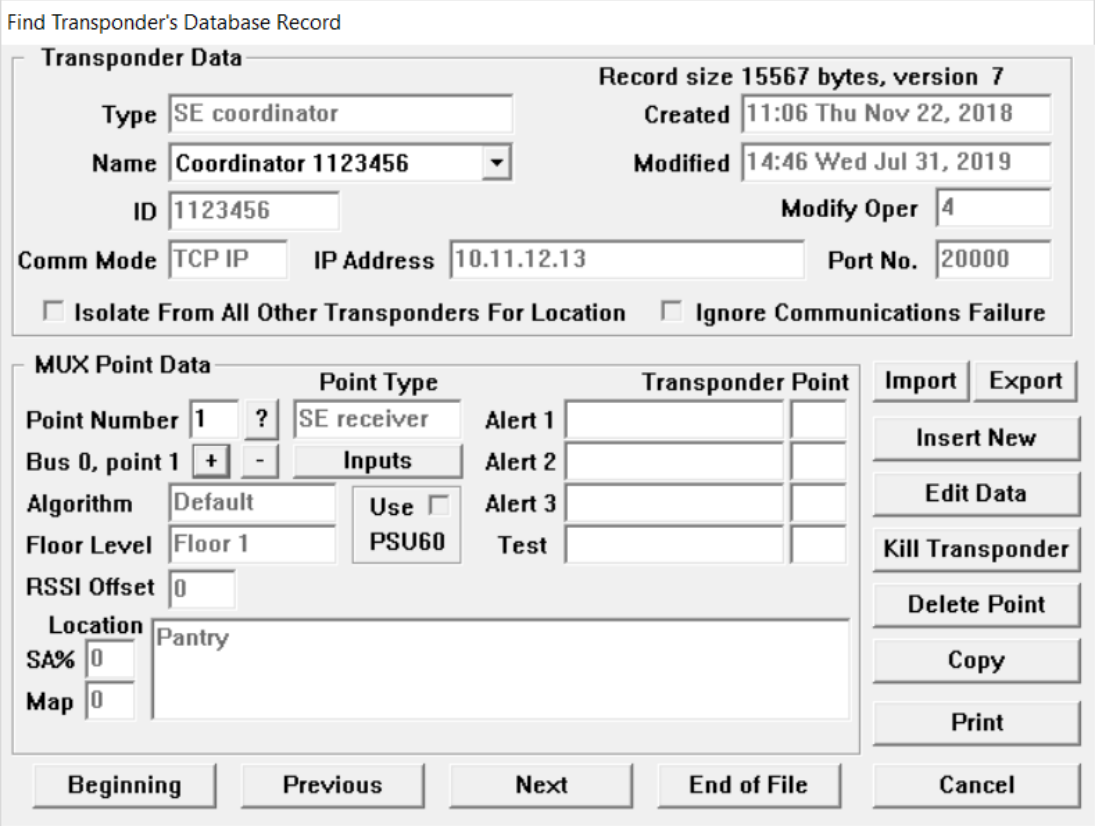


Figure 9.1: Find Transponder's Database Record dialog

9.2.1 The XML file format

Notice!
Area data of the transponders is supported in the XML file format.

The XML tree consists of 3 main elements, namely the *<Transponder>*, *<Receivers>* and *<Areas>* elements. The *<Transponder>* element is the parent element, with child elements *<Receivers>* and *<Areas>*. The *<Receivers>* element has a sub element *<Receiver>*. The *<Areas>* element has a sub element *<Area>* which contains another level of sub element *<ProtectedAreaPoints>*.

Below is an example of a typical tree with an empty structure:

```
<Transponder>
    <Receivers>
        <Receiver />
    </Receivers>
    <Areas>
        <Area>
            <ProtectedAreaPoints />
        </Area>
    </Areas>
</Transponder>
```

9.2.2 Exporting the Transponder Database

To export data from the **Transponder Database**, go to menu **File > Transponder Database** dialog, and click the **[Export]** button.

Notice!
The export operation does not change the existing records in **Transponder Database**.

A file dialog appears for you to choose the folder where you wish to save the file in, and provide a name for the file.

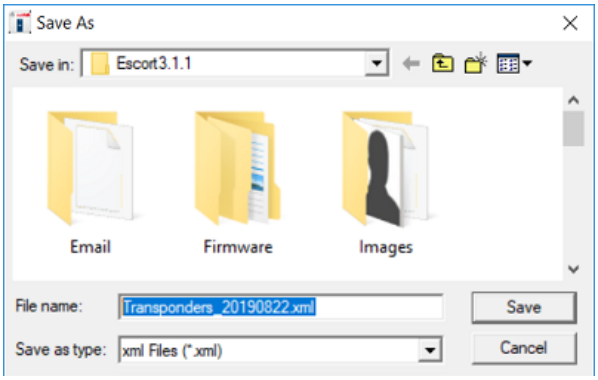


Figure 9.2: Export file dialog

If you wish to abort the task, click the **[Cancel]** button. Otherwise, click the **[Save]** button to export the **Operator database**. If a file of the same name already exists, a confirmation dialog appears asking if you wish to replace the file.

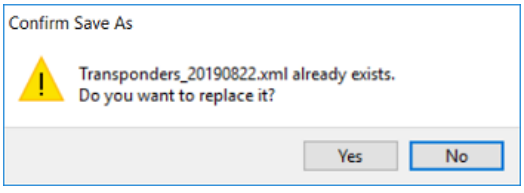


Figure 9.3: File replace confirmation dialog

Click the **[No]** button to abort and return to the file dialog box where you can choose a different name for the file. Otherwise, click the **[Yes]** button to proceed with replacement of the file. Be patient, as it may take a while, and watch for the disk activity to stop. If the export is successful, a confirmation dialog appears. You will find the file in the specified folder.

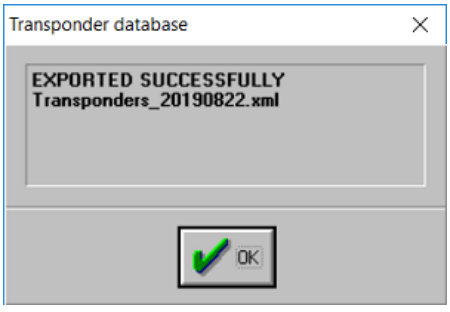


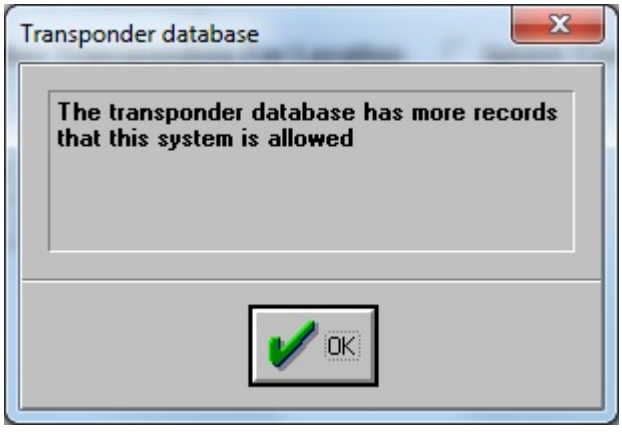
Figure 9.4: Transponder Database successfully exported dialog

9.2.3 Importing the Transponder Database

To import data into the **Transponder Database**, the file to imported must already be prepared in the XML file format. Go to menu **File > Transponder Database** dialog, and click the **[Import]** button.

Notice!
There is no way to undo the operations. Therefore, it is recommended to **perform a database backup** prior to starting the task. Upon completion of the task, verify the updated data before the new database is placed in service. If there are problems, restore the **Transponder Database** from the backup.

Notice!
Important!
Proceeding with the import operation will delete all existing records in **Transponder Database**. The record entries in import file are then imported to the **Transponder Database,** validated by the **Transponder ID**.
The number of record entries that is imported is subject to the number of transponders allowed for the purchased license. You can find this limit in the menu **About > About** dialog. If this limit is reached during the import, a pop-up message appears to inform the user.



A popup dialog appears asking for the file to be imported. Click the **[Cancel]** button to abort if you are still unsure. Otherwise, navigate the folders, select the file and click the **[Open]** button.

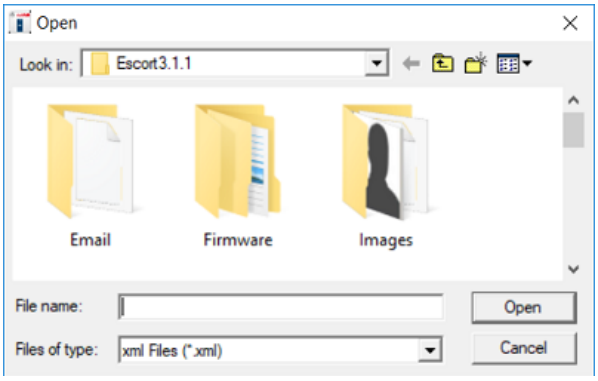


Figure 9.5: Import file dialog

A popup dialog appears, asking for confirmation to proceed with the import or to abort the operation. Click the **[No]** button to abort if you are still unsure. Click the **[Yes]** button to proceed with the import.

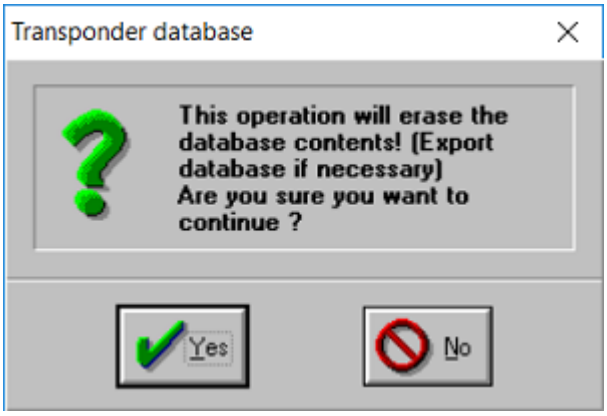


Figure 9.6: Import confirmation dialog

Be patient, as it may take a while, and watch for the disk activity to stop. If the data is imported successfully, a popup confirmation dialog appears. If the data is not imported successfully, a popup error message appears. The error message will indicate the likely cause of the import to fail.

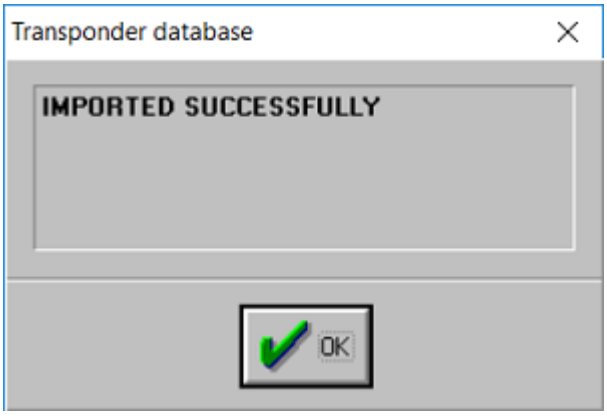


Figure 9.7: Transponder Database successfully imported dialog

9.3 System Preferences

The **System Preferences** dialog under the **Setup** menu contains a number of settings that govern the behavior of the Security Escort system.

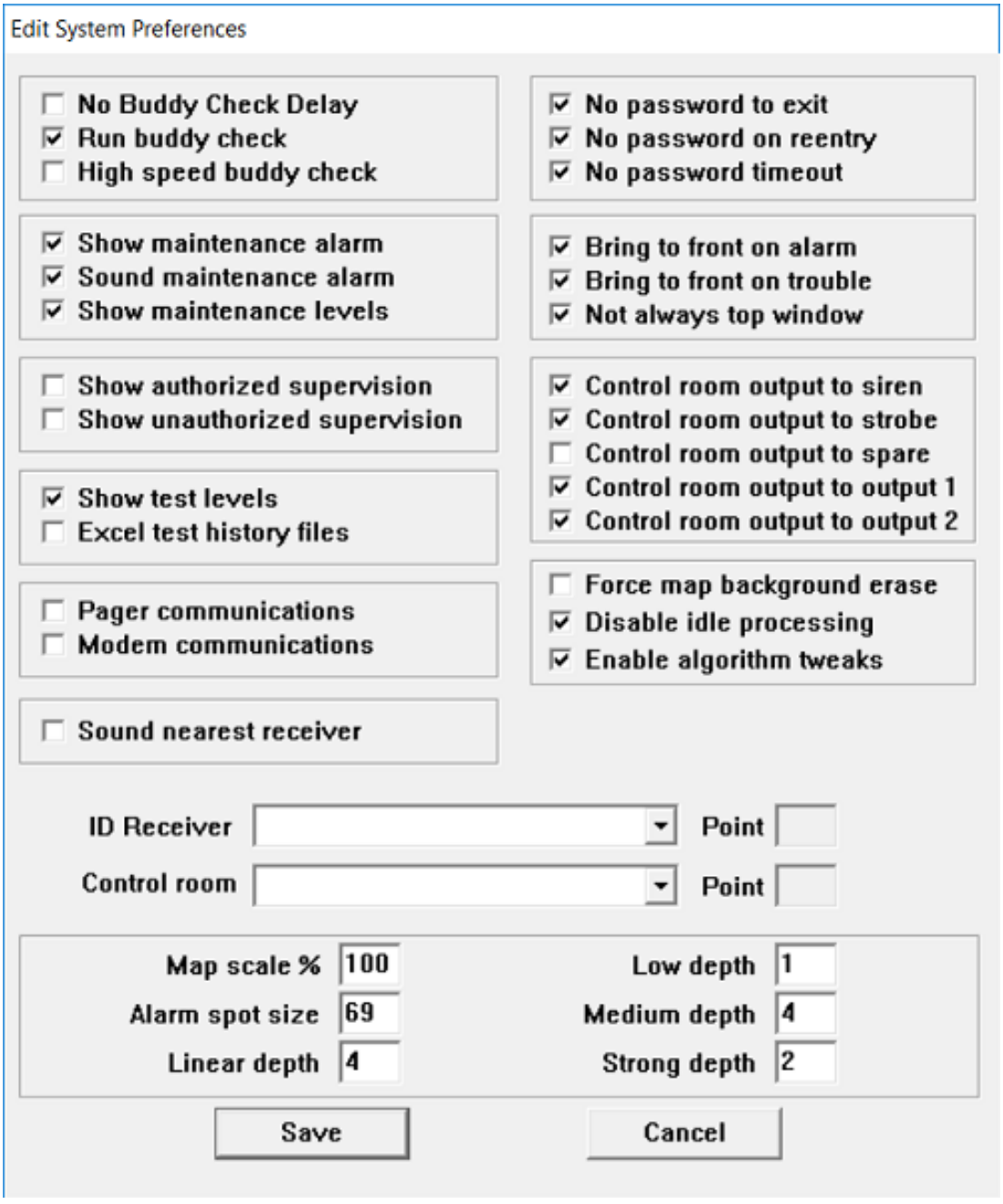


Figure 9.8: System Preferences dialog

Most of the options given are simple checkboxes. To activate or deactivate the option given, click on the checkbox adjacent to the text. A check mark appears in the checkbox adjacent to activated option, empty checkboxes signify deactivated options. Some options in the **System Preferences** dialog require numerical values. To change the current values, click the text box containing the values, then type in a new value.
Click the **[Save]** button to save the changes, and exit the **System Preferences** dialog. Click the **[Cancel]** button to exit the **System Preferences** dialog if no changes have been made. If there are changes, clicking the **[Cancel]** button opens a dialog window to confirm saving the changes. Click the **[Yes]** button to save the changes, or the **[No]** button to discard the changes, and exit the **System Preferences** dialog. Click the **[Cancel]** button to return to the **System Preferences** dialog to continue with the changes.

Element	Usage/Description
No Buddy Check Delay	If the checkbox is selected, the software does not impose the hour between buddy checks from the same SE receiver. Normally, this checkbox is not selected, and should not be selected for live systems.
Run buddy check	This checkbox enables and disables the buddy check feature of the system. When selected, the Central Console periodically issues a command (via the SE coordinator) to each SE receiver, to activate its on-board transmitter. The Central Console then compares the signals received from neighboring SE receivers to the results of earlier buddy checks, thus identifying SE receivers, which appear to have changed sensitivity.
High speed buddy check	Checking this checkbox allows the buddy check to run as fast as it can. Normally, only one buddy check transmission is sent each minute.
Show maintenance alarm	Normally, when a maintenance alarm is received from a maintenance transmitter, the red LED on all SE receivers will flash for 5 seconds hearing the transmission. If this checkbox is selected, the SE receiver with the loudest reception level will turn on both the red and green LED for 5 seconds.
Sound maintenance alarm	If this checkbox is selected, the SE receiver with the loudest reception level on a maintenance alarm will turn on its sounder for 5 seconds. Normally, this checkbox is not selected.
Show maintenance levels	Selecting this checkbox causes the Central Console to display the signal strength measured by each SE receiver as a number (from 1 to 15) inside the SE receiver icon when maintenance alarms are displayed. Otherwise, the floor number is displayed.
Show authorized supervision	Selecting this checkbox causes the Central Console to supervise only authorized supervision alarms.
Show unauthorized supervision	Selecting this checkbox causes the Central Console to supervise unauthorized supervision alarms.
Show test levels	Selecting this checkbox causes signal strength levels to appear on the SE receiver icons when displaying tests on the main map screen. Otherwise, the green test icons are displayed.
Excel test history files	**Do not select this checkbox in a live Security Escort System.** It is for diagnostic Engineering testing only.
Pager communications	Normally, this checkbox is not selected. If selected, the communication to the dial-up wide area paging system through the modem will be displayed on the history screen. This function is only used to diagnose communication problems to the paging system.

Element	Usage/Description
Modem communications	Normally, this checkbox is not selected. If selected, the communication to the modem will be displayed on the history screen. This function is only used to diagnose communication problems with the modem.
Sound nearest receiver	Normally, this checkbox is not selected. If selected, the nearest receiver will be sounded during an alarm. In the event that two or more receivers received the same level of signal strength, two of the receivers will be sounded.
No password to exit	If selected, the software will exit without asking for a password. Normally, this checkbox is not selected.
No password on reentry	If selected, the software will not ask for a password when the user switches to another program and then switches back to the still running Security Escort. Normally, this checkbox is not selected.
No password timeout	If selected, the software will not ask for a password after the screen saver kicks in. Normally, this checkbox is not selected.
Bring to front on alarm	If selected, the software will jump to the front when a new alarm occurs. Normally, this checkbox is selected.
Bring to front on trouble	If selected, the software will jump to the front when a trouble dialog pops up. Normally, this checkbox is selected.
Not always top window	If the Security Escort System is intended to be the only application running on this computer, leave this checkbox unselected. This will prevent other applications from taking over the screen. The Security Escort System will always be present. If the Security Escort System is to be run on a computer with other applications, select this checkbox and it will share the computer's display with all other Windows applications. After selecting this checkbox, stop and restart the Security Escort System for this feature to take effect. This checkbox is unselected by default.
Control room output to siren	If selected, whenever there is an unacknowledged alarm, the siren output of the **Control room / Point** fields will operate.
Control room output to strobe	If selected, whenever there is an unacknowledged alarm, the strobe output of the **Control room / Point** fields will operate.
Control room output to spare	If selected, whenever there is an unacknowledged alarm, the spare output of the **Control room / Point** fields will operate.
Control room output to output 1	If selected, whenever there is an unacknowledged alarm, output 1 of the **Control room / Point** fields will operate. This option is disabled if either one of the **Turn on Output 1** or **Turn on Output 2** field is not "None" in the **Security Preferences** dialog.
Control room output to output 2	If selected, whenever there is an unacknowledged alarm, output 2 of the **Control room / Point** fields will operate. This option is disabled if either one of the **Turn on Output 1** or **Turn on Output 2** field is not "None" in the **Security Preferences** dialog.

Element	Usage/Description
Force map background erase	Use this checkbox to erase the map screen. It should only be selected if there are problems with icons not being cleared properly from the screen. Otherwise, it will cause the screen to flicker.
Disable idle processing	Normally, this software registers with Windows to return to the Security Escort system if there is any idle time. The Security Escort system can use it to speed up its response to serial communications and other background tasks. If selected, the software will not register for the idle time. Normally, this checkbox is not selected. Windows can show the amount of time each application (task) is taking. When this checkbox is not selected, it may appear that Security Escort system is “hogging” the processor resources. This is not true, because the Security Escort system is only taking the time that Windows gives it through the idle process. To prove this, select this checkbox. The amount of time that the Security Escort System needs will drop dramatically, and it will continue to operate normally (same communications responses will be slowed by several hundred milliseconds).
Enable algorithm tweaks	Selecting this checkbox causes the **Map scale**, **Alarm spot size**, and **Linear/Low/Medium/Strong depth** settings to be visible on this dialog. It also controls the display of the **SA%** and **Algorithm** settings in the **Edit Transponder**’**s Database Record** dialog.
ID Receiver / Point	Assign an SE receiver for automated transmitter exchanges. The Security Escort system contains a feature where the transmitter identification number can be automatically entered into the **Subscriber Database**. This is used for entering transmitters when issuing them to subscribers for the first time, and for transmitter exchanges. This automatic capture of the transmitter identification number is accomplished by performing certain procedural steps (see the Security Escort Operation Manual) and then using the transmitter to make a test transmission in close proximity to a designated SE receiver, usually located close to the Central Console. By capturing the transmitter identification number in this manner, keystroke errors are avoided during database entries and changes. The SE receiver chosen for this purpose is designated as the **ID Capture Receiver**. To assign the **ID Capture Receiver**, its SE coordinator name and its **Point Number** are selected using the **ID Receiver** and **Point elements.**
Control room / Point	The Security Escort system software can activate an output to attract attention, when there is an alarm that has been received, and no operator has responded to the system yet. To assign the output, select the SE coordinator that it is connected to, and the **Point Number**.

Element	Usage/Description
Map scale %	This value changes the scale that the maps are presented with. It is not intended for normal operation, but typically used for testing to allow more of the map to be seen. The setting may range from 30% to 400%. The **Enable algorithm tweaks** checkbox must be selected for this to be visible.
Alarm spot size	This setting changes the size of the yellow dot that marks the calculated location of the alarm. The settings range from 19 to 76 (half to double the default alarm dot size). It is best to set the size of the alarm spot so that represents a diameter of 15.24 m (50 ft.) on the displayed map, as this is the area where the transmission of the alarm most likely took place. The **Enable algorithm tweaks** checkbox must be selected for this to be visible.
Linear depth	This setting controls the involvement of SE receivers in the alarm location calculation only when the “Linear Algorithm” is being used. The setting can range from 0 to 6 (default is 2). When set to 0, only the SE receivers closer to the actual location of the alarm will be considered in the location calculation. As the setting is raised, more distant SE receivers will be included in the alarm calculation. Typically, lower settings are better than higher settings. This setting should be changed if there are known problems with the location using the “Linear Algorithm”. The **Enable algorithm tweaks** checkbox must be selected for this to be visible.
Low depth	This setting controls the involvement of receivers in the alarm location calculation only when the “Low Algorithm” is being used. The setting can range from 0 to 6 (default is 2). When set to 0, only the receivers closer to the actual location of the alarm will be considered in the location calculation. As the setting is raised, more distant receivers will be included in the alarm calculation. Typically, lower settings are better than higher settings. Change this setting if there are known problems with the location using the “Low Algorithm”. The **Enable Algorithm Tweaks** checkbox must be checked for this to be displayed.
Medium depth	This setting controls the involvement of SE receivers in the alarm location calculation only when the “Medium Algorithm” is being used. The setting can range from 0 to 6 (default is 2). When set to 0, only the SE receivers closer to the actual location of the alarm will be considered in the location calculation. As the setting is raised, more distant SE receivers will be included in the alarm calculation. Typically, lower settings are better than higher settings. Change this setting if there are known problems with the location using the “Medium Algorithm”. The **Enable algorithm tweaks** checkbox must be selected for this to be visible.
Strong depth	This setting controls the involvement of SE receivers in the alarm location calculation only when the “Strong Algorithm” is being used. The setting can range from 0 to 6 (default is 2). When set to

Element	Usage/Description
	0, only the SE receivers closer to the actual location of the alarm will be considered in the location calculation. As the setting is raised, more distant SE receivers will be included in the alarm calculation. Typically, lower settings are better than higher settings. Change this setting if there are known problems with the location using the “Strong Algorithm”. The **Enable algorithm tweaks** checkbox must be selected for this to be visible.
[Save]	Save the changes and close the dialog window.
[Cancel]	Cancel the changes and close the dialog window.

9.4 Security Preferences

The **Security Preferences** dialog is used to make important settings that govern how the Security Escort system reacts in the event of alarm and test transmissions from the subscribers’ transmitters. This dialog is available only to the Security Director or his/her key operator.

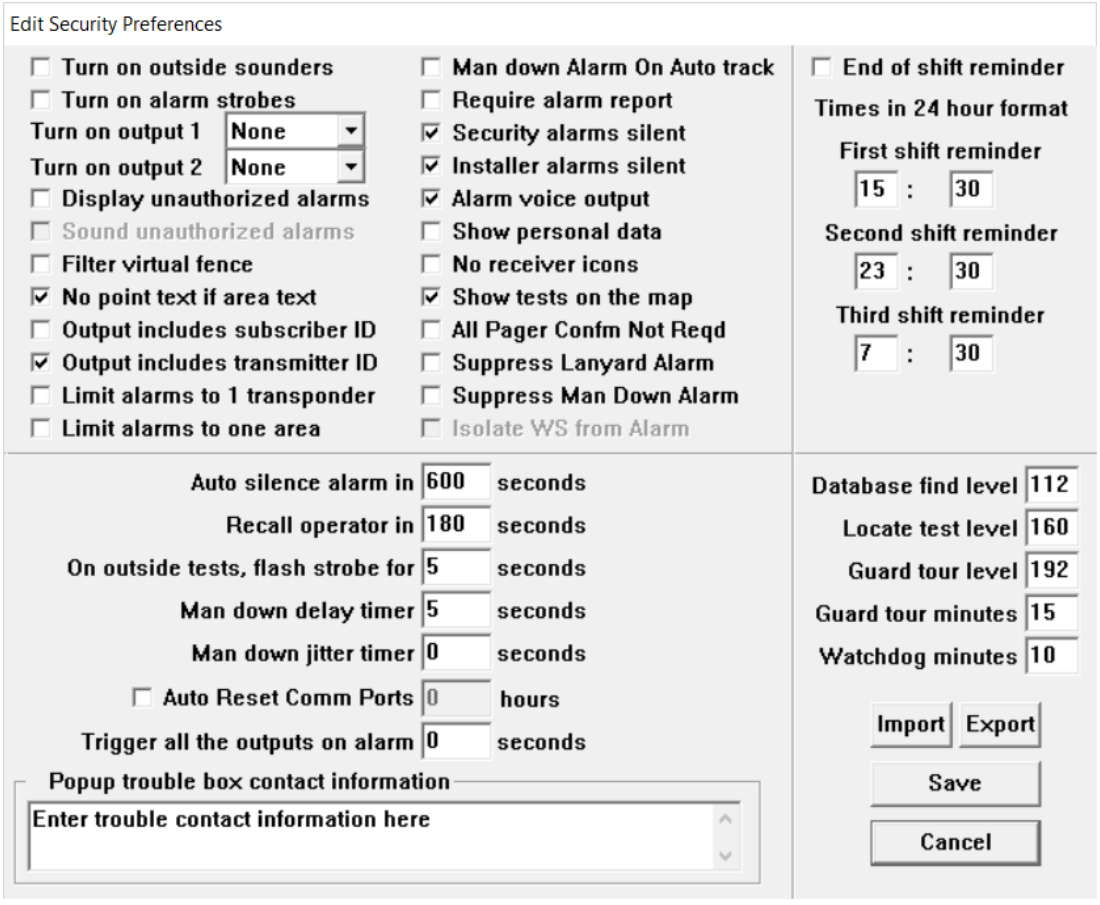


Figure 9.9: Security Preferences dialog

Most of the options given are simple checkboxes. To activate or deactivate the option given, click on the checkbox adjacent to the text. A check mark appears in the checkbox adjacent to activated option, empty checkboxes signify deactivated options. Some options in the **Security Preferences** dialog require numerical values. To change the current values, click the text box containing the values, then type in a new value.

Click the **[Save]** button to save the changes, and exit the **Security Preferences** dialog. Click the **[Cancel]** button to exit the **Security Preferences** dialog if no changes have been made. If there are changes, clicking the **[Cancel]** button opens a dialog window to confirm saving the changes. Click the **[Yes]** button to save the changes, or the **[No]** button to discard the changes, and exit the **Security Preferences** dialog. Click the **[Cancel]** button to return to the **Security Preferences** dialog to continue with the changes.

Element	Usage/Description
Turn on outside sounders	Some security directors prefer that all alarms be silent, while others choose to employ sirens. Select this checkbox to activate the sirens on Alert Units and SE coordinators to sound in the event of an alarm. Temporarily deactivating the sounders may be necessary during maintenance.
Turn on alarm strobes	Select this checkbox so that the strobe lights on the Alert Units and SE coordinators will flash in the event of an alarm.
Turn on output 1	Select the type of alarm from the drop-down list to activate output 1. The options are: "None" (default), "Duress", "Lanyard", "Mandown" and "All". Only when configured, output 1 of the SE coordinator or SE receiver in **Alert 1**, **Alert 2** and **Alert 3** of the **Transponder Database** will be turned on. **Note:** If the selected alarm type is not "None", the options for **Control room output to output 1** and **Control room output to output 2** in **System Preferences** are disabled.
Turn on output 2	Select the type of alarm from the drop-down list to activate output 2. The options are: "None" (default), "Duress", "Lanyard", "Mandown" and "All". Only when configured, output 2 of the SE coordinator or SE receiver in **Alert 1**, **Alert 2** and **Alert 3** of the **Transponder Database** will be turned on. **Note:** If the selected alarm type is not "None", the options for **Control room output to output 1** and **Control room output to output 2** in **System Preferences** are disabled.
Display unauthorized alarms	This checkbox determines if "unauthorized" alarms are to be displayed on the Central Console. Unauthorized alarms are those triggered by transmitters not currently registered in the **Subscriber Database**. These could be transmitters that have been removed from the database because they were lost or stolen, they could be transmitters not yet issued, or they could be transmitters issued to subscribers at another Security Escort system. Typically, this checkbox should not be selected.
Sound unauthorized alarms	This function is not available for this release.
Filter virtual fence	If some false alarms are generated, this checkbox is selected to reduce the number of these false alarms. The actual alarms will then be delayed by the supervision period of the transmitter.

Element	Usage/Description
No point text if area text	This checkbox affects the location text shown on the alarm screen. If this checkbox is selected, and the alarm is determined to be within a predefined area, then only the area text will be displayed (any SE receiver location text will be suppressed). Typically, this checkbox should be selected.
Output includes subscriber ID	If this checkbox is selected, any time the system prints or displays text for an alarm or test, the subscriber's ID number will also be displayed. Otherwise, the subscriber's ID will not be shown.
Output includes transmitter ID	If this checkbox is selected, any time the system prints or displays text for an alarm or test, the transmitter ID number will also be displayed. Otherwise the transmitter ID will not be shown. Typically, this checkbox would not be selected.
Limit alarms to 1 transponder	This checkbox should not be selected. It is used only in a system where all transponders operate in areas that are separate from each other. It would prevent all interactions between SE receivers on different transponders. Typically, this would be very undesirable and there is now a selection on an individual transponder basis to accomplish this feature.
Limit alarms to one area	This checkbox should not be selected. It is only used in a system where all transponders operate in areas that are separate from each other.
Man down Alarm On Auto track	If this checkbox is selected, any time there is a man down alarm, the auto track functionality will be activated. Otherwise there is no auto track functionality for the alarm.
Require alarm report	If this checkbox is selected, the operator will be prompted to complete an alarm report when the alarm is reset from the screen. If the responding officer is required to complete the report, or if no system report is desired, this checkbox should not be selected. If the operator should complete the report, then select this checkbox.
Security alarms silent	If this checkbox is selected, alarms transmitted by "Security" or "Watchman" transmitters are to be "silent", alerting the operator at the Central Console, but not sounding the sirens of the Alert Units or the sounders in the SE receivers.
Installer alarms silent	If this checkbox is selected, alarms transmitted by transmitters issued to installing company representatives and visitors are to be "silent", alerting the operator at the Central Console, but not sounding the sirens of the Alert Units or the sounders in the SE receivers. Typically, this checkbox would be checked.
Alarm voice output	If this checkbox is selected, predefined sound (.WAV) files can be played at the alarm console for specific alarm types. Typically, this checkbox would not be selected.

Element	Usage/Description
Show personal data	If this checkbox is selected, personal height, build, hair and eye color data will be displayed on the alarm screen.
No receiver icons	If this checkbox is selected, individual SE receiver icons will not be shown on the alarm map display. Typically, this checkbox would be selected.
Show tests on the map	If this checkbox is selected, tests from subscriber's transmitter will be displayed on the normal map screen as **OK** or **FAIL** icons, signifying a successful test by a valid subscriber or an attempted test transmission from a transmitter not in the **Subscriber Database**. This checkbox doesn't affect the display the subscriber receives from a SE receiver or Alert Unit's strobe. Typically, this checkbox would be selected.
All Pager Confm Not Reqd	If this checkbox is selected, the confirmation pager message is not sent to the any of the pagers when the alarm is acknowledged by an acknowledgement transmitter.
Suppress Lanyard Alarm	If this checkbox is selected, the lanyard alarm is suppressed and not reported.
Suppress Man Down Alarm	If this checkbox is selected, the man down alarm is suppressed and not reported.
Isolate WS from Alarm	This function is not available for this release.
Auto silence alarm in 'X' seconds	This field determines the length of time that the sirens and horns will sound, before being automatically silenced by the Central Console. When the sounders are automatically silenced in this way, the Central Console remains in its "Alarm" mode. The numerical value is in seconds, and it can be set between 0 and 9999. Typically, this value would be set to prevent violating local noise ordinances and it defaults to 240 seconds (4 minutes).
Recall operator in 'X' seconds	This field determines the length of time before a "Recall" alert is issued to the operator at the Central Console when an alarm is being displayed. If neither the mouse nor any key has been actuated for the specified length of time, the Console will trigger the "Alarm" sound once. This feature prevents inadvertently ignoring an active alarm event. The numerical value is in seconds, and it can be set between 0 and 240. Typically, this would be set to 60 seconds.
On outside tests, flash strobe for 'X' seconds	This field controls the approximate length of time the strobe on an Alert Unit will flash to signify a successful transmitter test. The value is in seconds, and can be set between 0 and 15. Typically, it is set to 5 seconds.
Man down delay timer 'X' seconds	This field controls the time that a transmitter must be in a man down condition before a man down alarm is displayed. Typically it would be set to 5 seconds. Setting this value too short will cause inadvertent man down alarms to be generated.

Element	Usage/Description
Man down jitter timer 'X' seconds	This field controls the time that a transmitter will not be considering any man down alarm if man down alarm is received immediately after restore and before jitter time expire. This setting will not be used in normal system.
Auto Reset Comm Ports 'X' hours	This checkbox controls whether all the comm ports in the system will be automatically reset after the configured time duration. This setting is used only if any communication failure is observed and should not be used unnecessarily.
Trigger all the outputs on alarm 'X' seconds	This option turns on all outputs of the SE coordinators, and alert units for the duration configured (1-255 seconds) when alarm is generated. If someone acknowledges an alarm during this duration, all these outputs will be turned off. Otherwise, after this duration has lapsed, all these outputs will be turned off automatically. If this value is set to 0, the system will trigger the outputs during alarms in the default normal behavior.
Popup trouble box contact information"	Each yellow, pop-up trouble box that is displayed on the Central Console advises of system problems, containing specific instructions for the operator. Entries in this text box will be displayed in the pop-up trouble boxes whenever a system problem occurs that requires attention. This information usually includes the name and telephone number of the designated Security Escort maintenance technicians.
End of shift reminder	If this checkbox is selected, a prompt will appear on the Central Console screen every 5 minutes for 30 minutes, prior to the end of each shift, if there are incident reports that have not yet been completed. It is intended for responding officers to complete alarm reports before the end of their shift.
First, Second, Third shift reminder	The entries in these fields are the times (24-hour clock) at which the Central Console will prompt the operator that there is one or more incident reports that have not yet been completed. Prompts will be given only if the **End of Shift Reminder** option is selected.
Database find level	This is the minimum receive level (1-255) that must be heard before the system will automatically enter the transmitter in the **Subscriber Locate** dialog. It determines the distance the subscriber's transmitter must be within the specified ID capture SE receiver (set in the **System Preferences** dialog) before the system will recognize the test.
Locate test level	This is the minimum receive level (1-255) that must be heard before the system will accept a test generated by a transmitter other than a guard, to be printed with a location. It determines the distance the transmitter must be within from a SE receiver before the system will recognize the test and print the location. If the transmitter is too far away from the SE receiver, that SE receiver's green light will not be displayed, so the guard knows that they must move closer to the SE receiver for the test to register.

Element	Usage/Description
Guard tour level	This field is the minimum receive level (1-255) that must be heard before the system will accept a test generated by the guard's transmitter to be entered as a location in the guard tour report. It determines the distance the guard's transmitter must be within from a SE receiver before the system will recognize the test and create the guard tour entry. If the guard is too far away from the SE receiver, that SE receiver's green light will not be displayed, so the guard knows that they must move closer to the SE receiver for the test to register.
Guard tour minutes	This field controls the time spacing, in minutes, for entries of the guard's current location in the automatically generated guard tour report. Therefore, if set to 15 minutes, an entry will be generated each 15 minutes that the guard's transmitter is within range of the system.
Watchdog minutes	This field controls the time spacing, in minutes, for entries of the guard's current location in the automatically generated guard tour report. Therefore, if set to 10 minutes, an entry will be generated each 10 minutes that the guard's transmitter is within range of the system.
[Import]	Click this button to import the global preference settings in the XML file format.
[Export]	Click this button to export the global preference settings in the XML file format.
[Save]	Click this button to save the changes and close the dialog window.
[Cancel]	Click this button to abort the changes and close the dialog window.

9.5 Exporting and importing the global preference settings

The following sections describe the steps to export and import the global preference settings of the Security Escort system from the **Security Preferences** dialog. Only users or operators who are assigned the minimum Authority Level of "Install" is able to perform the export and import. The file supported is the XML file format.

9.5.1 Settings used in the XML file format

The attributes and settings of the following dialogs are used in the XML file format for the import and export feature.

Menu	Dialog
Utilities	Security Preferences
	System Defaults
	System Labels
	Print/Export System Reports
	Schedules

Menu	Dialog
	Alarm Groups
Setup	History filter
	Popup trouble filter
	Transponder parameter change
	System preferences
	Transponder comm port setup
	Remote setup
	Pager setup
	Pager setup
Printer	Select alarm printer
Network	System directories and network address

9.5.2 Exporting the global preferences setting

To export the global preference settings from the Security Escort system, go to menu **Utilities > Security Preferences** dialog, and click the **[Export]** button.

Notice!
The export operation does not change the existing settings in Security Escort.

A file dialog appears for you to choose the folder where you wish to save the file in, and provide a name for the file.

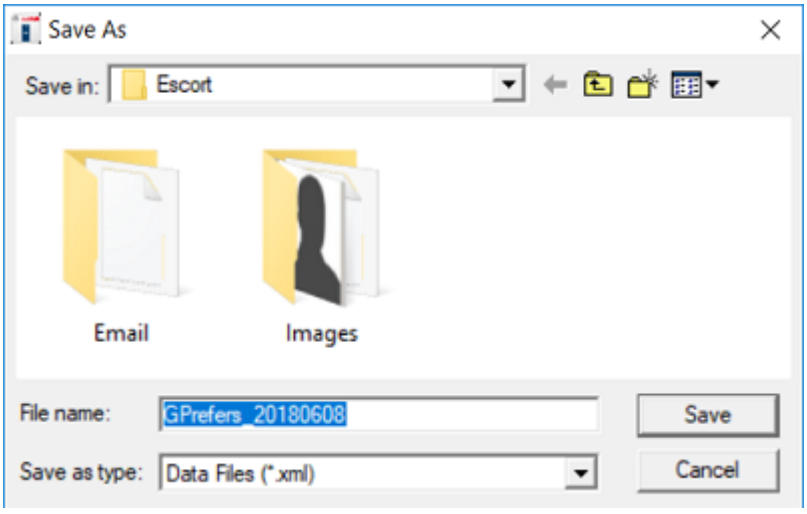


Figure 9.10: Export file dialog

If you wish to abort the task, click the **[Cancel]** button. Otherwise, click the **[Save]** button to export the global preferences setting. If a file of the same name already exists, a confirmation dialog appears asking if you wish to replace the file.

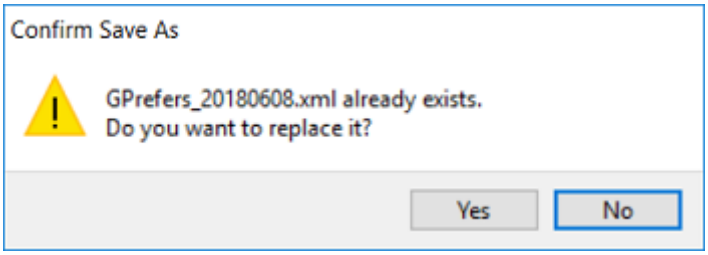


Figure 9.11: File replace confirmation dialog

Click the **[No]** button to abort and return to the file dialog where you can choose a different name for the file. Otherwise, click the **[Yes]** button to proceed with replacement of the file. If the export is successful, a confirmation dialog appears. You will find the file in the specified folder.

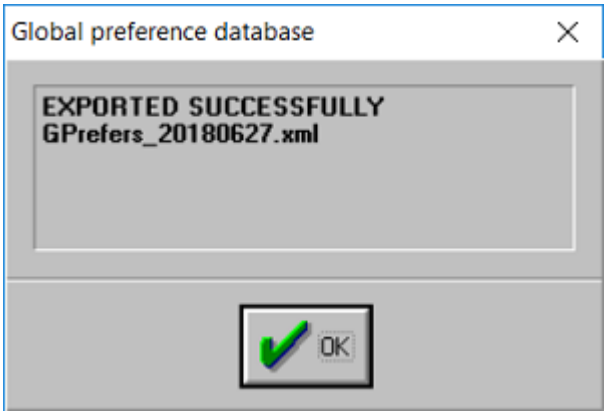


Figure 9.12: Global preferences successfully exported dialog

9.5.3 Importing the global preferences setting

To import the global preference settings into the Security Escort system, the file to imported must already be prepared in the XML file format. Go to menu **Utilities > Security Preferences** dialog, and click the **[Import]** button.

Notice!
This action is irreversible! There is no way to undo the operations.

A popup dialog appears asking for the file to be imported. Click the **[Cancel]** button to abort if you are still unsure. Otherwise, navigate the folders, select the file and click the **[Open]** button.

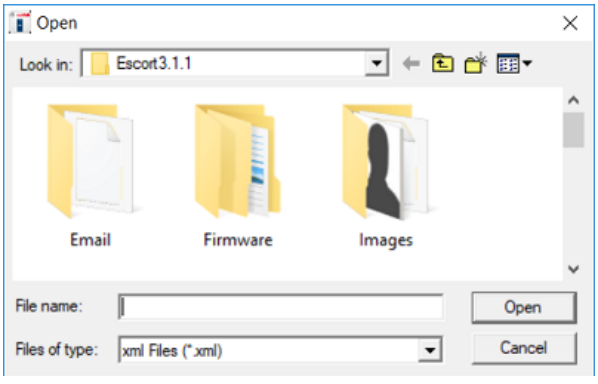


Figure 9.13: Import file dialog

A popup dialog appears, asking for confirmation to proceed with the import or to abort the operation. Click the **[No]** button to abort if you are still unsure. Click the **[Yes]** button to proceed with the import.

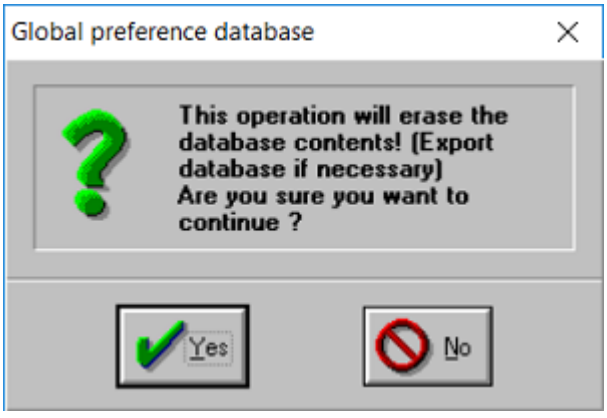


Figure 9.14: Import confirmation dialog

If the data is imported successfully, a popup confirmation dialog appears. If the data is not imported successfully, a popup error message appears. The error message will indicate the likely cause of the import to fail.

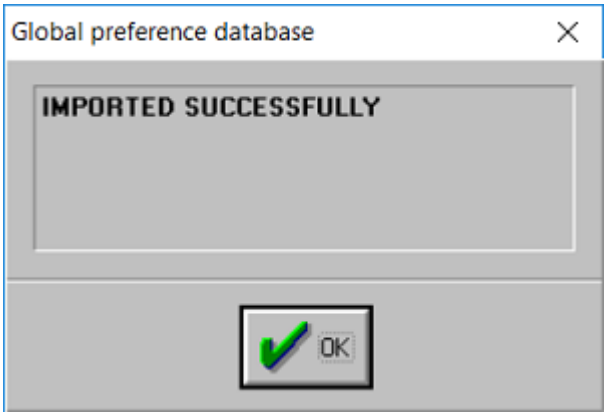


Figure 9.15: Global preferences imported successfully dialog

9.6 System Defaults

This dialog allows the names for each class of subscribers to be changed to match the specific application of this Security Escort system.

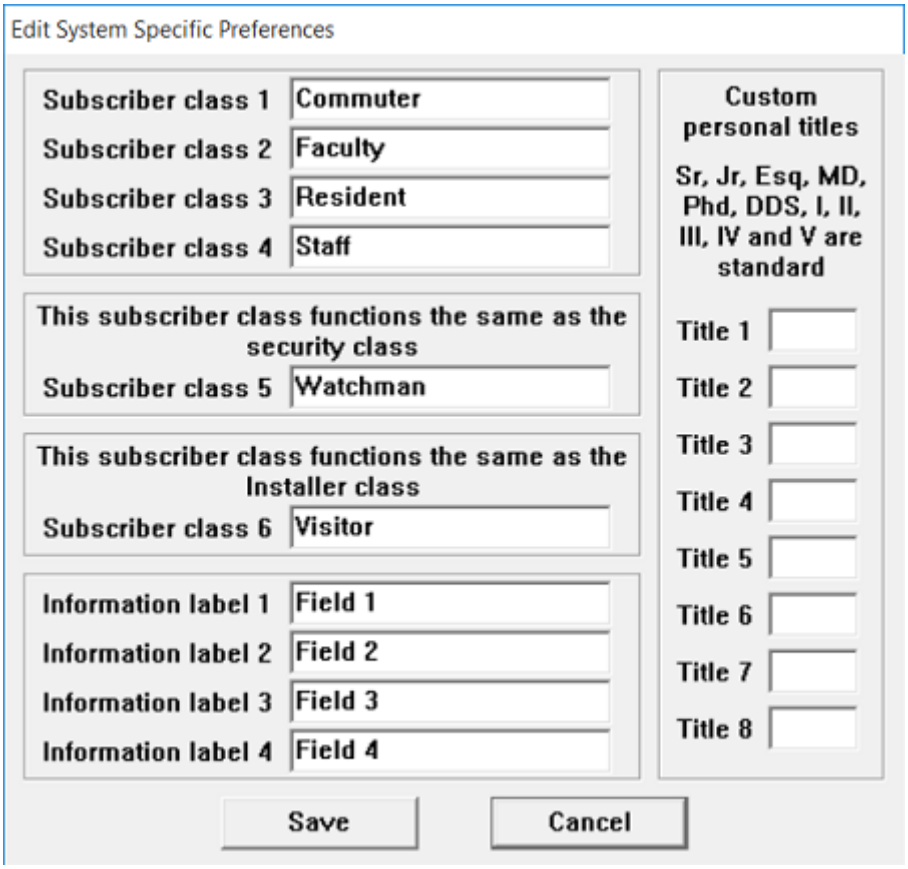


Figure 9.16: System Defaults dialog

Titles that are entered into the **Subscriber Name** field in the **Subscriber database** are entered here. The system alphabetizes the **Subscriber database** entries by last name. When a title is entered after the last name, the entry is alphabetized incorrectly by title. Entering the titles prevents this problem.

The labels for the four **Information label** in the **Subscriber database** are also changeable here.

9.7 System Labels

The alarm type definitions are customized to customer's requirements in this dialog window.

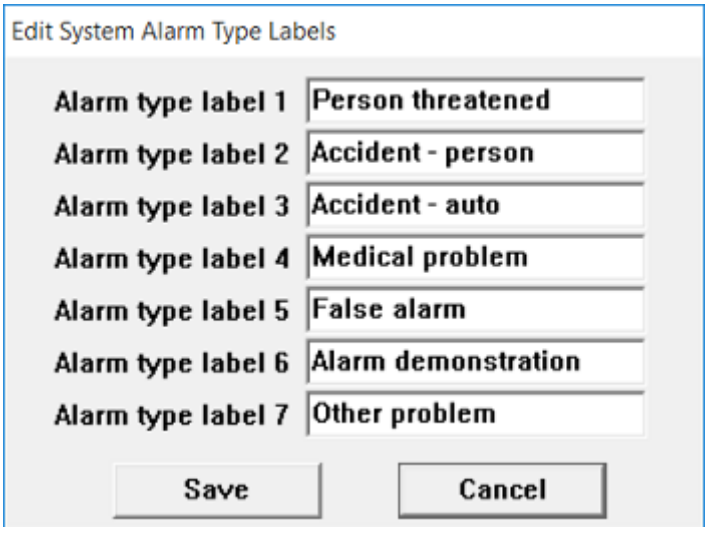


Figure 9.17: System Labels dialog

Overwrite the default labels by typing over the existing text. The length of the text is limited to maximum of 20 alpha numeric characters.

9.8 Subscriber Database

A subscriber is anyone who has been issued a transmitter. This database includes all transmitters assigned in the system, whether they are protecting people or things. The **Subscriber Database** is very similar to the **Operator Database**; the method by which the names and other information are stored is virtually identical.

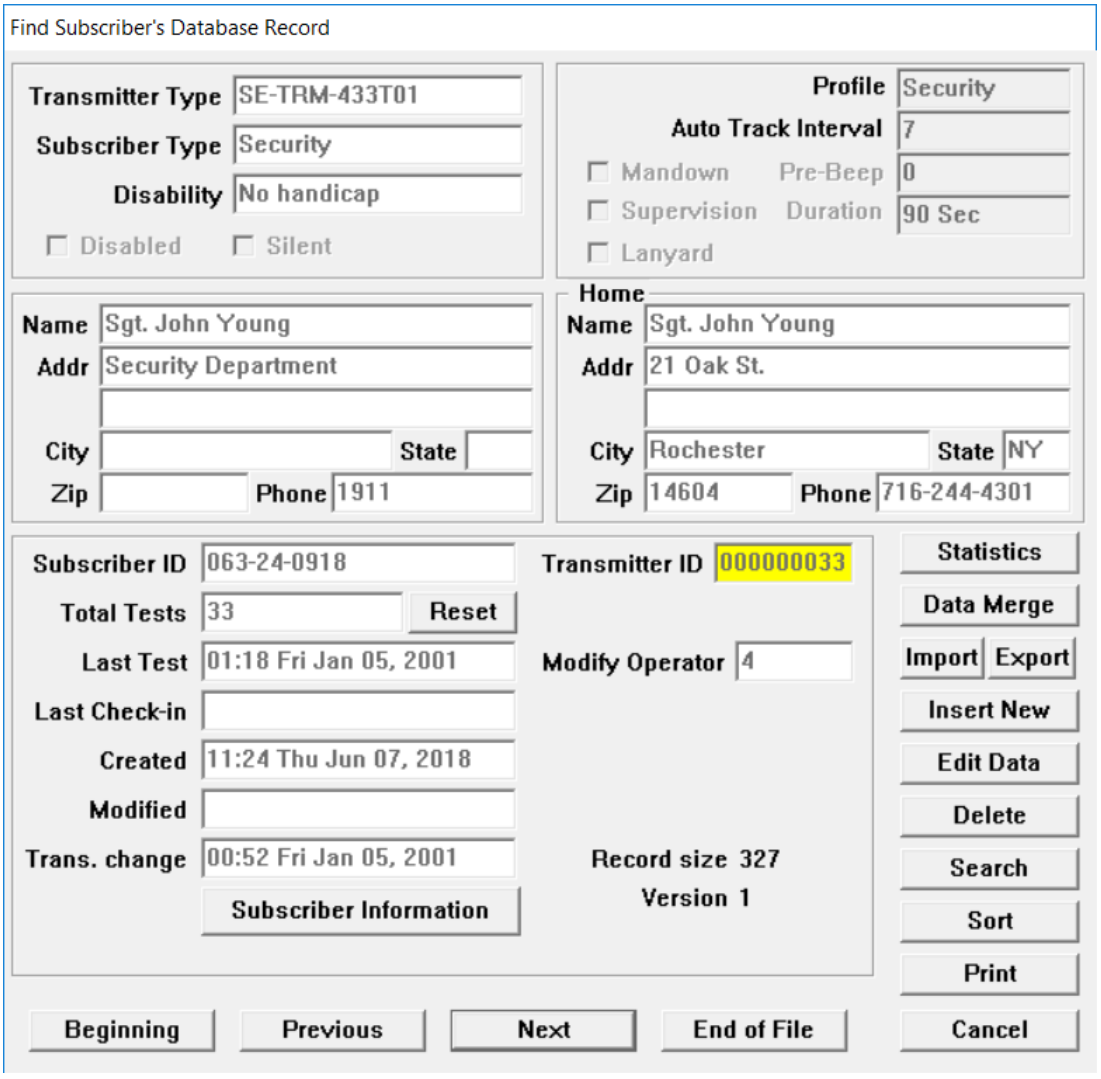


Figure 9.18: Find Subscriber's Database Record dialog

The information stored in a subscriber's file includes the person's name, local address and phone number, permanent address and phone number, subscriber identification number (typically the individual's Social Security number), the transmitter identification code (each transmitter has its own unique code which identifies the subscriber during tests and alarms), and the subscriber's classification (commuter, resident, faculty, staff, and so on).

Element	Usage/Description
[Reset]	Click the **[Reset]** button to clear the number of **Total Tests** count.

Element	Usage/Description
[Clear]	Click the **[Clear]** button to remove the **Low Battery** indication. This should only be done after the transmitter battery is replaced or a new transmitter is issued.
[Print]	Click the **[Print]** button to open the **Subscriber Print** dialog window.

9.8.1 Inserting a new Subscriber Database record

To create a new subscriber, the following information must be entered to complete the changes: subscriber name, subscriber identification number, and transmitter identification code. The computer does not allow the edit screen to be closed until all of the mandatory fields are completed. The accuracy of information in the **Subscriber Database** is very important: in the event that a subscriber transmits an alarm, the information displayed in the alarm screen is taken from this database. A faulty address could hinder security's response to an alarm.

Element	Usage/Description	
System Type	Select the option corresponding to the type of system that is installed. Different options will populate different fields for the transmitter accordingly.	
	Transponder	(default) Select this if the system is using the transponders. **Note: Transponder system will not be discussed in this manual. Please kindly refer to SE 2000 series manual for details.**
	Coordinator	Select this if the system is using the SE coordinators.
Model	Click the drop-down list to select the transmitter model that is assigned to the subscriber. You can select either the "SE-TRM-433T01", "SEC-3402-433" or "SEC-RFPB60M-433" transmitters.	
	SE-TRM-433T01	(default) Select this if subscriber is using the SE-TRM personnel transmitters.
	SEC-3402-433	Select this if subscriber is using the SEC-3402 point tracking transmitters.
	SEC-RFPB60M-433	Select this if subscriber is using the SEC-RFPB60M-433 pendant transmitters.
Subscriber Type	Click the drop-down list to select the appropriate class for this subscriber or asset. Selecting the subscriber type allows the alarm signal to be used to acknowledge alarms remotely. It does not create an alarm. When this transmitter transmits an alarm, the alarms appearing on the alarm screen are acknowledged in the order they were received. This is the same order the alarms would be received on a pager for an approving officer.	
	Acknowledgement	Subscriber with acknowledgement transmitters.

Element	Usage/Description	
	Commuter	Normal subscriber type.
	Faculty	Normal subscriber type.
	Installer	Subscriber with maintenance transmitters.
	Out of Service	Out of service transmitters.
	Point type	Point transmitter for monitoring assets.
	Resident	Normal subscriber type.
	Security	Subscriber with security transmitters.
	Staff	Normal subscriber type.
	Unclassified	(default)
	Visitor	Normal subscriber type.
	Watchman	Normal subscriber type.
Disability	Select a value from the drop-down list if this individual is handicapped. The item will be displayed on the alarm screen. If a handicap is selected, the **Notes** field will not appear on the alarm screen.	
	Blind	Subscriber is blind.
	Deaf	Subscriber is deaf.
	Handicapped	Subscriber is handicapped.
	No handicap	(default)
	Wheel chair	Subscriber requires wheel chair for movement.
Disabled	This option disables an individual subscriber's transmitter in such a way that it does not produce an alarm message on the Central Console. This can be used to halt a subscriber's misuse of the system. Disable or enable a subscriber by finding the subscriber record in the **Subscriber Database**, click the **[Edit Data]** button and select the **Disabled** checkbox. If this checkbox is selected, the subscriber's transmitter will be ignored by the system; otherwise, the transmitter is recognized and alarms will be displayed.	
Silent	If this checkbox is selected, a system that normally sounds the alarms is silent for all alarms generated by this transmitter.	
Profile	Profile of the transmitter.	
	User	Select this if transmitter is a user transmitter.
	Maintenance	Select this if transmitter is a maintenance transmitter.

Element	Usage/Description	
	Security	(default) Select this if transmitter is a security transmitter.
Auto-track Interval	This is the interval of auto-track feature in seconds. It is 7 seconds by default for all transmitter profiles and cannot be changed.	
Man-down	If this checkbox is not selected, the buzzer will not sound during a man-down alarm. If this checkbox is selected, the buzzer will sound during a man-down alarm, and you can change the **Pre-beep** field.	
Pre-beep	If the **Man-down** checkbox is selected, this field is enabled for user to change the period for sounding the buzzer in seconds during a man-down alarm. Default is 5, and valid values are numeric between 0 and 6.	
Supervision	If this checkbox is not selected, the supervision feature will not be enabled during an alarm. If this checkbox is selected, the supervision feature will be enabled during an alarm. This option also affects the availability of the **Supervision period** field.	
Supervision period	If the **Supervision** checkbox is selected, this field is enabled for user to change the period of the supervision feature during an alarm. Default is 90 seconds. Select the valid value from the drop down list box: 90 Sec, 3 Min, 10 Min, 1 Hr, 2 Hr.	
Lanyard	If this checkbox is selected, the lanyard feature will not be enabled. If this checkbox is selected, the lanyard feature will be enabled.	
Name	The individual or item assigned to this transmitter. This is a compulsory field.	
Addr	Address of the individual or item within the protected area. The first address line on the left side, which is not the home address, is shown on the alarm screen	
City	City of the individual or item within the protected area.	
State	State of the individual or item within the protected area.	
Zip	Zip code of the individual or item within the protected area.	
Phone	The phone number to access the individual within the protected area. The phone number on the left side, which is not the home phone, is shown on the alarm screen.	
Subscriber ID	The **Subscriber ID** (typically the Social Security Number) must be entered into this field. This is a compulsory field. It must be filled in with a unique ID.	
Transmitter ID / New ID	The transmitter identification code can be typed into this field, but a faster and error free method is to ensure that the **Transmitter ID** field is empty, and perform a test with the	

Element	Usage/Description
	transmitter to be assigned to this subscriber. The new transmitter ID will be populated in the **New ID** field. The new ID must then be manually entered into the **Transmitter ID** field, or use the mouse to highlight the existing **Transmitter ID** and press and hold the <Shift> key and press the <Insert> key. This transfers the new ID to the **Transmitter ID** field. This is a compulsory field that must be filled with a unique ID.
Alarm Zone	Specific alarm zones are assigned to the different computer workstations of the Security Escort system. Each transmitter entered in the **Subscriber Database** can be assigned to one or more of the alarm zones. You may control on which computer workstations alarms from this transmitter appear.
Alarm Background Color	Select the background color of the alarm when this transmitter is activated. The default background color is red.
Female/Male **Height** **Build** **Hair color** **Eye color**	These characteristics of the subscriber are shown on the alarm screen.
Image / [Browse]	Enter the filename for the image of this individual or item to be shown on the alarm screen. Otherwise, you can also click the **[Browse]** button to open a file dialog to select the filename from a list of available files.
[Advanced]	Used to set up special transmitters that monitor fixed locations. These features are not used for personal transmitters. This button is available only to the maintenance and installation personnel.
[Information]	Click this button to enter specific information about the holder of this transmitter.
[Save]	Click this button to save all changes to the database.
[Cancel]	Click this button to abort all changes to the database. A confirmation dialog box appears, requesting for confirmation to save changes before closing. Click the **[Yes]** button to save the changes, **[No]** button to abort the changes, or **[Cancel]** button to return to the **Edit Subscriber** dialog window.

9.8.2 Subscriber images

The images should not be larger than 160 pixels wide and 160 pixels high. If they are larger, they will have to be scaled and therefore may lose image quality. The path to the images is configured in **Subscriber image file path** field found in the menu **Network > System directories and network address** dialog window. The default location of the images is "C:\ESCORT\IMAGES", but they can be located anywhere.

In the same dialog window, the three-character file extension of the image files is set in **Extension** field. The default is “JPG” format, and this is the recommended format of the subscriber images. Subscriber images may also be saved in Windows bitmap "BMP" format, but this format is not encouraged as it requires significantly more disk storage.
When the display is set to non-recommended size, the **Scaling %** field (10 to 200) may be used to control the size of the image (try different settings to control the image size in the alarm screen).
From the menu **Files > Subscriber Database** dialog, select the desired subscriber, then click the **[Edit Data]** button. The **Image** field is the name of file of this subscriber's image. For example, if the subscriber's image is stored in a file with the name "Image1.jpg", enter "Image1" in this textbox.
To get the best color displayed on your LCD monitor, make sure to set the color depth to “True Color (32-bit)” from the Control Panel. The LCD monitor display resolution should be set to the recommended 1024 x 768 or higher pixels.

Element	Requirement
File Format	**Extension** field in **System directories and network address** dialog window. Default is JPG (recommended). BMP is not encouraged.
File Size	160 pixels x 160 pixels (width x height)
Path of Image Files	**Subscriber image file path** field in **System directories and network address** dialog window. Default is "C:\ESCORT\IMAGES".
Name of Image File	**Image** field in **Subscriber Database** dialog window.
Color Depth	True Color (32 bit) (recommended)
Display Resolution	1024 x 768 (recommended)

9.8.3 Advanced features of Subscriber Database

The **Subscriber Database** contains information on the transmitters that are assigned in the system. See the Security Escort Operation Manual for the basic operations of the **Subscriber Database** dialog. See the section on Exporting, importing and merging the Subscriber Database for information on the data merge, import and export functions of the **Subscriber Database**.
The following section explains the advanced features of the **Subscriber Database** dialog when you are inserting a new, or editing an existing subscriber. Click the **[Advanced]** button in the **Edit Subscriber's Database** dialog to open the **Edit Subscriber’s Advanced Features** dialog window.

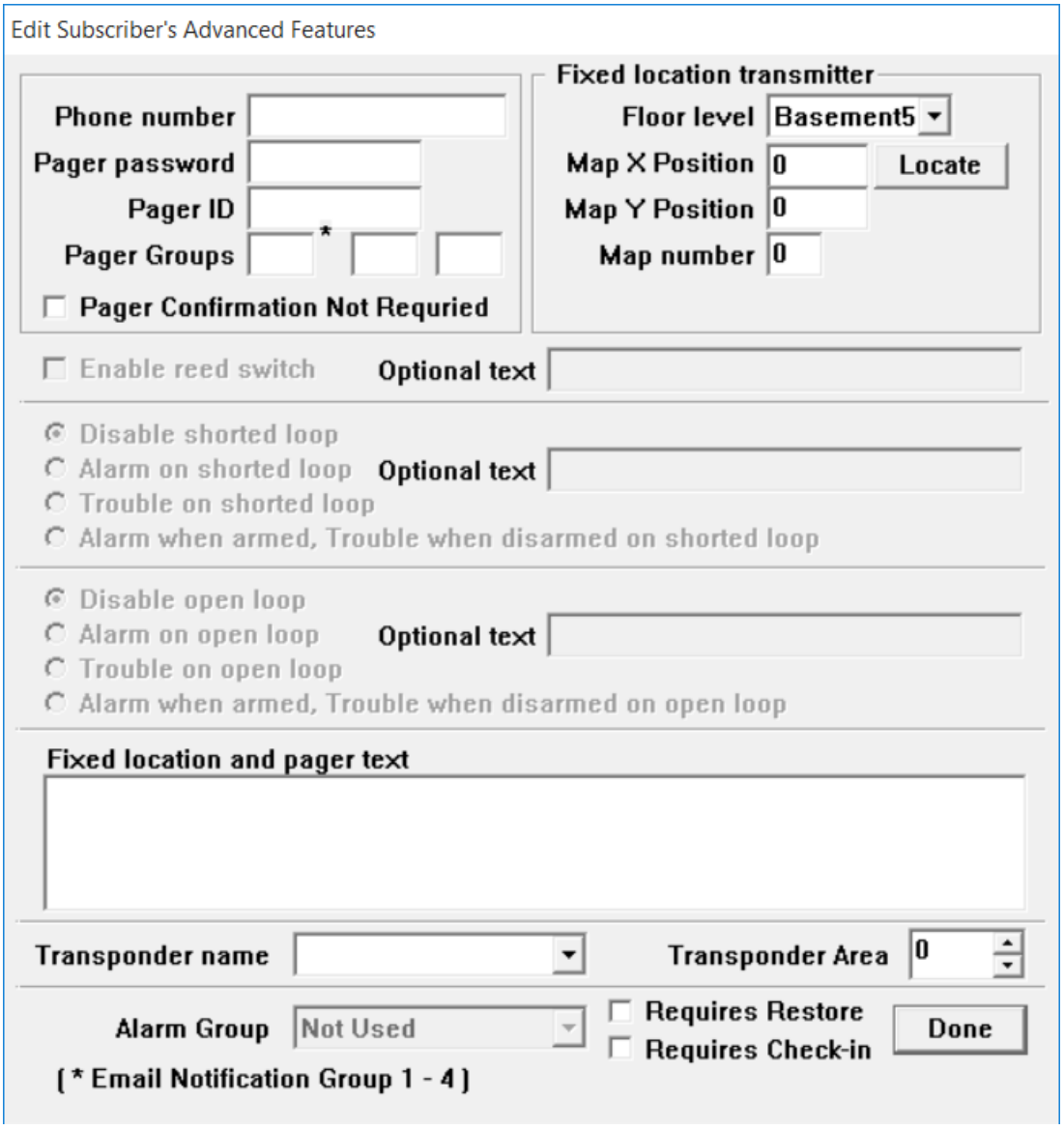


Figure 9.19: Subscriber's Advanced Features dialog window

The **Edit Subscriber's Advanced Features** dialog is used to set up special transmitters that monitor fixed locations, subscriber pager access, parameters for point transmitters, the virtual fence for a wandering alarm, the alarm group for arming of the transmitter and check-in requirements for this transmitter.

Elements	Usage/Description
Phone number	This phone number is dialed to send a pager message to this subscriber. Typically, this is a different phone number than the one that is manually dialed to access this pager. The phone number is assigned by the paging service.
Pager password	This is the password to be sent to the paging service when a page is sent to this subscriber. Leave blank if not required (typically, the pager password is not required). The pager password is assigned by the paging service.

Elements	Usage/Description	
Pager ID	This is the ID that identifies the pager to receive the pager message (many times this value is the last 7 digits that would be manually dialed to access this pager). The pager ID is assigned by the paging service.	
Pager Groups	The first pager group (*) can be used for email notification. You can enter the email notification group “01”, “02”, “03” or “04” to configure the notification of this specific subscriber alarm to be sent via email to that email notification group. If the pager group (*) is left empty, alarms for this subscriber will send an email to the default notification group “00”. Any data entered from 5 to 99 in the first pager group (*) will be treated as a pager group. The subscriber can be a member of up to 3 different pager groups. Enter the group numbers in the pager group fields respectively.	
Pager Confirmation Not Required	If checkbox is selected, the confirmation pager message is not sent to this pager if alarm is acknowledged by an acknowledgement transmitter.	
Fixed location transmitter	This section is to be used only when this transmitter is mounted in a fixed location (does not move). When this transmitter transmits an alarm, it will always be reported at the programmed location.	
	Floor level	This is the floor level where this alarm is to be located for a fixed location transmitter.
	Map X Position	This is the X coordinate of the map position where this alarm is to be located for a fixed location transmitter.
	Map Y Position	This is the Y coordinate of the map position where this alarm is to be located for a fixed location transmitter.
	[Locate]	When clicked, the dialog will disappear and the cursor will change to a cross hair. Moving the cursor to a point on the map and clicking the left mouse button will scroll the map so that point is at the center of the screen. When the map is showing the desired alarm location, move the cross hair to the exact location of the alarm to be reported and click the right mouse button. The dialog will reappear and the selected location will be entered into the X and Y coordinates. If while the cross hair cursor is being displayed, you desire to exit without changing any coordinate values, press the <Esc> key and the transponder edit dialog will reappear.
	Map number	Defines which bitmap is to be displayed for the fixed location of this transmitter. The default map is 0, which corresponds to bitmap MAP0.EDB stored in the “Escort” sub-directory. Map 1 would be MAP1.EDB. There can be 100 maps per Security Escort system, therefore the valid values are numeric from 0 to 99.

Elements	Usage/Description
Enable reed switch	If selected, the reed switch input of this transmitter is enabled to cause an alarm. Otherwise, the reed switch input will be disabled. The alarm group, where this transmitter is assigned to, must be armed in order for this input to cause an alarm (which is displayed). If no alarm group is assigned, the transmitter is always armed. For this option to be enabled, the transmitter's class must be set as "Point type".
Optional text	This is optional text that will be added to the location text when this input reports an alarm. For this option to be enabled, the transmitter's class must be set to "Point type".
Disable on shorted loop	If selected, a shorted loop on this transmitter will not cause an alarm or trouble report to be displayed. For this option to be enabled, the transmitter's class must be set to "Point type".
Alarm on shorted loop	If selected and the alarm group, where this transmitter is assigned to, is armed, then a shorted loop on this transmitter will cause an alarm report to be displayed. The alarm group this transmitter is assigned to must be armed, for this input to cause an alarm, which is displayed. If no alarm group is assigned, the transmitter is always armed. For this option to be enabled, the transmitter's class must be set to "Point type".
Trouble on shorted loop	If selected, a shorted loop on this transmitter will cause a trouble report to be displayed. For this option to be enabled, the transmitter's class must be set to "Point type".
Alarm when armed, Trouble when disarmed on shorted loop	If selected and the alarm group, where this transmitter is assigned to, is armed; then a shorted loop on this transmitter will cause an alarm report to be displayed. If selected and the alarm group, where this transmitter is assigned to, is disarmed, then a shorted loop on this transmitter will cause a trouble report to be displayed. If no alarm group is assigned, the transmitter is always armed. For this option to be enabled, the transmitter's class must be set to "Point type".
Disable open loop	If selected, an open loop on this transmitter will not cause an alarm or trouble report to be displayed. For this option to be enabled, the transmitter's class must be set to "Point type".
Alarm on open loop	If selected and the alarm group, where this transmitter is assigned to, is armed, then an open loop on this transmitter will cause an alarm report to be displayed. The alarm group, where this transmitter is assigned to, must be armed for this input to cause an alarm, which is displayed. If no alarm group is assigned, the transmitter is always armed. For this option to be enabled, the transmitter's class must be set to "Point type".
Trouble on open loop	If selected, an open loop on this transmitter will cause a trouble report to be displayed. For this option to be enabled, the transmitter's class must be set to "Point type".
Alarm when armed, Trouble when disarmed on open loop	If selected and the alarm group, where this transmitter is assigned to, is armed; then an open loop on this transmitter will cause an alarm report to be displayed. If selected and the alarm group, where this transmitter is assigned to, is disarmed, then an open loop on this transmitter will

Elements	Usage/Description
	cause a trouble report to be displayed. If no alarm group is assigned, the transmitter is always armed. For this option to be enabled, the transmitter's class must be set to "Point type".
Fixed location and pager text	This is the text that will be displayed as the location of the alarm for fixed location transmitters and on pagers reporting this alarm.
Transponder name	Select the transponder with the area that is defined for a wandering (virtual fence) alarm. See **Transponder Area** below for the operation and setup of the wandering alarm (virtual fence alarm).
Transponder Area	Wandering alarm - Create a protected area by placing a virtual monitor "fence" around an area of the main map. These areas are defined in the **Transponder Database**. If this transmitter is constrained to remain within one of these defined areas, first select the defining transponder in **Transponder name** above. Then select the desired area from this drop-down list of the transponder's area names. For the wandering alarm to work, the supervision period must also be programmed for this transmitter. Then specific transmitters are marked in the subscriber database, to be constrained within a specific fenced area defined by this option. If the transmitters leave their defined area, the system will report this as a Wandering alarm and continue to monitor and track the location of the transmitter until the alarm is canceled from the screen in the normal way. However, these tracking updates can only occur every supervision transmission period (not on an accelerated rate like a tracking alarm). The Security Escort system computes the location of the transmitters when they broadcast automatic supervision transmissions periodically. Because of the basic location accuracy and the floor-to-floor accuracy of the system, there is a potential for some false alarms. If false alarms are a problem, check the **Filter Virtual Fence** checkbox in the **Security Preferences** dialog. If you do this, two successive location calculations will have to indicate the transmitter has moved outside the protected area before an alarm is generated. The downside of this is a delay in the reporting of a wandering alarm of one extra transmitter supervision period.
Alarm Group	This is the alarm group that controls the arm/disarm status of this transmitter. Select the desired alarm group from the dropdown list of the alarm group names. This alarm group must be armed, for this transmitter to cause an alarm, which is displayed. If no alarm group is assigned, the transmitter is always armed.
Requires Restore	When this checkbox is selected, user needs to restore all active alarms at the transmitter, before resetting the alarm display on the SE console software. This function also requires the Supervision duration to be set.
Requires Check-in	When this checkbox is selected, this transmitter will have to be activated once each day during the **Check-in Schedule** time. At the end of the check-in period, if the subscriber fails to check-in, a **Failed to Check-in Report** will be generated and presented to the operator of the software.

Elements	Usage/Description
	This report contains all of the people who failed to check-in with their first address line and phone number. All subscribers in the report must be selected on to make sure they are not in need of assistance, as this may be a life-treating situation. A printed report may also be generated. If the transmitter is not a point type, then the transmitter can generate alarms and therefore a test transmission will be used for the check-in. If the transmitter is a point type, then any non-trouble transmission will serve as a check-in. One of the 10 schedules must be selected as the check-in schedule to define the check-in period.
[Done]	Click this button when all changes to this dialog are completed and return the main **Subscriber Database** edit dialog.

9.8.4 Additional subscriber information

The **[Information]** button is used to enter specific information about the holder of this transmitter. Car type, parking sticker number, license number, and medical information are examples of the types of information typically entered. Each field typically holds different information. The installer can change the field labels to labels that would define your intended usage.

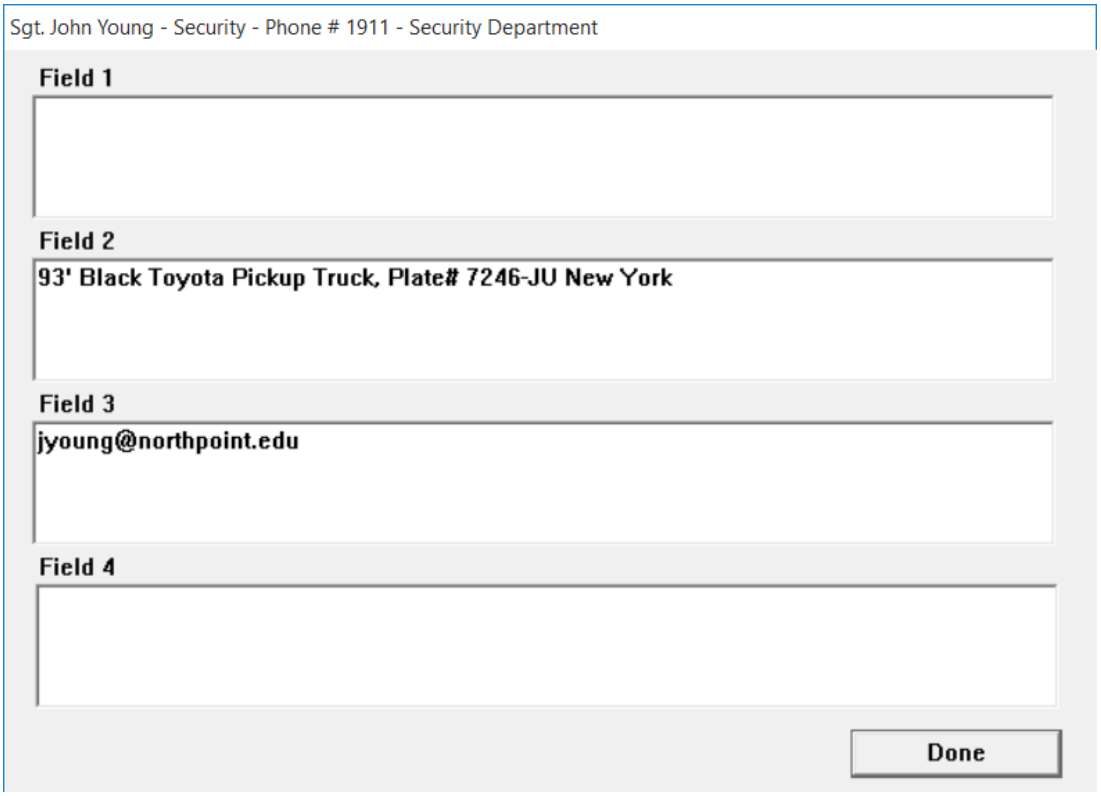


Figure 9.20: Information dialog window

Element	Usage/Description
Field 1 / Field 2 / Field 3 / Field 4	Enter the information as required for your intended usage. These information will appear during an alarm relating to the subscriber.

Element	Usage/Description
[Done]	Click this button to close the information entry dialog and return to the **Edit Subscriber's Database Record** dialog. Click the **[Save]** button to save all changes to the database.

9.8.5 Statistics of Subscriber Database

Click the **[Statistics]** button to summarize all type of subscribers in the database. The statistics window lists the number of subscribers according to their classification, gender, disability and subscriber type.

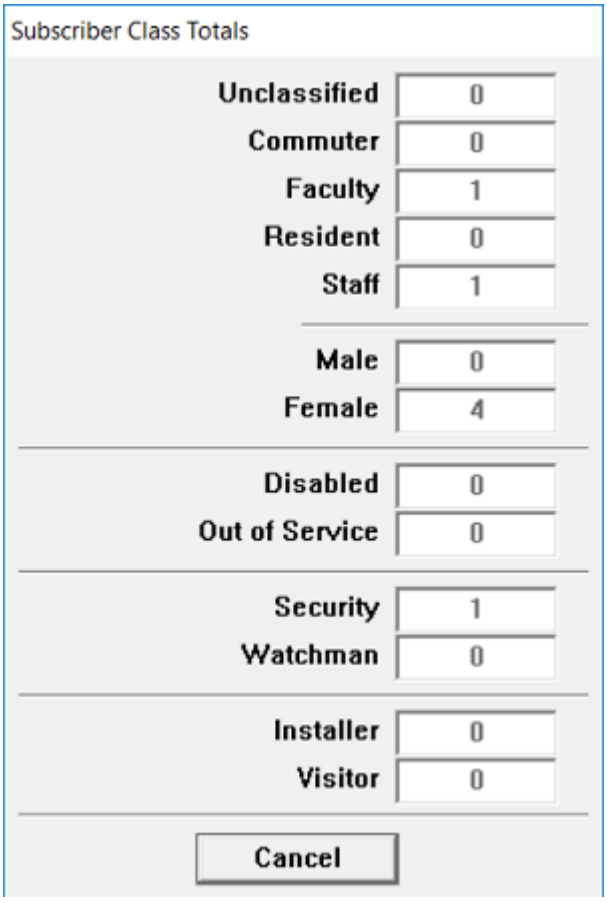


Figure 9.21: Subscriber Database statistics

9.8.6 Print Subscriber Database

Click the **[Print]** button to open the **Subscriber Print** dialog window. Select one of the sort order options (**Sort by** column) and any data fields (**Print fields** column) that you wish to include in the report.

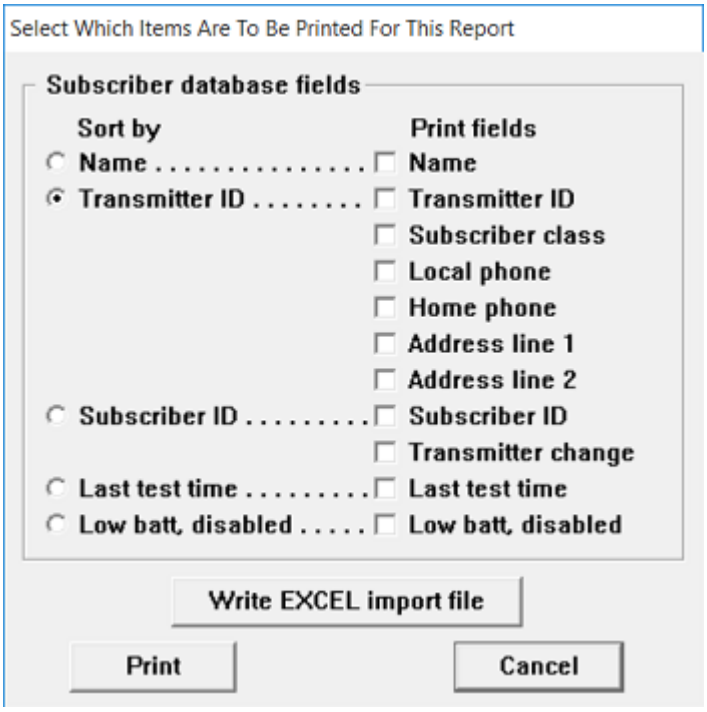


Figure 9.22: Print Subscriber dialog window

After selecting the sort order and the fields that you wish to print, click one of the following buttons to proceed.

Element	Usage/Description
[Write EXCEL import file]	Click this button to send all the fields of all the records to the “subscrib.txt” file in the folder where Security Escort was installed. This file may be directly imported into Microsoft Excel or any other application that accepts tab delimited text.
[Print]	Click this button to send the selected data fields to the report printer in the indicated sort order.
[Cancel]	Click this button to abort the print dialog and return to the previous screen.

9.8.7 Subscriber (individual) Pager Setup

In the **Subscriber Database**, select the record for the desired individual. Click the **[Edit Data]** button, followed by the **[Advanced]** button. The dialog below will be displayed.

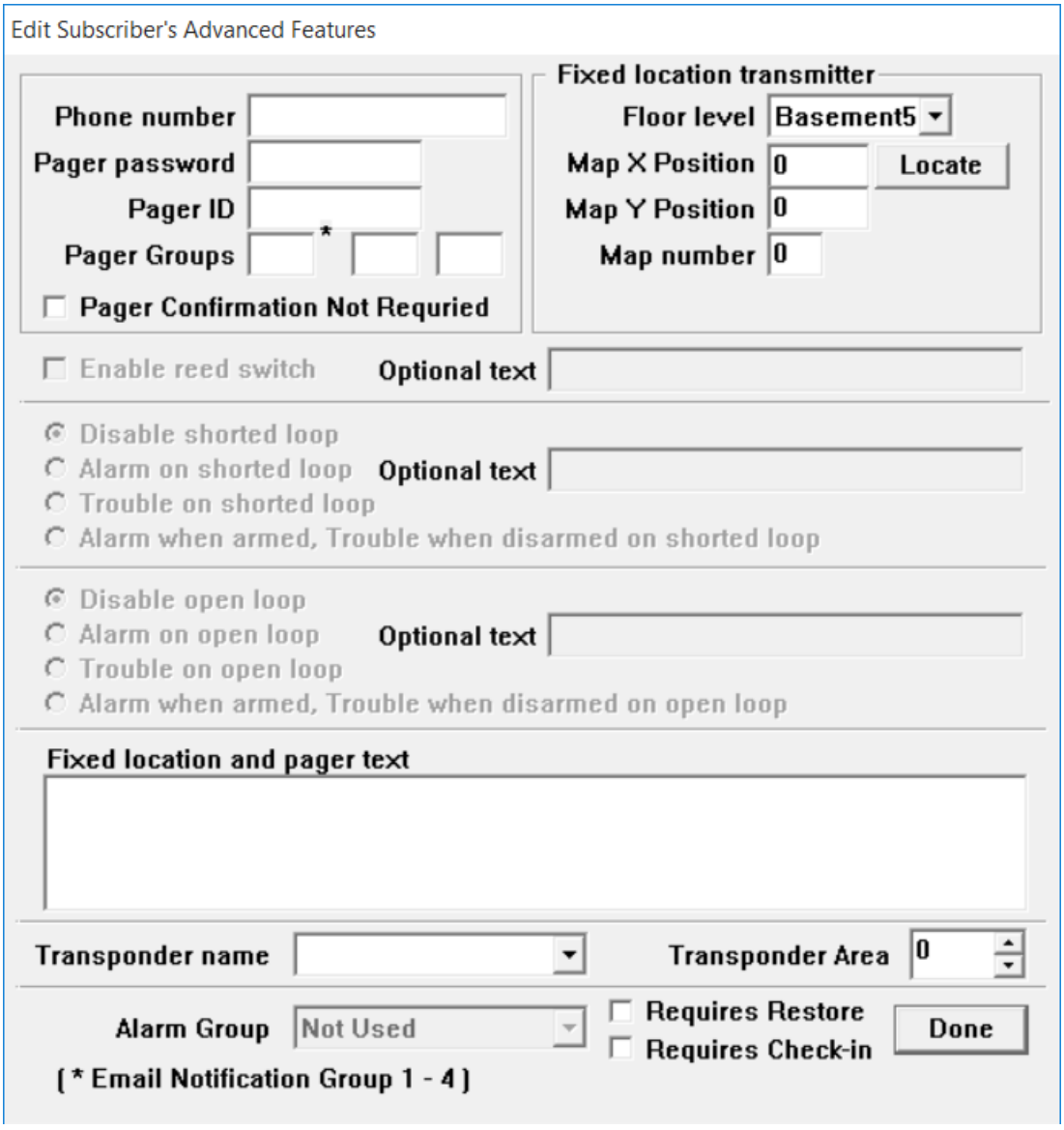


Figure 9.23: Subscriber Database Advanced Features dialog window

The pager ID is required for all individual pagers dial-up and local. If the phone number and password are assigned, the page will be sent over the modem connection. If the phone number and password fields are blank, the page will be routed to the local paging system. If you do not desire this individual to have pager support leave the phone number, password and pager ID fields all blank.

If the pager information is entered above, this individual may be assigned to 2 paging groups. Each group will accept 8 members maximum. Remember it takes time to communicate with a paging service, therefore only add members to a group if they need to be there, otherwise you may slow the paging report to people that must respond.

A pager group may contain members accessed by the local paging system and members that require dial-up access. Dial-up access typically takes much longer and it may slow pages to the local paging system.

9.8.8 Fixed Location Transmitters

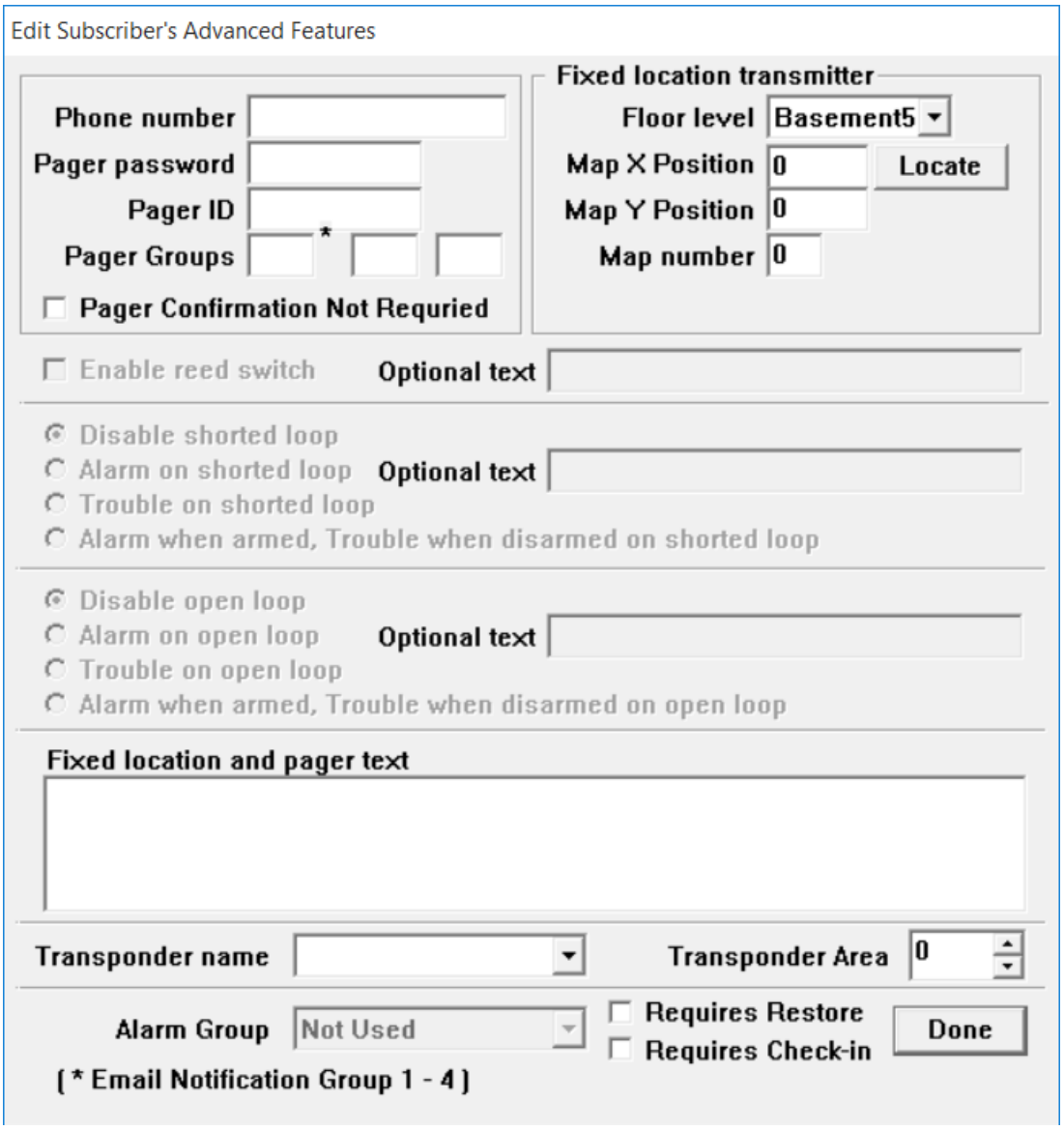


Figure 9.24: Fixed location transmitter dialog

The paging feature may use different paging companies and they may require different baud rates. Set the baud rate to the highest baud rate common to all of the paging companies to be accessed.
The character limit (characters per page), pages per call affect all pages of the indicated type (local and dial-up). These fields must be set to the lowest setting for any of the routes that may be used. Remember that dial-up pages may be routed to different paging companies and they may have different restrictions.

9.9 Exporting, importing and merging the Subscriber Database

The following sections describe the steps to export, import and merge data from and into the **Subscriber Database**. Only users or operators who are assigned the minimum security level of “View Subscribers” are able to perform the import, export and merge functions of the **Subscriber Database**. The files supported are the XML and DAT file formats.

9.9.1 The DAT file format

The DAT file must be in tab delimited text format. The fields must be in the exact specified order, delimited by the horizontal tab character (decimal 8) and the record must be terminated with a carriage return (decimal 13). If a field has no data, just store the terminating tab character for that field. The total number of characters in all the fields of a record must be 255 characters or less, including the tab and carriage return characters.

9.9.2 The XML file format

The XML tree consists of the *<Subscribers>* main element. The *<Subscribers>* element is the parent element of the *<Subscriber>* child elements. The *<Subscriber>* element has a list of sub-elements that defines the data of the subscriber.

A simplified example of a typical tree with an empty structure is as of below:

```
<Subscribers>
    <Subscriber>
    </Subscriber>
</Subscribers>
```

9.9.3 Exporting the Subscriber Database

To export data from the **Subscriber Database**, go to menu **File > Subscriber Database** dialog, and click the **[Export]** button.

Notice!
Important! The export operation does not change the existing records in **Subscriber Database**.

A file dialog appears for you to choose the folder where you wish to save the file in, and provide a name for the file. Click the **Save as type** drop-down list to choose the format of the file you wish to export to: the DAT or XML file format.

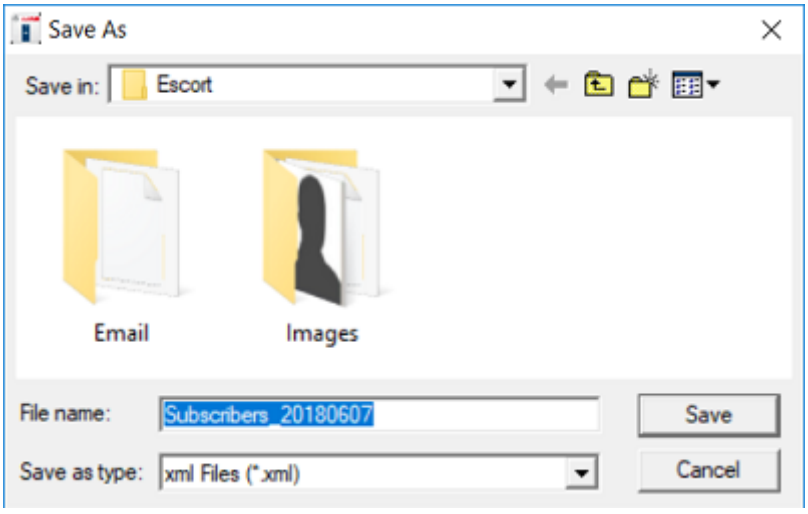


Figure 9.25: Export file dialog

If you wish to abort the task, click the **[Cancel]** button. Otherwise, click the **[Save]** button to export the **Subscriber Database**. If a file of the same name already exists, a confirmation dialog appears asking if you wish to replace the file.

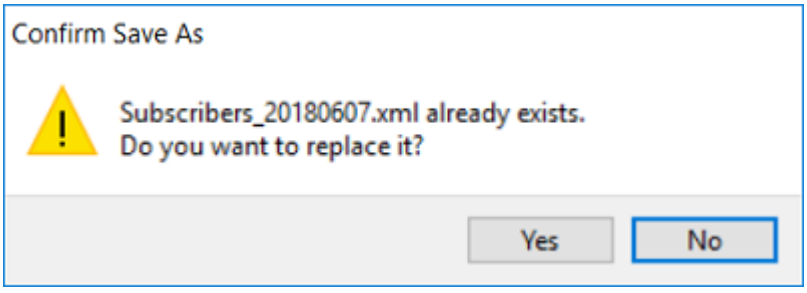


Figure 9.26: Replace file confirmation dialog

Click the **[No]** button to abort and return to the file dialog box where you can choose a different name for the file. Otherwise, click the **[Yes]** button to proceed with replacement of the file. If the export is successful, a confirmation dialog appears. You will find the file in the specified folder.

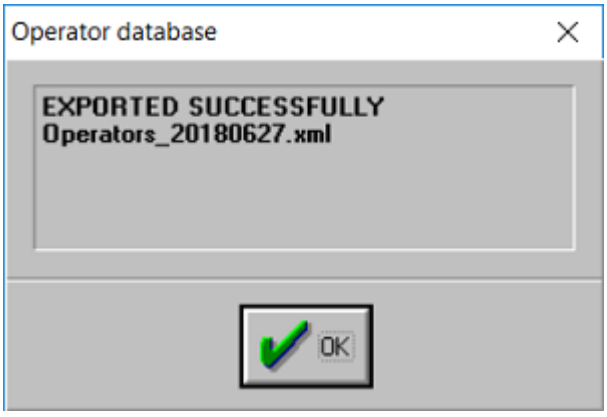


Figure 9.27: Operator database successfully exported dialog

9.9.4 Importing the Subscriber Database

To import data into the **Subscriber Database**, the file to imported must already be prepared in the XML or DAT file format. Go to menu **File > Subscriber Database** dialog, and click the **[Import]** button.

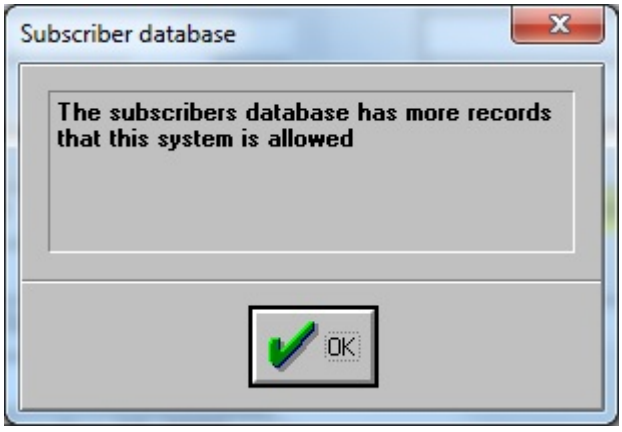
Notice!
There is no way to undo the operations. Therefore, it is recommended to **perform a database backup** prior to starting the task. Upon completion of the task, verify the updated data before the new database is placed in service. If there are problems, restore the **Subscriber Database** from the backup.

Notice!

Important!

Proceeding with the import operation will delete all existing records in **Subscriber Database**. The record entries in import file are then imported to the **Subscriber Database,** validated and sorted by the **Subscriber ID**.

The number of record entries that is imported is subject to the number of subscribers allowed for the purchased license. You can find this limit in the menu **About > About** dialog. If this limit is reached during the import, a pop-up message appears to inform the user.



A popup dialog appears asking for the file to be imported. Click the **[Cancel]** button to abort if you are still unsure. Otherwise, navigate the folders, select the file and click the **[Open]** button.

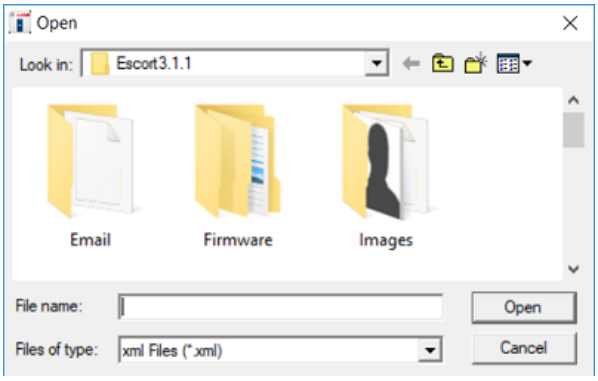


Figure 9.28: Import file dialog

A popup dialog appears, asking for confirmation to proceed with the import or to abort the operation. Click the **[No]** button to abort if you are still unsure. Click the **[Yes]** button to proceed with the import.

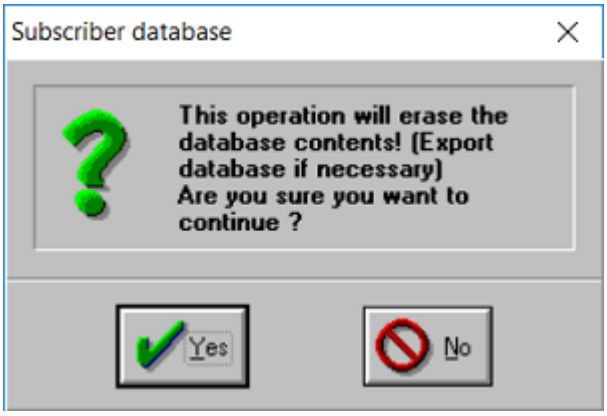


Figure 9.29: Import confirmation dialog

Be patient, as it may take a while, and watch for the disk activity to stop. If the data is imported successfully, a popup confirmation dialog appears. If the data is not imported successfully, a popup error message appears. The error message will indicate the likely cause of the import to fail.

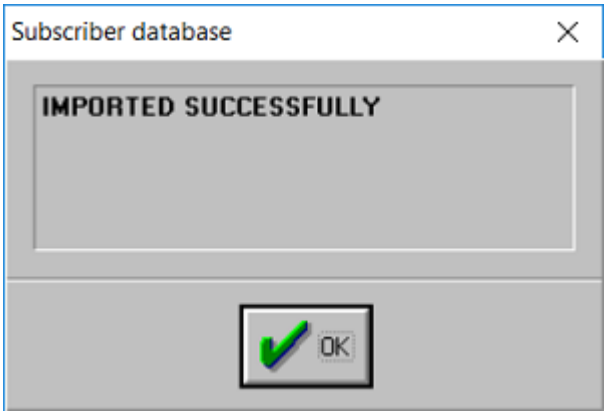


Figure 9.30: Subscriber Database successfully imported dialog

9.9.5 Merging the Subscriber Database

To merge data into the **Subscriber Database**, the file to merged must already be prepared in the XML or DAT file format. Go to menu **File > Subscriber Database** dialog, and click the **[Data Merge]** button.

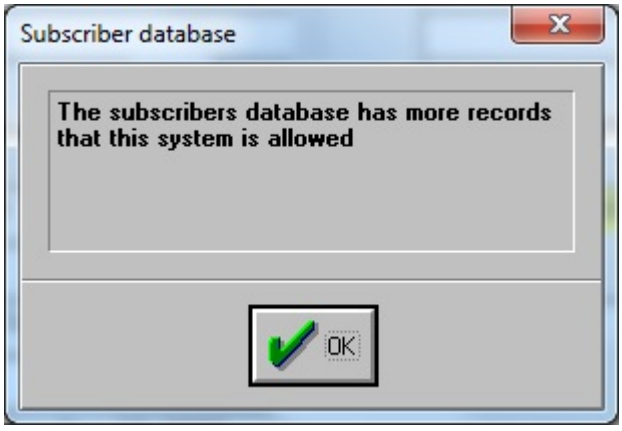
Notice!
There is no way to undo the operations. Therefore, it is recommended to **perform a database backup** prior to starting the task. Upon completion of the task, verify the updated data before the new database is placed in service. If there are problems, restore the **Subscriber Database** from the backup.

Notice!

Important!

The record entries in the file are merged with existing records in the **Subscriber Database**. If the **Subscriber ID** field in the file matches a record in the **Subscriber Database**, the existing record will be merged with the corresponding record entry in the file. Unmatched records will be inserted into the **Subscriber Database** as new records.

The total number of records is subject to the number of subscribers allowed for the purchased license. You can find this limit in the menu **About > About** dialog. If this limit is reached during the merge, a pop-up message appears to inform the user.



A popup dialog appears asking for the file to be merged. Click the Click the **[Cancel]** button to abort if you are still unsure. Otherwise, navigate the folders, select the file and click the **[Open]** button.

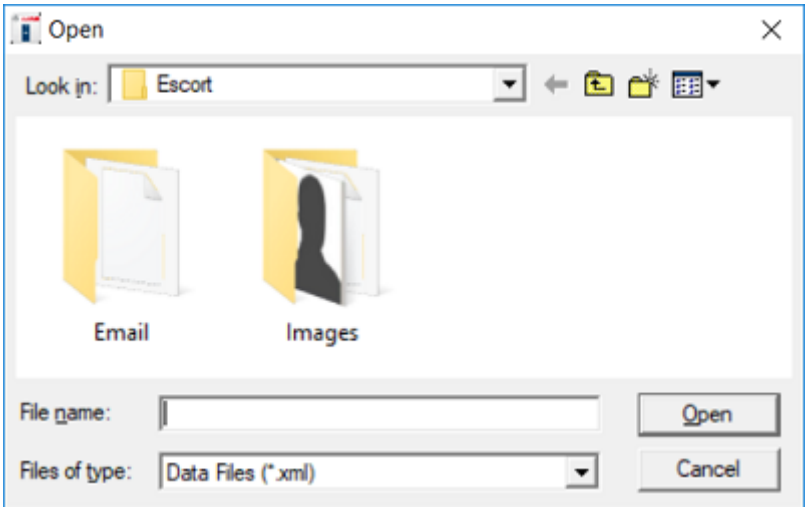


Figure 9.31: Merge file dialog

Be patient, as it may take a while, and watch for the disk activity to stop. If the data is merged successfully, a popup confirmation dialog appears. If the data is not merged successfully, a popup error message appears. The error message will indicate the likely cause of the merge to fail.

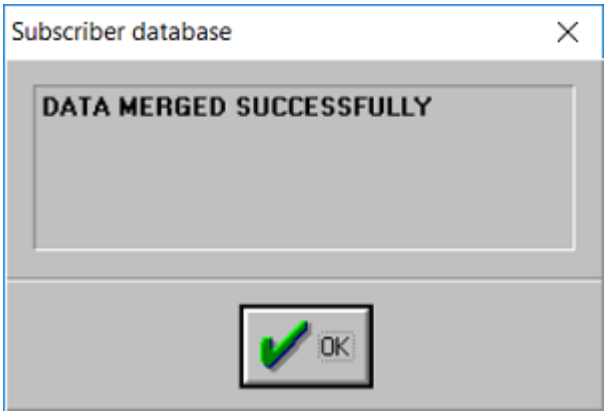


Figure 9.32: Subscriber Database successfully merged dialog

9.10 Schedules

This selection informs management of the ten-time of day/day of week schedules and holidays. The top portion of the display shows the ten-time-of-day/day-of-week schedules that Security Escort supports. For each schedule, there is an indication the schedule is currently active or armed (ACT); otherwise, the schedule is disarmed (OFF).

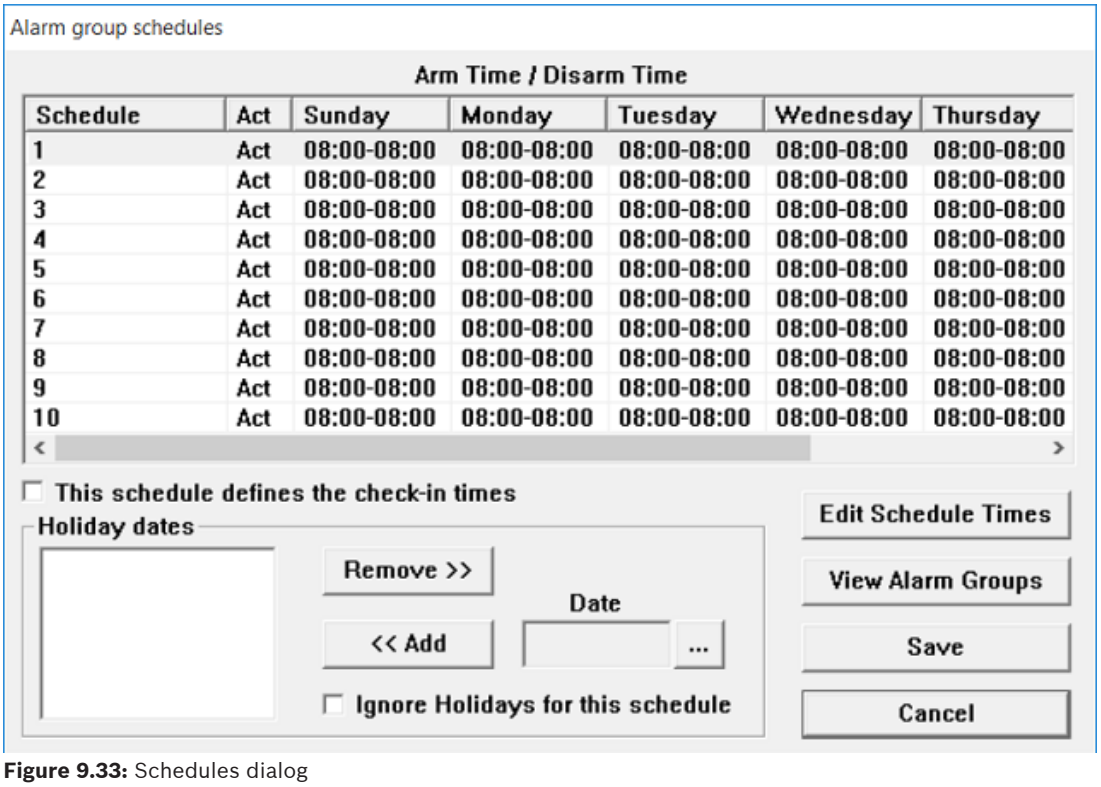


Figure 9.33: Schedules dialog

For each day-of-the-week, the arm time (time the schedule becomes active) and disarm time (time the schedule becomes inactive) are displayed. To edit the arm and disarm times, click the **[Edit Schedule Times]** button. Double clicking the number of the schedule allows you to name the schedules.

Element	Usage/Description
This schedule defines the check-in times	One of the ten schedules can be used to define the check-in times for those subscribers that must check-in. Click on the schedule for the check-in schedule, highlighting it. Then check

Element	Usage/Description
	this checkbox, to set the selected schedule as the check-in schedule. Both the arm time and disarm time must be programmed for every day the check-ins must take place. The arm time is the start of the check-in schedule and it must occur before the disarm time that marks the end of the check-in schedule for that day.
[Edit Schedule Times]	Clicking this button displays the **Edit Schedule Times** dialog so the day of week arm and disarm schedule times can be edited.
[View Alarm Groups]	Clicking this button displays the **View Alarm Groups** dialog. This screen shows the alarm groups assigned to the selected schedule and their current arming state.
Ignore Holidays for this Schedule	Each schedule can use the holiday dates as exceptions.

9.10.1 Ignore Holidays for this schedule

Each schedule can use the holiday dates as exceptions. Schedules are activated (armed) following the normal schedules if the holiday dates are configured to be ignored. Otherwise, the schedules are activated the entire day for the holiday dates.

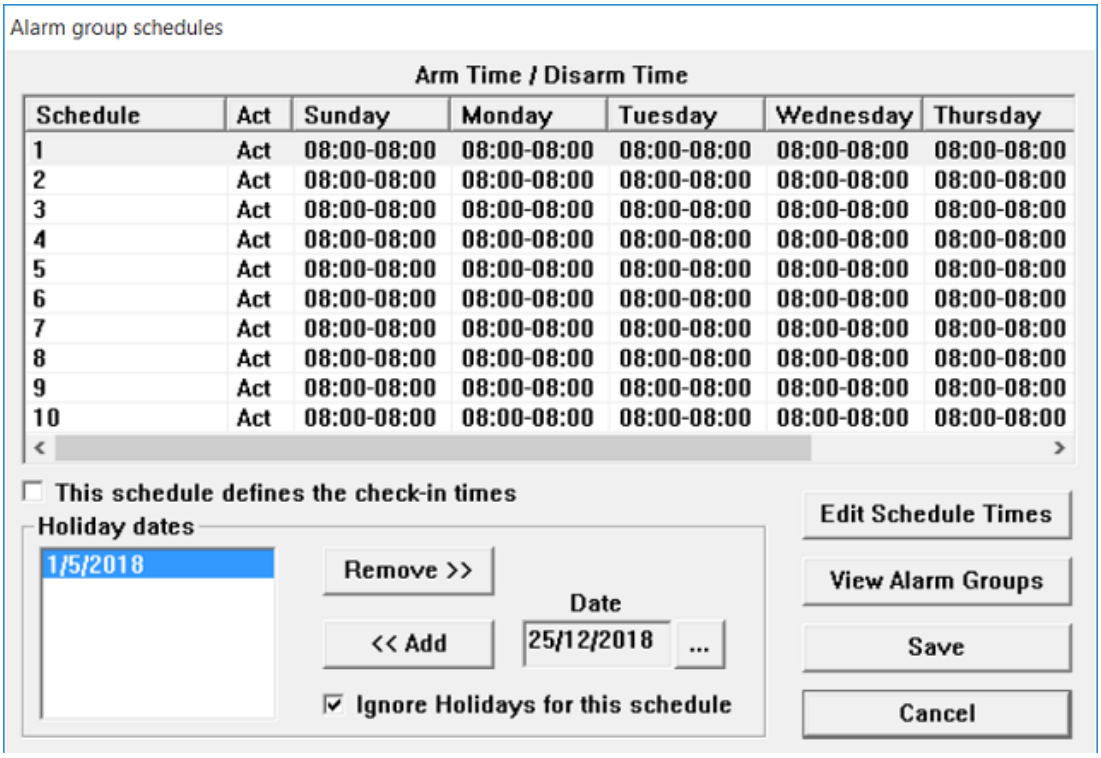


Figure 9.34: Holiday Selection in this schedule dialog

Element	Usage/Description
Ignore Holidays for this schedule	If the **Ignore Holidays** checkbox is selected for the indicated holiday dates, the schedules are activated (armed) that entire day. If the **Ignore Holidays** checkbox is not selected, the normal action of the schedules takes place on the holiday dates.

Element	Usage/Description
Date [...]	Clicking this button displays a calendar where you can graphically select a date. 
[Remove >>]	Clicking this button removes the selected date from the **Holiday dates** list box.
[<< Add]	Clicking this button adds the date shown to the **Holiday dates** list box.

9.10.2 Edit Schedule Times

This dialog allows the arming and disarming times to be programmed for each of the days of the week. All times are expressed in 24-hour time (00:00 to 23:59). Each schedule has one **Arm Time** and one **Disarm Time** for each of the 7 days of the week.

If both the **Arm Time** and **Disarm Time** are programmed to 00:00, the schedule will be active (armed) for the entire day.

If the **Arm Time** is 00:00 and the **Disarm Time** is programmed, the schedule will be active (armed) from midnight to the programmed **Disarm Time**. The schedule will be off (disarmed) from the **Disarm Time** to the end of the day.

If the **Disarm Time** is 00:00 and the **Arm Time** is programmed, the schedule will be off (disarmed) from midnight to the programmed **Arm Time**. The schedule will be active (armed) from the **Arm Time** to the end of the day.

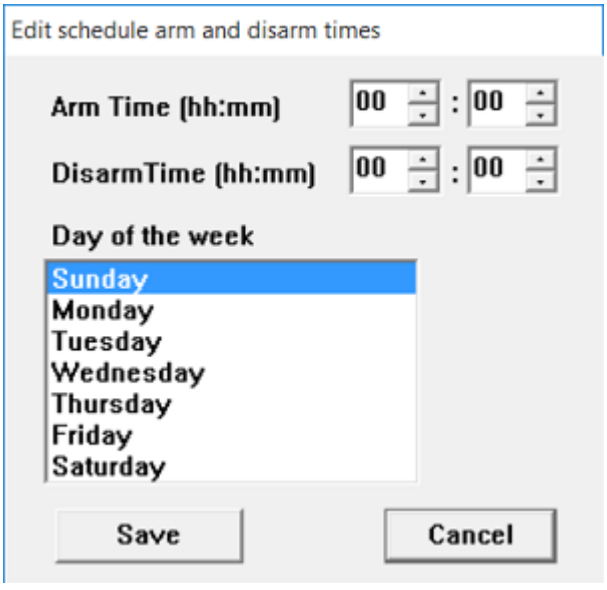


Figure 9.35: Edit Schedule Times dialog

If both the **Disarm Time** and the **Arm Time** are programmed, and the **Disarm Time** occurs before the **Arm Time** (normal 8 to 5 style day), the schedule will be active (armed) from midnight to the programmed **Disarm Time**. The schedule will be off (disarmed) from the **Disarm Time** to the **Arm Time**. The schedule will be active (armed) from the **Arm Time** to the end of the day.
If both the **Disarm Time** and the **Arm Time** are programmed, and the **Arm Time** occurs before the **Disarm Time**, the schedule is off (disarmed) from midnight to the programmed **Arm Time**. The schedule is active (armed) from the **Arm Time** to the **Disarm Time**. The schedule is off (disarmed) from the **Disarm Time** to the end of the day.

Element	Usage/Description
Arm Time	This is the time that the schedule becomes active (on or armed) for the selected day of the week. Times are expressed in 24-hour time (00:00 to 23:59).
Disarm Time	This is the time that the schedule goes off (disarmed) for the selected day of the week. Times are expressed in 24-hour time (00:00 to 23:59).
Day of the Week	Select the day you desire to change the time for. The **Arm Time** and **Disarm Time** are programmed separately for each day of the week. You must individually select each day of the week, and set the desired times.

9.10.3 View Alarm Groups

Select a schedule where you wish to view the associated alarm groups, and click the **[View Alarm Groups]** button. The list of alarm groups that are assigned to the selected schedule, and their current arming state are shown.

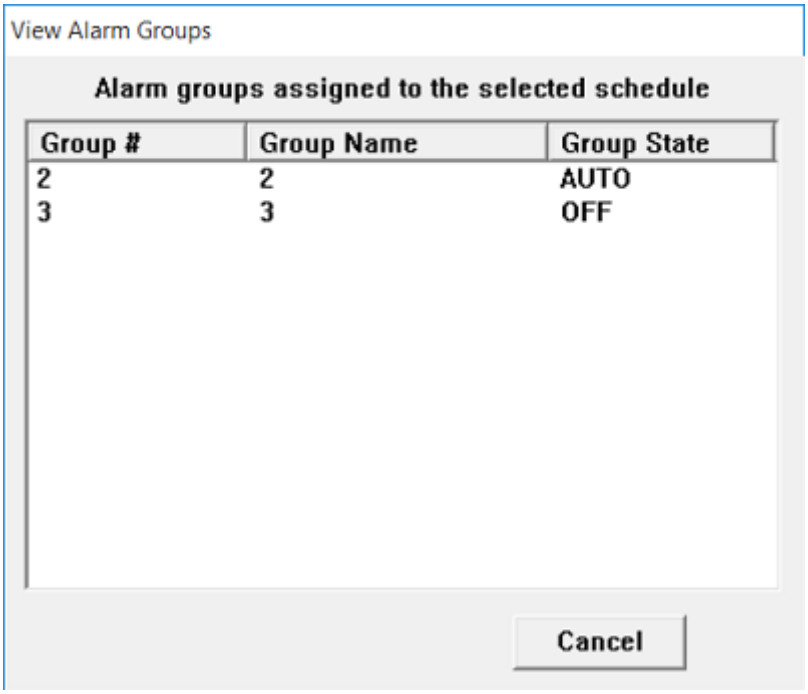


Figure 9.36: View Alarm Groups dialog

The “ON” and “OFF” **Group State** indicates that the alarm group is under manual control. “AUTO” indicates that the alarm group is under control of the selected schedule. This alarm group will be armed automatically once the schedule becomes active.

9.10.4 Alarm Groups

This dialog allows setup and arm/disarm control of the 99 alarm groups. Any number of point type transmitters can be assigned to an alarm group in the **Subscriber Database**’**s Advanced** dialog. However, each transmitter can only be assigned to one alarm group.

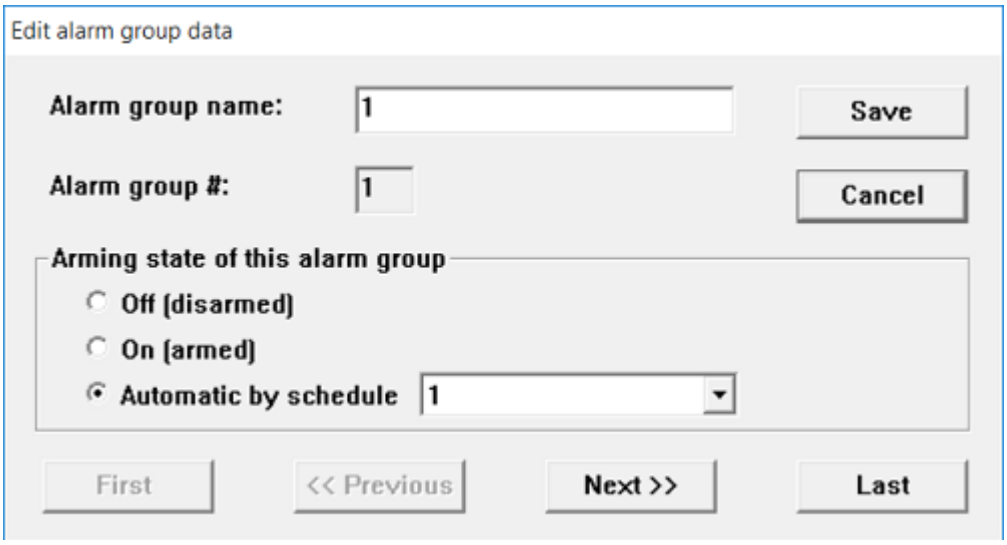


Figure 9.37: Alarm Groups dialog

An alarm group can be manually armed and disarmed, or assigned to a schedule to automatically arm and disarm the alarm group.

Element	Usage/Description
Alarm group name	Enter a descriptive name to identify the function of the points in this alarm group.
Alarm group #	This is the number of the alarm group (1-99).
Arming state of this alarm group	The **Off (disarmed)**, **On (armed)** and **Automatic by Schedule** selection control the arming state of this alarm group.
Off (disarmed)	Selecting this option disarms the alarm group. The alarm group will remain off (disarmed) until manually changed in this dialog to **On (armed)** or **Automatic by Schedule**.
On (armed)	Selecting this option arms the alarm group. The alarm group will remain on (armed) until manually changed in this dialog to **Off (disarmed)** or **Automatic by Schedule**.
Automatic by schedule	Selecting this option assigns the alarm group’s arming state to be controlled by the indicated schedule. When the schedule is active (on or armed) the alarm group will be armed. When the schedule is off (disarmed) the alarm group will be disarmed. Any number of alarm groups may be assigned to the same schedule.
[First]	Clicking this button takes you to alarm group 1.

Element	Usage/Description
[Previous]	Clicking this button takes you to the next lower alarm group from the one currently displayed. It will not wrap around. Therefore, it will be disabled at alarm group 1.
[Next]	Clicking this button takes you to the next higher alarm group from the one currently displayed. It will not wrap around. Therefore, it will be disabled at alarm group 99.
[Last]	Clicking this button takes you to alarm group 99.
[Save]	Clicking this button saves all the changes you made during the current dialog session.
[Cancel]	Clicking this button aborts all the changes you made during the current dialog session.

9.10.5 Alarm Group State

This dialog will display a list of the alarm groups that are currently armed, and have one or more transmitters (points) faulted. The points are presented because they were not restored when their automatic schedule armed, or there was an alarm while the alarm group was on.

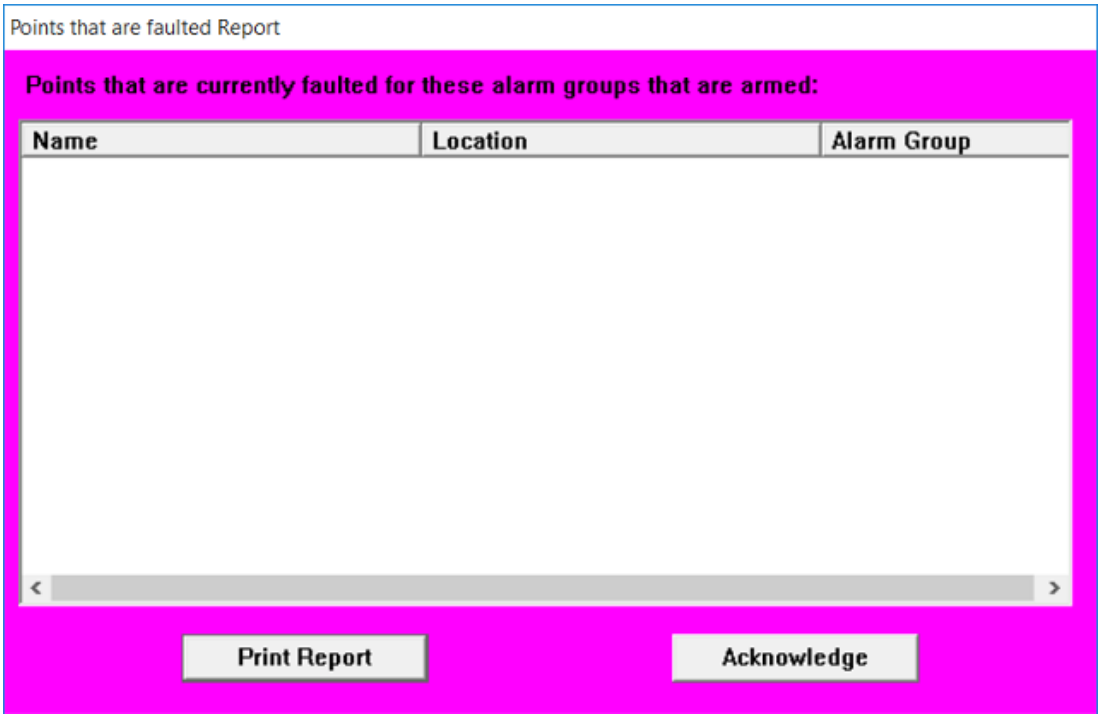


Figure 9.38: Alarm Group State dialog

Element	Usage/Description
[Print Report]	Clicking this button prints the displayed data to the report printer.
[Acknowledge]	Clicking this button closes the dialog if it was selected from the menu. However, if the dialog was presented automatically at the arm time of an alarm group's automatic schedule because they were not restored, or there was an alarm while the alarm group

Element	Usage/Description
	was on, then you are required to enter your password to acknowledge the dialog, and remove it from this computer's (and all other computer workstations) screens.

9.10.6 Current Check-in Status

This dialog displays a list of subscribers that are required to check-in and failed to do so during the last check-in period. Also shown are their addresses, phone numbers, and the last time they checked-in.

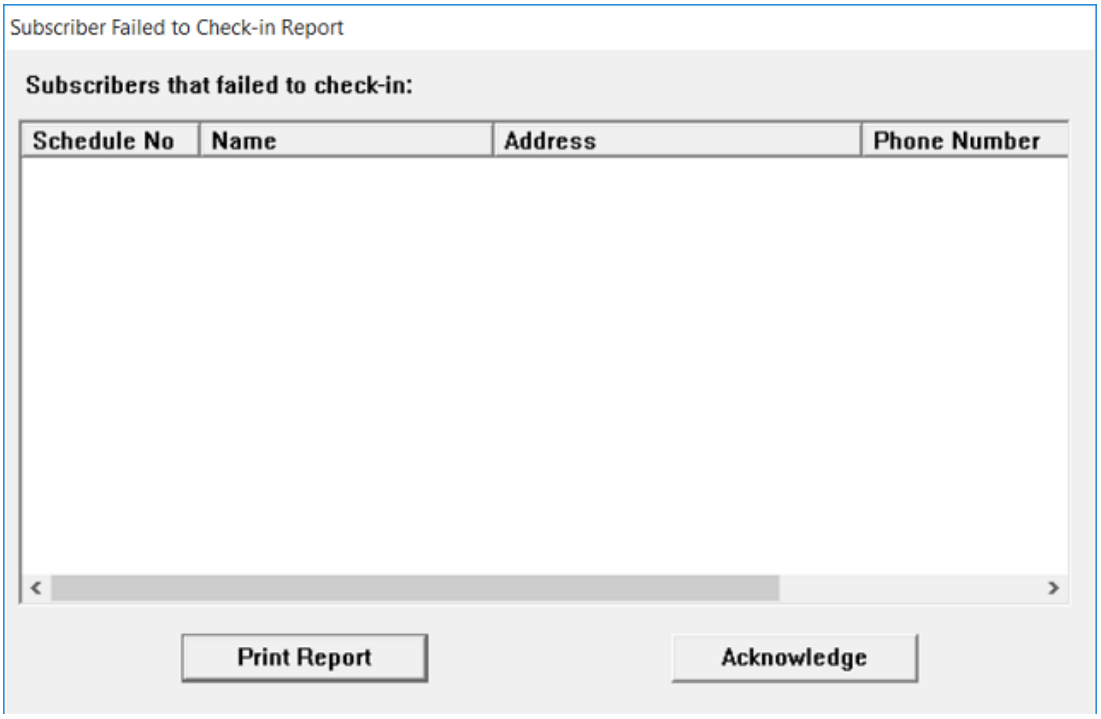


Figure 9.39: Current Check-in Status dialog

Element	Usage/Description
[Print Report]	Clicking this button prints the displayed data to the report printer.
[Acknowledge]	Clicking this button closes the dialog if it was selected from the menu. However, if the dialog appeared automatically at the end of the check-in period because some subscribers failed to check-in, you must enter your password to acknowledge the dialog and remove it from this computer's (and all other computer workstations) screens.

9.11 Operator Database

The figure below is a typical screen from the **Operator Database**. The term operator is used to refer to a person with the authority to use the various features of the Security Escort system software. The term includes the Security department's dispatchers who initiate responses to alarms, Security Officers who may be required to produce incident reports, and other employees of the Security department who may be responsible for maintaining the **Subscriber** and **Operator Databases**.

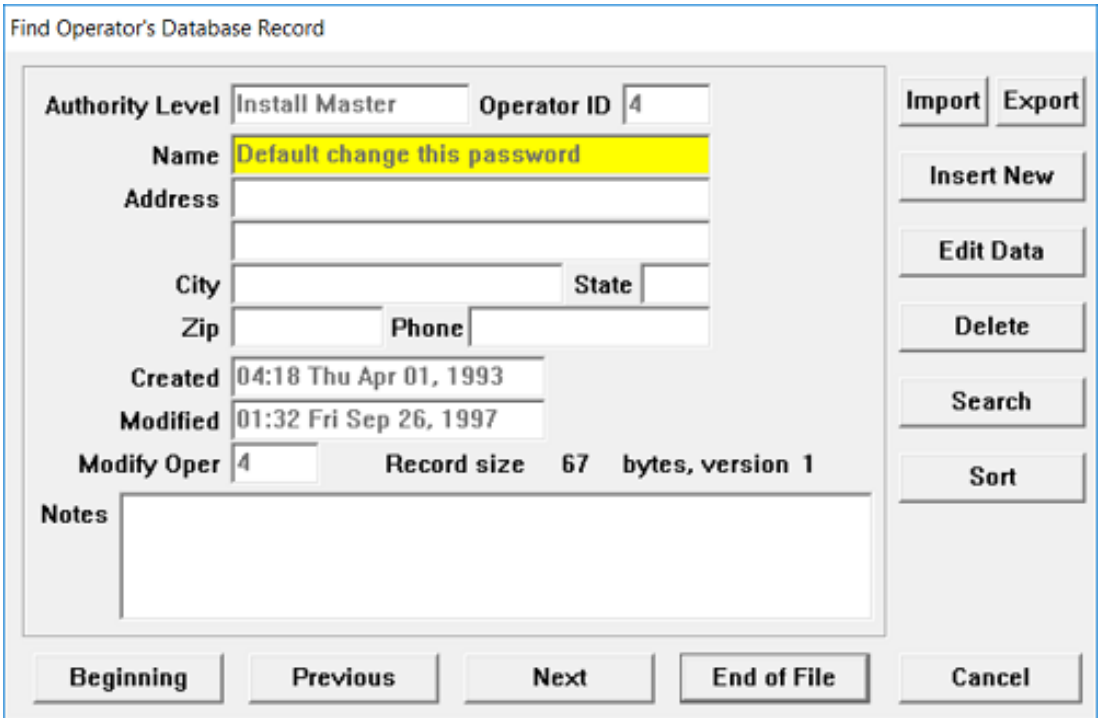


Figure 9.40: Find Operator's Database Record dialog

The information in an **Operator Database** record includes the individual's password, full name, a unique operator identification number, an authority level, local address and phone number, and notes. All fields except the **Password** field are displayed. Even when a specific operator's file is edited (via the **[Edit Data]** button); the password is represented by a number of asterisks for security reasons.

9.11.1 Edit Operator's Database Record

When adding a new operator using the **[Insert New]** button or editing the data for an existing operator using the **[Edit Data]** button, the **Edit Operator's Database Record** dialog appears. Certain information fields must be completed to produce a valid record. The password, the authority level, and the name must be entered. All the other information of the operator's record is optional, including the local address, local phone number, and notes.

Notice!

There are two boxes for passwords in the **Edit Operator's Databases Record** dialog, **Password**, and **Password Verify**. Since the operator cannot see what is being entered while typing in the password field, it must be entered twice to safeguard against errors; password modifications are not accepted if the entries in the **Password** and **Password Verify** text boxes are not identical or do not follow the password policy.

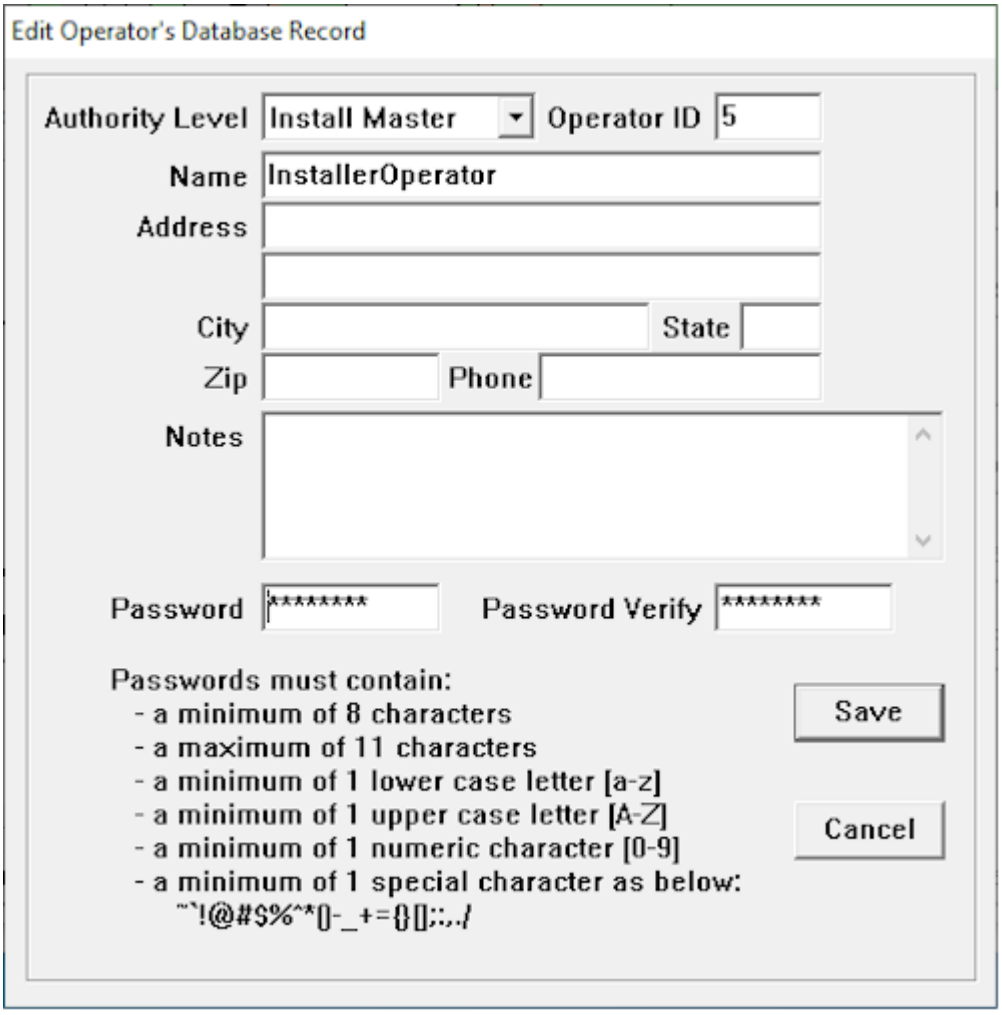


Figure 9.41: Edit Operator's Database Record dialog

The **Operator ID** field will be automatically filled in with the next available ID number, there is no need to change the number selected.

Element	Usage/Description
Authority Level	Select the authority level assigned to the operator from the drop-down list box. Different authority levels will determine different functions that the operator can perform on the system. See the following section for more details. If the drop-down list box is disabled, you do not have sufficient authorization to change the authority level.
Name	Key in the name of the operator. Maximum length is 30 alphanumeric characters.
Address Line 1	Key in the address of the operator. Maximum length is 30 alphanumeric characters.
Address Line 2	Key in the address of the operator. Maximum length is 30 alphanumeric characters.
City	Key in the city of the operator. Maximum length is 20 alphanumeric characters.

Element	Usage/Description
State	Key in the state of the operator. Maximum length is 10 alphanumeric characters.
Zip	Key in the zip code of the operator. Maximum length is 10 alphanumeric characters.
Phone	Key in the phone number of the operator. Maximum length is 16 numeric characters.
Notes	Key in the notes applicable to the operator.
Password	Key in the operator's password here. The password requirements may be different depending on the **Authority Level** chosen. **Authority Level** is “Acknowledgement”: Minimum length is 3 characters, maximum length is 11 characters. Password must be all lowercase or all uppercase. Other **Authority Level**: Minimum length is 8 characters, maximum length is 11 characters. Password must consist of at least: 1 lowercase letter, 1 uppercase letter, 1 number and 1 special character from ~`!@#$%^*()-_ +={}[];:,./
Password Verify	Repeat keying in the operator's password here. Requirement is the same as the **Password** field.
Operator ID	Non editable field. The ID is assigned by the system automatically using the running number.
[Save]	Click this button to save the changes to the operator record and return to the **Find Operator's Database Record** dialog window.
[Cancel]	Click this button to abort the changes to the operator record. A confirmation dialog will appear. Click the **[Yes]** button to save the changes, or the **[No]** button to abort the changes and return to the **Find Operator's Database Record** dialog window. Click the **[Cancel]** button to return to the **Edit Operator's Database Record** dialog window to continue making the changes.

9.11.2 Authority Level

An important consideration, when creating a new or editing an existing operator file, is the assignment of authority level. The authority level determines which functions an operator can perform on the system. Installing company representatives need access to almost every command in the Security Escort software; the key operator for the Security department usually requires access to alter the **Subscriber**, **Operator**, and **Report Database** while a dispatcher may only need access to view these databases.

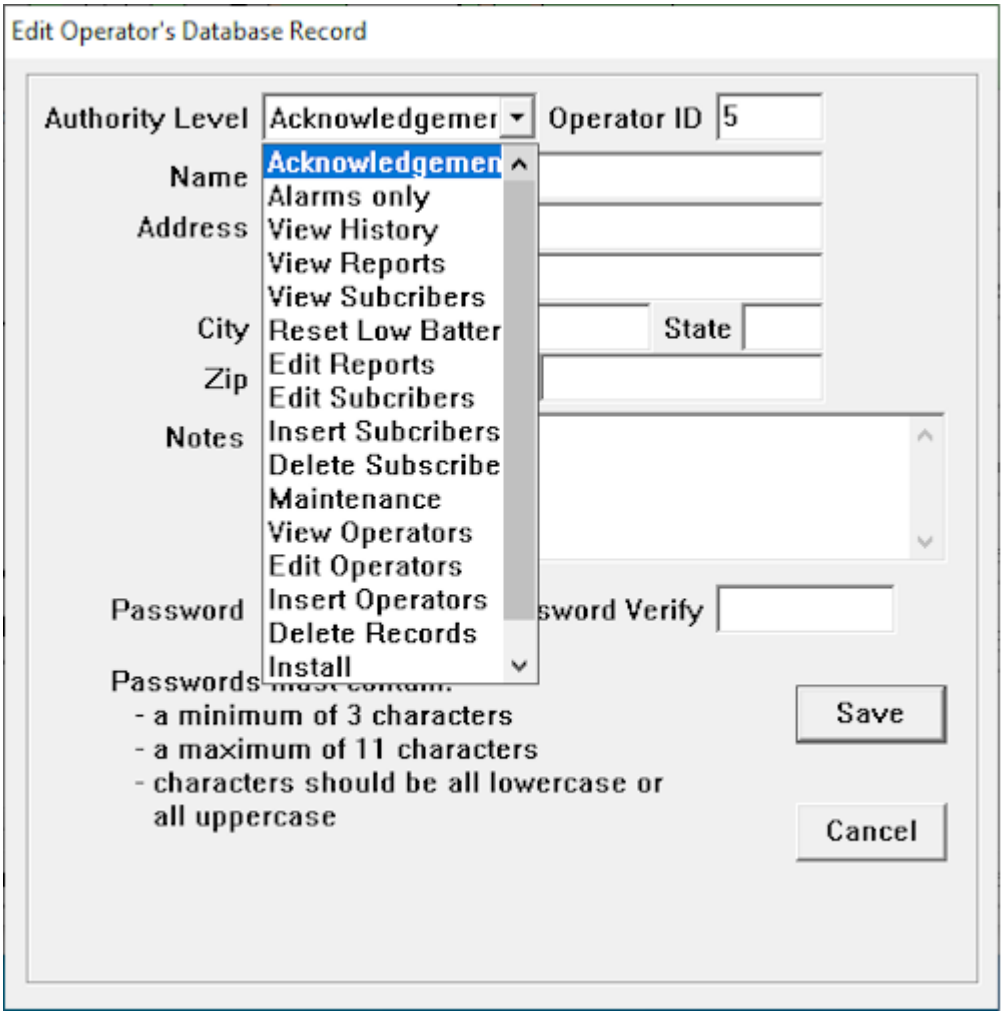


Figure 9.42: Authority Level of Edit Operator's Database Record dialog

As a rule, any operator should be assigned the minimum authority necessary to carry out their task. The authority levels shown are in order with the highest authority shown on the bottom. Each authority level has the ability to perform all of the functions of the authorities shown above it.

Operators assigned with the authority level "Acknowledgement" do not have the authority to login to SE. These operators are used for acknowledgement of alarms, "Subscriber Failed to Check-in Report" and "Points that are faulted Report" dialogs only. Attempts to login to SE using these passwords will be rejected by the system.

9.12 Exporting and importing the Operator Database

The following sections describe the steps to export and import data from and into the **Operator Database**. Only users or operators who are assigned the minimum security level of "Edit Operators" is able to perform the export and import of the **Operator Database**. The file supported is the XML file format.

9.12.1 The XML file format

The XML tree consists of the *<Operators>* main element. The *<Operators>* element is the parent element of the *<Operator>* child element. The *<Operator>* child element has the following sub-elements: *<Password>*, *<ModifyOp>*, *<ActualBufferLength>* and *<RecordVersion>*.

Below is an example of a typical tree with an empty structure:

```
<Operators>
    <Operator>
        <Password></Password>
        <ModifyOp></ModifyOp>
        <ActualBufferLength></ActualBufferLength>
        <RecordVersion></RecordVersion>
    </Operator>
</Operators>
```

9.12.2 Exporting the Operator Database

To export data from the **Operator Database**, go to menu **File > Operator Database** dialog, and click the **[Export]** button.

Notice!
The export operation does not change the existing records in **Operator Database**.

A file dialog appears for you to choose the folder where you wish to save the file in, and provide a name for the file.

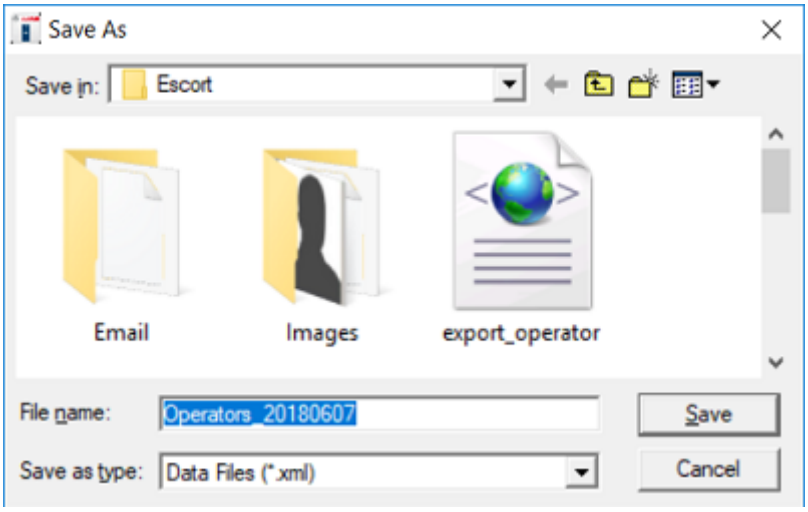


Figure 9.43: Export file dialog

If you wish to abort the task, click the **[Cancel]** button. Otherwise, click the **[Save]** button to export the **Operator Database**. If a file of the same name already exists, a confirmation dialog appears asking if you wish to replace the file.

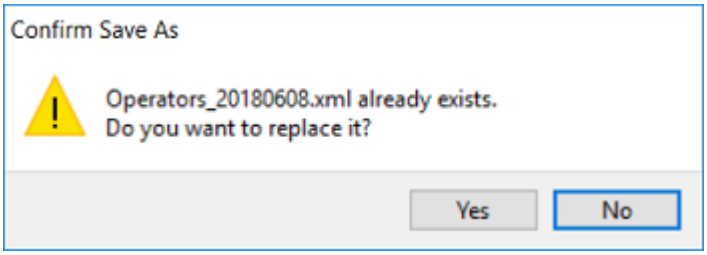


Figure 9.44: Replace file confirmation dialog

Click the **[No]** button to abort and return to the file dialog box where you can choose a different name for the file. Otherwise, click the **[Yes]** button to proceed with replacement of the file. If the export is successful, a confirmation dialog appears. You will find the file in the specified folder.

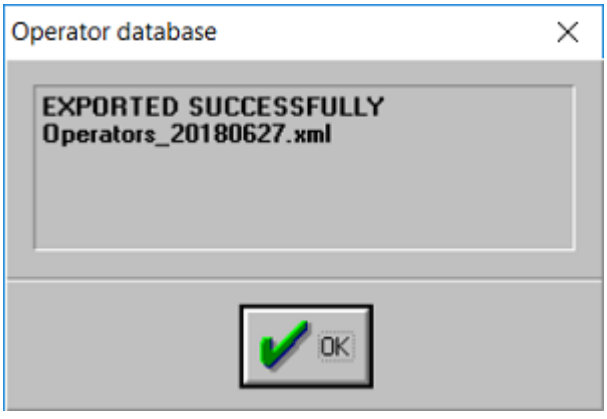


Figure 9.45: Operator Database successfully exported dialog

9.12.3 Importing the Operator Database

To import data into the **Operator Database**, the file to import must already be prepared in the XML file format. Go to menu **File > Operator Database** dialog, and click the **[Import]** button.

Notice!
There is no way to undo the operations. Therefore, it is recommended to **perform a database backup** prior to starting the task. Upon completion of the task, verify the updated data before the new database is placed in service. If there are problems, restore the **Operator Database** from the backup.

A popup dialog appears asking for the file to be imported. Click the **[Cancel]** button to abort if you are still unsure. Otherwise, navigate the folders, select the file and click the **[Open]** button.

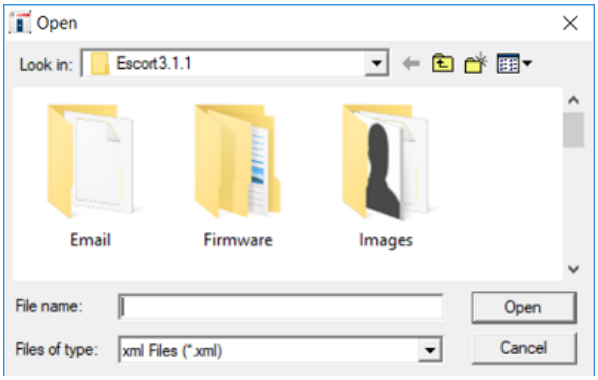


Figure 9.46: Import file dialog

A popup dialog appears, asking for confirmation to proceed with the import or to abort the operation. Click the **[No]** button to abort if you are still unsure. Click the **[Yes]** button to proceed with the import.

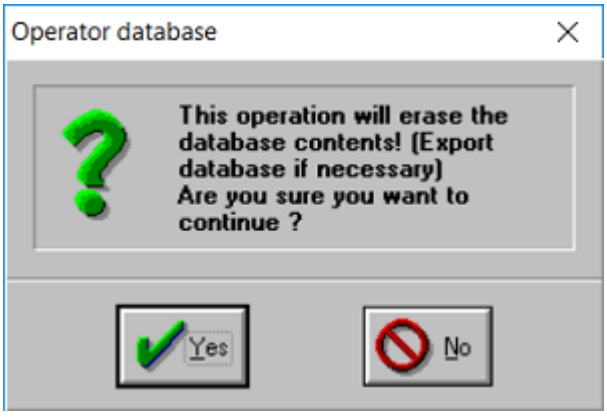


Figure 9.47: Import confirmation dialog

Be patient, as it may take a while, and watch for the disk activity to stop. If the data is imported successfully, a popup confirmation dialog appears. If the data is not imported successfully, a popup error message appears. The error message will indicate the likely cause of the import to fail.

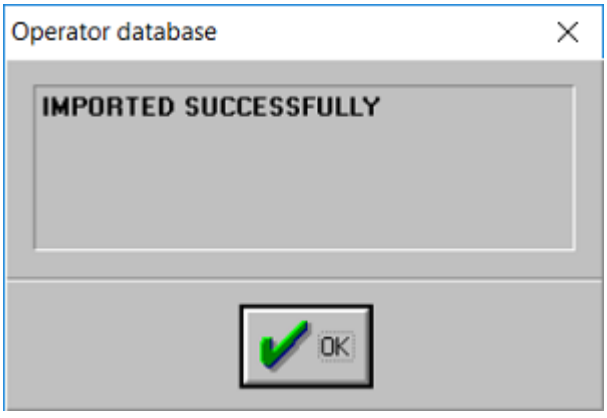


Figure 9.48: Operator Database successfully imported dialog

9.13 Reports Database

The Security Escort software contains a report-generating feature that encourages prompt, uniform reporting of incidents. A sample of the alarm report dialog is shown in the figure below. The system software automatically captures the alarm data displayed on the alarm screen and enters it into a report form. The form also contains fields that describe the nature of the incident and the action taken. These fields are to be filled in by the responding officer.

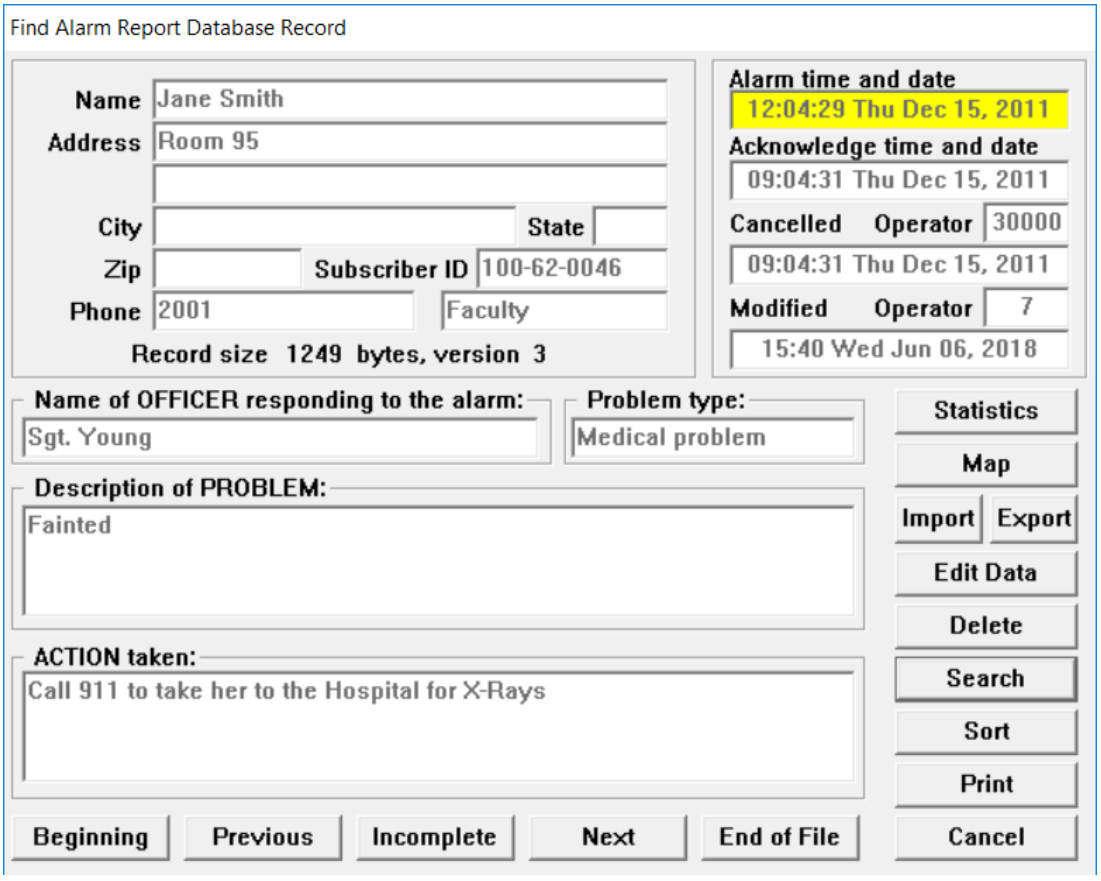


Figure 9.49: Find Alarm Report Database Record dialog window

The system software can be configured to require that a report be completed prior to the end of the shift in which the incident occurred. If the **Require Alarm Report** option is chosen in the **Security Preferences** dialog, the report can be filled out immediately after the alarm is reset. However, if the report is not completed a reminder prompt appears on the screen every 5 minutes for 30 minutes before the end of the shift. The time at which the prompt is to display is also set in the **Security Preferences** dialog.
All of the common database commands are available in the **Reports Database**, with the following additional commands.

9.13.1 Statistics

Click the **[Statistics]** button to summarize all the alarm reports that are captured in the database. The alarm reports statistics window lists the number of alarms reports according to their problem types.

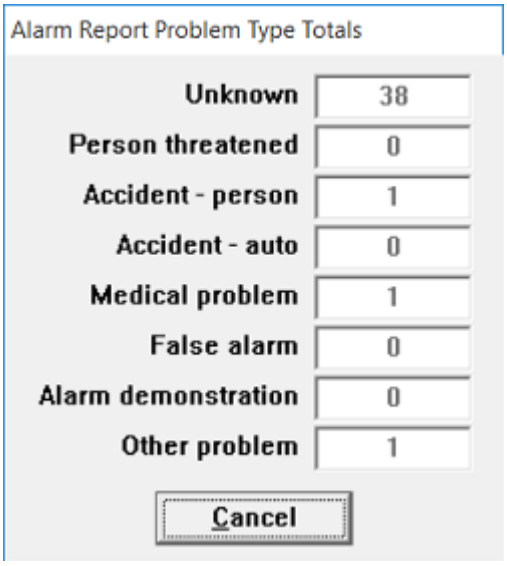


Figure 9.50: Alarm Report Statistics window

9.13.2 Map

The act of resetting an alarm causes a report to be saved into the **Reports Database**. A part of the alarm report record is a copy of the alarm screen that is displayed at the time of the incident. Clicking the **[Map]** button reconstructs the screen as it appeared to the dispatcher.

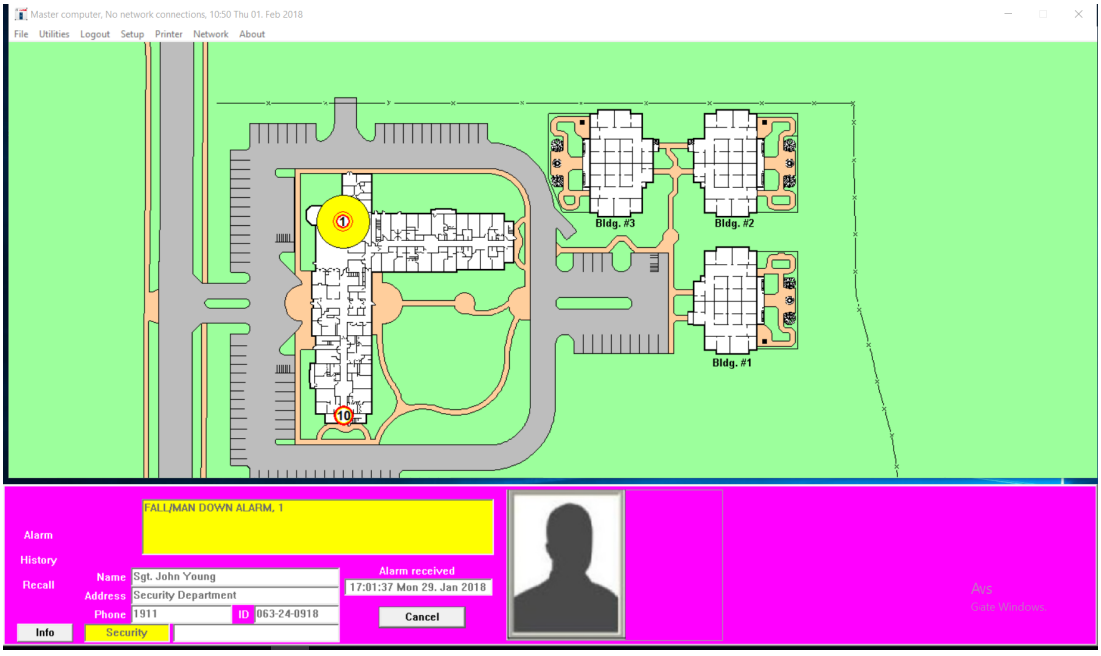


Figure 9.51: Active Alarm Map

9.13.3 Edit Data

Select the appropriate problem type, and then enter the name of the officer who responded to the alarm. Finish with a description of the problem and the action taken. Save the changes by clicking the **[Save]** button.

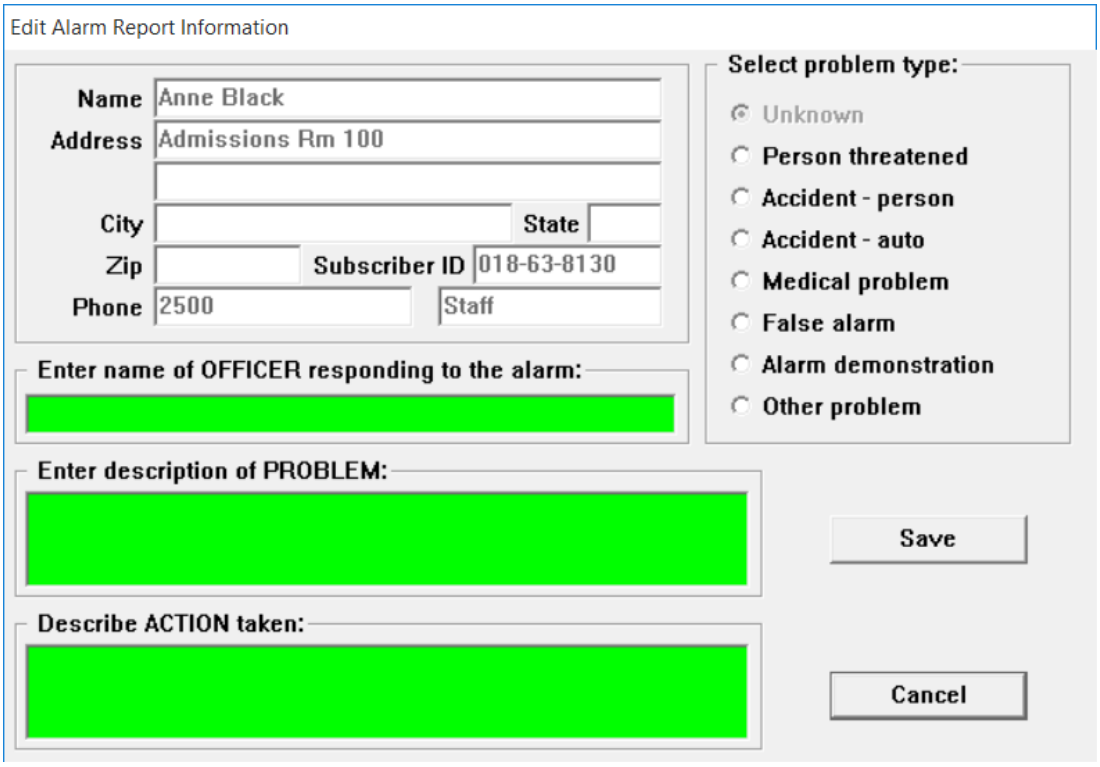


Figure 9.52: Edit Alarm Report Information dialog window

9.13.4 Delete

Click this button to delete the alarm report from the **Reports Database**. If the report is deleted, the data can not be recovered. A confirmation dialog appears.

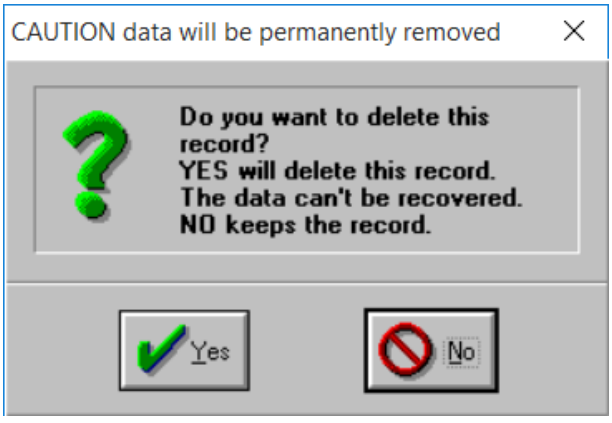


Figure 9.53: Delete Confirmation dialog window

Click the **[Yes]** button to delete the record permanently, or the **[No]** button to abort deletion, and return to the **Find Alarm Report Database Record** dialog window.

9.13.5 Search

This button works similarly to the **[Search]** button in the **Operator** and **Subscriber Database**. Entering the **Subscriber Name**, **Transmitter ID**, **Subscriber ID**, **Subscriber Class**, problem type, or a specific time and date can locate a specific report.

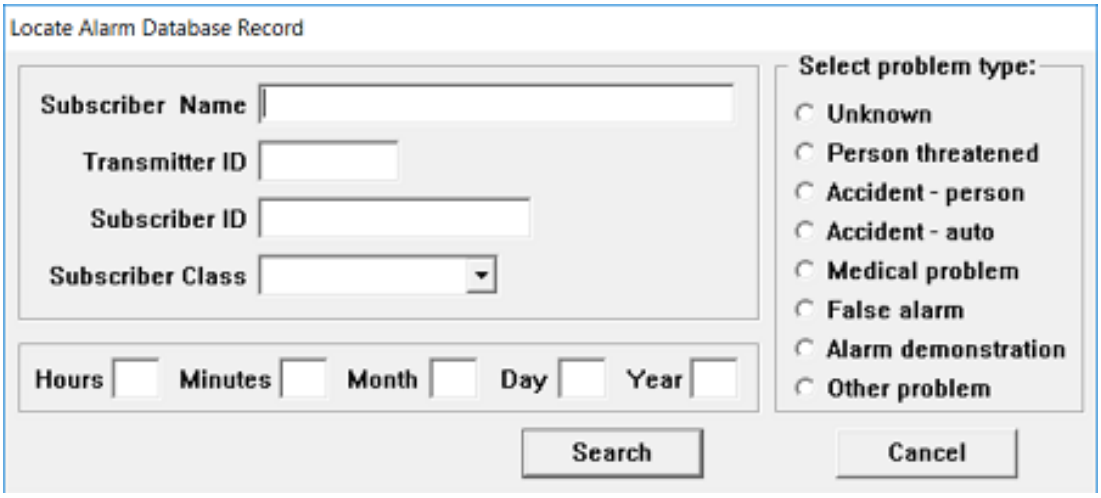


Figure 9.54: Locate Alarm Database Record dialog window

Click the **[Search]** button to search for the reports as specified by the selected criteria, and return to the **Find Alarm Report Database Record** dialog window. As in the **Operator** and **Subscriber Database**, the alarm reports are temporarily ordered according to the field entered in the **Search** dialog. The first report that matches the search is the record that you see in the **Find Alarm Report Database Record** dialog window.
Click the **[Cancel]** button to return to the **Find Alarm Report Database Record** dialog window without performing a search.

9.13.6 Sort

This button works similarly to those of **Operator** and **Subscriber Database**. Using it, the reports can be ordered by **Subscriber Name**, **Transmitter ID**, **Subscriber ID**, **Alarm Time**, **Problem Type**, or **Subscriber Type**.

Figure 9.55: Select Database Key dialog window

Click the **[Select]** button to sort the reports in the **Find Alarm Report Database Record** dialog window according to the key field selected. Click the **[Cancel]** button to return to the **Find Alarm Report Database Record** dialog window without sorting using the key field selected.

9.13.7 Incomplete

Click this button to jump to the most recent incident report file that has not been completed. The reports are not reordered when this command is used.

9.14 Exporting and importing the Reports Database

The following sections describe the steps to export and import data from and into the **Reports Database**. The file supported is the XML file format.

9.14.1 The XML file format

The XML tree consists of the *<Reports>* main element. The *<Reports>* element is the parent element of the *<Report>* child elements. The *<Report>* child element has a list of sub-elements that defines the data of the reports.

A simplified example of a typical tree with an empty structure is as of below:

```
<Reports>
    <Report>
    </Report>
</Reports>
```

9.14.2 Exporting the Reports Database

To export data from the **Reports Database**, go to menu **File > Reports Database** dialog, and click the **[Export]** button.

Notice!
The export operation does not change the existing records in **Reports Database**.

A file dialog appears for you to choose the folder where you wish to save the file in, and provide a name for the file.

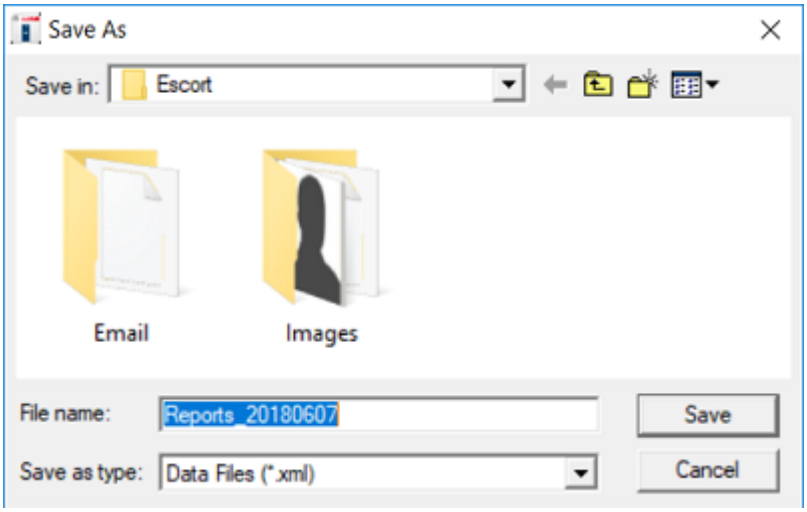


Figure 9.56: Export file dialog

If you wish to abort the task, click the **[Cancel]** button. Otherwise, click the **[Save]** button to export the **Reports Database**. If a file of the same name already exists, a confirmation dialog appears asking if you wish to replace the file.

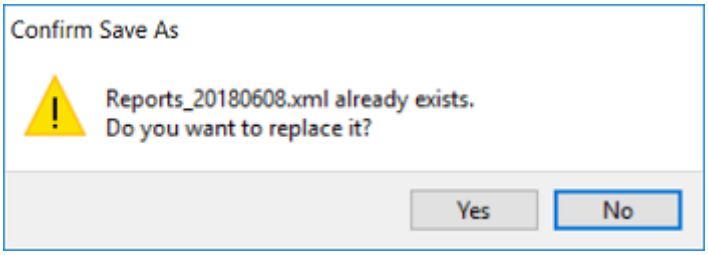


Figure 9.57: Replace file confirmation dialog

Click the **[No]** button to abort and return to the file dialog box where you can choose a different name for the file. Otherwise, click the **[Yes]** button to proceed with replacement of the file. If the export is successful, a confirmation dialog appears. You will find the file in the specified folder.

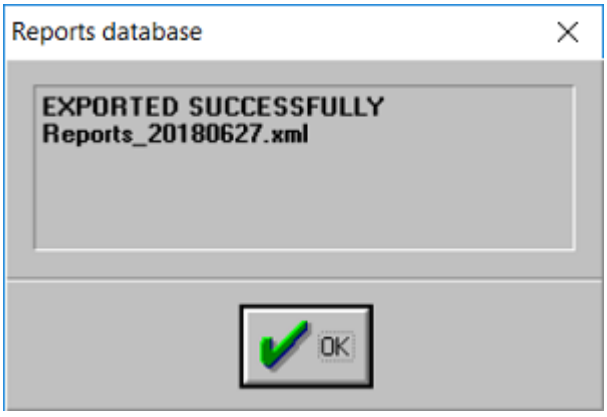


Figure 9.58: Reports Database successfully exported dialog

9.14.3 Importing the Reports Database

To import data into the **Reports Database**, the file to import must already be prepared in the XML file format. Go to menu **File > Reports Database** dialog, and click the **[Import]** button.

Notice!
There is no way to undo the operations. Therefore, it is recommended to **perform a database backup** prior to starting the task. Upon completion of the task, verify the updated data before the new database is placed in service. If there are problems, restore the **Reports Database** from the backup.

A popup dialog appears asking for the file to be imported. Click the **[Cancel]** button to abort if you are still unsure. Otherwise, navigate the folders, select the file and click the **[Open]** button.

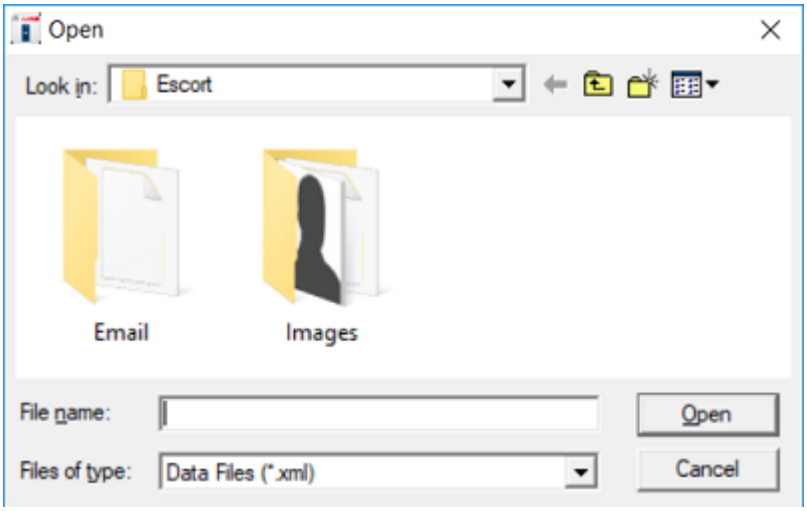


Figure 9.59: Import file dialog

A popup dialog appears, asking for confirmation to proceed with the import or to abort the operation. Click the **[No]** button to abort if you are still unsure. Click the **[Yes]** button to proceed with the import.

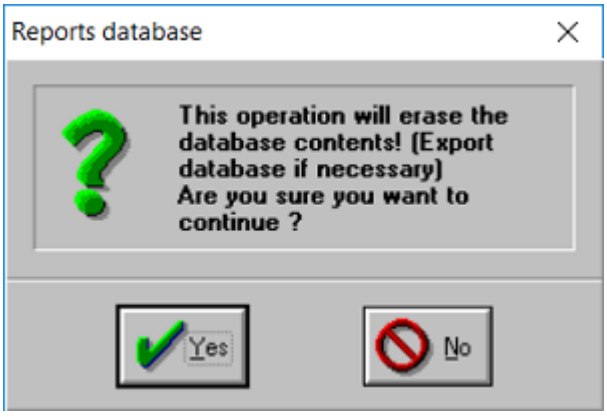


Figure 9.60: Import confirmation dialog

Be patient, as it may take a while, and watch for the disk activity to stop. If the data is imported successfully, a popup confirmation dialog appears. If the data is not imported successfully, a popup error message appears. The error message will indicate the likely cause of the import to fail.

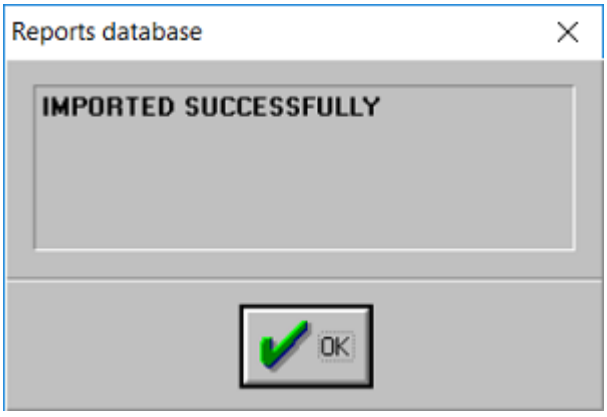


Figure 9.61: Reports Database successfully imported dialog

9.15 System redundancy

The Security Escort system redundancy is operational as long as master and slave controllers are configured in a network setup. By default, master computer is the one controlling the devices. If the master computer is unavailable for some reasons, slave computer could take over the operation automatically. Once the master computer is back online, slave computer will hand over the control to the master computer. If both the master and slave computers are not available, the system is not operational. Devices will take control by themselves.

Notice!
In the event where the master computer is unavailable and the slave computer takes control of the devices, alarms will be reported on the slave computer. If the master computer becomes available again, it will try to take control of the devices.
However, if there are still **unacknowledged alarms** on the slave computer, the master computer will not succeed in taking control, as the alarms need to be acknowledged on the slave computer first. The master computer will try to take control of the devices continuously until the unacknowledged alarms on the slave computer are acknowledged accordingly.
During the acknowledgement process, the receiver's sounders and red LEDs may not be turned off properly. You may need to turn these off manually from menu **Setup > Receiver configuration**.

System will automatically determine which computer will be the main controller based on the online availability of the master and slave computers. Automatic redundancy kicks in during the following circumstances:

1. Master computer information is not configured in slave computer - If the master computer's related information is not configured in the slave computer, the slave computer will consider the master computer as unavailable. As such, the control of devices will switch to the slave computer automatically.
2. Master computer not reachable from slave computer - If the master computer's related information is configured in the slave computer, but the slave computer is unable to connect to the master computer, the slave computer will keep attempting to connect for 10 consecutive times. If the slave computer is still unable to connect to the master computer, the control of devices will switch to the slave computer automatically.
3. Master computer not responding - The slave computer will send "heart beat" messages to the master computer every second. The master computer will acknowledge each "heart beat" messages to the slave computer. If the slave computer did not receive 6 continuous "heart beat" acknowledgements from the master computer, the slave computer will consider the master computer as unreachable. As such, the control of devices will switch to the slave computer automatically.
4. Master computer acknowledges "heart beat" message - The slave computer will send the "heart beat messages" continuously. Once the slave computer receives the "heart beat" acknowledgement from the master computer, the slave computer will consider the master computer as being back in operation. As such, the slave computer disconnects all the devices and requests the master computer to take control of the devices.

10 System menus and dialogs

10.1 File menu

This pull-down menu leads to the main databases for the system. Key operators with the appropriate authority levels can view and modify the operator, alarm report, and subscriber databases.

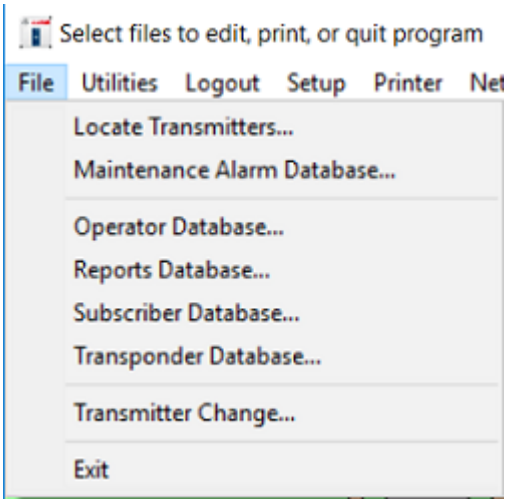


Figure 10.1: File menu

10.1.1 Locate transmitters

This selection allows the operator to display the last reported location of the transmitter assigned to the indicated individual or asset. When the individual or asset is selected from the list, the time of the last supervision report is shown (or “None” is displayed if no supervision report was received from that transmitter). On the map, the last report location is shown.

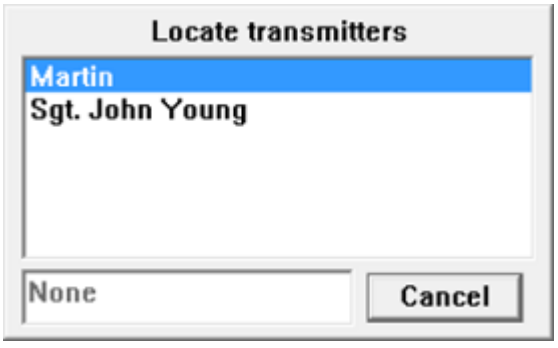


Figure 10.2: Locate transmitters dialog

10.1.2 Maintenance alarm database

Maintenance transmitters, when activated in the “test” or “alarm” mode, generate a series of multiple data packets like subscriber transmitters. However, a special code in each packet identifies the transmitter as a “Maintenance Transmitter”.

The receiver responds to a maintenance “alarm” or “test” transmission in the same way it responds to a subscriber “alarm” or “test”, unless the SE receiver has been put in the “setup” mode. The SE coordinator then reports the maintenance transmitter identification number and all signal levels to the Central Console, which then creates the location estimate and processes the data as it would for a normal alarm.

Notice!
All maintenance transmitters are assumed to be valid, so there is no need for the Central Console to check for the identification number in the Subscriber database.

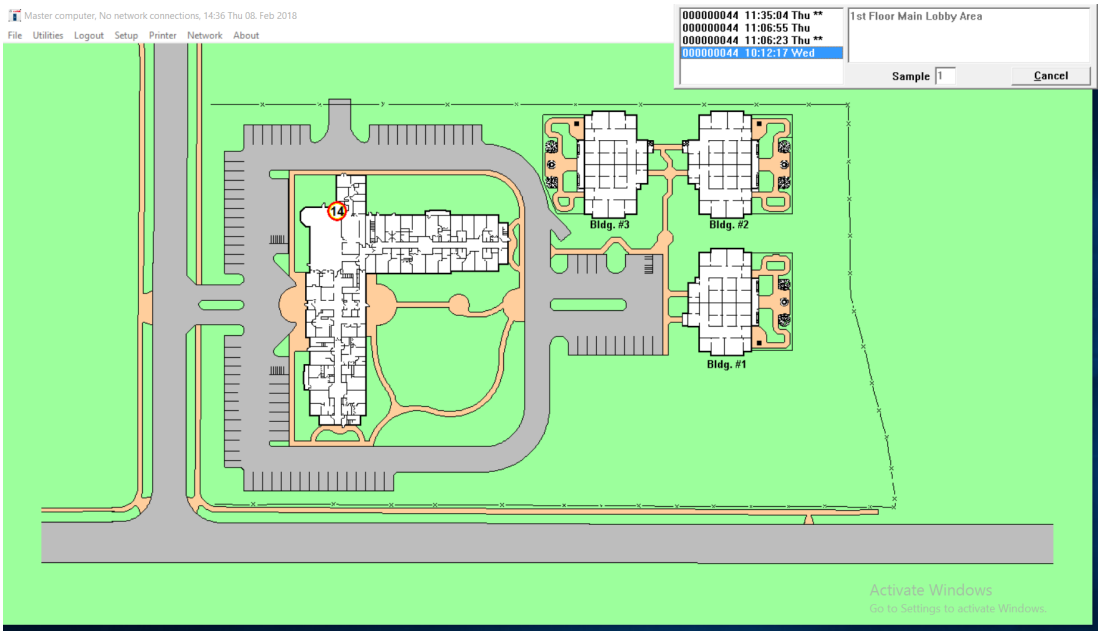


Figure 10.3: Maintenance "Alarm" with signal levels shown in icons

The Central Console will not generate an audible alert for the operator, nor will it create an "alarm" display on the main Central Console screen. Because they can be set to graphically display received signal levels, maintenance "alarms" are very useful to verify that the system coverage exists at any location in the protected area, and that SE receiver redundancy is adequate.

10.1.3 Operator Database

The **Operator Database** contains information on the individuals who are authorized to operate the system, their authority levels, and passwords. See *Operator Database, page 150* for details.

10.1.4 Reports database

The **Reports database** contains information of alarms that were previously processed by the system. Alarm data and maps showing the operators view can be recalled. See *Reports Database, page 157* for details.

10.1.5 Subscriber database

The **Subscriber database** contains information on the transmitters that are assigned in the system. See *Subscriber Database, page 124* for details.

10.1.6 Transponder database

The **Transponder database** is established at system set-up and contains all necessary configuration data for each SE coordinator and SE receiver. It describes the basic structure of the installation, including all device names, locations, types, multiplex addresses, etc. See *Transponder Database, page 66* for details.

10.1.7 Transmitter Change

The **Transmitter Change** feature on the **File** menu is used when it is necessary to change a subscriber's transmitter.

Selecting **Transmitter Change** opens the **Locate Subscriber's Database Record** dialog. The subscriber's record in the **Subscriber Database** can be quickly found by entering the information into the specific field as of below:

- **Subscriber Name**
- **Subscriber ID**
- **Transmitter ID**
- **Address Items**
- **Phone Number**
- **Info Field Search**
- **Pager Items**
- **Pager Group**

This method of locating a particular subscriber's record is identical to using the **[Search]** button in the **Subscriber Database**: the first record, which is identical to the entered data, is shown. It may be necessary to scroll using the **[Previous]** and **[Next]** buttons to find the correct record.

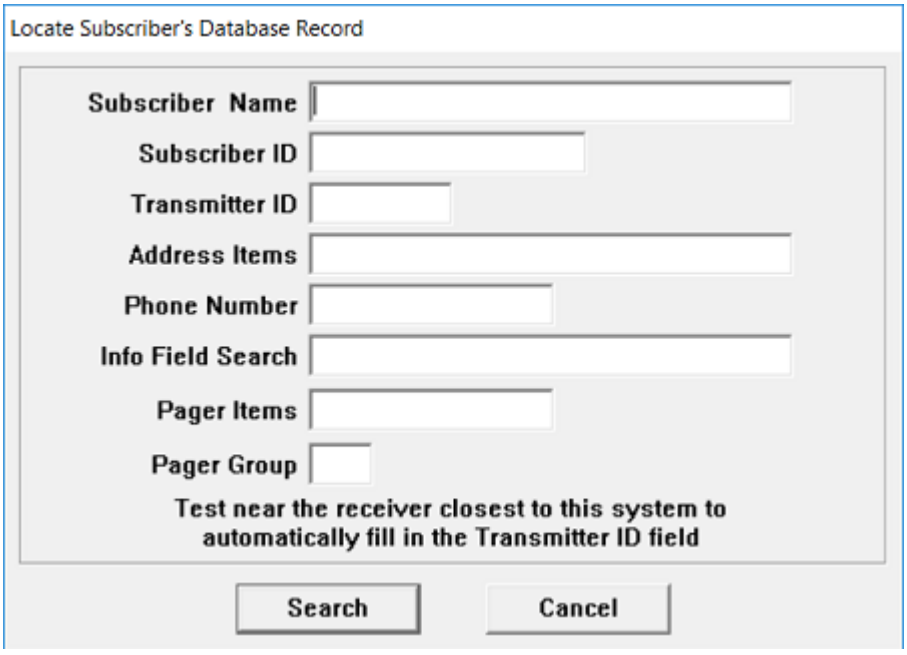


Figure 10.4: Locate Subscriber's Database Record dialog

Perform a test using the old transmitter if possible. This should populate the **Transmitter ID** field. Then click the **[Search]** button.

Notice!

Be absolutely certain that the correct record is displayed before entering the new **Transmitter ID** (Identification Code). Changing the wrong subscriber's record makes two records ineffective: the correct subscriber will be misidentified and the subscriber whose record was incorrectly altered will be disabled. If possible, perform a test with the subscriber's old transmitter after the change has been made: the test should fail.

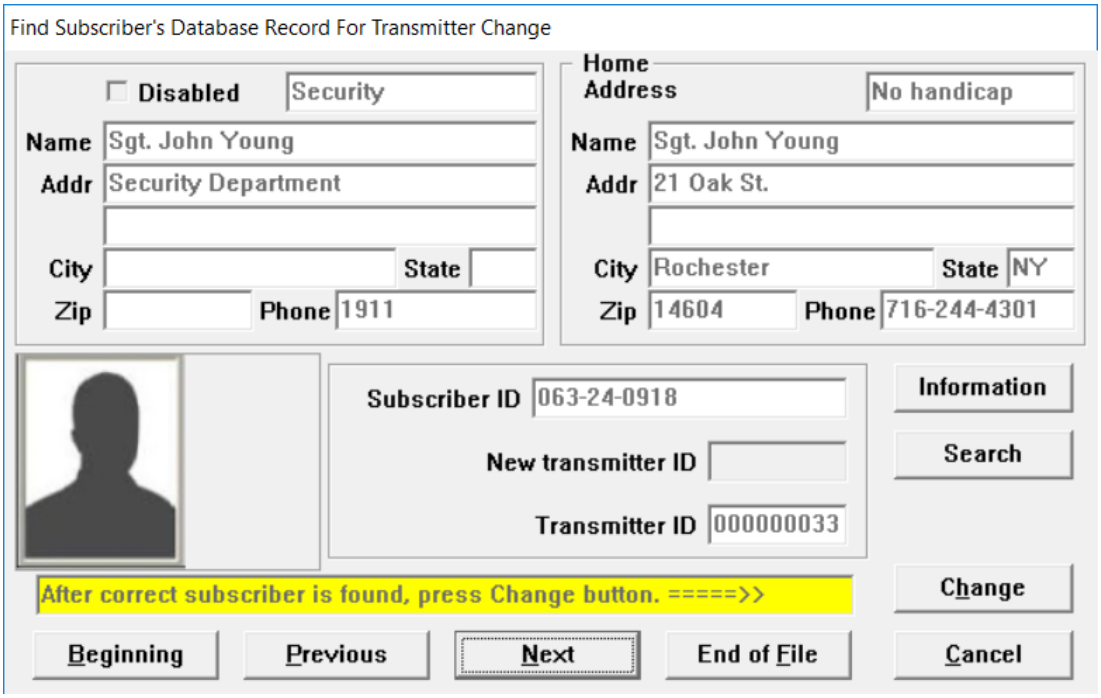


Figure 10.5: Subscriber's Database Record dialog window

When the correct subscriber record is displayed, click the **[Change]** button and perform a test using the new transmitter. The new transmitter identification code will automatically populate in the **New transmitter ID** field.

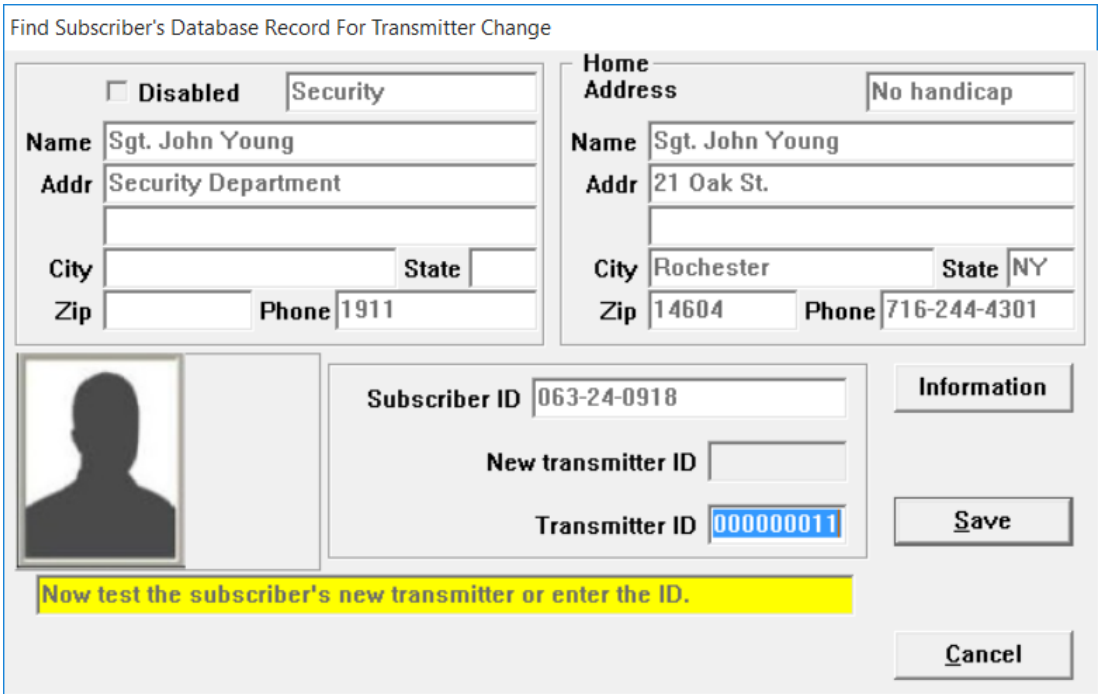


Figure 10.6: Subscriber's Database Record dialog

Enter the **New transmitter ID** into the **Transmitter ID** field manually, or use the mouse to highlight the old **Transmitter ID** value, press and hold the <Shift> key and tap the <Insert> key. Then, click the **[Save]** button. A prompt appears, asking for a second test to confirm the change.

Test the new transmitter again. You should see a green light on a nearby SE receiver, and this dialog should automatically disappear from the screen, confirming that the change was successful.

10.2 Utilities menu

From this menu, key operators can backup or restore the databases for the system, set the options for the operation of the system, clear the map screen, and other features.

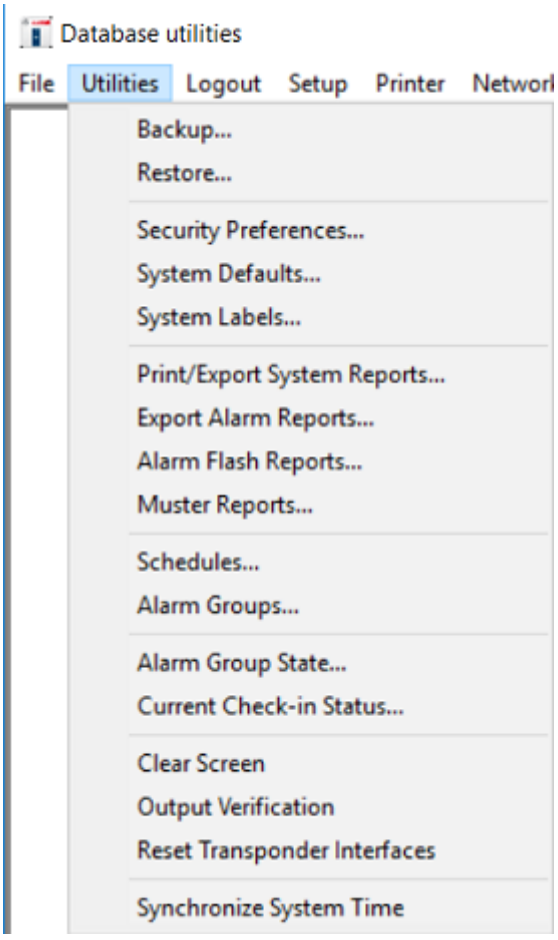


Figure 10.7: Utilities menu

10.2.1 Backup

This feature provides a convenient process for saving the information in the databases to backup files.

Warning!
To prevent the accidental loss, the databases should be backed up at least once a week to multiple backups. At least one of these backup copies should be kept in a different location from the Central Console's location.

Weekly backups are recommended to permit data recovery if the computer memory should become corrupted. If this unlikely event occurs, an operator can quickly restore the databases in question with the **Restore** feature. Backups should be made any time significant changes are made to any database.

Notice!
If the Security Escort system is configured to share the database, you will need to exit the Security Escort program on all slave and workstation computers. The master computer will not be able to perform the backup properly as other computers are also using the files. The master computer needs to have exclusive use of the database files.

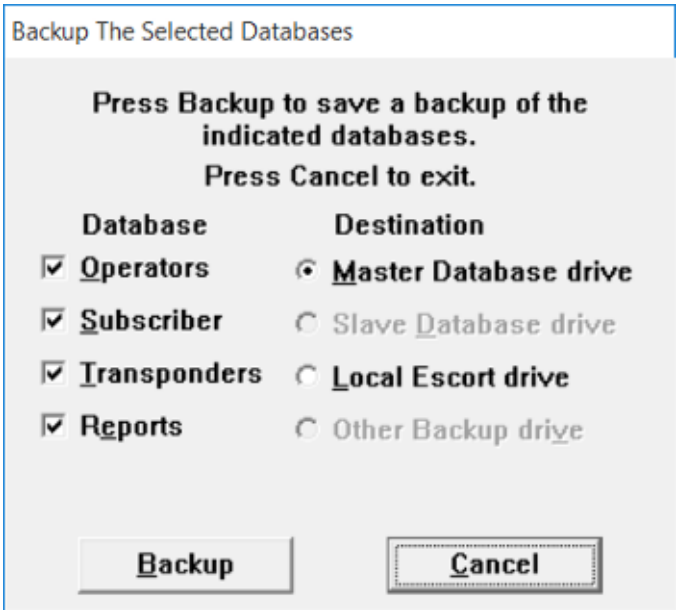


Figure 10.8: Backup dialog

When the **Backup** menu item is chosen, options are presented to save the databases to the master or slave computer's hard drive. Verify that the backup destination is available before clicking the **[Backup]** button. To abort the process, click the **[Cancel]** button in the dialog. Only the databases that are selected will be backed up. Typically all databases should be backed up at least once. As insurance against database problems, multiple backups to different disks should be made frequently. At least one backup copy should be stored in a different location from this system (remember to keep this copy current).

Element	Usage/Description
Operators	This is the database of all of the individuals with passwords to operate the system software and acknowledge alarms.
Subscriber	This database contains all transmitters assigned in the system.
Transponders	This database contains the configuration of the coordinators, receivers, virtual receivers and area data.
Reports	This database contains all of the alarm reports and related alarm map screens.
Master Database drive	Store the backup files in the Security Escort **Master Database path**. See the **System Directories and Network Address** dialog.
Slave Database drive	Store the backup files in the Security Escort **Slave Database path**. See the **System Directories and Network Address** dialog.

Element	Usage/Description
Local Escort drive	Store the backup files in the same sub-directory where the Security Escort system components are stored on this computer (typically "C:\ESCORT").
Other Backup drive	Store the backup files in the **Other Backup/Restore path** assigned in the **System Directories and Network Address** dialog. This path may be a local path, external drive or a network disk drive.
[Backup]	Click this button to save the selected databases to the selected destination drive.
[Cancel]	Click this button to cancel the backup.

10.2.2 Restore

Should one or more database files become corrupted or erased due to a hard drive failure, power surges or other unpredictable events, it is necessary to restore the databases from backup files. The **Restore** function allows loading of selected databases from backup files. It is not necessary to perform the **Restore** function on all databases in order to restore any one. All changes that occurred since the last backup are lost when a database is restored. Therefore, restore only those databases with a problem. Backups should be made whenever significant changes are made to any database.

Notice!
If the Security Escort system is configured to share the database, you will need to exit the Security Escort program on all slave and workstation computers. The master computer will not be able to perform the restore properly as other computers are also using the files. The master computer needs to have exclusive use of the database files.

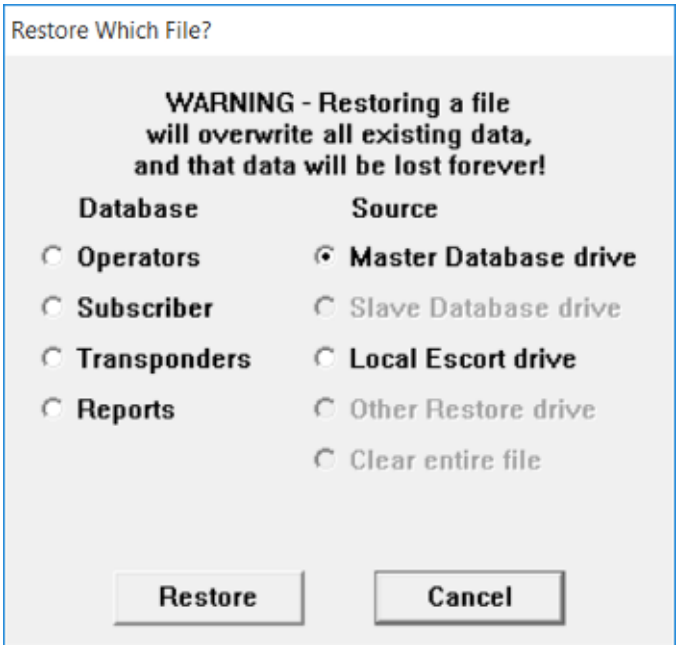
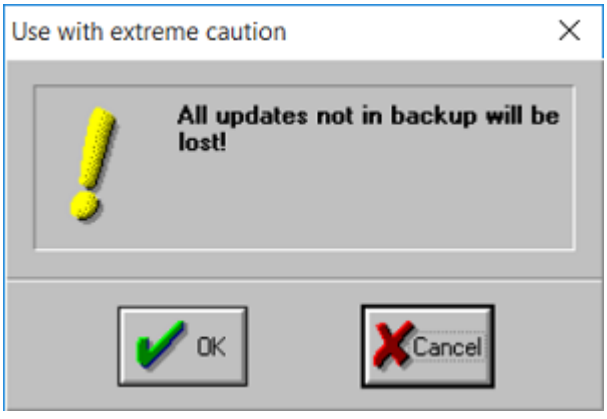
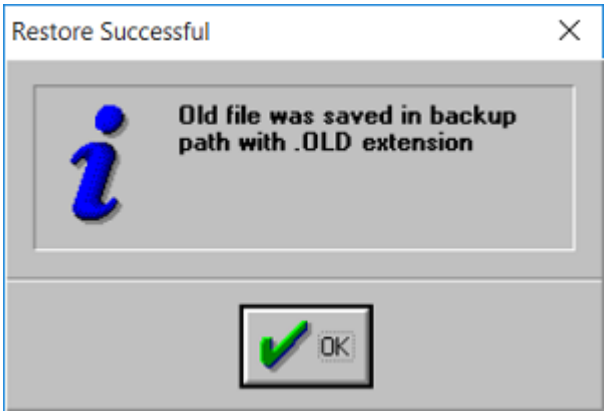


Figure 10.9: Restore dialog

Select the database to be restored on the left. On the right, this is where the database backup is currently located. Click the **[Restore]** button to replace the existing database file with the backup. This process also rebuilds the database and its index tables to correct most database structure problems. To abort the restore process, click the **[Cancel]** button.

Element	Usage/Description
Operators	This is the database of all of the individuals with passwords to operate the system software and acknowledge alarms.
Subscriber	This database contains all of transmitters assigned in the system.
Transponders	This database contains the configuration of the coordinators, receivers, virtual receivers and area data.
Reports	This database contains all of the alarm reports and related alarm map screens.
Master Database drive	Restore the backup files in the Security Escort **Master Database path**. See the **System Directories and Network Address** dialog.
Slave Database drive	Restore the backup files in the Security Escort **Slave Database path**. See the **System Directories and Network Address** dialog.
Local Escort drive	Restore the backup files in the same sub-directory where the Security Escort System components are stored on this computer (typically "C:\ESCORT").
Other Restore drive	Restore the backup files in the **Other Backup/Restore path** assigned in the **System Directories and Network Address** dialog. This path may be a local path, external drive or a network disk drive.
Clear entire file	Clear all records from the entire database. This selection must be used with extreme caution! Hold down the <Shift>+<Ctrl> keys when opening the dialog to enable the **Clear entire file** option.
[Restore]	Click this button to restore the selected database to the selected destination. The following message box appears.  This message box is a reminder that if changes to the system databases have been made since the backup was made, the changes will be lost. Therefore those changes must be redone to the restored database. Click the **[OK]** button to proceed with the restore, or the **[Cancel]**

Element	Usage/Description
	button to abort. Upon clicking the **[OK]** button, restore would proceed and the following message box should appear.  This message box indicates the restore has been completed. The previous database file has been renamed with an .OLD extension and saved in the Security Escort sub-directory. Only the most recent database of each type is retained with each restore.
[Cancel]	Click this button to abort restoring the database.

10.2.3 Security Preferences

The **Security Preferences** dialog is used to make important settings that govern how the Security Escort system reacts in the event of alarm and test transmissions from the subscribers' transmitters. This dialog is available only to the Security Director or his/her key operator.

See *Security Preferences, page 114* for details.

10.2.4 System Defaults

This dialog allows the names for each class of subscribers to be changed to match the specific application of this Security Escort system.

See *System Defaults, page 122* for details.

10.2.5 System Labels

The alarm type definitions are customized to customer's requirements in this dialog window.

See *System Labels, page 123* for details.

10.2.6 Print/Export System Reports

This dialog allows the system reports to be printed on demand, scheduled for printing each night at midnight or weekly on Sunday at midnight. To print a report, select the left-checkbox for each desired report and click the **[Print]** button. Select the **Midnight report** or the **Sunday only** checkboxes to automatically schedule the selected report at those times.

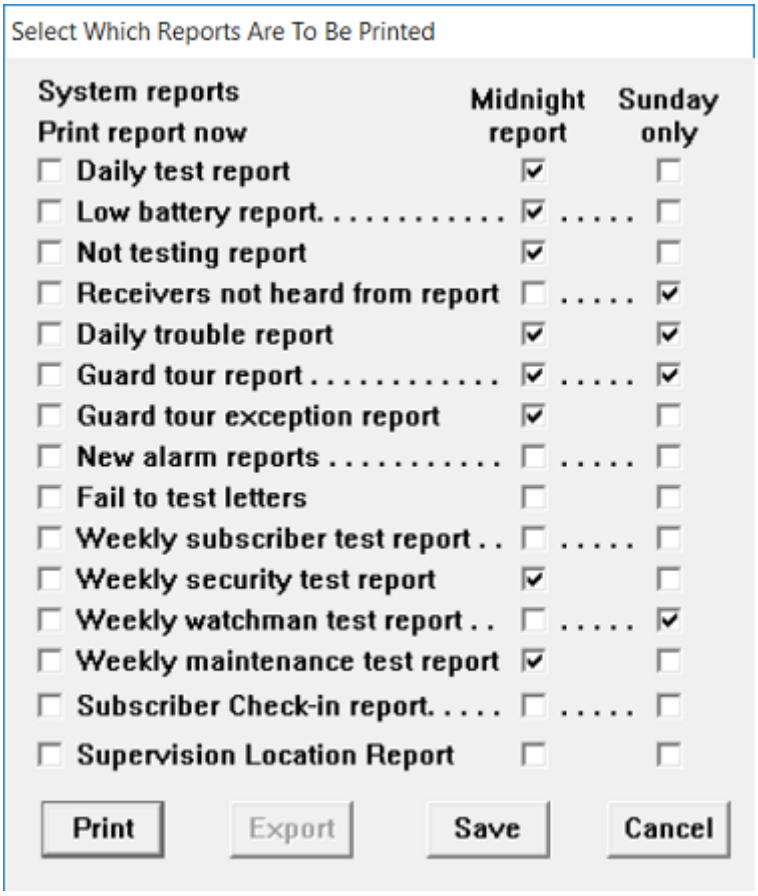


Figure 10.10: Print/Export System Reports dialog

Element	Usage/Description
Daily test report	Report of testing by classes of subscriber for the last 24 hours broken down by hour.
Low battery report	Report of all subscriber transmitters currently reporting low battery.
Not testing report	Report of all subscriber transmitters that have not tested their transmitters within the last 28 days.
Receivers not heard from report	Report of all SE receivers that have not heard transmissions recently. This could indicate a problem with the SE receiver's ability to hear alarms and test transmissions.
Daily trouble report	Report of all the troubles currently being reported by SE coordinators and SE receivers.
Guard tour report	Report of the guard tours collected within the last day. This selection does not generate a printed report. However, the **Midnight report** and **Sunday only** checkboxes must be checked to write a file of the guard tour information. Another application like Microsoft Excel can sort and print the desired reports.
Guard tour exception report	The guard tour exception reports collected within the last day. Not currently implemented.

Element	Usage/Description
New alarm reports	Alarm reports for all of the new alarms that have been received by the system.
Fail to test letters	Notices to all of the subscribers that have not tested within the last 28 days. Not currently implemented.
Weekly subscriber test report	Report of subscriber testing for the last 7 days broken down by hour.
Weekly security test report	Report of security personnel testing for the last 7 days broken down by hour.
Weekly watchman test report	Report of watchman personnel testing for the last 7 days broken down by hour.
Weekly maintenance test report	Report of maintenance testing for the last 7 days broken down by hour.
Subscriber Check-in report	Report of all subscribers that failed to check-in during the last scheduled check-in period.
Supervision Location report	Report of all supervision enabled subscribers and their last known location.
Print report now	Reports that are selected will be printed immediately when the **[Print]** button is clicked.
Midnight report	Reports are generated every midnight for all reports that are checked in the **Midnight report** checkboxes.
Sunday report	Reports are automatically generated every Sunday at midnight for all reports that are checked in the **Sunday report** checkboxes.
[Print]	Clicking this button prints all reports that are checked in the left-hand checkboxes.
[Export]	Clicking this button exports all reports that are checked in the left-hand checkboxes.
[Save]	Clicking this button saves the current configuration of selected reports and closes the dialog box. The reports that are selected previously are now marked as selected when you open the dialog box again subsequently.
[Cancel]	Clicking this button closes the dialog box without saving the current configuration of selected reports.

10.2.7 Export Alarm Reports

This dialog allows the alarm reports to be exported to CSV file. To export an alarm report, you may directly enter the alarm date range, or click the **[...]** (ellipsis) button in **From Date**, **To Date** fields and select **From Time**, **To Time** from the respective drop-down values. An alarm report can also be generated based on the subscriber details. Select the **Subscriber ID**, **Subscriber Name**, **Transmitter ID** or **Subscriber Type** from the drop down list to generate an alarm report only for the selected values.

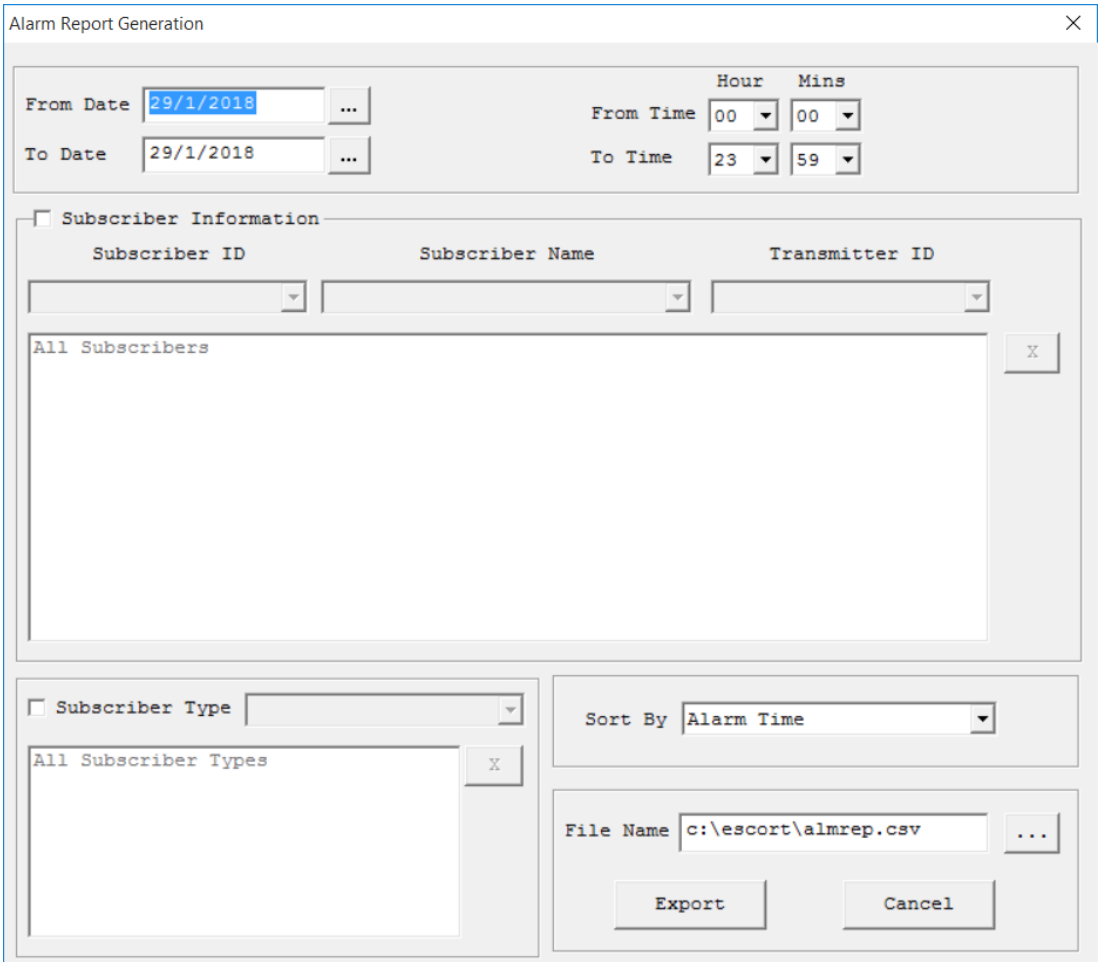


Figure 10.11: Export Alarm Reports dialog

The alarm report can be sorted by **Alarm Time**, **Transmitter ID**, **Subscriber Name**, **Problem Type**, **Subscriber Type**, by using the **Sort By** drop-down list. You can change the report name and file location by pressing the **[...]** (ellipsis) button. Click the **[Export]** button to save the report to the specified file. Click the **[Cancel]** button to cancel the report generation and exit from the dialog window.

10.2.8 Alarm Flash Reports

This dialog allows the operator to view the alarm history for the last 4, 8, 12 or 24 hours from the current time. The operator would be able to see details of the alarms from the report list. Alarms that were triggered within the time frame appear in the list box. The following are details of the **Alarm Flash Report** dialog.

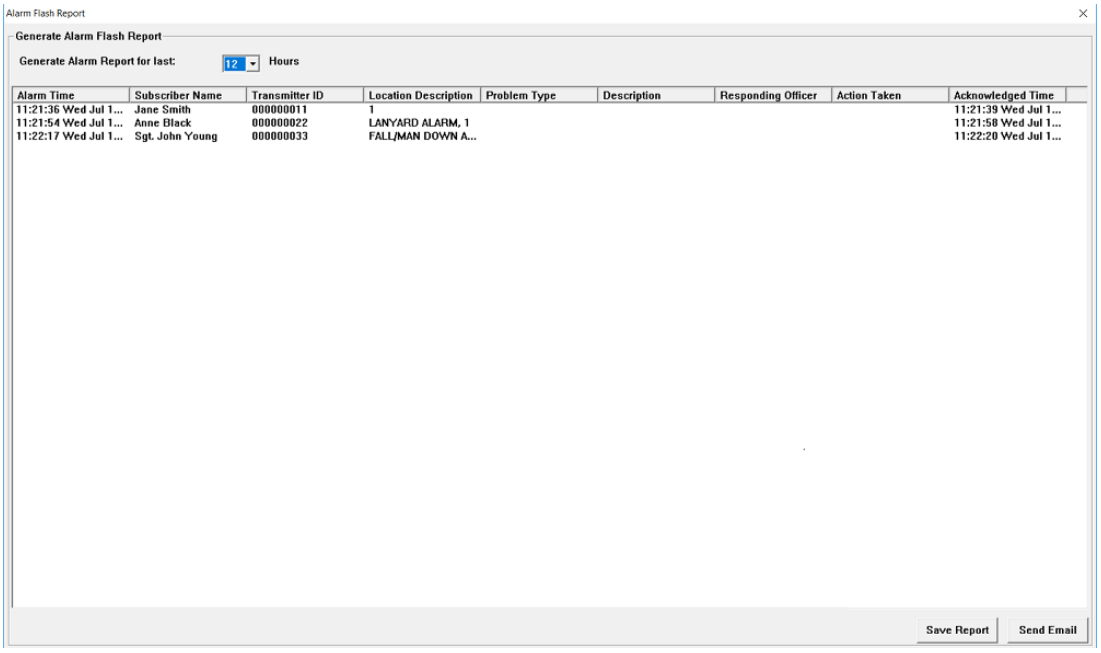
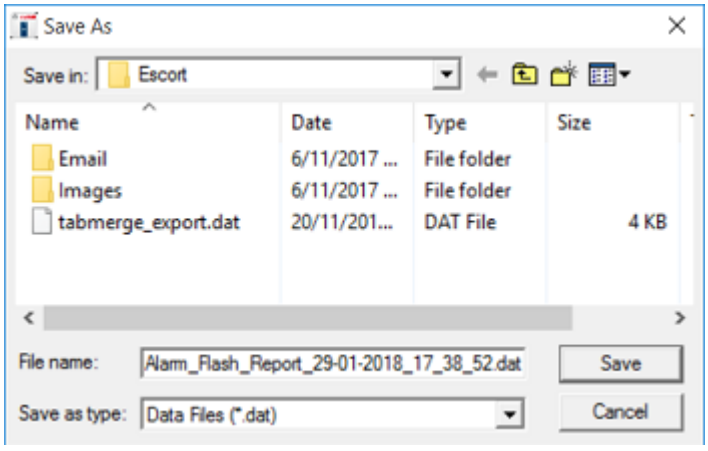


Figure 10.12: Alarm Flash Reports dialog

Element	Usage/Description
Generate Alarm Report for the last X Hours	Select the time period interval of 4, 8, 12 or 24 hours from the drop-down list.
Alarm Time	Date and time of the alarm
Subscriber Name	Name of the subscriber of triggered alarm.
Transmitter ID	ID of the transmitter that triggered the alarm
Location Description	Type (duress, man down, lanyard) and location of the alarm
Problem Type	The type of problem which is selected from the Reports Database when completing the alarm report.
Description	Description of problem which is entered from the Reports Database when completing the alarm report.
Responding Officer	Name of officer responding to the alarm which is entered from the Reports Database when completing the alarm report.
Action Taken	Action taken by the officer which is entered from the Reports Database when completing the alarm report.
Acknowledged Time	Date and time when the alarm was acknowledged.

Element	Usage/Description
[Save Report]	Click the button to save the report in tab delimited format (“.dat” file). A dialog appears to confirm the name and location of the file to be saved.  The default name of the file to be saved is **Alarm_Flash_Report_DD_MM_YYYY_HH_MM_SS** where DD is day of the month, MM is the month, YYYY is the year, HH is the hour, MM is the minute and SS is the second. Click the **[Save]** button to save the file, or **[Cancel]** button to abort the operation. If there are no records in the **Alarm Flash Reports**, clicking the **[Save]** button will generate an error message dialog.
[Send Email]	Click the button to send the report in tab delimited format (“.dat” file) attached in an email, with the filename as the subject header, to the default **Email Notification Group** “00”. The default **Email Notification Group** is configured in **Setup > Email Setup** menu. If there are no records in the **Alarm Flash Report**, clicking the **[Send Email]** button will generate an error message dialog.

10.2.9 Muster Reports

This dialog allows the operator to view the current locations of the transmitters that are in supervision mode. This would be helpful, for example, in the event of an emergency evacuation where the location of the subscribers can be known quickly. The operator would be able to see details of the transmitter from the list at one glance. The following are details of the **Muster Reports** dialog.

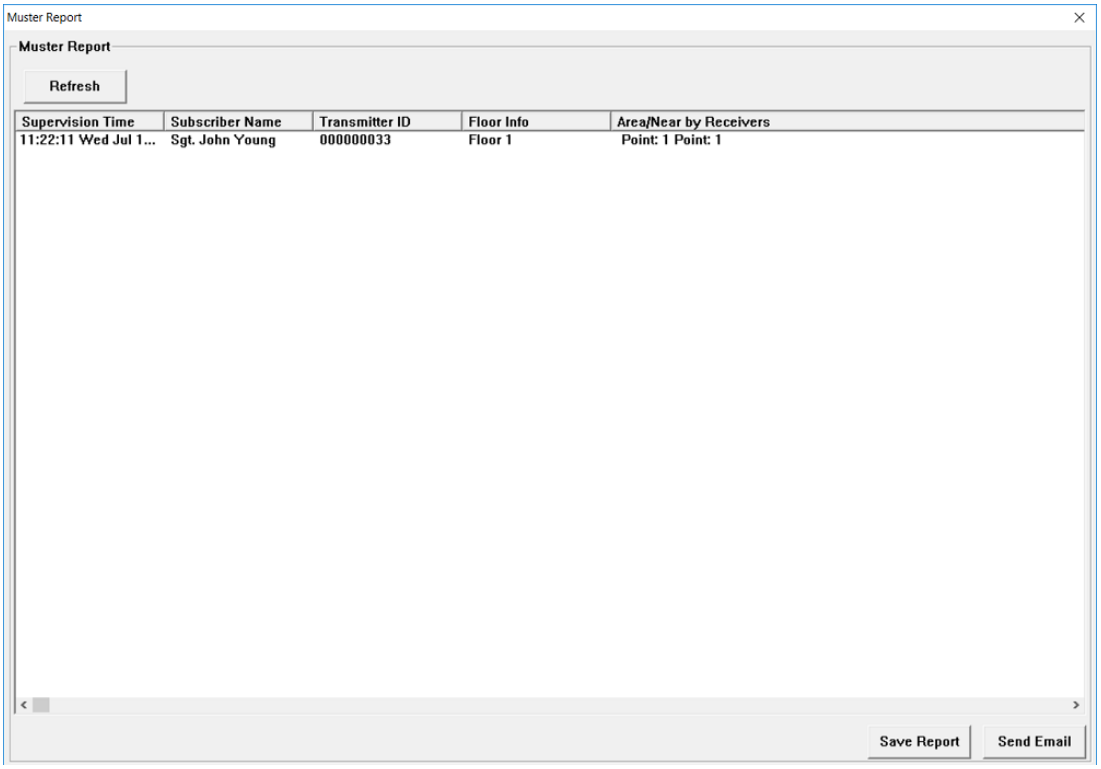
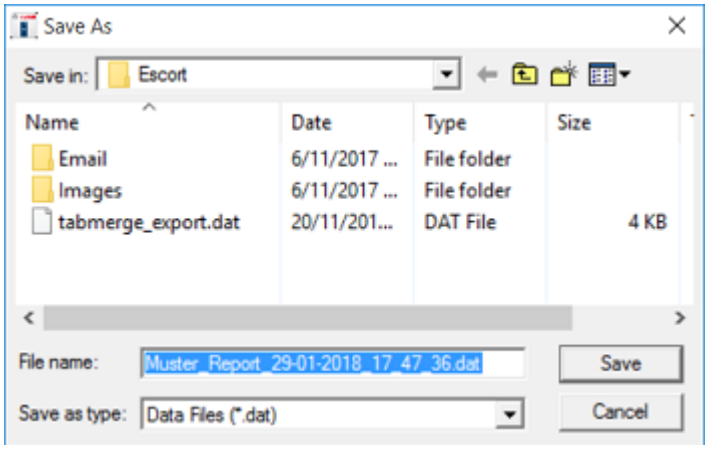


Figure 10.13: Muster Reports dialog

Element	Usage/Description
[Refresh]	Click the button to refresh the **Muster Report**.
Supervision Time	Time and date of the last supervision message from the transmitter.
Subscriber Name	Name of the subscriber.
Transmitter ID	ID of the transmitter.
Floor Info	Information of the floor where the transmitter is located.
Area/Nearby Receivers	Area and/or SE receiver ID nearest to the transmitter location.

Element	Usage/Description
[Save Report]	Click the button to save the report in tab delimited format (“.dat” file). A dialog appears to confirm the name and location of the file to be saved.  The default name of the file to be saved is **Muster_Report_DD_MM_YYYY_HH_MM_SS** where DD is day of the month, MM is the month, YYYY is the year, HH is the hour, MM is the minute and SS is the second. Click the **[Save]** button to save the file, or **[Cancel]** button to abort the operation. If there are no records in the **Muster Reports**, clicking the **[Save]** button will generate an error message dialog.
[Send Email]	Click the button to send the report in tab delimited format (“.dat” file) attached in an email, with the filename as the subject header, to the default **Email Notification Group “00”.** The default **Email Notification Group** is configured in **Setup > Email Setup** menu. If there are no records in the **Muster Report**, clicking the **[Send Email]** button will generate an error message dialog.

10.2.10 Schedules

This selection informs management of the ten-time of day/day of week schedules and holidays.

See *Schedules, page 144* for details.

10.2.11 Alarm Groups

This dialog allows setup and arm/disarm control of the 99 alarm groups. Any number of point type transmitters can be assigned to an alarm group in the **Subscriber Database’s Advanced** dialog. However, each transmitter can only be assigned to one alarm group.

See *Alarm Groups, page 148* for details.

10.2.12 Alarm Group State

This dialog will display a list of the alarm groups that are currently armed, and have one or more transmitters (points) faulted. The points are presented because they were not restored when their automatic schedule armed, or there was an alarm while the alarm group was on.

See *Alarm Group State, page 149* for details.

10.2.13 Current Check-in Status

This dialog displays a list of subscribers that are required to check-in and failed to do so during the last check-in period. Also shown are their addresses, phone numbers, and the last time they checked-in.
See *Current Check-in Status, page 150* for details.

10.2.14 Clear screen

To clear the screen of any outdated or unwanted data, choose this feature from the **Utilities** menu. The screen automatically resets to its normal operations mode.

10.2.15 Output verification

When selected, the system is scanned to verify that all alarm outputs are in the correct state. Any output found in the wrong state is corrected.

10.2.16 Reset Transponder interfaces

This feature reinitializes the communication interfaces between the Central Console and all the SE coordinators/SE receivers. For example, if a device is causing the communication interfaces to be sluggish or jammed, rendering the entire system to be non-responsive, use this feature to reset and reestablish the interfaces.

10.2.17 Synchronize system time

Selecting this option on the master computer causes the time on the slave and all of the workstation computers to be updated to the master computer's time.

10.3 Logout menu

This menu has only one command: Logout the current operator. When the **Logout** menu is selected, the operator currently logged in is logged out and the **Login** dialog appears on the screen, allowing another operator to login. All login and logout activity is recorded in the system history file and on the hard copy printout.

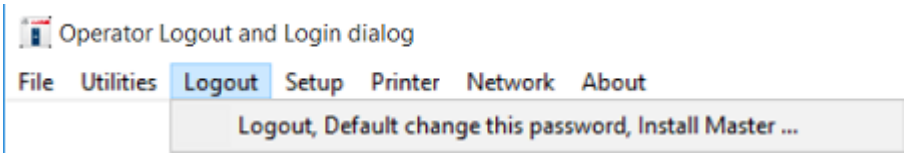


Figure 10.14: Logout menu

When the Central Console receives an alarm transmission, the system behaves the same whether or not an operator is logged in. The alarm screen is displayed, allowing any operator to acknowledge the alarm. When the operator's password is entered to silence the alarm, that operator is automatically logged in.

10.4 Setup menu

The options contained in the **Setup** menu are accessible only to Security Escort service and maintenance personnel. These options affect the system operating parameters and are used for diagnostic and maintenance purposes.

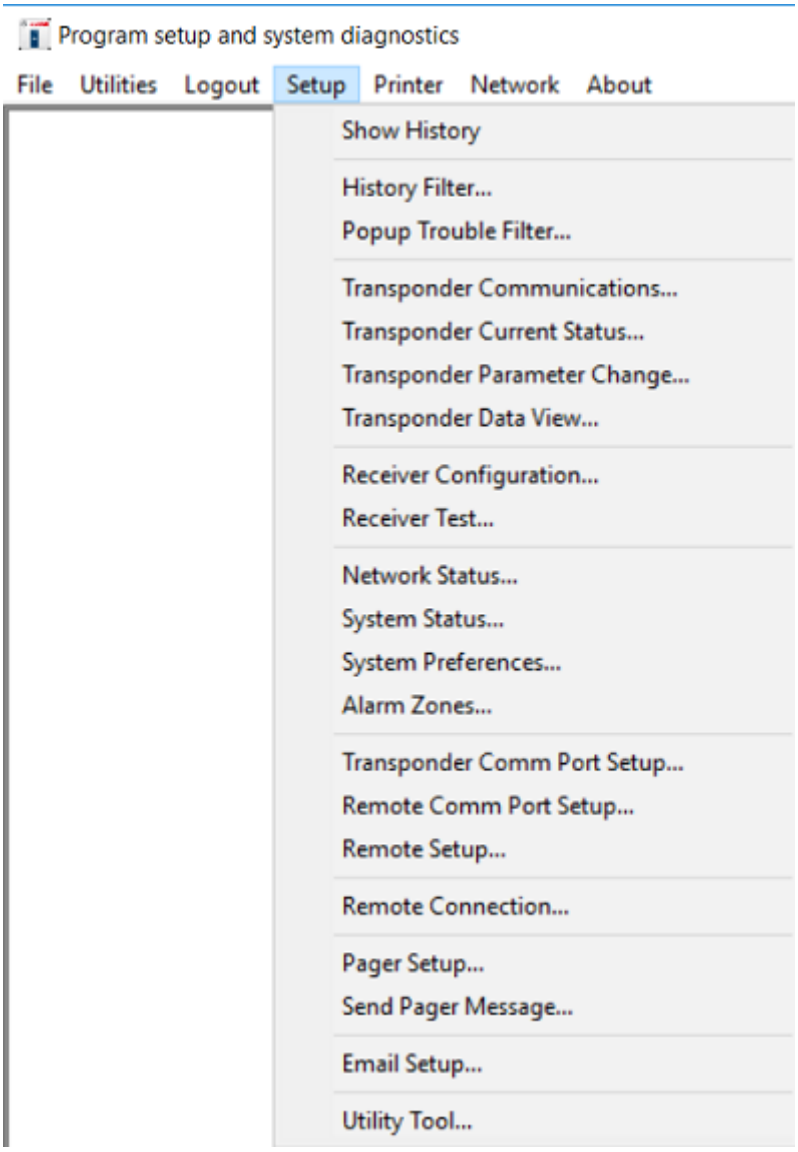


Figure 10.15: Setup menu

10.4.1 Show history

When selected, the default map display is replaced by a scrolling text window showing the most recent events that occurred in the system. The window can list historical events and operations of the Central Console software. Examples include list of any alarms and the actions taken, name of person who logged into the Central Console, changes to the database, communication results between the devices, and so on.

The events displayed can be selected in the **History filter** dialog under the **Setup** Menu. After **Show history** is selected, this menu item changes to **Show map**.

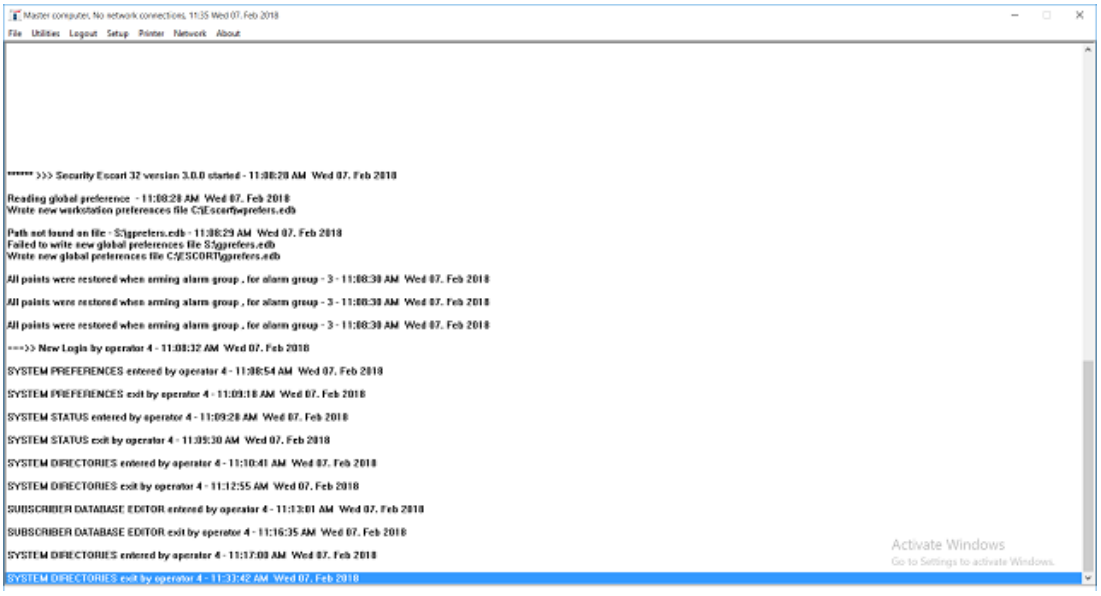


Figure 10.16: Show history log

10.4.2 History filter

This dialog selects the classes of events recorded for (sent to) specific output devices. From the **Select destination** group, select the **History screen**, **Printer**, **History archive files** or **System serial ports** option. Notice that when an option is selected, the **Check to output the event** options also change accordingly. There is a different set of events output for each destination selected. For each destination, the events must be individually configured.

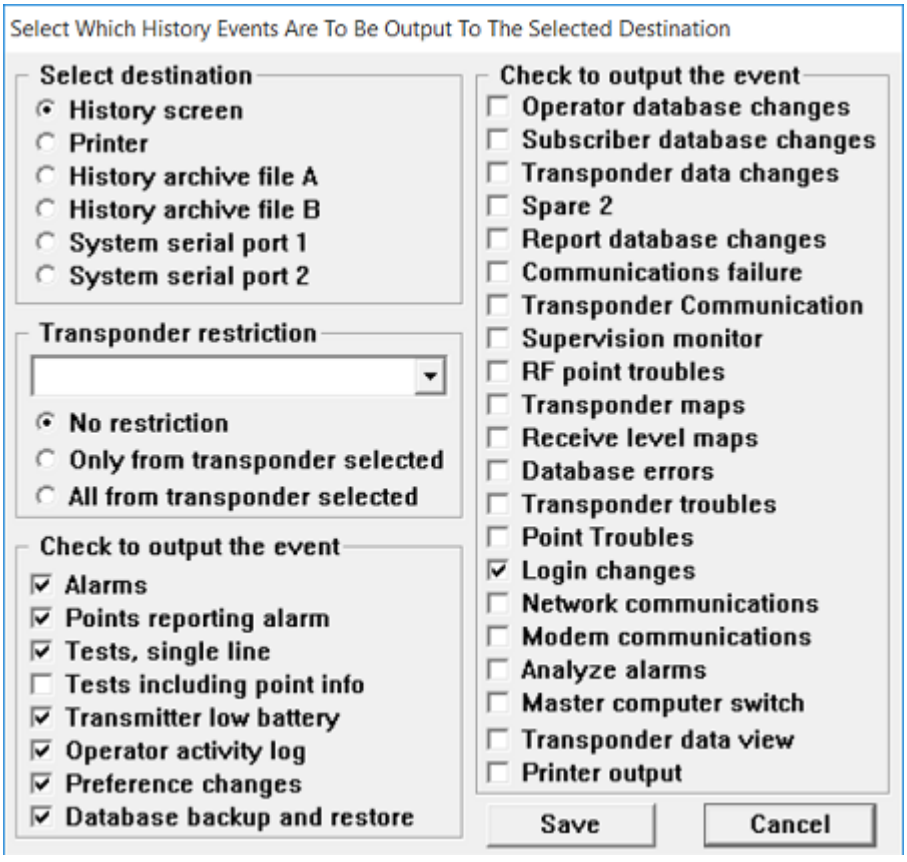


Figure 10.17: History filter dialog

Element	Usage/Description
Select destination group	
History screen	This option selects the events to be displayed on the computer screen when **Show history** is selected.
Printer	This option selects the events to be sent to the printer.
History archive file A	This option selects the events to be sent to the “a_audit.txt” file stored in the Security Escort sub-directory (typically “C:\ESCORT”). There is a minimum set of events that cannot be disabled, so they are always recorded.
History archive file B	This option selects the events to be sent to the “b_audit.txt” file stored in the Security Escort sub-directory (typically “C:\ESCORT”).
System serial port 1	This option selects the events to be sent to the system serial port 1. System serial port 1 is assigned a physical comm port in the **Remote Comm Port Setup** dialog, and the **History Filter Output** field must be set in the **Remote Setup** dialog.
System serial port 2	This option selects the events to be sent to the system serial port 2. System serial port 2 is assigned a physical comm port in the **Remote Comm Port Setup** dialog, and the **History Filter Output** field must be set in the **Remote Setup** dialog.
Transponder restriction group	
No restriction	This selection is typically left at this setting at all times. The output is not restricted by an individual SE coordinator.
Only from transponder selected	The selected events are only output if they were reported from the SE coordinator selected in the drop-down list box above.
All from transponder selected	All events are reported from the SE coordinator selected above. The selected events are reported from all other SE coordinators in the system.
Check to output the event group	
Alarms	Outputs the information about an alarm including location, but not the SE coordinator and SE receiver levels. This is the data typically sent to a printer.
Points, reporting alarm	Outputs the SE coordinator and SE receiver levels for an alarm. Typically, this is the data too detailed to send to a printer and is used for diagnostics, not normal system operation.
Tests, single line	Outputs the simple information about a test. Typically, this is the data normally sent to a printer.
Tests including point Info	Outputs the SE coordinator and SE receiver levels for a test. This is the data usually too detailed to send to a printer and is used for diagnostics, not normal system operation. If this option is selected, **Test, single line** option would not be selected for the same output device.

Element	Usage/Description
Transmitter low battery	Outputs low battery reports received from transmitters.
Operator activity log	Outputs all other operator activity (audit trail) not covered by specific event selections.
Preferences changes	Outputs all changes made to system preference selections.
Database backup and restore	Records all database backup and restore activity.
Operator database changes	Records all changes to the **Operator database**.
Subscriber database changes	Records all changes to the **Subscriber database**.
Transponder data changes	Records all changes to the **Transponder database**.
Spare 2	This is a future option that has no function at this time (leave unselected).
Report database changes	Records all changes to the **Report database**.
Communications failure	Records all communication failures and restorations.
Transponder communication	Records all communications to SE coordinator. This selection is only used for engineering diagnostics. Leaving this item selected generates a significant amount of history and fills up the hard disk drive quickly. Leave this item unselected.
Supervision monitor	Reports changes in the supervision status for all transmitters that are being supervised.
RF point troubles	Output all reported radio frequency communication of SE receiver troubles. Typically this item would be checked for devices used to monitor problems.
Transponder maps	Outputs all SE coordinator status maps. This selection is only used for diagnostics. Leave this item unselected.
Receive level maps	Outputs all maintenance alarm received level maps. This selection is only used for diagnostics. Leave this item unselected.
Database errors	Outputs all reported database errors. This item is checked.
Transponder troubles	Outputs all reported SE coordinator troubles. This item is checked for devices used to monitor problems.
Point Troubles	Outputs all reported SE receiver troubles. This item is checked for devices used to monitor problems.
Login changes	Reports all new system operator login and logout activity.

Element	Usage/Description
Network communications	Records all communications between networked computers. This selection is only used for engineering diagnostics. Leaving this item selected, generates a significant amount of history and fills up the hard disk drive very quickly and may bog down the system during high traffic times. Always leave this item unselected.
Modem communications	Records all communications to the modem for remote communications and pager access. This selection is only used for diagnosing pager communication problems. Leave this item unselected.
Analyze alarms	This option outputs data allowing an engineer to evaluate how well the location algorithm is performing. Leave this item unselected.
Master computer switch	Records when the master and slave computers switch roles.
Transponder data view	Sends the data created by the **Transponder data view** dialog to the output. This selection is only used for engineering diagnostics. Leave this item unselected.
Printer output	Allows the data being sent to the printer to be sent to other outputs. This item is unselected.
[Save]	Click this button to save the changes.
[Cancel]	Click this button to abort the changes.

10.4.3 Popup trouble filter

The Security Escort System contains many built-in self testing features. Each SE coordinator tests the condition of the SE receivers connected to it.
When the SE coordinator finds a device reporting a trouble condition, it communicates the problem and the device identity to the Central Console. This generates a brief alert tone, displays a pop-up message for the operator, and sends an optional pager message. The message indicates the nature of the trouble and instructs the operator on the proper course of action. The event is recorded on the hard disks of both the main and backup computers and on the printout.

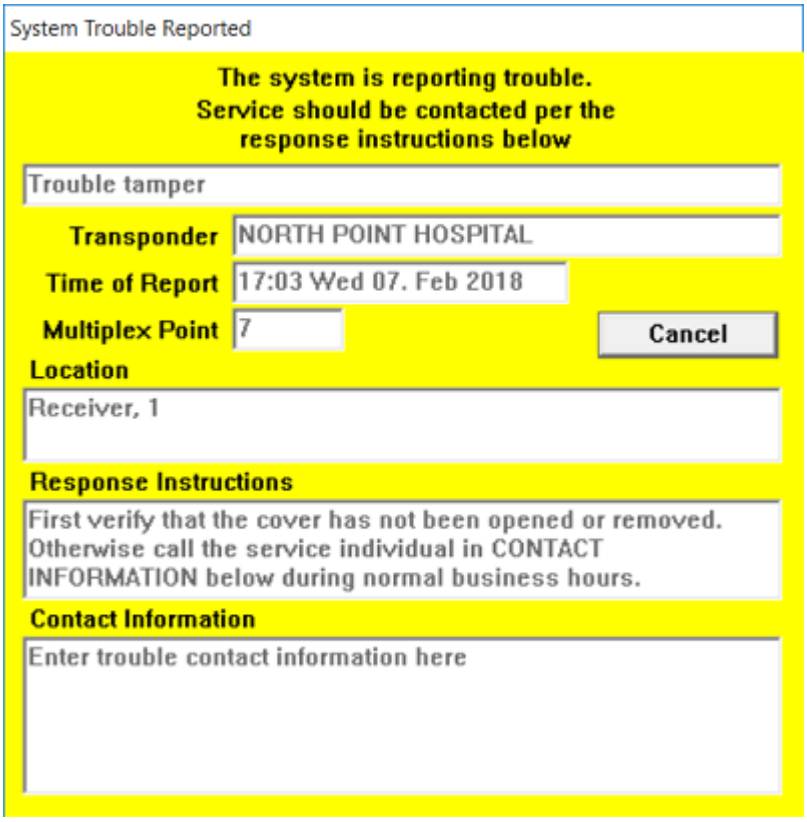


Figure 10.18: "Pop-Up" Alert Showing Tamper Trouble

This dialog allows the selection of which type of troubles that will appear in pop-up messages on the console screen, or be sent to the service pager. The troubles described below are always recorded in the **Transponder current status** window, but may or may not produce a pop-up display or pager message, depending on the selections for **Popup** or **Pager** checkboxes.

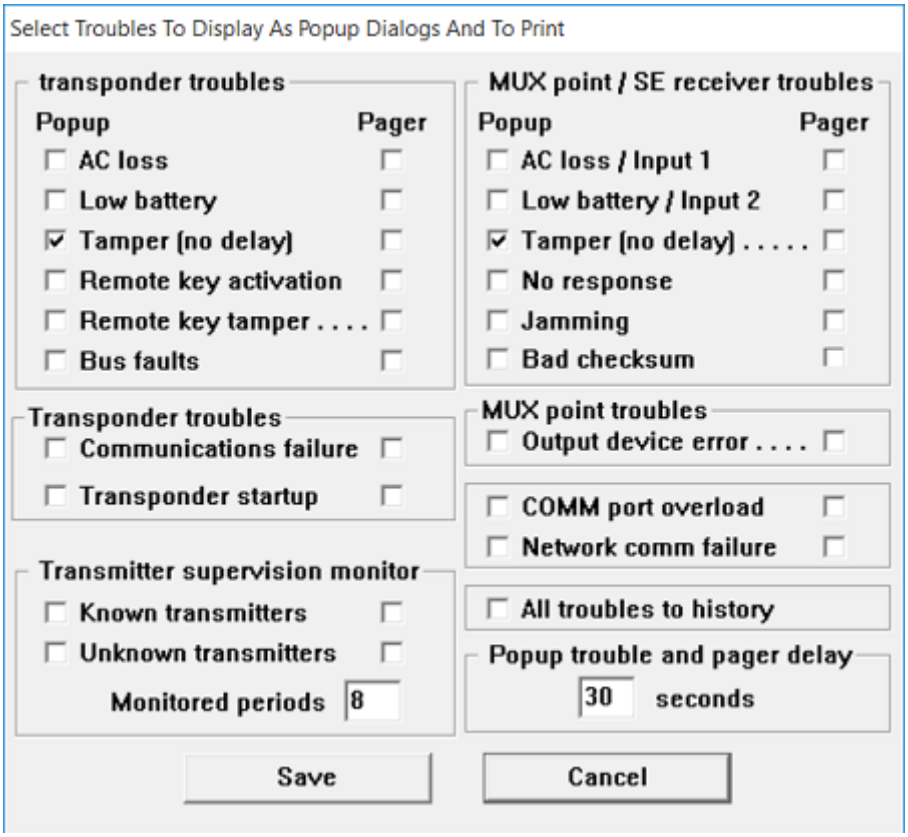


Figure 10.19: Popup trouble filter dialog

Element	Usage/Description
Transponder troubles group	
AC loss	The SE coordinator senses when it loses AC power and reports the condition to the Central Console. After a few seconds delay, the Central Console generates the notification and records the condition in the audit file. See **Transponder current status** dialog.
Low battery	Periodically during normal operation, the SE coordinator tests its battery. If the test fails, it immediately reports the condition to the Central Console. After a few seconds delay, the Central Console generates the notification and the condition is recorded in the audit file.
Tamper (no delay)	The SE coordinator immediately senses and reports the actuation of its tamper switch. The Central Console immediately generates the notification and records the condition in the audit file without delay.
Remote key activation	The SE coordinator immediately senses and reports the activation (shorting) of its remote key input when it is enabled in the **Transponder parameter change** dialog. The Central Console generates the notification and records the condition in the audit file.

Element	Usage/Description
Remote key tamper	The SE coordinator immediately senses and reports the fault (open) of its remote key input when it is enabled in the **Transponder parameter change** dialog. The Central Console immediately generates the notification and records the condition in the audit file.
Bus faults	When the SE coordinator is unable to communicate to any SE receivers on one or more of its multiplex busses, it immediately reports the condition to the Central Console. The Central Console reports the condition by generating the notification if the condition persists more than a few seconds. The condition is also recorded in the audit file.
Communications failure	To continually assure that communications between the Central Console and each SE coordinator are functioning properly, each SE coordinator is required to send a message to the Central Console periodically. If there is no response from the SE coordinator, the Central Console displays a communications failure warning and records the condition in the audit file. If an SE coordinator determines it lost communication with the Central Console, it assumes control of the outputs of the devices connected to it and transmits “I’M OK” messages until it is acknowledged by the Central Console. The Central Console also attempts to reestablish communications by continually requesting transmissions from the SE coordinator and listening on the communications channel. When communications are restored with the Central Console, the SE coordinator transmits any alarm and trouble conditions that occurred during the communications loss. Control of the horns, LEDs, strobes, and sirens reverts to the Central Console. This approach to managing a communications loss assures that alarm events cannot go undetected even if the Central Console is out of operation temporarily.
Transponder startup	The SE coordinator reports to the Central Console when it first starts up. This can be caused by a technician turning on the SE coordinator or by a watchdog failure of the on board microprocessor. The Central Console immediately generates the notification and records the condition in the audit file.
Transmitter supervision monitor group	
Known transmitters	To continually monitor the status of all transmitters programmed in the database that send periodic supervision transmissions. If any monitored transmitters stop sending supervision transmissions, notification will be generated.
Unknown transmitters	To monitor for periodic supervision transmissions from transmitters not programmed in the database, notification will be generated if transmissions from transmitters not programmed in the database are received.

Element	Usage/Description
Monitored periods	This is the number of supervision intervals that are consecutively missed before notification is generated for a specific transmitter that stopped reporting supervision transmissions. Default is 8.
MUX point / SE receiver troubles group	
AC loss / Input 1	The SE receiver tested the presence of Input 1 and the test failed. For information on AC loss, please refer to the Security Escort manuals.
Low Battery / Input 2	The SE receiver tested for presence of Input 2 and the test failed. For information on Low Battery, please refer to Security Escort manuals.
Tamper (no delay)	Whenever the cover is removed from an SE receiver, the on-board microprocessor detects the tamper and it is reported without delay to the SE coordinator.
No response	Whenever an SE receiver fails to respond to a command from the SE coordinator, a “No Response” message is sent by the SE coordinator to the Central Console. This can occur if a bus wire is cut or a device is damaged.
Jamming	Each SE receiver monitors the level of radio energy being received at all times. If the level exceeds a preset threshold, for a preset length of time, the on-board microprocessor reports jamming.
Bad checksum	This message is generated by the SE coordinator and sent to the Central Console whenever the SE coordinator detects message errors in the communications between SE receivers.
MUX point troubles group	
Output device error	The SE coordinator generates this message when it commands an SE receiver to activate or deactivate an output device (siren, strobe, horn, or LED) and the device fails to respond correctly.
Others	
COMM port overload	The notification is generated if the communications traffic to the SE coordinator exceeds the system is capability.
Network comm failure	The notification is generated if the communication between the master and slave computers fails.
All troubles to history	Saves all troubles to history file.
Pop-up trouble and pager delay	The delay in seconds before a trouble displays on the computer screen or pager message is dispatched. If a restore for a trouble is received before a trouble is displayed (this delay expires), the trouble and the restore are ignored. Tamper troubles are not delayed. Default is 30 seconds.
[Save]	Click to save all changes.
[Cancel]	Click to abort all changes.

Notice!
If during this loss of communications, an alarm transmission is received by one or more of the SE receivers attached to the SE coordinator, the SE coordinator activates outputs attached to it as well as the horns and red LEDs on any of its SE receivers which detected the alarm transmission. Since the SE coordinator does not have access to the **Subscriber database**, it must assume that all transmitters are valid, so even unauthorized (not in the **Subscriber database**) transmitters produce audible alarm indications (if the system is set for audible alarms in the **Security Preferences** dialog).

10.4.4 Transponder communications

From the Central Console, it is possible to perform detailed diagnostic tests using the **Transponder communications** dialog. From this dialog, the operator can request maps indicating the status of each device connected to a given transponder, and can control individual devices, turning LEDs, horns, strobes, and sirens on and off. The **Transponder communications** dialog appears on the right when it is opened, allowing the **History screen** to be viewed while the screen is open. This makes it possible to view the results of map commands issued from the console.

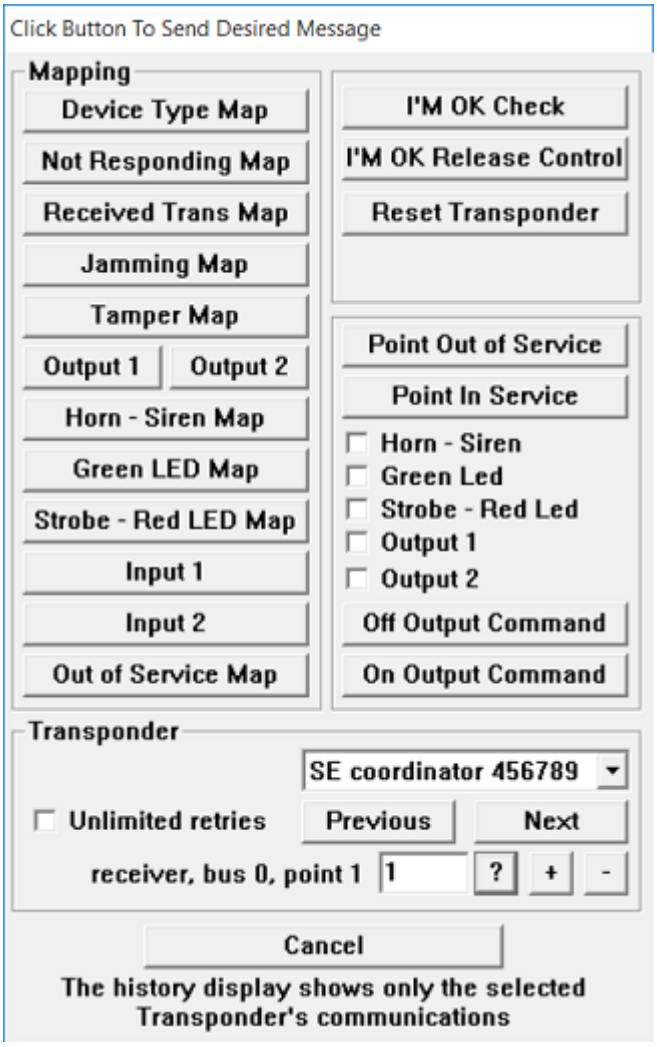


Figure 10.20: Transponder communications dialog

Diagnostic map commands are used to determine the status of all devices (connected to the selected transponder) with a single command. Maps are displayed on the **History screen** as an array of rows and columns, corresponding to point addresses and bus numbers.
The status of a particular device is shown by a “1” or “0” (zero) with “1” signifying the true state. The map location, corresponding to a device that is not responding to the transponder, contains a “1” when a **Not Responding Map** command is selected.
Similarly, a “1” is displayed in response to a **Tamper Map** command in locations that correspond to devices in a tampered state. All other locations display a “0” (zero), “a” — (if there is no device assigned to the location), or a “x”, there is a device connected to the system at that address, but it is not in the **Transponder database**.

Element	Usage/Description
Mapping group	
[Device Type Map]	Unlike all other types of map, the **Device Type Map** has two characters in each possible device location. The right most character indicates the device type. A “5” indicates a receiver, “3” indicates an alert unit, and “7” indicates that the **Transponder database** shows a device in that location but it is not currently communicating with the SE coordinator. The left character indicates the following: “0” (zero), the device is in its normal state, “1”, the device is off normal, and “x” there is a device connected to the system at that address, but it is not in the **Transponder database**. (Usually this results from an error during data entry in the **Transponder database**).
[Not Responding Map]	Requests a map of all the points that are not responding (missing) to the system on this SE coordinator. The **[Received Trans Map]** button produces a map display with one in the locations corresponding to SE receivers that are missing from the system. A “0” (zero) indicates that the point is responding. An “x” indicates there is a device connected to the system at that address, but it is not in the **Transponder database**.
[Received Trans Map]	As a means of self-diagnosis, the system software periodically reviews the SE receivers which have not received an alarm or test transmission. This list is printed as a part of the daily system status report and is a tool for assessing the health of the system. The **[Received Trans Map]** button produces a map display with “1” in the locations corresponding to SE receivers which received transmissions. Each time this map is read, the **Received Trans Map** image is cleared in the SE coordinator.
[Jamming Map]	Requests a map of all the SE receivers that are currently reporting RF jamming to the system. The **[Jamming Map]** button displays a map with “1” in the locations corresponding to SE receivers that are reporting jamming. A “0” (zero) indicates that the SE receiver is not jammed.

Element	Usage/Description
[Tamper Map]	Requests a map of all the points that are currently reporting a tamper condition to the system. The **[Tamper Map]** button displays a map with “1” in the locations corresponding to points that are reporting tamper. A “0” (zero) indicates points that are not tampered.
[Output 1]	Requests a map of all the **Output 1** of SE receivers that are turned on for this SE coordinator. The **[Output 1]** button displays a map with “1” in the locations corresponding to points that are turned on.
[Output 2]	Requests a map of all the **Output 2** of SE receivers that are turned on for this SE coordinator. The **[Output 2]** button displays a map with “1” in the locations corresponding to points that are turned on.
[Horn - **Siren Map]**	Requests a map of all the points that have their horn or sirens on, on this SE coordinator. The **[Horn** - **Sirens Map]** button displays a map with “1” in the locations corresponding to points which have their outputs on. A “0” (zero) indicates that the output is off.
[Green LED Map]	Requests a map of all the points on this SE coordinator that have their spare outputs - green LED on. The **[Green LED Map]** button displays a map with “1” in the locations corresponding to points which have their outputs on. A “0” (zero) indicates that the output is off.
[Strobe - **Red LED Map]**	Requests a map of all the points on this SE coordinator that have their strobe - red LED on. The **[Strobe - Red LED Map]** button displays a map with “1” in the locations corresponding to points which have their outputs on. A “0” (zero) indicates that the output is off.
[Input 1]	Requests a map of all the **Input 1** of SE receivers that are currently monitored for the SE coordinator. The **[Input 1]** button displays a map with “1” in the locations corresponding to inputs that are triggered.
[Input 2]	Requests a map of all the **Input 2** of SE receivers that are currently monitored for the SE coordinator. The **[Input 2]** button displays a map with “1” in the locations corresponding to inputs that are triggered.
[Out Of Service Map]	The **Out Of Service Map** shows those SE receivers that are currently out of service. Se receivers may be taken out of service and returned to service by selecting the point using **MUX Bus Point** dialog in the bottom right corner of the screen and clicking the **[Point Out Of Service]** or **[Point In Service]** button. Points can be selected by typing in the point number or by using the **[+]** and **[-]** buttons, or the **[?]** button.
Others	

Element	Usage/Description
[I'M OK Check] [I'M OK Release Control]	These buttons are used to diagnose and correct communications problems between the Central Console and the SE coordinator. The system software requires that each SE coordinator send a message to the Central Console periodically if no other communications have taken place. These messages are called “I’m OK” messages. If for some reason the communications link between the Central Console and the SE coordinator fails, the SE coordinator recognizes the fact when its “I’m OK” transmissions are not acknowledged by the Central Console. When the SE coordinator has retried transmitting an “I’m OK” message or any other message 6 times without acknowledgment, it assumes control of the outputs (LEDs, horns, strobes, and sirens) on devices connected to it and modifies the message to indicate that it is still okay and has taken control. These messages are transmitted once per minute until communications are reestablished. The **[I'M OK Check]** button requests that the SE coordinator send an “I’m OK” message. This is used to determine if an SE coordinator has taken control of its outputs. The **[I'M OK Release Control]** button generates a command to the SE coordinator to release control back to the Central Console. Normally, the Central Console automatically generates a release control message upon the re-establishment of communications following a failure.
[Reset Transponder]	Clicking this button resets the SE coordinator as if it was just powered up. Any test or alarm processing that was in progress at the time is lost.
[Point Out Of Service]	Clicking this button takes the currently selected point out-of-service. That point no longer responds to the system, as if it was disconnected. Use this function with caution.
[Point In Service]	Clicking this button restores the currently selected point to an in-service condition. That point returns to normal function.
Horn - Siren	If this checkbox is selected, the horn output of an SE receiver or the siren output is turned on if the **[On Output Command]** button is clicked, or off if the **[Off Output Command]** button is clicked. If this checkbox is not selected, the state of this output is not changed.
Green Led	If this checkbox is selected, the green LED of an SE receiver is turned on if the **[On Output Command]** button is clicked, or off if the **[Off Output Command]** button is clicked. If this checkbox is not selected, the state of this output is not change.
Strobe - **Red Led**	If this checkbox is selected, the red LED of an SE receiver or the strobe output is turned on if the **[On Output Command]** button is clicked, or off if the **[Off Output Command]** button is clicked. If this checkbox is not selected, the state of this output is not changed.

Element	Usage/Description
[Output 1] **[Output 2]**	If this checkbox is selected, the selected **Output 1 or 2** of an SE receiver is turned on if the **[On Output Command]** button is clicked, or off if the **[Off Output Command]** button is clicked. If this checkbox is not selected, the state of this output is not changed.
[Off Output Command]	When clicked, the selected **Horn-Siren**, **Green Led**, **Strobe -Red Led**, **Output 1** and **Output 2** are turned off for the selected SE receiver. If the output does not change, click the **[On Output Command]** button, and then click the **[Off Output Command]** button again.
[On Output Command]	When clicked, the selected **Horn -Siren**, **Green Led**, **Strobe -Red Led**, **Output 1** and **Output 2** are turned on for the selected SE receiver. If the output does not change, click the **[Off Output Command]** button, and then click the **[On Output Command]** button again.
Transponder group	
Transponder	Selects the SE coordinator that you desire to communicate with.
Unlimited retries	When this checkbox is selected, the Central Console continues trying to send commands to the SE coordinator even if the commands are not being acknowledged. (Normally, the Central Console would cease after 6 retries and declare a communication failure.) When this screen is closed, the system reverts to the normal 6 retries.
[Previous]	Returns to the previous SE coordinator.
[Next]	Advances to the next SE coordinator.
receiver, bus X, point Y	This field displays the current bus number and point number. The actual point number may be entered in the field to the right.
[?]	Opens up the **Select Point** dialog grid.
[+]	Advances to the next point.
[-]	Returns to the previous point.
[Cancel]	Click to abort all communication tests.

10.4.5 Transponder current status

This dialog, accessible from the **Setup** menu, provides a history of communications involving the selected SE coordinator. It also provides several buttons that can be used to diagnose problems with the SE coordinator and any of its SE receiver.

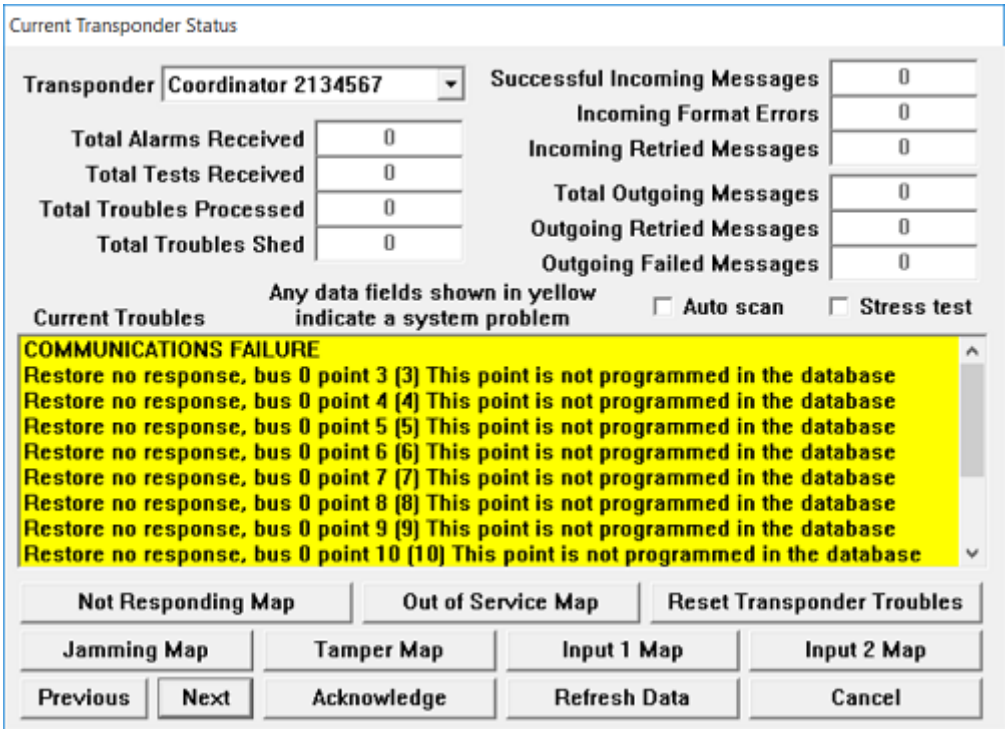


Figure 10.21: Transponder current status dialog

Element	Usage/Description
Transponder	Selects the SE coordinator from the drop-down list.
Total Alarms Received	The total number of alarm messages received by the Central Console from this SE coordinator since the data was last reset (using the **[Reset Transponder Troubles]** button).
Total Tests Received	The total number of test messages received by the Central Console from this SE coordinator since the data was last reset (using the **[Reset Transponder Troubles]** button).
Total Troubles Processed	The total number of trouble messages received by the Central Console from the SE coordinator and processed (see **Total Troubles Shed**) since the data was last reset (using the **[Reset Transponder Troubles]** button).
Total Troubles Shed	During certain rare occurrences, the communication traffic on the SE coordinator links becomes excessive and threatens to increase the system response time to tests and alarms. This can happen if faults are reported at a very high rate. To avoid slow response in such situations, the Central Console may go into a load shedding mode in which it ceases to record and display trouble reports until the communications traffic subsides. The **Total Troubles Shed** box indicates the number of trouble messages that were not processed since the last reset (using **[Reset Transponder Troubles]** button).
Successful Incoming Messages	The total number of messages successfully received from this Se coordinator.

Element	Usage/Description
Incoming Format Errors	The number of messages received from this SE coordinator where format error was detected. This field is yellow if 1.5% or more of the messages had errors. A high level of message errors indicates a serious communication problem.
Incoming Retried Messages	The total number of messages successfully received from this SE coordinator that indicated they were retried. This field is yellow if 1.5% or more of the messages are retried. A high level of retried messages indicates a serious communication problem.
Total Outgoing Messages	The total number of messages sent to this SE coordinator from the Central Console.
Outgoing Retried Messages	The total number of message retries to this SE coordinator. This field is yellow if 1.5% or more of the messages are retried. A high level of retried messages indicates a serious communication problem.
Outgoing Failed Messages	This is total number of messages that could not to be delivered to this SE coordinator. This field is yellow if there are any failed messages. Outgoing failed messages cause the Central Console to display an alert message that communications have failed.
Auto scan	The auto scan function performs the above stress test proceeding from one SE coordinator to the next after one of each type of map is requested and received. After the last map type and before proceeding to the next SE coordinator, a command is issued to refresh the SE coordinator data so that when an auto scan proceeds through all SE coordinators, all SE coordinators and point troubles are updated. Auto scan is terminated by unselecting the **Auto scan** checkbox or by closing the screen using the **[Cancel]** button. Run the “Auto scan” process to sync with the actual status of the SE coordinators after resetting the troubles, or programming the SE coordinators in the Database.
Stress test	This checkbox causes the Central Console to continually request maps from the SE coordinator. When in this mode, the Central Console sends a new map request as soon as it receives a map from the SE coordinator, rotating through the map types. This test is used when diagnosing communications problems to create artificially high traffic on the communication link without interfering with the processing of alarms and tests. The stress test ceases when the checkbox is cleared, or this screen is closed by clicking the **[Cancel]** button.
Current Troubles	This window displays all current troubles for this SE coordinator. In the **Current Transponder Status** dialog, there is a low battery and a tamper condition being reported for this SE coordinator. This window also displays the restoration to a normal condition when it

Element	Usage/Description
	occurs. When the fault is corrected, clicking the **[Acknowledge]** button eliminates any restoration reports. Conditions, which were not rectified, remain in the window.
[Not Responding Map]	To assist in diagnosing problems with the SE receivers associated with an SE coordinator, several commands can be issued from the Central Console to requesting information from the SE coordinator. This button requests a map of all the devices on this SE coordinator that are not responding to the system. The current troubles list is automatically updated.
[Out of Service Map]	This button requests a map of all devices on this SE coordinator that were manually taken out of service to the system. The current troubles list is automatically updated.
[Reset Transponder Troubles]	This button is used to reset all of the alarm, test and message counters to zero, and to remove any restoration reports.
[Jamming Map]	This button requests a map of all the SE receivers on this SE coordinator that are reporting a jamming condition to the system. The **Current Troubles** list is automatically updated.
[Tamper Map]	This button requests a map of all the devices on this SE coordinator that are reporting a tamper condition to the system. The current troubles list is automatically updated.
[Input 1 Map]	This button requests a map of all Input 1s on this SE coordinator that are reporting an activation to the system. The current troubles list is automatically updated.
[Input 2 Map]	This button requests a map of all the Input 2s on this SE coordinator that are reporting an activation to the system. The current troubles list is automatically updated.
[Previous]	Returns to the previous SE coordinator.
[Next]	Advances to the next SE coordinator.
[Acknowledge]	Clicking this button removes all restored troubles from the current troubles list.
[Refresh Data]	Clicking this button updates all of the SE coordinator level data in this screen. It does not update the device troubles (use stress test or auto scan to update the device troubles).
[Cancel]	Clicking this button cancels all commands and closes the dialog window.

10.4.6 Transponder parameter change

This dialog allows parameters stored in the SE coordinator's EEPROM memory to be viewed and changed.

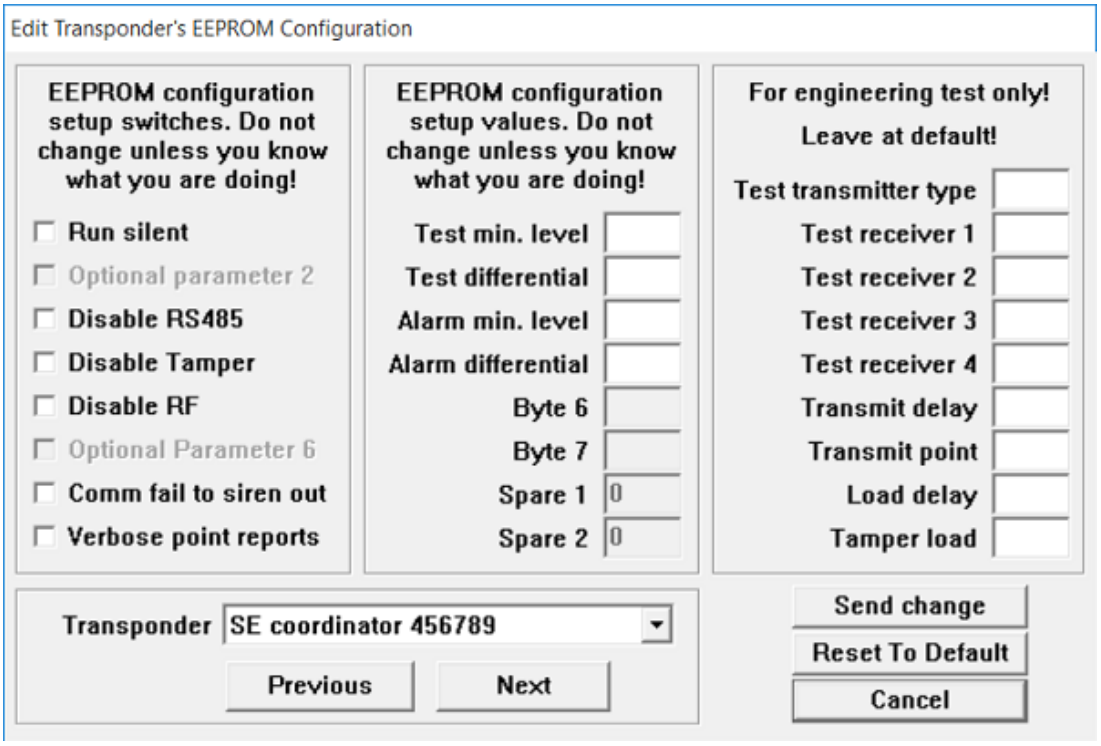


Figure 10.22: Transponder parameter change dialog

Element	Usage/Description
Run silent	If selected, the SE receivers on this SE coordinator bus do not sound an alarm. This includes alarms received during a communications failure with the Central Console.
Optional parameter 2	This option is currently disabled and reserved for future use.
Disable RS485	If selected, the RS485 bus on this SE coordinator is disabled.
Disable Tamper	If selected, the tamper on this SE coordinator is disabled.
Disable RF	If selected, the radio frequency (RF) functionality on this SE coordinator is disabled.
Optional Parameter 6	This option is currently disabled and reserved for future use.
Comm fail to siren out	If this item is selected, the siren output on this SE coordinator activates when a communications failure is detected at the Central Console.
Verbose point reports	If selected, alarm and test reports include average levels and packet count information. This extra information is for diagnostic proposes only and is not required for system operation. Since the additional data increases the system traffic load leave this item unselected.

Element	Usage/Description
Test min level	This is the minimum receive level (1 to 255) an SE receiver must see before the green light displays acknowledging a successful test. Leave this item at default (128).
Test differential	This is the minimum difference in receive level (1 to 255) an SE receiver must be less than the loudest receiver hearing a test before the green light displays acknowledging a successful test. Leave this item at default (64).
Alarm min. level	This is the minimum receive level (1 to 255) an SE receiver must see before the sounder and red light is displayed for an alarm. Leave this item at default (1).
Alarm differential	This is the minimum difference in receive level (1 to 255) an SE receiver must be less than the loudest SE receiver hearing an alarm before the sounder and red LED are displayed for an alarm. Leave this item at default (255).
Byte 6	This option is currently disabled and reserved for future use.
Byte 7	This option is currently disabled and reserved for future use.
Spare 1	This option is currently disabled and reserved for future use.
Spare 2	This option is currently disabled and reserved for future use.
Test transmitter type **Test receiver 1/2/3/4** **Transmit delay** **Transmit point** **Load delay** **Tamper load**	These parameters are used for engineering system load testing only. **Do not use in a live system**, as they can generate more traffic than a system can handle; therefore, actual alarms may be missed. Leave them at default.
Transponder	Select the SE coordinator the data is presented for from the drop down list.
[Previous]	Returns to the previous SE coordinator in the system.
[Next]	Advances to the next SE coordinator in the system.
[Send change]	Sends the changes made to the selected SE coordinator. Changes are not made to the transponder EEPROM memory unless this button is clicked.
[Reset to Default]	Reset the selected SE coordinator to the default settings.
[Cancel]	Cancel the operation and close the dialog window.

10.4.7 Transponder data view

This dialog is solely for engineering evaluation of the SE coordinator only.

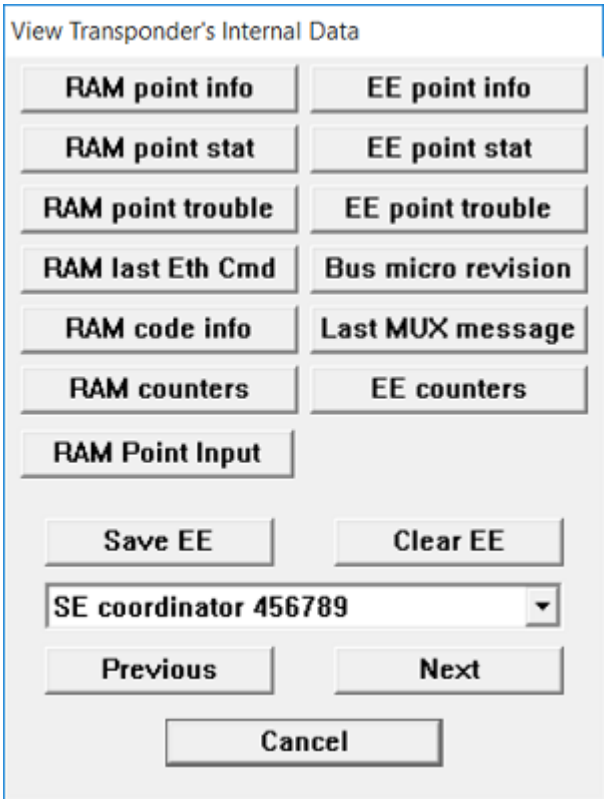


Figure 10.23: Transponder data view dialog

Element	Usage/Description
[RAM point info]	Views the RAM image of point information.
[RAM point stat]	Views the RAM image of point status.
[RAM point trouble]	Views the RAM image of point trouble.
[RAM last Eth Cmd]	Views the RAM image of last Ethernet command.
[RAM code info]	Views the RAM image of code information.
[RAM counters]	Views the RAM image of the process registers.
[EE point info]	Views the EEPROM image of point information.
[EE point stat]	Views the EEPROM image of point status.
[EE point trouble]	Views the EEPROM image of point trouble.
[Bus micro revision]	Views the bus micro revision for the connected points.
[Last MUX message]	Views the last MUX bus message received.
[EE counters]	Views the EEPROM image of the process registers.
[Save EE]	Saves the current RAM image to the EEPROM memory on the SE coordinator.
[Clear EE]	Clears the EEPROM memory on the SE coordinator and resets the transponder.
[Previous]	Returns to the previous SE coordinator in the system.

Element	Usage/Description
[Next]	Advances to the next SE coordinator in the system.
[Cancel]	Cancels the operation and closes the dialog window.

10.4.8 Receiver configuration

Once the SE receiver configuration for an SE coordinator has been entered into the **Transponder database**, this dialog is used to verify that each SE receiver is working and is properly addressed in the database. This setup tool identifies errors in the address switch settings of SE receivers as well as data entry errors in the **Transponder database**.

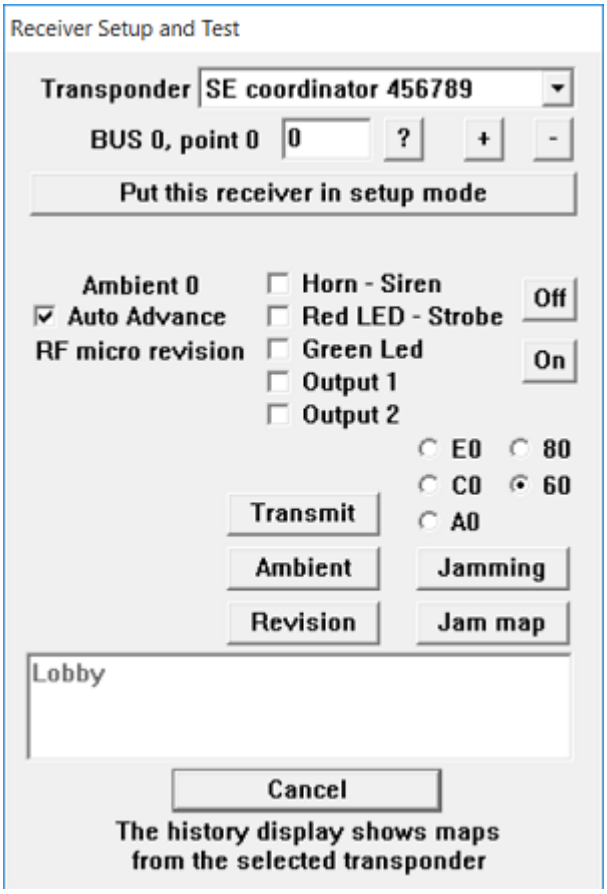


Figure 10.24: Receiver configuration dialog

Element	Usage/Description
Transponder	Select the SE coordinator from the drop down list.
BUS 0, point / [?] / [+] / [-]	Enter directly or use the grid or forward/backward buttons to select the SE receiver point number.
[Put this receiver in setup mode]	This button initiates the setup process by causing both the red and green LED of the selected SE receiver to light up. The red and green LED will be flashing. On the Central Console, this button changes to the **[Abort setup for this MUX Point]** button in order to proceed to the next device in the event that one SE receiver is not set up properly.

Element	Usage/Description
Ambient value	The **Ambient** value, above **Auto Advance,** shows the current ambient level at the SE receiver. To get an updated ambient reading, select the point and click the **[Transmit]** button followed by the **[Ambient]** button.
Auto Advance	If this checkbox is selected, the Central Console automatically selects the SE receiver with the next higher point address.
RF micro revision	The SE receiver's RF micro revision level is shown below **Auto Advance**. To get an updated reading, click the **[Revision]** button.
Horn - Siren	If this checkbox is selected, the horn output of the SE receiver is turned on upon clicking the **[On]** button, or turned off upon clicking the **[Off]** button. If this checkbox is not selected, the state of this output does not change. For details on the siren, please refer to the Security Escort manuals.
Red LED - Strobe	If this checkbox is selected, the red LED output of the SE receiver is turned on upon clicking the **[On]** button, or turned off upon clicking the **[Off]** button. If this checkbox is not selected, the state of this output does not change. For details on the strobe, please refer to the Security Escort manuals.
Green Led	If this checkbox is selected, the green LED output of the SE receiver is turned on upon clicking the **[On]** button, or turned off upon clicking the **[Off]** button. If this checkbox is not selected, the state of this output does not change.
Output 1	If this checkbox is selected, output 1 of the SE receiver is turned on upon clicking the **[On]** button, or turned off upon clicking the **[Off]** button. If this checkbox is not selected, the state of this output does not change.
Output 2	If this checkbox is selected, output 2 of the SE receiver is turned on upon clicking the **[On]** button, or turned off upon clicking the **[Off]** button. If this checkbox is not selected, the state of this output does not change.
[Off]	Upon clicking this button, any checked outputs (**Horn-Siren**, **Red LED - Strobe, Green Led, Output 1 and Output 2**) is turned off for the selected SE receiver. If the output does not change, click the **[On]** button followed by the **[Off]** button again.
[On]	Upon clicking this button, any checked outputs (**Horn-Siren**, **Red LED - Strobe, Green Led, Output 1 and Output 2**) is turned on for the selected SE receiver. If the output does not change, click the **[Off]** button followed by the **[On]** button again.
[Reset point]	Clicking this button causes the microprocessors on this SE receiver to reset as if they were just powered up. An SE receiver should not be reset in a working system, as it can cause receptions to be lost.
[Transmit]	Clicking this button causes this SE receiver to send one test transmission.

Element	Usage/Description
[Ambient]	Clicking this button causes the system to interrogate the current ambient levels of all SE receivers on this SE coordinator.
[Revision]	Clicking this button causes the system to interrogate the RF micro revision levels of all SE receivers on this SE coordinator.
[Jamming]	An SE receiver monitors the ambient level during normal operation. If the ambient level rises above the jamming setting and jamming trouble, it is reported to the Central Console. The SE receiver's jamming level can be adjusted by selecting the appropriate setting (shown in hexadecimal levels) and clicking the **[Jamming]** button.
[Jam map]	Clicking this button causes the system to interrogate the jamming setting levels of all SE receivers on this SE coordinator.
[Cancel]	Clicking this button closes the dialog window.

Put this receiver in setup mode

This button initiates the setup process by causing both the red and green LED of the selected SE receiver to light up. The red and green LED will be flashing. On the Central Console, this button changes to the **[Abort setup for this MUX point]** button to be able to proceed to the next device in the event that one receiver is not set up properly.

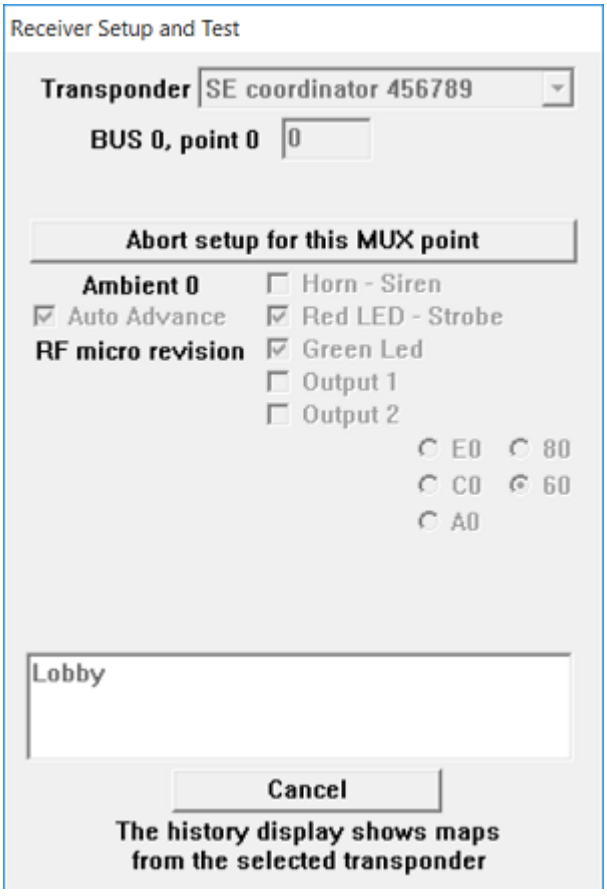


Figure 10.25: Abort button to remove a device from the Setup Mode

The next step is to use a maintenance transmitter to transmit an alarm while standing near the SE receiver.

Notice!
The illuminated LED indicate to the service person standing near the device that the SE receiver is actually the one currently in the setup mode. If the LED of the designated SE receiver is not illuminated, there is probably an error in the switch settings of the SE receiver or an error in the address in the **Transponder database**. To help resolve such problems, the person at the Central Console can command any device to illuminate its LED and/or sound its horn.

If the SE receiver in the setup mode detects the maintenance alarm, and if the received signal is the strongest of all SE receivers, the horn on the SE receiver sounds briefly and the LEDs go off. This indicates the SE receiver is functioning properly and the SE receiver's address is set correctly in the **Transponder database**, as well as on the SE receiver's switches.
The Central Console also confirms the successful setup with an audible and text message. The **[Abort setup for this MUX point]** button disappears, and is replaced by **[Test on this MUX point SUCCESSFUL]** button. Click the button to conclude the test of this point.

10.4.9 Receiver test

Use this dialog to set up and monitor four SE receivers, and listen to one SE receiver transmitting with its buddy check transmitter. Normally, the function is for engineering evaluation of new transmitter and SE receiver designs, but it can be used to test SE receiver boards and locations in a working system.

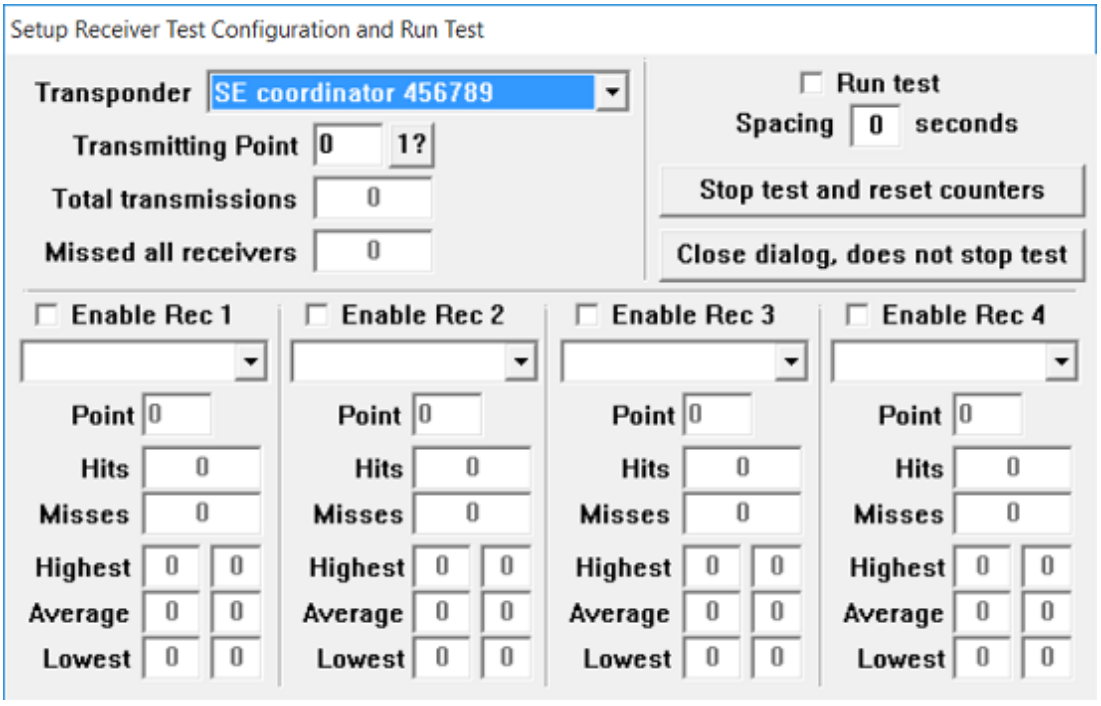


Figure 10.26: Receiver test dialog

Element	Usage/Description
Transponder	Select the SE coordinator for the transmitting point and each receiving point. They can be on the same or different SE coordinators.
Transmitting Point	Select the point (SE receiver) on the selected SE coordinator to generate the transmissions.

Element	Usage/Description
Total transmissions	The total number of times the designated SE receiver transmitted the test message.
Missed all receivers	The total number of times where the test transmission was not heard by any of the designated SE receivers.
Enable Rec	This checkbox must be selected for this SE receiver to monitor the test transmissions.
Point	Select the point (SE receiver) on this SE coordinator to monitor the test transmissions.
Hits	The number of times this SE receiver successfully heard the test transmission.
Misses	The number of times this SE receiver failed to hear the test transmission.
Highest	The left box displays the highest receive level at which the test transmission was heard. The right box displays the greatest number of packets heard from a single test transmission.
Average	The left box displays the average receive level at which the test transmission was heard. The right box displays the average number of packets heard from a single test transmission.
Lowest	The left box displays the lowest receive level at which the test transmission was heard. The right box displays the least number of packets heard from a single test transmission.
Run test	The test only runs when this checkbox is selected. To stop the test and retain the test values, unselect this checkbox.
Spacing	This slows the test by forcing this number of seconds between test transmissions. Normally, this setting is left at the default value 0 seconds.
Stop test and reset counters	Clicking this button stops the test and resets all values.
Close dialog, does not stop test	Clicking this button closes this dialog but does not stop the test from running. Reopening the dialog displays the current progress of the test. The test should not be left running unless there is a specific need, as it generates both RF and system traffic.

10.4.10 Network status

This dialog shows the status of communications on the network, modem, and system serial ports.

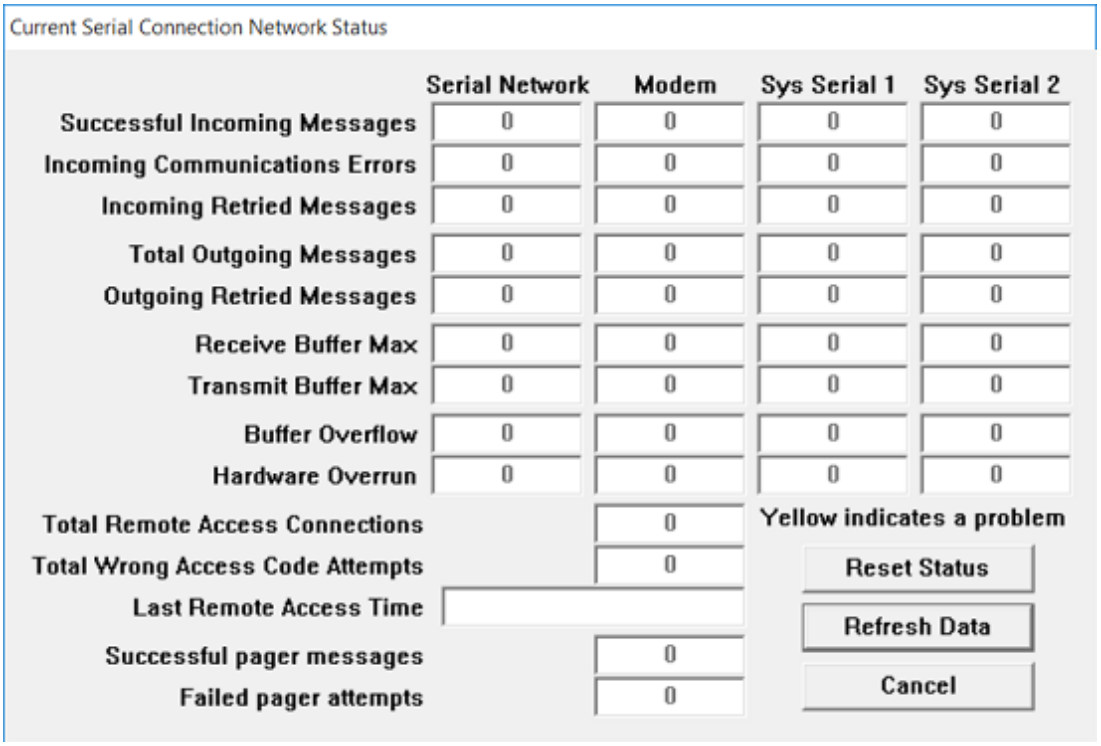


Figure 10.27: Network status dialog

Element	Usage/Description
Successful Incoming Messages	This value is the number of messages that the system successfully received on this communication port.
Incoming Communication Errors	This value is the number of messages that the system detected errors in, on this communication port. If displayed in yellow, this value is more than 1.5% of the **Successful Incoming Messages**.
Incoming Retried Messages	This value is number of successful receptions that indicated that they retried by the sending application. If displayed in yellow, this value is more than 1.5% of the **Successful Incoming Messages**.
Total Outgoing Messages	This value is total number of outgoing messages sent on this port.
Outgoing Retried Messages	This value is number of outgoing messages that were retried because the receiving application did not acknowledge them. If displayed in yellow, this value is more than 1.5% of the **Total Outgoing Messages**.
Receive Buffer Max	This value is maximum number of bytes received on this serial port, but not yet processed by the system. If displayed in yellow, more than 50% of the queue was in use.
Transmit Buffer Max	This value is maximum number of bytes processed by the system, but not yet transmitted on this serial port. If displayed in yellow, more than 50% of the queue was in use.

Element	Usage/Description
Buffer Overflow	This is the number of times a byte was lost by the software for a serial port because the input buffer overflowed. Bytes were placed into the input buffer faster than the system could process them.
Hardware Overrun	This is the number of times a byte was lost by the hardware for a serial port because it was not fast enough to process the byte into the input buffer.
Total Remote Access Connections	This value is the total number of times a remote access connection was successful.
Total Wrong Access Code Attempts	This value is the number of times a remote access connection was attempted and rejected because a valid remote access code was not received.
Last Remote Access Time	This is the time and date of the last successful remote access attempt.
Successful pager messages	This value is the number of successful pager messages sent.
Failed pager attempts	This value is the number of times a pager message dial-out was unsuccessful.
[Reset Status]	Clicking this button resets all values shown in this dialog.
[Refresh Data]	Clicking this button refreshes all values shown in this dialog. The values are not automatically updated when the dialog is left open.
[Cancel]	Clicking this button closes the dialog window.

10.4.11 System status

This dialog shows the status of internal system queues and communications on the serial ports assigned to SE coordinators.

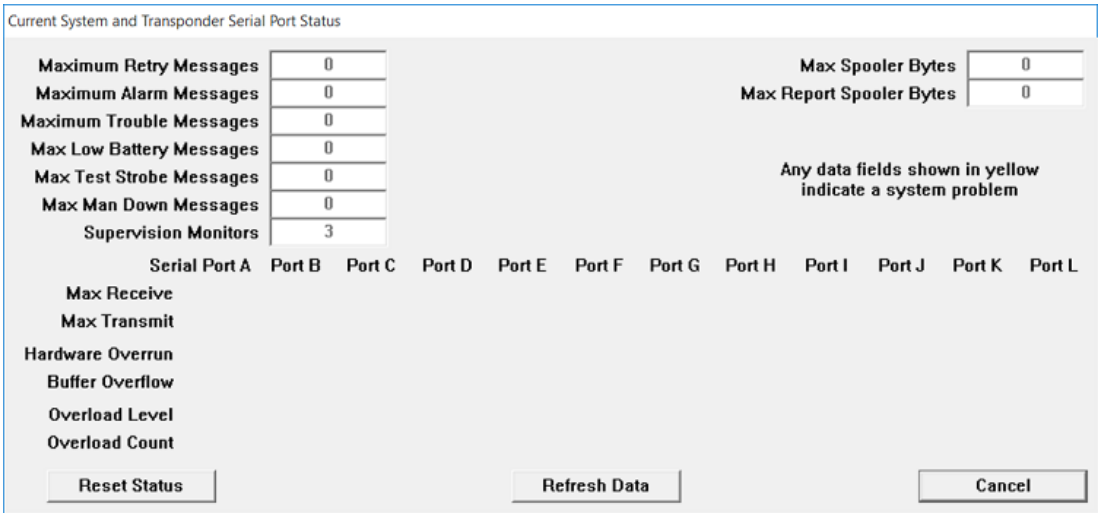


Figure 10.28: System status dialog

Element	Usage/Description
Maximum Retry Messages	This value is maximum number of messages in queue to be sent to all SE coordinators in the system, and were not yet acknowledged. If displayed in yellow, more than 50% of the queue was in use at this value.
Maximum Alarm Messages	This value is the maximum number of alarms that the system processed at its busiest time. If displayed in yellow, more than 50% of the maximum was in use.
Maximum Trouble Messages	This value is the maximum number of troubles in the queue yet to be displayed. If displayed in yellow, more than 50% of the queue was in use.
Max Low Battery Messages	This value is the maximum number of transmitters with low batteries yet to be displayed. If displayed in yellow, more than 50% of the queue was in use.
Max Test Strobe Messages	This value is the maximum number of test strobes in use at one time. If displayed in yellow, more than 50% of the queue was in use.
Max Man Down Messages	This value is the maximum number of transmitters timing man down events, at one time. If displayed in yellow, more than 50% of the queue was in use.
Supervision Monitors	This value is the current number of transmitters being monitored for supervision transmissions.
Max Spooler Bytes	This value is the maximum number of bytes spooled for the printer at one time. If displayed in yellow, more than 50% of the queue was in use.
Max Report Spooler Bytes	This value is the maximum number of bytes spooled for the printer for Guard Tour Reports at one time. If displayed in yellow, more than 50% of the queue was in use.
Max Receive	This value is the maximum number of bytes received from SE coordinator on this serial port, but not yet processed by the system. If displayed in yellow, more than 50% of the queue was in use.
Max Transmit	This value is the maximum number of bytes processed by the system, but not yet transmitted to the SE coordinators on this serial port. If displayed in yellow, more than 50% of the queue was in use.
Hardware Overrun	This is the number of times a byte was lost by the hardware for a serial port because it was not fast enough to process the byte into the input buffer.
Buffer Overflow	This is the number of times a byte was lost by the software for a serial port because the input buffer overflowed. Bytes were placed into the input buffer faster than the system could process them.

Element	Usage/Description
Overload Level	This is a measure of the amount of time peak traffic on this serial port was greater than the system's ability to handle it. The system automatically sheds non-essential tasks when this value rises.
Overload Count	This is a measure of the number of times peak traffic on this serial port was greater than the system's ability to handle it. The system automatically sheds non-essential tasks when this value rises.
[Reset Status]	Clicking this button resets all values in this shown in this dialog.
[Refresh Data]	Clicking this button refreshes all values shown in this dialog. The values are not automatically updated when the dialog is left open.
[Cancel]	Clicking this button closes the dialog window.

10.4.12 System preferences

The **System Preferences** dialog under the **Setup** menu contains a number of settings that govern the behavior of the Security Escort system.
See *System Preferences, page 108* for details.

10.4.13 Transponder comm port setup

Go to menu **Setup > Transponder comm port setup...** This dialog connects the communication port indexes set for each transponder in the **Transponder database** to the physical communication ports on the computer.

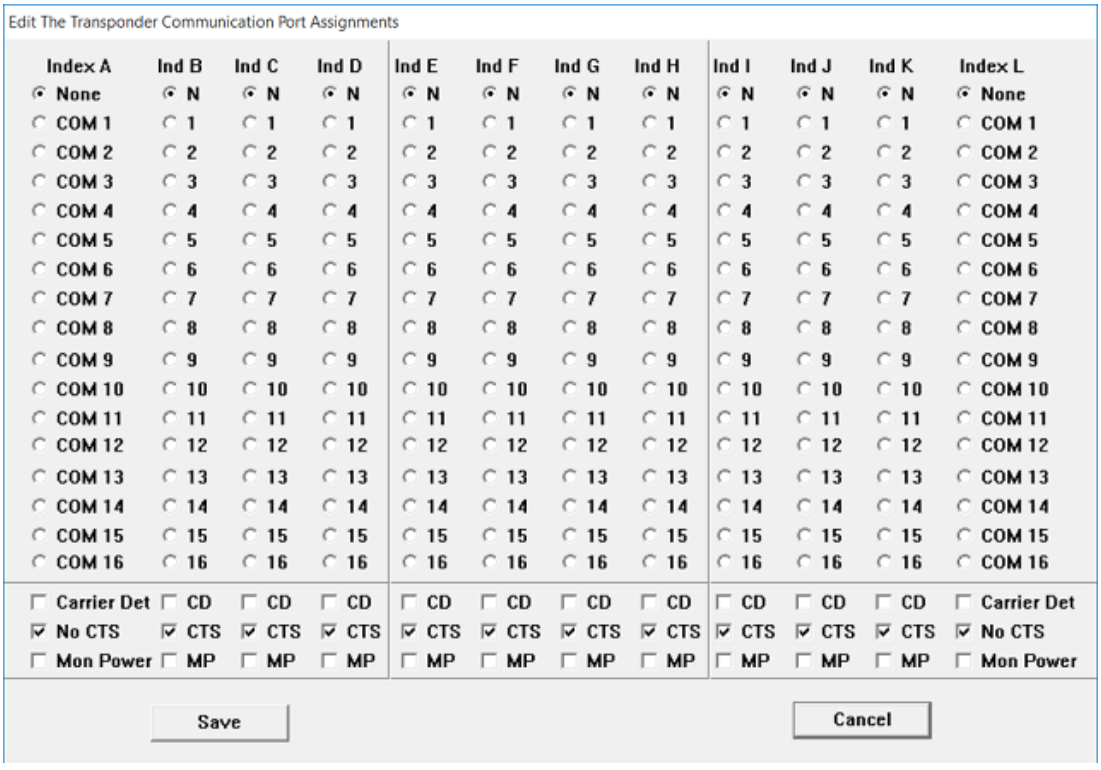


Figure 10.29: Transponder comm port setup dialog

Element	Usage/Description
COM	The actual physical communication port over which communications to the transponder will be carried.
Carrier Det	If selected, verify that the communications port is not in use before communicating. Only to be used on half duplex links where Carrier Detect indicates that the link is in use. This setting is normally unselected and rarely used.
No CTS	If selected, do not monitor the Clear to Send before communicating. This setting is normally selected.
Mon Power	If selected, monitor the Ring Indicator pin to indicate a remote power supply used on this communication link has not failed. This setting is normally unselected.

10.4.14 Remote comm port setup

This dialog connects the network, modem and system serial ports to the physical communication ports on the computer and sets their baud rate.
See *Remote comm port setup, page 61* for details.

10.4.15 Remote setup

This dialog sets up the remote access and system serial port parameters.
See *Remote setup, page 63* for details.

10.4.16 Remote connection

10.4.17 Pager setup

This dialog sets up remote pager access for troubles (service) and alarms (security).

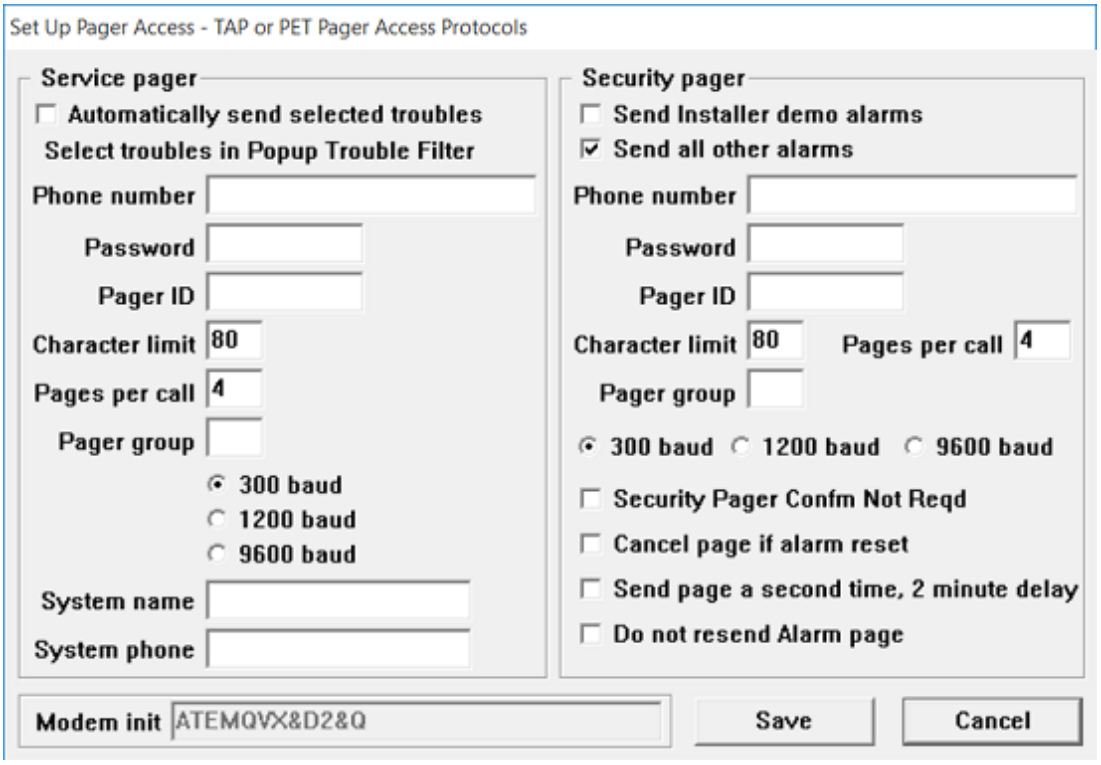


Figure 10.30: Pager setup dialog

Element	Usage/Description
Automatically send selected troubles	If this checkbox is selected, the system sends all the selected troubles from the **Popup trouble filter** dialog to the service pager.
Phone number	Phone number to be dialed to access the paging service. This phone number is usually different from the number you would manually dial to send a page. The paging company assigns this value.
Password	This is the password that must be sent to the paging service to send the page. If not required, leave this field black. Usually a password is not required. The paging company assigns this value.
Pager ID	This is the ID that identifies the specific pager that this message is to be sent to. Many times, it is the last 7 digits of the phone number that you would manually dial to access this pager. The paging company assigns this value.
Character limit	This is the maximum number of characters allowed per page. Default is set to 80 characters. The Security Escort system will truncate the pager message at this number of characters. The paging company assigns this value.
Pages per call	This is the maximum number of pager messages allowed per phone call. Default is set to 4 pages per call. When this number of messages have been sent, and there are more messages to be delivered; the Security Escort system will hang up and redial the paging service to deliver the remaining messages. The paging company assigns this value.
Pager group	This is the group of up to 8 pagers that this message is to be sent to. You may program the individual pager as well as a group of pagers. The pager group will be sent the page before the individual.
Baud rate	Select the baud rate that will be used to communicate with the paging computers. The paging company assigns this value.
System name	This identifies the Security Escort system when multiple Security Escort systems report to the same service pager. Keep this field as short as reasonably possible since these characters, including space character, will be sent before each trouble message and they are included in the **Character limit** set above. If not desired, leave blank.
System phone	This will present phone number to be called in response to the service page. Only use if required since these characters, plus a space, will be sent before each trouble message. They are included with the **System name** in the **Character limit** set above. If not desired, leave as blank.

Element	Usage/Description
Send installer demo alarms	If the checkbox is selected, demo alarms will be sent to the security pager.
Send all other alarms	If the checkbox is selected, all actual alarms will be sent to the security pager.
Security Pager Confm Not Reqd	If the checkbox is selected, the confirmation pager message is not sent to the security pager when the alarm is acknowledged by an acknowledgement transmitter.
Cancel page If alarm reset	If the checkbox is selected, the alarm page will be canceled if the alarm is reset before it can be communicated to the paging service.
Send page a second time, 2 minute delay	If the checkbox is selected, an alarm page will be sent a second time to the security pager. Do this in case the pager was in an area where pages could not be heard when the first page was sent.
Do not resend Alarm page	If the checkbox is selected, a pager message is sent to the security person only once till the alarm is cancelled or acknowledged.
Modem init	This is the initialization string sent to the modem to set it up for pager communications. Normally, this setting would not have to be changed. To allow changes to this string, hold down the <Shift>+<Ctrl> keys when this dialog is first opened. This string is specific to each modem model. The default setting should work with most modems.
[Save]	Save the changes and close the dialog window.
[Cancel]	Cancel the changes and close the dialog window.

10.4.18 Send pager message

This dialog allows manually entered messages to be sent to the service or security pagers. Service and security pagers are configured in the **Pager setup** dialog. Individuals and group pager assignments are configured in the **Subscriber database**.

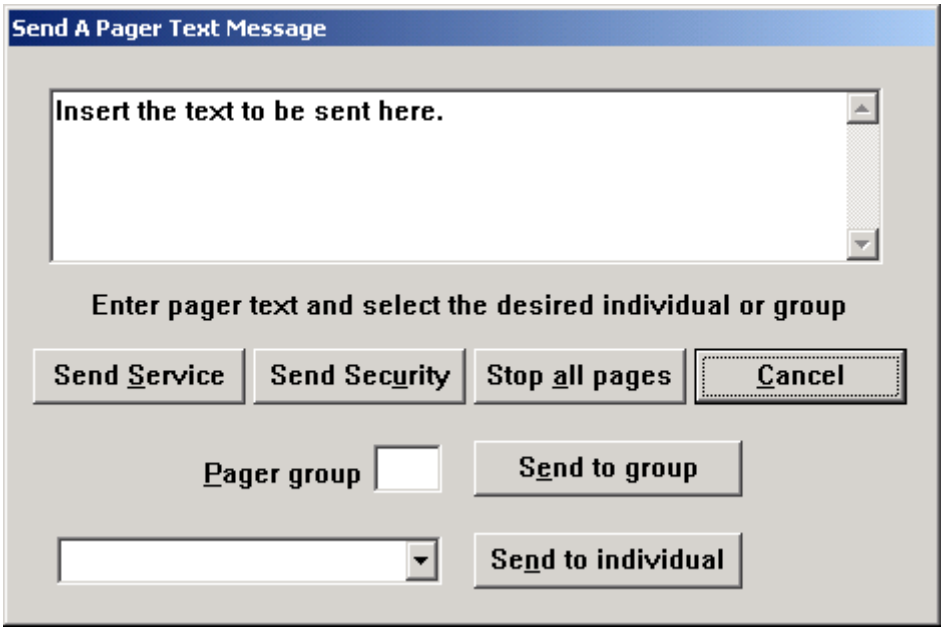


Figure 10.31: Send pager message dialog

Element	Usage/Description
Insert the text to be sent here.	Enter the text to be sent to the pagers in the large text box at the top of the dialog.
[Send Service]	Click this button to send the entered text message to the service pager and service pager group.
[Send Security]	Click this button to send the entered text message to the security pager and security pager group.
[Stop all pages]	Click this button to abort and delete all pages currently queued (automatic or manual). Use with caution.
Pager group	To send a page to all members of a group, enter the pager group number here (1 to 99).
[Send to group]	Click this button to send the entered text message to the indicated pager group.
[Send to Individual]	Click this button to send the entered text message to the individual that is selected from the drop down list.
[Cancel]	Click this button to cancel and close the dialog window.

10.4.19 Utility tool

Use the **Utility tool** to modify network information of the SE coordinators, scan and enroll SE receivers/SE transmitters to the SE coordinators, and upload firmware for SE coordinators, SE receivers and SE transmitters.

See *Configuring equipment using Utility tool, page 86* for details.

10.4.20 Email Setup

This dialog allows you to configure the settings of the SMTP server and the emails for the notification groups so that emails, for example alarms or reports, can be sent to the groups.

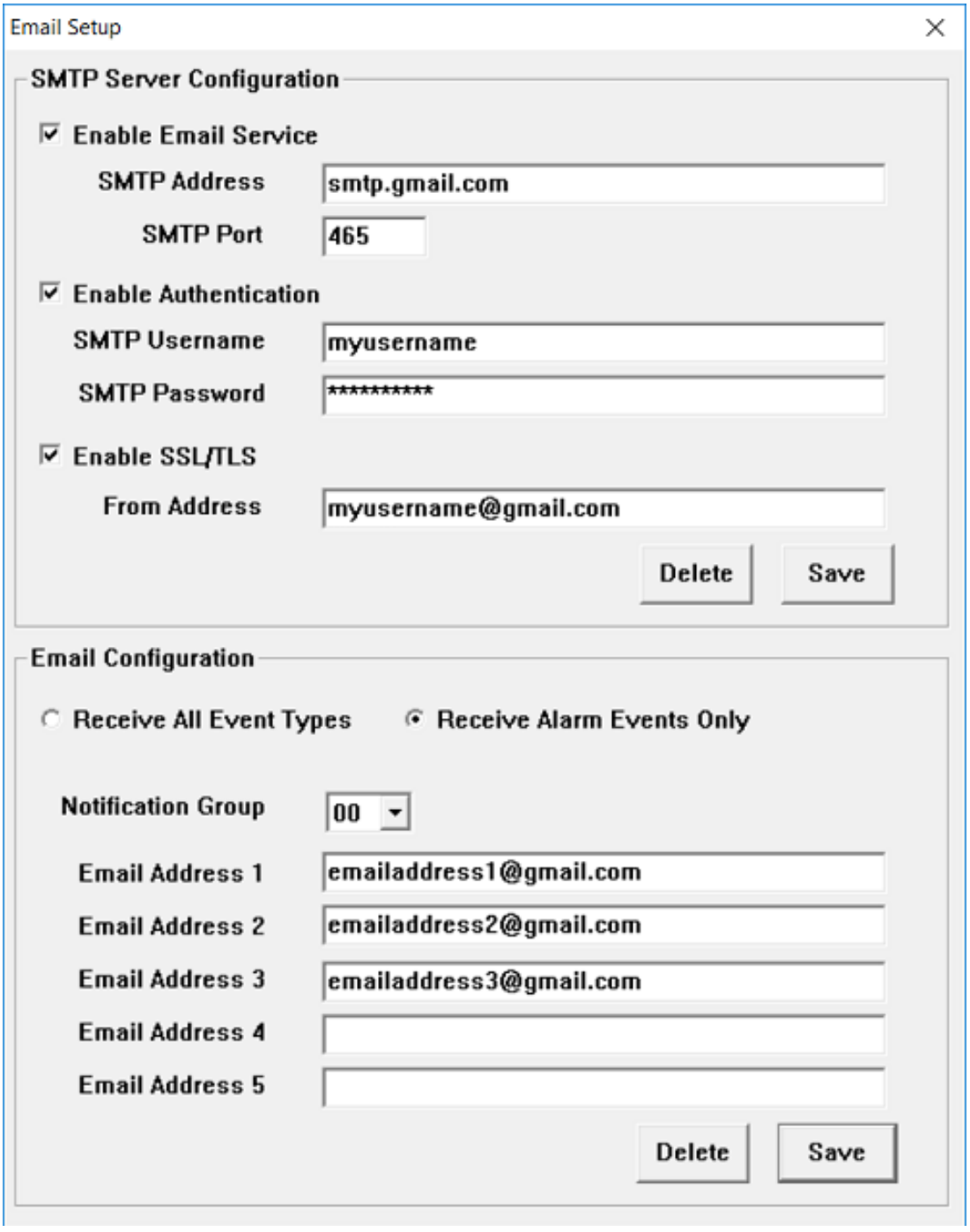


Figure 10.32: Email Setup dialog

Notice!
To setup the email notification, you need to configure your SMTP server settings. Check with your SMTP server provider if you are unsure of the configuration.

Element	Usage/Description
SMTP Server Configuration group	

Element	Usage/Description
Enable Email Service	Select this checkbox to configure the SMTP server information. If this is not selected, email will not be sent out.
SMTP Address	SMTP server address, e.g. “smtp.gmail.com”. Maximum number of characters is 74.
SMTP Port	Port number that the SMTP server uses for communication. Generally, port 25, 465 or 587 is used, but some may use customized port from 1 to 65535. **Note:** Ensure that the port is not blocked on your network.
Enable Authentication	Select this checkbox if the SMTP server requires username and password authentication before the email can be sent out.
SMTP Username	Enter the SMTP username for authentication by SMTP server. Maximum number of characters is 31.
SMTP Password	Enter the SMTP password of the user for authentication by SMTP server. Maximum number of characters is 31.
Enable SSL/TLS	Select this checkbox if the SMTP server requires secure communication for the authentication between the SMTP server and client.
From Address	Enter the email address that will authenticate with the SMTP server, e.g. “myusername@gmail.com”. Maximum number of characters is 74.
[Delete]	This button only appears after you have configured and saved the SMTP Server configuration. Click this button to delete the configuration.
[Save]	Click this button to save the changes made to the **SMTP Server Configuration** section.
Email Configuration group	
Receive All Event Types	Select this radio button option for email to be sent whenever an alarm and its auto track is received.
Receive Alarm Events Only	Selected by default. Select this radio button option for email to be sent only on the first instance of the alarm. Subsequent auto track events will not trigger sending of the email notification.
Notification Group	Select the **Notification Group** “00”, “01”, “02”, “03” or “04” from the drop-down list. **Notification Group** “00” is the default group where email notifications for alarms are sent to the recipients. **Note:** If unauthorized alarms are set up to display on the screen (see **Security Preferences** section), these alarms will also be sent via email to the default notification group. **Notification Group** “01”, “02”, “03” and “04” are used to customize emails of alarms for specific subscribers. See the **Subscriber Database Advanced Features** section for details.

Element	Usage/Description
Email Address 1	Alarm email will be sent to email address of person 1. Maximum number of characters is 74.
Email Address 2	Alarm email will be sent to email address of person 2. Maximum number of characters is 74.
Email Address 3	Alarm email will be sent to email address of person 3. Maximum number of characters is 74.
Email Address 4	Alarm email will be sent to email address of person 4. Maximum number of characters is 74.
Email Address 5	Alarm email will be sent to email address of person 5. Maximum number of characters is 74.
[Delete]	This button only appears after you have configured and saved the email configuration. Click this button to delete the selected **Notification Group** configuration.
[Save]	Click this button to save the changes made to the **Email Configuration** section.

The alarm emails that were sent contain the alarm type, location area and date/time of the alarm as the subject header. Name of the subscriber and the subscriber ID, phone number and address are also included in the email content.

10.5 Printer menu

From the **Printer** menu, the printers can be selected to print alarms, reports, history screen, and other files. However, the printers should be turned on or off only by the installation company personnel.

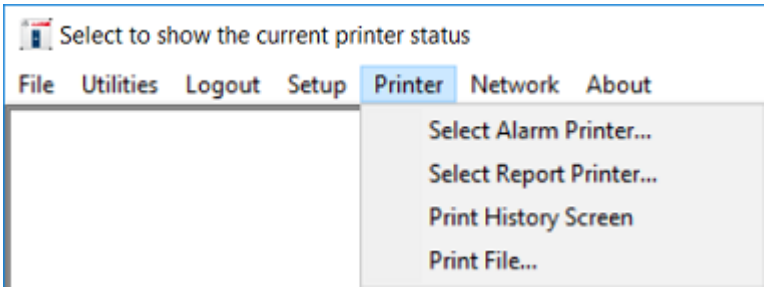


Figure 10.33: Printer menu

10.5.1 Select alarm printer

The alarm printer is used to print all real time event data (alarm, tests, troubles and so on) as they happen. Typically, the alarm printer is a continuous form printer and not a page at a time printer such as a laser printer.

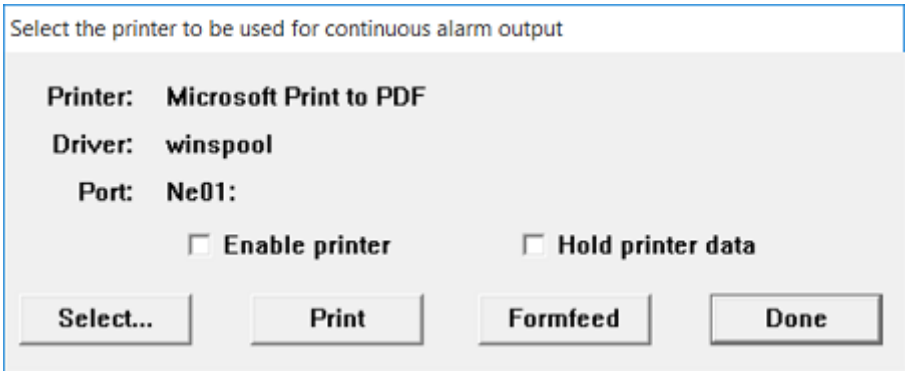


Figure 10.34: Select alarm printer dialog

Element	Usage/Description
Enable printer	Select this checkbox to allow the system to send the real time events to the selected alarm printer.
Hold printer data	Select this checkbox to force the system to hold the data and not send it to the selected alarm printer. This is not a recommended operation, but it allows a page at a time printer to be used as an alarm printer. Use the **[Print]** button to force the data to print on demand.
[Select]	Click this button to open the Window's system printer selection dialog. This dialog is used to select the alarm printer from all of the printers that are installed on this computer.
[Print]	Click this button to print the data that is currently held in Security Escort's alarm printer buffer.
[Formfeed]	Click this button to send a formfeed to the alarm printer.
[Done]	Click this button to close the dialog window.

10.5.2 Select report printer

The report printer is used to print all reports as they are requested automatically or by the operator. Typically, the report printer is a page at a time printer like a laser printer.

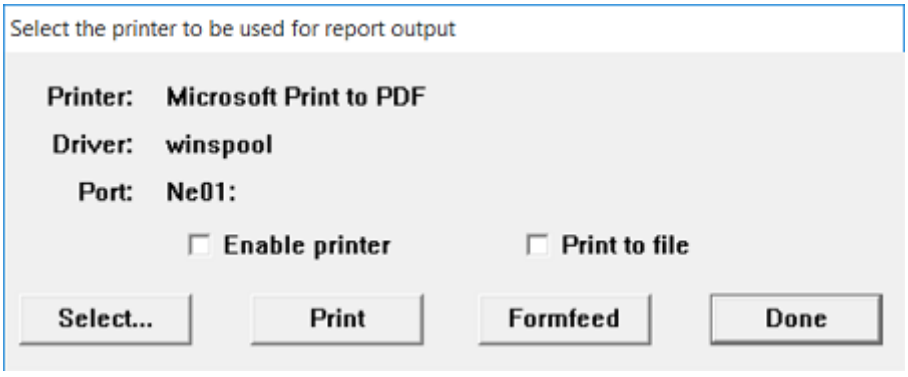


Figure 10.35: Select report printer dialog

Element	Usage/Description
Enable printer	Select this checkbox to allow the system to send the reports to the selected report printer.
Print to file	Select this checkbox to create file copies of all reports. This option is independent of the report printer, which can also be used at the same time.
[Select...]	Click this button to open the Window's system printer selection dialog. This dialog is used to select the report printer from all of the printers that are installed on this computer.
[Print]	Click this button to print the data that is currently held in Security Escort's report printer buffer.
[Formfeed]	Click this button to send a formfeed to the report printer.
[Done]	Click this button to close the dialog window.

10.5.3 Print history screen

The **Print history screen** menu item is disabled when the map is shown on the Security Escort main screen. To enable this menu item, select **Setup > Show history** menu item. This will switch the main screen from the map to the history log. You can now select the **Print history screen** menu item to print all current data in the history screen buffer to the report printer.

10.5.4 Print file

The **Print file** menu item is only available if the report printer is enabled. Otherwise, the menu item remains disabled in grey. Click the Print file menu item to open the dialog window.

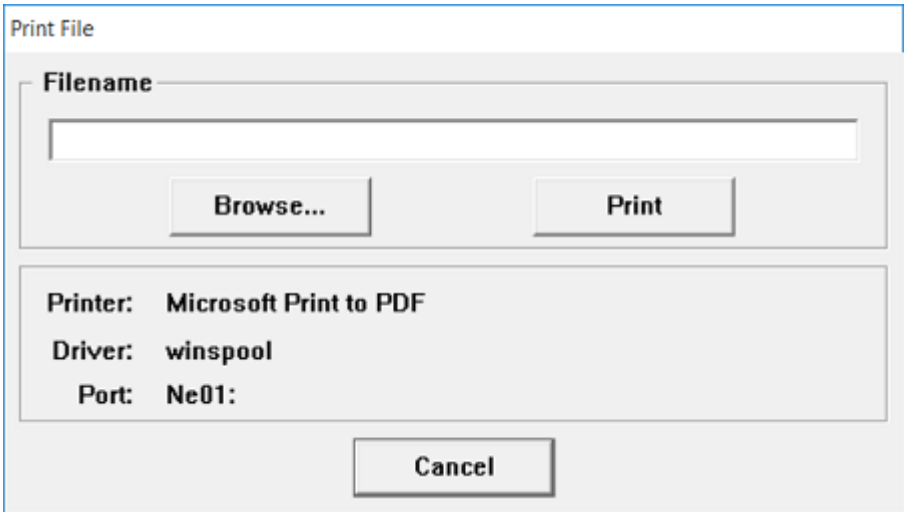


Figure 10.36: Print file dialog

Enter the name of the file to be printed, or click the **[Browse...]** button to open the **Common Open File** dialog and select the file. Then click the **[Print]** button to print the file to the report printer.

10.6 Network menu

The **Network** menu allows an installer to setup and monitor the computer network connections.

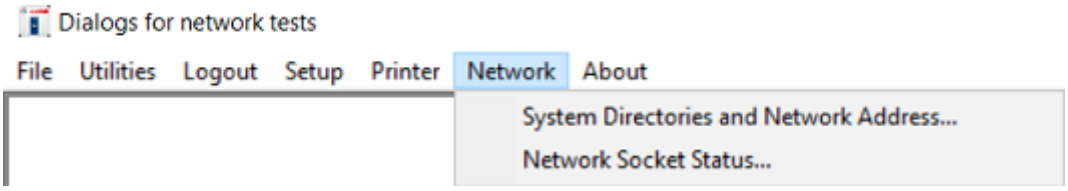


Figure 10.37: Network menu

10.6.1 System directories and network address

Use this dialog to set up the network IP addresses, ports and related options. Database file and backup paths is also configured using this dialog window.

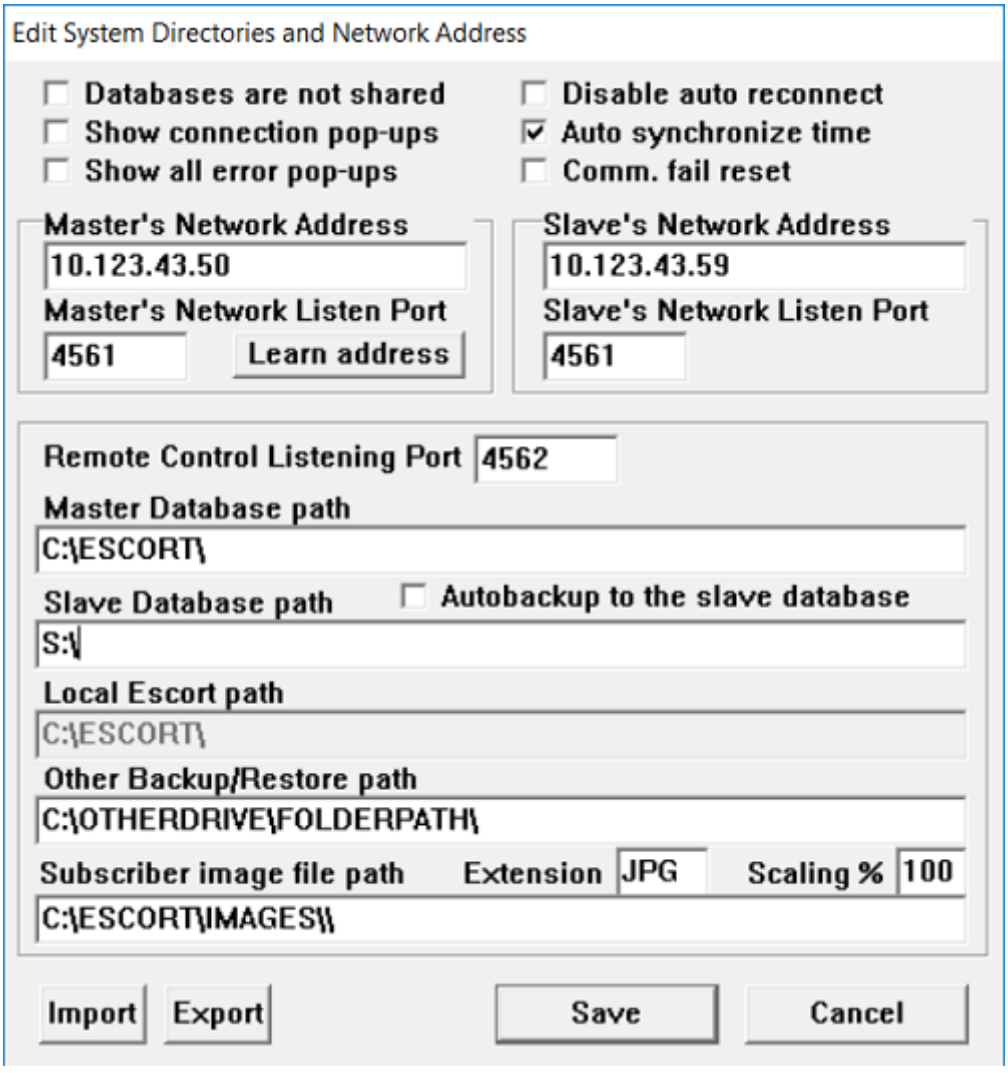


Figure 10.38: System directories and network address dialog

Element	Usage/Description
Databases are not shared	If this option is not selected, the master and all the slave and workstation computers share the same database files. This checkbox must only be selected if each computer has its own copy of the databases stored locally. In normal operation, this checkbox is

Element	Usage/Description
	typically not selected. If this checkbox is selected, the databases must be manually updated using **Backup** and **Restore** every time changes are made to the database.
Show connection pop-ups	If this option is selected, it will display a pop-up message box whenever a network connection is initiated or released with another computer. Unselecting this checkbox stops the message boxes from displaying. In normal operation, this checkbox is typically not selected.
Show all error pop-ups	If this option is selected, it will display a pop-up message box whenever a network error is reported. Unselecting this checkbox stops the message boxes from displaying. In normal operation, this checkbox is typically not selected.
Disable auto reconnect	If this option is selected, the system will not automatically attempt to reconnect a lost connection each minute. Unselecting this checkbox allows the system to automatically reconnect a lost connection. In normal operation, this checkbox should not be selected.
Auto synchronize time	If this option is selected, the master computer will automatically synchronize the time on the slave and workstation computers once each night.
Comm. fail reset	If this option is selected, the master computer will reset when communication failure occurs.
Master's Network Address:	The IP address of the master computer. The Security Escort system requires a fixed IP address for the master computer.
Master's Network Listen Port	A unique number that indicates the Security Escort software is attempting to set up a connection. Other software uses different port numbers, allowing the network interface card to be shared with other network applications. Typically, this is set as “4561”.
Slave's Network Address	The IP address of the slave computer. The Security Escort system requires a fixed IP address for the optional slave computer.
Slave's Network Listen Port	A unique number that indicates the Security Escort software is attempting to set up a connection. Other software uses different port numbers, allowing the network interface card to be shared with other network applications. Typically, this is set to “4561”.
[Learn address]	Clicking this button on the master computer automatically populates the master’s IP address in the **Master’s Network Address** textbox, and the master’s network port in the **Master’s Network Listen Port** textbox. Clicking this button on the slave computer automatically populates the master’s IP address in the **Slave’s Network Address** textbox, and the master’s network port in the **Slave’s Network Listen Port** textbox. If the computer has more than one network interface card (NIC), you must verify that the correct IP address was selected

Element	Usage/Description
	by comparing this address to the IP address that was programmed in the Control Panel TCP/IP protocol. If the address is not correct, manually enter the correct IP address.
Remote Control Listening Port	The Security Escort will be listening on this port to communicate with the OPC server. A separate OPC server is created to communicate between the OPC client and the Security Escort system. The OPC server holds the alarm and trouble messages, and sends the same to the available client once it is connected. The OPC server will send the status of the Security Escort to the OPC client. The OPC sever also acknowledges and deletes alarm and trouble messages from OPC client. If the connection between OPC server and Security Escort goes down, the OPC server will try to reconnect with Security Escort. Once the connection to the Security Escort becomes active, the Security Escort will send all the available alarms to the OPC server. The OPC server in turn sends the alarm back to OPC client; hence the OPC client may display some duplicate alarms.
Master Database path	The path that this slave or workstation computer uses to access the shared database files on the master computer. This path may have a different drive letter on the different slave and workstation computers. They are typically on the master computer, but they may be on a file server or any other network accessible drive.
Autobackup to the slave database	If this option is selected, the slave computer will back up all databases in the **Master Database path** to the **Slave Database path** each night at 3:00 am.
Slave Database path	The path that this master or workstation computer uses to access the hot backup database files on the slave computer. This path may have a different drive letter on the different master and workstation computers. They are usually on the slave computer, but they may be on a file server or any other network accessible drive. Typically, they would not be stored on the same computer as the **Master Database path**, so a single failure would not prevent access to both the master and slave database files.
Local Escort path	The path on this workstation where the Security Escort was installed in. Typically it is “C:\ESCORT”.
Other Backup/ Restore path	When backing up the database to or restoring it from external disks, this is the path that is used.
Subscriber image file path	The Security Escort System software can display an image for each subscriber on the alarm screen. This parameter tells the software the path where the image files are stored. The default is “C:\ESCORT \IMAGES”.
Extension	The subscriber images can be in JPEG or Windows Bitmap format. All images in a system must be in the same format. For the JPEG format, enter the Windows extension “JPG”. For the Bitmap format, enter the Windows extension “BMP”.

Element	Usage/Description
Scaling %	When the display is set to 640x480 pixels, and subscriber images are being displayed, this parameter controls the image size. This value can range from 10 to 100%, and should be adjusted while viewing alarms to get the desired image size. When the display is set to 800x600 or larger (recommended), this parameter has no effect.
[Import]	Import the workstation settings in the XML file format.
[Export]	Export the workstation settings in the XML file format.
[Save]	Clicking this button saves the changes and closes the dialog window.
[Cancel]	Clicking this button aborts the changes and closes the dialog window.

Settings used in the XML file format of the import and export feature

The attributes and settings of the following dialogs are used in the XML file format for the import and export feature.

Menu	Dialog
Utilities	Security Preferences
Setup	History filter
	System preferences
	Alarm zones
	Transponder comm port setup
	Remote comm port setup
Printer	Select alarm printer
	Select report printer
Network	System directories and network address

Exporting the workstation settings

To export the workstations settings, go to menu **Network > System directories and network** dialog, and click the **[Export]** button.

Notice!

The export operation does not change the existing settings in Security Escort.

A file dialog appears for you to choose the folder where you wish to save the file in, and provide a name for the file.

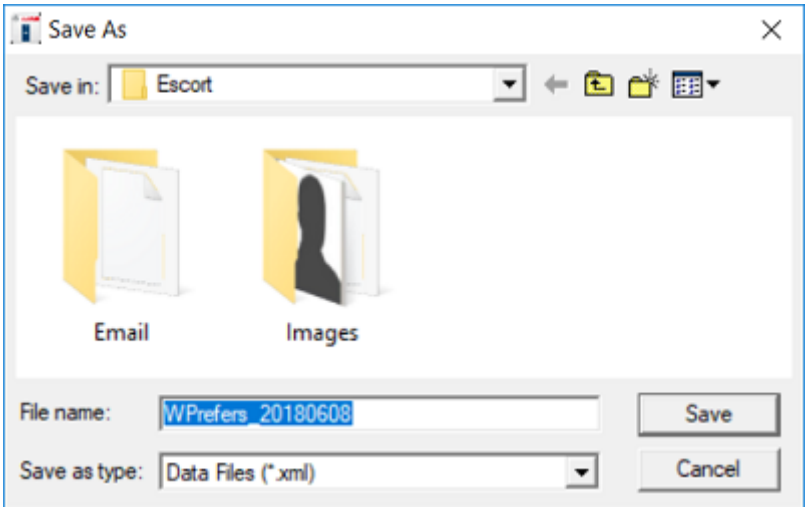


Figure 10.39: Export file dialogt

If you wish to abort the task, click the **[Cancel]** button. Otherwise, click the **[Save]** button to export the global preferences setting. If a file of the same name already exists, a confirmation dialog appears asking if you wish to replace the file.

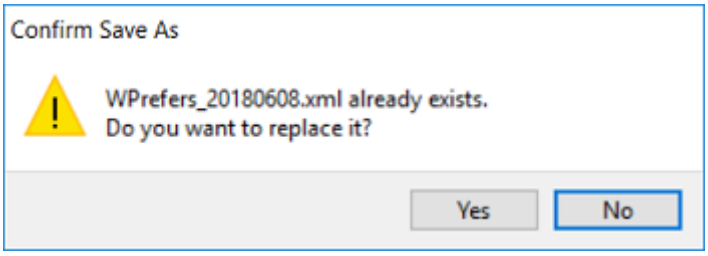


Figure 10.40: Replace file confirmation dialog

Click the **[No]** button to abort and return to the file dialog where you can choose a different name for the file. Otherwise, click the **[Yes]** button to proceed with replacement of the file. If the export is successful, a confirmation dialog appears. You will find the file in the specified folder.

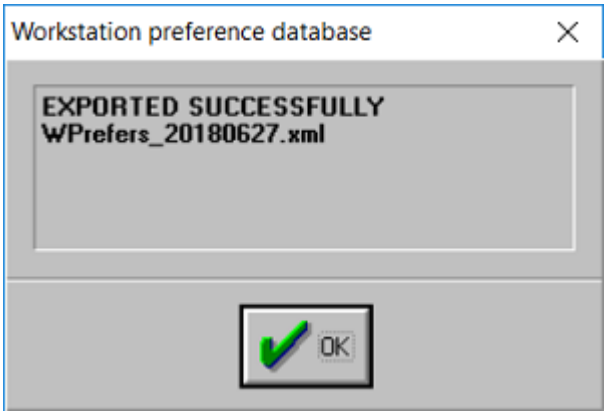


Figure 10.41: Workstation preference successfully exported dialog

Importing the workstation settings

To import the workstation settings into the Security Escort system, the file to be imported must already be prepared in the XML file format. Go to menu **Network > System directories and network address** dialog, and click the **[Import]** button.

Notice!
This action is irreversible! There is no way to undo the operations.

A popup dialog appears asking for the file to be imported. Click the **[Cancel]** button to abort if you are still unsure. Otherwise, navigate the folders, select the file and click the **[Open]** button.

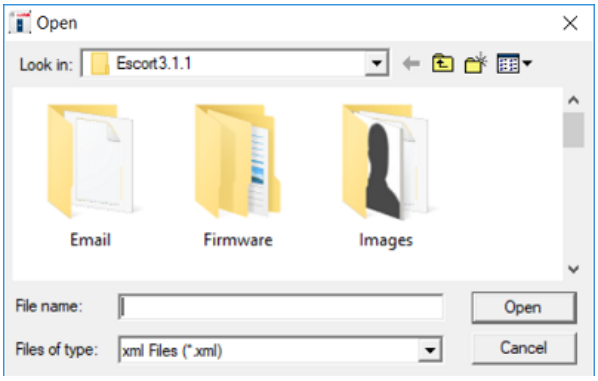


Figure 10.42: Import file dialog

A popup dialog appears, asking for confirmation to proceed with the import or to abort the operation. Click the **[No]** button to abort if you are still unsure. Click the **[Yes]** button to proceed with the import.

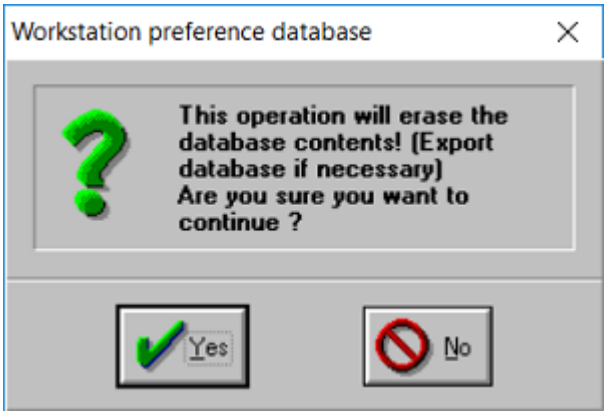


Figure 10.43: Import confirmation dialog

If the data is imported successfully, a popup confirmation dialog appears. If the data is not imported successfully, a popup error message appears. The error message will indicate the likely cause of the import to fail.

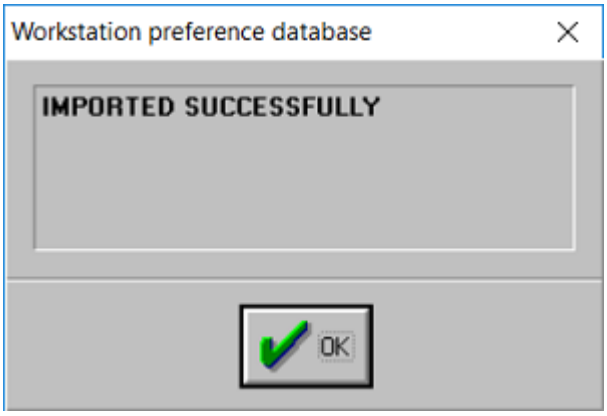


Figure 10.44: Workstation preference successfully imported dialog

10.6.2 Network socket status

This dialog shows diagnostic information for the selected TCP/IP socket.

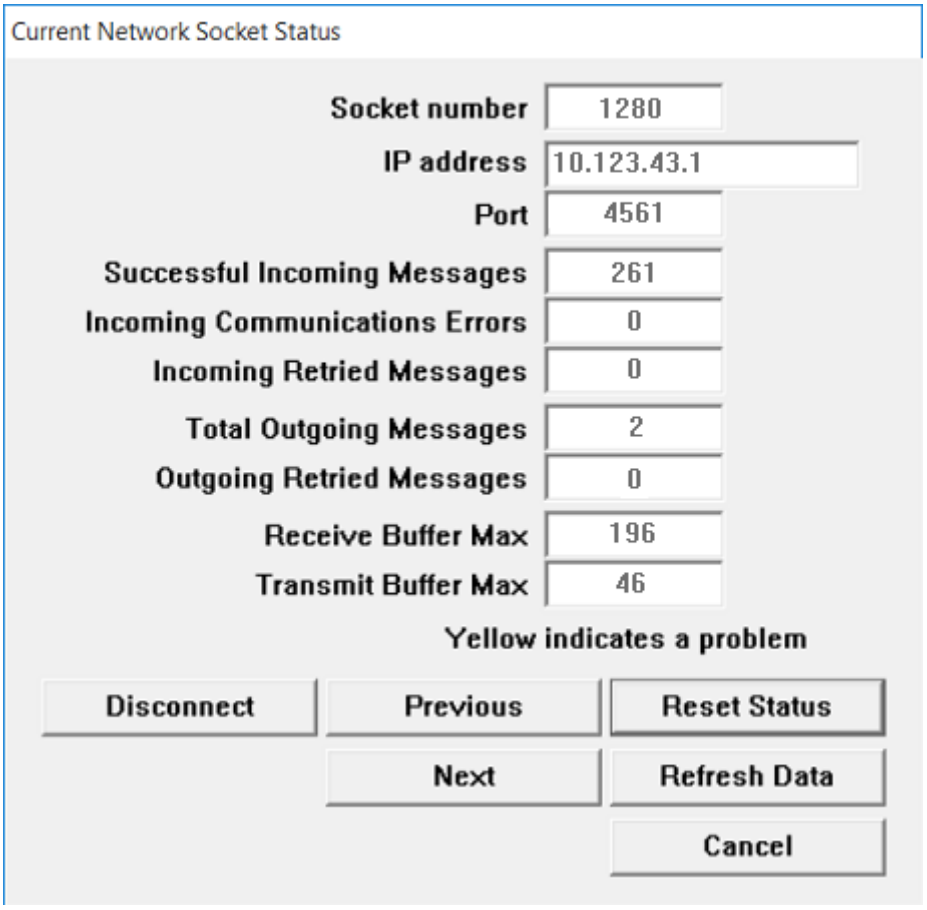


Figure 10.45: Network socket status dialog

Element	Usage/Description
Socket number	Socket number of the SE Central Console software communication port.
IP address	IP address of the SE Central Console software.

Element	Usage/Description
Port	Port number of the SE Central Console software, for communication with the SE system.
Successful Incoming Messages	Number of messages that the system has successfully received on this socket.
Incoming Communication Errors	Number of messages that the system detected errors in, on this socket. If displayed in yellow, this value is more than 1.5% of the **Successful Incoming Messages**.
Incoming Retried Messages	Number of successful receptions which indicated that the retries by the sending application. If displayed in yellow, this value is more than 1.5% of the **Successful Incoming Messages**.
Total Outgoing Messages	Total number of outgoing messages that were sent on this socket.
Outgoing Retried Messages	Number of outgoing messages that were retried because the receiving application did not acknowledge them. If displayed in yellow, this value is more than 1.5% of the **Total Outgoing Messages**.
Receive Buffer Max	Maximum number of bytes that were received on this serial port, but not yet processed by the system. If displayed in yellow, more than 50% of the queue was in use.
Transmit Buffer Max	Maximum number of bytes that were processed by the system, but not yet transmitted on this socket. If displayed in yellow, more than 50% of the queue was in use.
[Disconnect]	Click this button to disconnect the socket connection between this computer and the connected computer. The **IP address** will show as "Not connected" status, while the **Port** will show as "None". This also stops the increment of the displayed messages and buffer counts. Close and restart the SE Central Console software to restore the connection.
[Previous]	Click this button to display information of the previous socket connection.
[Next]	Click this button to display information of the next socket connection.
[Reset Status]	Click this button to reset all values shown in this dialog.
[Refresh Data]	Click this button to refresh all values shown in this dialog. The values are not automatically updated when the dialog is left open.
[Cancel]	Click this button to close the dialog window.

10.7 About menu

The **About** menu provides detailed information about the performance of the Central Console computer, and options to simulate various demo use cases (not applicable in a live system).

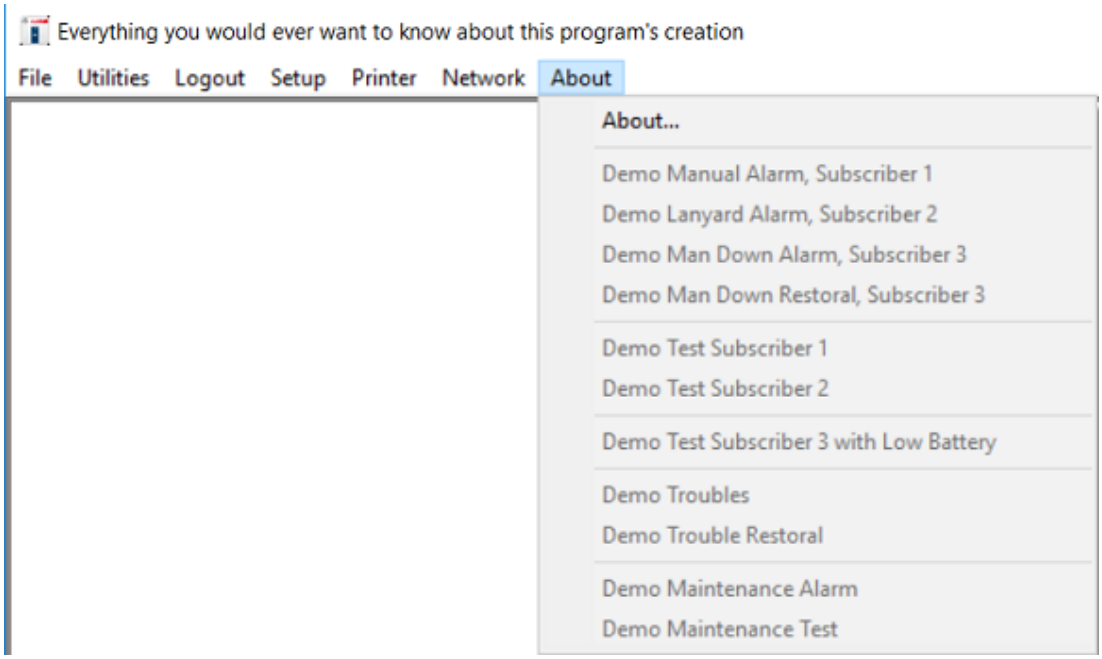


Figure 10.46: About menu

10.7.1 About

The **About** dialog presents the version information, copyright data, internal processing timers, and other system limit information.

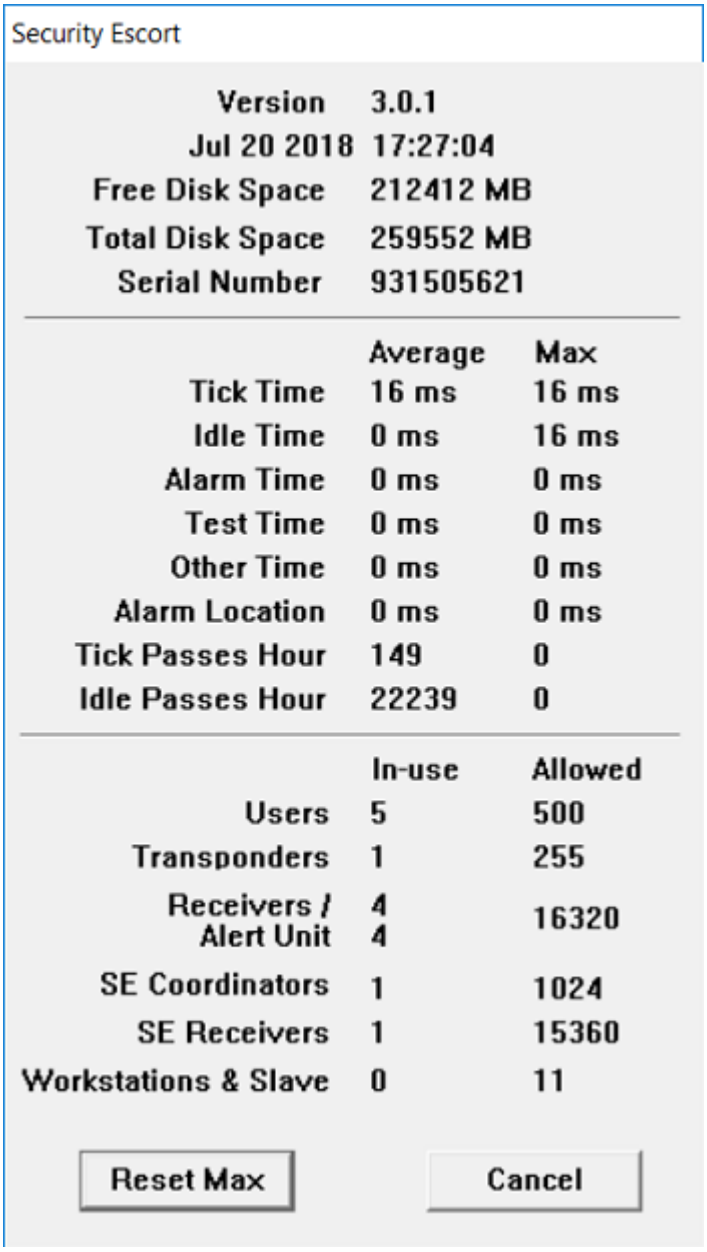


Figure 10.47: About dialog

Element	Usage/Description
Version	At the top of the dialog, the software version and the date and time that it was compiled, is displayed.
Free Disk Space	This shows the free disk space on the “C” drive of this computer.
Total Disk Space	This shows the total disk space on the “C” drive of this computer.
Serial number	Displays the serial number of this Security Escort system installation as read from the software key.
Tick Time	The amount of time spent in the time tick processor per pass.
Idle Time	The amount of time spent In the idle time processor per pass.

Element	Usage/Description
Alarm Time	The amount of time spent to process each alarm report from an SE coordinator.
Test Time	The amount of time spent to process each test report from an SE coordinator.
Other Time	The amount of time spent to process each trouble and other message reports from an SE coordinator.
Alarm Location	The amount of time spent to compute an alarm location.
Tick Passes Hour	The number of passes through the tick time processor that occurred in an hour.
Idle Passes Hour	The number of passes through the idle time processor that occurred in an hour.
Users	Displays the in-use and allowed number of subscribers that this Security Escort system installation allows. The maximum number is programmed into the software key.
Transponders	Displays the in-use and allowed number of transponders that this Security Escort System installation allows. The maximum number is programmed into the software key.
Receivers	Displays the in-use and allowed number of receivers that this Security Escort System installation allows. The maximum number is programmed into the software key.
Alert Unit	Displays the in-use and allowed number of alert units that this Security Escort System installation allows. The maximum number is programmed into the software key.
SE coordinators	Displays the in-use and allowed number of SE coordinators that this Security Escort System installation allows. The maximum number is programmed into the software key.
SE receivers	Displays the in-use and allowed number of SE receivers that this Security Escort System installation allows. The maximum number is programmed into the software key.
Workstations	Displays the in-use and allowed number of workstations that this Security Escort System installation allows.
[Reset Max]	Click this button to reset all of the max timers.
[Cancel]	Click this button to close the dialog window.

10.7.2 Demo options

There is a number of demo options to simulate various alarm and test scenarios. However, these options are greyed out and unavailable in a live system. They are only available in the demo version of the Security Escort.

Element	Usage/Description
Demo manual alarm, subscriber 1	For demonstration only, and can't be used in a live system. It causes system to display an alarm from the subscriber with transmitter ID number 1. In the **System Preferences** dialog, select **Enable Demo Selections** checkbox to enable these demo alarm and trouble selections. The transponder communication ports and network communication ports must also be disabled, and the operator of the system must login at "Installer" or "Installer Master" authority level.
Demo lanyard alarm, subscriber 2	For demonstration only, and can't be used in a live system. It causes system to display a lanyard alarm from the subscriber with transmitter ID number 2.
Demo man down alarm, subscriber 3	For demonstration only, and can't be used in a live system. It causes system to display a man down alarm from the subscriber with transmitter ID number 3. The man down alarm is delayed by the programmed man down delay (usually 10 seconds).
Demo man down restoral, subscriber 3	For demonstration only, and can't be used in a live system. It will restore a previous man down alarm from the subscriber with transmitter ID number 2, if it has not timed out and is not being displayed.
Demo test subscriber 1	For demonstration only, and can't be used in a live system. It simulates a test from the subscriber with transmitter ID number 1.
Demo test subscriber 2	For demonstration only, and can't be used in a live system. It simulates a test from the subscriber with transmitter ID number 2.
Demo test subscriber 3 with low battery	For demonstration only, and can't be used in a live system. It simulates a test from the subscriber with transmitter ID number 3. This test also reports low battery.
Demo troubles	For demonstration only, and can't be used in a live system. It simulates troubles from a transponder. Point troubles are simulated for AC loss, tamper and no response. Transponder troubles are simulated for remote key and remote key tamper. The individual troubles can be enabled or disabled in the **Popup Trouble Filter** dialog. The trouble delay in the **Popup Trouble Filter** dialog will also affect these troubles. Therefore, for demo purposes, it should be set to 0.
Demo trouble restoral	For demonstration only, and can't be used in a live system. It simulates trouble restorals for all the troubles sent in **Demo Troubles**.
Demo maintenance alarm	For demonstration only, and can't be used in a live system. It simulates an alarm from a maintenance transmitter.
Demo maintenance test	For demonstration only, and can't be used in a live system. It simulates a test from a maintenance transmitter.

11 Files required for Security Escort

The following files must be in the same directory as ESC32.EXE (default “C:\ESCORT”).

Files	Description
Esc32.exe	the main program
Bwcc32.dll	support for the dialog appearance
Cdrvdl32.dll	communications support
Cdrvhf32.dll	communications support
Cdrvxf32.dll	communications support
Commsc32.dll	communications support
W32mkde.exe	the database manager
W32mkrc.dll	support for the database manager
Wbtrcall.dll	support for the database manager
Wbtrv32.dll	support for the database manager
Lfbmp70n.dll	support for the screen images
Lfcmp70n.dll	support for the screen images
Ltkrn70n.dll	support for the screen images
Ltfil70n.dll	support for the screen images

The following files are preferences for this workstation and stored in the same directory as ESC32.EXE.

Files	Description
Wprefers.edb	the workstation preferences settings
Prefersc.edb	Old system preferences settings. This file is converted to gprefers.edb and wprefers.edb, and then is automatically deleted.

The map of the facility is a standard Windows bitmap (BMP) file. It must be stored in the same directory as ESC32.EXE.

Files	Description
MAP0.EDB	Main map bitmap file.
MAP1.EDB	Extra map bitmap file if used.
MAP2.EDB	Extra map bitmap file if used.

The following files are the system databases that are stored at the Master Database path (duplicate copy in the Slave Database Path).

Files	Description
Operator.edb	System Operators Database
Reports.edb	Alarm Reports database
Subscrib.edb	Database of the Subscribers/ Transmitters
Transpon.edb	Database of the System Configuration
Gprefers.edb	Global system preferences settingss

The following sound files should be in the Windows\media directory:

Files	Description
SEtroubl.wav	trouble sound
SEalarm.wav	alarm sound

These are sample images for demo and test. The following files should be in the IMAGES directory, which is a sub-directory to the ESC32.EXE directory (default “C:\ESCORT\IMAGES”)

Files	Description
Image1.jpg	sample subscriber image
Image2.jpg	sample subscriber image
Image3.jpg	sample subscriber image

Index

Symbols

A

B

C

N

O

P

R

S

T

Bosch Security Systems B.V.
Torenallee 49
5617 BA Eindhoven
Netherlands
www.boschsecurity.com

Building solutions for a better life.

202203221022