Security Escort

SE2000 Series

en Operation Manual

Table of contents

1	**Copyright and warranty**	**5**
1.1	Trademarks	5
1.2	Software license agreement	5
1.3	Limited warranty	5
1.4	Remedy	5
2	**About this manual**	**7**
3	**The components**	**8**
3.1	Transmitter	8
3.2	Receiver	8
3.3	Alert unit	9
3.4	Transponder	9
3.5	Central Console	9
4	**Daily operations**	**10**
4.1	Normal (no alarm) operations	10
4.2	Test icons	10
4.3	Answering an alarm	11
4.3.1	Interpreting the alarm screen	11
4.3.2	Acknowledging an alarm	12
4.3.3	Silencing an alarm	12
4.3.4	Resetting the system	13
4.3.5	Handling multiple alarms	13
4.3.6	Filing an alarm report	14
5	**Database management**	**15**
5.1	Operator Database	18
5.1.1	Edit Operator Database record	19
5.1.2	Authority levels	19
5.2	Subscriber Database	20
5.2.1	Print Subscriber Database	21
5.2.2	Edit Subscriber Database record	22
5.2.3	Additional subscriber information	26
5.3	Transmitter Change	26
5.4	Reports Database	29
5.4.1	Statistics	29
5.4.2	Map	30
5.4.3	Edit Data	30
5.4.4	Delete	31
5.4.5	Locate Key	31
5.4.6	Key Select	32
5.4.7	Incomplete	32
6	**The online tools**	**33**
6.1	File menu	33
6.2	Utilities menu	33
6.2.1	Backup dialog	34
6.2.2	Restore dialog	36
6.2.3	Security Preferences	38
6.2.4	System Defaults	43
6.2.5	System Labels	43
6.2.6	Print/Export System Reports	43

6.2.7	Export Alarm Reports	45
6.2.8	Schedules	46
6.2.9	Alarm Groups	46
6.2.10	Alarm Group State	46
6.2.11	Current Check-in Status	46
6.2.12	Clear screen	47
6.2.13	Output verification	47
6.2.14	Synchronize system time	47
6.3	Logout menu	47
6.4	Setup menu	47
6.5	Printer menu	48
6.6	Network menu	49
6.7	About menu	49
7	**Troubleshooting**	**50**
7.1	Transmitters with low batteries	51
7.2	Broken or lost transmitters	51
7.3	Receiver and alert unit problems	51
7.3.1	AC loss	51
7.3.2	Low battery	51
7.3.3	Tamper	51
7.3.4	No response	51
7.3.5	Jamming	52
7.3.6	Output device error	52
7.3.7	Bad checksum	52
7.4	Transponder problems	52
7.4.1	Communications failure	52
7.4.2	AC loss	52
7.4.3	Low battery	52
7.4.4	Tamper	52
7.4.5	Bus faults	52
7.4.6	Other troubles	53
8	**Appendix: Software licenses**	**54**
8.1	Bosch software	54
8.2	Other licenses — copyright notices	54
8.3	Warranties and disclaimer of warranties	54
	Index	**55**

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

2 About this manual

The purpose of this manual is to provide information on the basic operations of the Security Escort system. With this manual, the operators or dispatchers should be able to manage the various database records (if access rights are provided), perform daily maintenance tasks (database backup, printing reports), and respond to incidents and alarms efficiently and correctly.

For other advanced tasks including configuration of system setup, please refer to the Security Escort *Technical Reference Manual.*

3 The components

This section provides a basic understanding of each of the Security Escort system components and how they interact. The system is comprised of five basic components: transmitters, receivers, transponders, alert units, and the Central Console.

3.1 Transmitter

The transmitter is a miniature radio transmitter. Refer to the transmitter *User Guide* for its operation. Each transmitter contains a unique code that identifies the subscriber. When an alarm signal has been sent, the Central Console displays the alarm in approximately two sec. and the sounders in any nearby receivers may activate, as well as the strobes and sirens on nearby alert units.
The transmitters have a second feature which is the test mode. When indoors, in sight of an interior receiver or outdoors, in sight of an alert unit, a test can be performed (refer to the transmitter's *User Guide*). If the test is successful, a small green light flashes on the interior receiver, or the strobe on an alert unit flashes briefly. There is no response at all if the test fails. If the test fails, the user should try again; if there is still no response, he or she should contact the Security Office as soon as possible (see *Troubleshooting, page 50*).

Special transmitters
In addition to the standard transmitters, there are other special purpose transmitters (security and maintenance transmitters).
The transmitters provided to security personnel are unique in the way that both tests and alarms are processed. Outwardly, security transmitters perform in the same manner as normal transmitters during testing. That is, the strobes flash on alert units and green lights flash on receivers to confirm a successful test. However, when a security transmitter is tested near a receiver, the Central Console can record the location of the officer and the time of the test. This can be used to generate a Guard Tour Report.
The security transmitters also differ in the way alarms are managed. Unlike regular transmitters, no sound is emitted from the transmitter itself, no sounders are activated on receivers, and no strobes or sirens are activated. The console in the security office displays the alarm as usual except for a yellow background and a text warning that the event is a silent alarm. This allows security personnel to call for assistance without attracting unwanted attention.
Another form of special transmitter, the maintenance transmitter, is used by the installation and service company's employees. It provides special test capabilities for diagnosing system performance. Another type of special transmitter, the point transmitter, protects assets and buildings, not people.

3.2 Receiver

The receivers are located throughout the grounds and buildings. These devices contain radio receivers to detect alarms and test transmissions from transmitters. They also contain sounders that can be activated if the receiver detected an alarm transmission and if the central console verified that it is a valid alarm. Outdoor receivers, contained in small gray weatherproof boxes, are typically mounted on the sides of buildings and on light posts. Indoor receivers are typically mounted on interior walls and are in small beige rectangular units.
The indoor devices have one red and one green light. The green light indicates a successful test of a transmitter. The red light is only on during certain system tests or during an alarm. Outdoor receivers do not have these visible lights. Outdoor, the strobe units on the alert units (see *Alert unit, page 9*) flash for successful tests.

3.3 Alert unit

These devices, mounted outdoors on the sides of buildings and on light poles contains a siren and strobe light controlled in response to commands from the Central Console. Its primary purpose is to provide visual and audible signals to create an awareness that an emergency may exist in the area. Its secondary purpose is to provide a means for subscribers to test the transmitters while outdoors. It does not receive test or alarm signals itself.

3.4 Transponder

The transponder continuously monitors the operation of a group of receivers and alert units to detect system faults (such as tampering) and to query the receivers for data in the event of an alarm or test from a transmitter. It collects and summarizes alarm and test data and relays that data to the Central Console. The transponder also commands the receivers and alert units, activating lights, sounders and sirens as appropriate. The transponder has a battery backup to maintain protection during local power outages.
The transponder is contained in a steel box approximately 30.5 cm (12 in) wide and 45.7 cm (18 in) high. It is usually mounted on a wall in the basement or in a utility closet.

3.5 Central Console

The Central Console is the control center for the Security Escort system. It consists of one to eight personal computers, one of which is an instantly available back-up (the slave computer). The system software is designed to run on the Microsoft Windows operating system and requires little or no computer literacy on the part of the dispatcher. The Central Console is usually located in the security dispatch center.
The Central Console is responsible for receiving alarm and test data from the transponders and calculating the location of the transmitter that produces the alarm or test. It also identifies the individual to whom the transmitter was issued and for alarms, presents the location and identity information on the computer screen. The Central Console contains the subscriber and operator databases used to check subscriber identity and operator passwords and authority levels.
The Central Console also monitors all transponders and reports component or system faults by displaying alert messages on the screen. The messages provide instructions for the dispatcher or key operator. All alarms and trouble messages are logged in memory and can be printed as a paper record.

4 Daily operations

4.1 Normal (no alarm) operations

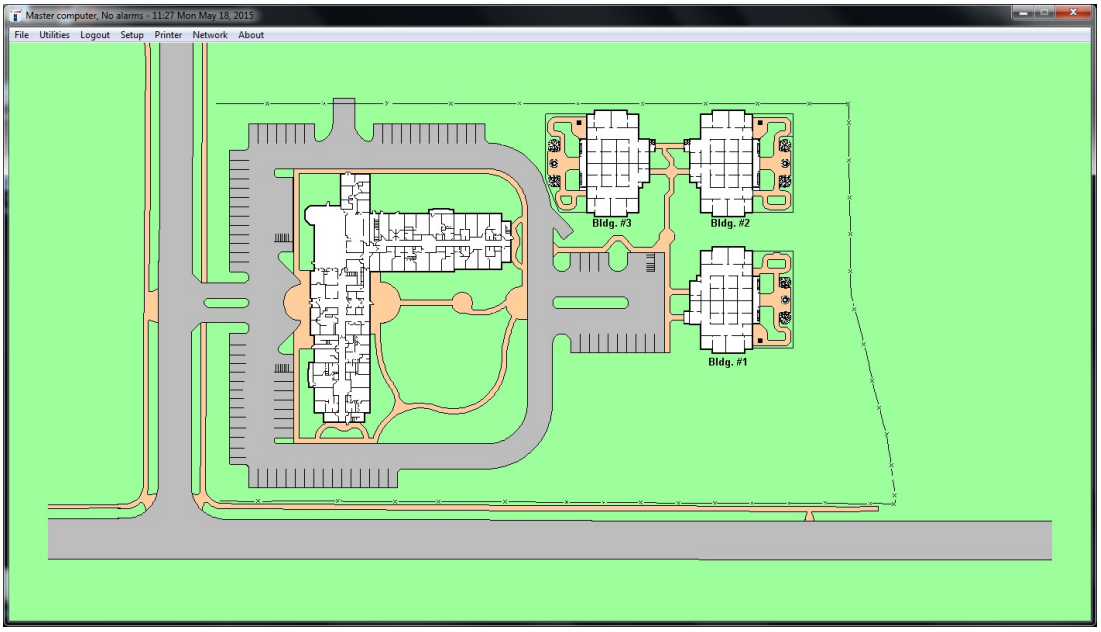


Figure 4.1: Security Escort Central Console (Normal Operations)

The figure above shows the screen of the Security Escort Central Console during normal operations, when there are no active alarms. The map is displayed and a menu bar allows access to all system functions.

Notice!
Special passwords are required to access some of the functions. At the top of the screen, the current time and date is shown along with the words “No alarms”.

The map can be scrolled to show any region of the protected area. Placing the cursor anywhere on the map and clicking the left mouse button centers that point on the screen.

4.2 Test icons

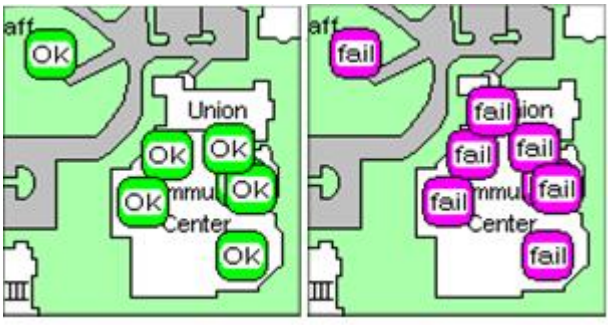


Figure 4.2: Test Icons

When a subscriber tests his or her transmitter, optional test icons are displayed on the map, indicating the location of the receivers that detected the test transmission. If the test was successful, green “OK” icons are shown, as in the figure above. If the test failed, purple “fail”

icons appear (see figure above). The fail icons appear when the transmission was produced by a transmitter that is either not in the subscriber database, or disabled (usually because it has been lost or stolen). Each new test removes the testing icons of the previous test from the map. No operator action is required.

4.3 Answering an alarm

Whenever a subscriber within the protected area activates an alarm (see the transmitter's *User Guide*) with his or her transmitter, the Security Escort Central Console:

– sounds the console alarm tone to alert the dispatcher,
– replaces the "normal operations" screen with the red alarm screen, and
– optionally prints the identity and text location information on hard copy.

This section of the manual explains in detail how an alarm situation should be handled at the Central Console.

4.3.1 Interpreting the alarm screen

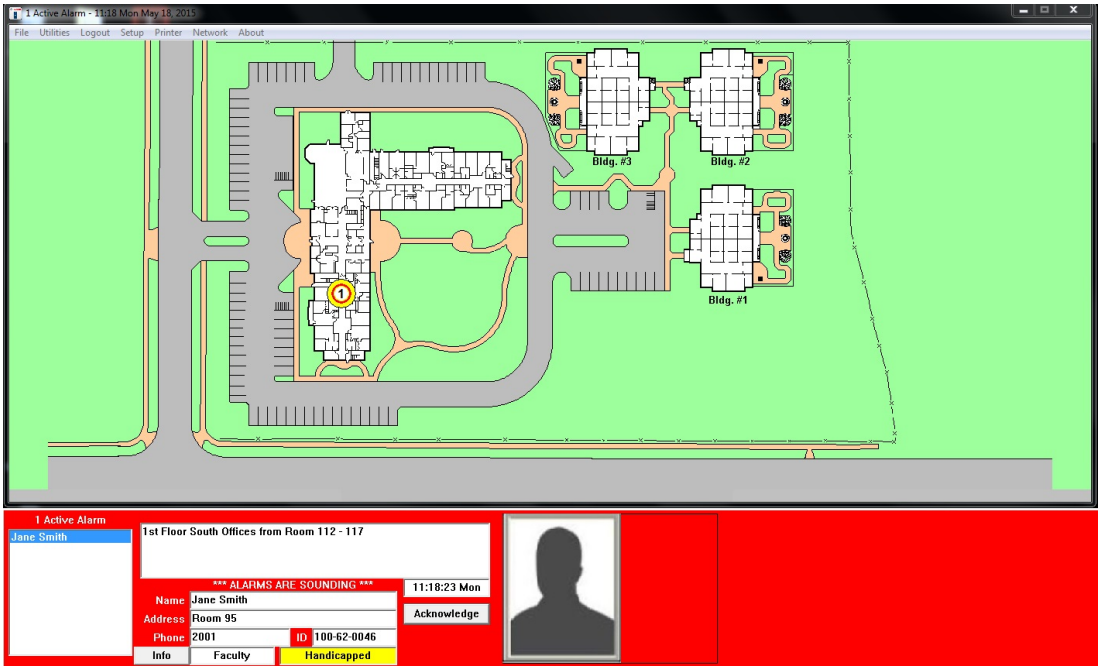


Figure 4.3: Active Alarm

The figure above shows how the screen appears immediately after the Security Escort system detects an alarm transmission. Across the top of the screen, the words "No alarms" are replaced with the words "Active Alarm". A new map appears, centered on the computed location of the alarm.
The computed location is on the first floor of the building (indicated by the numeral "1" within the icon).

Figure 4.4: Receiver Icons

The figure above shows several types of receiver icons that might appear. A bull's-eye indicates an outdoor location. Indoor locations contain a number signifying the floor. "G", "T", and "B" icons represent ground floor, tunnel and basement locations, respectively.
The yellow circle on the map indicates the subscriber's most likely location.

The red panel beneath the map displays subscriber and location information. The subscriber's name, local address, phone number, identification number and classification (such as resident, commuter, staff, and so on) are displayed. Above the subscriber information is a text box containing the location description of the alarm. Note that the subscriber's location is updated automatically due to the transmitter alarm's subsequent transmissions.
In the lower left corner of the screen, the **Active Alarm** list box displays all active alarms. In most cases, this list contains only one name, but in the case of multiple alarms, the names of each subscriber appear in this list box. In the example above, there is only one name, since only one alarm was sounded.
Just above the block of subscriber information, the words "ALARMS ARE SOUNDING" appear whenever the (optional) sirens and strobes are active. When the alarm is canceled by the dispatcher, or the alarm is automatically silenced, this message is replaced with the words, "Sounders have been silenced".

4.3.2 Acknowledging an alarm

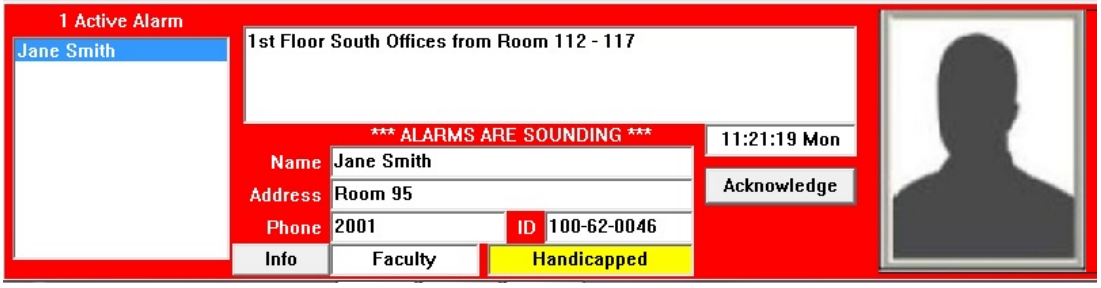


Figure 4.5: Acknowledging an Alarm

The Central Console continues to sound alert tones on its speakers until the dispatcher acknowledges the alarm. To silence the alert tones, click the **[Acknowledge]** button in the lower right corner of the alarm screen. Alternatively, press the <A> key.

Notice!
This only silences the Central Console speakers. The (optional) sirens and strobes of the alert units and the sounders in the receivers will continue to be active.

4.3.3 Silencing an alarm

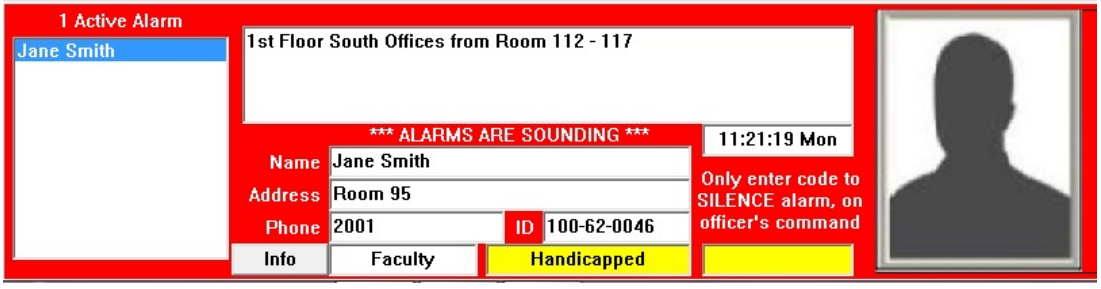


Figure 4.6: Silencing an Alarm

To cancel the alarm, and silence the sounders and strobes, the operator enters a password in the yellow text box in the lower right corner of the screen), and presses the <Enter> key. The message "ALARMS ARE SOUNDING" is replaced with the message, "Sounders have been silenced". The yellow password text box is replaced with a **[Reset]** button.

Warning!
In most installations, department policy prohibits a dispatcher from silencing an alarm until instructed to do so by a Security Officer who has visited the scene.

4.3.4 Resetting the system

Figure 4.7: Resetting the System

Even when the alarm is silenced, the alarm screen remains on the display until the system is reset. To reset the system, click the **[Reset]** button. Alternatively, press the <R> key. This replaces the alarm screen with the normal operation screen.

4.3.5 Handling multiple alarms

Figure 4.8: Multiple Alarms

When two or more alarms are active, each alarm is handled as a separate event by the system, and can be viewed individually. The name of each subscriber who transmitted an alarm is listed in the **Active Alarm** list box. One name can be selected at a time by clicking on the name in the **Active Alarm** list box to highlight it. The information displayed in the alarm screen then applies only to the highlighted subscriber. To display the alarm information of another subscriber with an active alarm, click on that subscriber's name in the **Active Alarm** list box, or use the up and down arrow keys on the keyboard to select the desired subscriber. Each alarm must be acknowledged and silenced separately.

4.3.6 Filing an alarm report

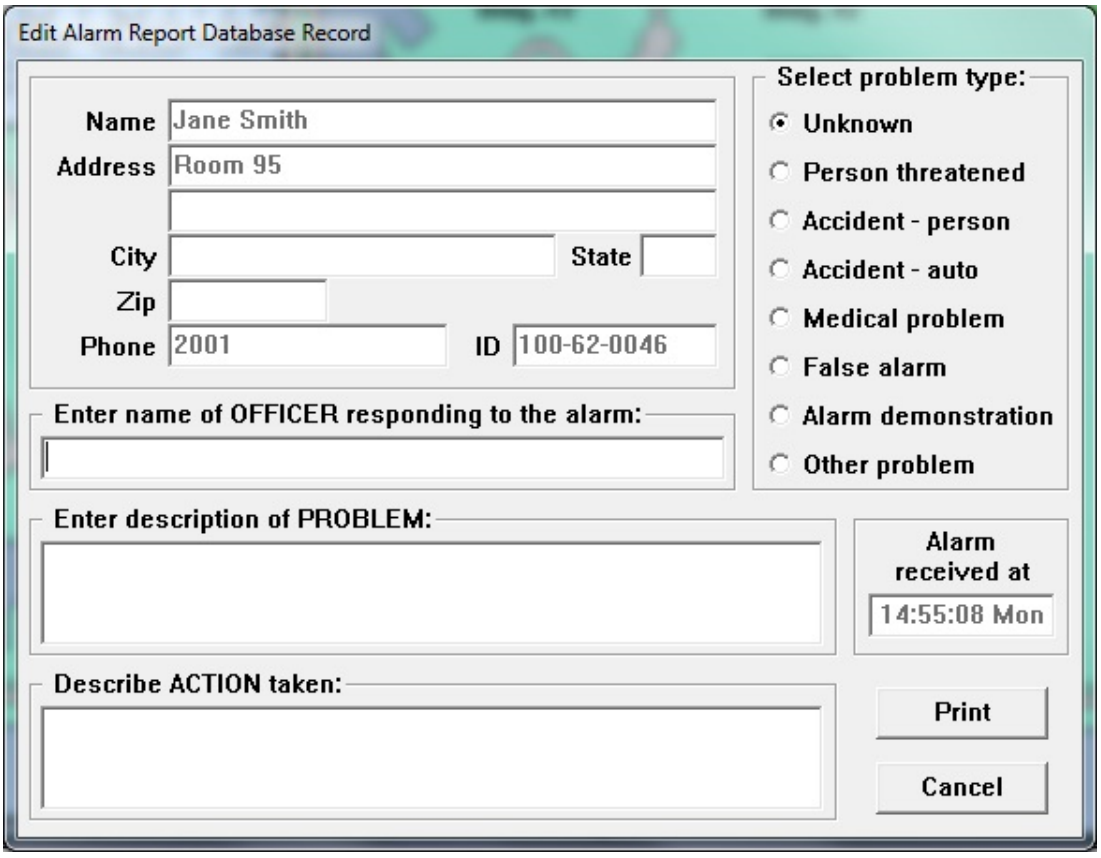


Figure 4.9: Example of Alarm Report

If the optional alarm report was selected during the setup of the Security Escort system, an officer is prompted to enter an alarm report after the alarm was reset. The Central Console software displays the above dialog window for the officer to fill in details of his or her response to the alarm. All of the subscriber identity and location information is automatically entered into the report, along with the dates and times. The responding officer only needs to enter information on the type of problem, a description of the problem specifics, and the action taken. Clicking the **[Cancel]** button completes the report.
If there is a need to modify the report after it is saved, the report can be recalled from the **Report Database** found under the **File** menu. A description of how to edit an existing report is explained in *Database management, page 15*. If it is inconvenient to fill out the alarm report immediately after the alarm is reset, it can be deferred to a later time. Near the end of the work shift, the Central Console can produce a prompt if an alarm was received but no report was entered into the computer.

5 Database management

The Security Escort software contains several distinct databases:

- The **Subscriber Database** contains names, addresses, identification numbers, and other information about the users of the system.
- The **Operator Database** contains information on the Security Officers, including the passwords assigned and the authority level granted.
- The **Reports Database** contains all of the alarm reports created by the system and completed by the officers.
- The **Transponder Database** contains information on the system hardware configuration and on testing data taken by Security Escort service personnel. Access to these databases is only available to installation and service company employees.

These databases are accessed from the **File** menu. The three databases operate very similarly. Each subscriber, operator, and report entry contained in its respective database is called a record. The common commands of the databases are described first, before focusing on each specific database.

The records in the **Subscriber** and **Operator Databases** can be sorted by name, identification number, transmitter identification number, time of last test, or time of low battery report, by using the **[Key Select]** or **[Locate Key]** buttons to select the method of sorting and searching. Additionally, the records in the **Reports Database** can be sorted by alarm time, problem type, and subscriber classification.

Common commands

Most of the commands are common to the various databases. As an example, the following **Subscriber Database** dialog window is typical.

Notice!

Any individual operator's access to the databases is controlled by authority level settings in the **Operator Database**. The manager of the Security department usually controls these access settings through a high level password.

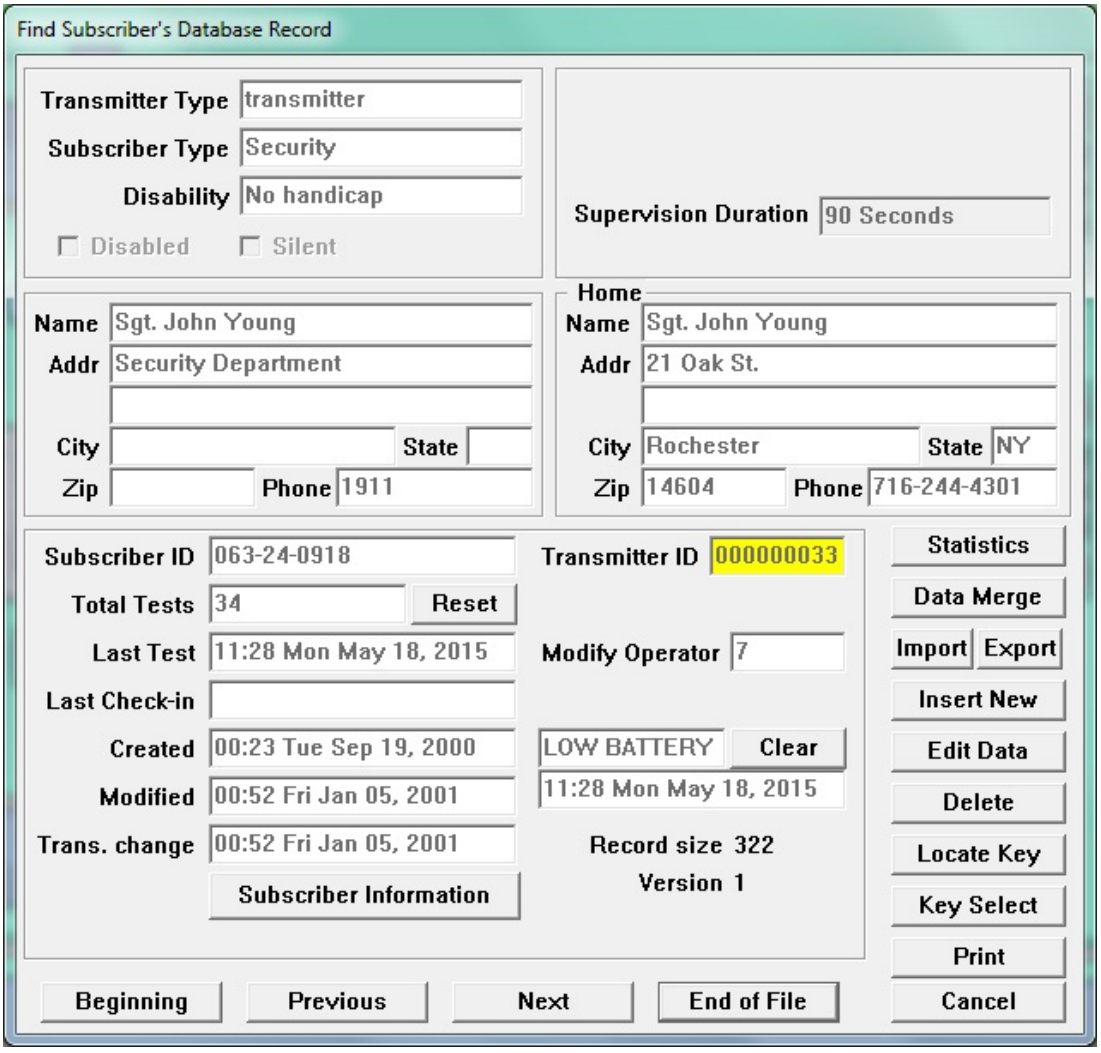


Figure 5.1: Find Subscriber's Database Record

The four buttons across the bottom of the window allow the operator to step through the individual records of the database.

[Beginning]/[End of File] — **[Beginning]** and **[End of File]** buttons call up the first or last record in the database respectively.

[Previous]/[Next] — These two buttons allow you to scroll through the records in the database one record at a time. These can be useful when searching for a name without knowing the exact spelling, or reviewing a sequence of alarm events.

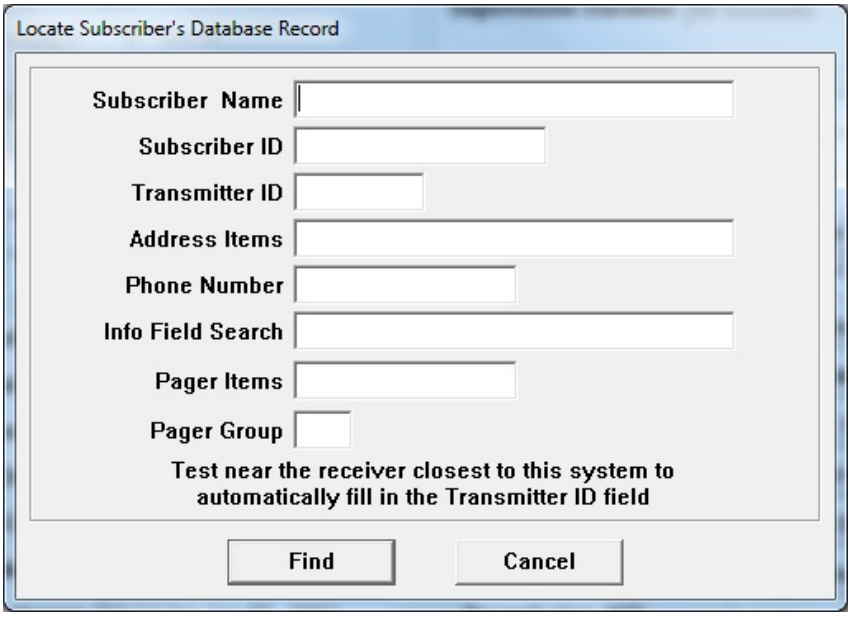
Some of the buttons on the right pane that are common across the databases include:

[Insert New] — Creates a new record in the database. An **Edit Subscriber Database Record** dialog opens, for entry of the appropriate information into the database. Use the <Tab> key to step through the data fields in order, or click the mouse on any field to place the cursor for data entry. The specific **Edit Subscriber Database Record** options are discussed in more detail.

[Edit Data] Allows the operator to edit the information in the current displayed record. Click this button to open the appropriate **Edit Subscriber Database Record** dialog and modify the data. Clicking the **[Save]** button replaces the old information with the new. Clicking the **[Cancel]** button maintains the changes or reverts to the old information.

[Delete] Removes the currently displayed record from the database. The operator must confirm a delete decision before the record is actually deleted.

[Locate Key] Scrolling through the database using the **[Previous]** and **[Next]** buttons is not the most efficient way of locating a specific subscriber or operator. Pressing the **[Locate Key]** button from any operator data record displays the figure below. An entry in one of the blank fields, followed by left clicking on the **[Find]** button searches all records for the closest match. For example, if an operator identification number is entered, the operators are sorted by their operator identification numbers. The operator whose number most closely matches the one entered will be displayed. If a last name is entered, the operators are sorted in alphabetical order by last name, and then the operator whose last name is closest in alphabetical order is displayed. Therefore, if “P” is entered as the last name, the operators are sorted in alphabetical order by name, and then the first operator whose last name began with “P” is displayed. Clicking the **[Next]** button steps through the records in alphabetical order.
When this dialog is displayed in the subscriber’s database, testing a transmitter fills in the **Transmitter ID** field with the ID of the transmitter tested. Click the **[Find]** button to locate that transmitter’s record.



[Key Select] Choose the default setting for the order in which the data records are sorted. In the case of the **Operator Database**, the records can be ordered by last name, by authority level in ascending order, or by operator identification number in ascending order. The choice is made by placing the cursor on the small diamond to the left of the text and clicking with the left mouse button and then clicking the **Select** option.

The specific choices in the **Subscriber** and **Reports Databases** are different but the techniques for searching are the same.

[Print] When this button is clicked, the printer produces a hard copy (paper printout) of the record currently displayed.

[Cancel] This button allows the operator to exit the current dialog. If changes were made, the operator can save the changes to memory or restore the data to its previous state.

5.1 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**.

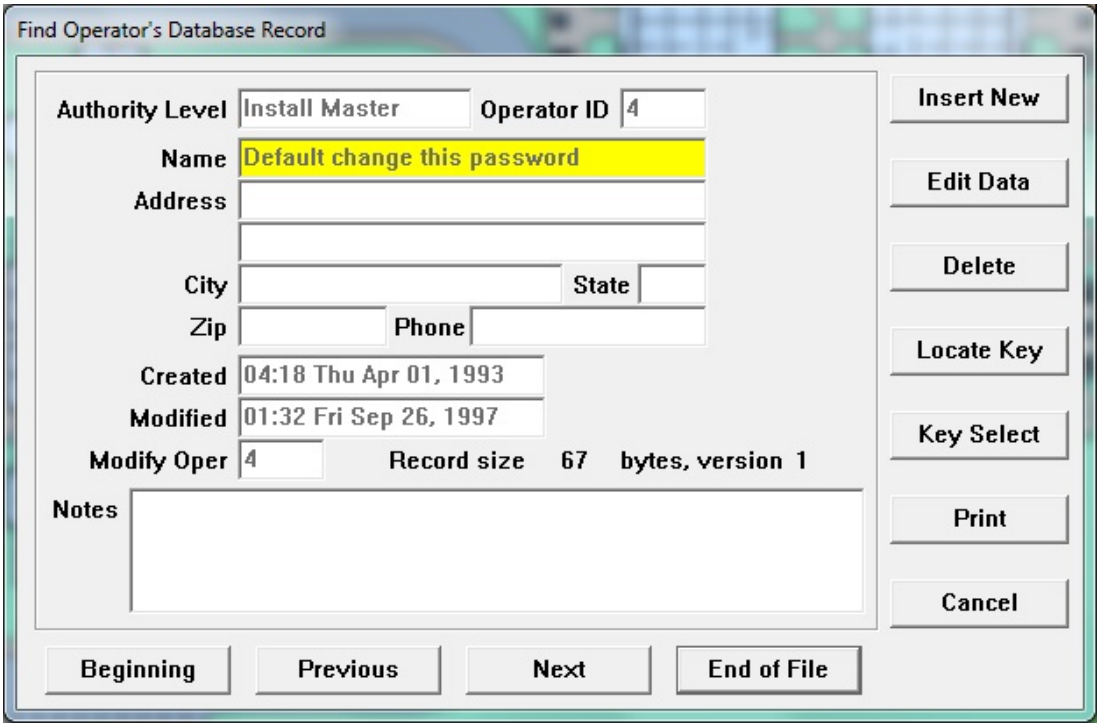


Figure 5.2: Find Operator's Database Record

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.

5.1.1 Edit Operator Database record

When adding a new operator or editing the data for an existing operator, the **Edit Operator 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 in the operator's file is optional, including the local address, local phone number, and notes.

Notice!

There are two boxes for passwords in the **Edit Operator 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.

Figure 5.3: Edit Operator's Database Record

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

5.1.2 Authority levels

An important consideration, when creating a new 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 Databases** while a dispatcher may only need access to view these databases.

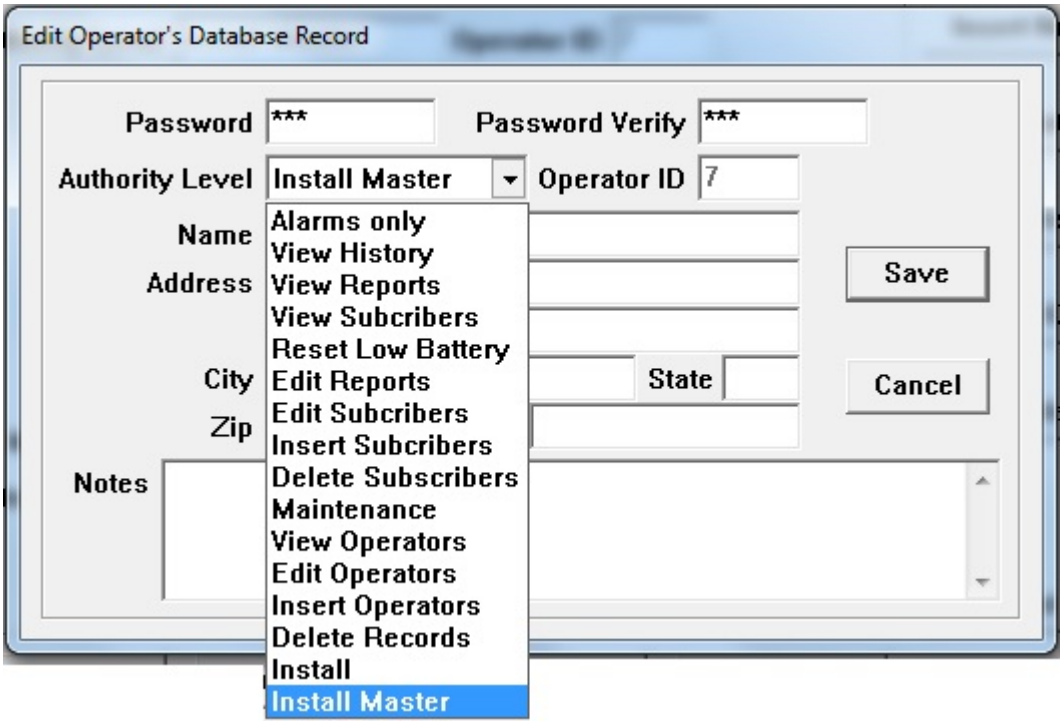


Figure 5.4: Edit Operator's Database Record

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.

5.2 Subscriber Database

A subscriber is anyone who has been issued a Security Escort 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.

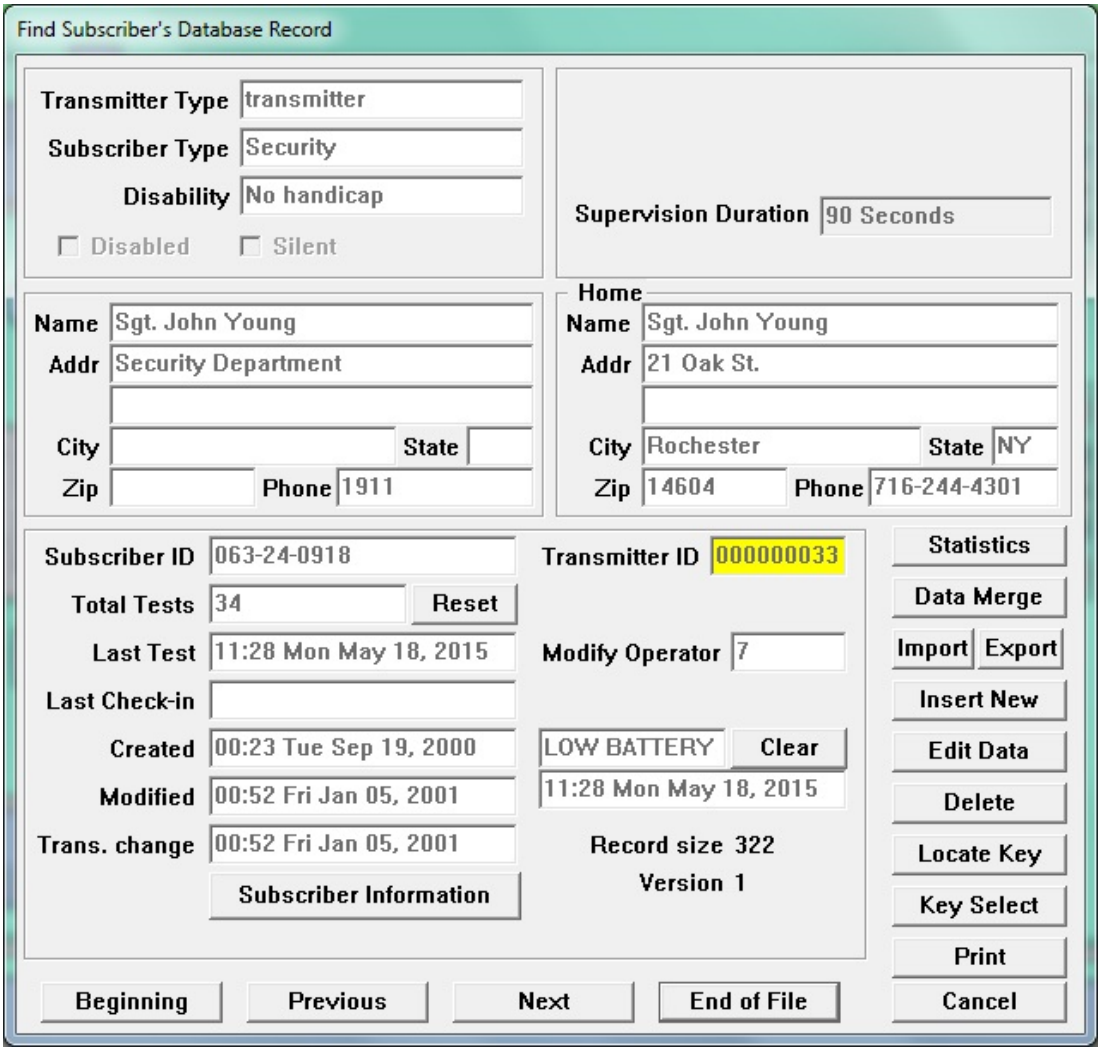


Figure 5.5: Find Subscriber's Database Record

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).

[Reset] Clicking the **[Reset]** button clears the number of **Total Tests** count.

[Clear] Clicking the **[Clear]** button removes the **Low Battery** indication. This should only be done after the transmitter battery is replaced or a new transmitter is issued.

[Print] Clicking the **[Print]** button displays the **Subscriber Print** dialog.

5.2.1 Print Subscriber Database

Clicking the **[Print]** button displays the **Subscriber Print** dialog. Select one of the indicated sort orders and the data fields that you desire in the report.

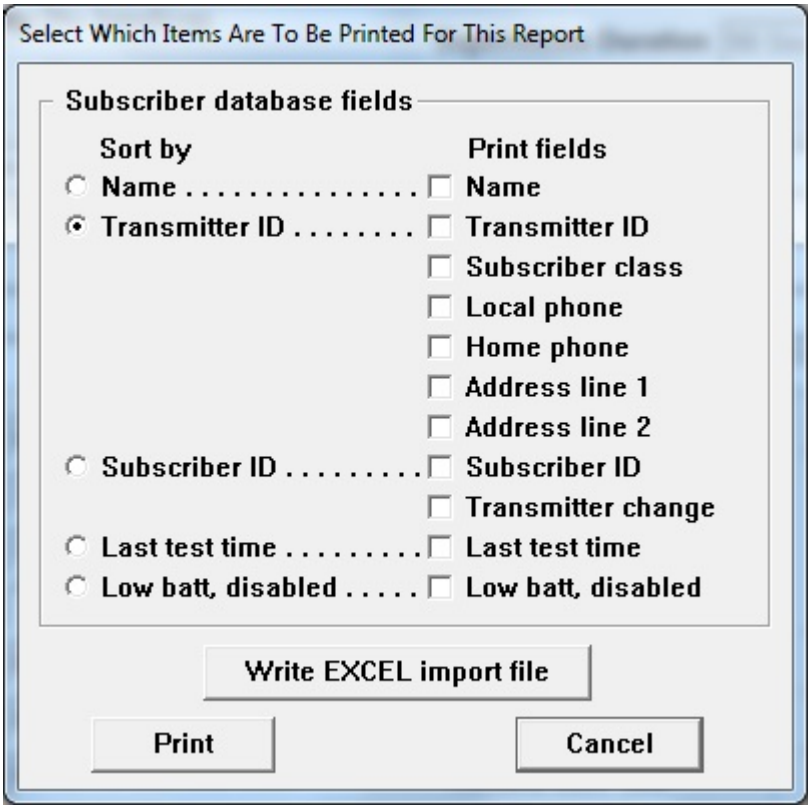


Figure 5.6: Subscriber Print Dialog

[Write EXCEL import file] Clicking the **[Write EXCEL import file]** button causes all the fields of all the records to be sent to the “subscrib.txt” file in the folder in which Security Escort was installed. This file may be directly imported into Microsoft Excel or any other application that accepts tab delimited text..

[Print] Clicking the **[Print]** button causes the selected data fields to print on the report printer in the indicated sort order.

[Cancel] Clicking the **[Cancel]** button aborts the print dialog and returns to the previous screen.

5.2.2 Edit Subscriber Database record

When editing a subscriber’s file or creating a new file, the following information must be entered to complete the file: 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.

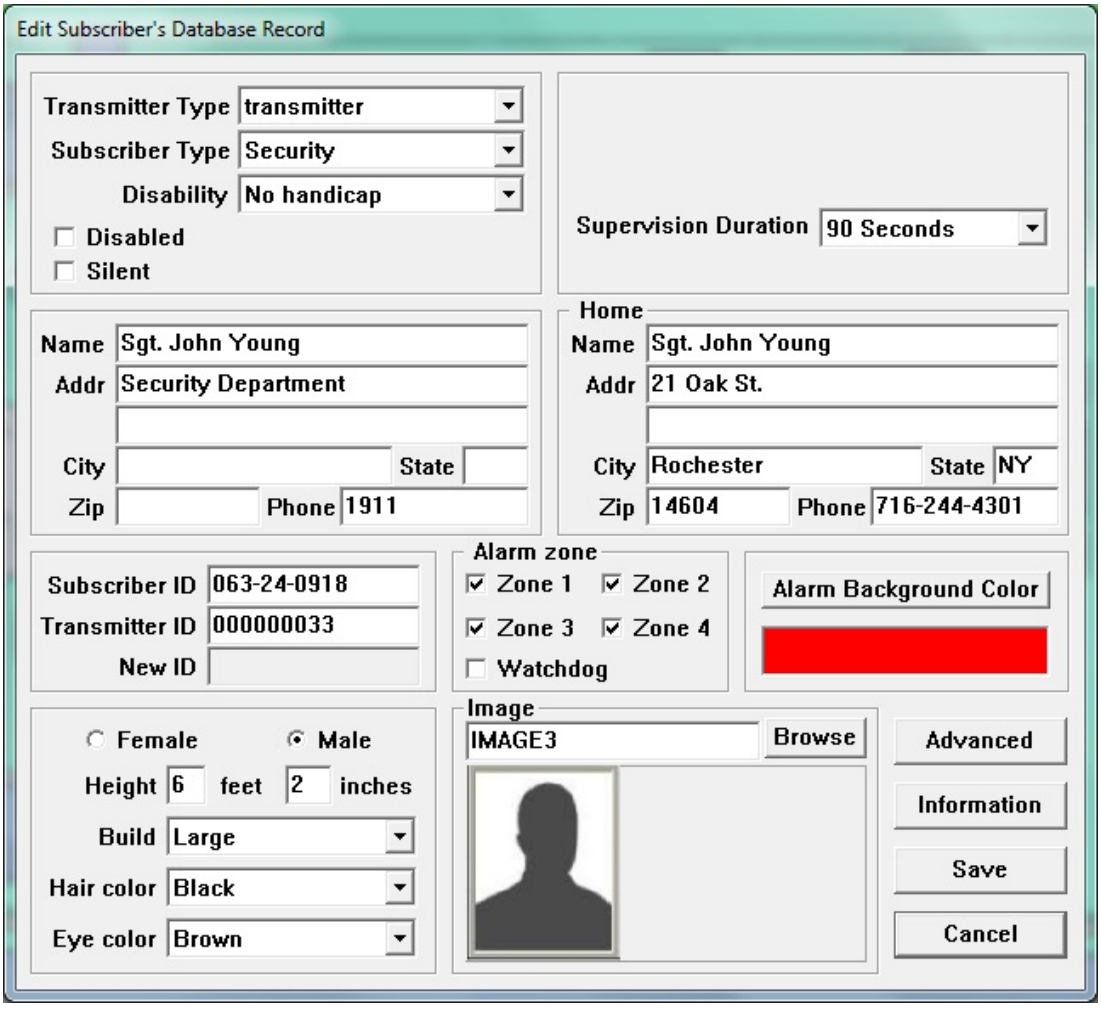


Figure 5.7: Edit Subscriber's Database Record (Transmitter)

Transmitter Type

Click the drop-down list to select the type of transmitter that is assigned to the subscriber. Currently, only the standard transmitter is supported.

Subscriber Type

Click the drop-down list 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 present 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 a approving officer.

The **Subscriber Type** available:

Acknowledgement – subscriber with acknowledgement transmitters

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	If this individual is handicapped, select an item from this drop down list. The condition is displayed on the alarm screen. If a handicap is selected, the **Notes** field will not show on the alarm screen.
Disabled	There is an option to disable 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. Disabling or enabling a subscriber is accomplished by locating the subscriber in the **Subscriber Database**, clicking on the **[Edit Data]** button, and clicking the checkbox next to **Disabled** in the upper-left corner of the dialog. If the box has a check mark, the subscriber's transmitter is ignored by the system; if it does not, the transmitter is recognized and alarms are displayed.
Silent	If checked, a system that normally sounds alarms is silent for all alarms generated by this transmitter.
Supervision Duration	Specific transmitter types periodically transmit supervisory messages so the system can monitor their function and location. The supervisory feature must be enabled in the transmitter. For transmitters with the supervisory feature enabled, select the interval for these Supervisory messages from the drop-down list. The values for the drop-down list are “None”, “10 Seconds”, “30 Seconds”, “90 Seconds” and “1 Hour”. The supervision period specific to the assigned transmitter must be selected if this feature is used.
Name	The individual or item assigned to this transmitter. This is a required field.
Address	Address of this 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 this individual or item within the protected area.
State	State of this individual or item within the protected area.
Zip	Zip code of this individual or item within the protected area.
Phone	The phone number to access this 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 typed into this field. This is a required 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 much faster and error free method is to delete any existing entry in the **Transmitter ID** field and then perform a test with the transmitter to be assigned to this subscriber. The new **Transmitter ID** displays in the **New ID** field. The new **Transmitter ID** must 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 **Transmitter ID** to the correct field.) This is a required field; it must be filled in with a unique ID. Complete the change to the Subscriber information by clicking the **[Save]** button.
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 desired background color to display for alarm when this transmitter is activated.
Female/Male **Height** **Build** **Hair color** **Eye color**	These characteristics 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. Click the **[Browse]** button to open a dialog box 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 (see the Security Escort *Technical Reference Manual*).
[Information]	The **[Information]** button is used to enter specific information about the holder of this transmitter.
[Save]	Clicking the **[Save]** button saves all changes to the database.
[Cancel]	Clicking the [**Cancel]** button allows you to abort and cancel all changes to the database. A confirmation dialog box appears asking 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.

5.2.3 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.

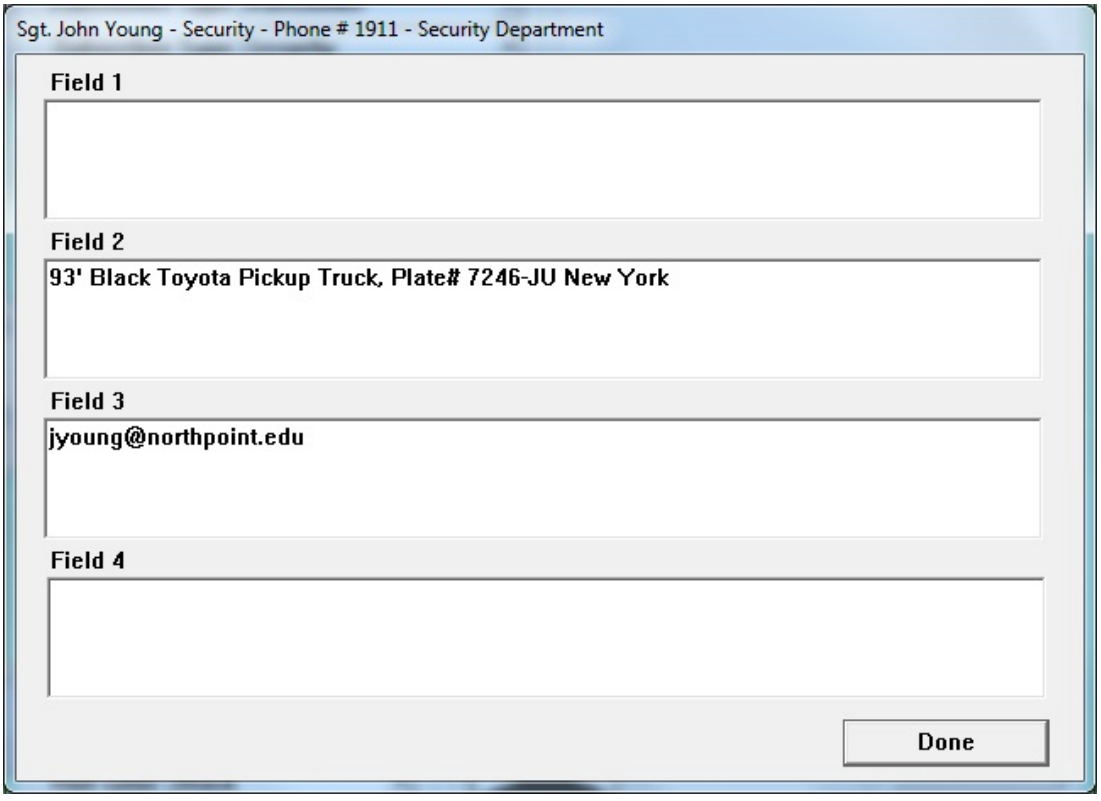


Figure 5.8: Information Entry Screen

[Done] Clicking the **[Done]** button closes the information entry dialog and returns to the **Edit Subscriber's Database Record** dialog. Clicking the **[Save]** button saves all changes to the database.

5.3 Transmitter Change

The **Transmitter Change** command 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 **Subscriber Name**, **Subscriber ID**, current **Transmitter ID**, **Address Items**, **Phone Number**, **Pager Items** or **Pager Group**. This method of locating a particular subscriber's record is identical to using the **[Locate Key]** 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 appropriate record.

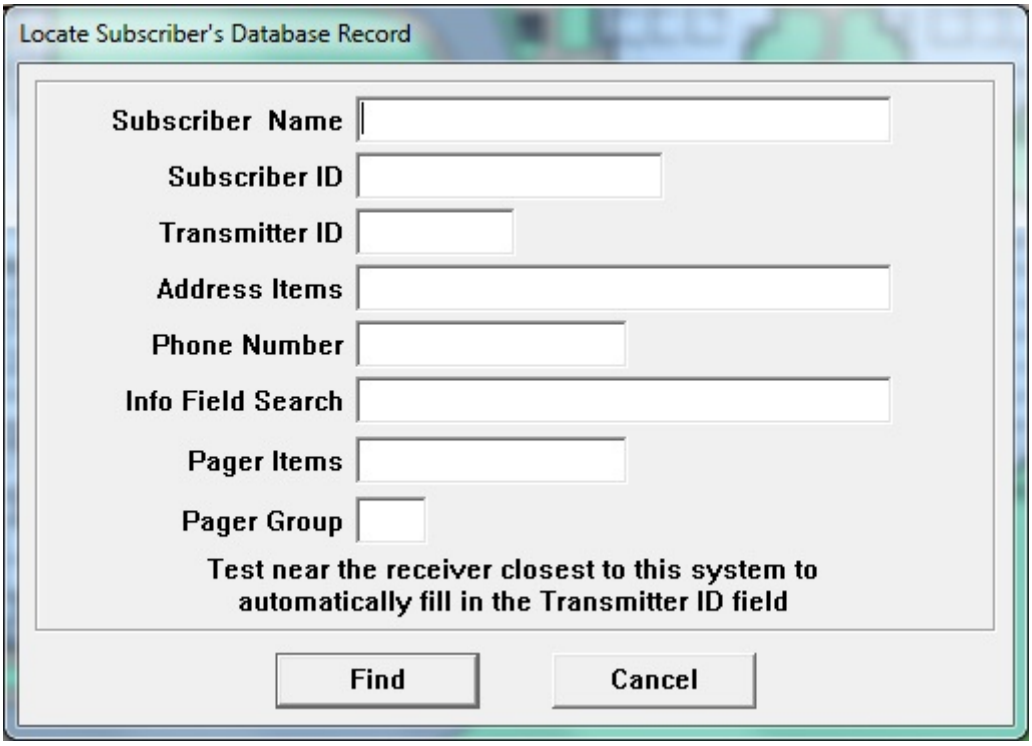


Figure 5.9: Locate Subscriber's Database Record

Perform a test using the old transmitter if possible. This should fill in the **Transmitter ID** field. Then click the **[Find]** 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.

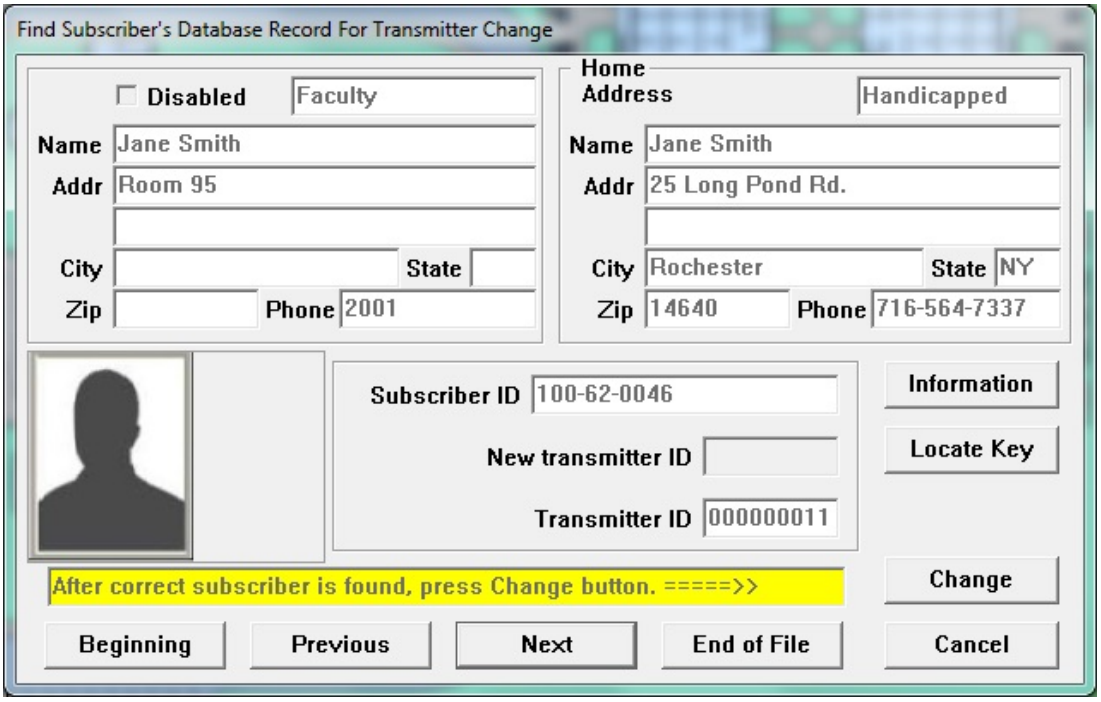


Figure 5.10: Find Subscriber's Database Record

When the correct subscriber's record is displayed, click on the **[Change]** button and perform a test using the new transmitter. The new transmitter identification code will be automatically populated into the **New transmitter ID** field.

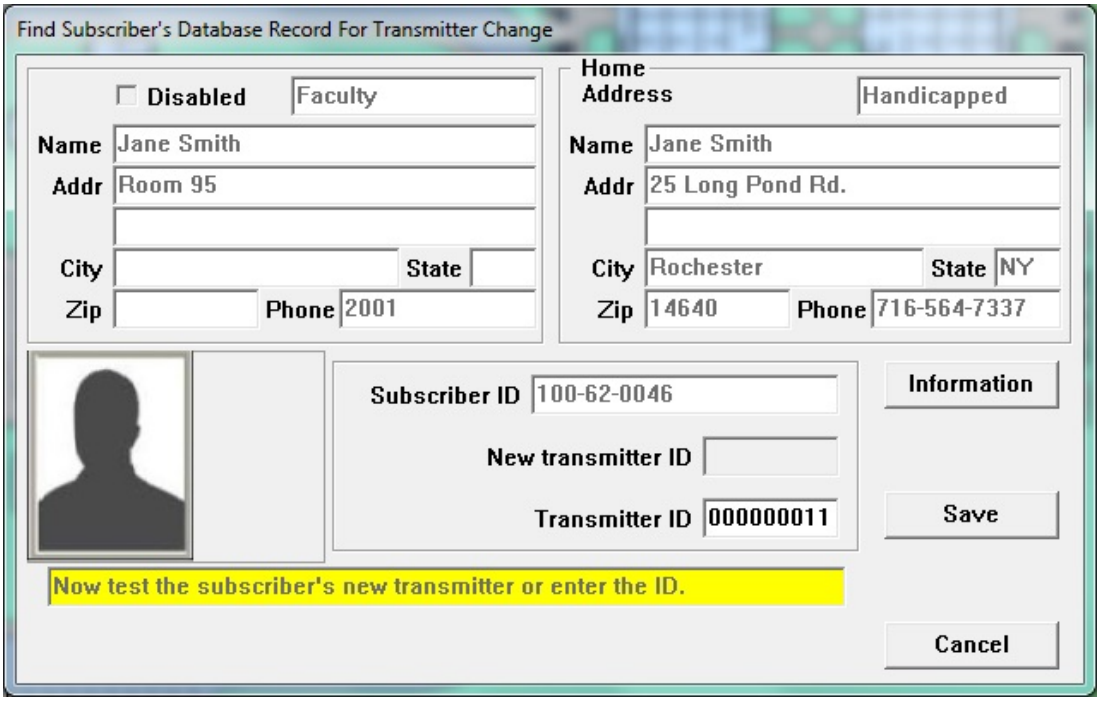


Figure 5.11: Save Subscriber's Database Record after Change of Transmitter ID

Manually enter the **New transmitter ID** into the **Transmitter ID** field 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 receiver, and this dialog should automatically disappear from the screen, confirming the change was successful.

5.4 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.

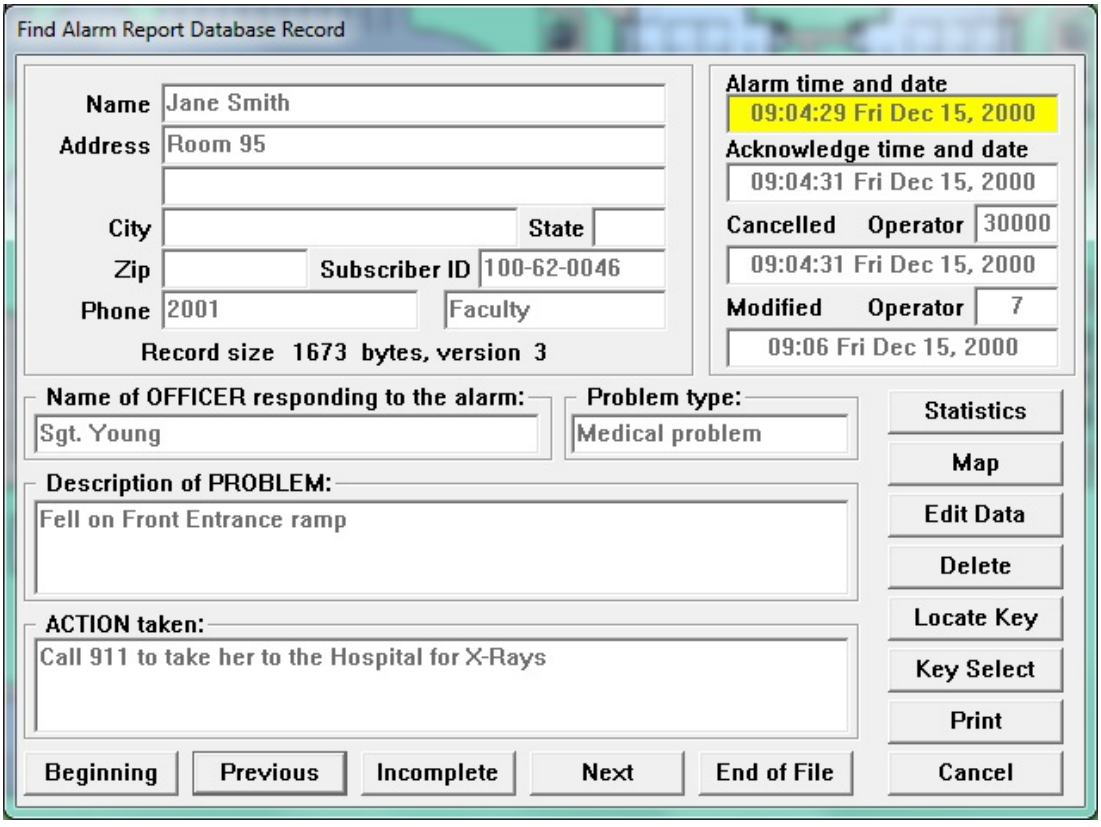


Figure 5.12: Find Alarm Report Database Record

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 **Edit 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 min. for 30 min. before the end of the shift. The time at which the prompt is to display is also set in the **Edit Security Preferences** dialog.
All of the common database commands are available in the **Reports Database**, with the following additional commands.

5.4.1 Statistics

Clicking the **[Statistics]** button summarizes 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.

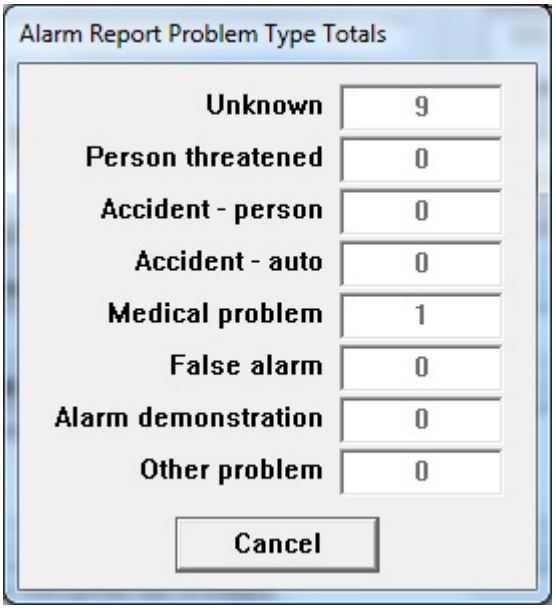


Figure 5.13: Alarm Report Statistics

5.4.2 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.

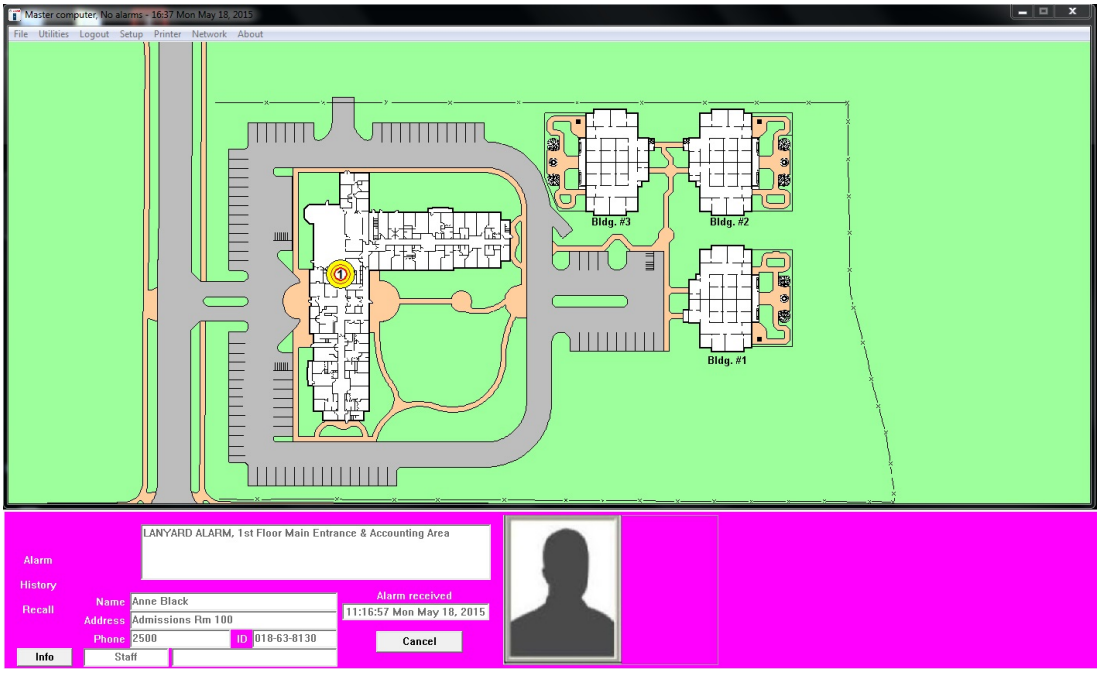


Figure 5.14: Active Alarm Map

5.4.3 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 updated record by clicking the **[Save]** button.

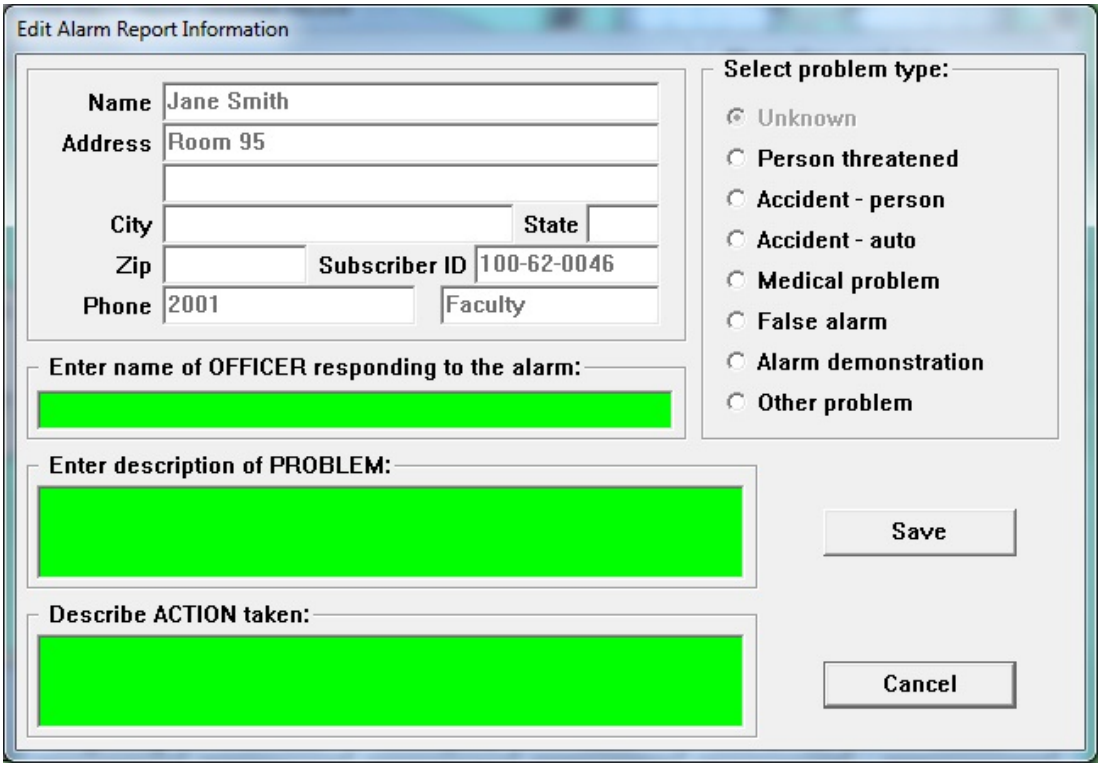


Figure 5.15: Edit Alarm Report Information

5.4.4 Delete

This button deletes the alarm report from the database. If the report is deleted, the data can not be recovered.

5.4.5 Locate Key

This button works similarly to the **[Locate Key]** 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.

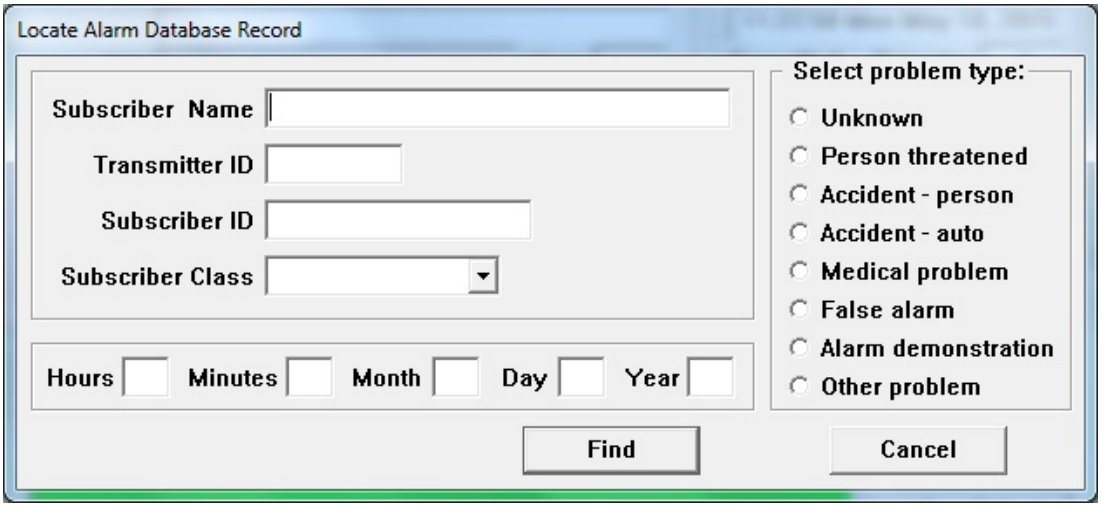


Figure 5.16: Locate Alarm Database Record

As in the **Operator** and **Subscriber Database**, the subscriber records are temporarily ordered according to the field entered in the **Locate Key** dialog.

5.4.6 Key Select

This button also works similarly to its counterparts in the **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 5.17: Select Database Key

5.4.7 Incomplete

When this button is clicked, the most recent incident report file that has not been completed will be displayed. The reports are not reordered when this command is used.

6 The online tools

This section of the manual contains a description of the online tools available in the system software. Access to these tools varies according to the authority level of the user, as assigned in the **Operator Database** for each operator. When an operator enters his or her password in the **Password** dialog box, the system software provides access to the authorized menu functions for that individual. Any activities subsequently performed on the system are then associated with that operator in the system history files, until the operator logs out by selecting **Logout** from the main menu.

6.1 File menu

This pull-down menu leads to the main databases for the system. The **Operator**, **Reports**, and **Subscriber Databases** and **Transmitter Change** have been described already. The **Locate Transmitters**, **Maintenance Alarm Database**, and **Transponder Database** are solely for use by installation and maintenance personnel and are described in the Security Escort *Technical Reference Manual*. Key operators with the appropriate authority levels can view and modify the operator, alarm report, and subscriber databases.

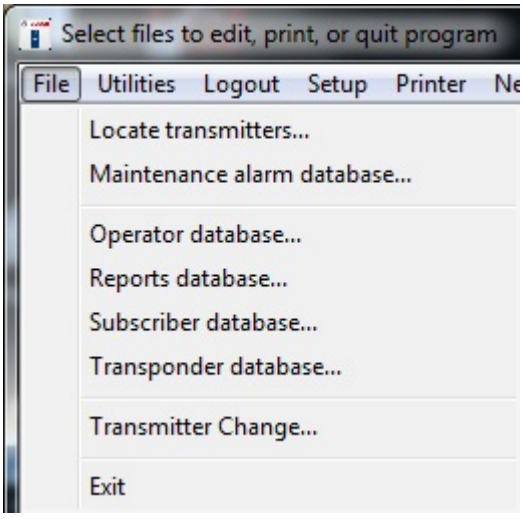


Figure 6.1: File Menu

6.2 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, and clear the map screen.

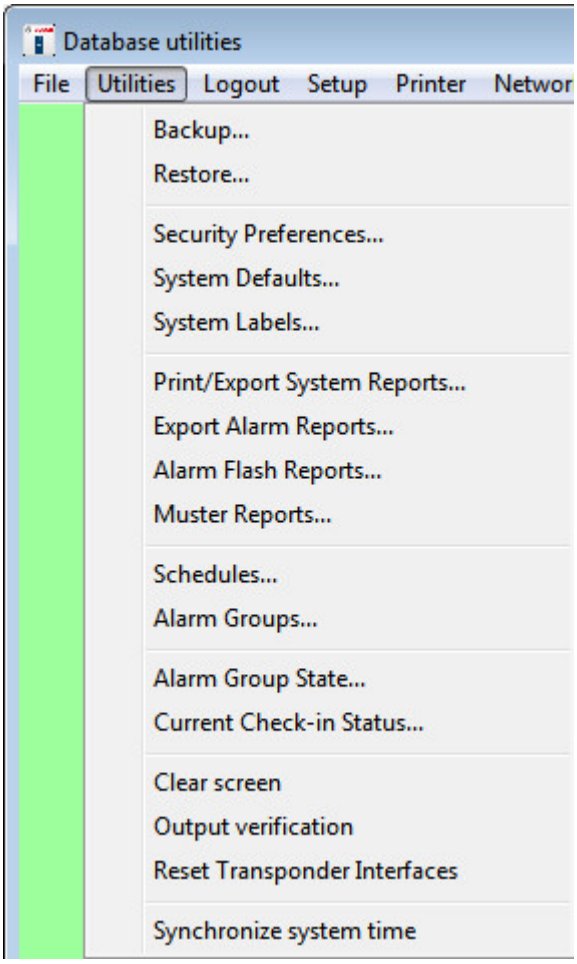


Figure 6.2: Utilities Menu

6.2.1 Backup dialog

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** command. 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.

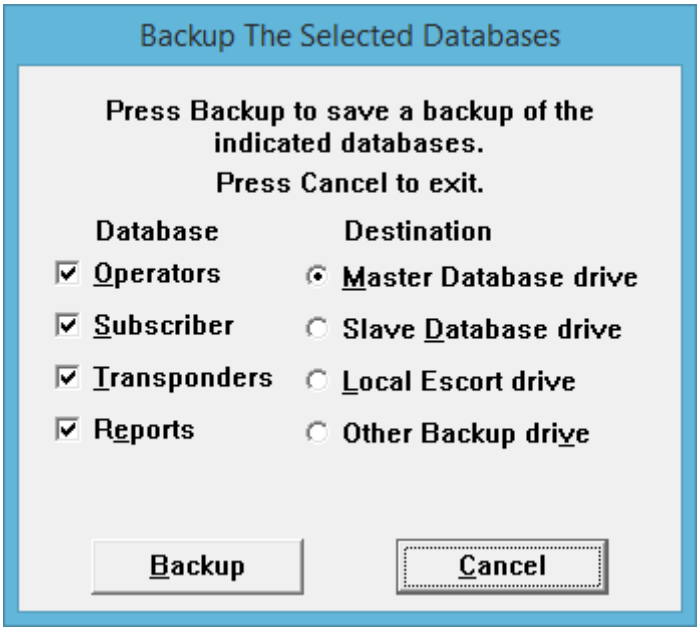


Figure 6.3: Backup Dialog

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 with a checkmark will be backed up. Typically all databases should be backed up at 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).

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 transponders, receivers, virtual receivers and alert units.
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.
Local Escort drive	Store the backup files in the save sub-directory as 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]	When the **[Backup]** button is clicked, all databases selected with a checkmark will be saved to the destination selected on the right.

6.2.2 Restore dialog

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.

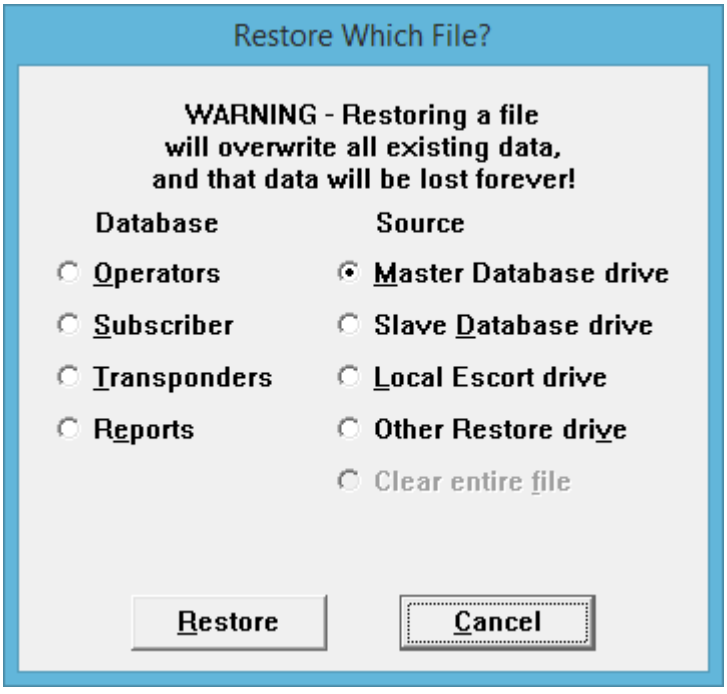


Figure 6.4: Restore Dialog

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.

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 transponders, receivers, virtual receivers and alert units.
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 save sub-directory as the Security Escort System components are stored on this computer (typically “C:\ESCORT”).

Other Restore drive

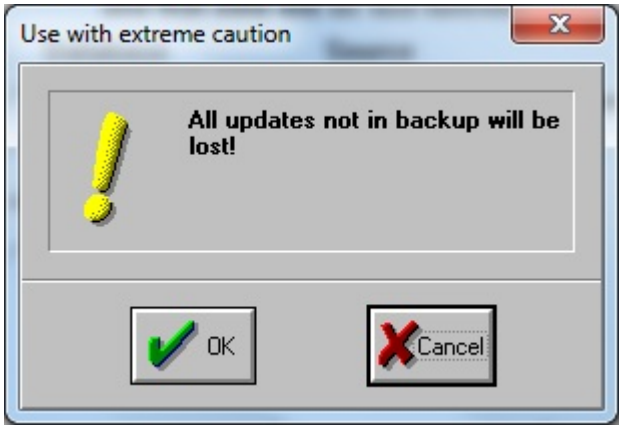
Restore the backup files in the **Other Backup/Restore path** assigned in the **System Directories and Network Address** dialog. This path may point to a local path, external drive, or network disk drive.

Clear entire file

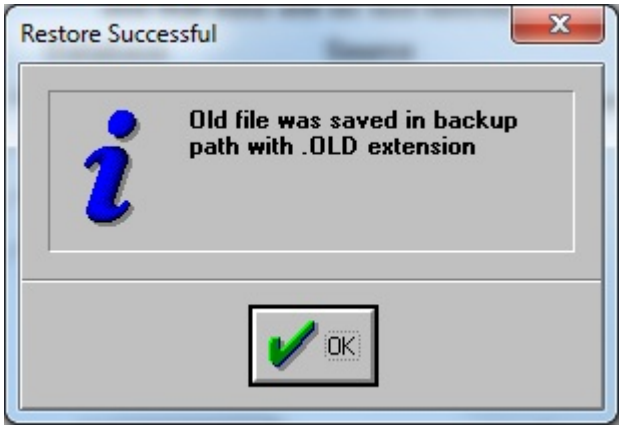
If selected and the **[Restore]** button clicked, then that entire database will be cleared of all records. This selection must be used with extreme caution! Hold down the <Shift>+<Ctrl> keys when opening the dialog to enable the **Clear entire file** option.

[Restore]

When the **[Restore]** button is clicked the database selected will be restored from the destination selected on the right.



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.



This message box indicates the restore has been completed. The previous database file has been renamed with an .OLD extension and saved in the Escort sub-directory. Only the most recent database of each type is retained.

6.2.3 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.

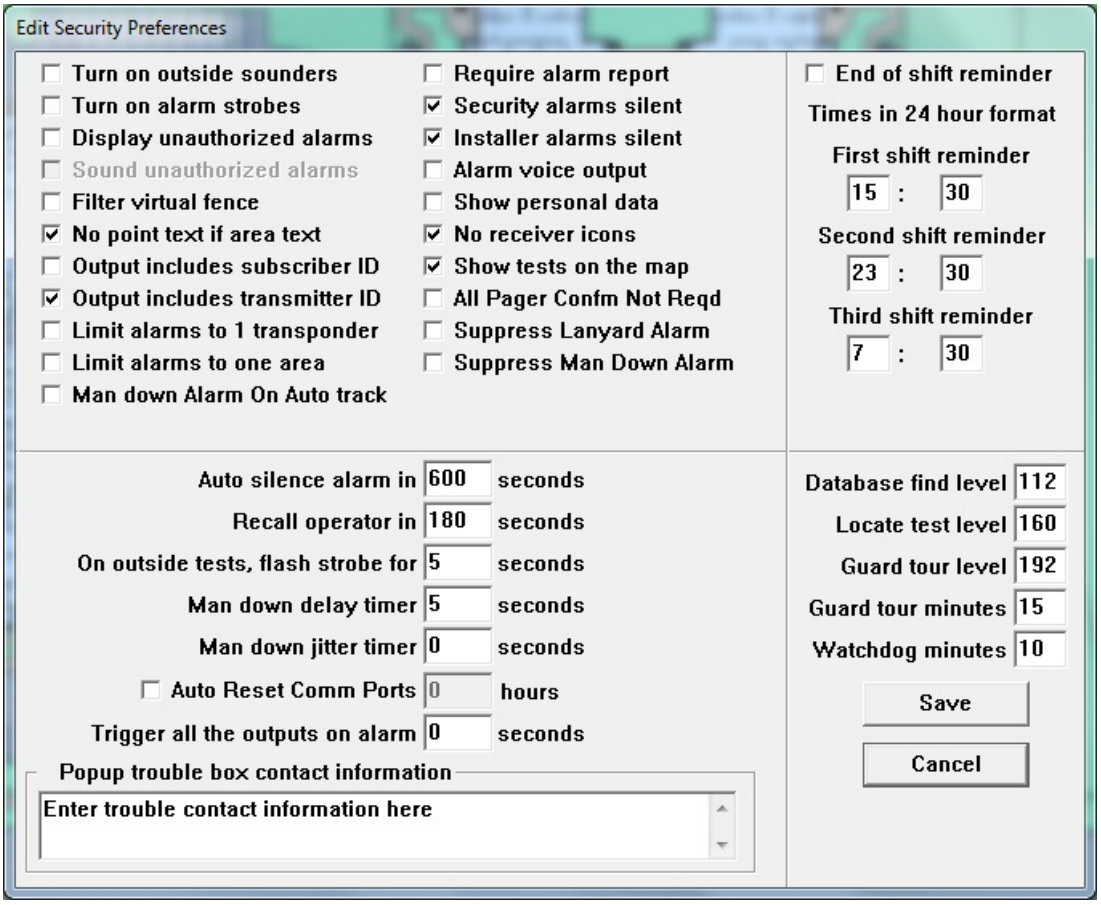


Figure 6.5: Security Preferences Dialog

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.
Clicking the **[Save]** button saves the modifications and exits the **Security Preferences** dialog. Click the **[Cancel]** button to save the changes made so far, to discard the changes, or to remain in the **Security Preferences** dialog.

Turn on outside sounders	This checkbox is used to activate or deactivate the sirens on alert units and transponders. Some security directors prefer that all alarms be silent, others choose to employ sirens. Checking this option causes the sirens on the alert units, to sound in the event of an alarm. Temporarily deactivating the sounders may be necessary during maintenance.
Turn on alarm strobes	Checking this option causes the strobe lights on the alert units and transponders, to flash in the event of an alarm.
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 checked.
Sound unauthorized alarms	This checkbox determines if "unauthorized” alarms are to be sounded on the horns of the receivers and the sirens of the alert units and transponders. The option is not available unless the **Display unauthorized alarms** option is selected. Typically this checkbox should not be checked.
Filter virtual fence	If the virtual fence option is be used, this box may be checked if some false alarms are generated to reduce the number of the false alarms. If it is checked then the actual alarms will be delayed by the supervision period of the transmitter.
No point text if area text	This checkbox affects the location text shown on the alarm screen. If this checkbox is checked and the alarm is determined to be within a predefined area then only the area text will be displayed (any receiver location text will be suppressed). Typically this checkbox should be checked.
Output includes subscriber ID	If this checkbox is checked, then 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 checked, then 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 checked.

Limit alarms to 1 transponder	This checkbox should not be checked. It was used only in a system where all transponders operate on areas that are separate from each other. It would prevent all interactions between 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 checked. It is used only in a system where all transponders operate on areas that are separate from each other.
Man down Alarm On Auto track	If this checkbox is checked, then 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 checked, 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 box should not be checked. If the operator should complete the report then check this box.
Security alarms silent	If this checkbox is checked, then 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 horns in the receivers.
Installer alarms silent	If this checkbox is checked, then 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 horns in the receivers. Typically this checkbox would be checked.
Alarm voice output	If this checkbox is checked, then predefined sound (.WAV) files can be played at the alarm console for specific alarm types. Typically this checkbox would not be checked.
Show personal data	If this checkbox is checked, then personal height, build, hair and eye color data will be displayed on the alarm screen.
No receiver icons	If this checkbox is checked, then individual receiver icons will not be shown on the alarm map display. Typically this checkbox would be checked.
Show tests on the map	If this checkbox is checked, 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 option doesn't affect the display the subscriber receives from a receiver or alert unit's strobe. Typically this checkbox would be checked.
All Pager Confm Not Reqd	If this checkbox is checked, 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 checked, the lanyard alarm is suppressed and not reported.
Suppress Man Down Alarm	If this checkbox is checked, the man down alarm is suppressed and not reported.
Auto silence alarm in 'X' seconds	This box 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 box 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 Central 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	The entry in this box 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 value 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 10 seconds. Setting this value too short will cause inadvertent man down alarms to be generated.
Man down jitter timer 'X' seconds	This value 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 value controls the time that all the comm ports in the system will be automatically reset after configured 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 transponders, 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.

End of shift reminder	A check in this checkbox causes a prompt to 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 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 receiver before the system will recognize the test and print the location. If the transmitter is too far away from the receiver, that receiver's green light will not be displayed, so the guard knows that they must move closer to the receiver for the test to register.
Guard tour level	This 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 receiver before the system will recognize the test and create the guard tour entry. If the guard is too far away from the receiver, that receiver's green light will not be displayed, so the guard knows that they must move closer to the receiver for the test to register.
Guard tour minutes	This setting 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 setting 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.

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.

6.2.4 System Defaults

The options contained in the **System Defaults** dialog are accessible only to Security Escort service and maintenance personnel. These options affect the system operating parameters and are to be setup by installing personnel. The Security Escort*Technical Reference Manual* describes the functions accessible under this dialog.

6.2.5 System Labels

The options contained in the **System Labels** dialog are accessible only to Security Escort service and maintenance personnel. These options affect the system operating parameters and are to be setup by installing personnel. The Security Escort *Technical Reference Manual* describes the functions accessible under this dialog.

6.2.6 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 (only visible when printer is enabled from **Printer > Select report printer** dialog box). Select the **Midnight report** or the **Sunday only** checkboxes to automatically schedule the selected report at those times.

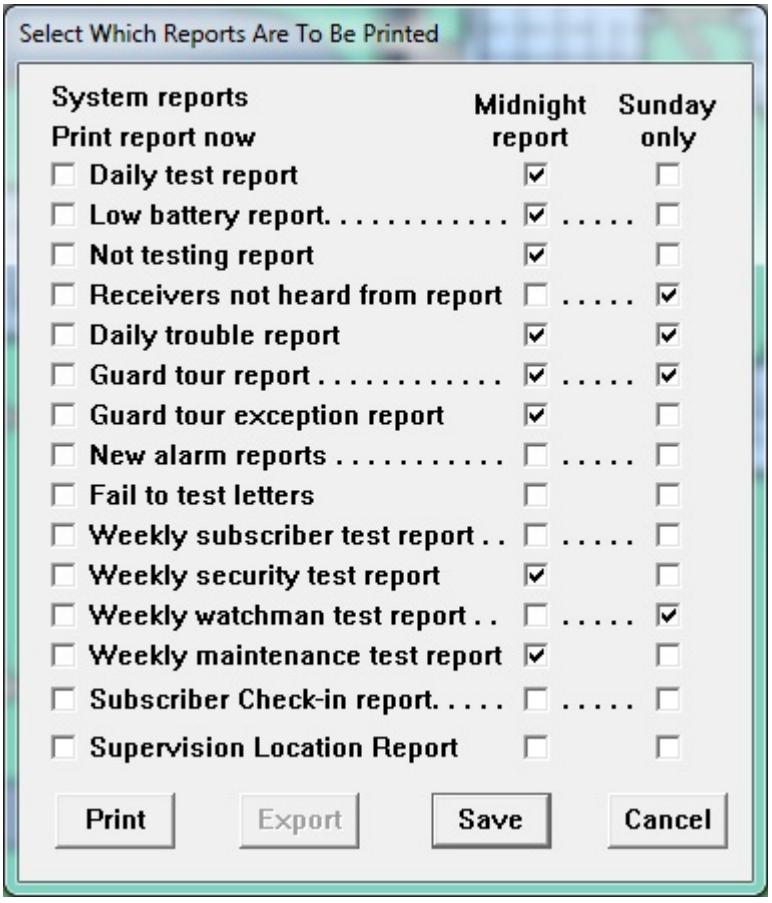


Figure 6.6: Print/Export System Reports Dialog

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 receivers that have not heard transmissions recently. This could indicate a problem with the receiver's ability to hear alarms and test transmissions.
Daily trouble report	Report of all the troubles currently being reported by transponders, receivers and alert units.
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.
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]	The **[Print]** button is only enabled if the printer is enabled from the **Printer > Select report printer** dialog box. Clicking this button prints all reports that are checked in the left-hand check boxes.
[Export]	The **[Export]** button is enabled if only the **Not testing report** is selected. Other reports must not be selected. Clicking this button exports the **Not testing report** in a ".csv" file format.
[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.
Print report now	Reports that are selected are printed when the **Print** button is clicked.
Midnight report	Reports are automatically 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.

6.2.7 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.

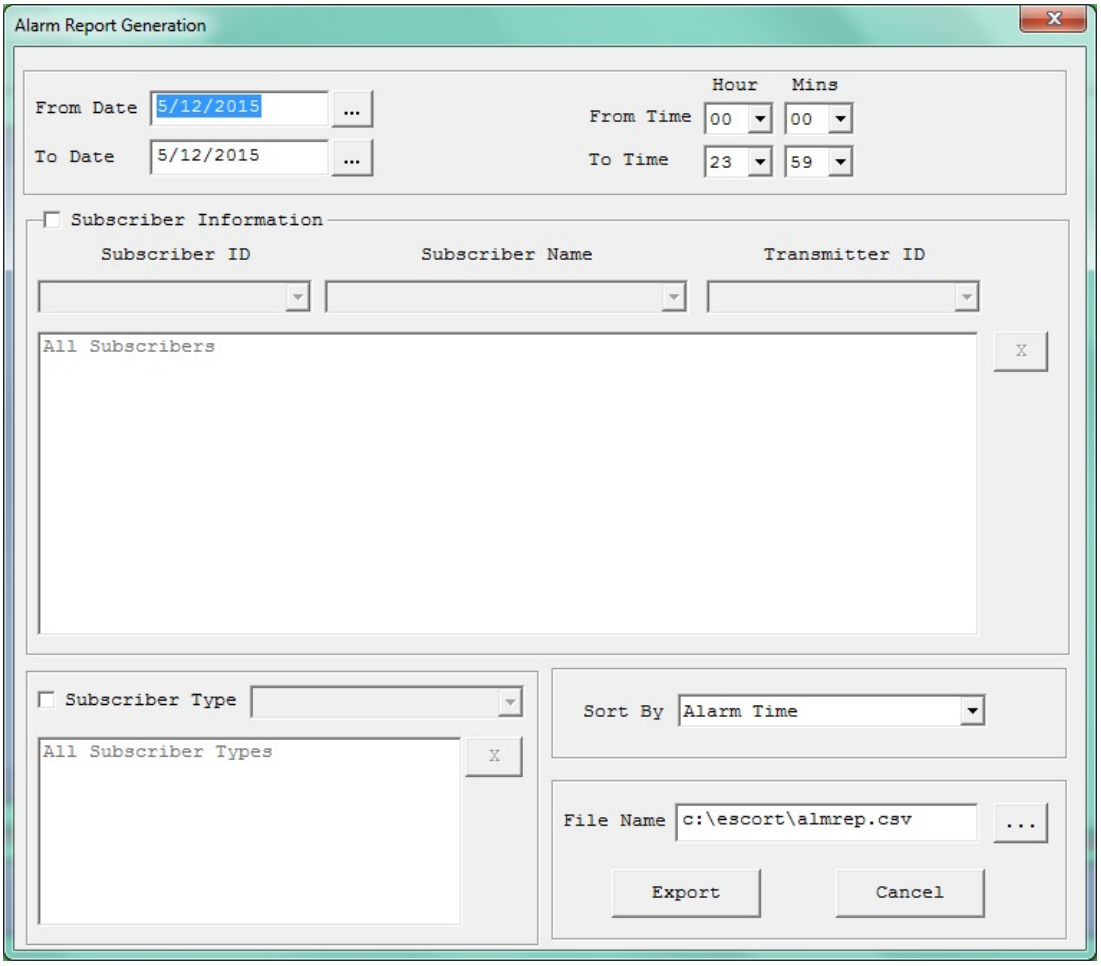


Figure 6.7: Export Alarm Report

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. Clicking the **[Export]** button saves the report to the specified file. Clicking the **[Cancel]** button cancels the report generation and exits from the dialog window.

6.2.8 Schedules

Manage time of day/day of week schedules and holidays. The operation of the schedules is covered in the Security Escort *Technical Reference Manual*.

6.2.9 Alarm Groups

This selection allows setup and arm/disarm control of the alarm groups. The operation of the alarm groups is covered in the Security Escort *Technical Reference Manual*.

6.2.10 Alarm Group State

This selection displays a list of the alarm groups that are currently armed and have one or more transmitters faulted.

6.2.11 Current Check-in Status

This selection displays a list of the subscribers who were required to check-in and failed to do so during the last check-in period.

6.2.12 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.

6.2.13 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.

6.2.14 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.

6.3 Logout menu

This menu has only one command: Logout the current operator. When the **Logout** option is selected, the operator currently logged in is logged out and the **Password** 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.

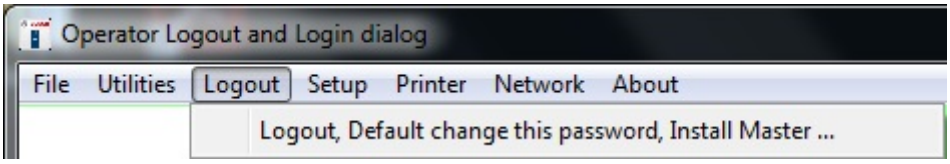


Figure 6.8: Logout Menu

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.

6.4 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. The Security Escort *Technical Reference Manual* describes the functions accessible under this menu.

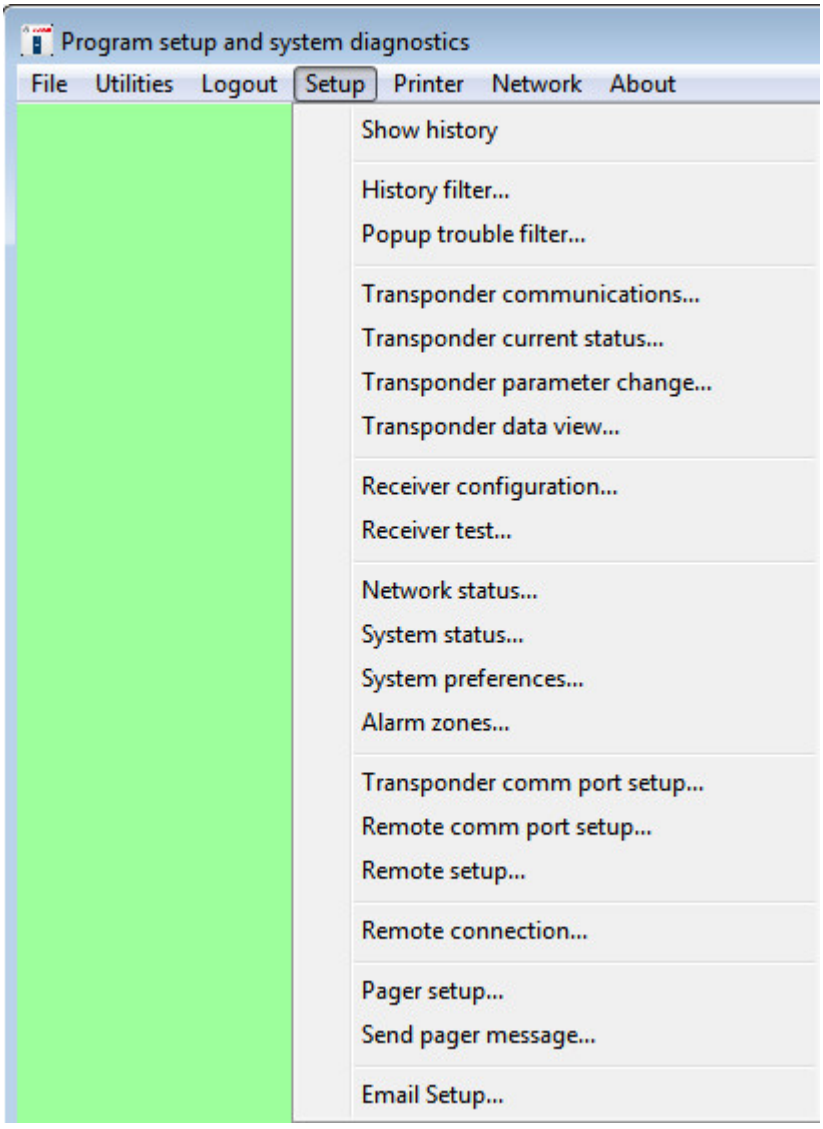


Figure 6.9: Setup Menu

6.5 Printer menu

The **Printer** option in the command line indicates printer status, such as out of paper, printer not selected, printer off, and so on. The printer can be turned on or off only by installation company personnel. The Security Escort *Technical Reference Manual* describes the functions accessible under this menu.

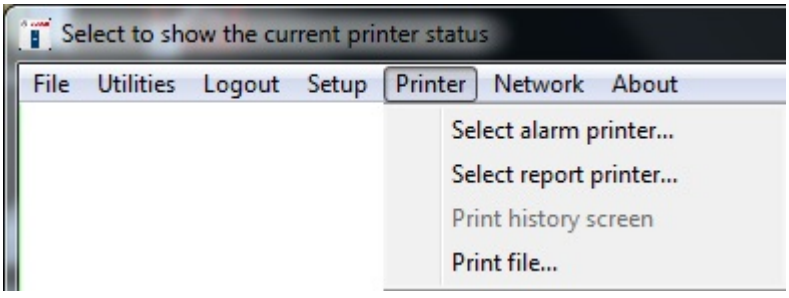


Figure 6.10: Printer Menu

6.6 Network menu

The **Network** menu allows an installer to setup and monitor the computer network connections. The Security Escort *Technical Reference Manual* describes the functions accessible under this menu.

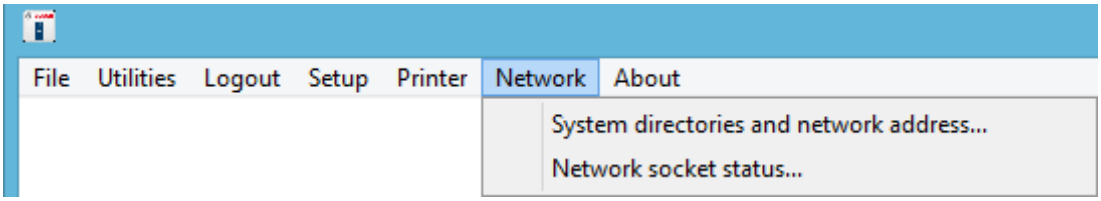


Figure 6.11: Network Menu

6.7 About menu

Choosing the **About...** option opens a dialog that displays information about the Central Console computer and the version of the Security Escort software currently installed. There also are demo selections that are disabled (grayed out) in a live system.

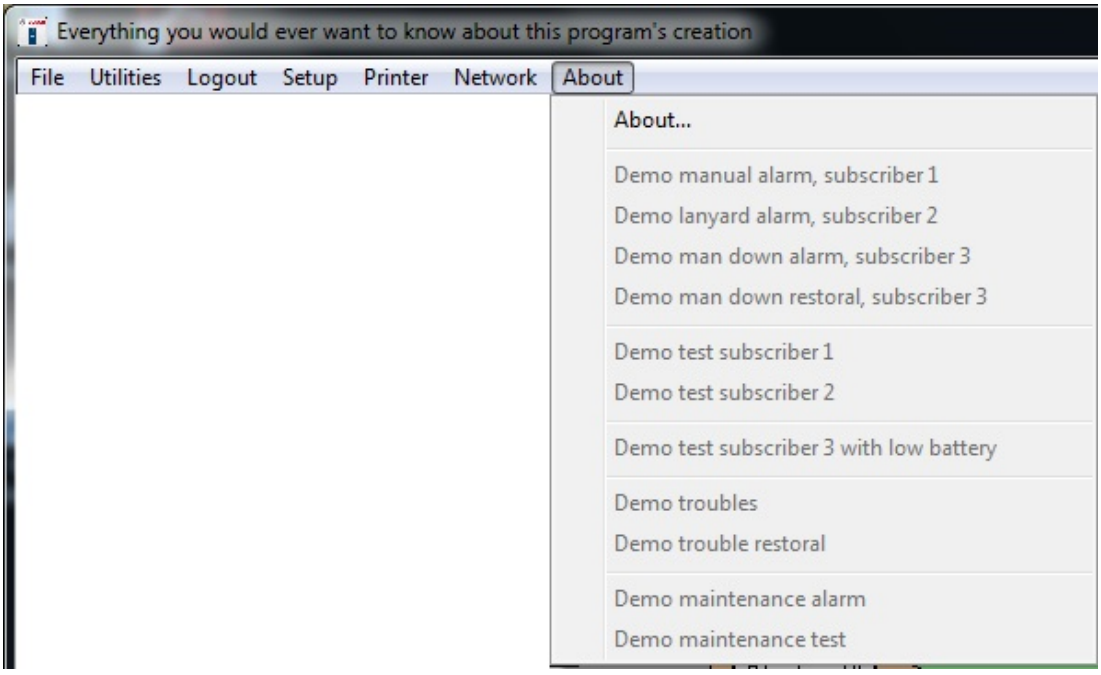


Figure 6.12: About Menu

7 Troubleshooting

The Security Escort system has many built in diagnostic features to detect system malfunctions. The Central Console computer identifies potential problems continuously monitors each transponder, receiver and alert unit. Whenever a problem is detected, trouble alerts are presented on the display of the Central Console. These alerts provide problem descriptions, emergency phone numbers, and other instructions for resolving the problem. This section describes the significance of system trouble alerts and the action Security personnel should take in response to the problems. Examples of the **Trouble pop-up** dialog are given in each section. Note that some system trouble alerts involve aspects of the system which Security department personnel will be unable to correct themselves. When these troubles occur, the installation company service representative should be contacted as soon as possible, using the phone number that appears in the pop-up dialog.

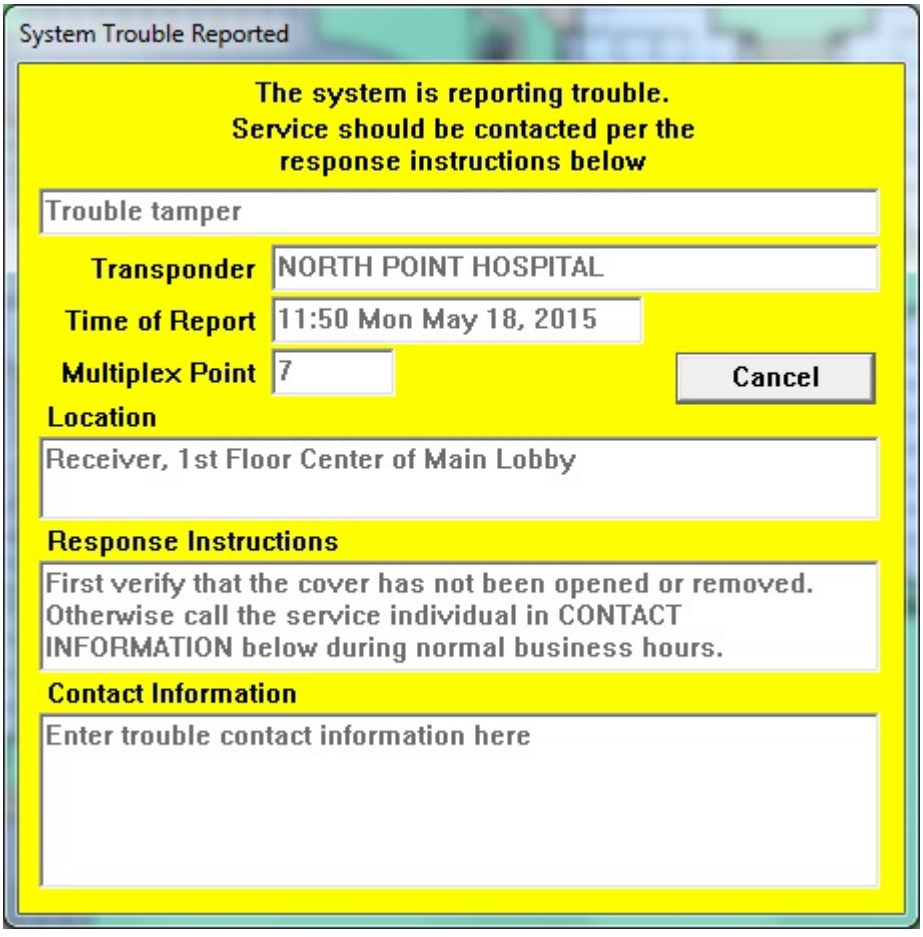


Figure 7.1: Example of System Trouble

Be sure to inform the service representative of the words in the pop-up trouble dialog, which describe the problem. Clicking the **[Cancel]** button should clear the pop-up dialog, after the problem is corrected or the installation company service representative is contacted.
Note that, after a problem is corrected, the system confirms the correction with a **Restored pop-up** dialog. This “restored” message should appear within 30 sec. after the trouble is corrected. When attempting to correct a problem, clear the trouble pop-up dialog and wait for 30 sec. for the “restored” message to be certain the problem is corrected.

7.1 Transmitters with low batteries

The transmitter senses that its battery is low well before the point at which it can no longer transmit an alarm message. It then inserts a “Low Battery” indication in every test (or alarm) message sent by the transmitter, advising the Central Console of the low battery condition. The **Low Battery Trouble** dialog appears whenever a subscriber attempts to test his or her transmitter, and the battery in that transmitter is low. Security department personnel should promptly advise the subscriber to bring the transmitter to the Security office for an exchange. It should be exchanged for a new one, using the **Transmitter Change** command in the **File** menu as described earlier.

7.2 Broken or lost transmitters

When a damaged transmitter is returned to the Security office, it should be clearly marked as faulty and given to the installation company service representative so that a replacement can be made to the inventory of spare transmitters. The damaged transmitter should be exchanged for a new one, using the **Transmitter Change** command in the **File** menu.
Lost transmitters should be replaced promptly and the old transmitter ID should be removed from the **Subscriber Database**.

7.3 Receiver and alert unit problems

This section lists the potential receiver and alert unit problems and their descriptions.

7.3.1 AC loss

Each alert unit requires its own AC power source for long term operation, however, each unit contains a backup battery which provides power to the strobe and siren in the event of loss of AC power. The **AC Loss Trouble** dialog appears whenever the power supply of an alert unit is interrupted. A Security officer should check to see if the wiring to the alert unit was disturbed or if one of the building’s circuit breakers was tripped. If the trouble cannot be resolved, the installing company service representative should be contacted promptly**.** The alert unit’s internal batteries will keep it operational for several hours.

7.3.2 Low battery

This trouble dialog signifies that an alert unit’s internal batteries are beginning to run low. A security officer should be sent to check the device’s power source (see *AC loss, page 51*). When the AC power is restored, the batteries recharge automatically. If power cannot be restored the installation company service representative should be informed the next business day.

7.3.3 Tamper

This pop-up trouble dialog signifies that a receiver or alert unit was tampered with. The location of the device is shown in the pop-up dialog. A Security officer should be sent to inspect the device. If the cover is loose, or missing, tightening or replacing the cover may fix the problem. If the cover is secure and there is no visible reason for the tamper warning, the installation company service representative should be contacted as soon as possible.

7.3.4 No response

This pop-up trouble dialog appears to indicate that a receiver or alert unit is no longer responding to the system. The installation company service representative should be informed the next business day if a single receiver or alert unit is affected. However, if many receivers or alert units are reporting, then the installing company should be contacted as soon as possible.

7.3.5 Jamming

This pop-up trouble dialog appears to indicate that a receiver is experiencing radio interference that may effect its ability to hear alarm signals. The installing company service representative should be informed the next business day.

7.3.6 Output device error

This trouble dialog appears when there is no response to a signal sent by a transponder to an alert unit or receiver. It means that a single output did not operate correctly when commanded by the system. The installing company service representative should be informed the next business day.

7.3.7 Bad checksum

When this pop-up dialog appears, there has been an error in the communications between a transponder and its receivers or alert units. The installation company service representative should be informed the next business day.

7.4 Transponder problems

This section lists the potential transponder problems and their descriptions.

7.4.1 Communications failure

This trouble alert indicates that the Central Console is having problems communicating with one of the transponders. This could mean that a significant portion of the protected area might not be able to report alarms to the Central Console. The installation company service representative should be contacted **immediately.**

7.4.2 AC loss

This trouble alert indicates that the power supply of a transponder was interrupted. A security officer should check if the transponder's input power line was disturbed. If that is not the problem, one of the building's circuit breakers may be tripped. If the trouble cannot be resolved, the installing company service representative should be informed as soon as possible**.** The transponder's internal batteries will keep it operational for several hours, which should be sufficient time for the problem to be resolved.

7.4.3 Low battery

This trouble dialog signifies that a transponder's internal batteries are beginning to run low. If not already done, the source of AC power to the transponder should be checked (see *AC loss, page 52*). When the AC power is restored, the batteries recharge automatically. If the power cannot be restored, the installation company service representative should be informed as soon as possible.

7.4.4 Tamper

This pop-up trouble alert signifies that a transponder was disturbed. A security officer should be sent to inspect it. If the door is ajar, it should be closed and secured. If the problem cannot be identified and corrected, the installation company service representative should be informed as soon as possible.

7.4.5 Bus faults

This trouble alert indicates that a transponder cannot communicate with one or more of its receivers or alert units. The installation company service representative should be contacted **immediately.**

7.4.6 Other troubles

Other trouble alerts that are site specific may be displayed at the Central Console. For these trouble warnings, follow the directions on the screen. The installation company service representative should be informed as soon as possible.

8 Appendix: Software licenses

This product contains both software that is proprietary Bosch software licensed under the Bosch standard license terms, and software licensed on the basis of other licenses.

8.1 Bosch software

All Bosch software © Bosch Security Systems. Bosch software is licensed under the terms of the End User License Agreement (EULA) of Bosch Security Systems B.V. or Bosch Security Systems Inc, as available together with the physical carrier (CD or DVD). Any use is subject to agreement and compliance with such EULA, as applicable.

8.2 Other licenses — copyright notices

Bosch is committed to comply with the relevant terms of any open source license included in its products. The open source licenses for Security Escort are listed in the **OpenSourceLicensing.doc** file in the Open Source folder of the CD-ROM. The relevant open source software or source code can also be obtained by downloading from the Bosch product catalog website.

8.3 Warranties and disclaimer of warranties

Software provided under other licenses has specific disclaimers of warranties. These are repeated in the full license texts, and apply in full to the relevant software components. All software components provided under the other licenses are provided "as is" without any warranty of any kind, including but not limited to any implied warranty of merchantability or fitness for a particular purpose, unless stated otherwise in writing. Please see the full text of the relevant software licenses for further details. The Bosch standard product warranty only applies to the combination of hardware and software as delivered by Bosch. Without prejudice to any licensee's right to apply the provisions of a relevant software license, any modification of any software delivered with or as part of the product may render any warranty on the whole product or any parts thereof null and void, and Bosch is entitled to charge fees for any services in relation thereto.

Index

A

About menu 49
AC loss 51, 52
Acknowledge subscriber type 23
Acknowledging an alarm 12
Address 24
Advanced 25
Alarm 11
  acknowledging 12
  interpreting 11
  multiple 13
  resetting 13
Alarm Background Color 25
Alarm Group State 46
Alarm Groups 46
Alarm map 30
Alarm report 14
  incomplete 32
Alarm Reports Database 29
Alarm screen 11
Alarm voice output 40
Alarm Zone 25
Alert unit 9
Alert unit problems 51
All Pager Confm Not Reqd 40
Authority levels 19
Auto Reset Comm Ports ‘X’ hours 41
Auto silence alarm in 'X' seconds 41

B

Backup 35
Backup and restore 36
Backup databases 34
Bad checksum 52
Beginning 16
Browse 25
Build 25
Bus faults 52

C

Cancel 18, 22, 25
Central Console 9
City 24
Clear 21
Clear screen 47
Communications failure 52
Components
  alert unit 9
  Central Console 9
  receiver 8
  special transmitter 8
  transponder 9
Contact information 43
Current Check-in Status 46

D

Daily test report 44
Daily trouble report 44
Database backup 34
Database commands 15
Database find level 42
Database management 15
Database restore 36
Databases
  operator:editing 18
  reports:map 30
  reports:sorting 31
  subscriber:editing 20
Delete 17, 31
Diagnostic features 50
Disability 24
Disabled 24
Display unauthorized alarms 39
Done 26

E

Edit data 17, 30
Edit operator record 19
End Of File 16
End of shift reminder 42
Export 45
Eye Color 25

F

Fail to test letters 45
Female 25
File menu 33
Filter virtual fence 39

G

Guard tour exception report 44
Guard tour level 42
Guard tour minutes 42
Guard tour report 44

H

Hair Color 25

Height 25

I

Image File 25
Incomplete alarm report 32
Information 25, 26
Insert New 16
Installer alarms silent 40

J

Jamming 52

K

Key Select 17, 32

L

Limit alarms to 1 transponder 40
Limit alarms to one area 40
Local Escort drive 35
Locate Key 17, 31
Locate test level 42
Logout menu 47
Lost transmitters 51
Low battery 51, 52
Low battery report 44

M

Maintenance transmitters 8
Male 25
Man down Alarm On Auto track 40
Man down delay timer ‘X’ seconds 41
Man down jitter timer ‘X’ seconds 41
Map
  alarm 30
Master Database drive 35
Midnight report 45
Multiple alarms 13

N

Name 24
Network menu 49
New alarm reports 44
New ID 25
Next 16
No point text if area text 39
No receiver icons 40
No response 51
Not testing report 44

O

On outside tests, flash strobe for 'X' seconds 41
Operator Database 18
Output device error 52
Output includes subscriber ID 39
Output includes transmitter ID 39
Output verification 47

P

Password 19
Phone 24
Point transmitter 8
Previous 16
Print 18, 21, 22, 45
Print report now 45
Print Subscriber Database 21
Print System Reports dialog 45
Print/Export System Reports dialog 43
Printer menu 48

R

Recall operator in 'X' seconds 41
Receiver 8
Receiver problems 51
Receivers not heard from report 44
Report
  End of shift reminder for 42
Reports Database 29
Require alarm report 40
Reset 21
Resetting the system 13
Restore database 36

S

Save 25
Schedules 46
Security alarms silent 40
Security preferences 38
Security transmitters 8
Setup menu 47
Shift reminder 42
Show personal data 40
Show tests on the map 40
Silencing an alarm 12
Silent 24
Slave Database drive 35
Sound unauthorized alarms 39
Special transmitters 8
State 24
Subscriber Check-in report 45
Subscriber Database 20
Subscriber Database editing 22
Subscriber ID 25
Subscriber Type 23
Sunday report 45
Supervision Duration 24
Supervision Location report 45
Suppress Lanyard Alarm 41

Suppress Man Down Alarm 41
Synchronize system time 47
System Defaults 43
System Labels 43

T

Tamper 51, 52
Transmitter 8
  exchanging 26
  low battery 51
  special types 8
Transmitter Change 26
Transmitter ID 25
Transmitter replacement 51
Transmitter supervision duration 24
Transmitter Type 23
Transponder 9
Transponder problems 52
Trigger all the outputs on alarm 'X' seconds 41
Trouble
  Emergency contact text box for 43
Troubles 53
Troubleshooting 50
Turn on alarm strobes 39
Turn on outside sounders 39

U

Utilities menu 33

V

virtual fence 39

W

Watchdog minutes 42
Weekly maintenance test report 45
Weekly security test report 45
Weekly subscriber test report 45
Weekly watchman test report 45
Write EXCEL import file 22

Z

Zip 24

Bosch Security Systems B.V.
Torenallee 49
5617 BA Eindhoven
Netherlands
www.boschsecurity.com
© Bosch Security Systems B.V., 2019