SPECTRUM ENHANCED SECURITY (ES)

Administrator's Guide

PerkinElmer®

Release History

Part Number	Release	Publication Date
L1050100	D	September 2014

Any comments about the documentation for this product should be addressed to:

User Assistance
PerkinElmer Ltd
Chalfont Road
Seer Green
Beaconsfield
Bucks HP9 2FX
United Kingdom

Or emailed to: info@perkinelmer.com

Notices
The information contained in this document is subject to change without notice.
Except as specifically set forth in its terms and conditions of sale, PerkinElmer makes no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.
PerkinElmer shall not be liable for errors contained herein for incidental consequential damages in connection with furnishing, performance or use of this material.

Copyright Information
This document contains proprietary information that is protected by copyright.
All rights are reserved. No part of this publication may be reproduced in any form whatsoever or translated into any language without the prior, written permission of PerkinElmer, Inc.

Copyright © 2014 PerkinElmer, Inc.

Produced in the UK.

Trademarks
Registered names, trademarks, etc. used in this document, even when not specifically marked as such, are protected by law.

PerkinElmer is a registered trademark of PerkinElmer, Inc.
Spectrum, Spectrum ES, Spectrum Two, Frontier, Spotlight, RamanStation, RamanFlex, RamanMicro and Raman IdentiCheck are trademarks of PerkinElmer, Inc.
Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and other countries.
Spotfire is a registered trademark of TIBCO Software, Inc.

Contents

Introduction

About this Guide

This manual describes the installation and administration of Spectrum ES software.

NOTE: This manual also covers the administration of Spectrum Quant ES, which is installed as part of the Spectrum ES installation and uses the same security database.

The Spectrum ES software can be used to control the following PerkinElmer instruments:

- Spectrum Two
- Frontier FT-IR Systems
- Spectrum 65/100/Spectrum 100 Optica/Spectrum One FT-IR
- Spectrum 100N/Spectrum One NTS FT-NIR
- Spectrum 400 FT-IR/FT-NIR and Spectrum 400 FT-IR/FT-FIR
- Spotlight 150 Microscope
- RamanStation 400 Series/RamanFlex 400 Series/RamanMicro 200 Series/ RamanMicro 300 Accessory/Raman IdentiCheck

Further Information

For more detailed information on using Spectrum ES software, access the on-screen Help by selecting the **Contents and Index** command from the Help menu.

For more information on your spectrometer consult the manuals that come with the instrument. The multimedia tutorials may also provide you with further information.

Overview of Spectrum ES Security

Spectrum ES software is designed to provide a secure environment in which the setup of instruments, and the collection and distribution of data is controlled in accordance with the requirements of 21 CFR Part 11, the Code of Federal Regulations that deals with the Food and Drug Administration (FDA) guidelines on electronic records and electronic signatures.

There are two main security components used by the Spectrum ES software:

- The Windows operating system security features, which manage access to the PC, its peripherals, the data files on the hard disk, and all aspects of the PC configuration.

- The Spectrum ES login security features, which manage access to the software, the data and any associated instruments.

These security features give a high degree of flexibility. They allow administrators to apply very tight restrictions on what a day-to-day user is able to do, and also to adhere to the company's 21 CFR Part 11 compliance procedures.

Day-to-day users of the system are not typically allowed to delete, change or rename data files. Whether or not they can access a particular function within the Spectrum ES software is determined by the permissions of the group they are assigned to. For any individual user, there are likely to be some features of the software to which they do not have access.

The Role of the Administrator

The role of the administrator in Spectrum ES is broadly two-fold:

- Administration of the Windows operating system (Windows Administrator).

- Administration of the Spectrum ES software (Software Administrator).

These roles can be carried out by a single person, if required.

Conventions Used in this Manual

Normal text is used to provide information and instructions.

Bold text refers to text that is displayed on the screen.

UPPERCASE text, for example ENTER or ALT, refers to keys on the PC keyboard. "+" is used to show that you have to press two keys at the same time, for example, ALT+F.

All eight digit numbers are PerkinElmer part numbers unless stated otherwise.

Notes, Cautions and Warnings

Three terms, in the following standard formats, are also used to highlight special circumstances and warnings.

NOTE: A note indicates additional, significant information that is provided with some procedures.

CAUTION

We use the term CAUTION to inform you about situations that could result in ***serious damage to the instrument*** *or other equipment. Details about these circumstances are in a box like this one.*

WARNING

We use the term WARNING to inform you about situations that could result in ***personal injury*** *to yourself or other persons. Details about these circumstances are in a box like this one.*

Folder Names

In this guide we use the term "C:\Program Files" to represent the name of the top-level folder location used to store software programs. In practice, this name will vary depending upon your operating system and your locale.

For example if you have a Windows 7 or 8 operating system, because Spectrum ES runs as a 32-bit application, on 64-bit systems the folder name will be C:\Program Files (x86). Alternatively, if you are running Windows XP on a non-English system, a local language variant of this folder name may be used.

Installation of Spectrum ES

PC Requirements

The PC you install the software on must meet the following minimum specification:

- Intel® Pentium 4, 1.6 GHz processor (or equivalent) – dual-core or hyper-threaded preferable.
- At least 1 GB of Random Access Memory (RAM).
- The capability of displaying at least High Color (16-bit) at 1280 x 768.
- 40 GB Hard disk with at least 1 GB free space as an NTFS drive.

NOTE: We have locked the system into using an NTFS drive because the alternative FAT32 file system doesn't provide enough protection at a folder and file level to ensure that users and groups of users cannot delete or amend data files, while at the same time being able to create new data files.

- DVD drive.
- Ethernet network connection (for Frontier FT-IR, Spectrum 100 Series and Spectrum 400 Series instruments).
- A keyboard and PS/2®-style mouse.
- Serial (RS232) port – for stage control box (systems with motorized stages only).
- Hi-Speed USB 2.0 port(s) – Spectrum Two and Raman instruments only.

  The number of USB ports required will depend on your instrument configuration. A miniumum of 1 port is required for Spectrum Two and Raman instrument connection. You require additional ports to connect a microscope and/or to connect a Triggered Fiber Optic Probe.

  You may also need a USB 2.0 port if your Spectrum ES software was supplied on a USB flash drive.

Operating System

This software requires that Windows® XP Professional Service Pack 3, or greater, or Windows® 7 Professional (32-bit or 64-bit), or Windows® 8.x Pro (32-bit or 64-bit) operating system is installed on the PC before you install Spectrum ES.

NOTE: The video camera used with the Spotlight 150 and some Raman instruments will only work on Windows XP or Windows 7 32-bit.

Microsoft Service Packs and Updates can be downloaded from www.microsoft.com/downloads.

Microsoft® Word/Microsoft® Excel

There is a function in Spectrum ES that enables you to export your results to a Microsoft Word document if you have Microsoft Word installed on your PC, or to a Microsoft Excel workbook if you have Microsoft Excel installed on your PC.

NOTE: Microsoft Word can also be used to work with .rtf format files created using the Spectrum ES Report option.

After installing Microsoft Office (2003 or later) on the PC, open Microsoft Word or Microsoft Excel so that it becomes initialized, then the Send-To-Word or Send-To-Excel functions in Spectrum ES should work correctly.

If an error occurs on trying to use this function, it could be that the primary interop assemblies (PIA) for Office were not installed correctly. These can be installed either using the Office install CD, or using files supplied on the root of the Spectrum ES installation DVD (O2003PIA.exe, for Office 2003; PrimaryInteropAssembly.exe, for Office 2007; and PIARedist.exe, for Office 2010). Run the relevant program; agree to the Microsoft license conditions; and select a directory to extract the files into (for example, C:\temp\office2003). Navigate to this folder and then run the .msi installer program. This installs the missing components, allowing Spectrum ES to send data to Word and Excel.

Adobe Reader

Reports in Spectrum ES are created in .spdf format. This format is decoded by the **Open ES Report** option (in the File menu of Spectrum ES) so that reports can be viewed using Adobe Reader. An installation of Adobe Reader is available on the *Software Utilities CD*.

TCP/IP Communication (FT-IR Instruments Only)

To operate your instrument using an Ethernet port you will need TCP/IP protocols established on the PC. We recommend that you do not install Spectrum ES until this has been set up. Refer to *Appendix 2: Configuring your PC Network Adapter* on page 97.

Instrument IP Address (FT-IR Instruments Only)

The IP address of your instrument may not be set to the factory default if:

- The instrument is available to a number of PCs on your network.
- There is more than one instrument on your network, in which case each instrument must have a unique IP address.

Typically, IP addresses are controlled by your network administrator.

For information about changing an instrument's IP address, refer to *Appendix 3: Changing the IP Address of your Instrument* on page 101.

Windows Administrator Level

It is important to note that you must be logged on to Windows as an Administrator before installing the software. Logging on as an Administrator ensures that installation of the software can be undertaken and that the necessary system registry updates that form part of the installation process are successfully completed.

Administrators have the capability to assign privileges and logon rights and therefore have the ability to make system-wide changes. Users on the other hand do not have this ability, or may have restricted abilities depending on the rights and privileges assigned by the Administrator.

Upgrading From Earlier Versions of Spectrum

You are strongly advised not to install Spectrum ES on a PC that has previously been used to run any version of the standard Spectrum software.

If Spectrum ES version 6 is present on your system, you must uninstall it before installing the new version of the software. The existing Security database, containing details of users, groups, instruments and permissions, can be upgraded for use with Spectrum ES version 10. When upgrading Spectrum ES version 10.3.3 to later versions, the same databases can be used with the new version of the software after they also have been upgraded. Details of how to upgrade the databases can be found in the Spectrum ES installation procedures and in *Setting up the shared databases* on page 62.

We recommend that you backup the existing Spectrum ES database files on your system before upgrading your software. This will allow you to restore the system to its present condition if any problems occur with the installation. Depending on the location of the database, the backup procedure may require the assistance of your system administrator (for example, in case SQL Server needs to be closed down to perform the backup). The files that should be backed up are listed under *Backing up Files and Databases* on page 58.

Spectrum ES Installation

Before you Start

We strongly suggest you read the *PC Requirements* on page 10 before attempting to install your software.

Before installing the software, we recommend that you read and print the release notes which can be found as an .rtf file and a .pdf file on the root of the *Spectrum ES Software* DVD, because they contain important information that may not be in the on-screen Help.

NOTE: To read .pdf files you will need Adobe Reader. An installation of this software is available on the *Software Utilities CD*.

If you intend using Spectrum ES with a Spotlight 150 Microscope, a Raman instrument (with or without a triggered fiber optic probe), or a Spectrum Two spectrometer, you should ensure that there is NO connection between these items and your PC, even if the instrument is not connected to mains power.

Spectrum ES requires Microsoft SQL Server 2008 R2 Express or later to be installed on your PC, and Microsoft SQL Server 2008 Express Service Pack 1 will be installed automatically as part of the Spectrum ES installation if no existing version is found. However, if you currently have a version that is earlier than Microsoft SQL Server 2005 Express, you should uninstall it before you install Spectrum ES.

You must be logged on to Windows as an Administrator before installing the software.

IMPORTANT	*If you are sharing the Spectrum ES Security database across a network, ensure that no-one is logged in to any other PC with access to the database while you are installing the new version of Spectrum ES on your PC.*

Installation Procedure

Spectrum Two only

NOTE: The Spectrum Two instrument is usually connected using the USB cable supplied. However, you can also connect to the instrument, either directly or over a network, using the Ethernet connection.

The *Spectrum ES Software* DVD supplied contains an Installation Wizard to help you install the software on your PC.

1. If you would like to connect your Spectrum Two to the PC using an Ethernet port, configure your PC network adaptor as described in *Appendix 2: Configuring your PC Network Adapter* on page 97.

2. If you would like to connect your Spectrum Two over a network, assign your instrument a unique IP address as described in *Appendix 3: Changing the IP Address of your Instrument* on page 101.

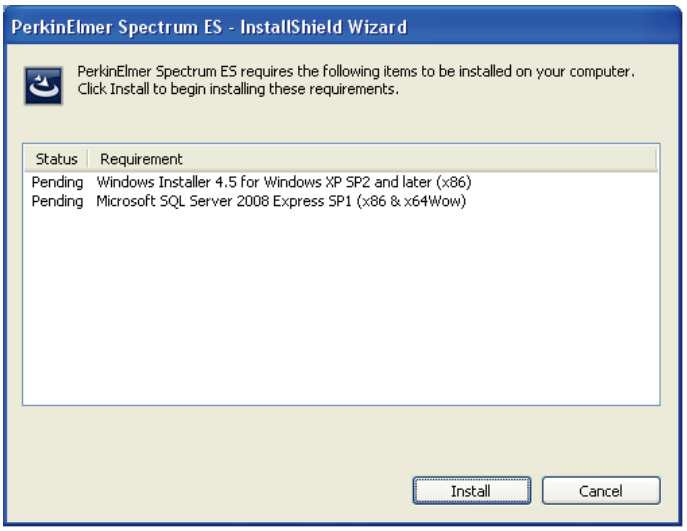
3. Place your *Spectrum ES Software* DVD into your DVD drive or insert the *Spectrum Software* USB Flash Drive in a USB port.

4. If the installation program does not start automatically, start the program **setup.exe** located in the root folder of the DVD or USB flash drive.

   The InstallShield Wizard starts.

   The wizard first checks your system and identifies any software packages required by Spectrum ES which are not already present on your system.

   A list of the required items is then displayed.



NOTE: The items listed on this screen will vary, depending upon your operating system and which additional software packages required to run Spectrum ES have already been installed on your computer. The list may include, for example, Microsoft .NET Framework version 3.5 Service Pack 1, Microsoft SQL Server 2008 Express Service Pack 1, Direct X9, and others.

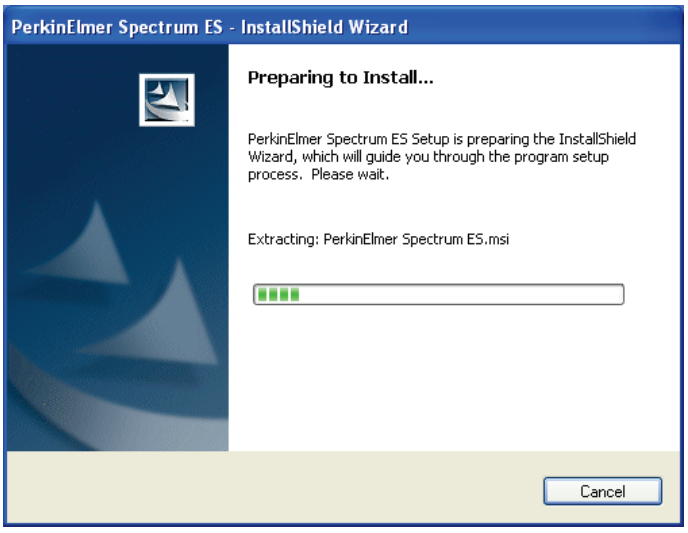
If no additional items are required, the installation procedure continues at step 6.

5. Click **Install**.

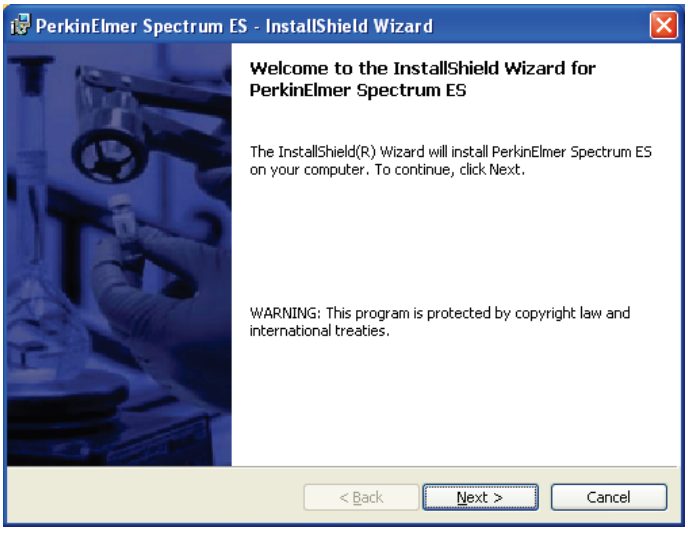
   Any software required to run Spectrum ES that has not already been installed on your computer must be installed. Follow the instructions displayed on-screen.

NOTE: The installer may require you to restart your computer on one or more occasions during the procedure. The installation should continue automatically when you log in to the computer after each restart.

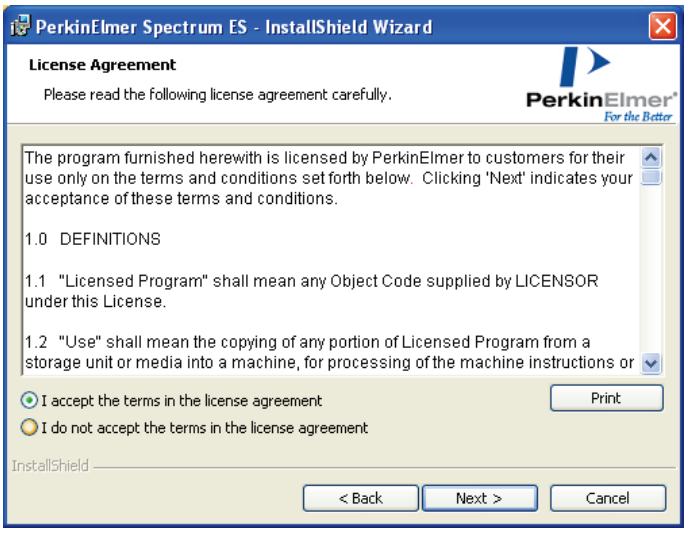
6. When the installation of any additional software is complete, the Spectrum ES installation continues.



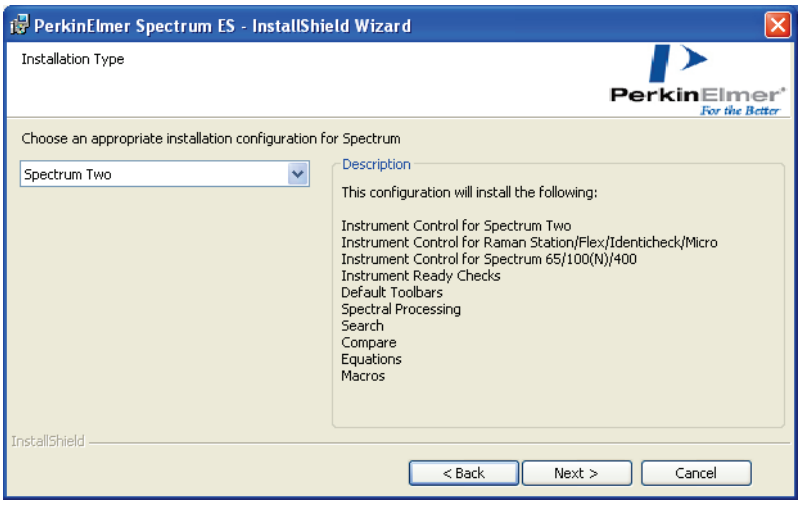
Then the Welcome page is displayed.



7. Click **Next**.
   The License Agreement page is displayed.

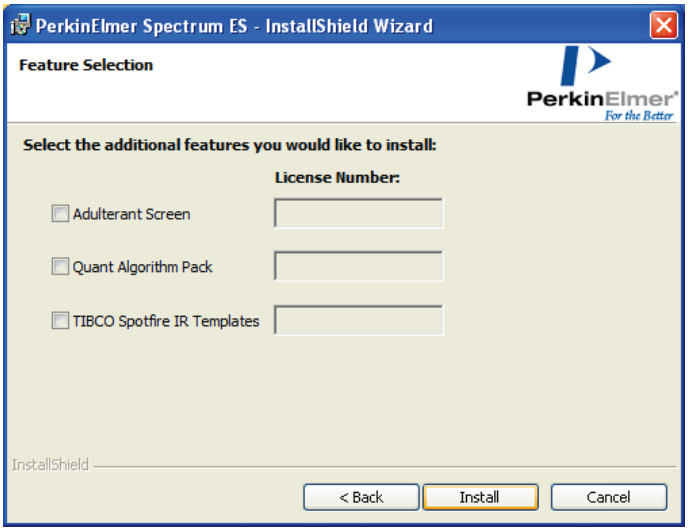


8. Read the license and if you accept the terms, select that option and then click **Next**.
   The Installation Type page is displayed.



9. Ensure that **Spectrum Two** is selected as the installation configuration and then click **Next**.

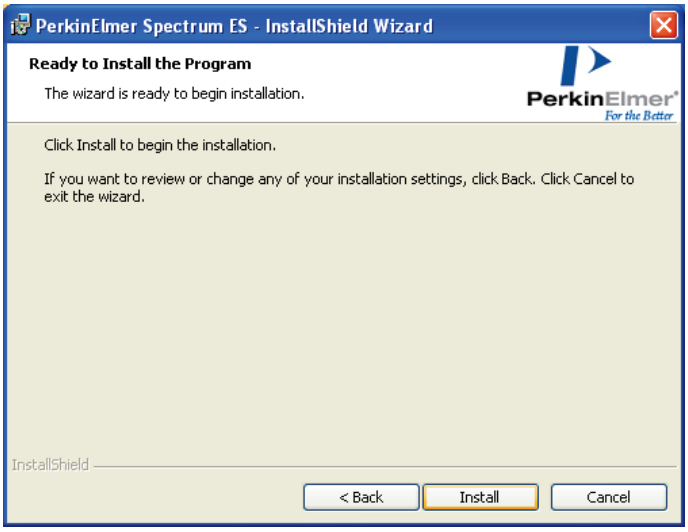
   The Feature Selection page is displayed.



10. If you have purchased a license for an additional feature in Spectrum, check the appropriate feature and enter the license number in the corresponding text box.

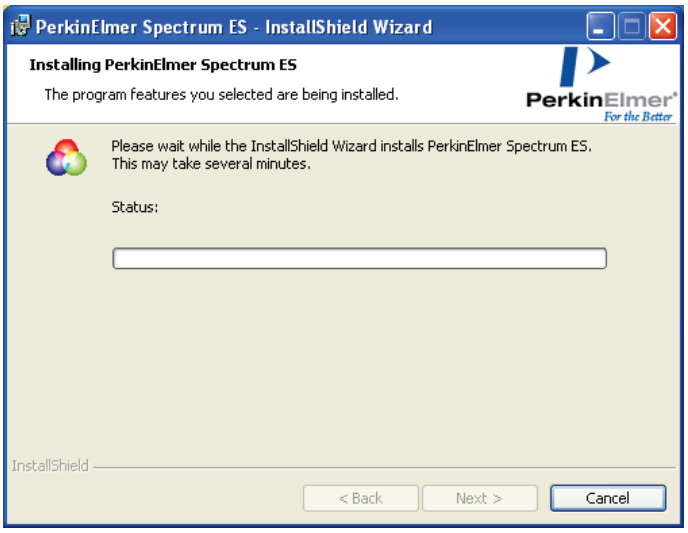
11. Click **Next**.

    The Ready to Install the Program page is displayed.

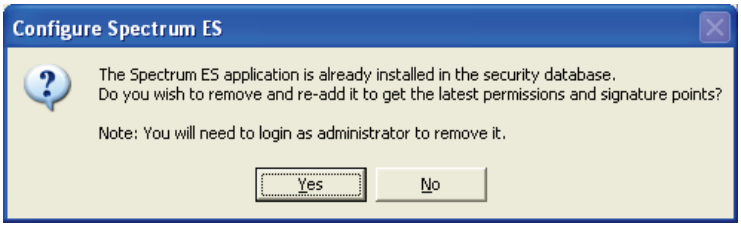


12. Click **Install** to begin installing Spectrum ES.

    The Installing PerkinElmer Spectrum ES page is displayed which informs you of the status of the installation.



When all the files have been copied from the DVD, and if you are upgrading your version of Spectrum ES or have already installed PerkinElmer software that contains the PerkinElmer security component on the PC, the following message is displayed.



13. Click **Yes** if you are upgrading to a newer version of the Spectrum ES software.

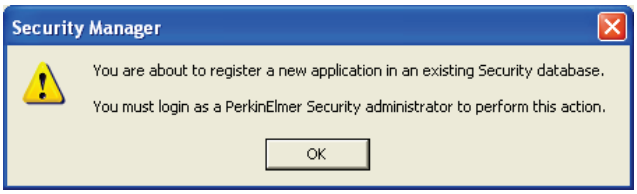
    You can click **No** if you are reinstalling a version of Spectrum ES that was installed previously, and go to step 21.

    The PerkinElmer Login dialog is displayed.

14. Log in as a PerkinElmer Software Administrator and click **OK**.

    Use the Administrator user name and password that you use for the PerkinElmer software that is already installed on the PC.

    The dialog below is displayed. The system requires a further login to upgrade the Security database to include the new version of Spectrum ES.



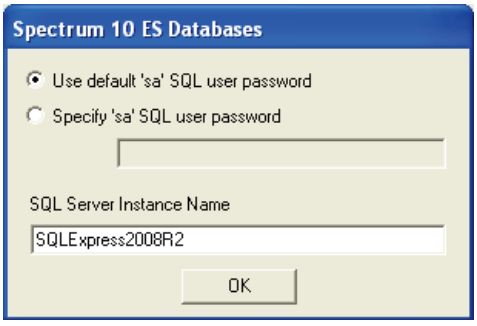
NOTE: This message may be displayed more than once during the installation.

15. Click **OK**.

    The PerkinElmer Login dialog is displayed.

16. Log in as a PerkinElmer Software Administrator.

    The dialog below is displayed.



    If you already use SQL Server Express on your computer with other applications, then you can choose to use it with the new version of Spectrum ES. This may simplify the administration of the system.

17. Click **OK** to select the default password option and use a new instance of SQL Server Express with the new version of Spectrum ES.

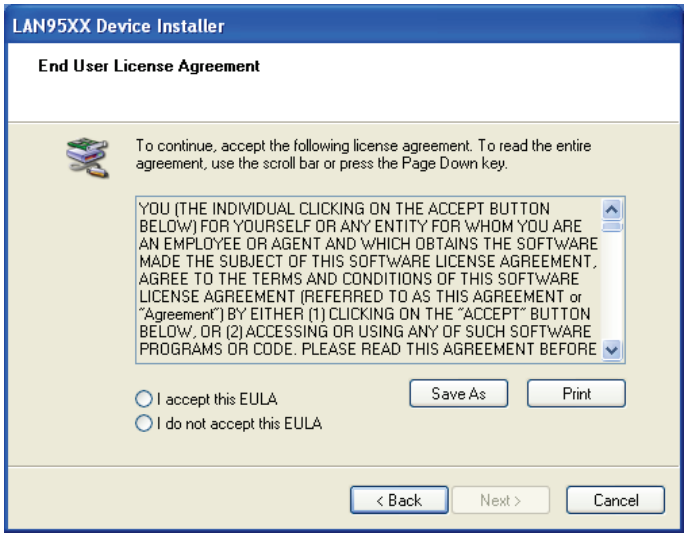
    OR

    Select **Specify 'sa' SQL user password**, enter the password and instance name for an existing version of SQL Server that you want to use with Spectrum ES, and click **OK**.

18. The LAN95XX Device Installer starts.

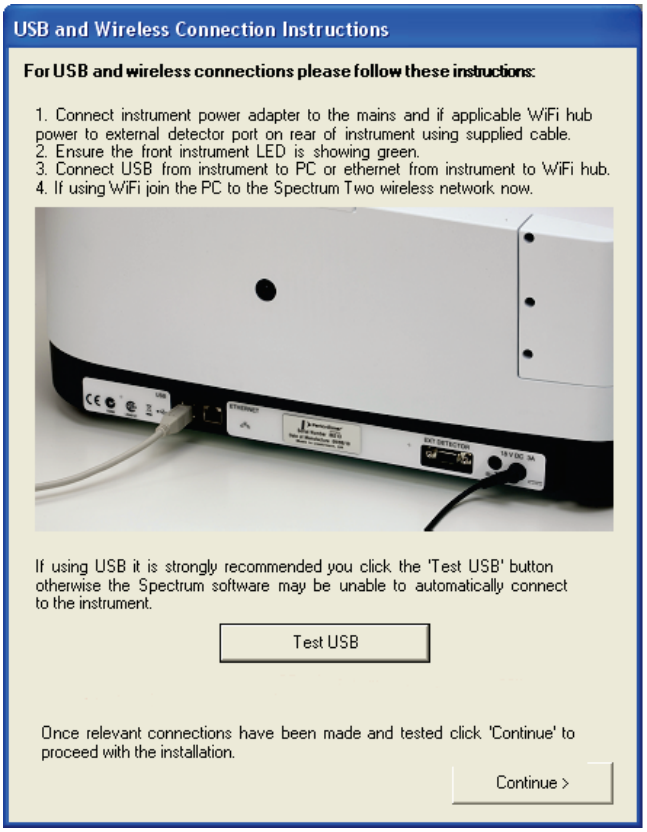
19. Click **Next**.

    The LAN95XX Device End User Licence Agreement page is displayed.



20. Read the license and if you accept the terms, select that option and then click **Next**.
    The LAN95XX Device is then installed.
    When the installation is complete, the screen shown below is displayed.

21. Click **Finish**.
    The USB and Wireless Connection Instructions dialog is displayed.

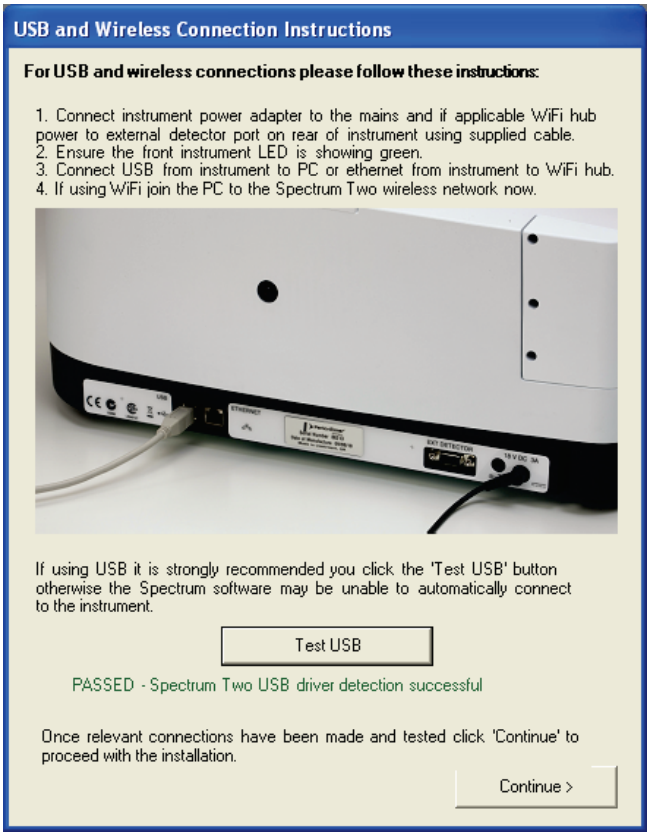


    Follow the instructions on the dialog.

NOTE: If you are installing Spectrum ES on a system running Windows XP and you connect via a USB, the New Hardware Wizard starts automatically when you plug the USB cable from the instrument into your PC.

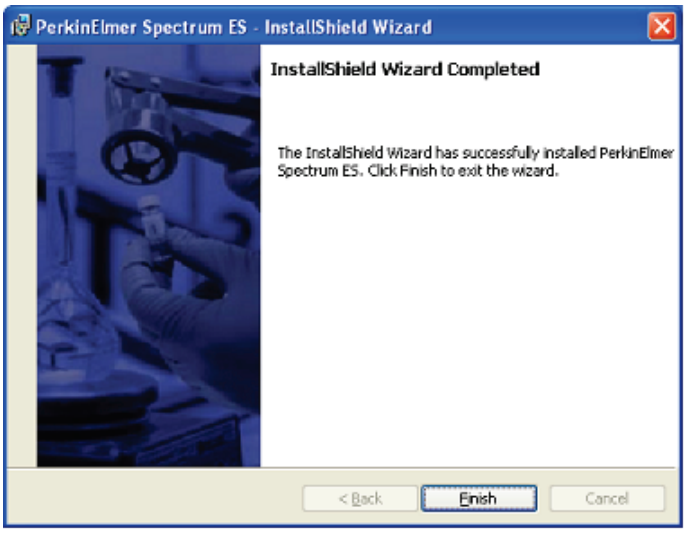
Follow the instructions provided by the wizard to let Windows install the required USB drivers for you.

If your instrument is connected via the USB cable, you should click **Test USB** to confirm that the drivers have been installed correctly. The result will be displayed on the dialog.



If the test fails and a failure message is displayed, check that the instrument is connected to the mains power, and is connected to the PC using the USB 2.0 cable provided and retry the test. If the test still fails, contact your PerkinElmer Service Representative, or go to the Technical Support website, www.perkinelmer.com/SpectrumTwoSupport.

22. Click **Continue**.
    The InstallShield Wizard Completed page is displayed.



23. Click **Finish**.
    The Spectrum ES software installation is completed. You must restart the computer if you want to select another user to run the software.

NOTE: Depending upon your operating system, you may be asked to restart your system to complete the installation of Spectrum ES.

When installing a new version of Spectrum ES, the Group permissions will be restored to their default settings.

- Reset the permissions for each group as described in *Defining what Members of a Group are able to do* on page 78.

Following the installation of a new version of Spectrum ES, the database(s) must be upgraded before you attempt to log in to Spectrum. Refer to *Setting up the shared databases* on page 62 for details of how to upgrade the Spectrum ES database(s). The databases do not need to be upgraded if the same version of Spectrum ES is being reinstalled.

For information on how to log in to Spectrum ES after installing the software, refer to *Logging on to Spectrum ES for the First Time* on page 35.

All other instrument types

The *Spectrum ES Software* DVD supplied contains an Installation Wizard to help you install the software on your PC.

1. If you have an FT-IR spectrometer and would like to connect to the PC using an Ethernet port, configure your PC network adaptor as described in *Appendix 2: Configuring your PC Network Adapter* on page 97.

2. If you have an FT-IR spectrometer and would like to connect to the instrument over a network, assign your instrument a unique IP address as described in *Appendix 3: Changing the IP Address of your Instrument* on page 101.

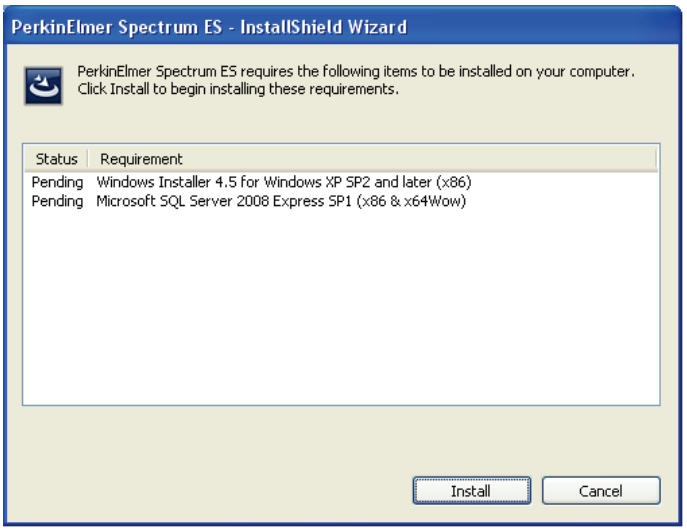
3. Place your *Spectrum ES Software* DVD into your DVD drive or insert the *Spectrum Software* USB Flash Drive in a USB port.

4. If the installation program does not start automatically, start the program **setup.exe** located in the root folder of the DVD or USB flash drive.

   The InstallShield Wizard starts.

   The wizard first checks your system and identifies any software packages required by Spectrum ES which are not already present on your system.

   A list of the required items is then displayed.



NOTE: The items listed on this screen will vary, depending upon your operating system and which additional software packages required to run Spectrum ES have already been installed on your computer. The list may include, for example, Microsoft .NET Framework version 3.5 Service Pack 1, Microsoft SQL Server 2008 Express Service Pack 1, Direct X9, and others.

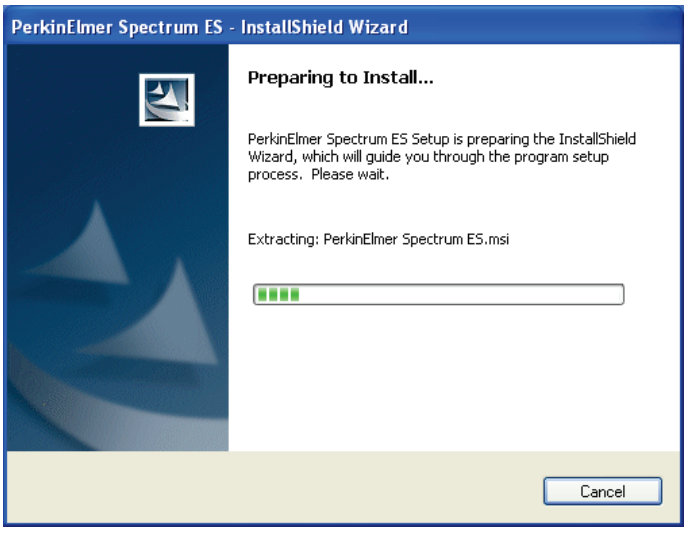
If no additional items are required, the installation procedure continues at step 6.

5. Click **Install**.

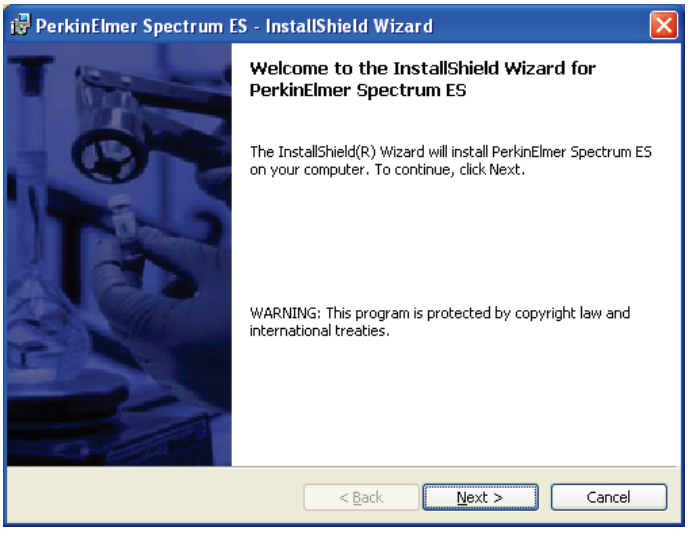
   Any software required to run Spectrum ES which has not already been installed on your computer must be installed. Follow the instructions displayed on-screen.

NOTE: The installer may require you to restart your computer on one or more occasions during the procedure. The installation should continue automatically when you log in to the computer after each restart.

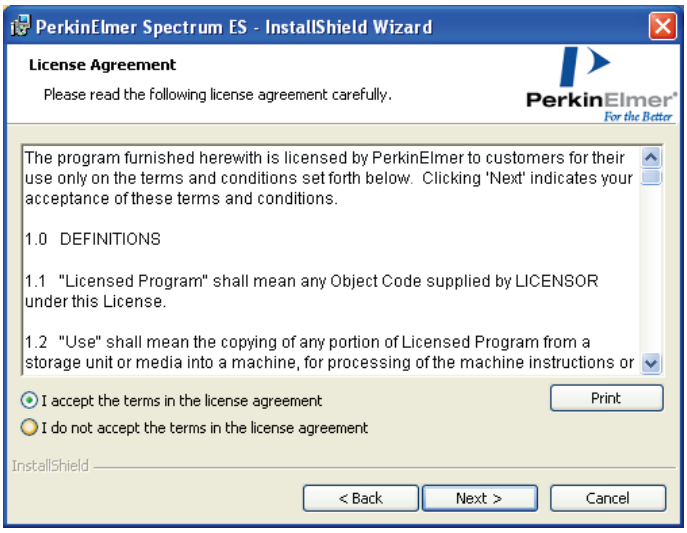
6. When the installation of any additional software is complete, the Spectrum ES installation continues.



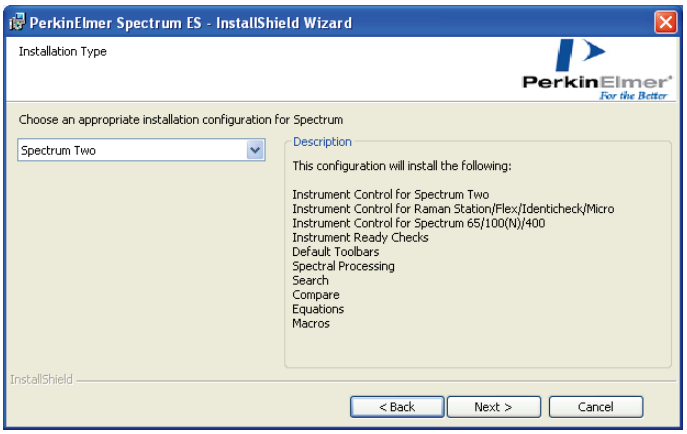
Then the Welcome page is displayed.



7. Click **Next**.
   The License Agreement page is displayed.

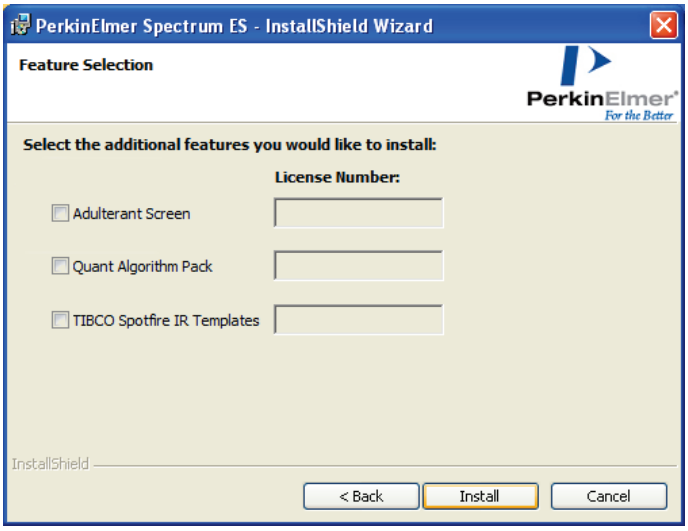


8. Read the license and if you accept the terms, select that option and then click **Next**.
   The Installation Type page is displayed.



9. Use the drop-down list to select the installation configuration that you require and then click **Next**.

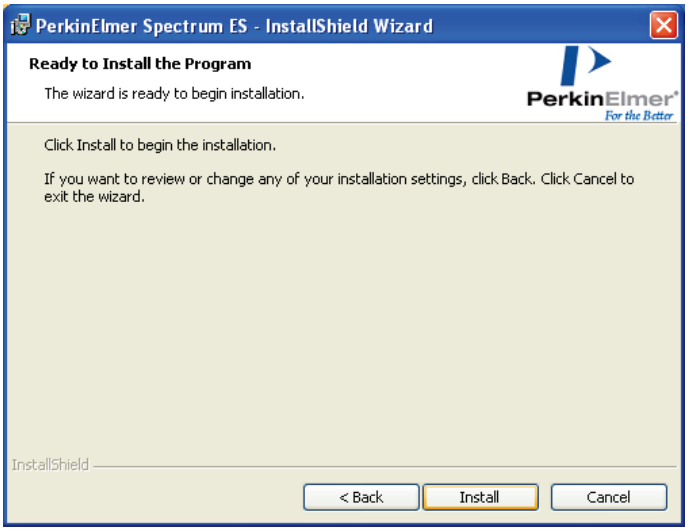
   The Feature Selection page is displayed.



10. If you have purchased a license for an additional feature in Spectrum, check the appropriate feature and enter the license number in the corresponding text box.

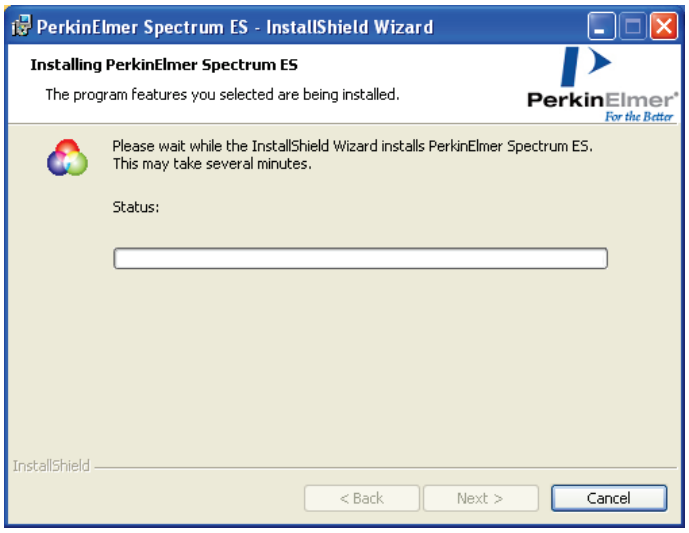
11. Click **Next**.

    The Ready to Install the Program page is displayed.

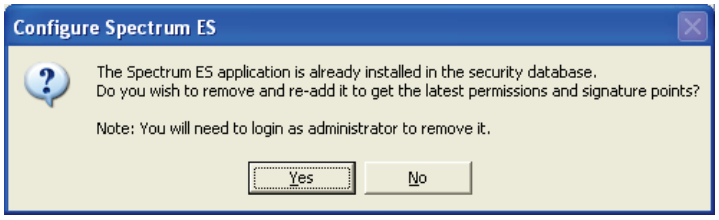


12. Click **Install** to begin installing Spectrum ES.

    The Installing PerkinElmer Spectrum ES page is displayed which informs you of the status of the installation.



    When all the files have been copied from the DVD, and if you are upgrading your version of Spectrum ES or have already installed PerkinElmer software that contains the PerkinElmer security component on the PC, the following message is displayed.



13. Click **Yes** if you are upgrading to a newer version of the Spectrum ES software.

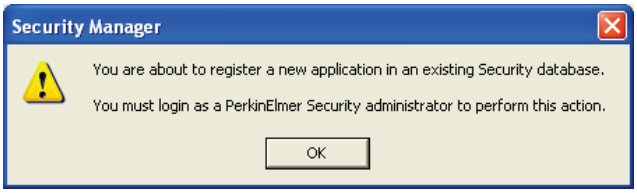
    You can click **No** if you are reinstalling a version of Spectrum ES that was installed previously, and go to step 15.

    The PerkinElmer Login dialog is displayed.

14. Log in as a PerkinElmer Software Administrator and click **OK**.

    Use the Administrator user name and password that you use for the PerkinElmer software that is already installed on the PC.

    The dialog below is displayed. The system requires a further login to upgrade the Security database to include the new version of Spectrum ES.



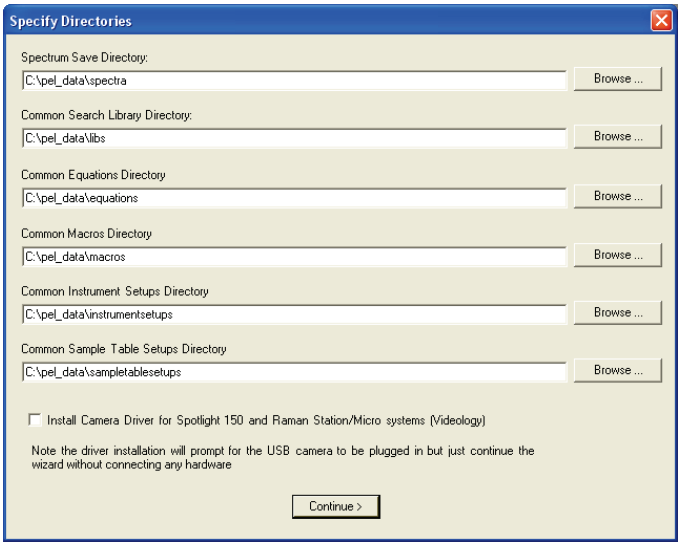
NOTE: This message may be displayed more than once during the installation.

15. Click **OK**.

    The PerkinElmer Login dialog is displayed.

16. Log in as a PerkinElmer Software Administrator.

    The Specify Directories dialog is displayed.



17. Specify the directories you want the software to use, as follows:

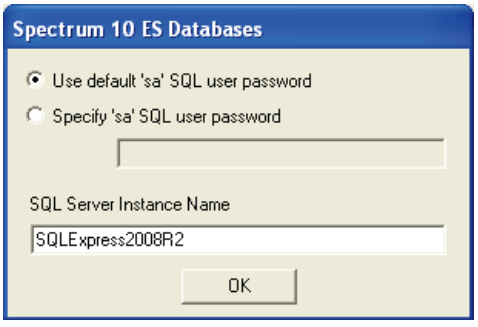
Directory	Description
Spectrum Save Directory	The default path for loading or saving spectra. **NOTE:** You can change the default directory by selecting **Save As** from the File menu in Spectrum ES when the installation is complete.
Common Search Library Directory	The path to your Common Search Libraries, from which the software will automatically add any libraries found to the Search library list. **NOTE:** In Spectrum ES, you can specify that any directory, or commercial file, containing compatible spectra is a Search Library. However, the same resource placed in the Common Search Library Directory is automatically made available.
Common Equations Directory	Use these fields to specify directories which will hold items that are to be made available to all users.
Common Macros Directory	
Common Instrument Setups Directory	
Common Sample Table Setups Directory	

If you want to use a different directory, click **Browse** and then navigate to the required location.

18. If you have a Spotlight 150 microscope or a Raman Instrument with a video camera (RamanStation 400 Series, RamanMicro 200 Series and RamanMicro 300 Accessory), you will need to select the check box to install the camera drivers.

19. Click **Continue**.

The dialog below is displayed.



If you already use SQL Server Express on your computer with other applications, then you can choose to use it with the new version of Spectrum ES as well. This may simplify the administration of the system.

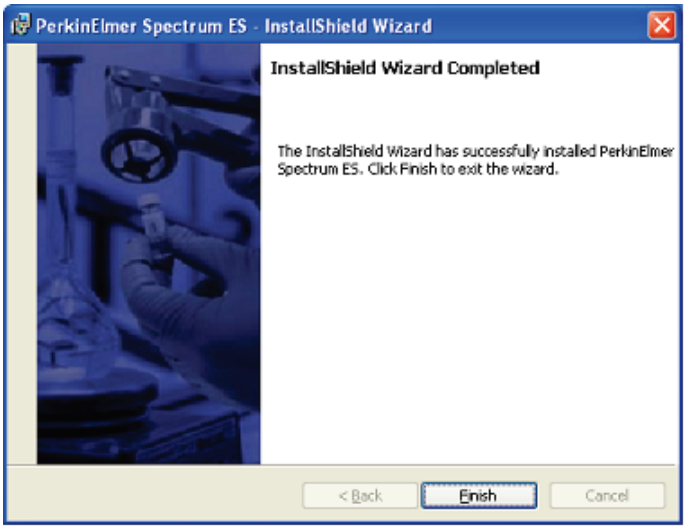
20. Click **OK** to select the default password option and use a new instance of SQL Server Express with the new version of Spectrum ES.

    OR

    Select **Specify 'sa' SQL user password**, enter the password and instance name for an existing version of SQL Server that you want to use with Spectrum ES, and click **OK**.

21. If you selected to install the camera drivers, the Welcome to Videology USB2.0 Camera Installation Wizard page is displayed. See *Installing Videology Camera Drivers* on page 33 for installation instructions.

    Otherwise the software is installed and the InstallShield Wizard Completed page is displayed.



22. Click **Finish**.

    The Spectrum ES software installation is completed. You must restart the computer if you want to select another user to run the software.

NOTE: Depending upon your operating system, you may be asked to restart your system to complete the installation of Spectrum ES. In this event, the automatic launching of the software, if selected, happens after the restart.

When installing a new version of Spectrum ES, the Group permissions will be restored to their default settings.

- Reset the permissions for each group as described in *Defining what Members of a Group are able to do* on page 78.

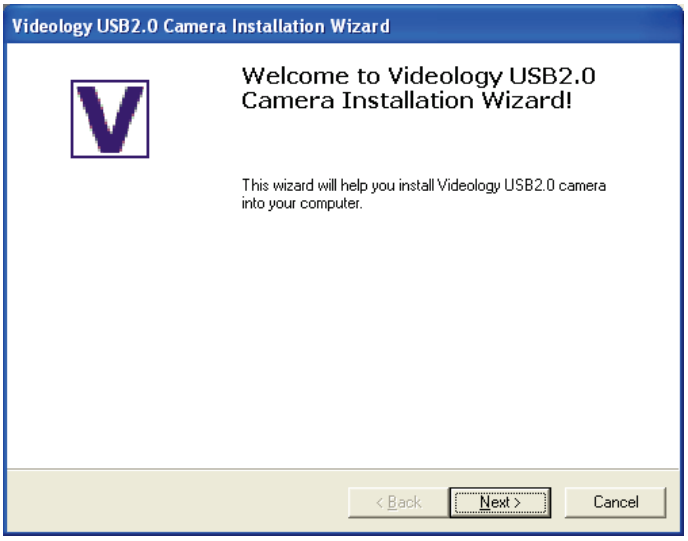
Following the installation of a new version of Spectrum ES, the database(s) must be upgraded before you attempt to log in to Spectrum. Refer to *Setting up the shared databases* on page 62 for details of how to upgrade the Spectrum ES database(s). The databases do not need to be upgraded if the same version of Spectrum ES is being reinstalled.

For information on how to log in to Spectrum ES after installing the software, refer to *Logging on to Spectrum ES for the First Time* on page 35.

Installing Videology Camera Drivers

If you have a Spotlight 150 microscope or a Raman Instrument with a video camera (RamanStation 400 Series, RamanMicro 200 Series and RamanMicro 300 Accessory), you should select to install the camera drivers as part of the installation procedure.

When you reach step 21 of the installation procedure, the Welcome to Videology USB2.0 Camera Installation Wizard page is displayed.



To complete the camera driver installation, and then return to the Spectrum ES software installation procedure, follow the steps below.

1. Click **Next**.
   The Please Plug in Your Camera Now page is displayed.

NOTE: There is no need to plug in your camera.

2. Click **Next**.
   The Your Camera is Successfully Installed page is displayed.

3. Click **Finish**.
   You are returned to the Spectrum ES installation procedure.

Logging on to Spectrum ES for the First Time

1. For Windows XP and Windows 7, from the Start menu select **Programs**, the **PerkinElmer Applications** group, the **Spectrum** sub-group and then the **Spectrum** application.

   For Windows 8, right-click at the bottom of the Start screen to display the Apps toolbar, and click the All Apps icon to display the Apps. For Windows 8.1, click the down arrow on the Start screen to display the Apps. Double-click the Spectrum icon in the **PerkinElmer Applications** group.

   The Spectrum ES start-up splash-screen is displayed, followed by a dialog that prompts for your login details:

2. Enter your **User name** and **Password**, and then click **OK**.

   If you do not have any other PerkinElmer software installed on your PC, log in as the default user created during the installation of Spectrum ES:

   - **User name:** Administrator
   - **Password:** administrator

   Or log in using the Administrator **User name** and **Password** that you use for any PerkinElmer software that is already installed on the PC.

NOTE: Passwords are case-sensitive, but the user name is not case-sensitive.

3. Click **OK**.

4. If you use the default password, you are then prompted to change your password.

   This is a security feature, designed to ensure that the password created during the installation can only be used for the first login.

5. Enter and confirm your new password, and then click **OK**.

   Spectrum ES starts.

NOTE: During your first use of the software we ***strongly*** recommend that you create another user who is a member of the Administrators group, for emergency use in case of a problem with the primary Administrator.

For details of how to create a new user, see *Creating a New Spectrum ES User* on page 75.

Installing an FT-IR Instrument in Spectrum ES

After installing Spectrum, your FT-IR instrument must be set up in the software.

For details of how to install a Raman instrument, see *Installing a Raman Instrument in Spectrum ES* on page 42.

Installing a Spectrum Two Using a USB Cable or a WiFi Connection

The first time you log in to Spectrum ES with a Spectrum Two instrument connected to the PC via a USB cable or a WiFi connection, the instrument is installed and configured automatically for you.

NOTE: For details of how to connect your Spectrum Two instrument to a PC using a USB cable or WiFi connection, see *the Spectrum Two User's Guide* (L1050228), supplied with your instrument.

Installing an FT-IR Instrument Using an Ethernet Connection

Connecting a Spectrum Two directly to the PC

If you want to connect to a Spectrum Two instrument using an Ethernet connection, you must:

1. Configure the TCP/IP settings for the PC on which Spectrum ES software has been installed.

   We recommend that you do this before you install Spectrum ES software. You *must* do this before you start Spectrum ES software with your instrument connected. Refer to *Appendix 2: Configuring your PC Network* Adapter on page 97.

2. Log in to Spectrum ES with the Spectrum Two instrument connected to the PC via an Ethernet connection.

   The instrument is installed and configured automatically for you.

NOTE: For details of how to connect your Spectrum Two instrument to a PC using an Ethernet connection, see *the Spectrum Two User's Guide* (L1050228), supplied with your instrument.

Connecting any other FT-IR instrument directly to the PC

If you want to connect to an FT-IR instrument (other than a Spectrum Two) using an Ethernet connection, you must:

1. Configure the TCP/IP settings for the PC on which Spectrum ES software has been installed.

   We recommend that you do this before you install Spectrum ES software. You *must* do this before you start Spectrum ES software with your instrument connected. Refer to *Appendix 2: Configuring your PC Network* Adapter on page 97.

2. Add the instrument to the software using the Instrument Install Wizard.

NOTE: For details of how to connect your FT-IR instrument to a PC using an Ethernet connection, refer to the user's guide for your instrument.

Connecting to an FT-IR instrument over a network

If you want to install connect to an FT-IR instrument over a network you must:

1. Assign each instrument a unique IP address.

   When using a network, the TCP/IP port of the PC will normally obtain an automatic address from a DHCP server. To connect to an FT-IR over a network, the FT-IR must have a compatible network address. A subnet mask of **255 255 0 0** means that the first two parts of the instrument IP address must match the network IP address given to the PC by the DHCP server.

   Refer to *Appendix 3: Changing the IP Address of your Instrument* on page 101.

2. Add the instrument to the software using the Instrument Install Wizard.

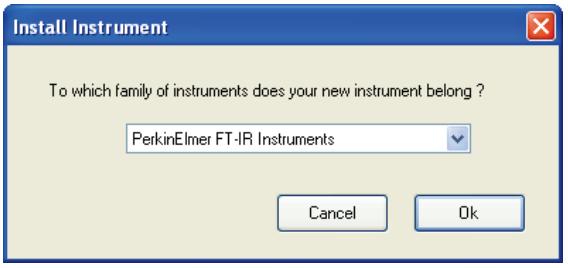
Instrument Install Wizard

1. Log in to the Spectrum ES as a Software Administrator.

   If an instrument has already been installed, select to **work offline**.

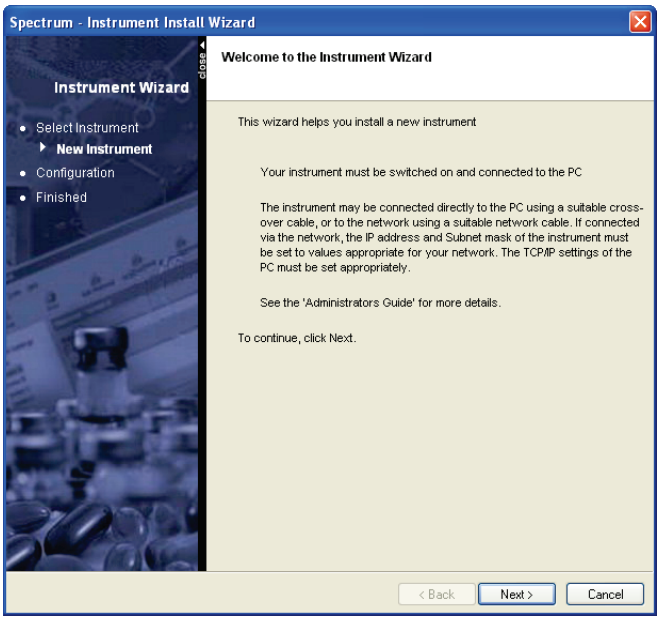
2. From the Setup menu, select **Instruments**, then select **Add Instrument** from the sub-menu.

   The Install Instrument dialog is displayed.



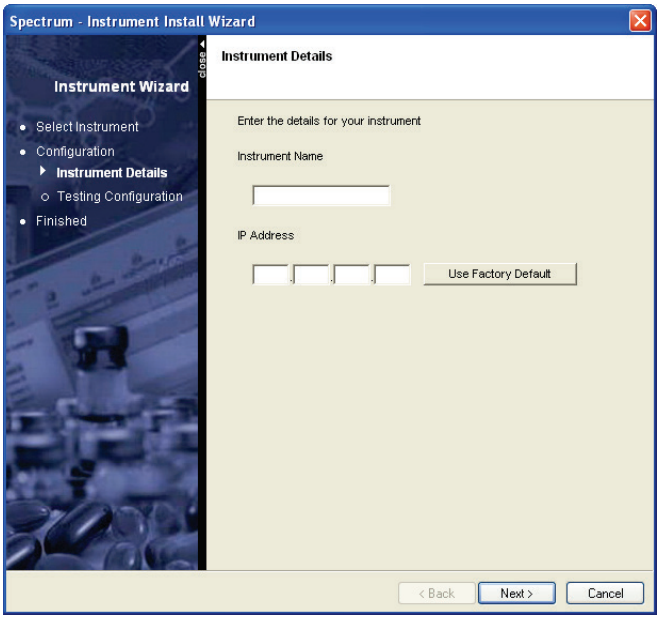
3. Select **PerkinElmer FT-IR Instruments** from the drop-down list and then click **OK**.

   The Instrument Install Wizard starts with advice on how to connect your FT-IR instrument to your PC or network.



4. Click **Next**.

   The Instrument Details page is displayed.



5. Enter an **Instrument Name**, which will be used by the Spectrum ES software to identify your instrument.

6. If the instrument is connected to your network, enter the instrument **IP Address**.

   Typically, this address will have been provided by your network administrator when the instrument was first installed. See *Instrument IP Address (FT-IR Instruments Only)* on page 11.

   If the instrument is connected directly to your PC using the crossover cable supplied with your instrument or an Ethernet cable (Spectrum Two only), click **Use Factory Default**. The TCP/IP port will have to be configured to a static IP address of 167.116.185.71.

7. Click **Next**.

   If you have a Spectrum Two instrument, the Test Configuration dialog is displayed as described in step 8.

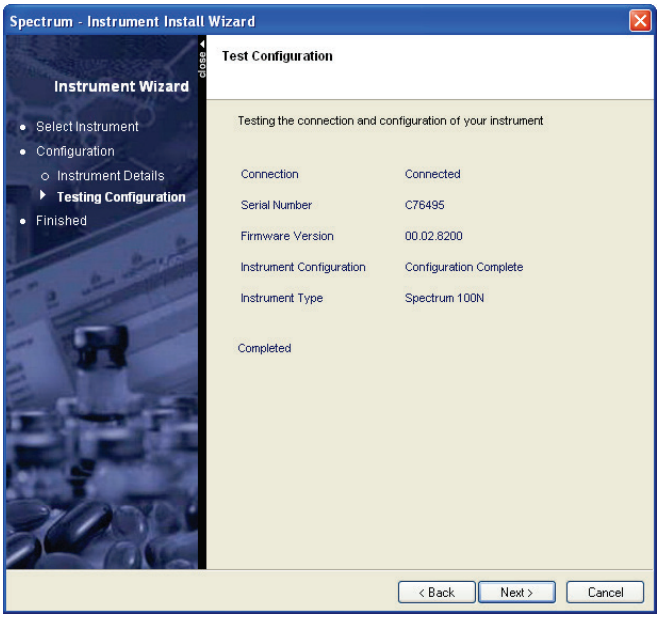
   OR

   For all other FT-IR instrument types, the Instrument Configuration Disk page is displayed, which prompts for the <serial number>.cfg of the configuration file required by your instrument. This file is shipped on a CD with your instrument.

   Browse to the configuration file, and then click **Copy Configuration**.

   If a suitable configuration file has been installed on your PC on a previous occasion, this dialog is amended to enable you either to **Use Existing Configuration**, or to **Overwrite Configuration**.

8. The Test Configuration page is displayed.



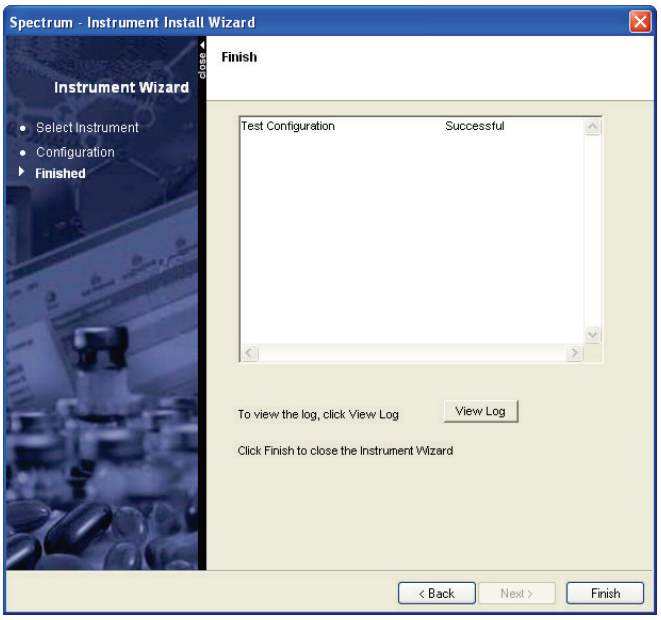
This test automatically checks whether your PC and instrument can communicate with each other.

Assuming this **Connection** is working, the page then displays the **Serial Number** and **Firmware Version** reported by your instrument, confirms that the installation of the **Instrument Configuration** is complete, and displays the **Instrument Type** recognized by Spectrum ES software.

When this page is **Completed**, check that the information displayed is as expected.

Likely causes of any discrepancies include out-of-date firmware or configuration data. Contact your PerkinElmer Service Representative for advice.

9. Remove the configuration CD, if applicable, and then click **Next**.
   The Finish page is displayed.



   This page of the Instrument Install Wizard offers a summary of the configuration tests. You can also click **View Log** to see the results of the configuration tests in more detail.

10. Click **Finish**.

11. Click **Yes** to complete the installation and close the Instrument Wizard.

Installing a Raman Instrument in Spectrum ES

After installing your software you will need to install your instrument. To install a Raman instrument, follow the steps described below. For details of how to install an FT-IR instrument, see *Installing an FT-IR Instrument in Spectrum ES* on page 36.

1. Switch on your instrument as described in the user's guide for your instrument.

2. Connect your instrument to a USB port on the PC on which you have installed Spectrum ES.

   You should use the same USB port each time you connect to your Raman instrument.

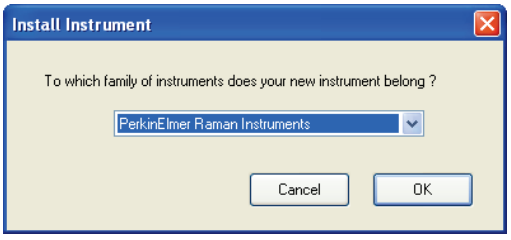
NOTE: Your instrument should be installed by a PerkinElmer Service Representative, who will install the correct drivers. If you install your instrument on a different PC, you will need to ensure that you have the appropriate drivers. See *Appendix 4: Reinstalling the Raman Instrument CCD Drivers* on page 107 for more information or contact your PerkinElmer Service Representative.

3. Log in to the Spectrum ES as a Software Administrator.

   If an instrument has already been installed, select to **work offline**.

4. From the Setup menu, select **Instruments**, then select **Add Instrument** from its sub-menu.

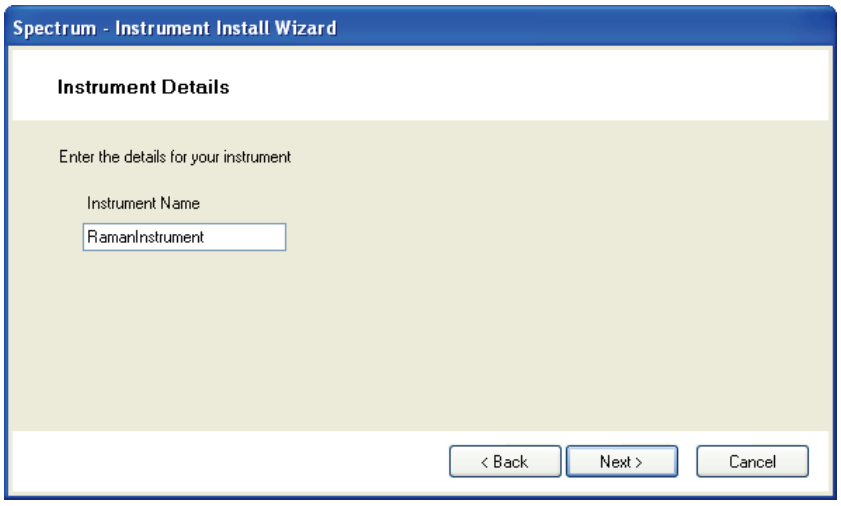
   The Install Instrument dialog is displayed.



5. Select **PerkinElmer Raman Instruments** from the drop-down list and then click **OK**.

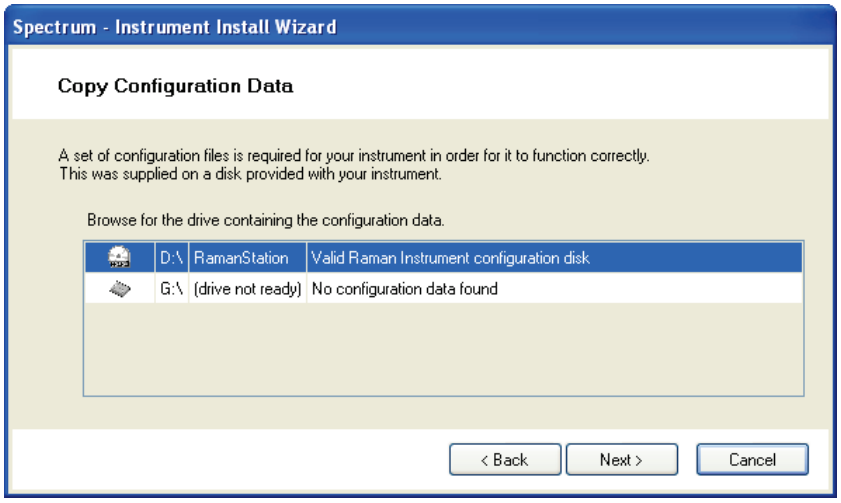
   The Instrument Install Wizard starts with advice on how to connect your instrument to your PC.

6. Click **Next**.
   The Instrument Details page is displayed.

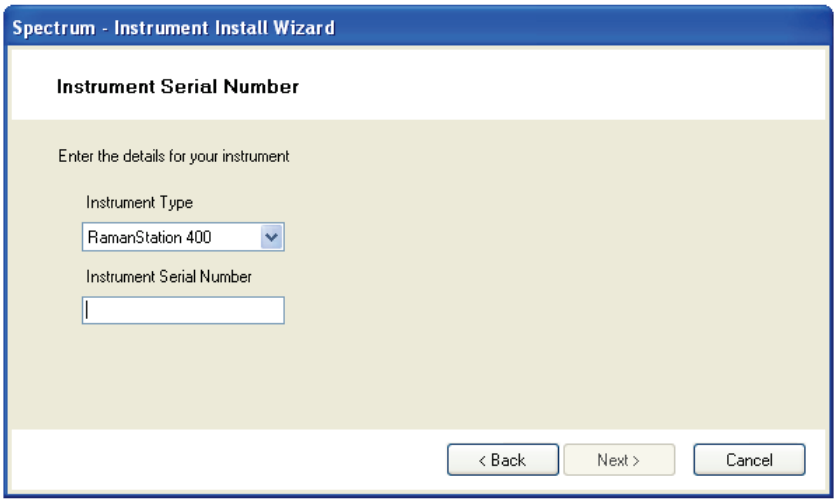


7. Enter an **Instrument Name**, which will be used by the Spectrum ES software to identify your instrument.

8. Click **Next**.
   The Copy Configuration Data page is displayed, which prompts you to select the drive containing the configuration data. This data is supplied on a CD with your instrument.

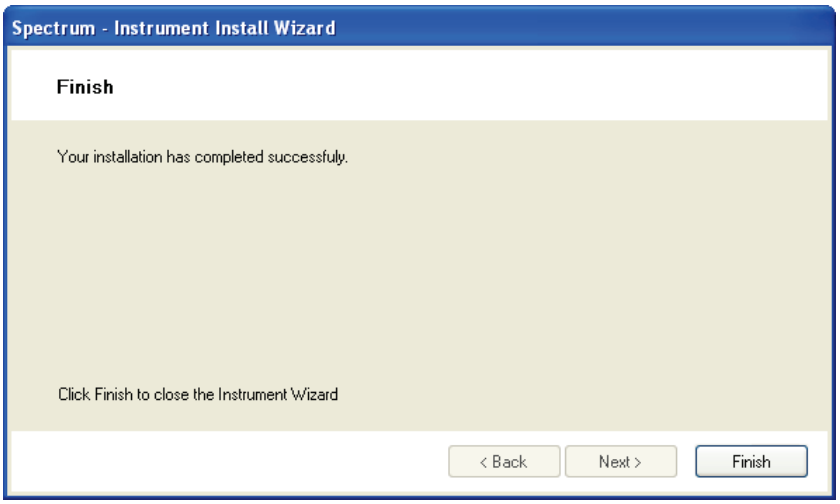


9. Click **Next**.
   The Instrument Serial Number page is displayed.



10. Select your **Instrument Type** from the drop-down list.

11. Enter your instrument serial number and click **Next**.
    The Finish page is displayed.



12. Remove the configuration disk from the DVD drive.

13. Click **Finish**.
    The Instrument Installation dialog is displayed asking if you want to connect to your newly installed Raman instrument.

14. Click **Yes** to complete the installation and close the Instrument Wizard.

NOTE: If you have installed a Raman Instrument, you should not allow the PC to enter Standby mode. On the Screen Saver page of the Display Properties dialog, click **Power** and then set **System standby**.

NOTE: If you disconnect the Raman instrument USB cable from the PC and reattach it to a different USB port, then you will be prompted for the drivers. By default the drivers are stored in C:\Program Files\PerkinElmer\ServiceIR\Raman. See *Appendix 4: Reinstalling the Raman Instrument CCD Drivers* on page 107 for more information.

Restricting the use of an Instrument

By default, all instruments added to Spectrum ES are available for use by all users. For information on how to restrict an instrument to specific user groups, see *Defining which Instruments Members of a Group can use* on page 80.

Removing an Instrument

If you have instrument connections you no longer need you can remove them:

- Select **Remove Instrument** from the Instruments sub-menu of the Setup menu.

NOTE: If you have other PerkinElmer software installed on your PC, remember that the instrument connection is removed from your system, not just Spectrum ES software.

Spectrum ES Windows Administration

Overview

A Windows Administrator is tasked with managing the PC on which the Spectrum ES software is installed. They are responsible for all Windows user/password settings, Windows auditing and NTFS file security.

NOTE: End users (that is, people using the Spectrum ES software and instruments to collect data) should run as Windows Users, never as Windows Administrators.

The Windows Administrator should:

- Set up password and user name policies according to the company's internal security policy.
- Ensure that users only have access to the folders and files that they need access to. This includes network drives.
- Setup the Start menu so that the users can only access the applications that they require to carry out their assigned tasks.
- Consider whether to set up a password protected screen saver to guard against unauthorized use of the system when unattended.
- Make sure that users are prevented from deleting or appending any files (by using the security features in NTFS) in the file locations where data is saved.
- Manage the PKIUsers group. For details, see *Administering the PKIUsers Group* on page 50.
- Use the Windows auditing features to track attempts to log in and delete files.
- Setup file control, as discussed in *Protecting Data Files using NTFS* on page 53.
- Ensure that appropriate backup procedures are in place for data files and the Security and Spectrum ES databases. For details, see *Backup and Recovery* on page 58.

Windows Login Security

During installation of the software, folder and file security permissions are automatically set so that Spectrum ES can run on an NTFS system under the Windows operating system. The Windows Administrator should review these settings and consider whether further changes are required.

The Windows Administrator account is a member of the Administrators group, and this gives the administrator full access to the whole system, including the ability to delete and rename files, run any application, and change user and file/folder permissions.

The Windows User account provides a minimum set of permissions for someone to run the software and use the instrument.

NOTE: Being logged on as a Windows Administrator gives full read/write permissions to the system. To avoid negating the 21 CFR Part 11 compliance, end users (individuals using the Spectrum ES software and instruments to collect data) should run as Windows Users, never as Windows Administrators.

Default Windows Groups and Accounts

The installation of Spectrum ES sets up the following default Windows groups and accounts:

- PKIUsers group – This group is used to set permissions on files, folders and registry entries required for Spectrum ES to work correctly. See below for details of how to administer this group.
- 21CFR_Admin group – A group used for Windows login functionality. This contains the Windows Administrator account, 21cfr, used by Windows login functionality to authenticate Windows user names and passwords.

Administering the PKIUsers Group

All users of Spectrum ES must be members of the PKIUsers group on their local PC.

NOTE: If the Spectrum ES login type is set to Windows Login, users may also need to be made members of a separate Windows Login group. See *Setting up Windows Login* on page 69.

When the PKIUsers group is created during installation of the Spectrum ES software, it contains the global user, "Everyone". However, to provide security, the Windows Administrator should identify the individual Windows users who are to be allowed to use Spectrum ES, add them to this group, and then remove "Everyone".

To add users to the PKIUsers group on a local PC, follow the steps described below.

1. Log in to the PC as a Windows Administrator.
2. On the Control Panel, open **Computer Management** (you wil need to click **Administrative Tools** first in Windows 7 and 8).
   The Computer Management dialog is displayed.
3. In the left-hand panel, click **Local Users and Groups**.
4. In the right-hand panel, double-click the **Groups** folder to see the list of available Groups on the PC.
5. Double-click **PKIUsers**.
   The PKIUsers Properties dialog is displayed.
6. To add a user to the Group, click **Add**.
   The Select Users, Computers, or Groups dialog is displayed.
7. To select a user from a different location (domain), click **Locations** and then select the required location for the user you want to add.
   Click **OK**.

8. Enter the name of the user in the **Enter the object name to select** field and then click **Check Names**.

   Clicking **Check Names** validates the name on the specified domain.

NOTE: To add more users, repeat steps 6–8.

9. Once you have added all the required users, click **OK**.

   The Select Users, Computers, or Groups dialog is closed and the user is added as a member to the PKIUsers Properties dialog.

10. Click **OK** and then close all the Control Panel dialog boxes.

Administering PKIUsers When Using Spectrum ES Across a Network

If Spectrum ES is to be used across a network, with a single, shared, Security database, the Windows Administrator should create a user group on an accessible domain, and add users to that group. This domain group should then be added to the local PKIUsers group on each PC where the software is to be used.

NOTE: For further information on using Spectrum ES across a network, see *Sharing the Databases Across a Network* on page 62.

Windows Auditing

Within the Windows NTFS file system it is possible to audit activities carried out on folders or files. This allows the Windows Administrator to keep a log of which user is accessing what data, and whether this is failing or succeeding.

For example, it is possible to set auditing of the folder where the data files are stored, and monitor attempts to delete files.

NOTE: Audit logs can get very large, and occupy a lot of disk space, if not set up and managed carefully.

Login auditing is also available within Windows to monitor access to the system. For example, this may be used to look for failed attempts to log in. Login auditing can be set from the **Audit Policy** section of the local security settings for your PC, accessible using the Microsoft Management Console. Consult your system administrator for further details, as some security settings may be controlled by your company's IT policy.

Protecting Data Files using NTFS

The NTFS file system allows the Windows Administrator to set security permissions for each file and folder, as required. If accidental or malicious deletion of data is to be avoided, setting up the right permissions on data files is an important consideration within a 21 CFR Part 11 compliant environment.

Users must be able to write data files to the NTFS file system, but must not be able to change or delete them.

Viewing the Security Tab

If you are using Windows XP, carry out the following procedure to ensure that the Security tab within the file/folder Properties dialog is available when applying the security settings.

NOTE: If the Security tab is already visible when accessing the Properties dialog for files and folders, this procedure may be ignored. This procedure is also not required if you are using Windows 7 or 8.

1. Open Windows Explorer and select the C: drive, or the drive where Spectrum ES has been installed.

NOTE: If you do not want to apply the change to all folders within the drive, this procedure must be repeated for each folder where the change needs to be applied, and you should ignore step 6.

2. From the Tools menu, select **Folder Options**.
   The Folder Options dialog opens.
3. Select the View tab.
4. Within **Advanced settings** scroll to the very bottom.
5. Deselect **Use simple file sharing (Recommended)**.
6. Click **Apply to All Folders**.
7. Click **OK**.
   The Folder Options dialog closes.

Applying Security Settings

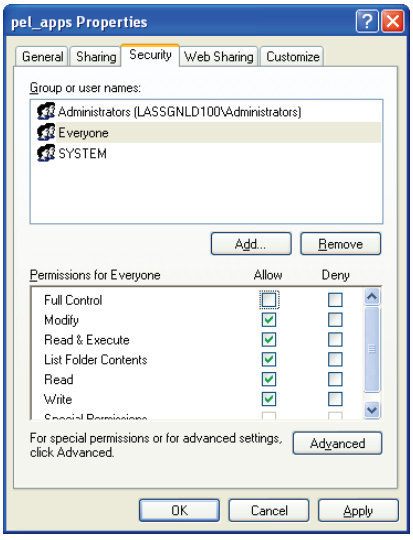
It is important to set the security settings for a number of Spectrum ES files and folders. A number of files and folders need the Modify permission set for Everyone.

NOTE: In each case, C:\ refers to the drive on which Spectrum ES is installed.

1. In Windows Explorer, right-click the C:\pel_apps folder and select **Properties**.
2. In Windows XP, select the Security tab and highlight the **Everyone** group.

   OR

   In Windows 7 or 8, select the Security tab, click the **Edit** button and highlight the **Everyone** group.
3. Remove the tick on the **Full Control Allow** permission, as shown below, and click **OK**.



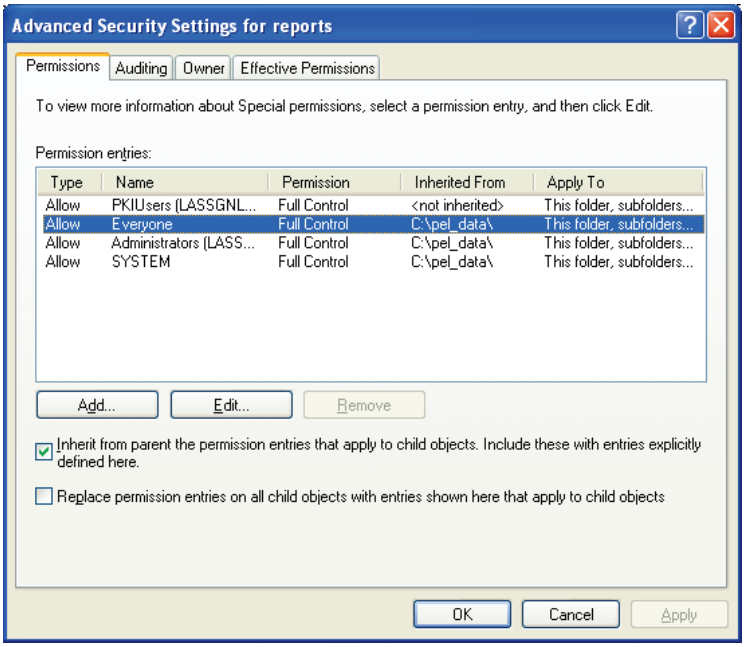
4. Repeat steps 1–3 for the C:\pel_data folder.

Write Once, Read permission must be set on all the subfolders within C:\pel_data:

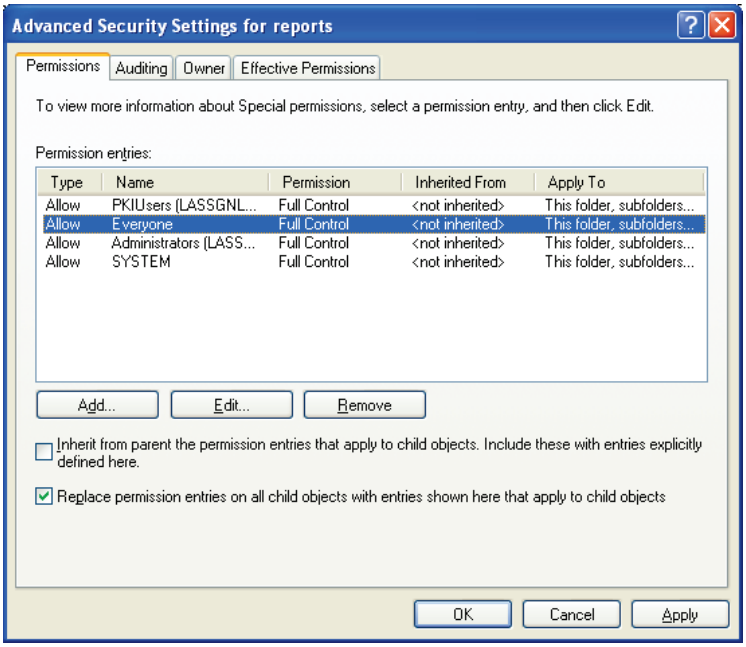
- C:\pel_data\config
- C:\pel_data\equations
- C:\pel_data\export
- C:\pel_data\instrumentsetups
- C:\pel_data\libs
- C:\pel_data\macros
- C:\pel_data\quant (if you are using Spectrum Quant ES)
- C:\pel_data\reports
- C:\pel_data\sampletablesetups
- C:\pel_data\spectra

Follow the steps described below for each subdirectory:

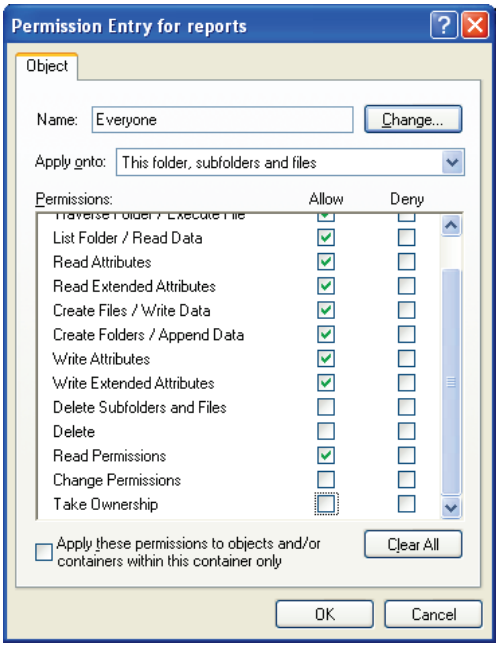
1. Right-click on the subfolder name in Windows Explorer and select **Properties**.
2. Select the Security tab and highlight the **Everyone** group.
3. Click the **Advanced** button.
4. In Windows 7 or 8, click the **Change Permissions** button.
   A screen similar to the one shown below is displayed.



5. Un-check the checkbox with the text starting with *"Inherit from parent the permission entries..."*
   A **Security** message is displayed. Click **Copy** in Windows XP and **Add** in Windows 7 or 8**.**
6. Check the checkbox with the text *"Replace permission entries on all child objects."*
   The **Inherited From** column should now display **<not inherited>**, as shown below.



7. Highlight the **Everyone** group and click **Edit.**
8. Un-check the following permissions in the **Allow** column.
   - Delete Subfolders and Files
   - Delete
   - Change Permissions
   - Take Ownership



9. Click **OK** to apply the settings and return to Windows Explorer.

Backup and Recovery

Backing up Files and Databases

It is essential that backups of key files and databases are taken regularly, to secure data in the event of computer failure or accidental loss or damage. The following files and folders (including sub-folders) should be included in a back-up schedule.

NOTE: Some of these folders are hidden by default.

File / Folder name	Function
C:\pel_data (and sub-folders)	Default location for user data saved to disk; for example, spectra.
C:\pel_apps	Contains instrument installation and AVI calibration information.
C:\Documents and Settings\All Users\ Application Data\PerkinElmer\Security System\Users.mdb (Windows XP) OR C:\ProgramData\PerkinElmer\Security System\Users.mdb (Windows 7/8)	The Security database, containing information about users, groups, permissions, etc., including the Setup Users audit trail.
C:\Documents and Settings\All Users\ Application Data\PerkinElmer\Security System\Backup\Users.bak* (Windows XP) OR C:\ProgramData\PerkinElmer\Security System\Backup\Users.bak* (Windows 7/8)	A backup of the Security database, Users.mdb; overwritten each time the software is closed. Up to three backup files are maintained.
C:\Documents and Settings\All Users\ Application Data\PerkinElmer\Spectrum\ Spectrum10ES*.mdf (Windows XP) OR C:\ProgramData\PerkinElmer\Spectrum\ Spectrum10ES*.mdf (Windows 7/8)	The current and any previous Spectrum ES databases. The Spectrum ES database contains information about all user activities on the system, including the Spectrum ES audit trail.
C:\Documents and Settings\All Users\ Application Data\PerkinElmer\Spectrum\ Spectrum10ES_log*.ldf (Windows XP) OR C:\ProgramData\PerkinElmer\Spectrum\ Spectrum10ES_log*.ldf (Windows 7/8)	A log of the changes in the Spectrum ES database.

File / Folder name	Function
C:\Documents and Settings\All Users\ Application Data\PerkinElmer\Spectrum\ Spectrum10ESdatabases.mdf (Windows XP) OR C:\ProgramData\PerkinElmer\ Spectrum\Spectrum10ESdatabases.mdf (Windows 7/8)	A file containing information about all the Spectrum ES databases, necessary for their management by the software.
C:\Documents and Settings\All Users\ Application Data\PerkinElmer\Spectrum\ Spectrum10ESdatabases_log.ldf (Windows XP) OR C:\ProgramData\PerkinElmer\ Spectrum\Spectrum10ESdatabases_log.ldf (Windows 7/8)	A log of the changes in previous Spectrum ES databases.
C:\Documents and Settings\All Users\ Application Data\PerkinElmer\Quant\ QuantES.mdf (Windows XP) OR C:\ProgramData\PerkinElmer\Quant\ QuantES.mdf (Windows 7/8)	The current Spectrum Quant database, containing information on all user activities in the Spectrum Quant ES software, including the audit trail.
C:\Documents and Settings\All Users\ Application Data\PerkinElmer\Quant\ QuantES_log.ldf (Windows XP) OR C:\ProgramData\PerkinElmer\Quant\ QuantES_log.ldf (Windows 7/8)	A log of the changes in the Quant database.
C:\Windows\Pel_inst.ini	Contains instrument settings.

Recovering the Security Database

Spectrum ES automatically creates a backup of the security database (Users.mdb) each time the software is closed. A maximum of three backup files are maintained: users.bak1, users.bak2, and users.bak3. These are replaced in sequence, with users.bak1 always being the most recent and users.bak3 the oldest.

If the active database becomes corrupt or gives a checksum failure, the Windows Administrator can use these files to recover the database, as follows:

1. Log in as a Windows Administrator.

2. Rename or move the current database file C:\Documents and Settings\All Users\Application Data\PerkinElmer\Security System\users.mdb (Windows XP) or C:\ProgramData\PerkinElmer\Security System\users.mdb (Windows 7/8).

3. Copy the most recent backup file C:\Documents and Settings\All Users\Application Data\PerkinElmer\Security System\Backup\Users.bak1 to C:\Documents and Settings\All Users\Application Data\PerkinElmer\Security System\Users.mdb (Windows XP) or C:\ProgramData\PerkinElmer\Security System\Backup\Users.bak1 to C:\ProgramData\PerkinElmer\Security System\Users.mdb (Windows 7/8).

It should then be possible to log in again. Some data may be lost if there were any changes to the users and groups made since the last time the software was closed.

If the most recent backup continues to give a checksum failure message, repeat step 3 above using the users.bak2 file and then, if the problem persists, users.bak3.

The older the backup you have to use to recover the Security database, the more likely it is that some data will have been lost.

Recovering the Spectrum ES Database

If the Spectrum ES database becomes corrupted, the Windows Administrator should recover the current and previous databases.

NOTE: The Spectrum ES database has a default maximum size of 5.5 GB. When it reaches this size, a new database is automatically created by the software. The last part of the filename is a sequence number, which is incremented for each new database.

The system also maintains a file called Spectrum10ESdatabases.mdf. This file contains information about all the Spectrum ES databases, necessary for their management by the software, and should also be recovered.

- Copy the 'Spectrum10ES*' and 'Spectrum10ESdatabases' .mdf and .ldf files from backup into the locations listed in the table on page 58.

Any changes made since the most recent backup was taken will be lost.

Changing the Spectrum ES maximum database size

The default Spectrum ES maximum database size is 5.5 GB. If required, you can increase this up to the maximum size supported by the version of Microsoft SQL Server Express installed on your system:

- SQL Server Express 2005 – 4 GB
- SQL Server Express 2008 – 4 GB
- SQL Server Express 2008 R2 – 10 GB

1. Navigate to the folder C:\Program Files\PerkinElmer\Spectrum.

2. Open the file IRWinLab.exe.config in Notepad.

3. Search for the text string MaxAuditTrailDatabaseFileSize.

4. Amend the current value to the new maximum size you require, in bytes.

5. Save the file.

The new maximum database size comes into effect the next time you use Spectrum ES.

NOTE: If you decrease the Spectrum ES maximum database size to a value which is below its current size, a new database, with an incremented sequence number, is created the next time you use Spectrum ES.

Recovering Other Files

Any other files that become corrupted, .ini and .cfg for example, can be recovered by copying the appropriate backup file to the correct location.

Other Considerations

Sharing the Databases Across a Network

If you have multiple installations of PerkinElmer software that use the Security and Spectrum ES databases, containing details of Spectrum ES users, groups and audit trails, you should consider whether to share the databases across a network.

The advantages of sharing the databases are:

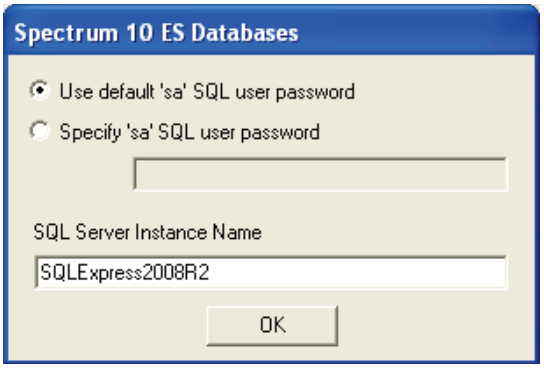
- PerkinElmer user names and passwords are global, and so can be re-used with multiple products.
- The security policies for all PerkinElmer applications using the security system can be applied consistently.
- The Setup Users audit trail is located in one database.
- Network file storage is typically more reliable than PC hard disk storage.
- Backups might be easier to manage as they can be incorporated into your company's IT-based backup process.

Setting up the shared databases

SQL Server 2008 R2 Express is used by Spectrum ES to communicate with the databases that are shared across the network. SQL Server 2008 R2 Express is installed on the local PC during the software installation (see *Spectrum ES Installation* on page 14), but it needs to be installed on your network if databases are to be shared. A port on the network server must then be opened to allow access to the databases.

Network Installer

1. Browse to the file **SQLExpress2008R2NetworkInstall** on your *Spectrum ES Software* DVD, and double-click the file to run the installation.
2. Click Run when prompted to run the Shared Management Objects application.
   The dialog below is eventually displayed.



   If you already use SQL Server 2008 R2 Express on your network with other applications, then you can choose to use it with the new version of Spectrum ES as well. This may simplify the administration of the system.

3. Click **OK** to select the default password option and use a new instance of SQL Server Express with the new version of Spectrum ES.

   OR

   Select **Specify 'sa' SQL user password**, enter the password and instance name for an existing version of SQL Server Express that you want to use with Spectrum ES, and click **OK**.

NOTE: This instance of SQL Server Express only applies to the sharing of databases across the network. It is separate from the instance of SQL Server Express installed on the local PC (refer to *Spectrum ES Installation* on page 14).

4. Open Windows Firewall from the Control Panel of your PC, and set up a connection to the UDP 1434 port on the network server.

   In Windows XP, an exception can be created to add a port for connecting to the network. In Windows 7/8, use the New Outbound Rule Wizard to select the port and apply the connection when your computer detects that it is present (that is, when the computer is connected to your corporate domain).

This procedure creates Spectrum ES (Audit Trail) databases on the network that you can use.

Database Tools

The Database Tools application is used to configure and register the databases for Spectrum ES. You must have local Windows Administrator permissions to carry out operations using Database Tools.

1. From the Start menu, select Programs\PerkinElmer Applications\Spectrum\Database Tools.

2. Login with your PerkinElmer administrator account Username and Password.

   The Database Tools application starts.

3. Select the type of database you want to work on, Security database or Audit Trail (Spectrum ES) database, by clicking the appropriate icon in the left panel.

   A list of available databases of that type is displayed, with a tick in a green circle showing the current database.

Security Database

When Spectrum is installed, the Security database is installed on the local PC. It is recommended that you create a version on the network. You can then use Database Tools to register this database and use it with Spectrum ES. The Security database must be registered to share it across a network.

If you wish to continue using the same Security database as used by the previous version of Spectrum ES, then carry out the following steps:

1. Use Windows to copy the Security database to a location on the network server.

2. Highlight the Security database in Database Tools.

3. Click **Register Database** and specify the name and full path to the Security database on the network server.

Spectrum ES (Audit Trail) Database

Spectrum ES version 10.3.3 or earlier did not permit Spectrum ES (Audit Trail) databases to be shared across a network. Later versions give the user the following options for sharing a database:

- Register and use the new network database created by the network installer;
- Upgrade an existing database on the local PC and move it to the network.

To use the new network database:

1. Select the database in the Audit Trail Database screen of Database Tools.
2. Click **Register Database**.
3. Browse to the database location on the network server and enter the full path, including the filename.
4. Enter the local path on the server for the database, and click **OK**.
5. Highlight the Spectrum ES database in the list and click **Set Active Database**.
   The active database is marked with a green circle.

To upgrade an existing database:

1. Select the database in the Audit Trail Database screen of Database Tools.
2. Click **Upgrade**, **Yes** and then **OK** once the upgrading process is completed.
   The software will inform you if the database does not require upgrading.

NOTE: If there is more than one Spectrum ES database, each one will need to be upgraded separately.

The upgraded database can be shared across the network by carrying out the following steps:

1. Use Windows to copy the Spectrum ES database to a location on the network server.
2. Select the database in the Audit Trail Database screen of Database Tools.
3. Click **Register Database**.
4. Browse to the database location on the network server and enter the full path, including the filename.
5. Enter the local path on the server for the database, and click **OK**.
6. Highlight the Spectrum ES database in the list and click **Set Active Database**.
   The active database is marked with a green circle.

For further details, see the Database Tools on-screen Help.

NOTE: Remember to regularly backup any databases used by Spectrum ES that are shared on the network. Refer to *Backing up Files and Databases* on page 58 for a list of the essential files to backup.

Creating a Dedicated User for Spectrum ES

If required, the Spectrum ES Windows Administrator can use the Spectrum Stand Alone Configurator utility, provided with the software, to restrict the activity of specified Windows Users to the Spectrum ES software only, and deny any access to the Windows operating system. If appropriate, the system can also be set up to automatically login as one of the dedicated Spectrum ES users when the PC is switched on.

Full details on how to run the Spectrum Stand-Alone Configurator can be found at C:\Program Files (x86)\PerkinElmer\Spectrum\Documents\Configuring a PC for Stand-Alone Operation.RTF.

Shut Down Windows with Spectrum ES Still Running

When you want to shut down Windows, first make sure that you have exited from Spectrum ES (ensuring all data is saved, if necessary). We do not recommend that Windows is shut down before exiting from the software as this can cause problems with the shut down procedure, and may require the use of Task Manager to ensure a clean Windows shutdown.

Recovering from Power Failures and Unexpected Software Events

In the event of a sudden power failure or software "crash", some of the workspace data may be left unsigned.

When the software is next started, it compares the current workspace setup with the signed information held in the database and, if a difference is found, the user is given the option to reload the previously saved workspace, and a new entry is added to the audit trail to indicate Workspace Recreated. The user can then work on the data and apply their electronic signature to it.

If the user chooses not to reload, the old data is left unmodified and a new workspace is created.

Removing Accessories During a Scan

Spectrum ES tries to cater for most unexpected occurrences, but if an accessory is removed from the instrument during a scan or a background scan this will cause an error. This is not recommended practice, as the act of removing an accessory will invalidate the data.

Spectrum ES Software Administration

Overview

The Spectrum ES Software Administrator must maintain the security of Spectrum ES software, to ensure technical compliance to 21 CFR Part 11. To do this, the Software Administrator is required to:

- Define how users log in to Spectrum ES; see *Spectrum ES Login Types* on page 69.
- Administer users of the Spectrum ES software, including adding new users, assigning them to groups and setting group permissions; see *Managing Users and Groups* on page 73.
- Configure the activities where changes made by users trigger the need for an electronic signature; see *Configuring Electronic Signature Points* on page 83.
- Monitor the Setup Users audit trail, the Login History, and the Security Summary; see *Viewing and Managing the Setup Users* Audit Trail on page 86, *Viewing the Security Summary* on page 87, and *Viewing the Login History* on page 88.

NOTE: The Software Administrator does not need to be a Windows Administrator; they can be a Windows User if required.

NOTE: It is important to remember that the Software Administrator assigned to administer the Spectrum ES software will automatically have the permissions required to administer any other PerkinElmer applications that have been installed and which use the PerkinElmer Security system.

In the same manner, user names are global; that is, a user name assigned to one PerkinElmer application is automatically made available to all other PerkinElmer applications.

However, although administrators and users are global in nature, groups and instruments assigned to the software are application specific. The exception is Spectrum Quant, which is installed with Spectrum ES and shares the same security database.

Spectrum ES Login Types

There are two ways to log in to Spectrum ES. The Software Administrator is responsible for determining which login type is used.

- PerkinElmer Login

  This involves creating a user name and password for each Spectrum ES user, in addition to their Windows login on the PC.

- Windows Login

  This allows Windows users to log in to Spectrum ES using their Windows user name and password, instead of having a separate Spectrum ES user name and password.

NOTE: Changing the login type within Spectrum ES will automatically change the login type for all other PerkinElmer software that shares the same Security database.

Setting up PerkinElmer Login

When Spectrum ES is installed, it is set to PerkinElmer Login by default. This login type is ideal when users do not have individual Windows accounts, and log in to Windows systems using common or generic user names.

When PerkinElmer Login is used, the Software Administrator can create user names and passwords specifically for Spectrum ES.

To setup the Spectrum ES users and groups see *Managing Users and Groups* on page 73.

Setting up Windows Login

Windows Login is appropriate if your users all have individual Windows user names (either on a Windows domain, or locally on the PC) and you want to use the same user names and passwords when running Spectrum ES.

NOTE: A Windows user account which does not have a password cannot be used to log in to Spectrum ES.

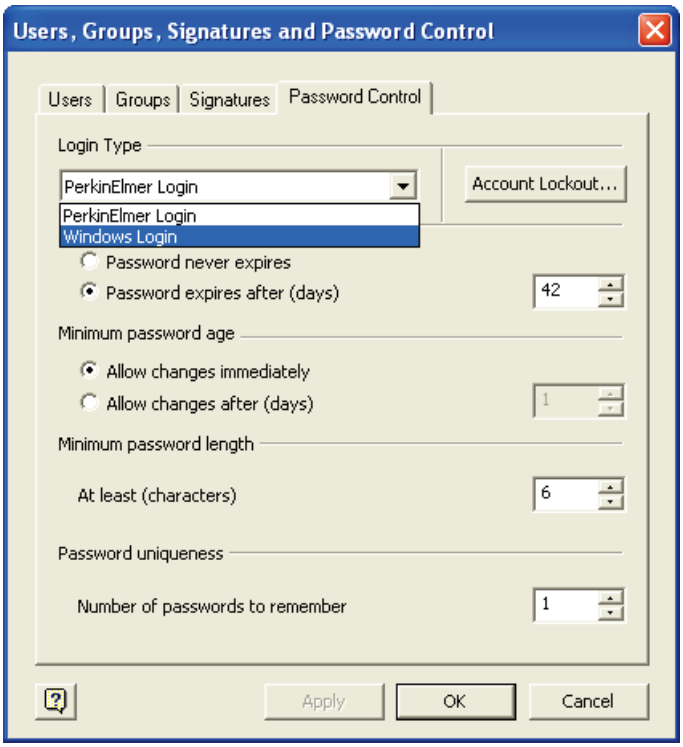
When you set the Spectrum ES login type to Windows Login, you must specify the name of a Windows group whose members are to be allowed to use the Windows Login facility. By default this is the PKIUsers group on the local PC, created when the software was installed.

However, if appropriate, the Windows Administrator can create an alternative group, containing details of users who are to be allowed access using Windows Login. The software will then only allow members of the specified Windows group, who are also members of the PKIUsers group on the local PC, to access Spectrum ES. For further details, see *Administering the PKIUsers Group* on page 50.

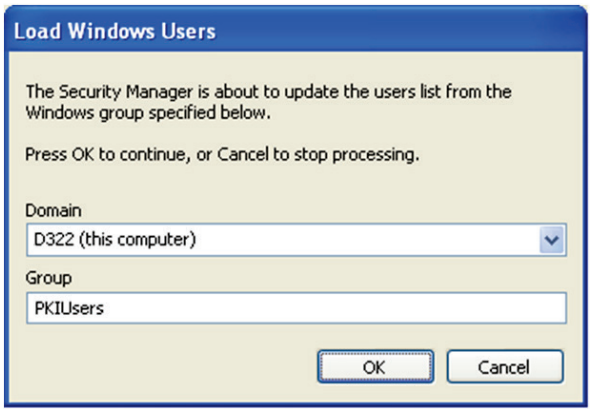
NOTE: All members of the Windows Login group must be members of PKIUsers on the local PC they are going to use.

To set the Spectrum ES login type to Windows Login, follow the steps described below.

1. Log in to Spectrum ES software as a Software Administrator.
2. From the Administration menu, select **Setup Users**.
3. On the Password Control tab, change the Login Type to **Windows Login**.



The Load Windows Users dialog is displayed.

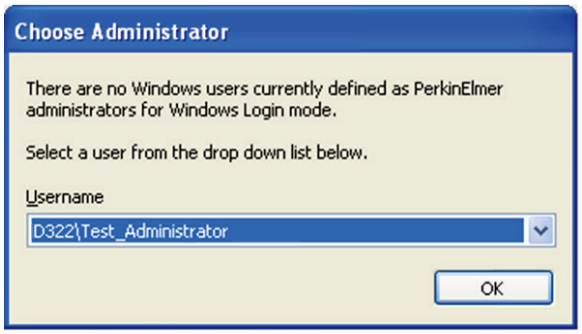


4. If appropriate, select the Domain and Group containing the Windows users you want to be able to access the software.

   The default is the PKIUsers group on your local PC.

5. Click **OK**.

   As there is no administrator defined for PerkinElmer software, the Choose Administrator dialog is displayed.



6. Use the drop-down to select the user who is to be the PerkinElmer Software Administrator and then click **OK**.

7. Click **OK** again to close the Setup Users dialog.

8. Exit the Spectrum ES software.

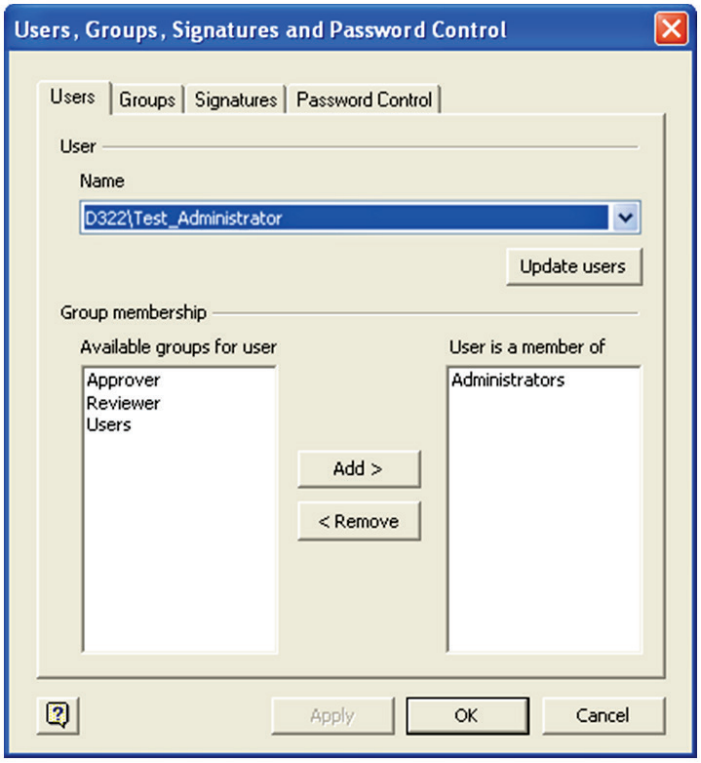
At this point, the login type is set to Windows Login, but only one user (the Software Administrator) has access to the software. The Software Administrator must now log in to Spectrum ES to specify permissions for the other users in the specified Windows group.

The steps below describe how to set up your remaining users and configure your administrator.

1. Log in to Spectrum ES software as the Software Administrator.

2. From the Administration menu, select **Setup Users**.

   On the Users tab, the **Name** drop-down contains all the users who are members of the Windows Login group. Each of these users must be assigned to the appropriate group or groups within Spectrum ES.



- Any user required to be a Spectrum ES Software Administrator must be made a member of the Administrators group. We recommend that at least two users are set up as Software Administrators, for emergency use.
- Any user requiring access to Spectrum ES software must be made a member of at least one group.

3. Select each user in turn from the **Name** drop-down and configure them appropriately. See *Assigning a User to a Group* on page 77 for details.
4. When you are finished, click **OK**.

Users can now access the Spectrum ES software.

Managing Users and Groups

A user's access to functions within the Spectrum ES software depends on the permissions set by the Software Administrator. Part of the planning process for establishing Spectrum ES within a 21 CFR Part 11 compliant environment must be to plan the permissions allocated to the users and groups that best fit the company's working procedures.

Each user of Spectrum ES is assigned to one or more user groups. Each group is able to perform operations such as acquiring data or approving results, as defined by the permissions allocated to that group by the Software Administrator.

NOTE: Only a person who is a member of the Administrators group is able to set up Users and Groups.

Managing users and groups involves:

- Understanding the Spectrum ES pre-defined groups; see *Pre-defined Groups* on page 74 for details.
- Creating new users and assigning them to groups; see *Creating a New Spectrum ES User* on page 75 and *Assigning a User to a Group* on page 77.
- Defining group permissions, in terms of both software activities that can be performed and instruments that can be used; see *Defining what Members of a Group are able to do* on page 78 and *Defining which Instruments Members of a Group can use* on page 80.
- Adding and deleting your own groups; see *Creating and Deleting Groups* on page 81.

For details of other user administration activities such as managing user passwords, disabling user access, and what to do if a user is locked out, see the on-screen Help by selecting **Contents and Index** from the Help menu in the Spectrum ES software.

Pre-defined Groups

The following pre-defined groups are provided in Spectrum ES:

- Administrators
- Users
- Reviewer
- Approver

Each group is given permission to access various features of the program. Some of these permissions can be defined by Administrators and others are always enabled.

Administrators group

Members of this group are able to administer the software, manage users and groups, and add and remove instruments. Their activities are restricted to administrative tasks and they are excluded from typical user activities.

NOTE: The permissions associated with this group cannot be changed.

NOTE: Members of the Administrators group cannot be assigned permissions allowing access to other, non-administrative, Spectrum ES functions.

If a Software Administrator needs to carry out other activities, they must be added to one of the other groups such as Users, which would typically allow them to carry out a wide-range of day-to-day tasks.

Users group

The software permissions available to members of this group are defined by the Software Administrator. By default, members of this group can perform all operations other than the tasks associated with Administrators, and the Review and Approve functions. These include:

- Selecting an instrument from those available to the group.
- Setting instrument parameters and carrying out instrument verifications and ready-checks.
- Collecting and saving data.
- Setting-up and running processes.
- Setting-up equations, Quant parameters, and macros.
- Running reports and exporting data.
- Creating, editing and saving Quant methods in Spectrum Quant software.

Reviewer group

Members of this group are intended to act as reviewers of changes that have been made by other users, and then signed with an electronic signature. By default, members of this group are assigned to the Review and Return Workspace functions, and can also import and export various objects to make them available to users as required.

Approver group

Members of this group are intended to act as approvers of changes that have been made by other users, signed with an electronic signature and then reviewed. By default, members of this group are restricted to the Approve and Return Workspace functions, and can also import and export various objects to make them available to users as required.

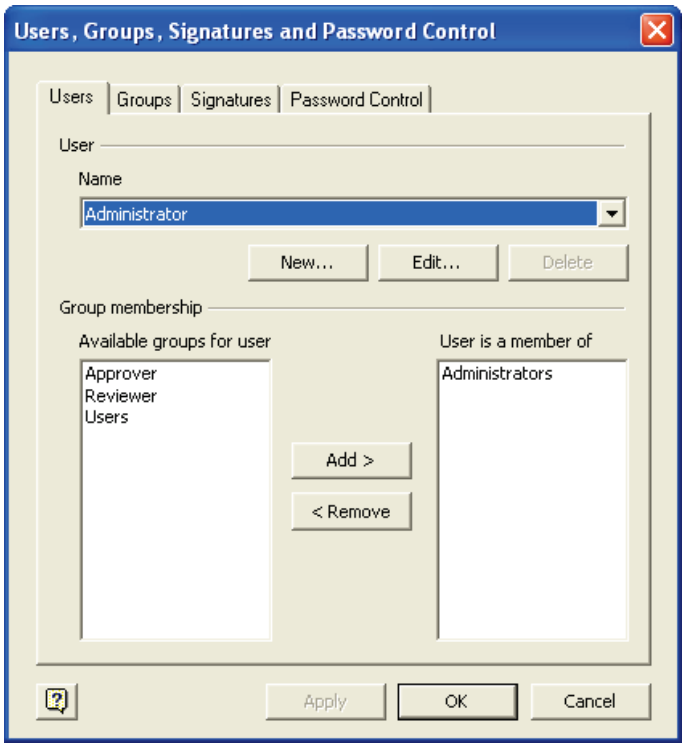
Creating a New Spectrum ES User

Each person using Spectrum ES must be set up as a user by the Software Administrator.

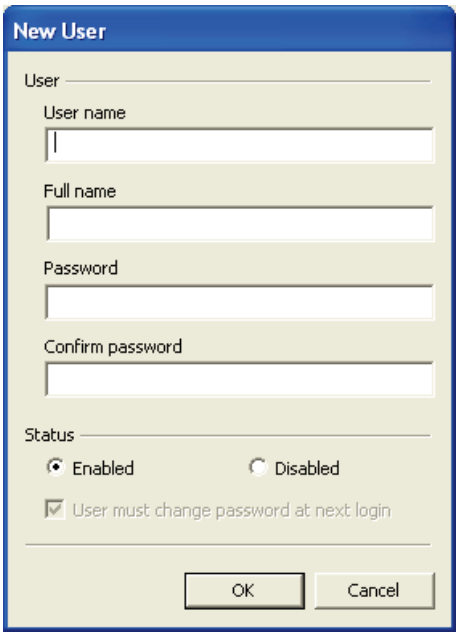
For PerkinElmer Login Type

To create a new user for the Spectrum ES software within a PerkinElmer Login environment, follow the steps described below.

1. From the Administration menu, select **Setup Users**.
   The Users, Groups, Signatures and Password Control dialog is displayed.



2. Select the Users tab and then click **New**.
   The New User dialog is displayed.



3. Enter the **User name**, **Full name**, **Password**, and then re-enter the password in the **Confirm password** entry field.
   The password is case-sensitive. It can consist of letters, numbers and single spaces only.

NOTE: Each user name must be unique.

4. Select **Enabled** if you want the user to be able to log in, or **Disabled** if you do not want them to be able to log in at the current time.
   User must change password at next login is always selected when a new user is created. This ensures that the user is forced to change their password when they first log in, and means that the password is known only to the user and not the Software Administrator.

5. Click **OK**.
   The **Name** drop-down list is updated with the new user.

6. Add the user to a group, to allow access to the software.
   See *Assigning a User to a Group* on page 77.

For Windows Login Type

To create a new user for the Spectrum ES software within a Windows Login environment, follow the steps described below.

NOTE: Before you start, a Windows Administrator must have created the new Windows user and added that user to both the PKIUsers group and, if appropriate, to the group defined for Windows Login users. See *Administering the PKIUsers Group* on page 50 and *Setting up Windows Login* on page 69 for details.

1. Log in to Spectrum ES as a Software Administrator.
2. From the Administration menu, select **Setup Users**.
   The Users, Groups, Signatures and Password Control dialog is displayed.
3. Select the Users tab and then click **Update Users**.
4. Add the user to the appropriate groups, to allow access to the software.
   See *Assigning a User to a Group*, below.

Assigning a User to a Group

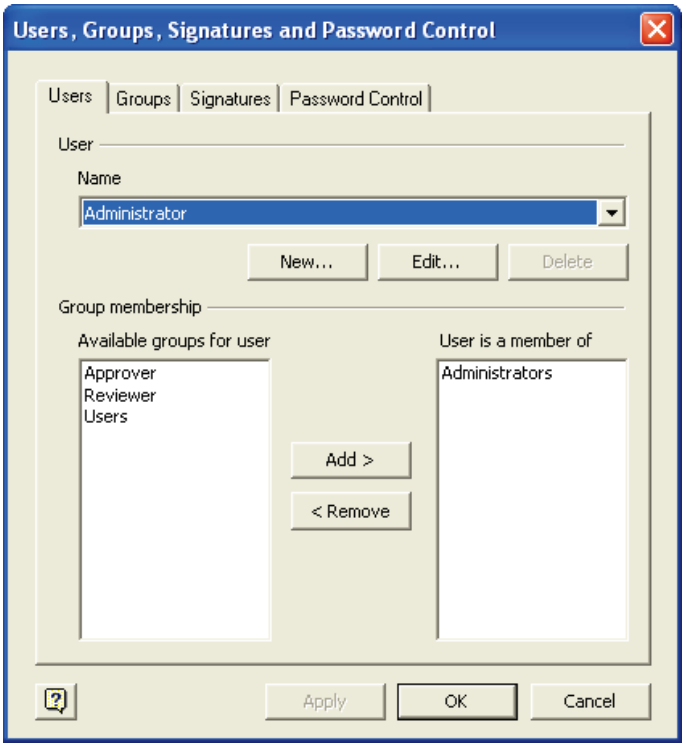
Users must be assigned to one or more groups. The user acquires the permissions assigned to all the groups of which they are a member.

NOTE: When using the Windows Login, at least one user must be assigned to the Administrator group. If not, it will not be possible to exit the software.

NOTE: If a user is not added to at least one group, an error message is displayed when they try to log in, informing them that they do not have access to the application.

To assign a user to a Spectrum ES group, follow the steps described below.

1. From the Administration menu, select **Setup Users**.
   The Users, Groups, Signatures and Password Control dialog is displayed.



2. Select the Users tab and then select the user from the **Name** drop-down list.

3. Select the Group from the list of **Available groups for user** and then click **Add**.
   The Group is moved to the **User is a member of** list.

NOTE: When a group is moved to the **User is a member of** list, it no longer appears in the **Available groups for user** list.

4. Click **OK** to close the dialog and apply the changes.

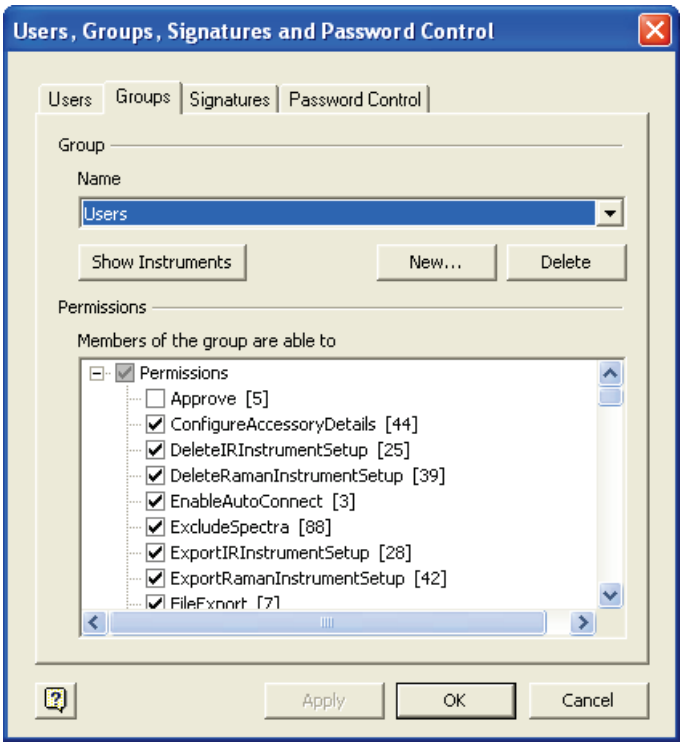
Defining what Members of a Group are able to do

The permissions available to each group are selected on the Groups tab. The permissions are listed as a tree structure. Some permissions are selected by default.

NOTE: A Software Administrator cannot modify the default group permissions assigned to Administrators.

1. From the Administration menu, select **Setup Users**.
   The Users, Groups, Signatures and Password Control dialog is displayed.

2. Select the Groups tab and then select the group from the **Name** drop-down list.



The Permissions area shows the currently selected and unselected permissions for the group.

A tick indicates that the permission is selected for the group.

3. To select all the permissions, click **Permissions** at the top of the tree.

   All the permissions are then automatically checked.

   OR

   To assign one or more (but not all) permissions, click the box next to the permission you want to assign to the group.

NOTE: When only some of the permissions are selected, the check box at the top of the tree is grayed to indicate that not all of the options are selected.

4. When all the required permissions are selected, click **Apply**.

   The available options for the group are updated.

NOTE: The numbers at the end of each permission are used in the Setup Users audit trail. When you change group permissions, it is these numbers that are shown rather than the description of the permission.

Defining which Instruments Members of a Group can use

By default, all groups are able to use all instruments. When a new instrument is added, it becomes available for use by all members of all groups.

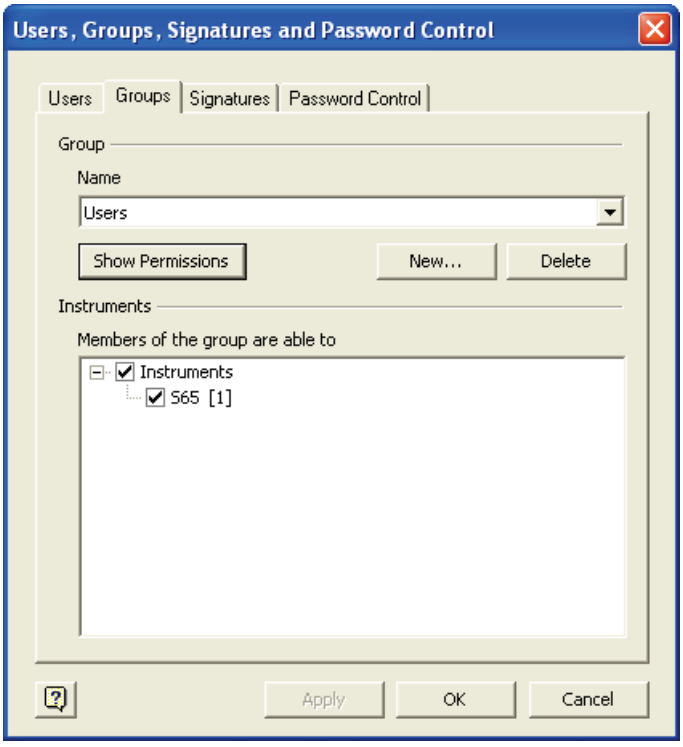
However, if required, the Software Administrator can restrict access to particular instruments to members of specified groups.

1. From the Administration menu, select **Setup Users**.
   The Users, Groups, Signatures and Password Control dialog is displayed.

2. Select the Groups tab.

3. Select the required group from the **Name** drop-down list.

4. Select **Show Instruments**.



5. Select those instruments you want members of the group to be able to use. Deselect those not required by members of the group.

6. Click **OK**.

NOTE: The numbers assigned to the instruments are used in the Setup Users audit trail. When you change group access to instruments, it is these numbers that are shown rather than the description of the instrument.

Checking which Groups a User has been Assigned to

1. From the Administration menu, select **Setup Users**.
   The Users, Groups, Signatures and Password Control dialog is displayed.
2. Select the Users tab.
3. Select the required user from the **Name** drop-down list.

The groups to which the User belongs are listed in the **User is a member of** panel.

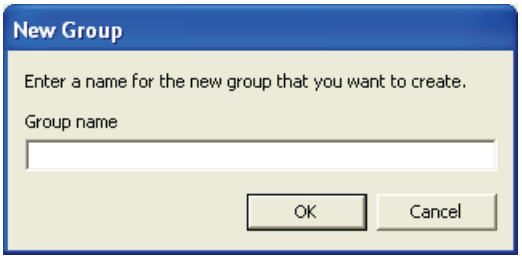
Creating and Deleting Groups

If required, a Software Administrator can create further groups in addition to the pre-defined groups provided by the software. Groups can also be deleted, if required.

Creating a new group

To create a new group, follow the steps described below.

1. From the Administration menu, select **Setup Users**.
   The Users, Groups, Signatures and Password Control dialog is displayed.
2. Select the Groups tab and then click **New**.
   The New Group dialog is displayed.



3. Enter the **Group name**, and then click **OK**.
   The Groups tab is then displayed with the name of the new group shown in the **Name** field and all **Permissions** shown unchecked.
4. Specify the permissions you require for the new group.
   See *Defining what Members of a Group are able to do* on page 78.
5. Select which instruments you want members of the group to be able to use.
   See *Defining which Instruments Members of a Group can use* on page 80.

Deleting a group

To delete a group, follow the steps described below.

1. From the Administration menu, select **Setup Users**.
   The Users, Groups, Signatures and Password Control dialog is displayed.

2. Select the Groups tab and then select the group to be deleted from the **Name** drop-down list.

3. Click **Delete**.
   You are asked to confirm the deletion.

NOTE: If the group you are deleting contains users, the users themselves are NOT deleted. However, if this is the only group they are a member of, they will not be able to access the system until they are assigned to another.

Configuring Electronic Signature Points

An electronic signature as defined by 21 CFR Part 11 is a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

Some activities carried out within the Spectrum ES software are considered critical and require the user to provide an electronic signature. The list of Signature Points within the software is pre-defined. These Signature Points include:

- Data collection.
- Using **Load and Save** to store or reuse instrument settings.
- Reporting on ready checks and instrument validation.
- Generating report output.
- Deleting graphs.
- Approving and reviewing items that have been signed by other users.
- Creating or making changes to equations and macros.

Additional Signature Points are included that pertain to Spectrum Quant ES:

- Saving a Quant method.
- Opening non-ES data.
- Importing or exporting Quant methods.
- Generating report output.
- Locking methods for review or approval.
- Approving and reviewing items that have been signed by other users.

All Signature Points for both Spectrum ES and Spectrum Quant can be viewed and modified from within both applications and, where appropriate, apply to both applications.

The Software Administrator is able to define the settings (that is, whether a signature and comments are required) for each Signature Point individually, or apply the same settings to all Signature Points. In addition, the Software Administrator can, if required, define lists of reasons that may have caused each Signature Point to occur.

When providing a signature, the user must enter their user name and password and select from a list of reasons. They may also be able to add additional comments, if this option has been selected by the Software Administrator.

A user can enter an electronic signature in a number of places:

- Using the **Sign** option from the Setup menu.
- Using the **Sign** button on certain dialogs.
- When they exit the Spectrum ES software.

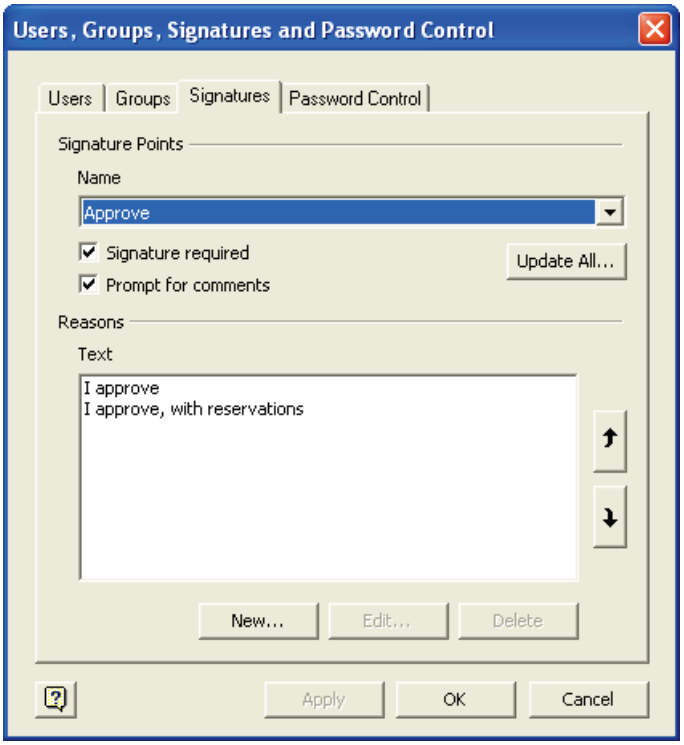
Other than when signing for a particular dialog, a user's signature applies to the whole workspace, and covers all currently unsigned activities logged for the user in the Spectrum ES audit trail.

Once a workspace has been signed by a user, it can be reviewed and approved. See the on-screen Help for details.

Defining Settings for Individual Signature Points

To define the settings and maintain the list of reasons associated with a particular Signature Point, follow the steps described below.

1. From the Administration menu, select **Setup Users**.
   The Users, Groups, Signatures and Password Control dialog is displayed.
2. Select the Signatures tab and then the appropriate Signature Point **Name** from the drop-down list.



3. If an electronic signature is required for a Signature Point, select **Signature required**.
4. If you want the user to be able to add comments, select **Prompt for comments**.

NOTE: A Signature Point will only require a signature if **Signature required** and/or **Prompt for comments** is selected. Otherwise, the software will ignore the Signature Point and the user will not be prompted for a signature.

The list of reasons for the Signature Point is also defined on this tab.

5. To add a new reason, click **New** and use the New Reason dialog to enter the new reason text.

6. To delete a reason, select the Reason from the **Text** list and click **Delete**.

7. To edit a reason, select the Reason from the **Text** list, click **Edit** and modify the text.

8. To change the order in which reasons will be displayed to users, select a reason and click  or  to move it in the list.

NOTE: If **Signature required** and **Prompt for comments** are not selected, when a Signature Point occurs in the software a reason drop-down list will still appear and the user will be required to select a reason. To prevent the dialog appearing, all reasons for the particular Signature Point must be deleted.

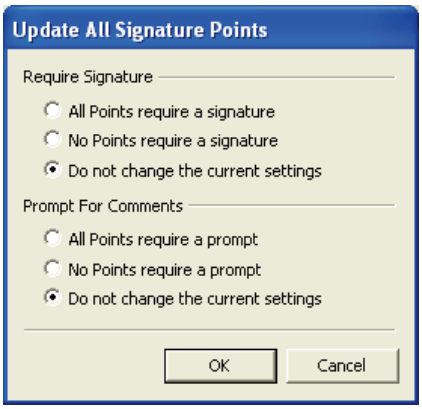
9. Click **OK** to close the dialog and apply the changes.

Defining the Same Settings for all Signature Points

To define the same settings for all Signature Points, follow the steps described below.

1. From the Administration menu, select **Setup Users**.
   The Users, Groups, Signatures and Password Control dialog is displayed.

2. Select the Signatures tab and click **Update All**.
   The Update All Signature Points dialog is displayed.



3. In the Require Signature section, select either **All Points require a signature**, **No Points require a signature**, or **Do not change the current settings**.

4. In the Prompt For Comments section, select either **All Points require a prompt**, **No Points require a prompt**, or **Do not change the current settings**.

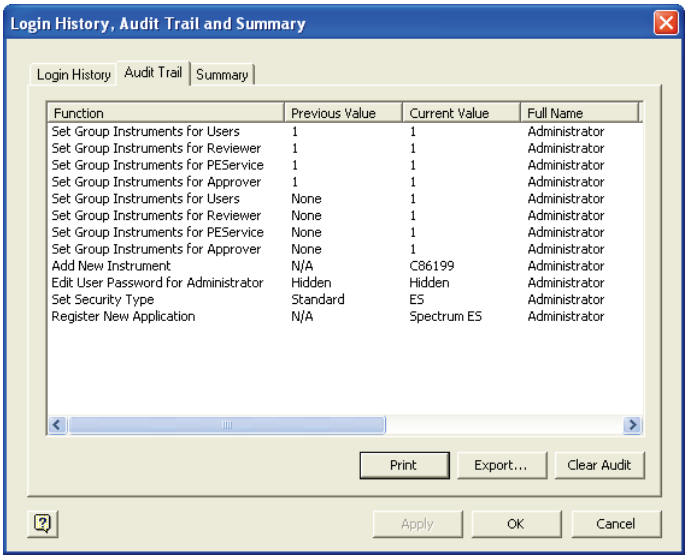
5. Click **OK**.
   The Update All Signatures dialog closes and the Signature Points dialog is re-displayed.

Viewing and Managing the Setup Users Audit Trail

The Setup Users audit trail records all changes to security settings in compliance with 21 CFR Part 11. All changes to users, groups and password settings are recorded.

1. Select **Setup Users Audit Trail** from the Administration menu.
   The Login History, Audit Trail and Summary dialog is displayed.

2. Select the Audit Trail tab.
   The audit trail is displayed.



For each user administration activity performed, the following information is recorded:

- Function – the activity performed; for example, Add New User.
- Previous Value – the state of the item before it was changed.
- Current Value – the new state.

NOTE: Numeric values shown in the Previous Value or Current Value columns represent permissions or instruments. To see the full description of the permission or instrument, refer to the Groups tab on the Setup Users, Groups, Signatures and Password Control dialog or look at the Security Summary where both the number and the description of the permission or instrument is given.

- Full Name – the full name of the user who carried out the activity.
- User Name – the user name of the user who carried out the activity.
- Computer – the name of the computer used.
- Date Modified – the date and time of the activity.

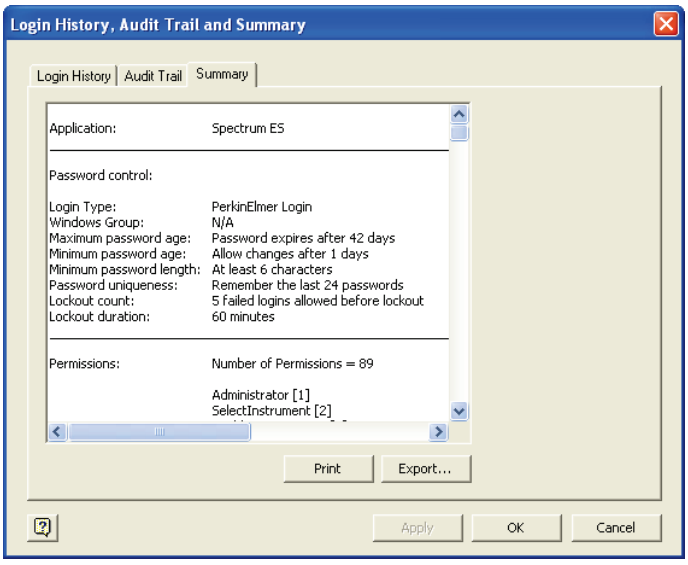
The audit trail can be printed, and exported as a .csv file. After exporting, it can be cleared. We recommend that the exported audit trail is backed up and kept in a secure location.

Viewing the Security Summary

The Security Summary records all information about the security settings.

1. Select **Setup Users Audit Trail** from the Administration menu.
   The Login History, Audit Trail and Summary dialog is displayed.

2. Select the Summary tab.
   The Security Summary is displayed.



The Security Summary shows:

- Password control – the maximum password age, minimum password age, minimum password length, password uniqueness, lockout count and lockout duration.
- Permissions – the number of permissions and a list of all the permissions with their associated number.
- Users – for each user it records the username, full name, status, last login, the groups the user belongs to, and the permissions of the groups.
- Groups – for each group it records the group name, the users in the group, and the group permissions.

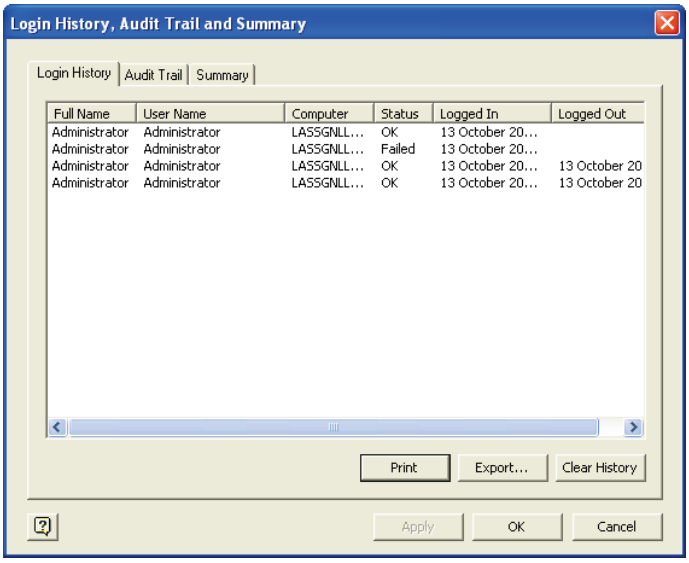
The Security Summary can be printed, and exported as a .csv file.

Viewing the Login History

The Login History details all attempts to log in to the software since the history was last cleared.

1. Select **Setup Users Audit Trail** from the Administration menu.
   The Login History, Audit Trail and Summary dialog is displayed.

2. Select the Login History tab.
   The Login History is displayed.



The Login History shows:

- Full Name – the full name of the user.
- User Name – the user name.
- Computer – the name of the computer.
- Status – **OK** indicates that the user logged in with the correct password, **Failed** indicates that a login was attempted with an incorrect password.
- Logged In – date and time.
- Logged Out – date and time.

NOTE: If a non-existent user name is entered during login, a failed login attempt is recorded. ***Not Found*** is entered in the **Full Name** field of the Login History, and the invalid user name is also recorded.

NOTE: The only limit to the size of the Login History is disk space, but we recommend that you review and archive it at regular intervals.

The Login History can be printed, and exported as a .csv file. After exporting, it can be cleared. We recommend that the exported Login History is backed up and kept in a secure location.

Viewing and Managing the Spectrum ES Audit Trail

NOTE: This is not applicable to Spectrum Quant ES. Refer to *Viewing and Managing the Spectrum Quant ES Audit Trail* on page 91.

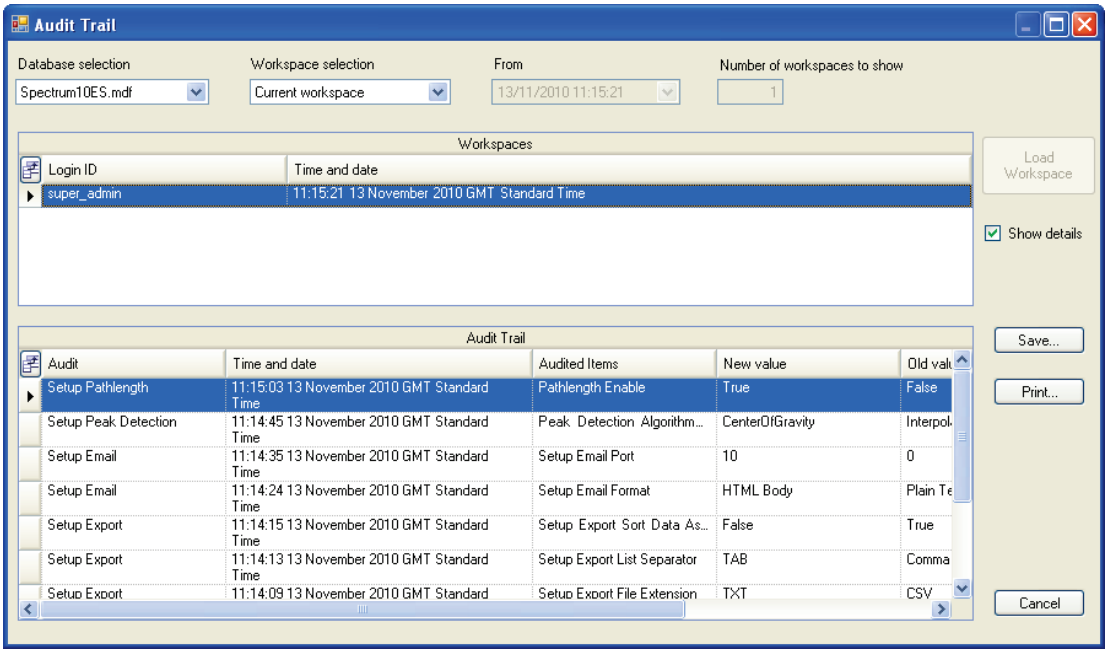
Any activity carried out within Spectrum ES that affects the way data is collected or stored is recorded in a workspace audit trail. These activities include:

- User logins and exits from the software.
- Activities that affect the instruments and accessories that are connected, instrument setup parameters, and instrument verification and ready checks.
- Activities that involve options available from the File menu, Process menu, and Setup menu.
- Data collection activities, using options available from the menu or equivalent toolbar buttons.
- Changing or removing spectral libraries and equations from the workspace.
- Deletion, renaming or opening of spectra.
- Entry of electronic signatures; including those applied when a user exits the software, when the workspace is reviewed, and when it is approved.

Entries are written to the audit trail at the point where a change that has been made affects the recording of data. For example, changes to instrument settings are recorded in the audit trail when the Scan button is pressed, rather than when the change itself is made, as this is when they are applied to the instrument and affect data collection. This means that any changes made to settings that are subsequently cancelled without being used are not recorded.

Displaying the ES Audit Trail

➢ Select **Audit Trail** from the Audit Trail menu.
The Audit Trail dialog is displayed.



Initially, information for the current workspace is displayed.

The Workspaces area, in the upper part of the screen, shows:

- The Login ID of the user who created the workspace.
- The date and time when the workspace was last updated.

The Audit trail area, in the lower part of the screen, shows a chronological list of activities carried out within the workspace (most recent at the top).

For further information on how to use the audit trail, see the on-screen Help.

Viewing and Managing the Spectrum Quant ES Audit Trail

Any activity carried out within Spectrum Quant ES that affects the way data are stored is recorded in a method Audit Trail. These activities include:

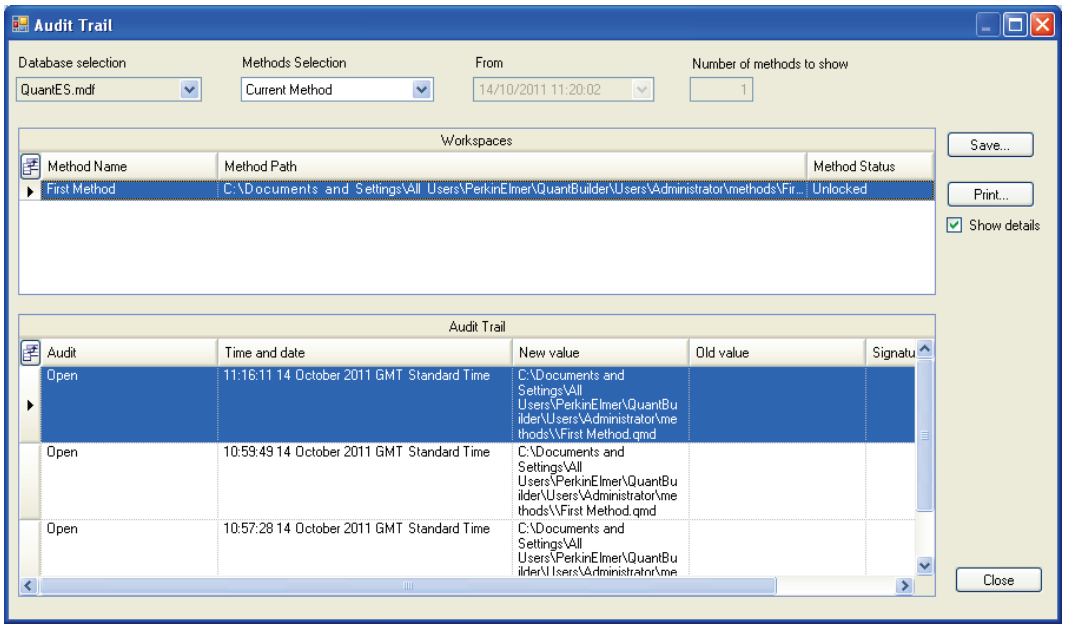
- Opening a method.
- Saving a method.
- Activities that involve options available from the File menu, such as Report and Print.
- Entry of electronic signatures.

Entries are written to the audit trail at the point where a change that has been made affects the recording of data. This means that any changes made to settings that are subsequently cancelled without being used are not recorded.

Displaying the Spectrum Quant ES audit trail

➢ Select **Audit Trail** from the Audit Trail menu.

The Audit Trail dialog is displayed.



Initially, information for the current method is displayed.

The upper part of the screen shows:

- The name of the method.
- The path to the location where the method is saved.
- The status of the method, for example, Unlocked, Locked, Reviewed or Approved.

The Audit trail area, in the lower part of the screen, shows a chronological list of activities carried out within the method (most recent at the top).

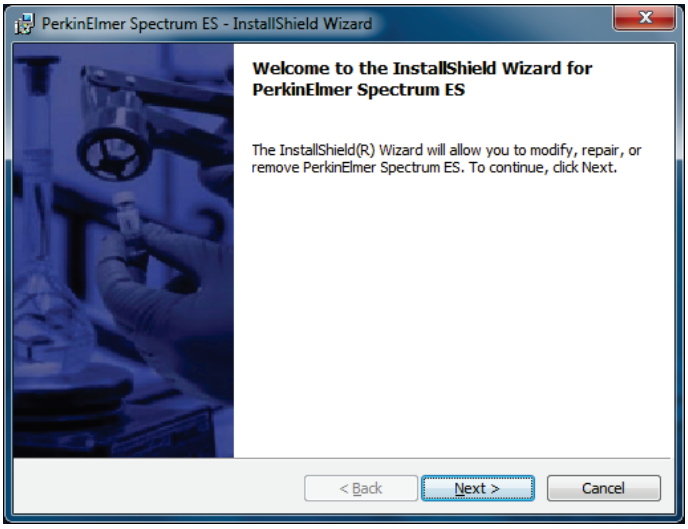
For further information on how to use the audit trail, see the on-screen Help.

Appendices

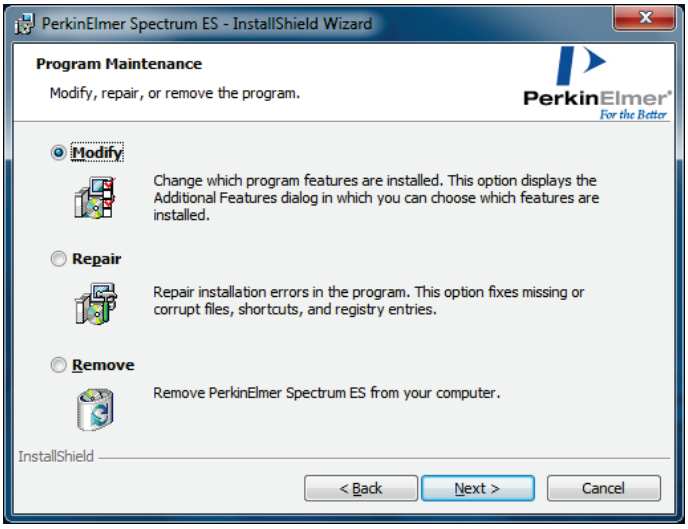
Appendix 1: Installing A New Feature in Spectrum ES

If you have already installed Spectrum ES and you then purchase a license for a new feature, you will need to add this feature by following the procedure below:

1. Start the program **setup.exe** located in the root folder of the DVD or USB Flash Drive.
   The InstallShield Wizard starts and the Welcome page is displayed.

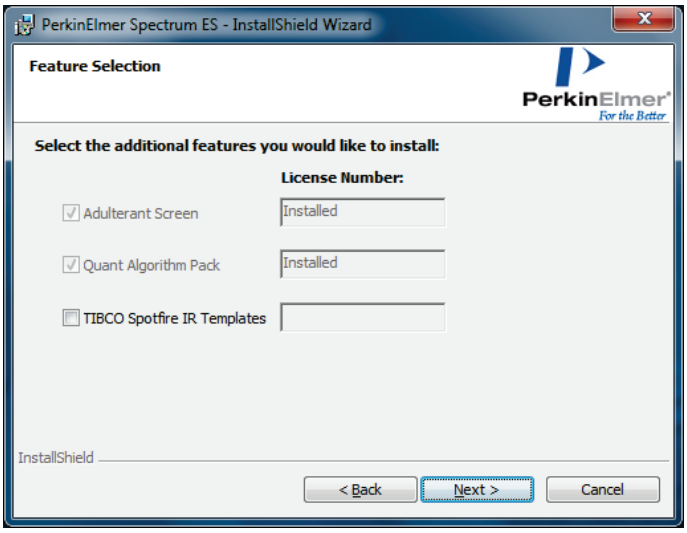


2. Click **Next**.
   The Program Maintenance page is displayed.



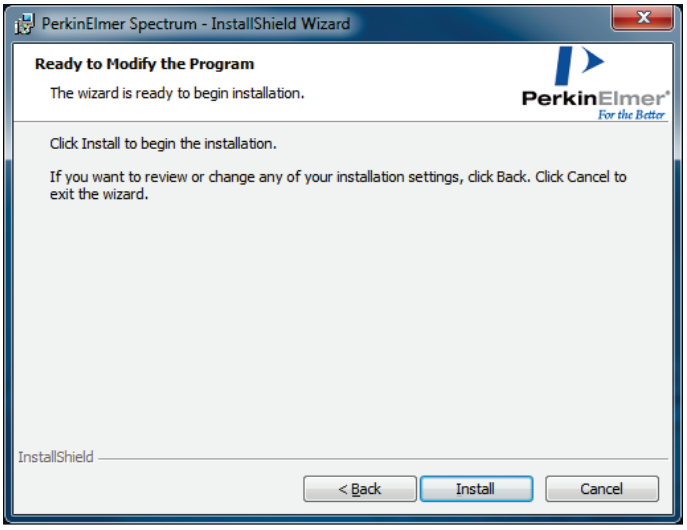
3. Select the **Modify** option, and then click **Next**.

   The Feature Selection page is displayed, showing any features previously installed. In the example below, Adulterant Screen and Quant Algorithm Pack are already installed.



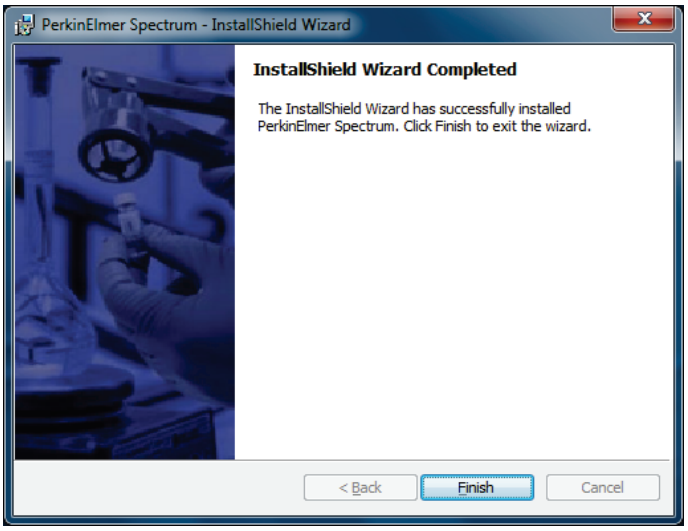
4. Check the checkbox and enter the license number for the new feature you want to install, and then click **Next**.

   The Ready to Modify the Program page is displayed.



5. Click **Install**.

   The software installs the new feature. When completed, the InstallShield Wizard Completed page is displayed.



6. Click **Finish**.

   The installation of the new feature is complete.

NOTE: You cannot use the Feature Selection page of the installer to remove features. To remove licensed features, you must uninstall Spectrum ES completely from your system, and then re-install the software with only the required features selected.

Appendix 2: Configuring your PC Network Adapter

To connect to your instrument using an Ethernet port you will need TCP/IP protocols established on the PC. If TCP/IP communication is not configured on your PC, you will need to do so before you can establish communications between the PC and your instrument. We recommend that you do not install Spectrum ES until this has been set up.

NOTE: The dialogs shown below are typical examples of a straightforward installation; they should not be taken as exact representations of what you will see on your PC. If you need assistance, please talk to your network administrator.

To configure the TCP/IP settings for your PC:

1. For Windows XP and Windows 7, from the Start menu, select **Settings** and then **Control Panel**.

   For Windows 8, right-click at the bottom of the Start screen to display the Apps toolbar, and click the All Apps icon to display the Apps. For Windows 8.1, click the down arrow on the Start screen to display the Apps. Double-click the Control Panel icon in the **Windows System** group.

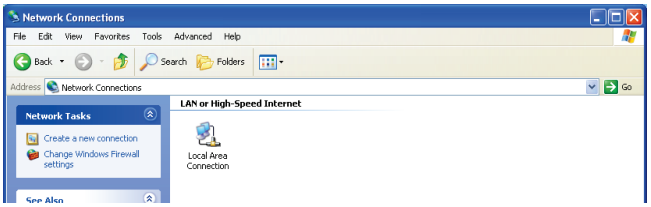
   The Control Panel dialog is displayed.

2. For Windows 7 and 8, display the Network and Sharing Center dialog, and then select **Change adaptor settings**.

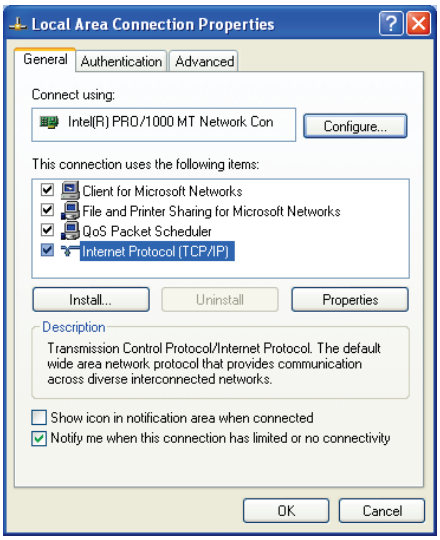
   OR

   For Windows XP, click **Network Connections**.

   The Network Connections dialog is displayed.

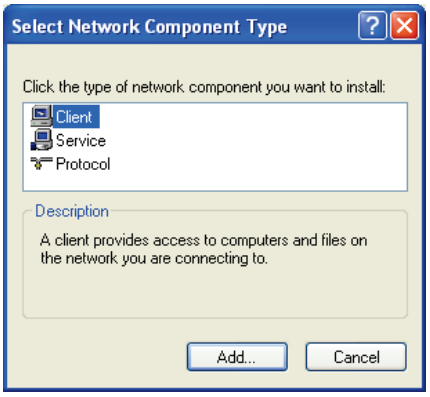


3. Select the Local Area Connection you want to use, right-click and then select **Properties**.
   The Local Area Connection Properties dialog is displayed.



4. If **Internet Protocol TCP/IP** or **Internet Protocol (TCP/IPv4)** is already listed on the dialog, go to step 8.

5. If **Internet Protocol (TCP/IP)** or **Internet Protocol (TCP/IPv4)** is not listed on the dialog, click **Install**.
   The Select Network Component Type dialog is displayed.



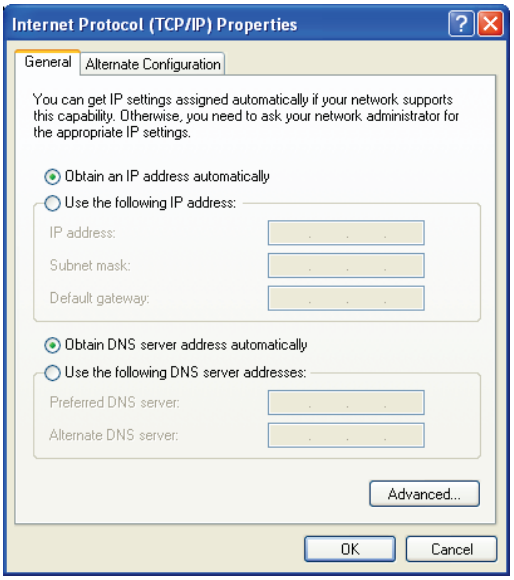
6. Select **Protocol** and then click **Add**.
   The Select Network Protocol dialog is displayed.

7. Select **Internet Protocol (TCP/IP)** and then click **OK**.
   The Local Area Connection Properties dialog is re-displayed, and **Internet Protocol (TCP/IP)** has been added to the list.

8. For Windows 7 and 8, select **Internet Protocol Transfer 4 (TCP/IPv4)** and then click **Properties**.
   The Internet Protocol Version 4 (TCP/IPv4) Properties dialog is displayed.

   OR

   For Windows XP, select **Internet Protocol (TCP/IP)** and then click **Properties.**
   The Internet Protocol (TCP/IP) Properties dialog is displayed.



9. Select **Use the following IP address**.

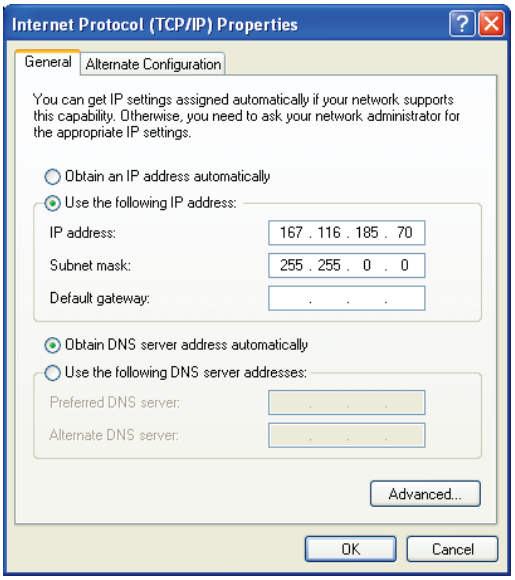
10. Enter the IP address and Subnet mask.

    If your PC is on a network, you may need to consult your network administrator to get an IP address or it may be automatically assigned.

NOTE: If you connect the PC to an Internet-enabled network, you must make sure that the IP address and Subnet mask you use are safe.

If your PC is not on a network, you should enter **167 116 185 70** for the first port and enter **255 255 0 0** as the subnet mask.

For subsequent ports you should enter **167 116 185 69** or lower. The Spectrum Two instrument IP address will be set at **167 116 185 71** or higher, so you should not use these numbers.



11. Select **Obtain DNS server address automatically**.

12. Click **OK** to exit the dialog.

Appendix 3: Changing the IP Address of your Instrument

If you want to use your instrument over a network, then you will need to assign a unique IP address to your instrument. Use the Set IP Address Utility to amend the IP address of your FT-IR instrument.

CAUTION	*Take care to enter new IP address information correctly. We recommend that you keep a record of the new address.* *You cannot communicate with an instrument if its IP address is unknown.*

If you are unable to connect to your Spectrum Two instrument because you do not know the IP address, contact your PerkinElmer Service Representative, or go to the Technical Support website:

www.perkinelmer.com/SpectrumTwoSupport

For other types of FT-IR instrument, contact your PerkinElmer Service Representative.

NOTE: Ensure that Spectrum ES software is not running while using this utility, as the Set IP Address utility may not run correctly.

If you have not yet installed the instrument

1. Connect the Ethernet cable between the instrument and the PC.

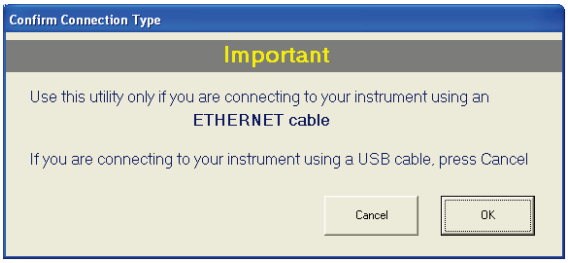
NOTE: At this stage neither the PC nor the instrument should be connected to the network.

2. Connect the instrument to mains power and switch it on.
   For details of how to connect up your FT-IR spectrometer, refer to the user's guide supplied with your instrument.

NOTE: The PC's TCP/IP address must be compatible with the instrument's IP address so that you can connect to the instrument. Refer to *Appendix 2: Configuring your PC Network Adapter* on page 97.

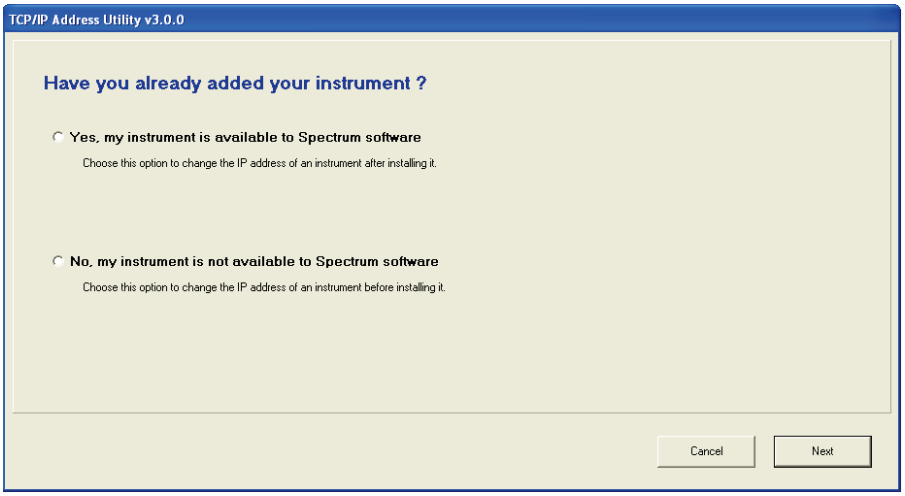
3. Open Windows Explorer and double-click the **Set IP Address** shortcut, which is found in the C:\Program Files\PerkinElmer\ServiceIR or C:\Program Files(x86)\PerkinElmer\ServiceIR directory.

   The Confirm Connection Type dialog is displayed.



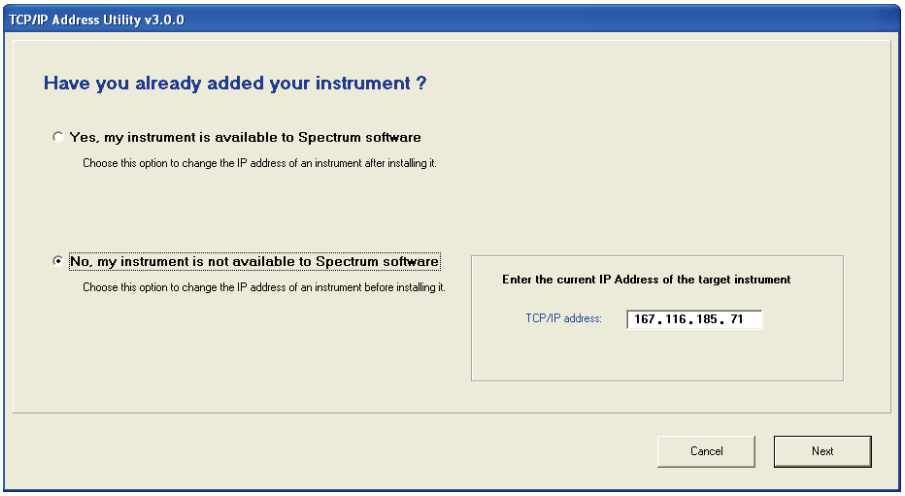
4. Ensure that you are connected using an Ethernet cable, and then click **OK**.

   The Set IP Address program starts.



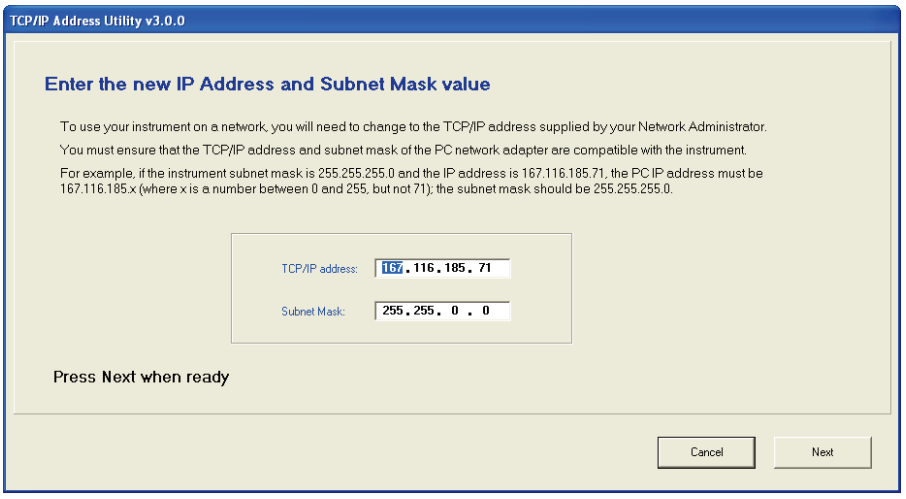
5. Select **No, my instrument is not available to Spectrum software**.

   The dialog updates to show the factory default IP address for instruments.



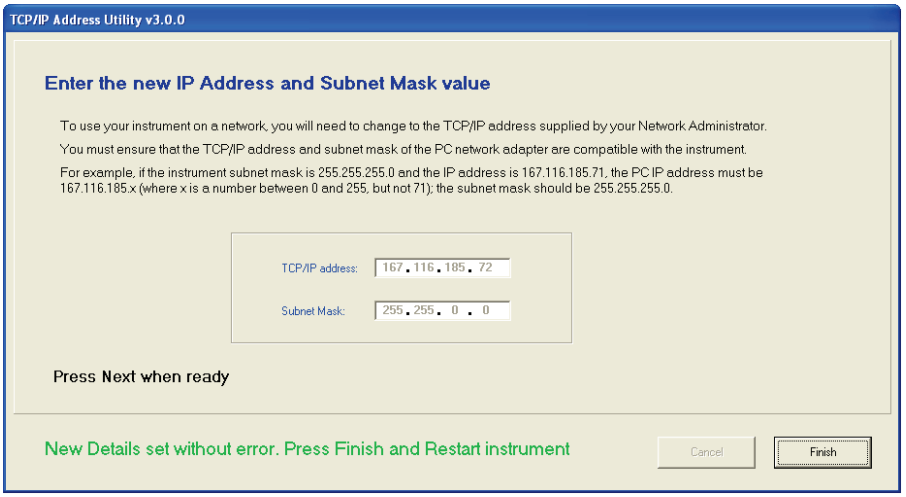
6. Enter the current IP address for the instrument and then click **Next**.

   The Enter the new IP Address and Subnet Mask value dialog is displayed. Refer to the instructions on the dialog.



7. Enter the new address in **TCP/IP address** and **Subnet Mask** and then click **Next**.

   The dialog updates to display a confirmation message and further instructions.



NOTE: The address shown here is only an example and may not reflect the TCP/IP address that you need to use.

8. Click **Finish** to close the Set IP Address utility.

9. Switch the instrument off and then, a couple of seconds later, switch the instrument on again.

The TCP/IP address of the instrument has been successfully changed.

The instrument will not be recognized by Spectrum ES until it has been installed. For information on how to add your instrument to Spectrum ES for connection via a network, see *Instrument Install Wizard* on page 37.

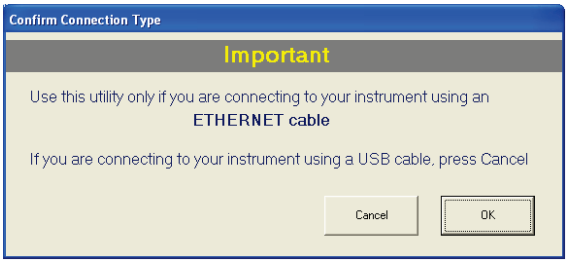
If you have already installed the instrument

1. Ensure that the Ethernet cables between the instrument and the network and between the PC and the network are connected.

2. Connect the instrument to mains power and switch it on.

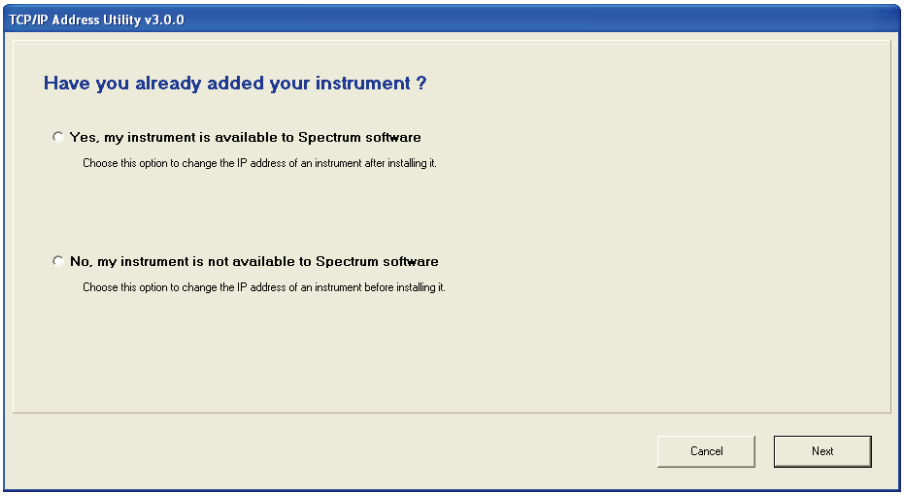
3. Open Windows Explorer and double-click the **Set IP Address** shortcut, which is found in the C:\Program Files\PerkinElmer\ServiceIR or C:\Program Files(x86)\PerkinElmer\ ServiceIR directory.

   The Confirm Connection Type dialog is displayed.



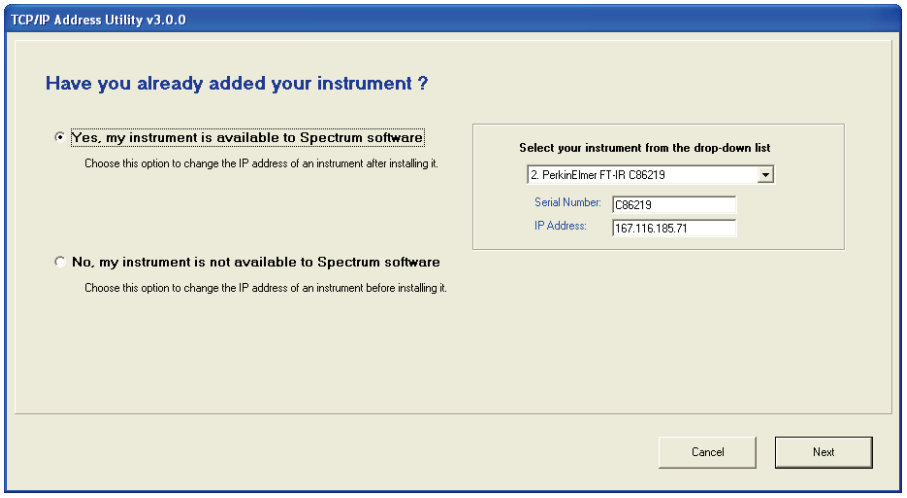
4. Ensure that you are connected using an Ethernet cable, and then click **OK**.

   The Set IP Address program starts.



5. Select **Yes, my instrument is available to Spectrum software**.

   The dialog updates to display a drop-down list of instrument installed in Spectrum software. The Serial Number and current IP Address for the currently selected instrument are also displayed.

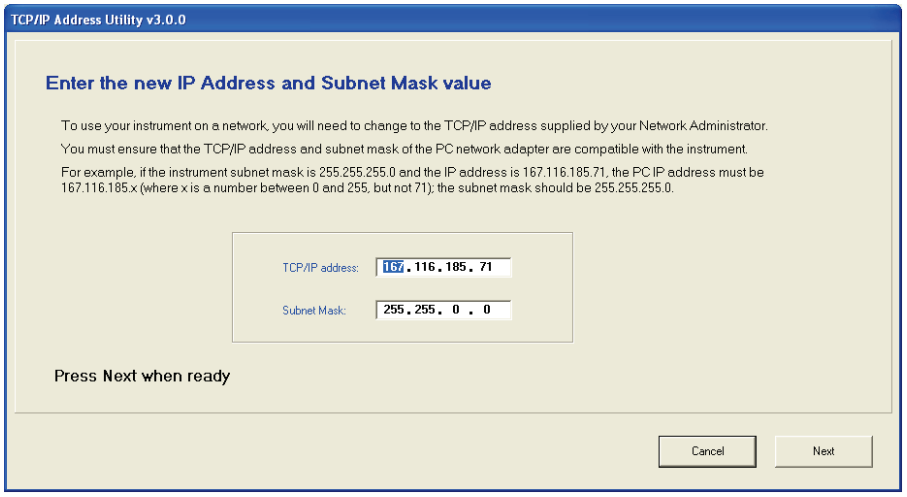


6. Select the instrument you connected to in step 1 from the drop-down list.

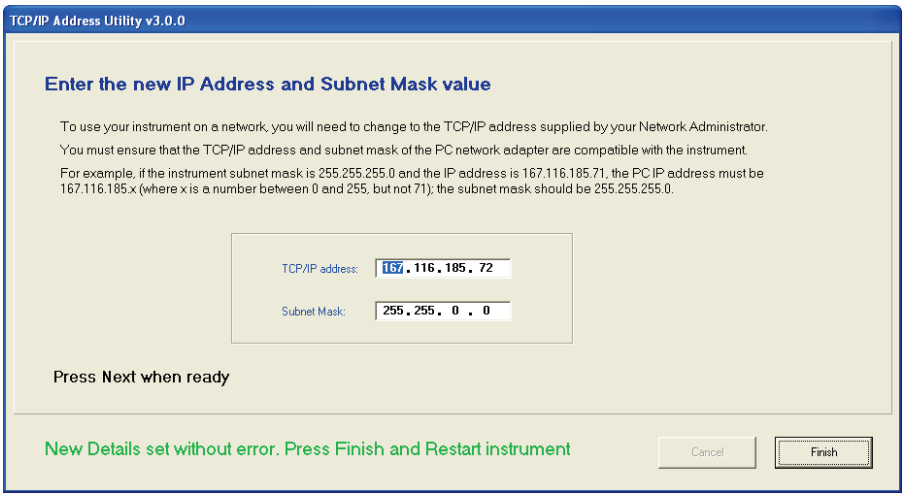
   The Serial Number and current IP Address of the instrument are displayed.

7. Click **Next**.

   The Enter the new IP Address and Subnet Mask value dialog is displayed. Refer to the instructions on the dialog.



8. Enter the new address in **TCP/IP address** and **Subnet Mask** and then click **Next**. The dialog updates to display a confirmation message and further instructions.



NOTE: The address shown here is only an example and may not reflect the TCP/IP address that you need to use.

9. Click **Finish** to close the Set IP Address utility.

10. Switch the instrument off and then, a couple of seconds later, switch it on again.

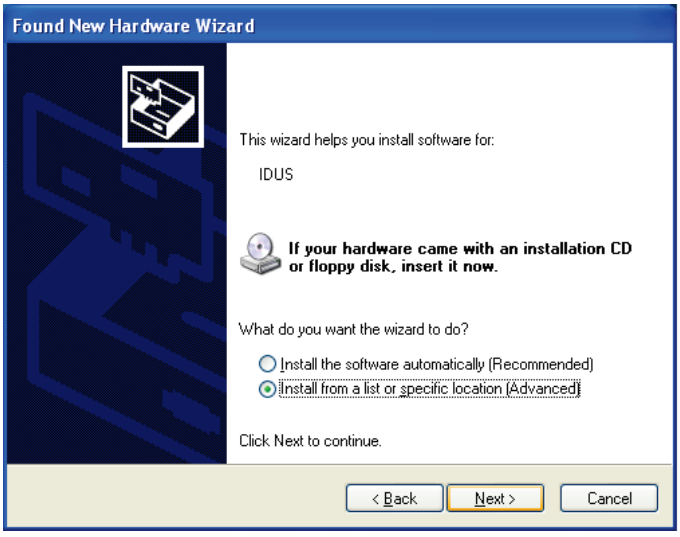
The TCP/IP address of the instrument has been successfully changed.

Appendix 4: Reinstalling the Raman Instrument CCD Drivers

You may be prompted to reinstall the drivers if you disconnect the instrument control USB cable and reattach it to a different USB port, or, on rare occasions, if you switch the instrument off and then switch it on again.

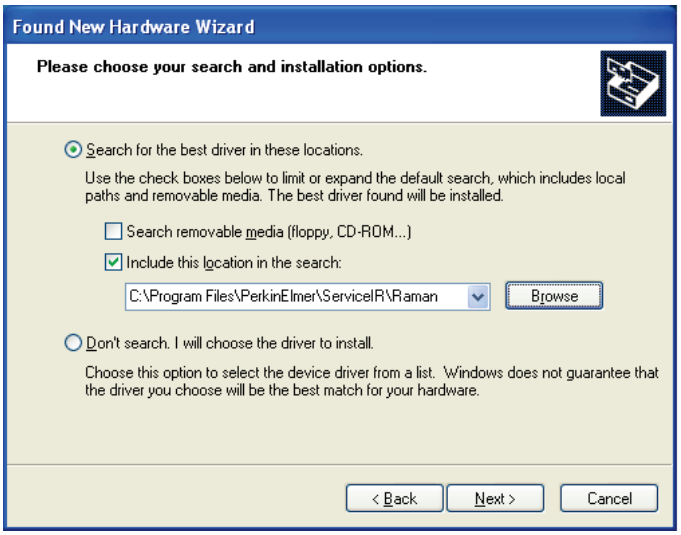
The Found New Hardware Wizard is displayed:

1. Select **No, not this time** and then click **Next.**
   The Found New Hardware Wizard page is displayed.



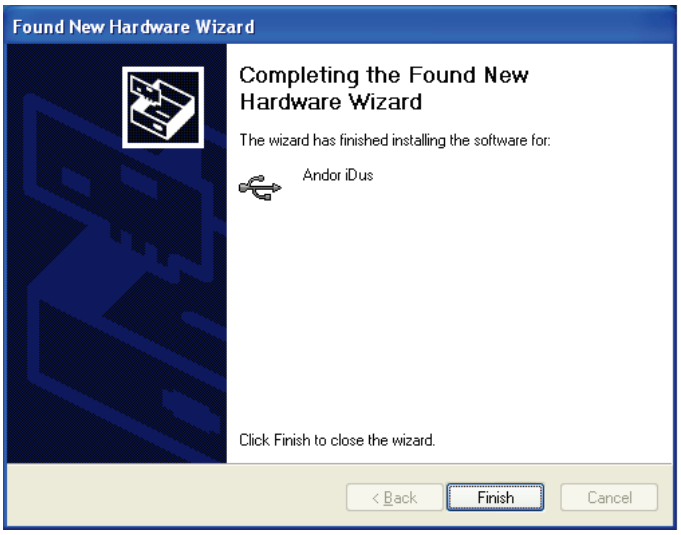
NOTE: The Found New Hardware Wizard page may inform you that it is helping you install software for **USB Device**. In this case continue with the installation in the same way as for **IDUS**.

2. Select **Install from a list or specific location (Advanced)** and then click **Next.**
   The Please choose your search and installation options page is displayed.



3. Select **Include this location in the search,** click **Browse,** and then navigate to C:\Program Files\PerkinElmer\ServiceIR\Raman.
   These options may be displayed automatically as you work through the wizard.

4. Click **Next.**
   The Completing the Found New Hardware Wizard is displayed.



5. Click **Finish.**
   The Found New Hardware Wizard closes.

Appendix 5: Administering the PerkinElmer Enhanced Security Application Account

NOTE: The Enhanced Security Configuration program should be used when you wish to change the default User name and/or Password for the default account **21cfr**. This account is called the Enhanced Security Application Account.

The Security Server functions as an extension of the computer's operating system and is used by the Windows Login functionality of the Spectrum ES software. The Security Server passes to the Windows operating system the account credentials of any user that attempts to log in to the software or perform a signature. Windows can then verify the account credentials of the user. If the account credentials are verified, the user is allowed to log in to the software and sign off signatures.

The Enhanced Security Configuration program allows the Windows Administrator (Local_Administrator) to set preferences and maintain the PerkinElmer Enhanced Security Application Account used by the Windows Login functionality.

To run the Enhanced Security Configuration program:

1. Ensure that the Enhanced Security Application Account is a member of the Administrators, Users and 21CFR_Admin groups on your PC.

2. Start the program C:\Program Files\PerkinElmer\PE21CFR\config21cfr.exe or C:\Program Files (x86)\PerkinElmer\PE21CFR\config21cfr.exe, and log in using the Enhanced Security Application Account name and password.

NOTE: If you are using Windows 7 or 8, you will need to right-click on the config21cfr.exe file and select **Run as administrator** to start the program.

NOTE: The default initial Enhanced Security Application Account is called 21cfr and has the initial password PerkinElmer1.

For details of how to change the account see *Changing the Enhanced Security Application Account* on page 110. For details of how to change the account password, see *Using the Passwords Tab* on page 112.

The Enhanced Security Configuration program is displayed.

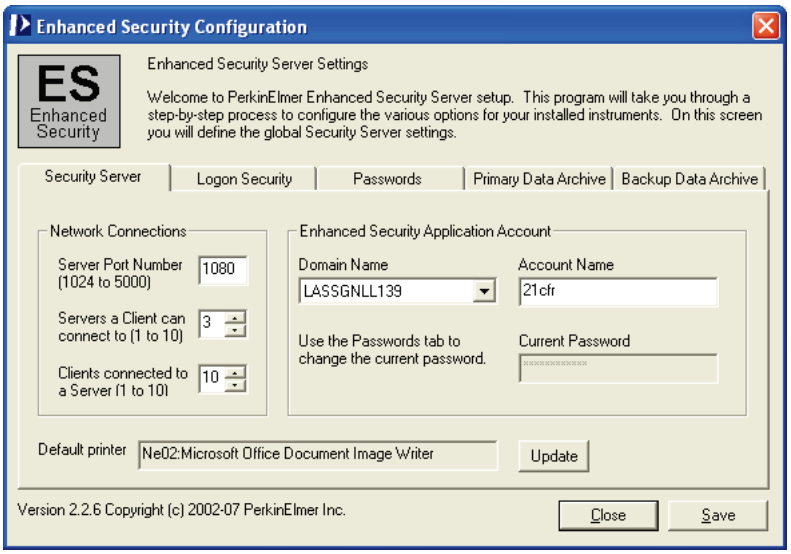
There are five tabs, only two of which are applicable to Spectrum ES users:

- Security Server – Allows you to change the Enhanced Security Application Account details, the Network Connection settings, and the default printer.

- Passwords – Allows you to change the password for the Enhanced Security Application Account.

Using the Security Server Tab

The Security Server functions as an extension of the computer's operating system and is used by the Windows Login functionality of the Spectrum ES software. The Security Server passes the account credentials of any user that attempts to log in to the software or apply an electronic signature to the Windows operating system.



Changing the Enhanced Security Application Account

If your company's security policy requires you to use an account other than 21cfr as the PerkinElmer Security Server Windows User Account, you should follow the steps described below to change it.

1. Create a new Administrator account in Windows.
   The new account must be a member of the local Administrators, Users, and 21CFR_Admin groups.
2. Enter the name of the new account in the **Account Name** field.
3. Ensure that the **Domain Name** is correct.
   The domain name is most likely to be the local PC.
4. Click **Update**.
5. Enter the password of the new account in the **Current Password** field.
6. Click **Save** to save the changes to the Enhanced Security Configuration program.

Changing the Network Connection settings

It is unlikely that you will need to change the Network Connection settings for the Enhanced Security Application Account. However, if there are problems connecting to the security server or an instrument, the following steps may be necessary:

1. If you have installed an application that has the same TCP/IP server port number as that shown in the **Server Port Number** field, change the server port number.

   The **Servers a Client can connect to** field represents the maximum number of Security Servers (including the local computer) that a client application can be connected to at any one time. This value will be greater than one if an application must start programs on other computers on the network.

2. The **Clients connected to a Server** field represents the number of applications that a server can have connected at any one time.

   The default value is 10.

Changing the printer

To change the default printer:

1. Change the printer using the Windows operating system tools.

2. Return to this tab and click **Update**.

Using the Passwords Tab

The Passwords tab of the Enhanced Security Configuration program allows you to change the password for the Enhanced Security Application Account.

Changing the password for the Enhanced Security Application Account

To change the Enhanced Security Application account password, follow the steps described below.

1. Leave the Enhanced Security Configuration program open at the Passwords tab.
2. On the Control Panel, open **User Accounts**.
   The User Accounts dialog opens.
3. Select the Enhanced Security Application Account name (displayed in the **Account Name** field in the Enhanced Security Configuration program), and then click **Reset Password**.
   The Reset Password dialog is displayed.
4. Enter the new password, confirm the new password, and then click **OK**.
5. In the Enhanced Security Configuration program, select **Update password in this program after changing in Operating System** in the Password Policy section.
   The **New Password** and **Confirm Password** fields are enabled.
6. Enter the new password in the **New Password** and **Confirm Password** fields.
7. Click **Save** to save the changes to the Enhanced Security Configuration program.
   You must restart your PC after making any changes.

Troubleshooting the Enhanced Security Configuration Program

The information below describes how to respond to error messages you may encounter when running the Enhanced Security Configuration program.

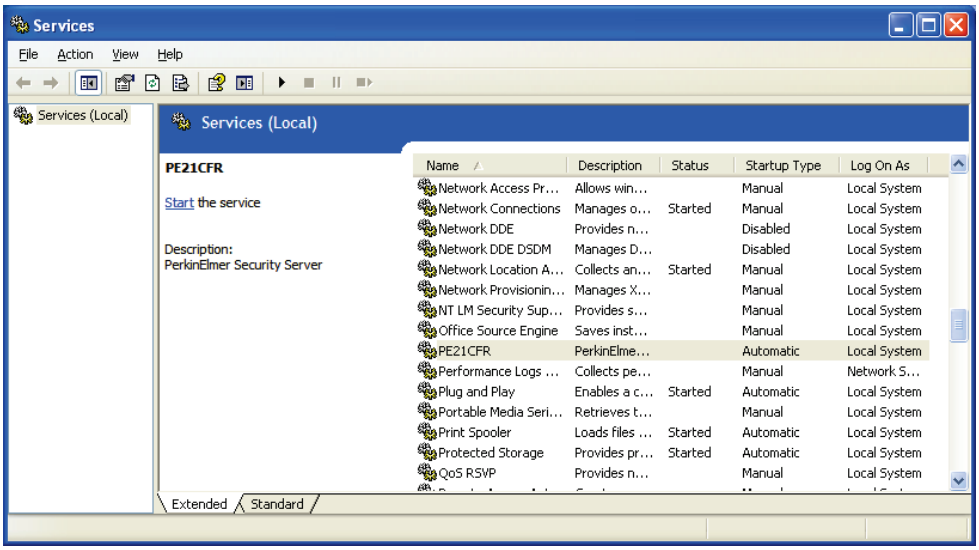
Server error message

The Server error message, shown below, is typically displayed when you try to run the Enhanced Security Configuration program when the Security Server is not running.

To resolve this issue:

1. Restart the computer and try again.
   If restarting does not resolve the problem, continue with the steps described below.
2. On the Control Panel, open **Administrative Tools** and then select **Services**.

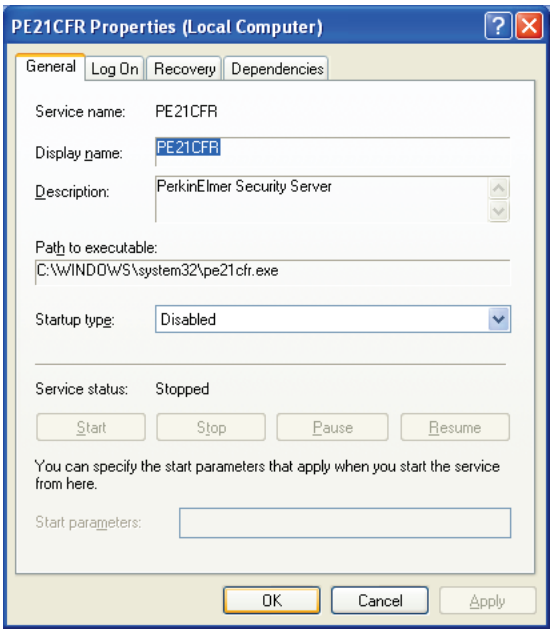
3. Under **Services**, select **PE21CFR.**
   The Services dialog is displayed.



4. At this point:
   - If the Startup Type is Automatic, click **Start the service**. The Security Server should start running.
   - If the Startup Type is either Manual or Disabled, you must change this to Automatic, and then click **Start the service**. This change may require the intervention of your Windows System Administrator.

To change the Startup Type:

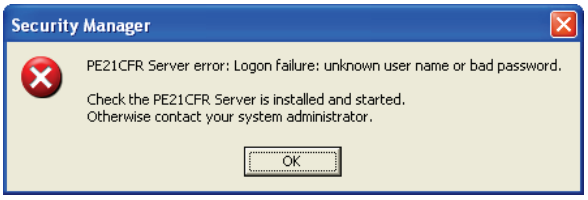
1. Right-click **PE21CFR**.
2. Select **Properties** from the menu.
   The PE21CFR Properties (Local Computer) dialog is displayed.



3. Select **Automatic** from the **Startup type** drop-down list.
4. Click **OK**.
5. Press **Start** in the Services window.

Logon failure message

If the password for the 21cfr account (or the account it has been changed to) has been changed but the system has not been properly updated, the following error message is displayed whenever a user tries to log in to Spectrum ES.



To resolve the problem, follow the instructions in *Changing the Enhanced Security Application Account* on page 110, and *Changing the password for the Enhanced Security Application Account* on page 111 that describe how to change the account name and password respectively.

Installation error message

During installation of the Enhanced Security Configuration program, you may see a Configuration error message stating *"Program does not have access rights to continue*".

This message is displayed in response to the following circumstances:

- The password for the Enhanced Security Application Account was changed prior to running the Enhanced Security Configuration program for the first time.

  You must run the Enhanced Security Configuration program prior to changing the password for the Enhanced Security Application Account for the first time. This allows the Enhanced Security Application Account credentials to be verified correctly.

  To resolve this issue, you must delete the Enhanced Security Application Account and reinstall the Enhanced Security program.

- The Enhanced Security Configuration program will not run.

  The local operating system Administrators users group may have been deleted.

  Recreate the Administrators users group on the local system computer. Add the Instrument Application account and the Enhanced Security Application Account to this users group.

Error when running the Enhanced Security Configuration Program (config21cfr.exe)

The following error indicates that the password for the Enhanced Security Application Account has been changed using Windows but not updated in the Enhanced Security Configuration program.

To resolve the problem, enter the new password in the **Enhanced Security Administrator Password** field and then click **Restart**. The Enhanced Security Configuration program and Spectrum ES will work correctly once the PC has been restarted.

Status Monitor

The Status Monitor is a troubleshooting tool that you can use to learn about the status of the Enhanced Security program's Security Server. The Security Server is the portion of the Enhanced Security program that communicates with the Windows operating system to verify the credentials of the accounts that attempt to log in to it.

Starting the Status Monitor

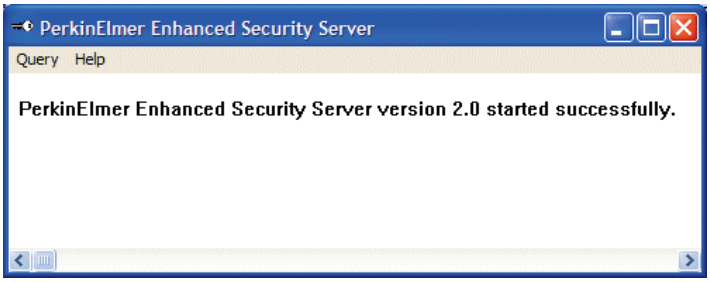
If you have enabled Password Notification with the Enhanced Security Configuration program, the Status Monitor should start automatically. If it does not, follow the steps below to start it manually:

1. Start the program C:\Program Files\PerkinElmer\PE21CFR\pe21cfrsvr.exe or C:\Program Files (x86)\PerkinElmer\PE21CFR\pe21cfrsvr.exe.

   This starts the Status Monitor, as indicated by a key icon in the system tray.

NOTE: If you are using Windows 7 or 8, you will need to right-click on the .exe file and select **Run as administrator** to start the program.

2. Double-click the key icon to display the Status Monitor.

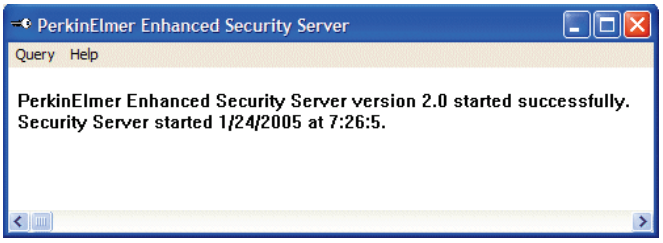


The Query menu allows you to view:

- The status of the Security Server.
- Information about the connections made to the Security Server.
- Information about the software applications that have connected to the Security Server.
- A list of users that have logged on to the Security Server.
- The password status for the Application accounts.

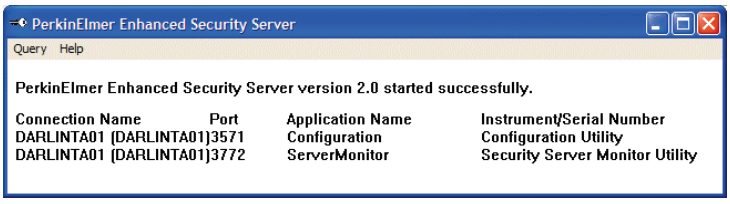
Status

This indicates when the Security Server starts and stops running.



Connections

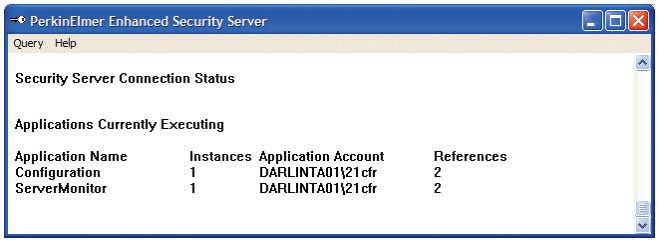
This shows the computer name, application name, and the instrument and serial number that are connected to the Security Server. It also shows the name and port number of the connection.



Applications

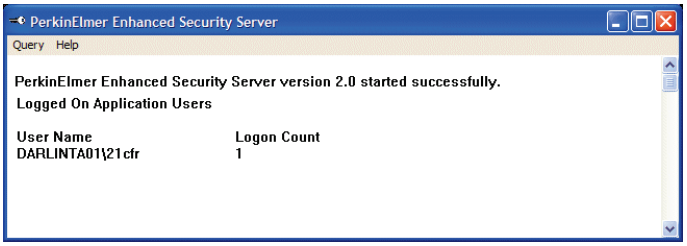
This shows the software applications that are connected to the Security Server. It also shows the number of instances of these applications, the names of the Application accounts, and the name of the computer on which each Application account is stored. It also shows the References, that is, the number of applications that are using an Application account.

In the example shown below, there are two software applications running: Configuration and ServerMonitor. There is one instance of each application. The name of the computer on which the Application account is stored is DARLINTA01. The name of the Application account is 21cfr. The number of references for the Application account is 2.



Users

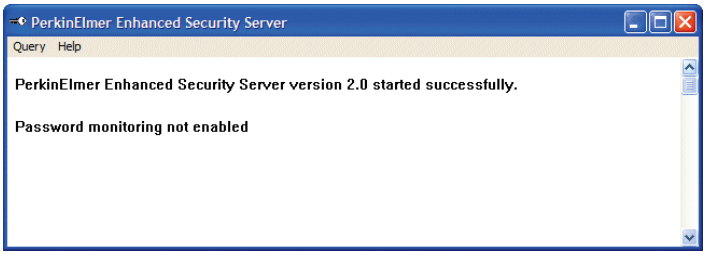
This shows the name of the user(s) that have logged onto the Security Server. In the example shown below, the user named DARLINTA01 has logged on to the Security Server. The Logon Count is the number of logon sessions for the user DARLINTA01.



Passwords

This shows the Application account(s) password status.

In the example shown below, password monitoring is not enabled.



You can change the status of the password on the Passwords tab of the Enhanced Security Configuration program. See *Changing the password for the Enhanced Security Application Account* on page 112 for details.