# Security Escort

SE2000 Series

**en** Software Installation Manual

# Table of contents


| | | |
|---|---|---|
| **1** | **Copyright and warranty** | **4** |
| 1.1 | Software license agreement | 4 |
| 1.2 | Limited warranty | 4 |
| 1.3 | Remedy | 4 |
| **2** | **Introduction** | **6** |
| **3** | **Demo installations** | **7** |
| **4** | **Non-Network installations** | **8** |
| **5** | **Network installations** | **9** |
| **6** | **Installing the Security Escort software** | **10** |
| 6.1 | Software installation procedure | 10 |
| 6.2 | Uninstalling the Security Escort program | 19 |
| **7** | **Network setup** | **21** |
| 7.1 | Install a network interface card in the master and slave computers | 21 |
| 7.2 | Network setup on Windows 7 | 21 |
| 7.3 | Install the Security Escort software on the master and slave computers | 27 |
| 7.4 | Configure the Security Escort folder to be shared | 27 |
| 7.5 | Map the master’s network drive from each slave and workstation | 31 |
| 7.6 | Map the slave’s network drive from each master and workstation | 32 |
| 7.7 | Install the software key on the master computer | 34 |
| 7.8 | Configure the Security Escort software | 37 |
| 7.8.1 | Configure the software on the master computer | 42 |
| 7.8.2 | Configure the software on the slave computer | 43 |
| 7.8.3 | Configure the software on the workstation computers | 44 |
| **8** | **Troubleshooting** | **46** |
| 8.1 | “CAN'T OPEN THE OPERATOR.EDB FILE” error | 46 |
| 8.2 | Network connection fails | 47 |
| 8.3 | “THE MASTER COMPUTER MUST BE ON-LINE TO RETURN THE SYSTEM TO OPERATIONAL STATUS” message | 47 |
| **9** | **Maintenance** | **49** |
| 9.1 | Workstation and slave system synchronization | 49 |
| 9.2 | Reloading database to the workstation or slave | 49 |
| **10** | **Files required for Security Escort** | **50** |
| **11** | **Appendix: Software licenses** | **52** |
| 11.1 | Bosch software | 52 |
| 11.2 | Other licenses — copyright notices | 52 |
| 11.3 | Warranties and disclaimer of warranties | 52 |

# 1 Copyright and warranty

## 1.1 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.

## 1.2 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.

## 1.3 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 Introduction

**Warning!**
If this is a live system, back up the databases, maps, and preferences before installing the software! Refer to the Security Escort *Technical Reference Manual*, **Utilities** menu > **Backup** dialog.

This document describes the Security Escort software setup. The system setup for Windows® network connections for master computers, slave computers, and workstation computers is also covered.
Version 2.0 and later of the Security Escort software requires a software key connected to the universal serial bus (USB) port of the master computer to operate.

**Notice!**
If you do not have a programmed software key, do not install the program on a live system.

The system can communicate with the transponders and modifies the operator's database and preference settings. The sole exception to this is software that is used for demo purposes only.
The software key is programmed with the allowable number of slave and workstation computers that may be concurrently connected to the master computer. This setting is displayed in Security Escort's **About** dialog under the **About** menu.

# 3 Demo installations

When the software is used for demo purposes, it is limited to ten records in the **Subscriber Database**, one transponder in the **Transponder Database** and only receivers 0 through 3 on bus 0 can be defined for that transponder (no other points can be programmed for that transponder). If these limitations are observed, the software will communicate with the single transponder and the system can be used with full functionality for demo purposes. Refer to the Installing the Security Escort software section of to install the software.
After the software has been installed, do not run it. Double-click the HDD32.EXE file in the Security Escort directory (“C:\ESCORT”). This will install the driver for the software key. This is required even for demo installations that will not have the software key. If the HDD32.EXE installer is not run before the Security Escort software is run the first time, the Security Escort software will stop with an error and HDD32.EXE will automatically run. The demo installation is complete at this point and you do not have to refer to the rest of this document.
In demo mode, communications are allowed to one transponder even if the **Transponder Database** has more than one transponder in it for diagnostic purposes. The transponder selected in the **Transponder current status** or **Transponder communications** dialog will be the transponder that can be communicated with. The transponder can be reselected at any time to change the current transponder in communication. All tests, supervisions and maintenance alarms will function normally; however only subscriber alarms that contain reports from receivers 0 through 3 on bus 0 will function. If an alarm also includes other receivers reporting, that alarm will be ignored. Therefore, actual Security Escort operation can be demonstrated using up to 4 receivers. Also a demo system can be used to directly connect to transponders using the actual **Transponder Database** from the system to perform all functions except subscriber alarms. This is desirable to allow a laptop to be plugged directly into a transponder to diagnose problems. In both of these modes the **Subscriber Database** must have five or less subscribers.

# 4 Non-Network installations

If this system is not using the network to connect master, slave and workstation computers, refer to the Security Escort software installation section of this document to install the software. After the software has been installed, do not run it. Plug the software key into the USB port on the computer and double-click the HDD32.EXE file in the Security Escort directory (“C:\ESCORT”). This will install the driver for the software key.
If the HDD32.EXE installer is not run before the Security Escort software is run the first time, the Security Escort software will stop with an error and HDD32.EXE will automatically run. A non-network installation is complete at this point and you do not have to refer to the rest of this document.

# 5 Network installations

The Security Escort software supports a single master computer, a single slave computer (optional) and a maximum of eight workstations (limited to the number programmed in the software key). The master computer normally processes the real time communications to the transponders and controls the system. The slave computer can assume the master's role by switching the transponder communications to the slave computer. This system redundancy feature is explained in further details in the System redundancy chapter of the *Technical Reference Manual*. The workstation computers allow other computers to respond to alarms, perform maintenance and edit the databases.

# 6 Installing the Security Escort software

## 6.1 Software installation procedure

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

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

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

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

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

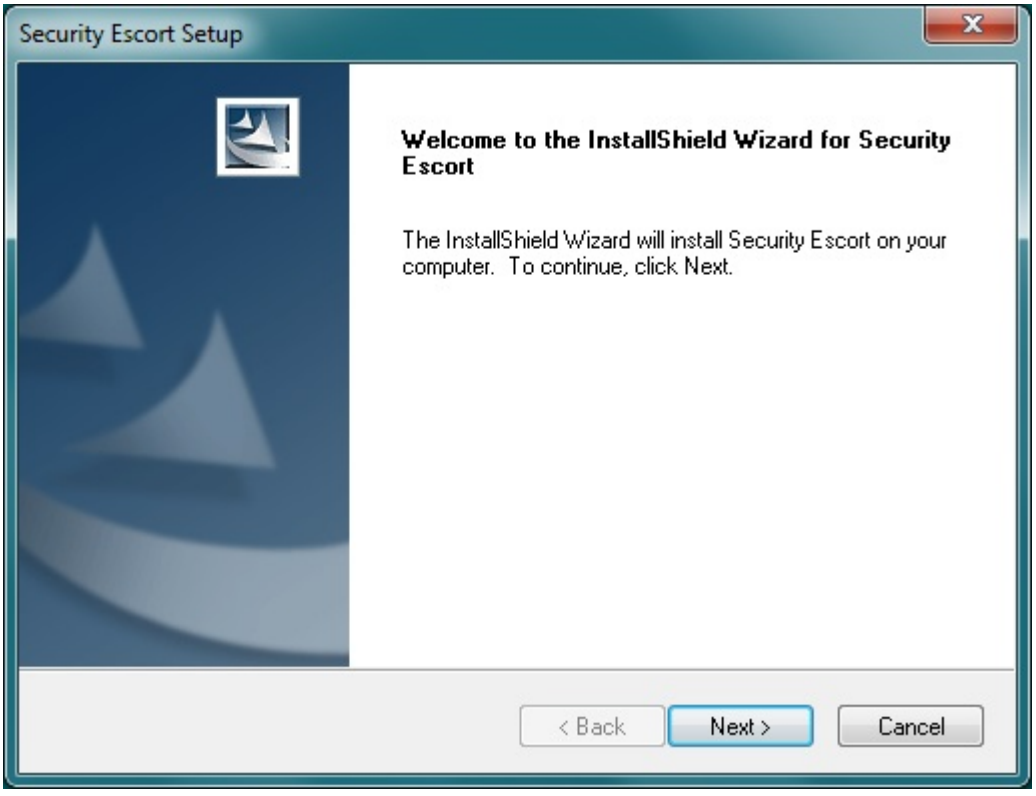



**Figure 6.1: Security Escort Setup Welcome Dialog**

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

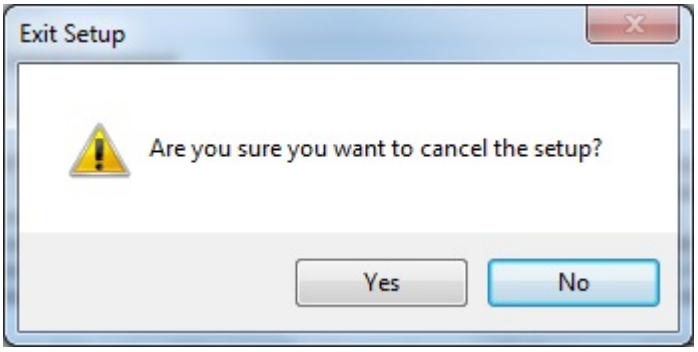



**Figure 6.2: Exit Setup Dialog**

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

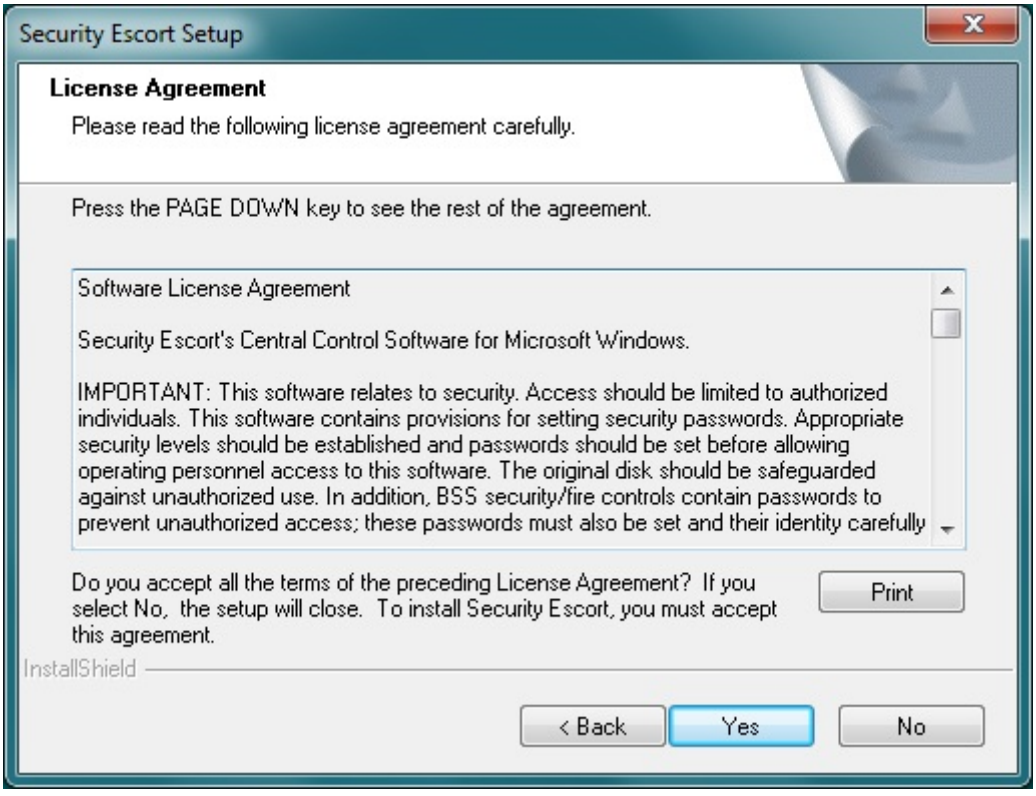



**Figure 6.3: License Agreement Dialog**

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

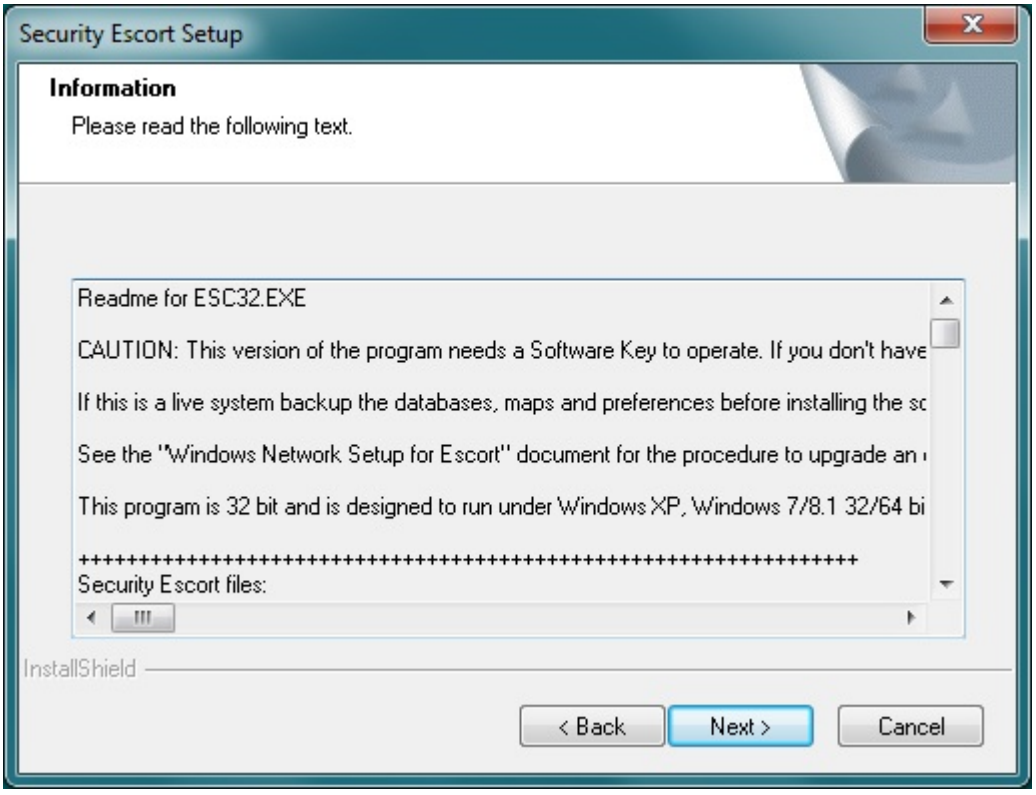



**Figure 6.4: Readme Information Dialog**

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

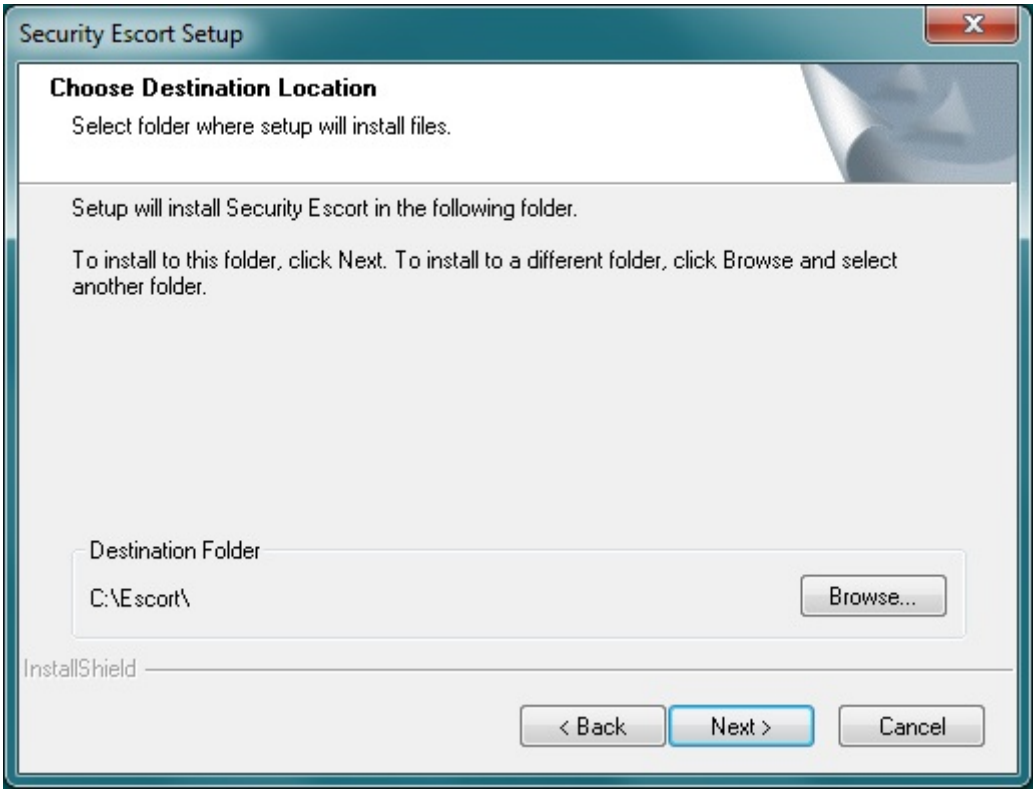



**Figure 6.5: Choose Destination Location Dialog**

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

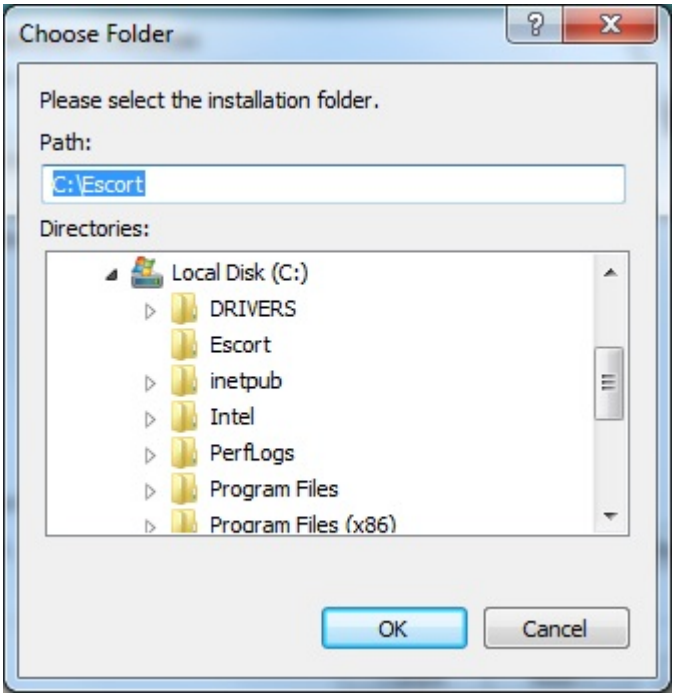



**Figure 6.6: Choose Folder Dialog**

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

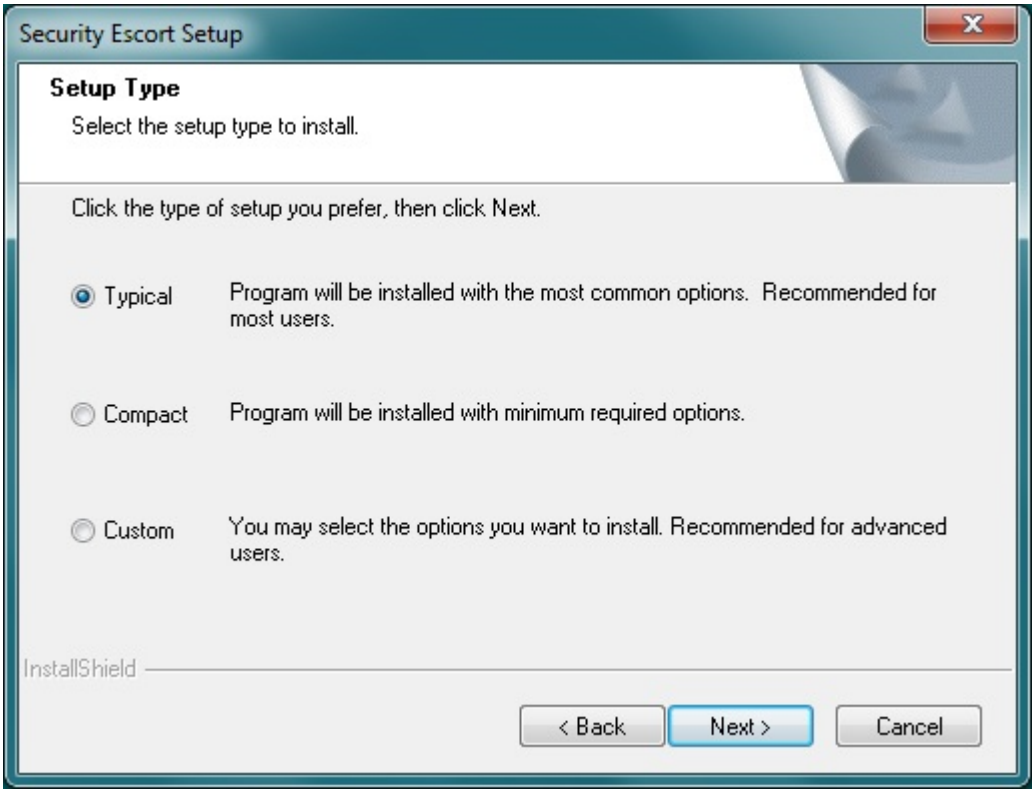



**Figure 6.7: Setup Type Dialog**

Select the type of installation you desire.

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

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

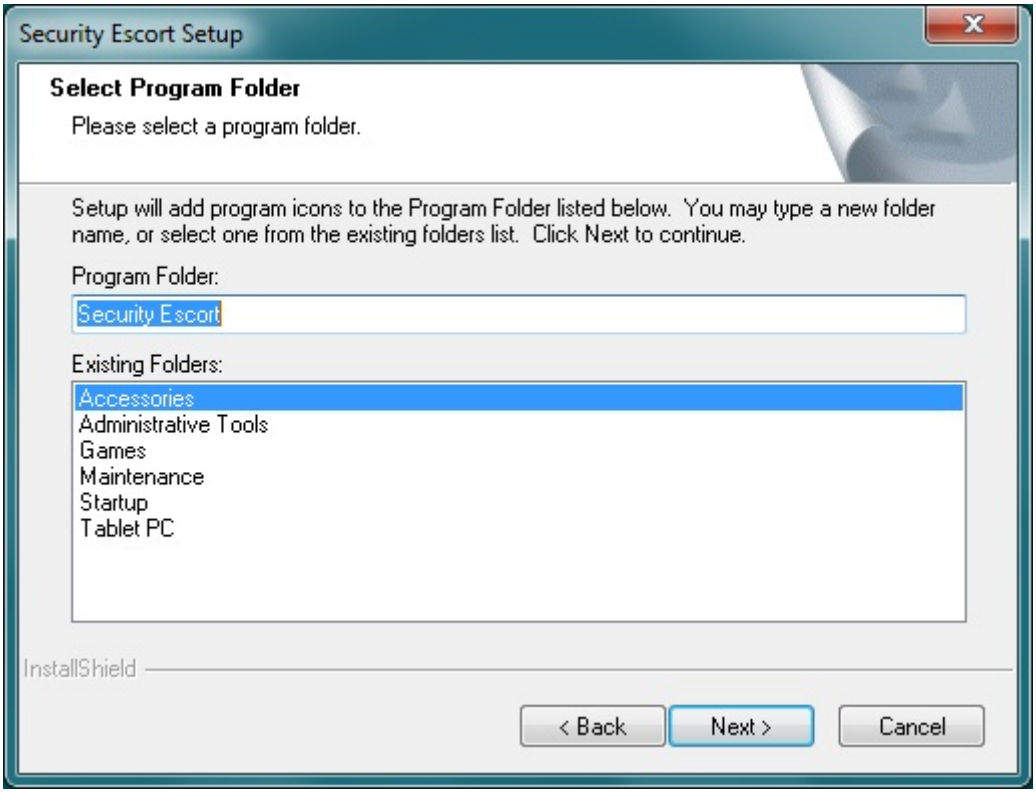



**Figure 6.8: Select Program Folder Dialog**

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

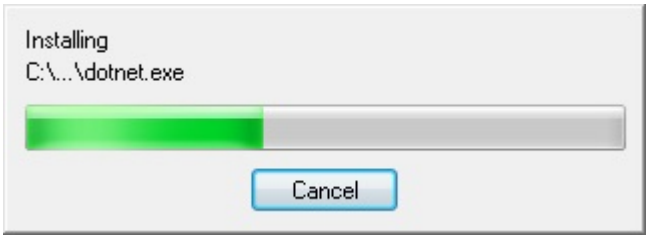



**Figure 6.9: Installation Progress Dialog**

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

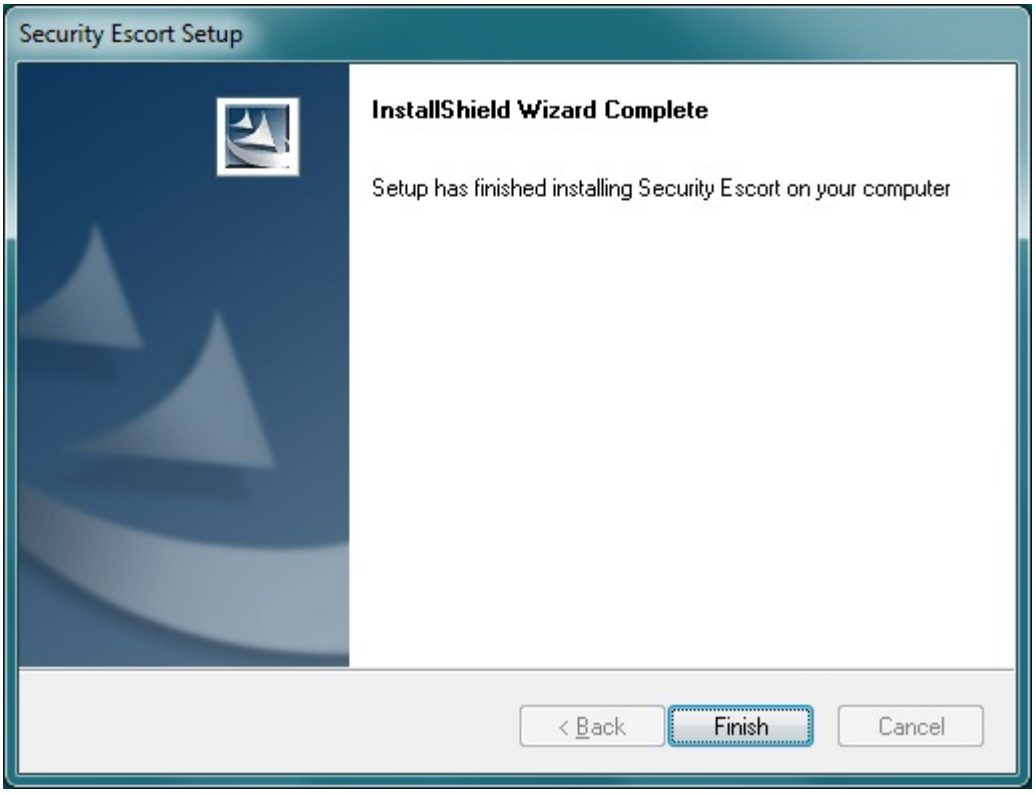



**Figure 6.10: Installation Complete Dialog**

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

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

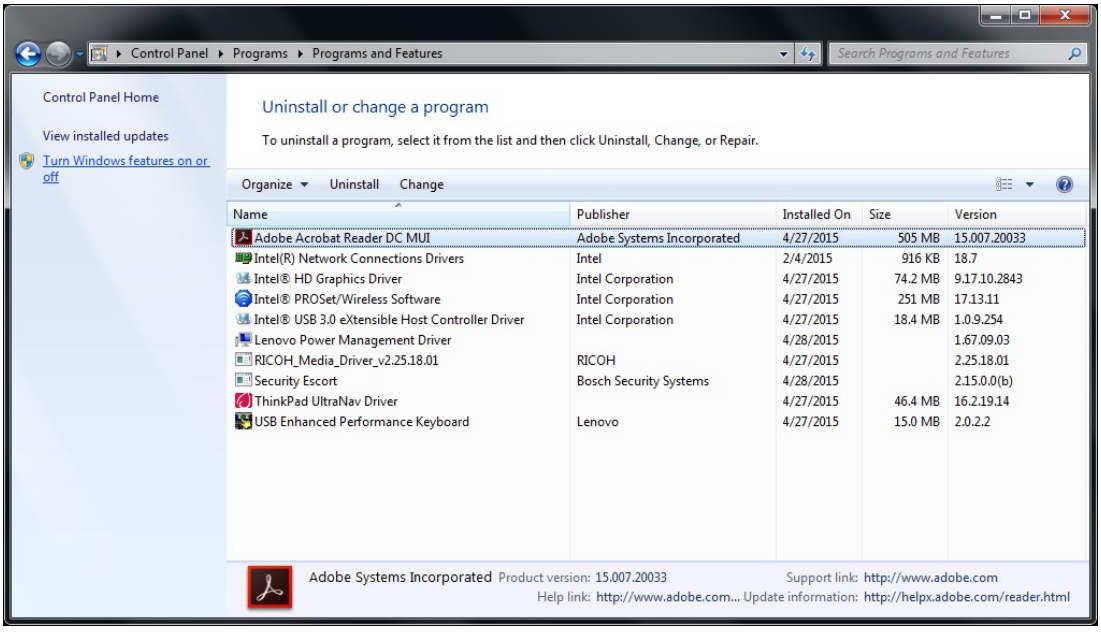



**Figure 6.11: Control Panel**

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

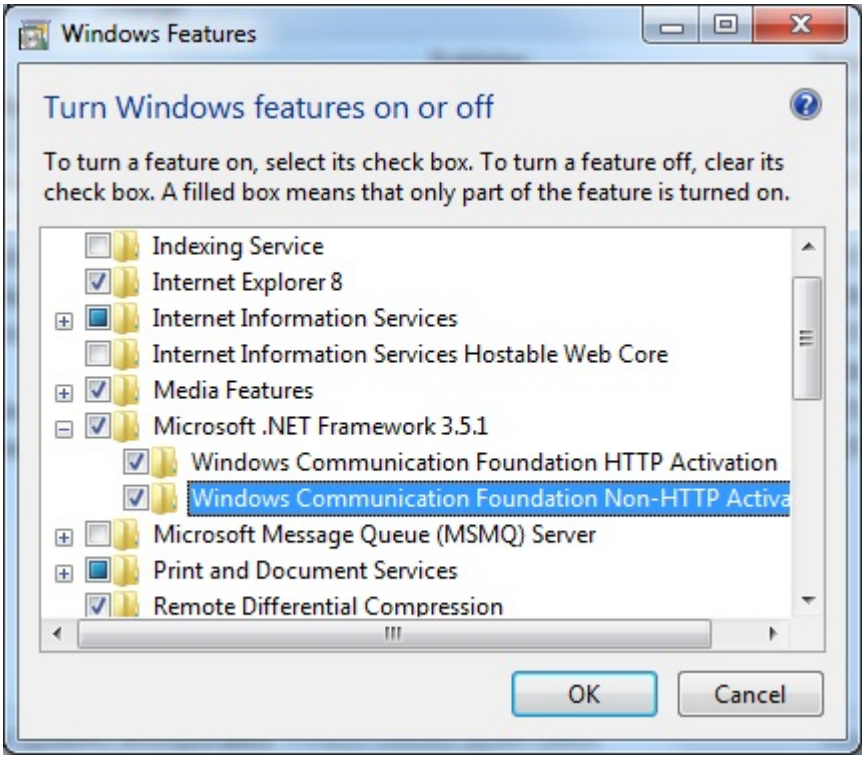



**Figure 6.12: Windows Features Dialog**

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

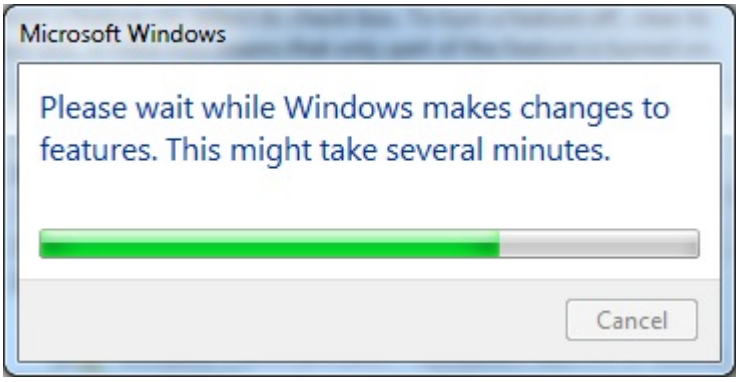



**Figure 6.13: Change Progress Dialog**

## 6.2 Uninstalling the Security Escort program

**Notice!**
Do not do this unless you desire to remove the Security Escort program from this computer! Make sure you have backups of the databases and map files, after the uninstall, they can not be recovered.

Click **Start** > **Control Panel > Programs and Features**. From the list of programs, select **Security Escort** and click the **Uninstall** menu.

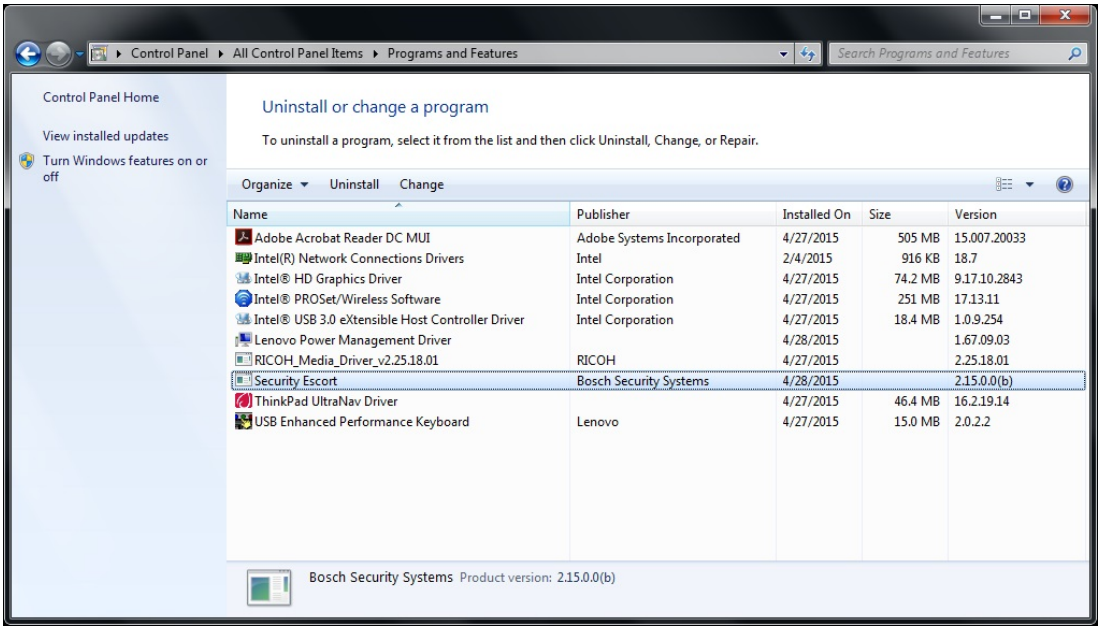



**Figure 6.14: Control Panel Programs and Features Dialog**

The dialog below appears. Click the **[Yes]** button and the Security Escort program uninstalls.

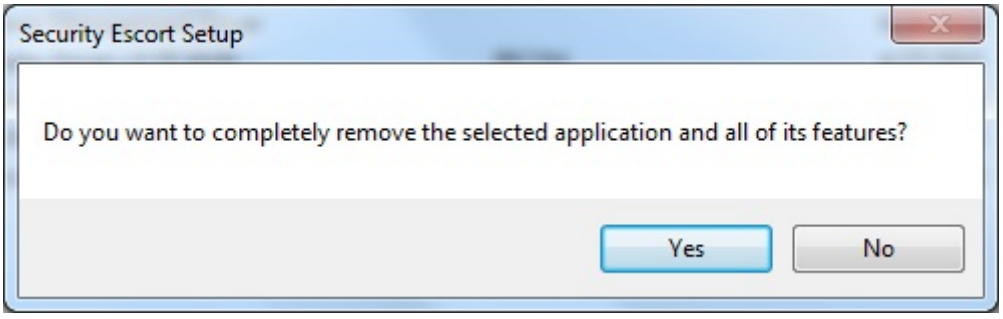



**Figure 6.15: Confirm Remove Application Dialog**

Once completed, the **Uninstall Complete** dialog window appears. Click the **[Finish]** button to return to your desktop.

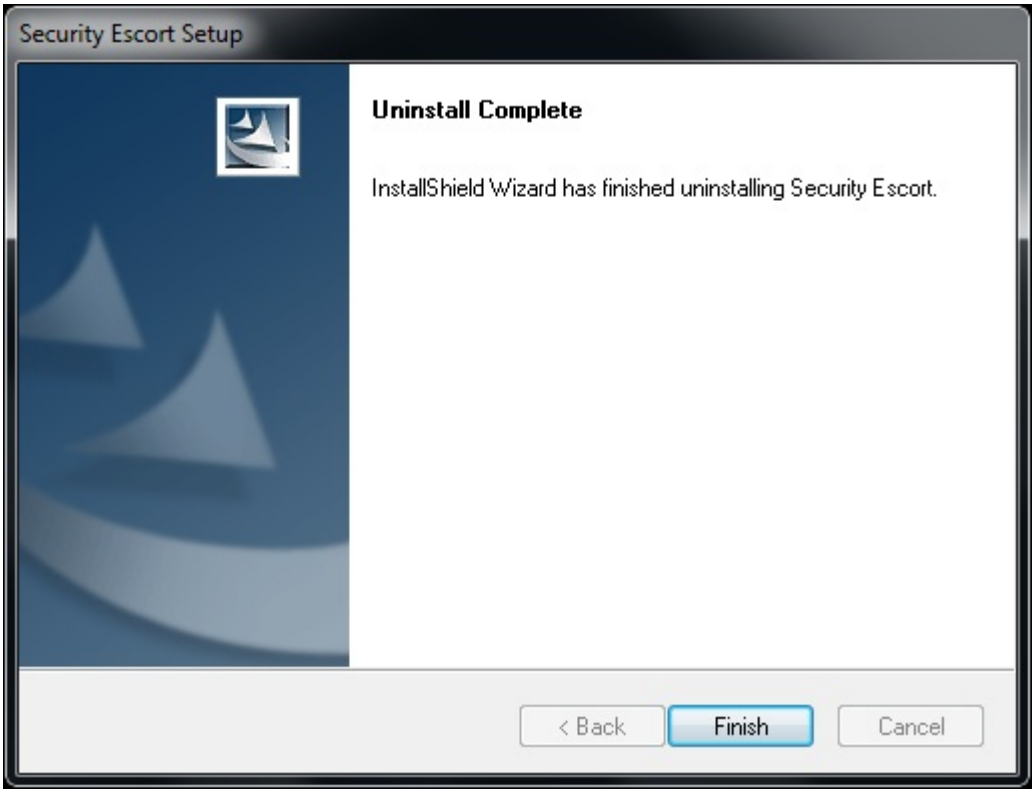



**Figure 6.16: Uninstall Complete Dialog**

# 7 Network setup

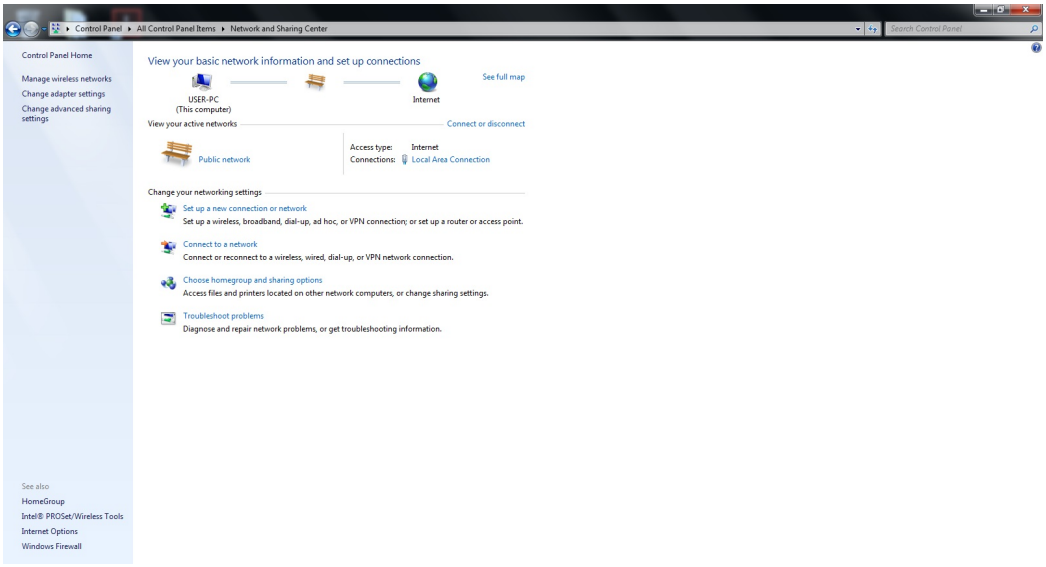
## 7.1 Install a network interface card in the master and slave computers

If the computer already has a network interface card, there is no need to install another for Security Escort. It can share the existing card.

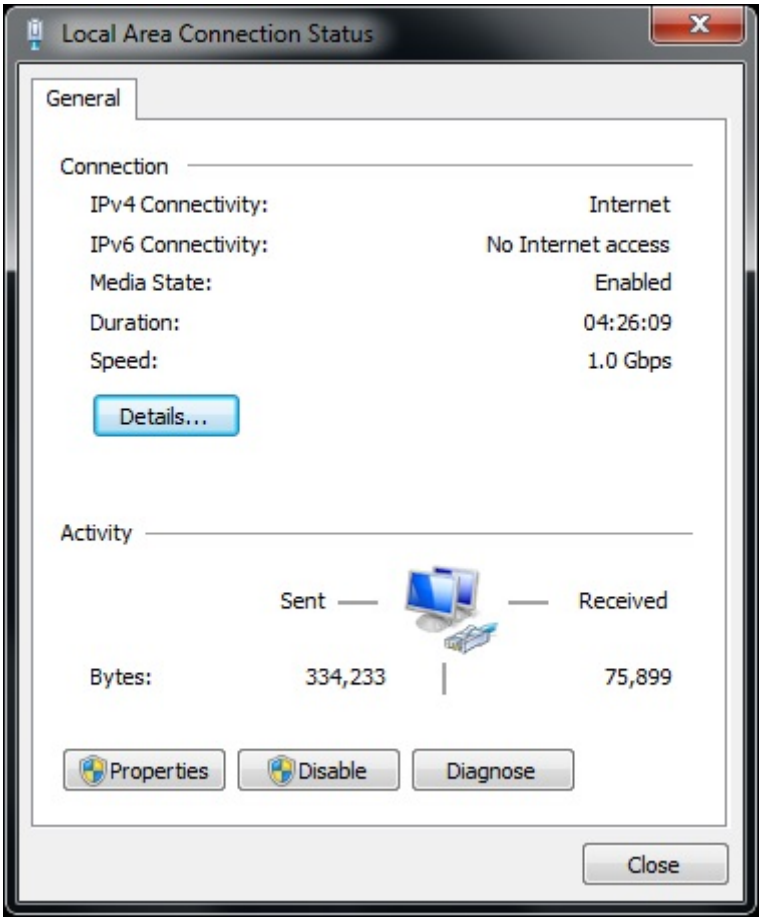
## 7.2 Network setup on Windows 7

Windows 7 and later installs the TCP/IP protocol by default; there should be no need to install it.

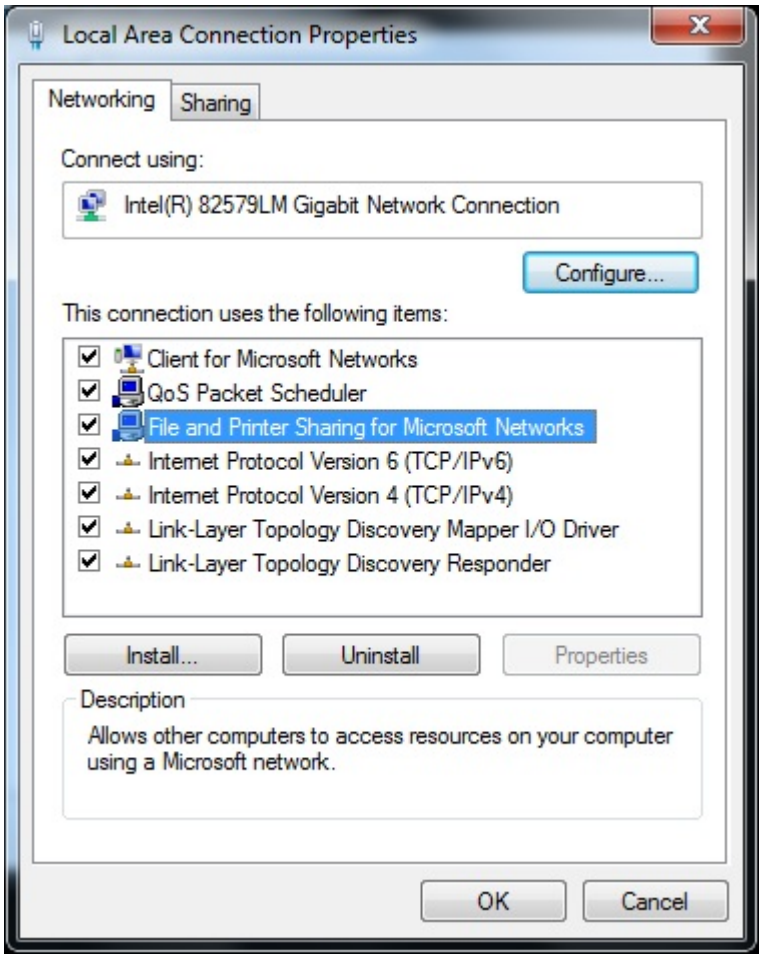
1. To setup the TCP/IP protocol, go to **Start > Control Panel > Network and Sharing**.



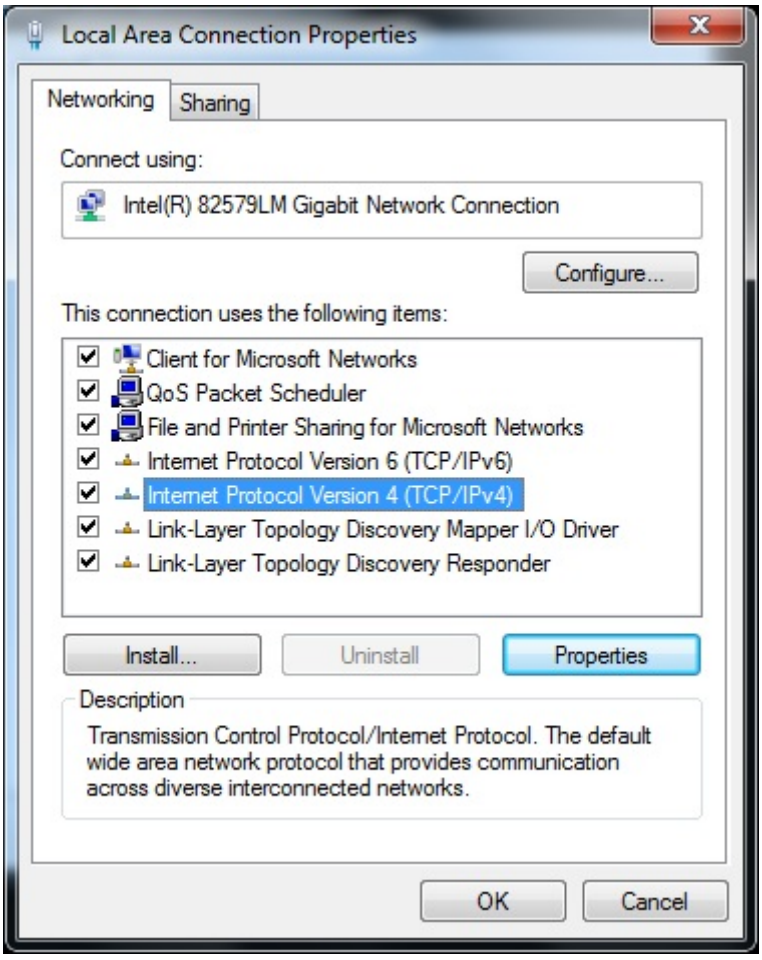
2. Click the **Local Area Connection** link. The **Local Area Connection Status** dialog appears.



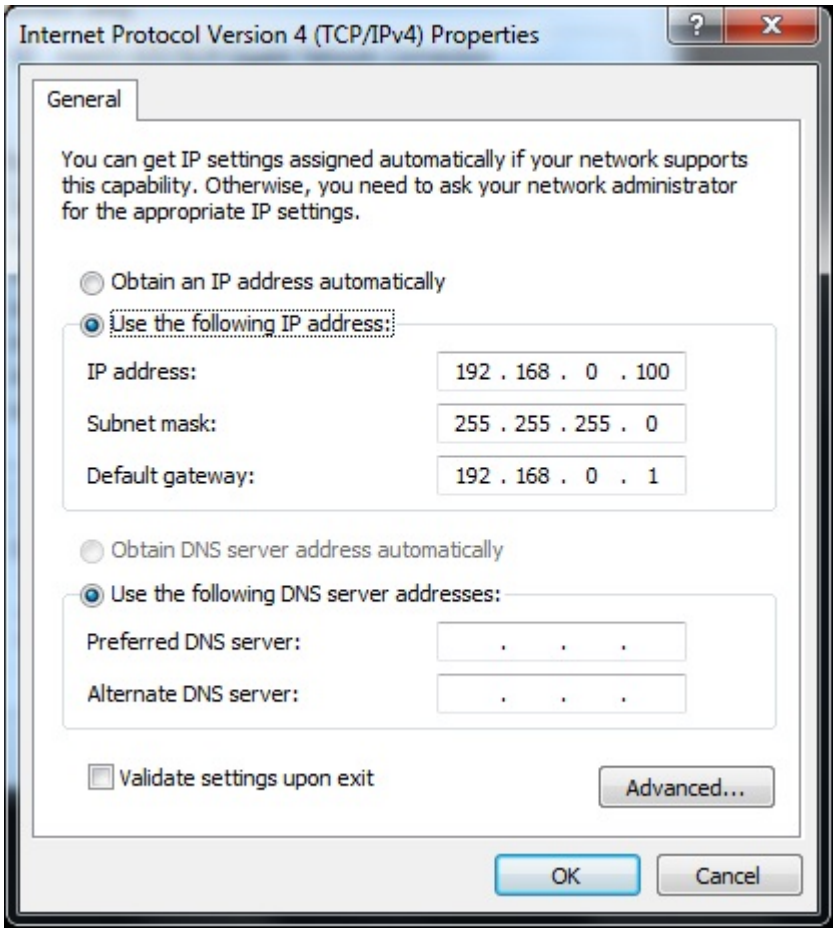
3. Click the **[Properties]** button. The **Local Area Connection Properties** dialog appears. Scroll to the **File and Printer Sharing for Microsoft Networks** item and ensure that the checkbox is checked.



4. In the same **Local Area Connection Properties** dialog, scroll to the **Internet Protocol Version 4 (TCP/IPv4)** item and select it.

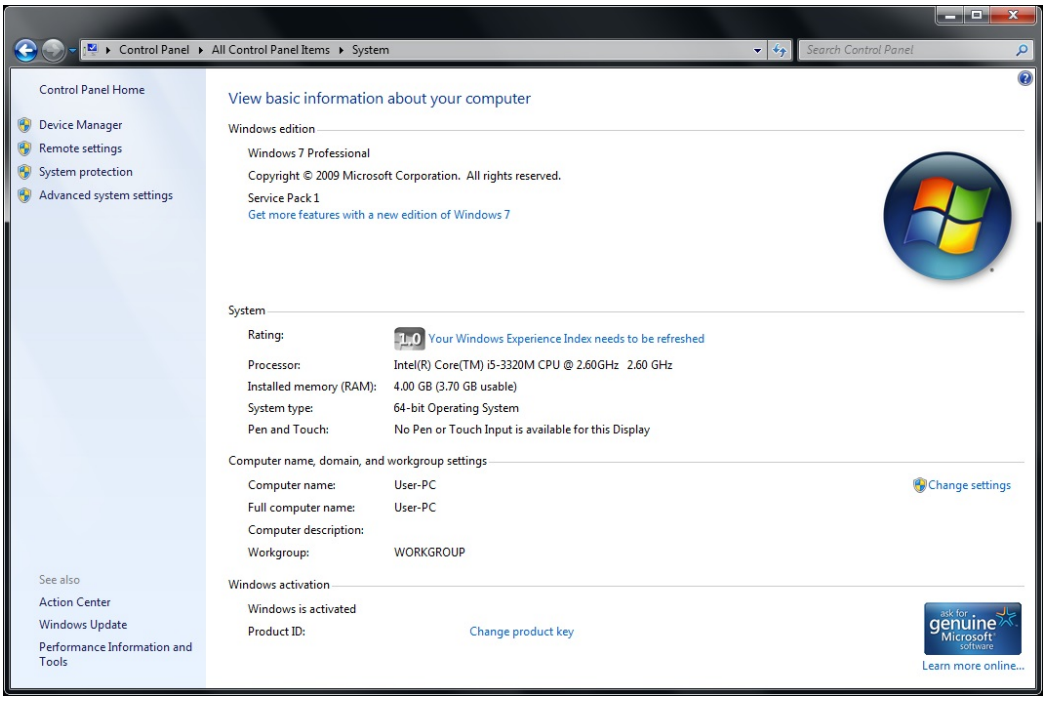


5. Click the **[Properties]** button. The **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog appears.

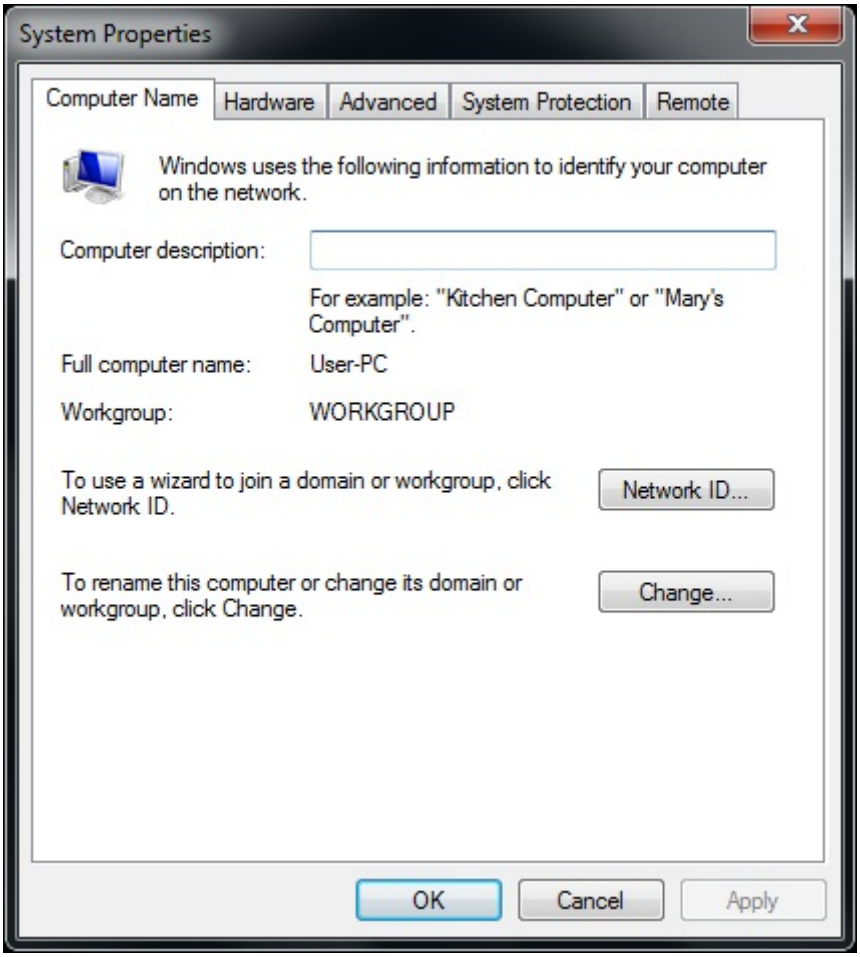



6. You must program a fixed IP address for each of the master and slave computers. On the workstation computers, a fixed IP address is not required if your network supports DHCP. The **Obtain an IP address automatically** radio button can be selected for the workstation computers (not applicable for master and slave computers).
7. On the master and slave computers, select **Use the following IP address** radio button.
8. Program the **IP address** and **Subnet mask** uniquely for each master and slave computers. Do not guess the **IP address** and **Subnet mask** values. Ask the network administrator for the proper settings.
9. Program the **Default gateway** if all computers are not on the same LAN segment. Obtain this setting from the network administrator. Many sites do not require a gateway setting.
10. Click the **[OK]** button.

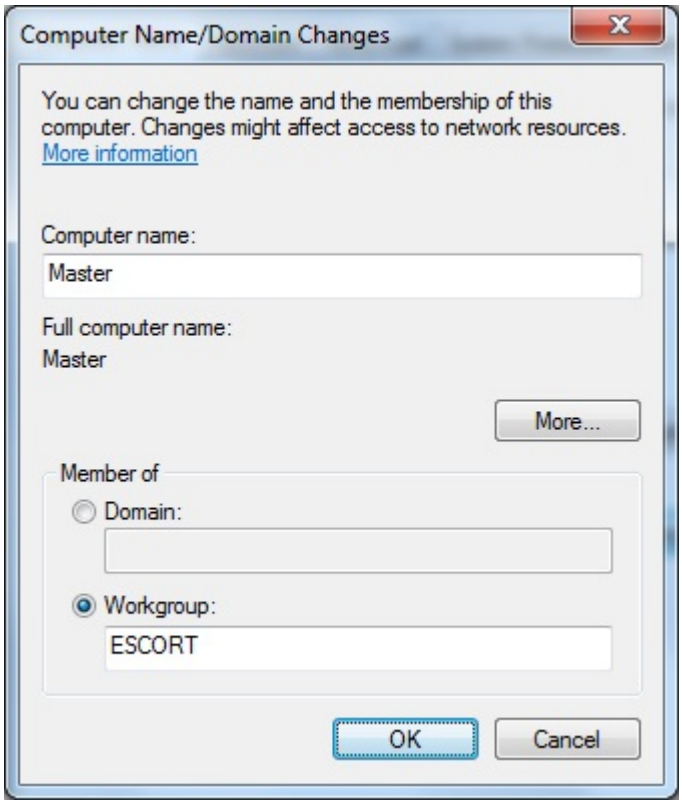
11. To set the Computer Name and Workgroup for the network, go to **Start > Control Panel > System**.




12. In the **Computer name, domain, and workgroup settings** group, click the **Change settings** link.



13. Click the **[Change]** button to change the computer name and workgroup. The **Identification Changes** dialog appears.




14. Assign a unique computer name (perhaps “MASTER” for the master computer and “SLAVE” for the slave computer) for each computer.
15. Under the **Member of** section, select the **Workgroup** radio button and assign a workgroup name, which can be any name (the same workgroup must be used for all workstations, slave, and master computers).
16. Click the **[OK]** buttons to return to the desktop.

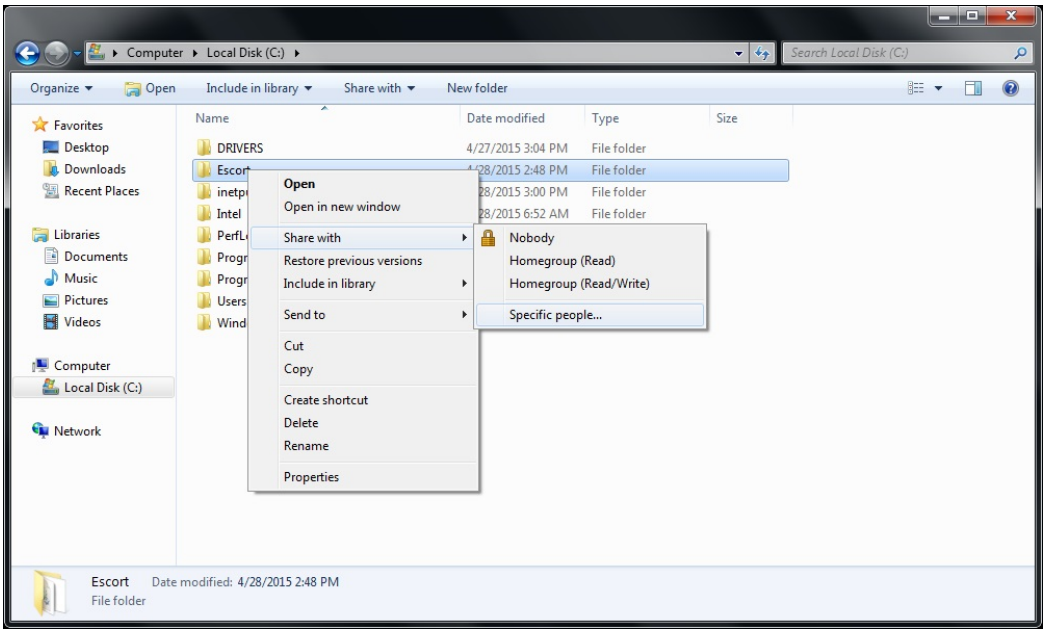
## 7.3 Install the Security Escort software on the master and slave computers

On the master and slave computers only, install the Security Escort program if not already installed (typically in the “C:\ESCORT” folder). At the end of the install process, do not run the Security Escort program.

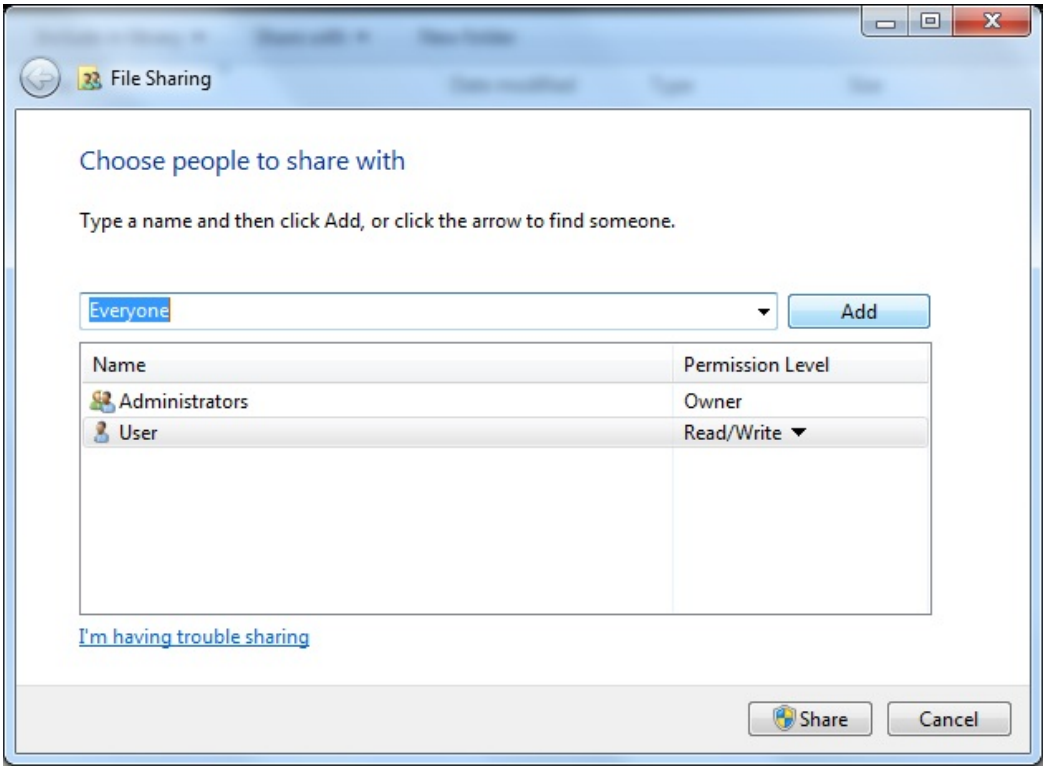
## 7.4 Configure the Security Escort folder to be shared

1. From the master computer, double-click the **Computer** icon and select the Security Escort folder where you have just installed it (typically “C:\ESCORT”).

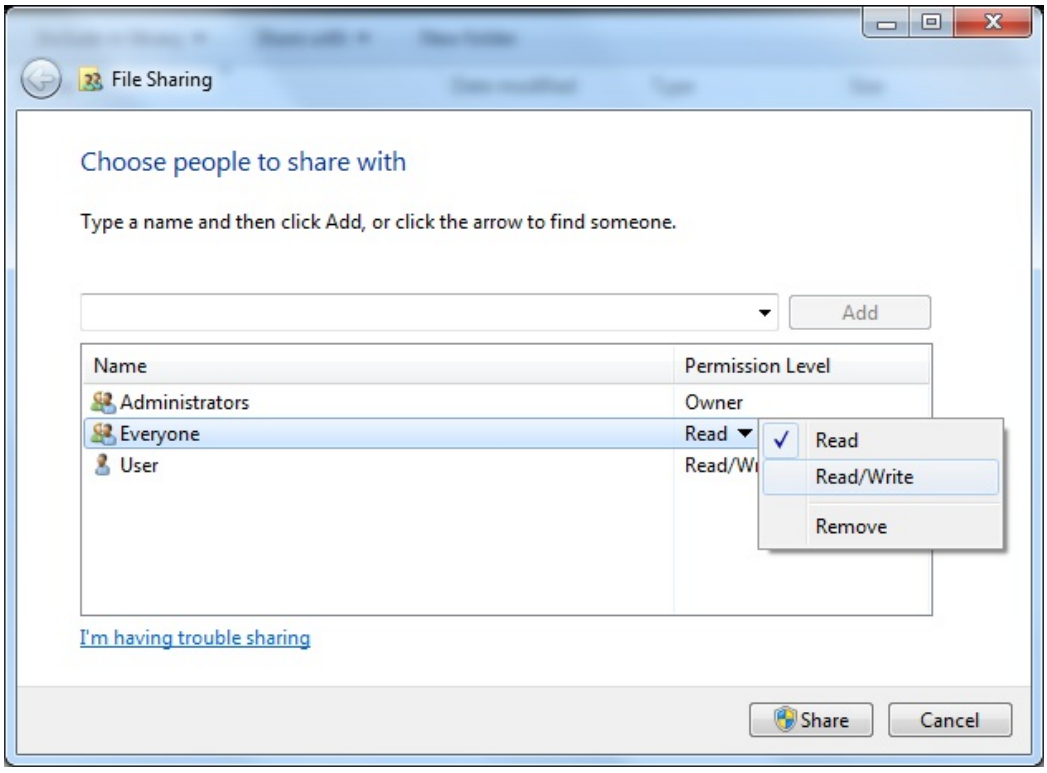
2. Click on the Security Escort folder icon with the right mouse button and a list of menu appears. Select **Share with > Specific people... menu** item.



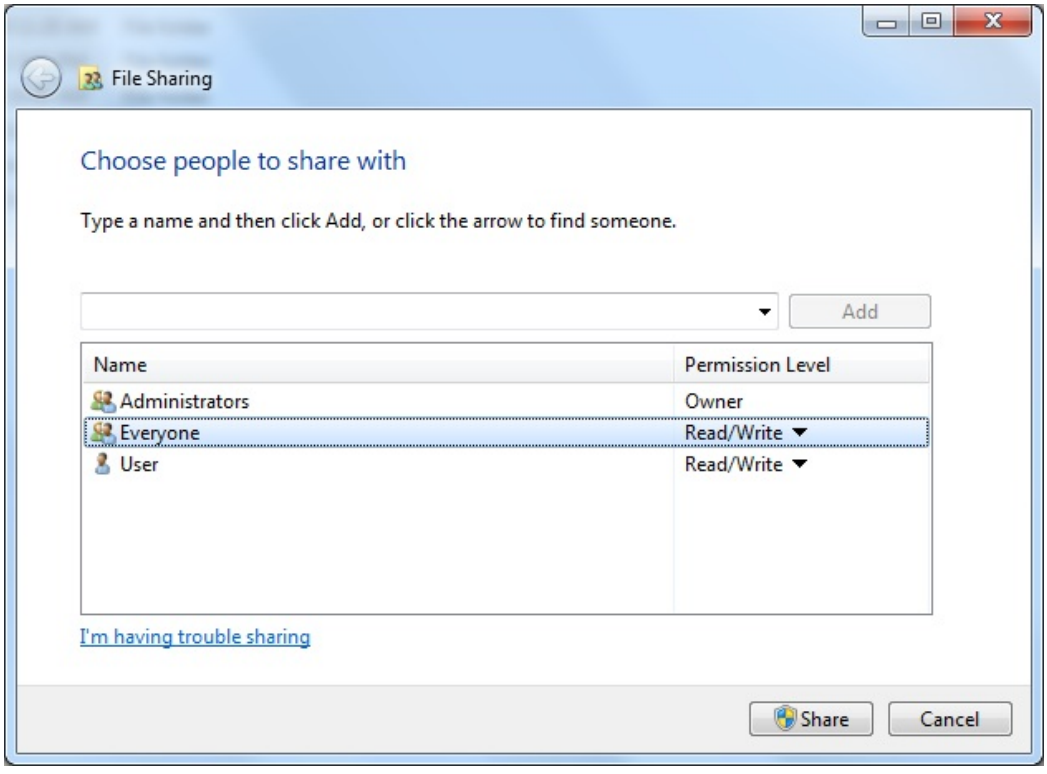

3. The **File Sharing** dialog appears. Click the drop-down list and select “Everyone”. Click the **[Add]** button to share the folder with “Everyone”. “Everyone” appears in the list with **Permission Level** set as “Read”.



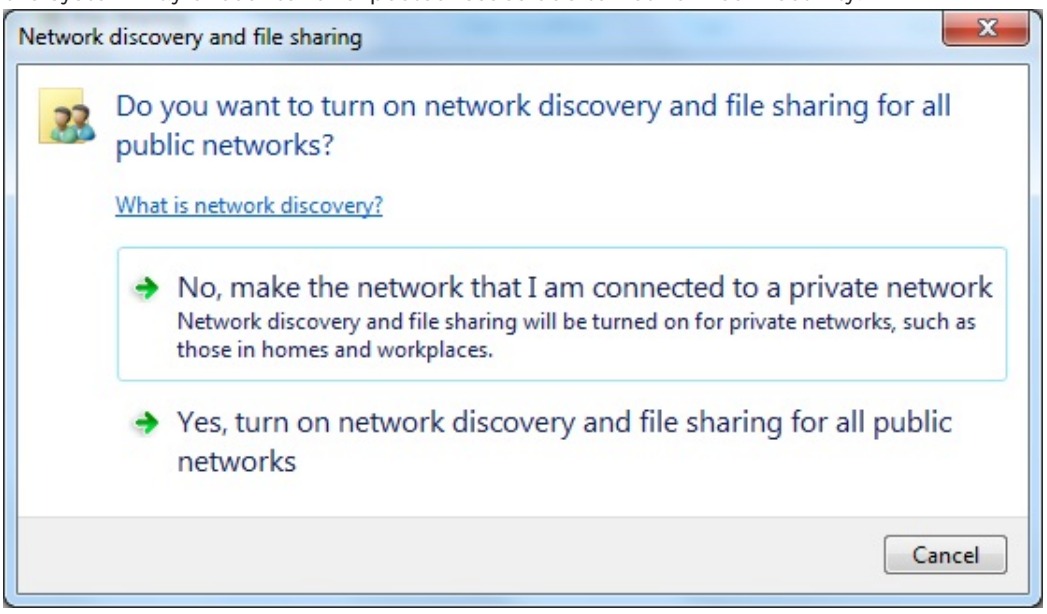
4. Click the **Read** drop-down button of “Everyone” and a list of menu appears. Select “Read/Write”. Repeat this step for each group that must have access to the Security Escort master database.



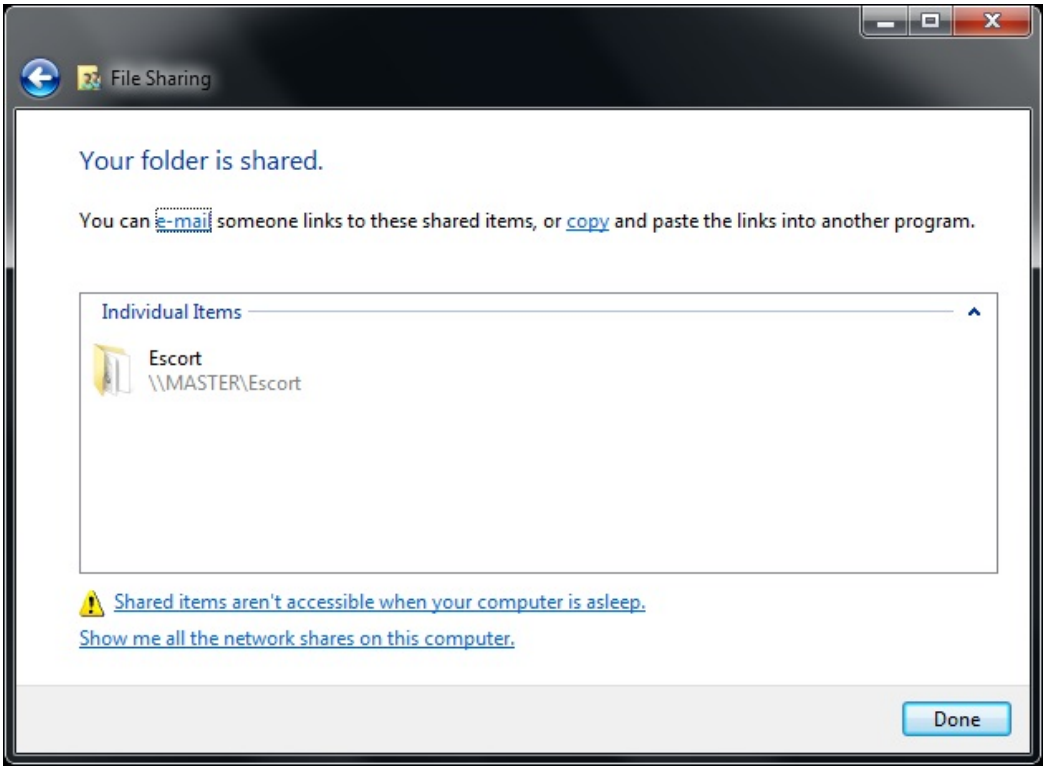

5. Click the **[Share]** button once all permissions have been assigned.



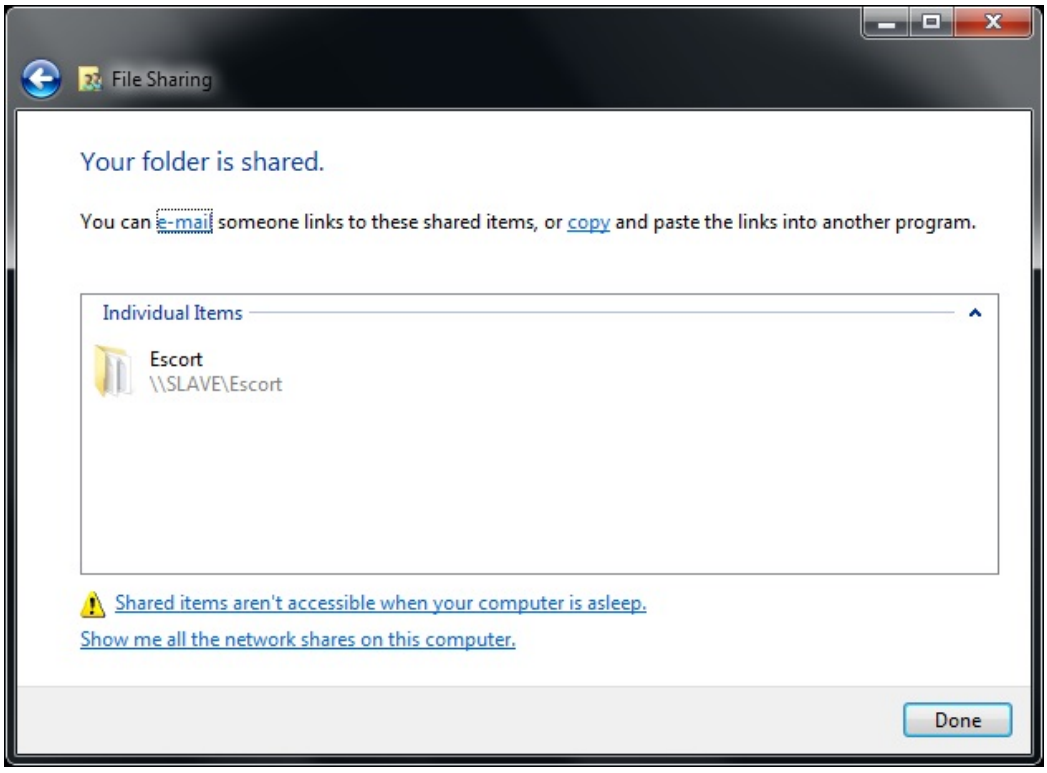
6. If network discovery and file sharing have not been turned on, the following dialog may appear. Select **Yes** to turn on the network discovery and file sharing option. Otherwise, the system may encounter unexpected issues due to network connectivity.




7. Once sharing is successful, a confirmation dialog appears with information of the shared link. Click the **[Done]** button to return to the desktop.



8. Repeat the steps above to share the slave computer's Security Escort folder. Similarly, if sharing is successful, a confirmation dialog as of below appears with the information of the shared link.

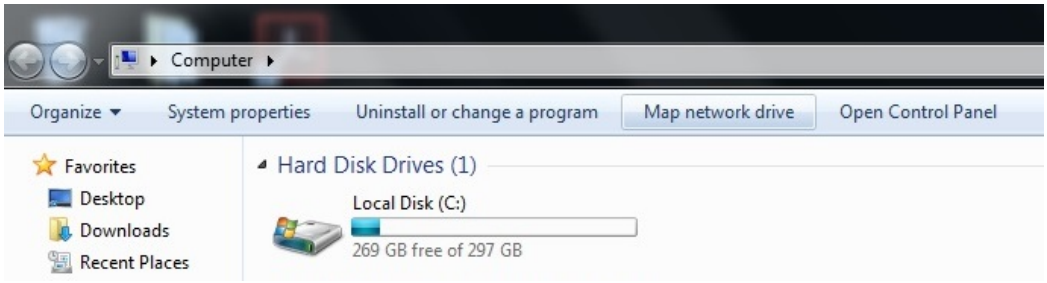



**Notice!**
Password-protected sharing is turned on by default. The person you want to share with must have a user account and password on your computer for full access to shared items. Password-protected sharing is located in the Window's **Control Panel** under **Advanced sharing settings**.

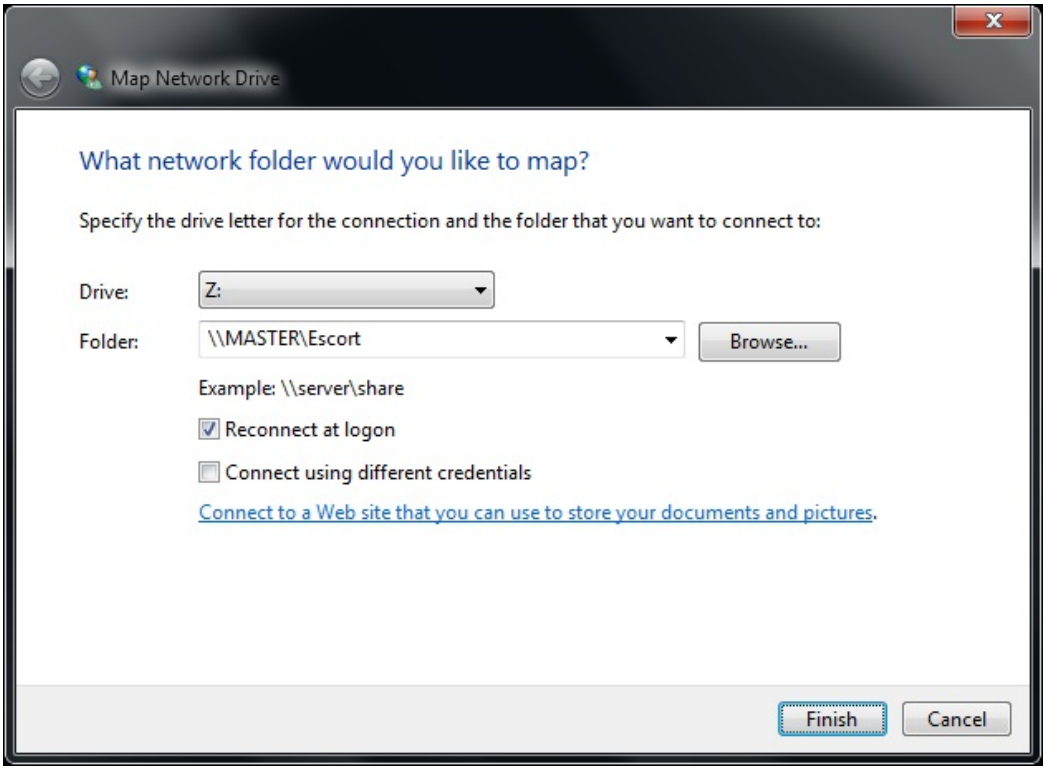
## 7.5 Map the master's network drive from each slave and workstation

**Notice!**
With version 2.04 of the software, it is possible to use UNC path names in the Security Escort software rather than mapping drive letters.

1. From each of the slave and workstation computers, go to menu **Start > Computer**. Select the **Map network drive** menu from the window.



2. The **Map Network Drive** dialog appears.

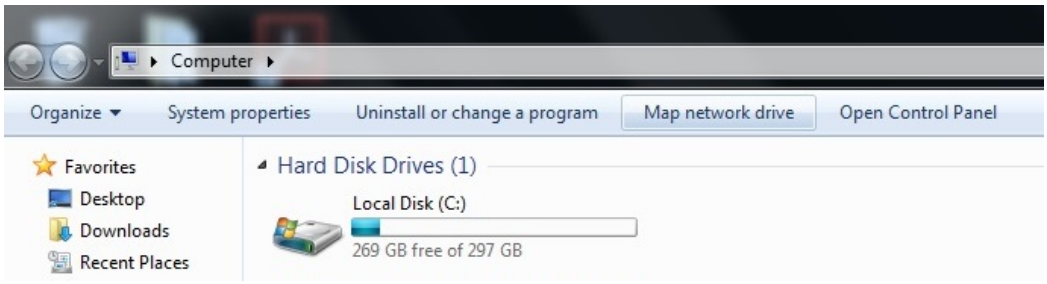



3. The **Drive:** field should already be filled with an available drive letter. This drive letter will be needed for setting up the database access in the Security Escort program on the slave and workstation computers. This drive letter can be different for the respective slave and workstation computers.
4. In the **Path:** field, type the path of the shared folder of the master computer, “\\MASTER \ESCORT”.
5. Check the **Reconnect at logon** checkbox.
6. Click the **[Finish]** button.
7. Windows Explorer will show a drive letter as ESCORT(\\MASTER), the shared folder on the master computer.
8. To verify the connection on the slave or workstation computer, double-click the drive. Look for the a_audit.txt file, and double-click it.
9. If you are able to open it successfully, there are no issues with the connection. Close the file and repeat the mapping of the drive for every slave and workstation computers. If there are errors or issues, you need to rectify them before you will be able to use the workstation computers with Security Escort.

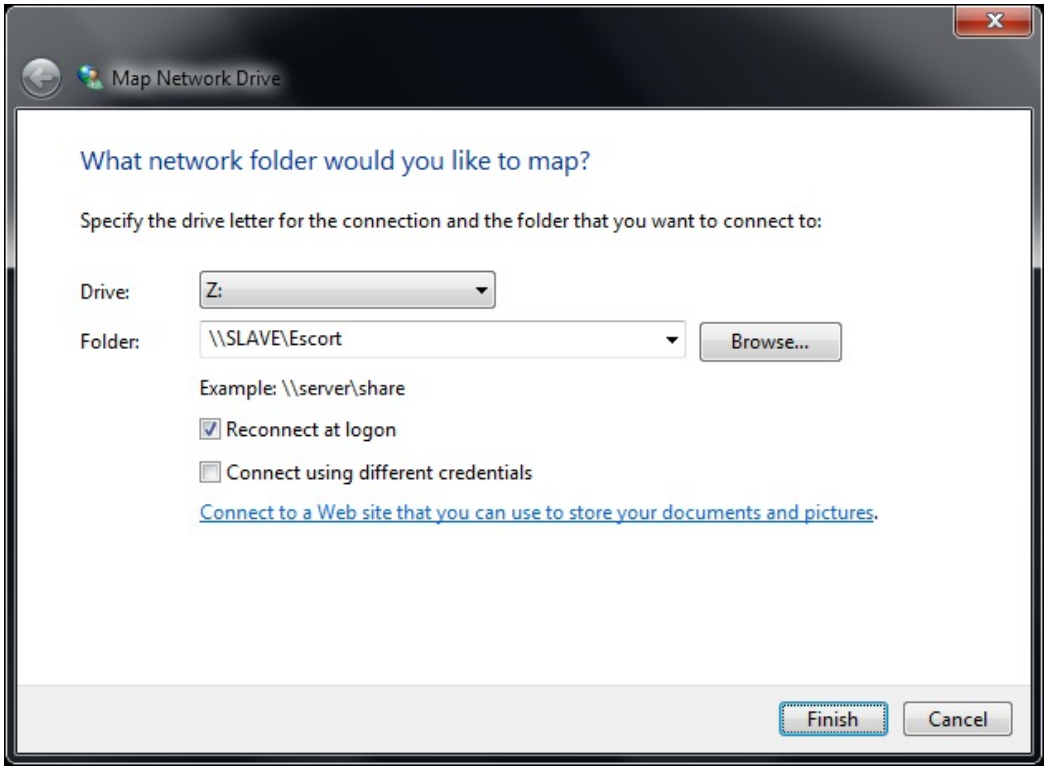
## 7.6 Map the slave’s network drive from each master and workstation

**Notice!**
With version 2.04 of the software, it is possible to use UNC path names in the Security Escort software rather than mapping drive letters.

1. If a slave computer is used in this system, from each of the master and workstation computers, go to menu **Start > Computer**. Select the **Map network drive** menu from the window.



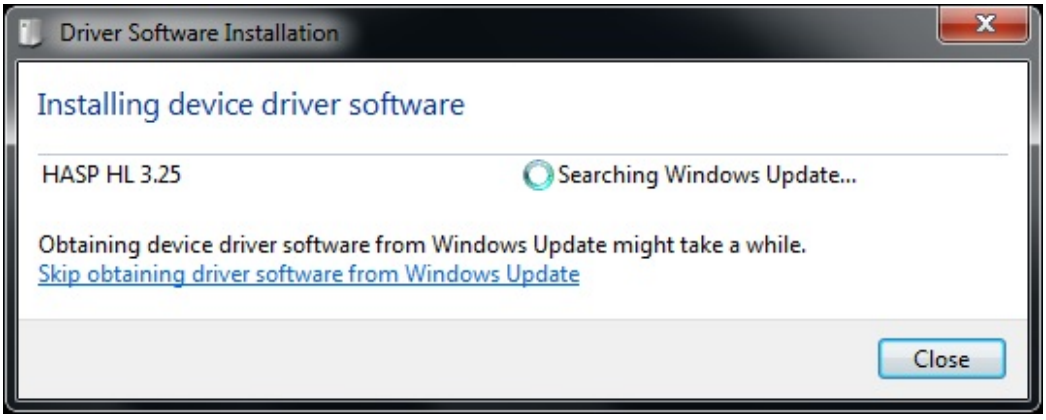

2. The **Map Network Drive** dialog appears.



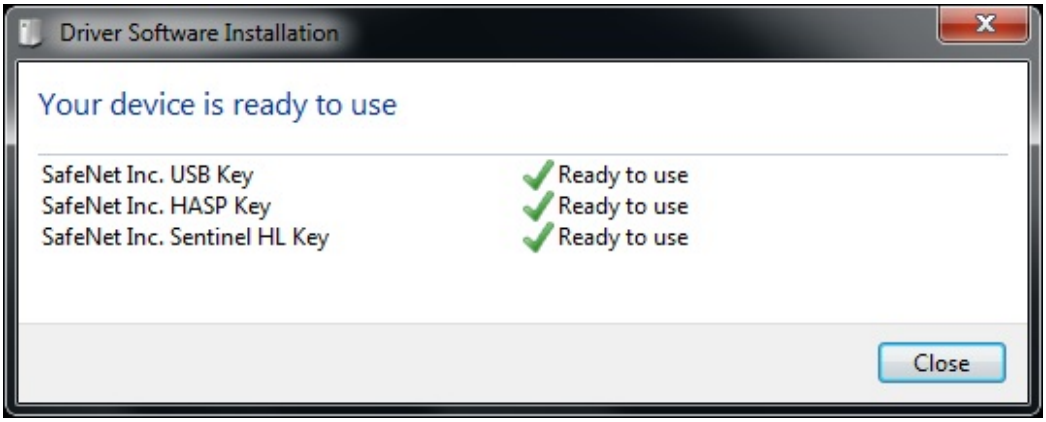

3. The **Drive:** field should already be filled with an available drive letter. This drive letter will be needed for setting up the database access in the Security Escort program on the master and workstation computers. This drive letter can be different for the respective master and workstation computers.
4. In the **Path:** field, type the path of the shared folder of the master computer, “\\SLAVE \ESCORT”.
5. Check the **Reconnect at logon** checkbox.
6. Click the **[Finish]** button.
7. Windows Explorer will show a drive letter as ESCORT(\\SLAVE), the shared folder on the slave computer.
8. To verify the connection on the master or workstation computer, double-click the drive. Look for the a_audit.txt file, and double-click it.
9. If you are able to open it successfully, there are no issues with the connection. Close the file and repeat the mapping of the drive for every master and workstation computers. If there are errors or issues, you need to rectify them before you will be able to use the workstation computers with Security Escort.

## 7.7 Install the software key on the master computer

1. Return to the master computer and plug the software key into the USB port.
2. Windows will automatically detect the device and attempts to search and install the driver software.



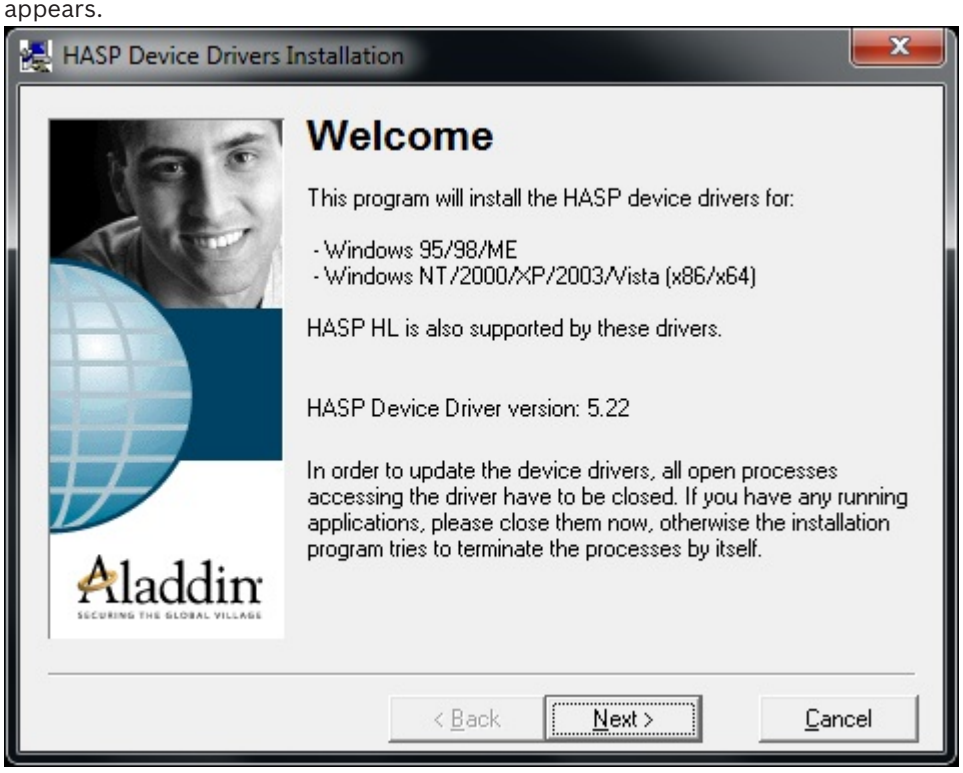

3. If the driver is found, it will be installed and Windows will confirm that the device is ready to use.



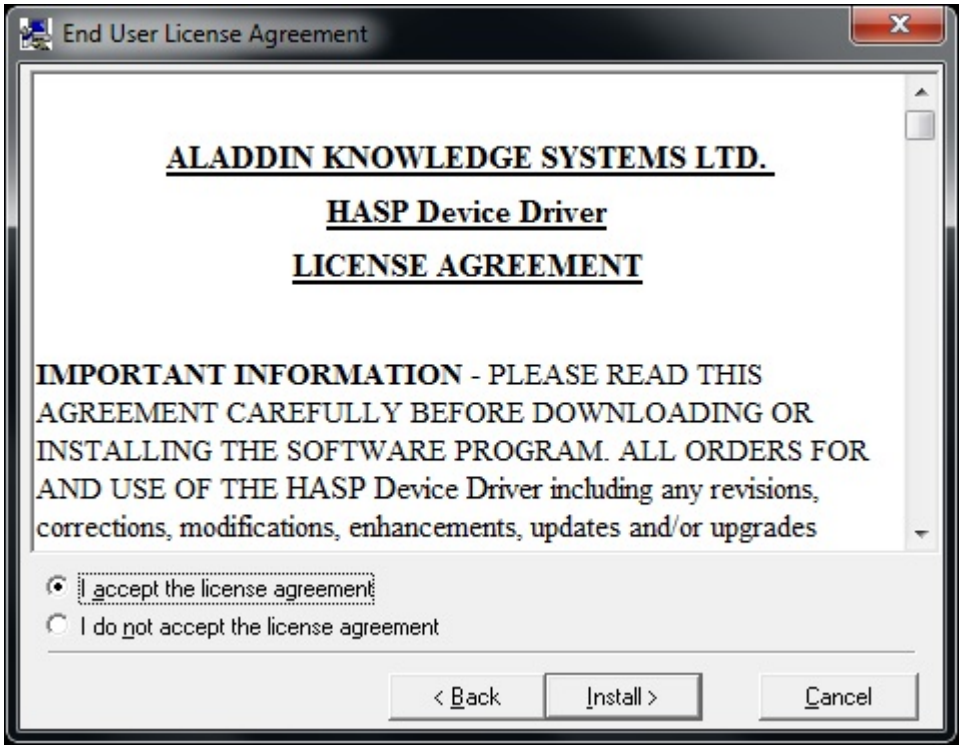

If there are issues with the driver installation, there will be a warning message. The device will not be usable, and additional steps need to be taken to install the driver.

4. Click the **[Close]** button to return to your desktop.

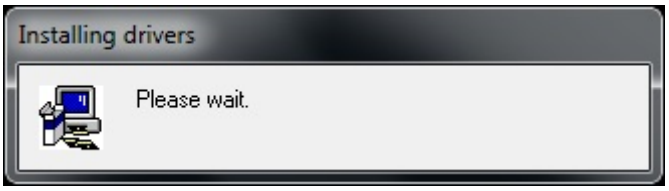
5. **If there are no issues and the device is ready to use, skip the following steps and proceed to step 9.** Otherwise, go to the “C:\ESCORT” folder and double-click the **HDD32.EXE** program to install the driver. The **HASP Device Drivers Installation** dialog appears.



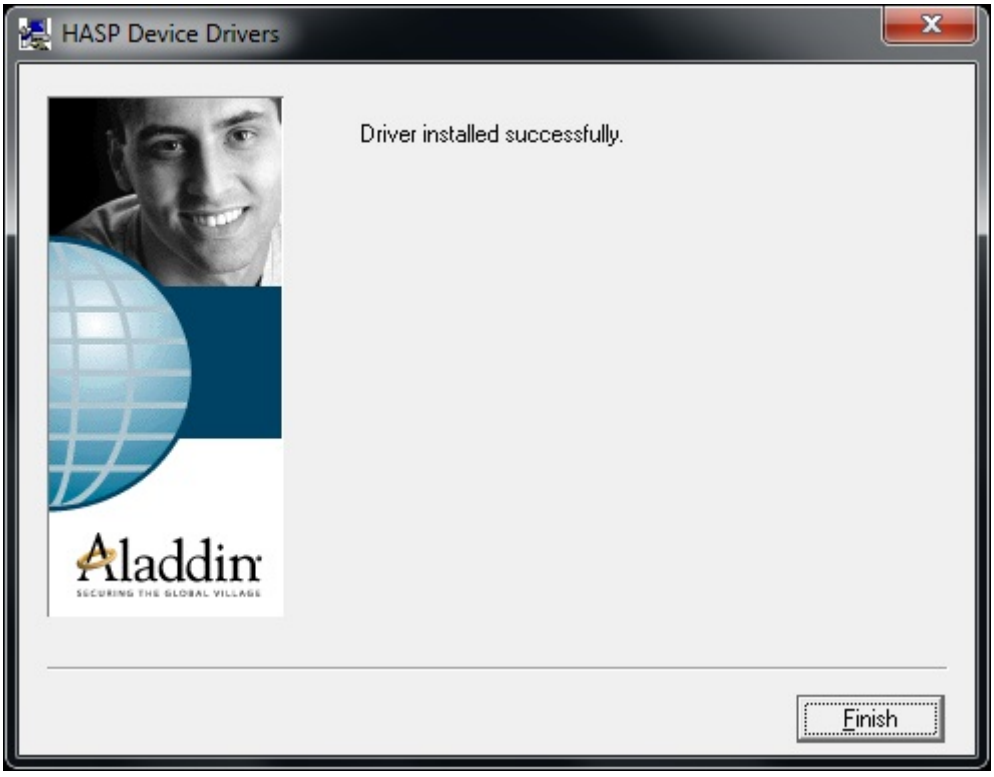

6. Click the **[Next >]** button. The **End User License Agreement** dialog appears.



7. Accept the license agreement by clicking the radio button accordingly. Click the **[Install >]** button to proceed with installation.

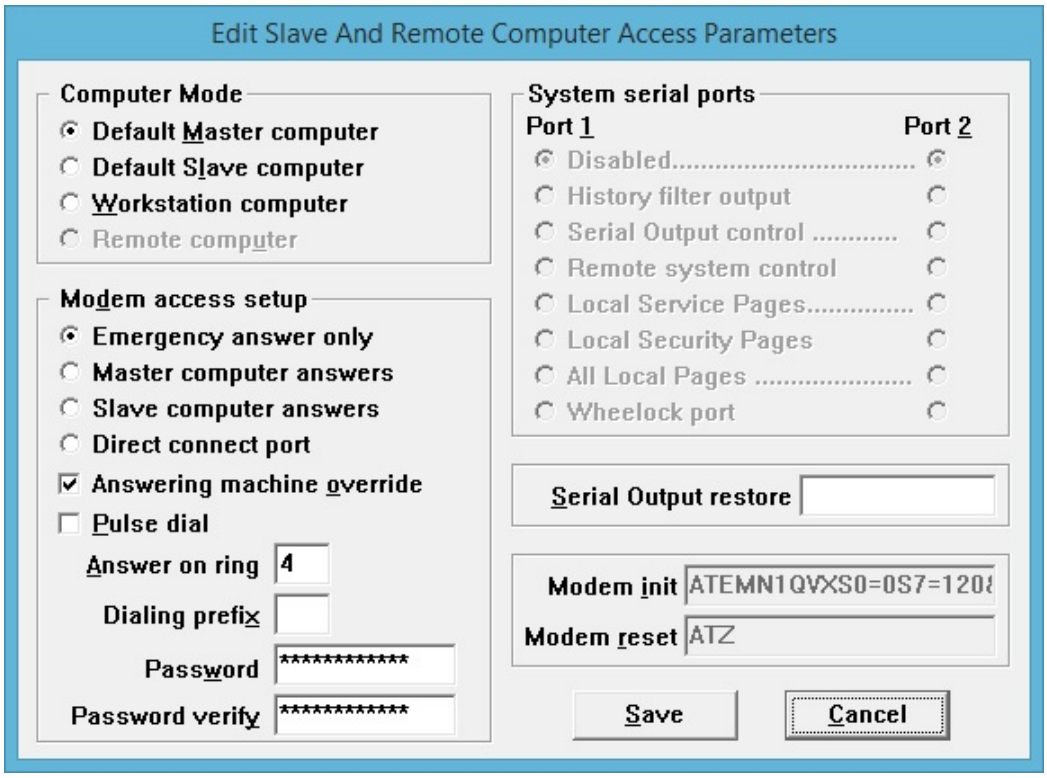



8. Once the driver has been installed successfully, a confirmation dialog appears. Click the **[Finish]** button to return to your desktop.




9. Start the Security Escort program (ESC32.EXE).
10. Go to menu **Setup > Remote setup**.

11. Verify that **Default Master computer** option is selected. Otherwise, select the **Default Master computer** option and click the **[Save]** button.




12. Exit the Security Escort program and restart it.
13. The program should not be running in the demo mode. If it is running in demo mode, there could be some issues with the software key, the HDD32.EXE installation, or the USB port configuration. This must be corrected before you continue. Otherwise, the Security Escort system will not communicate with the slave, workstation computers, or transponders.

## 7.8 Configure the Security Escort software

Firstly, assign the computers accordingly as the default master, the default slave or the workstation computers by selecting the menu **Setup > Remote Setup**.

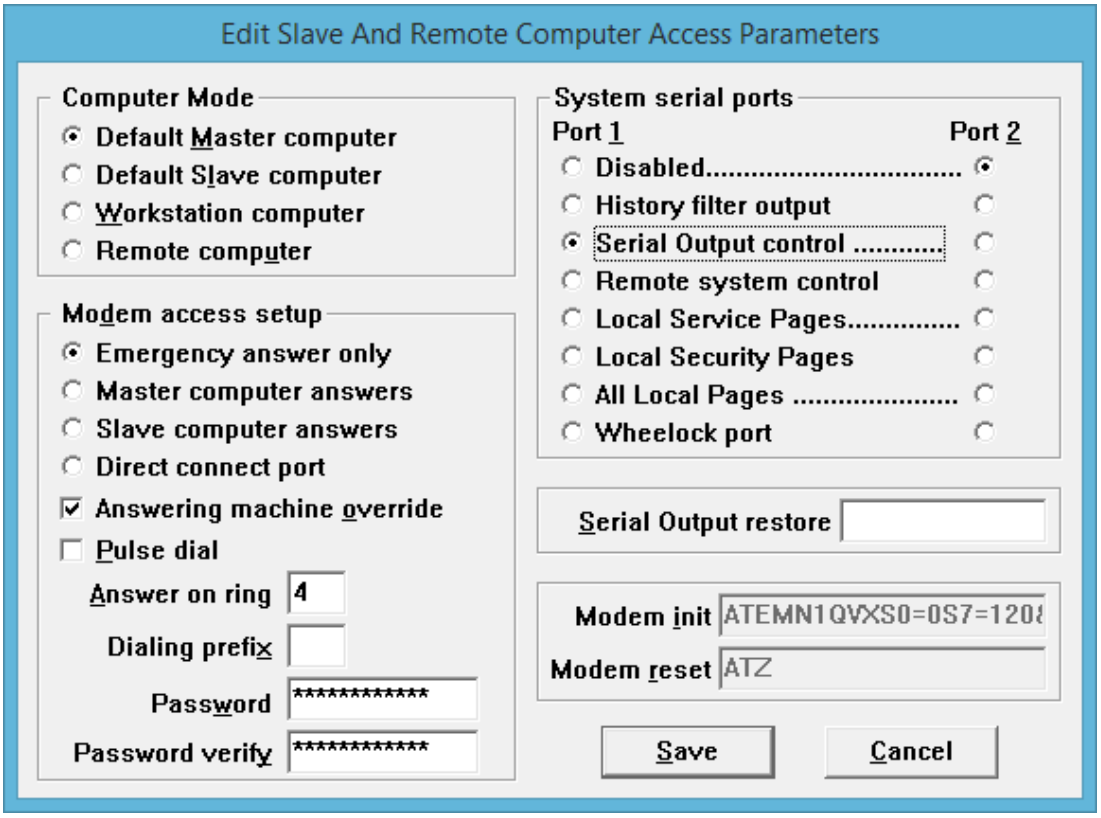



**Figure 7.1: Remote Setup Dialog**

Use this dialog to set up the network IP addresses, ports and related options. File paths can also be configured.

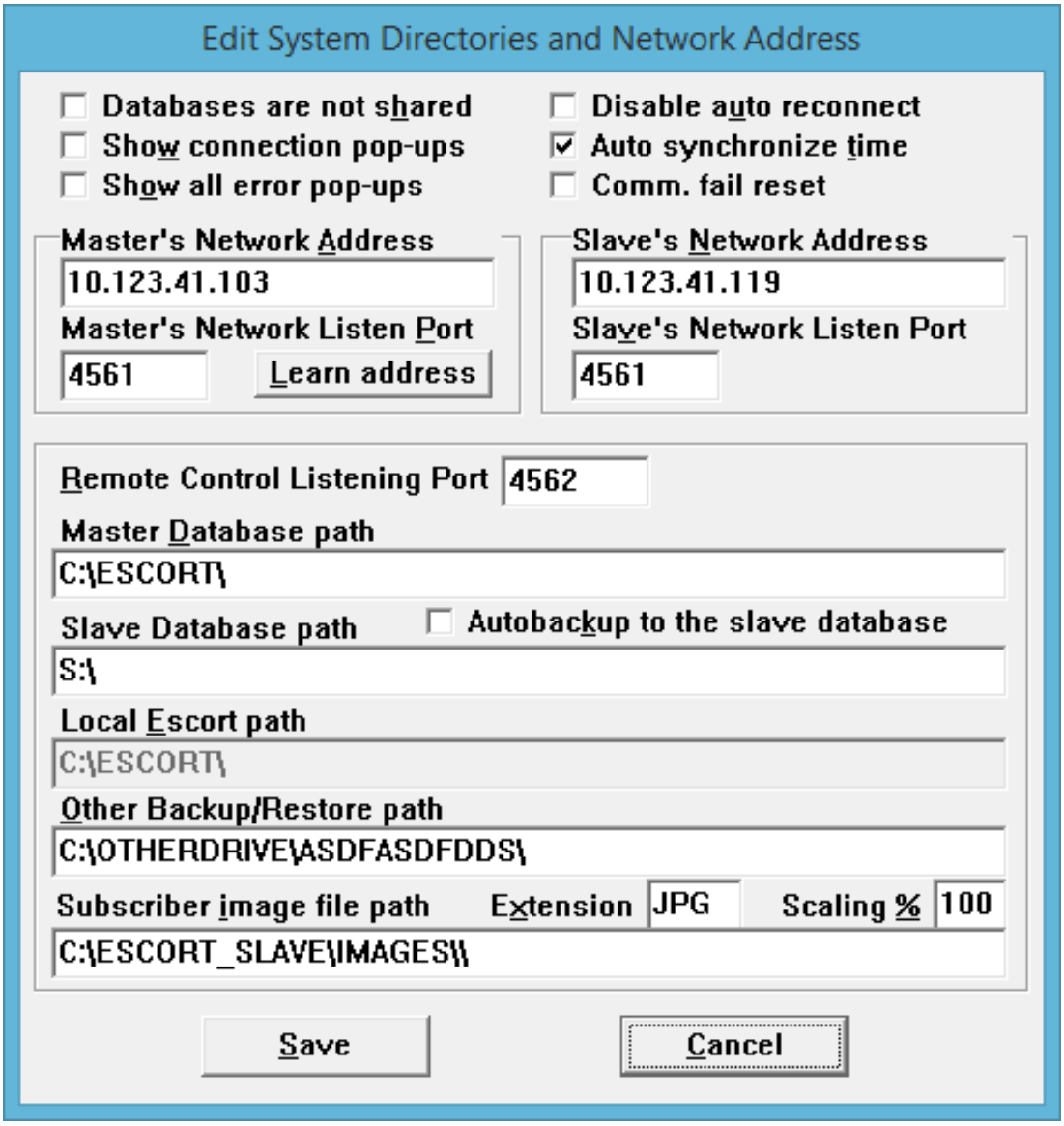



**Figure 7.2: System Directories and Network Address Dialog**

**Databases are not shared** If this option is not checked, the master and all the slave and workstation computers share the same database files. This checkbox must only be checked if each computer has its own copy of the databases stored locally. In normal operation, this checkbox is typically unchecked. If this checkbox is checked, the databases must be manually updated using **Backup** and **Restore** every time changes are made to the database.

**Show connection pop-ups** If this option is checked, it will display a pop-up message box whenever a network connection is initiated or released with another computer. Unchecking this checkbox stops the message boxes from displaying. In normal operation, this checkbox is typically unchecked.

| | |
|---|---|
| **Show all error pop-ups** | If this option is checked, it will display a pop-up message box whenever a network error is reported. Unchecking this checkbox stops the message boxes from displaying. In normal operation, this checkbox is typically unchecked. |
| **Disable auto reconnect** | If this option is checked, the system will not automatically attempt to reconnect a lost connection each minute. Unchecking this checkbox allows the system to automatically reconnect a lost connection. In normal operation, this checkbox should be unchecked. |
| **Auto synchronize time** | If this option is checked, the master computer will automatically synchronize the time on the slave and workstation computers once each night. |
| **Comm. fail reset** | If this option is checked, the master computer will reset when communication failure occurs.. |
| **Master's Network Address:** | The IP address of the master computer. The Security Escort system requires a fixed IP address for the master computer. |
| **Master's Network Listen Port** | A unique number that indicates the Security Escort software is attempting to set up a connection. Other software uses different port numbers, allowing the network interface card to be shared with other network applications. Typically, this is set as “4561”. |
| **Slave's Network Address** | The IP address of the slave computer. The Security Escort system requires a fixed IP address for the optional slave computer. |
| **Slave's Network Listen Port** | A unique number that indicates the Security Escort software is attempting to set up a connection. Other software uses different port numbers, allowing the network interface card to be shared with other network applications. Typically, this is set to “4561”. |
| **[Learn address]** | Clicking this button on the master computer automatically populates the master’s IP address in the **Master’s Network Address** textbox, and the master’s network port in the **Master’s Network Listen Port** textbox. Clicking this button on the slave computer automatically populates the master’s IP address in the **Slave’s Network Address** textbox, and the master’s network port in the **Slave’s Network Listen Port** textbox. If the computer has more than one network interface card (NIC), you must verify that the correct IP address was selected by comparing this address to the IP address that was programmed in the Control Panel TCP/IP protocol. If the address is not correct, manually enter the correct IP address. |
| **Remote Control Listening Port** | The Security Escort will be listening on this port to communicate with the OPC server. A separate OPC server is created to communicate between the OPC client and the Security Escort system. The OPC server holds the alarm and trouble messages, and sends the same to the available client once it is connected. The OPC server will send the status of the Security Escort to the |

OPC client. The OPC sever also acknowledges and deletes alarm and trouble messages from OPC client. If the connection between OPC server and Security Escort goes down, the OPC server will try to reconnect with Security Escort. Once the connection to the Security Escort becomes active, the Security Escort will send all the available alarms to the OPC server. The OPC server in turn sends the alarm back to OPC client; hence the OPC client may display some duplicate alarms.

**Master Database path** The path that this slave or workstation computer uses to access the shared database files on the master computer. This path may have a different drive letter on the different slave and workstation computers. They are typically on the master computer, but they may be on a file server or any other network accessible drive. **Note: With version 2.04 and above of the software, it is possible to use UNC path names instead of mapping drive letters. Therefore, the path to the master computer's database would be "\\MASTER\ESCORT".**

**Autobackup to the slave database** If this option is checked, the slave computer will back up all databases in the **Master Database path** to the **Slave Database path** each night at 3:00 am.

**Slave Database path** The path that this master or workstation computer uses to access the hot backup database files on the slave computer. This path may have a different drive letter on the different master and workstation computers. They are usually on the slave computer, but they may be on a file server or any other network accessible drive. Typically, they would not be stored on the same computer as the **Master Database path**, so a single failure would not prevent access to both the master and slave database files. **Note: With version 2.04 or above of the software, it is possible to use UNC path names instead of mapping drive letters. Therefore, the path to the slave computer's database would be "\\SLAVE\ESCORT".**

**Local Escort path** The path on this workstation where the Security Escort was installed in. Typically it is "C:\ESCORT".

**Other Backup/Restore path** When backing up the database to or restoring it from external disks, this is the path that is used.

**Subscriber image file path** The Security Escort System software can display an image for each subscriber on the alarm screen. This parameter tells the software the path where the image files are stored. The default is "C:\ESCORT\IMAGES".

**Extension** The subscriber images can be in JPEG or Windows Bitmap format. All images in a system must be in the same format. For the JPEG format, enter the Windows extension "JPG". For the Bitmap format, enter the Windows extension "BMP".

**Scaling %** When the display is set to 640x480 pixels, and subscriber images are being displayed, this parameter controls the image size. This value can range from 10 to 100%, and should be adjusted while viewing alarms to get the desired image size. When the display is set to 800x600 or larger (recommended), this parameter has no effect.

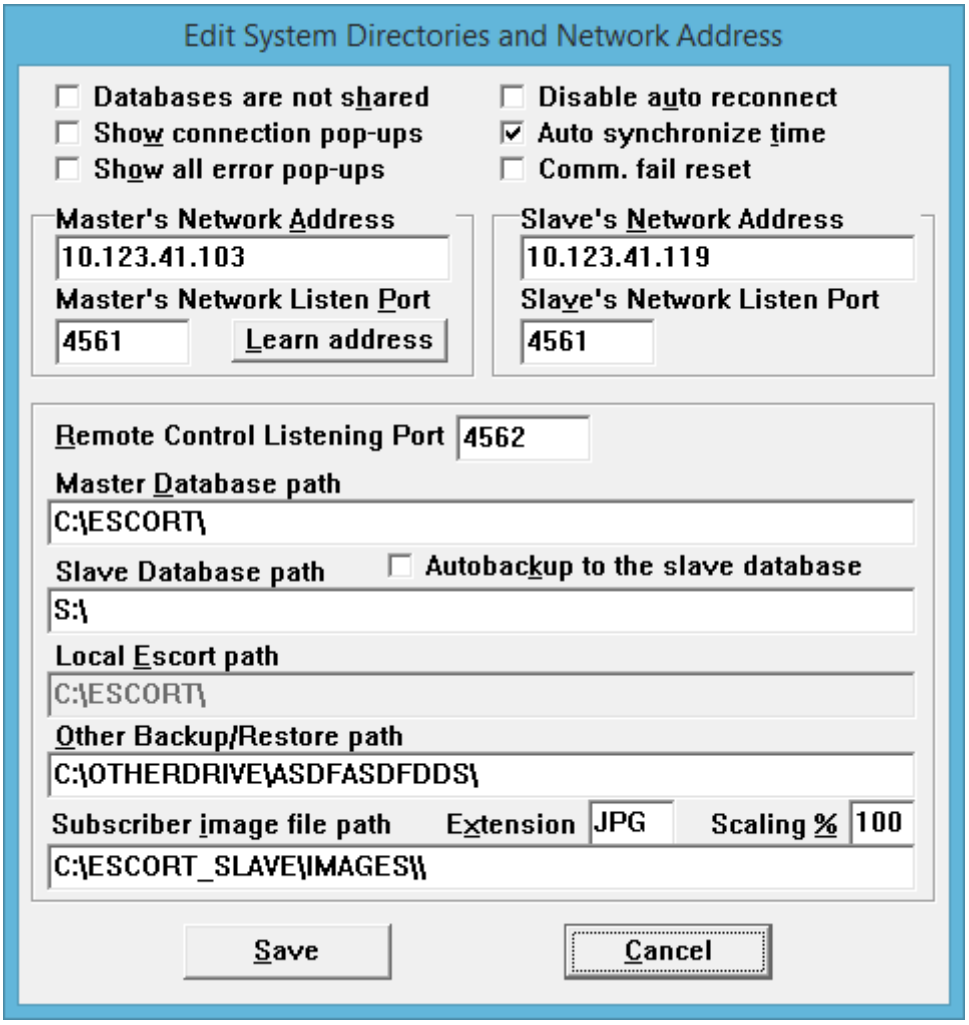
**[Save]** Clicking this button saves the changes and closes the dialog window.

**[Cancel]** Clicking this button aborts the changes and closes the dialog window.

The following section shows how to use these dialogs to configure the software on the master, slave and workstation computers.

### 7.8.1 Configure the software on the master computer

1. On the master computer, go to menu **Network > System directories and network address...**.




2. Ensure that the **Databases are not shared** checkbox is unchecked. The **Show connection pop-ups** and **Show all error pop-ups** checkboxes can be checked while the network is being set up and verified. Typically, they are unchecked in normal operation.

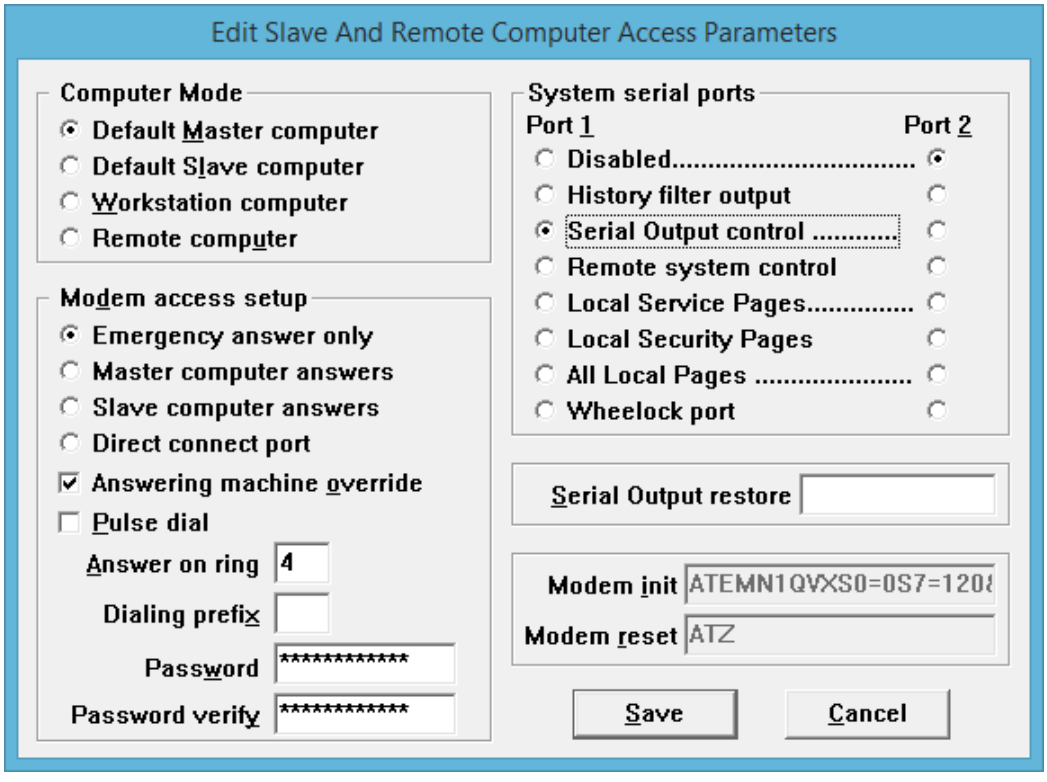
3. Click the **[Learn address]** button to automatically populate the **Master's Network Address** textbox. This information should be the same IP address that was programmed in the network control panel TCP/IP protocol for the master computer's network card. In the **Master's Network Listen Port** textbox, key in "4561". (This can be any number from 2000 to 65535 that is not already used by another program. It is unlikely that there will be conflicts with this number.)
4. The database path should already be set to "C:\ESCORT". The image path should already be set to "C:\ESCORT\IMAGES".
5. If the Security Escort system is using shared database, enter the mapped drive letter or the UNC path of the slave's shared folder in the **Slave Database path** textbox.
6. Click the **[Save]** button, exit Security Escort, and restart the program.

**Notice!**
If Security Escort is using mapped share folders on Windows 8 or 8.1, you need to run it as an administrator.

7. Make any other changes to the Security Escort settings you want.

### 7.8.2 Configure the software on the slave computer

1. Run the Security Escort program on the slave. Select menu **Setup > Remote Setup**.




2. Verify that **Default Slave computer** is selected. If it is not, select **Default Slave computer** and click the **[Save]** button. Terminate the Security Escort program and restart it.
3. Go to menu **Network > System directories and network address...**. Do not change the settings of the **Databases are not shared**, **Show connection pop-ups**, or **Show all error pop-ups** options.
4. Information of the **Master's Network Address** and **Master's Network Listen Port** should already be populated automatically when the master computer was already set up and established. If the information is incorrect, enter them manually.

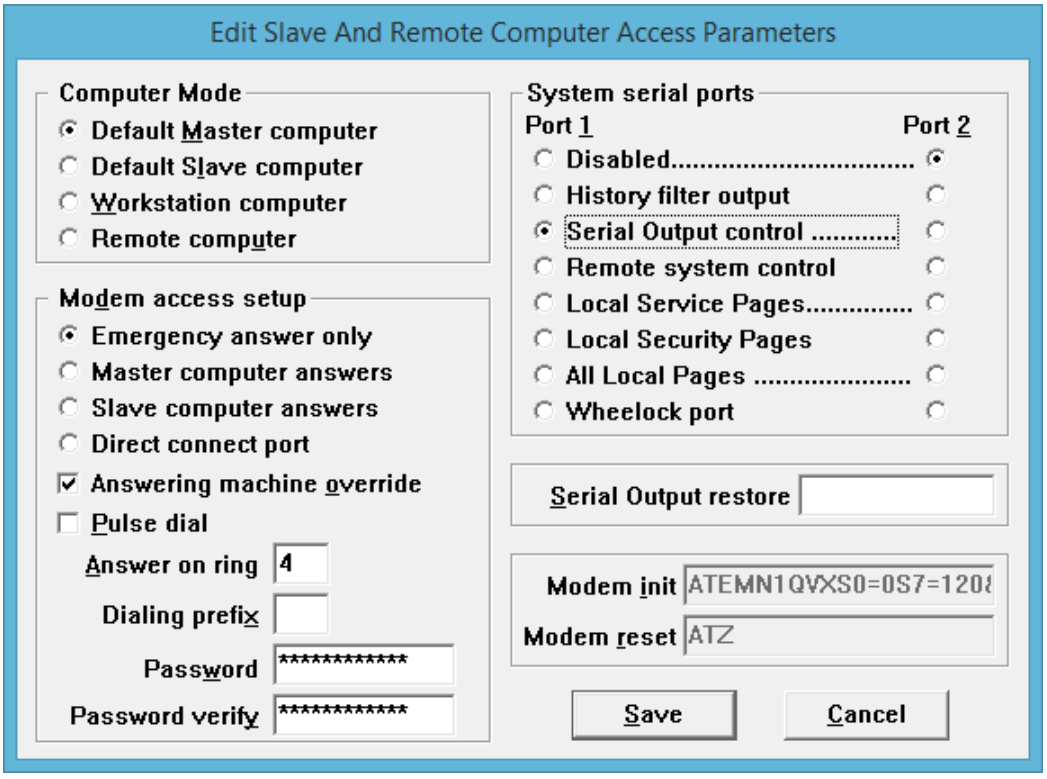
5. Click the **[Learn address]** button to populate the **Slave's Network Address** or **Slave's Network Listen Port** information. If the information is incorrect, enter them manually.
6. Enter the mapped drive letter or UNC path of the master's shared folder in the **Master's Database path** textbox.
7. The **Subscriber image file path** can be left as "C:\ESCORT\IMAGES" if images of the subscribers are not used, or are stored locally. If the images are stored only on the master, change this to the mapped drive letter or UNC path of the master's shared folder.
8. Click the **[Save]** button, exit Security Escort, and restart the Security Escort program. Most likely you do not need to make any other preferences changes at the slave computer.

**Notice!**
If Security Escort is using mapped share folders on Windows 8 or 8.1, you need to run it as an administrator.

9. When Security Escort restarts on the slave computer, the caption bar on both the slave and master computer should indicate that there is a connection.
10. Try an alarm, making sure it appears on all computers and can be acted on from any computer.

### 7.8.3 Configure the software on the workstation computers

1. Install Security Escort on each workstation computer.
2. Run the Security Escort program on the workstation computer. Select menu **Setup > Remote Setup**.




3. Verify that **Workstation computer** is selected. If it is not, select **Workstation computer** and click the **[Save]** button.
4. Terminate the Security Escort program and restart it.

5. Go to menu **Network > System directories and network address...**. Do not change the settings of **Databases are not shared**, **Show connection pop-ups**, **Show all error pop-ups, Master's Network Address**, **Master's Network Listen Port, Slave's Network Address**, or **Slave's Network Listen Port** fields.
6. Enter the mapped drive letter or UNC path of the master's shared folder in the **Master's Database path** textbox.
7. The **Subscriber image file path** can be left as "C:\ESCORT\IMAGES" if images of the subscribers are not used, or are stored locally. If the images are stored only on the master, change this to the mapped drive letter or UNC path of the master's shared folder.
8. Click the **[Save]** button, exit Security Escort, and restart the Security Escort program. Most likely you do not need to make any other preferences changes at the workstation computer.

**Notice!**
If Security Escort is using mapped share folders on Windows 8 or 8.1, you need to run it as an administrator.

9. When Security Escort restarts on the workstation computer, the caption bar should indicate there is a connection with both the slave and master computer if they are online.
10. Try an alarm, making sure it appears on all computers and can be acted on from any computer.

# 8 Troubleshooting

Security Escort uses two network connections between the master computer and the slave computer and workstations.
The retrieve database access to all the Security Escort databases is through the Micro Kernel Database Engine (MKDE). The MKDE on each computer automatically opens a connection to the master databases. The path to the master databases is defined under the **Network** menu in the **System Directories and Network Address** dialog as the **Master Database Path** textbox.
The second connection is through a TCP/IP socket that the slave computer or workstation opens to the master. The IP address and port to the master computer is defined under the **Network** menu in the **System Directories and Network Address** dialog as the **Master's Network Address** textbox and the **Master's Network Listen Port** textbox. There is also a similar address and port for the slave computer.
Stored with the master database path is the global preference file (gprefers.edb). The Security Escort application on the master computer must be run first. Under the **Network** menu in the **System Directories and Network Address** dialog, click the **[Learn Address]** button. This automatically fills in the **Master's Network Address** and the **Master's Network Listen Port** textboxes". Save the change. This places the master's network address and port in the global preferences file.
When the slave and workstation computers are first started, set the path to the master database under the **Network** menu in the **System Directories and Network Address** dialog as the **Master Database Path** textbox. When the path is set, shut down the Security Escort application without making any other changes and restart it. The slave or workstation computer then reads the software key information and the master's network address and port from the global preferences file. This allows the **Operator Database** to open successfully and the network connection to open to the master computer.

## 8.1 "CAN'T OPEN THE OPERATOR.EDB FILE" error

If a yellow box is displayed with the message "Can't open the OPERATOR.EDB file," the file might be missing or corrupt, the software key or its driver might not be installed, or the database manager might not be loaded. To correct, use the Restore or Install buttons. If the slave computer cannot open the Operator database, check the following:

- Verify the master computer can access the databases by starting Security Escort first. Also verify the Security Escort software does not indicate it is running in "Demo" mode.
- Verify the correct type (default master computer, default slave computer or workstation computer) is set in the **Remote Setup** dialog under the **Setup** menu. There can be only one master computer and one slave computer in a system. Only the master computer has a software key installed.
- Check to see if the master database path is set up correctly in the **System directories and Network Address** dialog under the **Network** menu on both the slave and workstation computers. Confirm the drive letter used is the correct letter that was set up in the Map Network drive. You might have to double click the Security Escort icon and immediately press and hold down the <Ctrl>, <Shift>, and <Tab> keys on the keyboard. Do not release the keys until the **System directories and Network Address** dialog displays. Make any changes required and click the **[Save]** button. Repeat through all of the setup screens.
- Determine if the slave computer can access the shared drive on the master computer. We verified this access in the *Map the master's network drive from each slave and workstation, page 31* for the slave computer when we read the readme.txt file. Re-verify this connection and that you can read and write files (edit the readme.txt file remotely to test the ability to write).

- Determine if the slave computer can access the global preferences file (gprefers.edb) that is stored in the same directory as the OPERATOR.EDB file on the master computer.
- Determine if the master computer saved the global preferences correctly. Verify the preference settings on the master computer. Even if they appear correct, change something in the System directories and network address dialog on the master computer and click the Save button. This forces the global preferences to be rewritten. Now change the setting back to where it should be and click the Save button again.
- Verify the TCP/IP settings in the network control panel are correct.

## 8.2 Network connection fails

If the databases can be accessed and the Security Escort program starts up but indicates that a network connection failed:

- Check that the master and slave (if used) computers have a static IP address. The workstations can have dynamic IP addresses.
- Check to see if the **Master's Network Address** and **Master's Network Listen Port** fields are saved correctly in the **System directories and Network Address** dialog under the **Network** menu on the slave and workstation computers. Verify these preference settings on the master computer. Even if they appear correct, change something in the **System directories and network address** dialog on the master computer and click the **[Save]** button. This forces the global preferences to be rewritten. Now change the setting back to where it should be and click the **[Save]** button again.
- Stop and start the Security Escort program on the master computer. Then stop and start the Security Escort program on the slave computer.
- Confirm the **Slave's Network Address** and **Slave's Network Listen Port** fields are saved correctly in the **System directories and network address** dialog under the **Network** menu on the workstation computers.
- Try changing the **Master's Network Listen Port** number and click the **[Save]** button. If you do change the port number, exit the Security Escort program on the master computer and then restart it. Then restart the slave computers. Try port numbers in this order 4561, 5001, 6001, 7001, 8001, and so on.
- If the master and slave computers are on different LAN or WAN segments, verify the gateway setting in the TCP/IP section of the network control panel is correct.
- Verify the TCP/IP settings in the network control panel are correct. Database edits can be made from any computer and all computers instantly see the changes. If another computer has a database record open in the editor and another computer attempts to edit that record, the record is locked, a message pops-up, and you cannot edit the record from the second computer. Another computer cannot edit that record even after the first computer saved the record, until the first computer edits another record.

## 8.3 "THE MASTER COMPUTER MUST BE ON-LINE TO RETURN THE SYSTEM TO OPERATIONAL STATUS" message

This may be normal.

The system is designed to allow the slave and workstation computers to operate for about a week if the master computer fails. To accomplish this, the master computer writes specific data to the global preferences file each evening that is based on the software key and the time and date. The slave and workstation computers then read this data to determine if they are allowed to run a system. Until the master computer has run continuously over night with a valid software key attached, these specific values are not in the global preferences file. Therefore the "THE MASTER COMPUTER MUST BE ON-LINE TO RETURN THE SYSTEM TO

OPERATIONAL STATUS” message is displayed. Once the master computer has run overnight, this message disappears. If the master computer fails, has its software key removed, or is taken off-line, the “The slave computer has xxx hours of operation left before an operational master must be online” message appears. This happens when there is approximately four days of operation left.

# 9 Maintenance

## 9.1 Workstation and slave system synchronization

On successful connection with the workstation or slave, the master system sends a request to sync to the workstation or slave. On receiving the request, the workstation or slave deletes all its existing alarms and sends an acknowledgement to the master. On receiving the acknowledgement the master sends all the available alarms to the workstation or slave one by one.
After this sync at any point of time the slave, workstation and master will be having the same number of alarms.

## 9.2 Reloading database to the workstation or slave

When a workstation or slave system is not able to load the database from the master, a retry dialog box consisting of **[Silence]**, **[Retry]** and **[Terminate]** options appears. On displaying this dialog, an alarm sound will be generated. Clicking the **[Silence]** button will silence the sound, clicking the **[Retry]** button will give another try to access the database and clicking the **[Terminate]** button will quit from the application. At any point of time if the connection to the master database is successful, then the retry dialog box will close automatically.

# 10 Files required for Security Escort

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

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

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

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

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

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

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

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

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

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

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

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

# 11 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.

## 11.1 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.

## 11.2 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.

## 11.3 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.

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