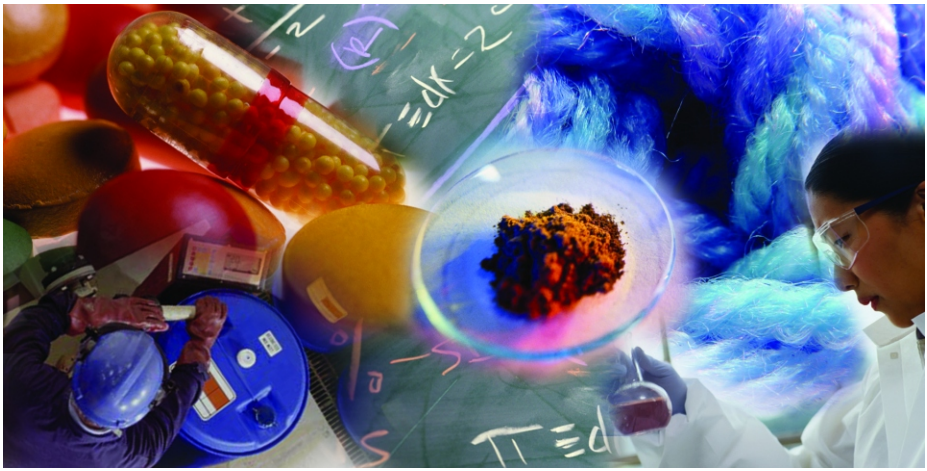
MOLECULAR SPECTROSCOPY

Spectrum



Administrator's Guide

PerkinElmer®
For the Better

Release History

Part Number	Release	Publication Date
L1050020	C	October 2008

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 © 2008 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 is a trademark of PerkinElmer, Inc.

Contents

Introduction

About this Guide

NOTE: This *Administrator's Guide* covers the Enhanced Security (ES) and Standard versions of Spectrum. The information provided is applicable to both versions of the software except where explicitly stated otherwise.

This *Administrator's Guide* is divided into four sections:

Installation of Spectrum – The step-by-step procedure for installing the software.

Administration of Spectrum – Details of the role of an Administrator (Windows Administrator and Software Administrator), login types, creating users and assigning them to groups.

An Overview of Spectrum – An introduction to the software.

Appendices – There are eight appendices that describe the following: (i) configuring TCP/IP communication, (ii) using the Windows Configuration Script to add increased security to your Windows system, (iii) backing up and recovering database files and recovering from Checksum failures, (iv) using the Legacy File Converter to convert old spectra, (v) an introduction to the Quant Import Utility, (vi) Windows login security, NTFS Permissions and Spectrum security, (vii) administering the PerkinElmer security server Windows user account, and (viii) Enhanced Security Settings provided by the security server configuration utility.

Further Information

For more detailed information on using Spectrum 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.

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.

Spectrum software can be used with the Spectrum 400, Spectrum 100, Spectrum 100N, Spectrum One and Spectrum One NTS spectrometers. In this *Spectrum Administrator's Guide* we have used Spectrum 100 to indicate Spectrum 100 and Spectrum One FT-IR spectrometers, and Spectrum 100N to indicate Spectrum 100N and Spectrum One NTS FT-NIR spectrometers.

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.*
D	***Caution (Achtung)*** *Bedeutet, daß die genannte Anleitung genau befolgt werden muß, um einen **Geräteschaden** zu vermeiden.*
DK	***Caution (Bemærk)*** *Dette betyder, at den nævnte vejledning skal overholdes nøje for at undgå en **beskadigelse af apparatet**.*
E	***Caution (Advertencia)*** *Utilizamos el término **CAUTION** (ADVERTENCIA) para advertir sobre situaciones que pueden provocar **averías graves en este equipo** o en otros. En recuadros éste se proporciona información sobre este tipo de circunstancias.*
F	***Caution (Attention)*** *Nous utilisons le terme **CAUTION** (ATTENTION) pour signaler les situations susceptibles de provoquer de **graves détériorations de l'instrument** ou d'autre matériel. Les détails sur ces circonstances figurent dans un encadré semblable à celui-ci.*
I	***Caution (Attenzione)*** *Con il termine **CAUTION** (ATTENZIONE) vengono segnalate situazioni che potrebbero arrecare **gravi danni allo strumento** o ad altra apparecchiatura. Troverete informazioni su tali circostanze in un riquadro come questo.*
NL	***Caution (Opgelet)*** *Betekent dat de genoemde handleiding nauwkeurig moet worden opgevolgd, om **beschadiging van het instrument** te voorkomen.*
P	***Caution (Atenção)*** *Significa que a instrução referida tem de ser respeitada para evitar a **danificação do aparelho**.*

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.*

D

Warning (Warnung)

*Bedeutet, daß es bei Nichtbeachten der genannten Anweisung zu einer **Verletzung** des Benutzers kommen kann.*

DK

Warning (Advarsel)

*Betyder, at brugeren kan blive **kvæstet**, hvis anvisningen ikke overholdes.*

E

Warning (Peligro)

*Utilizamos el término **WARNING** (PELIGRO) para informarle sobre situaciones que pueden provocar **daños personales** a usted o a otras personas. En los recuadros como éste se proporciona información sobre este tipo de circunstancias.*

F

Warning (Danger)

*Nous utilisons la formule **WARNING** (DANGER) pour avertir des situations pouvant occasionner des **dommages corporels** à l'utilisateur ou à d'autres personnes. Les détails sur ces circonstances sont données dans un encadré semblable à celui-ci.*

I

Warning (Pericolo)

*Con il termine **WARNING** (PERICOLO) vengono segnalate situazioni che potrebbero provocare **incidenti alle persone**. Troverete informazioni su tali circostanze in un riquadro come questo.*

NL

Warning (Waarschuwing)

*Betekent dat, wanneer de genoemde aanwijzing niet in acht wordt genomen, dit kan leiden tot **verwondingen** van de gebruiker.*

P

Warning (Aviso)

*Significa que a não observância da instrução referida poderá causar um **ferimento*** ao usuário.

Installation of Spectrum

PC Requirements

The following pages provide details of the requirements for the PC that will run the Spectrum software and communicate with the instrument. To ensure successful installation of the software, please check these requirements before starting the installation.

Hardware Requirements

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

- Intel® Pentium 4 400 or 533 MHz processor.
- At least 256 MB of Random Access Memory (RAM).
- The capability of displaying at least High Color (16 bit) at 1024 x 768 SVGA.
- 10 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.

- CD-ROM drive.
- A 1.44-megabyte floppy disk drive for 3.5-inch floppy disks.
- Ethernet network connection.
- A keyboard and PS/2®-style mouse.

Software Requirements

Operating System

This software requires that Windows XP Professional Service Pack 2 operating system is installed on the PC before you install Spectrum.

We have specified Windows XP because it is a robust, industry strength operating system that provides inbuilt security and auditing.

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

TCP/IP Communication

To operate a Spectrum 400, Spectrum 100 or Spectrum 100N spectrometer you will need TCP/IP protocols established on the PC (see *Appendix I – Configuring TCP/IP Communication* on page 86).

Previous versions of IR Software

Spectrum ES Software has a security system that is incompatible with previous versions of IR software (including Spectrum and Spectrum CFR). We recommend you purchase a new PC to run Spectrum ES. If you are using an existing PC we recommend that you format the hard disk on the PC (after backing up any important data). After formatting, install the Windows operating system before installing the Spectrum ES Software.

Windows Administrator Level

It is important to note that you must be logged on at Administrator level on Windows 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.

SIMCA Procedures

SIMCA procedures are shipped on the CD in a separate folder called /SIMCA. These procedures can be copied into a folder on the hard disk directly from the CD. The procedures may then be added into the software.

NOTE: Although these SIMCA procedures are supplied in case you require them, it is important to note that these are not 21 CFR Part 11 compliant. If you need to develop these further then you can purchase Spectrum Procedures from PerkinElmer. Note that Spectrum Procedures is also not 21 CFR Part 11 compliant. Alternatively, the AssureID software already has 21 CFR Part 11 technically compliant SIMCA built in.

Installing Spectrum Software

NOTE: We strongly suggest you read the *PC Requirements* starting on page 14, before attempting to install your software.

NOTE: Before installing the software we recommend that you read and print the release notes because they contain important information that may not be in this *Administrator's Guide* or the on-screen help. The release notes can be found as an rtf file and a pdf file in the \Documentation\Spectrum folder on the *Spectrum Software CD*.

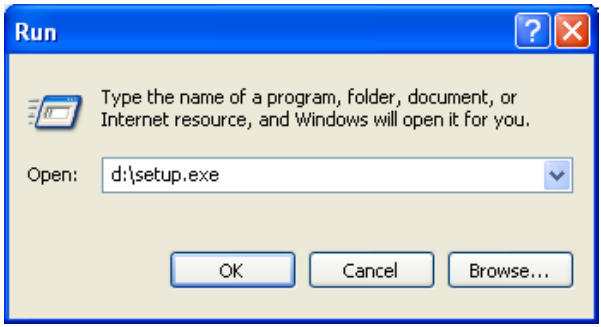
NOTE: To read .pdf files you will need Adobe Reader version 5.0 or later. An installation of this software is available on the *Software Utilities CD*.

NOTE: It is important to note that you must be logged on at Administrator level on Windows before installing the software.

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

1. Place your *Spectrum Software CD* into your CD drive.
2. If the installation program does not start automatically, from the Start menu select **Run**.

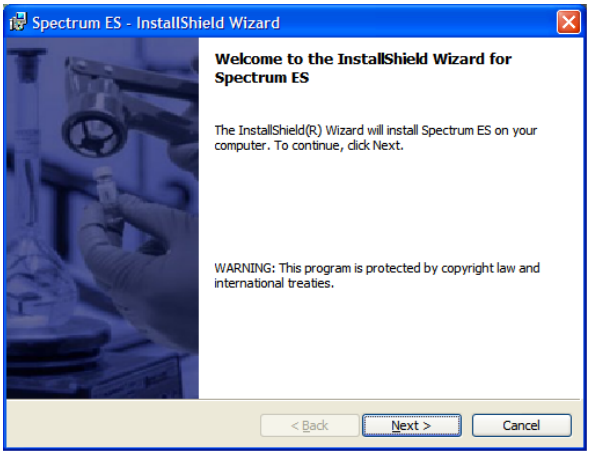
   The Run dialog is displayed.



3. Enter **d:\Setup.exe,** and then click **OK**.

   Replace d:\ with the drive letter for your CD.

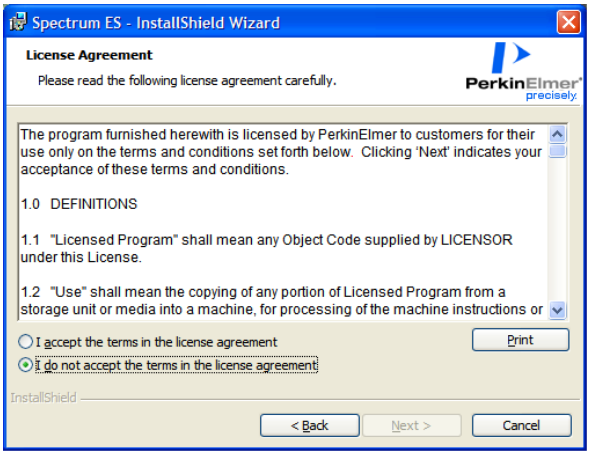
   The InstallShield Wizard dialog appears while the system is preparing to install the software. When the installer is ready, the Welcome dialog is displayed.



   If your PC does not meet the software requirements given in *Software Requirements* starting on page 15, an appropriate error message will inform you of the problem. You will need to correct this problem before the installation can be performed.

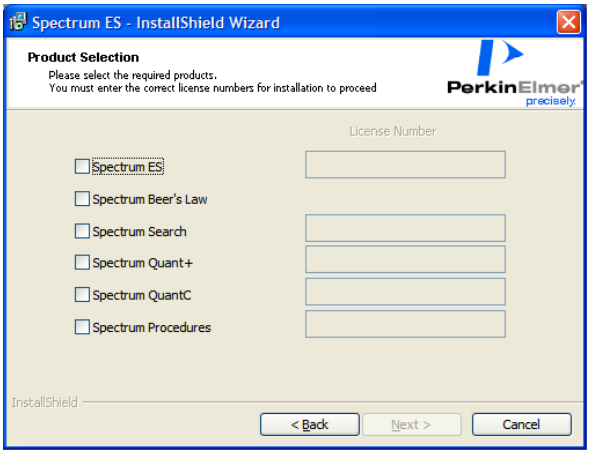
4. Click **Next**.

   The License Agreement is displayed.



5. Read the license and if you accept the terms, select that option and then click **Next**.

   You will then be asked which products you want to install.



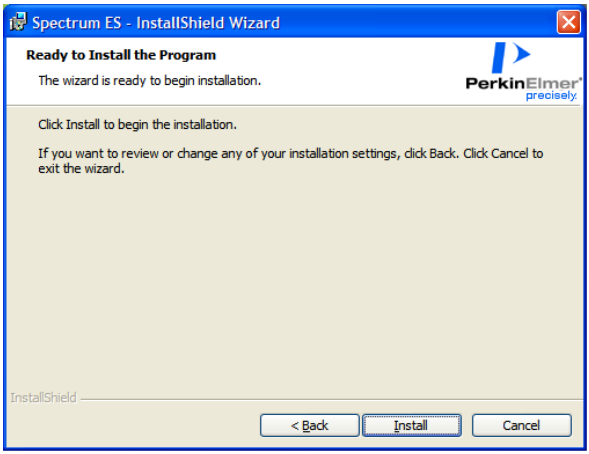
6. Select the required product(s) and then enter its **License Number** as found on the Software License Certificate.

   You must enter the correct license number(s) to proceed with the installation. If you enter an incorrect license number the **Next** button is disabled.

   If you are installing the Spectrum (Standard) software, the Spectrum Beer's Law check box is automatically selected when you select the Spectrum check box. If you are installing the Enhanced Security version of Spectrum, you must select the Spectrum Beer's Law check box to install the application.

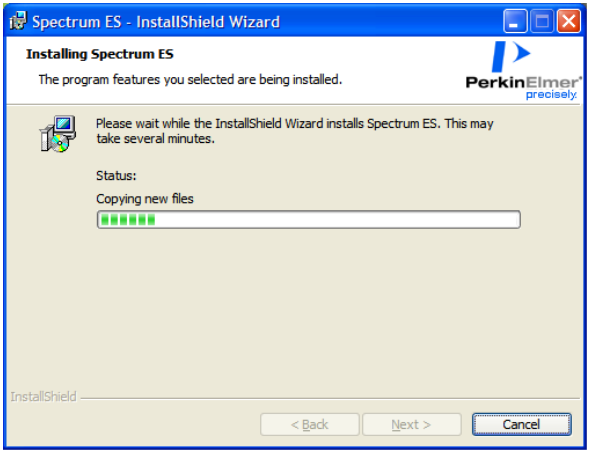
7. Click **Next**.

   The Ready to Install the Program page is displayed.

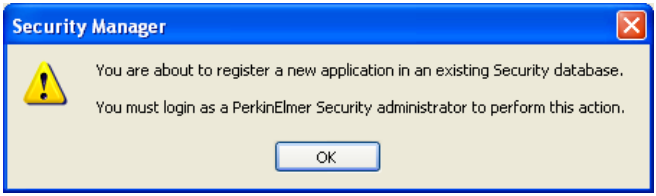


8. Click **Install** to begin installing Spectrum.

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



If you have already installed PerkinElmer software on the PC, the following message is displayed. Click **OK**.

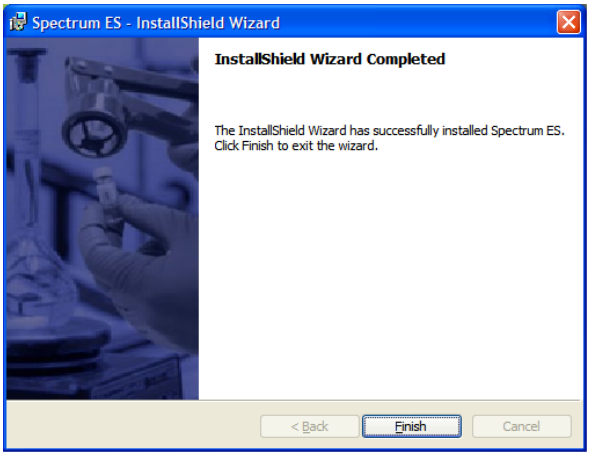


The PerkinElmer Login dialog is displayed.

Login as a PerkinElmer Software Administrator.

Use the Administrator **User name** and **Password** that you use for the PerkinElmer software that is already installed on the PC.

When the installation is complete, the InstallShield Wizard Completed page is displayed.



9. Click **Finish**.

If you are installing Spectrum ES in a 21 CFR Part 11 regulated environment you may wish to set further security to make sure that data files cannot be tampered with or deleted. In this case run the Lockdown script as detailed in *Appendix II – Windows Configuration Script* on page 92.

Before you can collect spectra you must configure an instrument, and then any accessories you want to use with the instrument. For more information see *Instrument and Accessory Configuration* on page 65.

NOTE: If you have a Raman instrument, you will need to install Raman Instrument Control. See the installation instructions in the user's guide that was supplied with your Raman instrument for details.

Upgrading Spectrum Software

Upgrading from Spectrum 5.x ES to Spectrum 6 ES

To upgrade from Spectrum 5.x ES to Spectrum 6 ES:

1. Before uninstalling your Spectrum 5.x ES software, restart the PC.
2. Log on to the PC as a Windows Administrator.
3. If you wish to preserve your instruments:
   - Copy all configuration files (*.cfg) from C:\pel_apps\bin to C:\pel_data\config
   - Copy C:\Windows\pel_inst.ini to C:\pel_data\config
4. Open the Control Panel and then select **Add or Remove Programs**.
   Remove the following programs:
   - IR Spectroscopy Software
   - Security Component
   - Spectrum ES Software
   - Spectrum Security Kit
   - AssureID (if installed)
5. Close the Add or Remove Programs and Control Panel dialogs.
6. Delete the following folders and files if they exist:
   - C:\pel_apps\
   - C:\Windows\pel_apps.bci
   - C:\Windows\pel_apps.ini
   - C:\Windows\pe_sopb.ini
7. Copy C:\pel_data\config\pel_inst.ini to C:\Windows\.
   Overwrite the existing file.

8. Restart the PC.

   The Spectrum 5.x ES software has now been removed from the PC. Note that instruments, databases and other files have not been removed. Therefore a re-installation will install the software and retain the existing instruments and data, including all existing spectra, users, and passwords.

9. If you want to completely remove all instruments and data associated with Spectrum 5.x ES before installing Spectrum 6 ES, then you must remove the following files:

   - C:\Documents and Settings\All Users\Application Data\PerkinElmer\Security System\users.mdb
   - C:\Documents and Settings\All Users\Application Data\PerkinElmer\Security System\backup\users.bak
   - C:\Documents and Settings\All Users\Application Data\PerkinElmer\Spectrum Audit\v5*.*
   - C:\pel_data and all subdirectories
   - C:\Windows\pel_inst.ini

10. Install the Spectrum 6 ES software.

    Refer to *Installing Spectrum Software* on page 17.

Upgrading from Spectrum 5.x (Standard) to Spectrum 6 (Standard)

To upgrade from Spectrum 5.x (Standard) to Spectrum 6 (Standard):

1. Before uninstalling your Spectrum 5.x (Standard) software, restart the PC.
2. Log on to the PC as a Windows Administrator.
3. If you wish to preserve your instruments, copy all configuration files (*.cfg) from *C:\pel_apps\bin* to *C:\pel_data\config*.

4. Open the Control Panel and then select **Add or Remove Programs**.
   Remove the following programs:
   - IR Spectroscopy Software
   - TimeBase (if installed)
   - Spotlight / Spotlight 200 (if installed)
   - Spectrum Repair CD (if installed)
   - AssureID (if installed)
5. Close the Add or Remove Programs and Control Panel dialogs.
6. Delete the following folders and files if they exist:
   - C:\pel_apps\
   - C:\Windows\pel_apps.ini
   - C:\Windows\pe_sopb.ini
7. Restart the PC.
   The Spectrum 5.x software has now been removed from the PC. Note that instrument and data files have not been removed, therefore an upgrade will install the software only and retain the existing instruments and data, including all existing spectra.
8. If you want to completely remove all instruments and data, remove the following:
   - C:\pel_apps and all subdirectories
9. C:\Windows\pel_inst.ini
10. Install the Spectrum 6 software along with any additional packages you have purchased (for example Spectrum Quant+ or Spectrum Search Plus).
    Refer to *Installing Spectrum Software* on page 17.

NOTE: The Users that were configured in Spectrum 5.x (Standard) will not be configured when you install Spectrum 6. You will need to set up these Users again. For more information see *Creating New Spectrum Users* on page 39.

Logins for Spectrum ES

Access control is facilitated using the Administration menu in Spectrum. You must set up the Spectrum logins before giving access to any users. The default passwords for the three default user groups are the same as the name of the user in lower case, as follows:

Login Name	Password	Member of Group
Administrator	administrator	Administrators, Supervisors
Supervisor	supervisor	Supervisors
Analyst	analyst	Analysts

NOTE: Passwords are case sensitive.

NOTE: We recommend that a backup software administrator is created as soon as possible after installation. To create an administrator, refer to *Creating Software Administrators* on page 55.

You are forced to change the password immediately.

Logins for Spectrum (Standard)

The default passwords and Group membership for the two default user groups are the same as the name of the user in lower case, as follows:

Login Name	Password	Member of Group
Administrator	administrator	Administrators, Users
Analyst	analyst	Analysts

You should immediately change these passwords to stop any unauthorized access to the software.

NOTE: We recommend that a backup administrator is created as soon as possible after installation. To create an administrator, refer to *Creating Software Administrators* on page 55.

Administration of Spectrum

Introduction

There are two main security systems used by the software:

- Windows login security system, which manages access to the PC, its peripherals, the data and files on the hard disk and all aspects of the PC configuration.
- The Spectrum software login security, which manages access to the software, the data and any associated instruments.

These security features give maximum flexibility, and allow you to very tightly restrict what a day-to-day user is able to do. In the Enhanced Security (ES) version of the Spectrum software, they also allow you to easily fit with company procedures designed to adhere to 21 CFR Part 11.

Day-to-day usage of the system will be by users, who are not typically allowed to delete, change or rename data files. There may be some application functionality to which a user does not have access.

The Role of the Administrator

There is a two-fold role for the Administrator, which could in fact be two different people:

- As Administrator for the Windows operating system (Windows Administrator).
- As Administrator for the Spectrum software (Software Administrator).

The differences between the two roles are shown in the table on page 102.

Windows Administrator

Someone trained as a Windows Administrator should control the PC that the Spectrum software is installed on. They will be responsible for all Windows User/Password settings, Windows Auditing and NTFS file security.

NOTE: End users, that is people using the 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. Pre-installed Windows groups and accounts are shown in *Default Windows groups and accounts* on page 32.
- Ensure that Users only have access to folders and files that they need access to. This includes network drives.
- Consider whether the floppy drive, CD Writer or USB ports should be disabled by Windows for Windows Users, given that all data from using the instrument must be retained.
- Setup the Start menu so that the users can only access applications that they need.
- 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.
- Setup file control as discussed in *Protecting Saved Data Files using NTFS* on page 47.
- Use the Windows auditing features to track login attempts or attempts to delete files.

- Consider whether to set up a password protected screen saver to guard against unauthorized use of the system when unattended.
- Ensure that appropriate backup procedures are in place for data files and the security and audit databases. This is covered extensively in *Appendix III – Backup and Recovery* on page 97.

NOTE: In Spectrum ES, some of these tasks can be automated by running the Windows Configuration Script. For more information see page 92.

Windows Login Security

The Windows configuration supplied with your system includes two main Windows user groups: Administrators and Users.

The Windows Administrator account is a member of the Administrators group, and 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. Clearly the administrator has great power, and so the person acting in this role should be suitably trained and qualified in Windows. It is recommended that this person is not the same person who will be using the instrument on a day to day basis.

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

Default Windows groups and accounts

The install sets up the following default Windows groups and accounts:

- PKIUsers group – A group used by default for the Windows login user members.
- 21CFR_Admin group – A group used for Windows login functionality.
- PEService – A Windows Administrator account for use by PerkinElmer Service Engineers.
- 21cfr – A Windows Administrator account used by Windows login functionality to authenticate Windows User names and Passwords.

NOTE: It is recommended that the Windows Administrator sets up different groups and accounts according to the company requirements, following standard procedures, and deletes the standard accounts, or as a minimum, changes the passwords. If the default accounts are left unchanged, it could be a way for an unauthorized person to access the system.

NOTE: Being logged on as a Windows Administrator gives full read/write permissions to the system, so Spectrum ES software should only be used to collect or process data when logged on as a Windows User, to avoid negating the 21 CFR Part 11 compliance.

Windows Auditing

Within Windows and the NTFS file system it is possible to audit activity within directories or files themselves. 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 directory where the data files are stored, and monitor attempts to delete files.

NOTE: Audit logs can get very large if not carefully set up and managed, and that they can fill up disk space very quickly.

Login auditing is also available within Windows to monitor access to the system. For example, this may be used to look for failed attempts at login. Login auditing can be set from the Control Panel by selecting **Administrative Tools**, **Local Security Policy**, **Local Policies** and then **Audit Policy**.

Spectrum Software Administrator

There is also a need to have a Software Administrator to set up and maintain the security of the Spectrum software.

The Software Administrator is required to:

- Define how users login to Spectrum, see *Spectrum Login Types* on page 34.
- Administer the database of users, including adding new users and setting their permissions and passwords, see *Spectrum Login Types* on page 34.

In the Enhanced Security (ES) version of Spectrum, they should also:

- Track the Login History, see *Spectrum Login Security* on page 44.
- Track the Audit Trails, see *Spectrum ES Administrator's Audit* Trail page 46.

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 software will automatically have the ability to administer any other PerkinElmer application that has been installed which uses the PerkinElmer Security Manager. In the same manner, user names are global, that is, a user name assigned to one PerkinElmer application is also made available to all other PerkinElmer applications. Although Administrators and Users are global in nature, groups and instruments assigned to the software are application specific.

Spectrum Login Types

There are three ways to login to Spectrum. The Software Administrator is responsible for determining which type is used.

- PerkinElmer Login

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

- Windows Login

  This allows Windows users to login to Spectrum using their Windows User name and Password instead of having a separate Spectrum User name and Password.

- No Passwords Login

  This is only available in the Standard version of Spectrum. It allows each Spectrum user to login by entering only a User name.

Setting up PerkinElmer Login

When Spectrum 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 on to Windows systems using common or generic user names. When PerkinElmer Login is running you can create user names and passwords specifically for Spectrum.

Outside 21 CFR Part 11 compliant environments, where security and audit trails are not important, you can also use No Passwords Login (Spectrum Standard version only). This involves each user logging in to Spectrum by selecting their User name from a drop-down list in the PerkinElmer Login dialog. No Password is required.

To setup the Spectrum users and groups go to *Creating New Spectrum Users* on page 39.

Setting up Windows Login

Windows Login is ideal if your users all have individual Windows user names (either on a Windows Domain, or locally on the PC) and you wish to keep the same user names/passwords when running Spectrum.

For Spectrum to recognize which Windows user names/passwords have permission to log in, they must be made members of a specific Windows group. The Spectrum security component will then allow them to log in to Spectrum. The default group created on the local PC during the installation of Spectrum is called PKIUsers. When Spectrum is installed and run on a local PC, the Windows Administrator should add users to the PKIUsers group on that PC. When Spectrum will be used across a network, the Windows Administrator should create a network group on an accessible domain and then add users to that group.

Depending on your company's security policy, you should consider whether to replace the default Windows Administrator account called 21cfr. This account is used by the Windows Login functionality. For a description how to create a new account and then change the password of the account see *Appendix VII – Administering the PerkinElmer Security Server Windows User Account* on page 104.

Adding users to the PKIUsers user group

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

NOTE: If you choose to use some other group as your Windows users' group, this procedure should be used for whichever group you decide to use.

1. Log into your PC as a Windows Administrator.
2. From the Start menu, select **Settings** and then select **Control Panel**.
3. Double-click on Administrative Tools.
4. Double-click on Computer Management.
   The Computer Management dialog is displayed.
5. Click Local Users and Groups.
6. Double-click on the **Groups** folder to see the list of available Groups on the PC.
7. Double-click on **PKIUsers**.
   The PKIUsers Properties dialog is displayed.
8. To add a user member to the Group, click **Add**.
   The Select Users, Computers, or Groups dialog is displayed.

9. To select a user from a different location (domain), click **Locations** and then select the required location for the user you wish to add.

   Click **OK**.

10. To add a user to the group, enter the name of the user in the **Enter the object name to select** field and then click **Check Names**.

    Clicking **Check Names** will validate the name on the specified domain.

NOTE: To add more users, repeat steps 7 to 10.

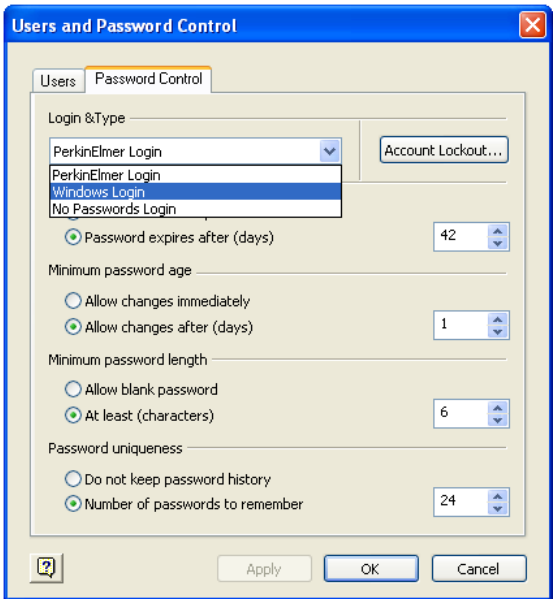
11. Once you have added all the required users, click **OK**.

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

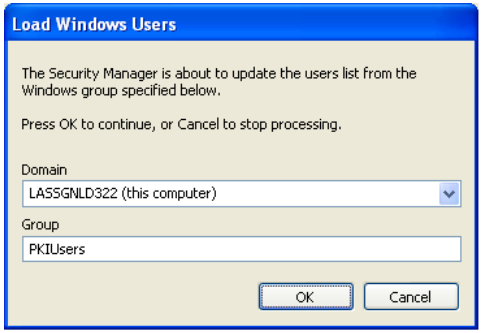
12. Click **OK** and then close all the Control Panel dialog boxes.

Setting the login type to Windows login

1. Start the Spectrum software and log in as a user with administrator permissions.
2. From the Administration menu select **Setup Users and Groups** in Spectrum ES, or **Setup Users** in Spectrum.
3. On the **Password Control** tab, change the Login Type to **Windows Login**.



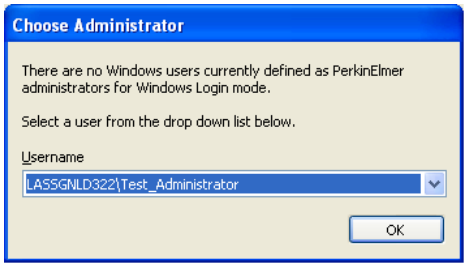
The **Load Windows Users** dialog is displayed.



4. Click **OK**.

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

5. Use the drop-down to select the user who is to be the PerkinElmer administrator and then click **OK**.



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

7. Spectrum will then prompt for you to create a configuration for this user. This configuration contains the toolbar and software settings for each user who has access to the system.

   Select the desired configuration and then click **OK**.

8. Exit the Spectrum software.

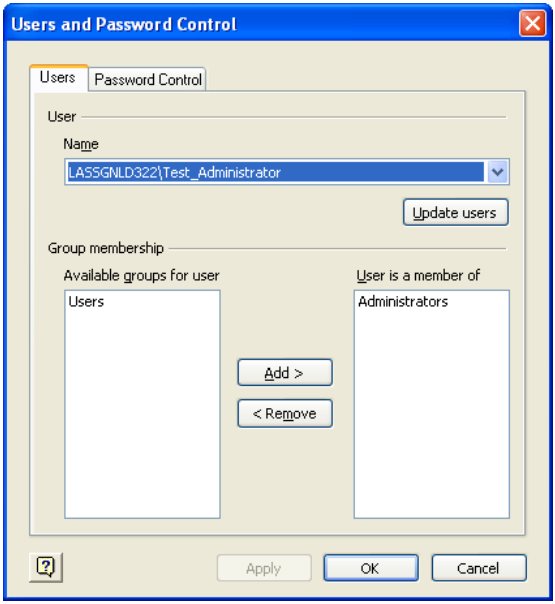
At this point, the login type is set to Windows Login, but only one user (the administrator) has access to the software. The administrator must log back into Spectrum in order to configure all the other users who need access to the software.

Additionally the administrator does not yet have permission to access instruments from Spectrum software.

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

1. Start the Spectrum software and log in using the administrator login.
2. From the Administration menu select **Setup Users and Groups** in Spectrum ES, or **Setup Users** in Spectrum.

   On the Users tab, the Name drop-down contains all the users who are members of the PKIUsers Windows group. Each of these users will need to be given appropriate PerkinElmer software access.



   - Any user required to be an Administrator in PerkinElmer software will need to be in the **Administrators** group. We recommend that at least two users are set up as administrators, for emergency use.
   - Any user requiring access to Spectrum software, including Instrument Access, needs to be a member of the **Users** group. In Spectrum ES they need to be either **Supervisors** or **Analysts**.

3. Select each user in turn from the **Name** drop-down and configure them appropriately.

4. When you are finished, click **OK**. You will be prompted to create new configurations for each new user. Select the desired configuration and click **OK**.

Users should now have access to Spectrum software.

Creating New Spectrum Users

Each person using Spectrum must be setup as a user by the Software Administrator.

For PerkinElmer Login Type

To define new User names and Passwords:

1. Start Spectrum.

   Login to Spectrum as a Software Administrator.

2. From the Administration menu select **Setup Users and Groups** in Spectrum ES, or **Setup Users** in Spectrum.

   In the Enhanced Security version of Spectrum, the Users, Groups and Password Control dialog is displayed. In the Standard version of Spectrum, the Users and Password Control dialog is displayed.

3. Select the Users tab and then click **New**.

   The New User dialog is displayed.

4. 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.

   The Password may be blank for the Standard version of Spectrum.

5. Select **Enabled** if you wish the user to be able to login, or **Disabled** if you do not wish them to be able to login at the current time.

   In Spectrum ES, **User must change password at next login** is always selected when a new user is created. This is to ensure that the first time the user logs in they will be forced to change their password. This means that the password is known only to the user and not the Administrator.

6. Click **OK**.

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

7. Add the user to a group, to allow access to the software.

For Windows Login Type

1. Create the new user in Windows.

   This may be on the local PC or on a network domain.

   Your IT department may have to do this for you.

2. Add the new user to the Windows users group that is allowed to run Spectrum.

   The default Windows users group is the PKIUsers group on the local PC.

3. Login to Spectrum as a Software Administrator.

4. From the Administration menu select **Setup Users and Groups** in Spectrum ES, or **Setup Users** in Spectrum.

   In the Enhanced Security version of Spectrum, the Users, Groups and Password Control dialog is displayed. In the Standard version of Spectrum, the Users and Password Control dialog is displayed.

5. Select the Users tab and then click **Update Users**.

   The new user will now be able to login to Spectrum.

6. Add the user to a group, to allow access to the software.

Assigning New Users to Spectrum Groups

New Users need to be assigned to one or more Spectrum groups. We recommend that where possible you only assign users to one group, but in some cases you may also consider assigning users to the Administrators group.

To assign Users to Spectrum Group(s):

1. From the Administration menu select **Setup Users and Groups** in Spectrum ES, or **Setup Users** in Spectrum.

   In the Enhanced Security version of Spectrum the Users, Groups and Password Control dialog is displayed. In the Standard version of Spectrum the Users and Password Control dialog is displayed.

2. 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 added to the **User is a member of** list.

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

NOTE: When using the Windows Login, at least one user must be assigned Administrator rights. If not, it will not be possible to exit the software. If a user is not added to at least one group, an error message will be displayed when they try to log in informing them that they do not have access to the application.

What are the Default Groups in Spectrum ES?

The following Spectrum groups are pre-defined when Spectrum ES is installed:

Group	Member of the Group is Able to:
Administrators	Software Administrator who creates and maintains Users and Groups, sets access permissions to instruments, sets security policies, controls Audit Trails, and uses the Legacy File Converter. Only Administrators have access to the Administration menu in Spectrum ES.
Supervisors	Supervisor with advanced access to instrument, most Spectrum ES functionality.
Analysts	End user with minimal access to instrument, some restrictions to Spectrum ES software.

NOTE: Passwords are case sensitive while User names are not.

What are the Default Groups in Spectrum?

The following Spectrum groups are pre-defined when Spectrum is installed:

Group	Member of the Group is Able to:
Administrators	Software Administrator who creates and maintains Users, sets access permissions to instruments, and sets security policies. Only Administrators have access to the Administration menu in Spectrum.
Users	End user with full access to instrument and Spectrum software.

Configuring Spectrum ES Groups

NOTE: Group Configuration is only available in the Enhanced Security version of Spectrum.

The Software Administrator can configure the settings for each group.

➢ To configure the group settings, select **Group Configuration** from the Administration menu.

The Group Configuration dialog is displayed.

The Group Configuration dialog enables you to:

- Disable individual menu commands
- Define the icons available on the toolbar and toolbox
- Set the default directories and other configuration settings
- Set the level of instrument access

Each instrument has a series of groups associated with it. Each group is able to perform a series of operations such as setting up an instrument and performing a scan. Users are assigned to a group per instrument.

Further information can be found in the on-screen help, viewed by selecting **Contents and Index** from the Help menu.

Configuring Spectrum Users

NOTE: User Configuration is only available in the Standard version of Spectrum.

The Software Administrator can configure the settings for each user.

➢ To configure the user settings, select **User Configuration** from the Administration menu.

The User Configuration dialog is displayed.

The User Configuration dialog enables you to disable individual menu commands and define the icons available on the toolbar and toolbox.

Further information can be found in the on-screen help, viewed by selecting **Contents and Index** from the Help menu.

Spectrum ES Group Audit Trail

NOTE: Spectrum Audit Trail is only available in the Enhanced Security version of Spectrum.

This Audit Trail records all changes to the Spectrum ES Software on the PC and the configuration of the user groups.

1. In Spectrum ES, select **View Spectrum Audit Trail** from the Administration menu.

   The Spectrum Audit Trail dialog opens.

2. Click Active Database.

   The current database is displayed, it shows:

   - changes to the software installed on the PC;
   - changes to the configuration of user groups.

Spectrum Login Security

The level of access available to users of Spectrum software depends on the permissions set by the Software Administrator, see *Creating New Spectrum Users* and Assigning New Users to Spectrum Groups on pages 39 and 40 respectively.

Part of the planning process for establishing the Enhanced Security version of Spectrum within a 21 CFR Part 11 compliant environment must be to plan the permissions allocated to the users and groups to best fit the company's working procedures.

Spectrum ES Login History

NOTE: Login History is only available in the Enhanced Security version of Spectrum.

The Login History can only be viewed by users who are members of a group that has permission to perform administration tasks.

1. In Spectrum ES, select **View Admin 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. This details every login attempt, since the history was last cleared, by:

   - **Full Name**
   - **User Name**
   - **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 incorrectly entered ***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 audit trails at regular intervals.

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

Spectrum ES Administrator's Audit Trail

NOTE: Audit Trail is only available in the Enhanced Security version of Spectrum.

This 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. In Spectrum ES, select **View Admin 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 change recorded, the following information is given in the Audit Trail:

   - **Function** — the item that was changed, for example, Add New User.
   - **Previous Value** — the state of the item before it was changed.
   - **Current Value —** the new state.
   - **Full Name —** the full name of the user who made the change.
   - **User Name** — the login user name of the user who made the change.
   - **Computer** – The name of the computer from which the change was made.
   - **Date Modified** – The date and time of the change.

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

Protecting Saved Data Files using NTFS

Spectrum saves most of its data in files, for example spectra are saved as .sp files. The NTFS file system allows the Windows Administrator to set security permissions for every file and subdirectory as required, and if accidental or malicious deletion of data is to be avoided, then setting up the right permissions on these data files is an important consideration within a 21 CFR Part 11 compliant environment.

Users clearly need the ability to write data files to the NTFS file system, but once written, they typically should not need to change or delete them. Before security settings are discussed the following must be undertaken when working with Windows XP. This is to ensure that the **Security** tab within the file/folder **Properties** dialog is available when applying the security settings.

NOTE: This section details how protection of the relevant files can be done manually. Should you wish to apply the protection automatically, then you can run the lockdown script as detailed in *Appendix II – Windows Configuration Script* on page 92.

NOTE: As Part of the installation process of the software the *Full Control* permission is applied to *'Everyone'* for the \windows\temp directory. This is essential for the software to operate correctly.

Procedure for Viewing the Security Tab

NOTE: If the ***Security*** tab is already visible when accessing the ***Properties*** dialog for files and folders then this procedure may be ignored.

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

NOTE: If you do not want to apply the change to all folders within the drive, then this procedure must be repeated for each relevant folder where this 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

The following default directories store important data and it is important to set the security settings as illustrated in the figures for the sub-directory and folders as follows.

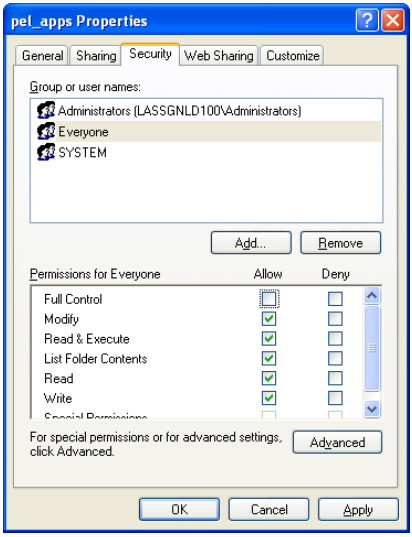
NOTE: C in each case refers to the drive Spectrum is installed to.

The following directories and files need the **Modify** permission set for **Everyone:**

- C:\pel_apps\
- C:\pel_data\
- C:\Windows\pel_inst.ini
- C:\Windows\pel_apps.ini
- C:\Windows\pel_apps.bci (Spectrum ES Only)
- C:\Windows\pe_sopb.ini

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

3. Remove the tick on the **Full Control Allow** permission, as shown below.



4. Repeat for the remaining files/folders.

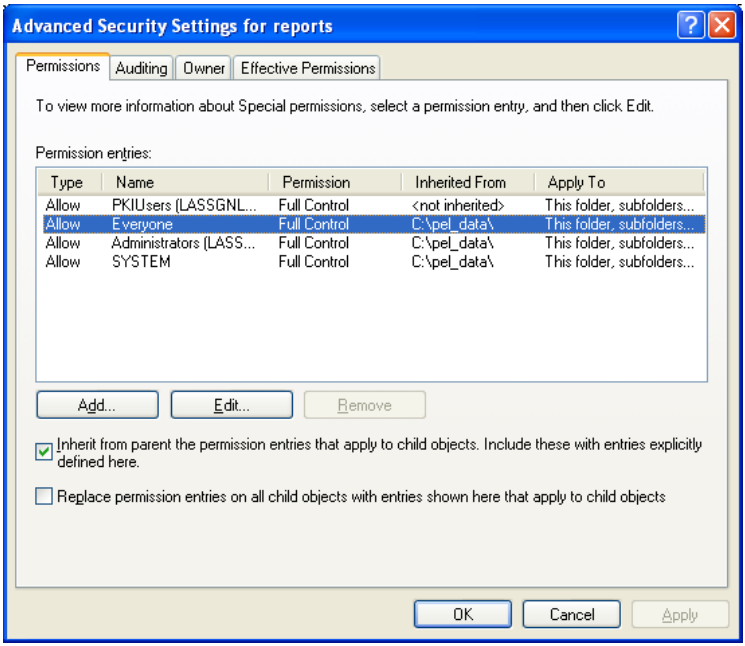
The following description sets the **Write Once**, **Read** permission on data folders. The following folders need to have this setting:

- C:\pel_data\reports
- C:\pel_data\spectra
- C:\pel_data\igram
- C:\pel_data\chrom
- C:\pel_data\pktables

The procedure for setting these permissions is as follows:

1. In Windows Explorer, right-click on c**:\pel_data\reports** and select **Properties**.
2. Select the **Security** tab and highlight the **Everyone** group.

3. Click the **Advanced** button. A screen similar to the one shown below is displayed.

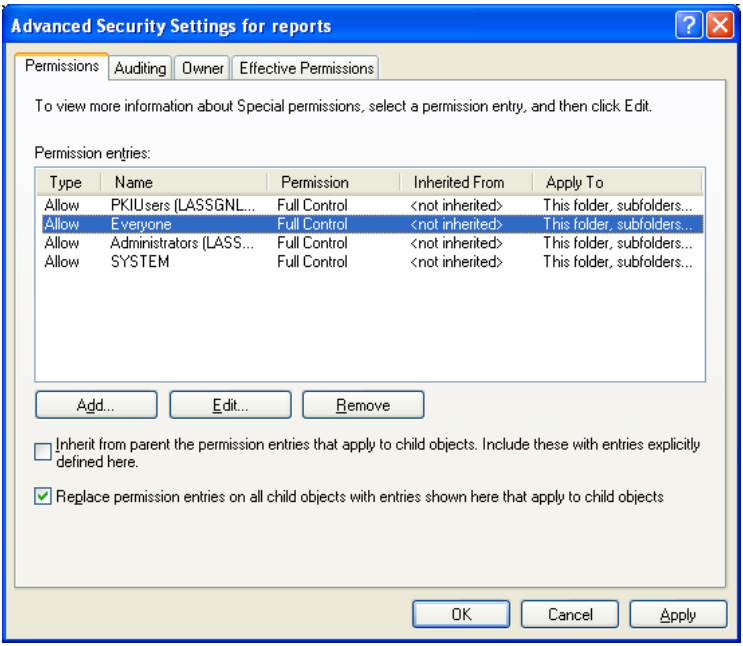


4. Un-check the checkbox with the text starting with "*Inherit from parent the permission entries…"*

5. A message titled **Security** will appear. Click **Copy.**

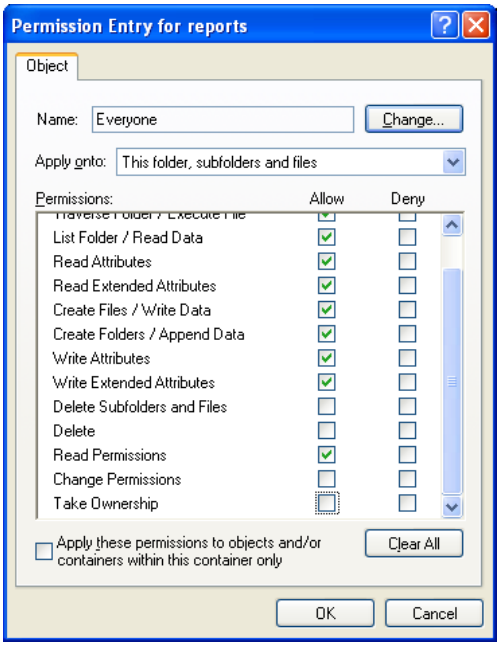
6. Check the checkbox with the text starting with "Replace permission entries on all child objects…"

7. The **Inherited From** column should now display **<not inherited>**, as shown below.



8. Highlight the **Everyone** group and click **Edit...**

9. Un-check the following permissions in the **Allow** column.
   - **Delete Subfolders and Files**
   - **Delete**
   - **Change Permissions**
   - **Take Ownership**



10. Click **OK** three times to apply the settings and return to Windows Explorer.
11. Repeat this process for the remaining data folders.

Spectrum Administration Made Simple

This section summarizes a number of the administration activities in Spectrum. For full details of each step involved in performing these activities refer to the Spectrum Help file. This can be accessed by selecting **Contents and Index** from the Help menu in the software.

Spectrum is shipped with default users and groups already setup. These are described on page 42.

Defining the Login Type

There are two ways to login to Spectrum. These are PerkinElmer Login and Windows Login. For more information see *Spectrum Login Types* on page 34.

Creating a New User and Assigning to a Group

If you want to add a new user and give them access to an instrument, then it is easiest if you make the new user a member of one of the pre-installed groups. See *Creating New Spectrum Users* and Assigning New Users to Spectrum Groups on pages 39 and 40 respectively.

Your new user is now able to access the instrument, and any other instrument which has the same group allocated to it.

Creating New Groups

NOTE: New Group is only available in the Enhanced Security version of Spectrum.

1. From the Administration menu, select **Setup Users and Groups**.
   The Users, Groups and Password Control dialog is displayed.
2. Select the Groups tab, and then click **New**.
   The New Group dialog is displayed.
3. Enter a **Group name** and then click **OK**.
   The new group is added to the **Name** drop-down list.
4. Select which **Instruments** the members of the group can access.
   By default none of the instruments in the list are selected.

5. Click **OK**.

   The Users, Groups and Password Control dialog closes and the New Group dialog is displayed.

6. From the drop-down list, select the existing group that you want to base the new group on.

7. Click **OK**.

   The new group is created.

Assigning the Group to an Instrument

NOTE: Groups are only available in the Enhanced Security version of Spectrum.

1. From the Administration menu, select **Setup Users and Groups**.

   The Users, Groups and Password Control dialog is displayed.

2. Select the Groups tab.

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

NOTE: The Administrators group is not present. Administrators have access to instruments as they are also members of the Supervisors group.

4. Select which **Instruments** you want members of the group to be able to access.

5. Click **OK**.

   The Group has now been assigned to the selected instrument(s).

Checking Which Groups the User has been Assigned to

1. From the Administration menu, select **Setup Users and Groups**.

   The Users, Groups and Password Control dialog is displayed.

2. Select the Users tab.

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

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

Creating Software Administrators

1. From the Administration menu select **Setup Users and Groups** in Spectrum ES, or **Setup Users** in Spectrum.

   In the Enhanced Security version of Spectrum the Users, Groups and Password Control dialog is diplayed. In the Standard version of Spectrum the Users and Password Control dialog is displayed.

2. Either select a User **Name** from the drop-down list.

   OR

   Create a new user by clicking **New**.

3. Select Administrators from the Available groups for user panel.

4. Click **Add**.

5. Click **OK**.

   The dialog closes.

The User is now an Administrator.

Other Administration Functions

This overview attempts to provide some of the key concepts on administering Spectrum software. For further details on these concepts including other relevant information, such as the Password Control tab, account lock out and what to do if a user is locked out, refer to the Help. The Help can be accessed via the Help menu within the Spectrum software.

An Overview of Spectrum

Starting Spectrum

Using PerkinElmer Login

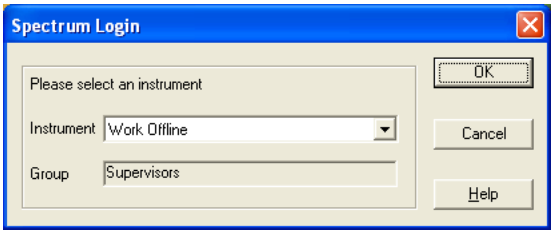
1. To start Spectrum, from the Start menu select **Programs**, **PerkinElmer Applications** and then **Spectrum** from the **Spectrum** group.

   The PerkinElmer Login dialog is displayed.

2. Enter your User name and Password as set up by the Software Administrator – see *What are the Default Groups in Spectrum ES?,* or *What are the Default Groups in Spectrum?* on page 42.

3. Click **OK**.

   The Spectrum Login dialog is displayed.



4. Select the **Instrument** to be controlled and then click **OK**.

   The **Group** that gives you access to that instrument is displayed.

   The software will start.

Using Windows Login

1. To start Spectrum, from the Start menu select **Programs**, **PerkinElmer Applications** and then **Spectrum** from the **Spectrum** group.

   The Windows Login dialog is displayed.

2. Enter your **User name** and **Password**.

   If the **Log on to** field is not displayed, click **Options** to show the field.

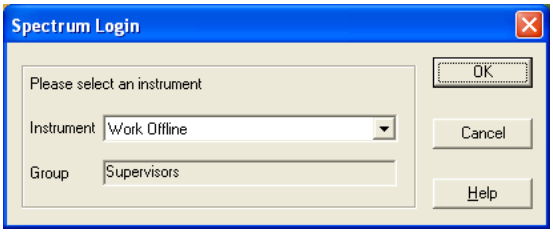
3. Select the required domain from the **Log on to** drop-down list.

   By default, the last domain that was logged on to is displayed.

NOTE: If all users are on the same domain, there is no need to show the **Log on to** field as the correct domain will be listed. It may avoid confusion to users if this field is hidden. If the **Log on to** field is shown, click **Options** to hide it.

4. Click **OK**.

   The Spectrum Login dialog is displayed.



5. Select the **Instrument** to be controlled and then click **OK**.

   The software will start.

   The **Group** that gives you access to that instrument is displayed.

Using No Passwords Login

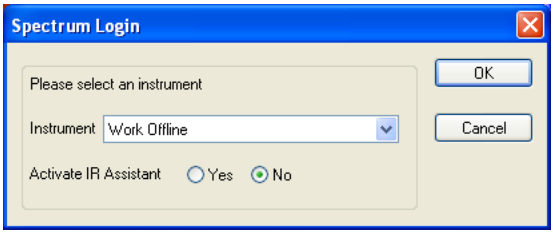
1. To start Spectrum, from the Start menu select **Programs**, **PerkinElmer Applications** and then **Spectrum** from the **Spectrum** group.

   The PerkinElmer Login dialog is displayed.

2. Select your User name from the drop-down list (see *What are the Default Groups in Spectrum?* on page 42).

3. Click **OK**.

   The Spectrum Login dialog is displayed.

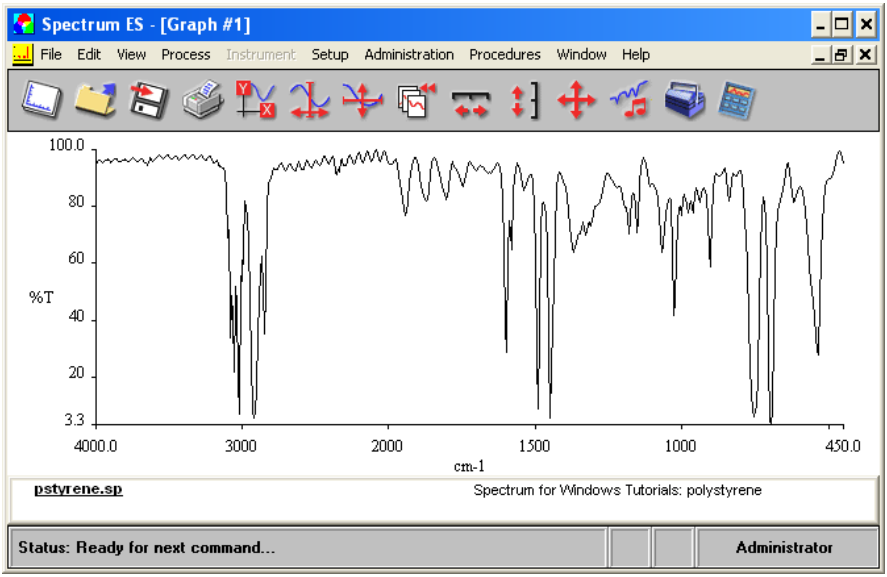


4. Select the **Instrument** to be controlled and then click **OK**.

   The software will start.

Using Spectrum

Spectrum is the main PerkinElmer software package for collecting, viewing and processing IR and NIR spectra.

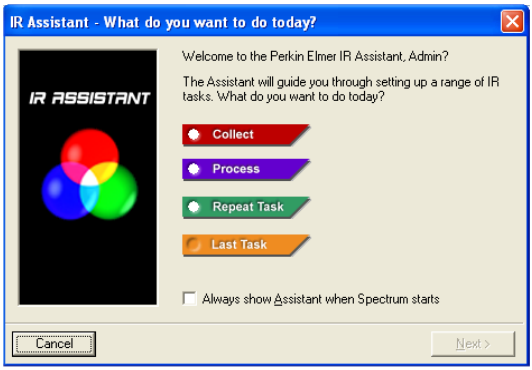


The View menu contains commands that enable you to change the way you view the spectrum, while the Process menu contains commands to manipulate the data including the ability to extract qualitative and quantitative information from the spectrum.

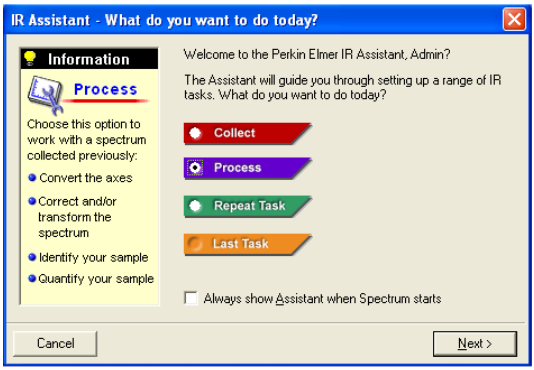
Spectrum is a very powerful software package, to familiarize yourself with its abilities we suggest you work through the on-screen tutorials by choosing **Learning Spectrum** on the Help menu.

IR Assistant

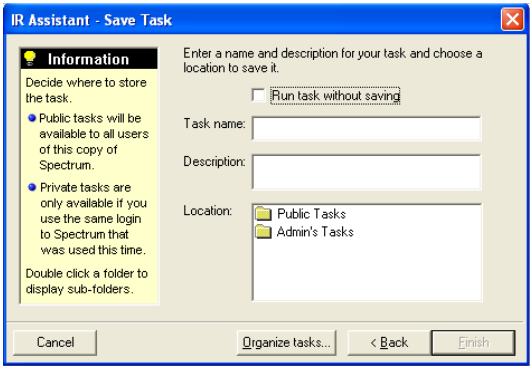
An alternative way to use Spectrum is the IR Assistant. This is a 'wizard' system that provides access to the full power of Spectrum, but uses default options where possible to avoid the complexity of the full Spectrum interface.



The IR Assistant has a unique help system, which displays information just when you need it. When you hold the mouse pointer over a control on the software, help for that control appears, to guide you in its function.



When you have built your task you can save it so that it can be used again.



This then becomes a simple way to automate tasks that are routinely performed.

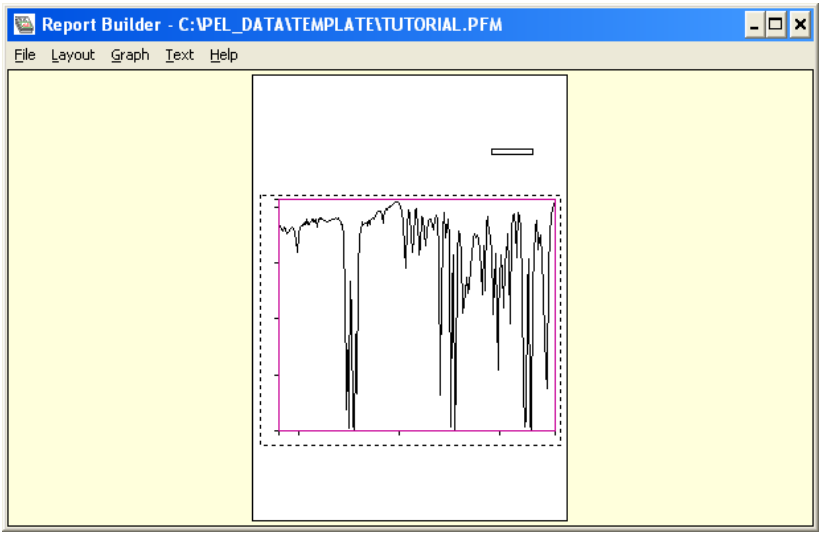
For details how to run the IR Assistant on a restricted system see *IR Assistant / Quant Import* on page 95.

Instrument Control

Spectrum is also used to control your instrument. Further information about controlling your instrument, or processing the spectra and data from samples is given in the on-screen help.

Report Builder

Report Builder is an integral Part of Spectrum that helps you turn your data into a single page report.



The report can contain System, Status and Instrument information related to the spectral data as well as text you enter yourself, and templates can be set up to always lay out the information in the same way.

Instrument and Accessory Configuration

Before collecting spectra you must configure an instrument, and then add any accessories that you want to use with the instrument.

Adding an Instrument

To add an instrument:

1. Login to Spectrum as an Administrator.

   The default User name is **Administrator** and the default Password is **administrator**.

   The Spectrum Login dialog is displayed.

2. Select **Work Offline** from the Instrument drop-down list and then click **OK**.

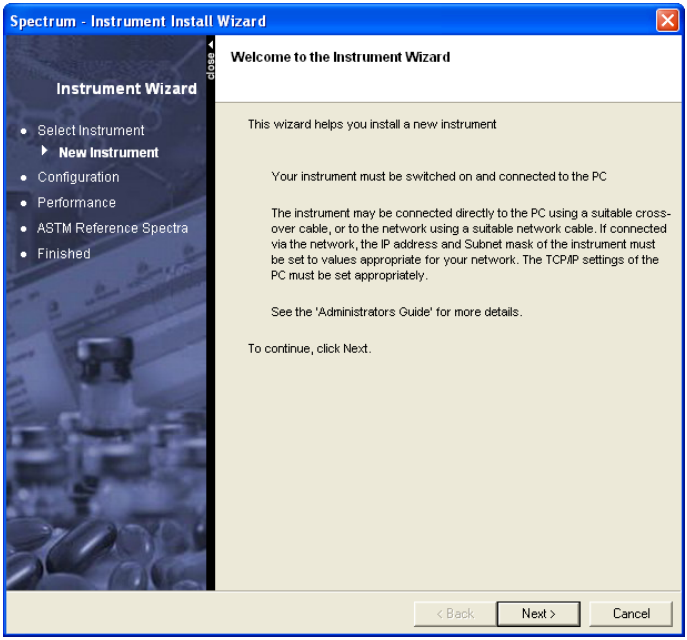
   The Spectrum software opens.

3. Select Instrument and Accessory Configuration from the Administration menu.

   A sub-menu is displayed.

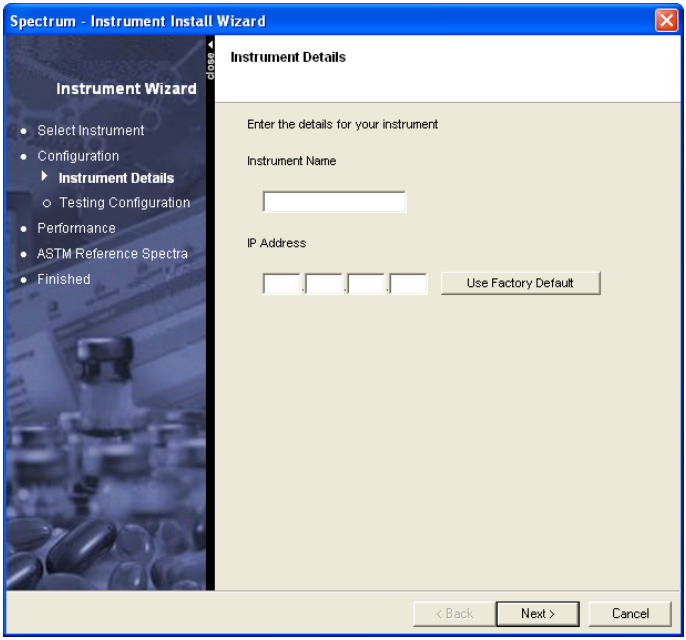
4. Select Add Instrument.

   The Instrument Install Wizard Welcome page is displayed. The Instrument Install Wizard will lead you through the installation procedure.



5. Click **Next**.

   The Instrument Details page is displayed.



6. Enter the Instrument Name.

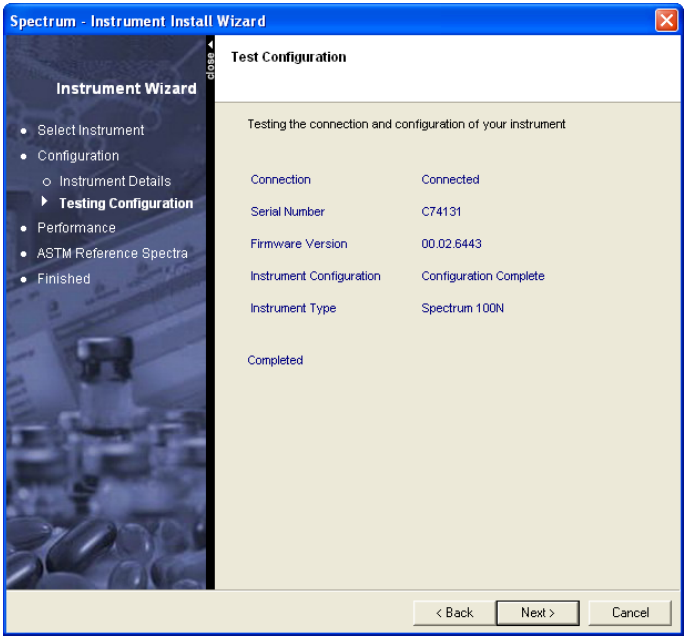
   This may be Spectrum 400, Spectrum 100, Spectrum 100N, or a name to distinguish your instrument.

7. Click **Use Factory Default** if your instrument is connected directly to the PC. If your instrument is connected to the network, enter the **IP Address** and then click **Next**.

   The **Instrument Configuration Disk** page is displayed. This page prompts you for the configuration file supplied on a CD with your instrument.

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

   The Test Configuration page is displayed. This automatically tests the connection and configuration of the new instrument. If any of the tests fail, you cannot proceed.

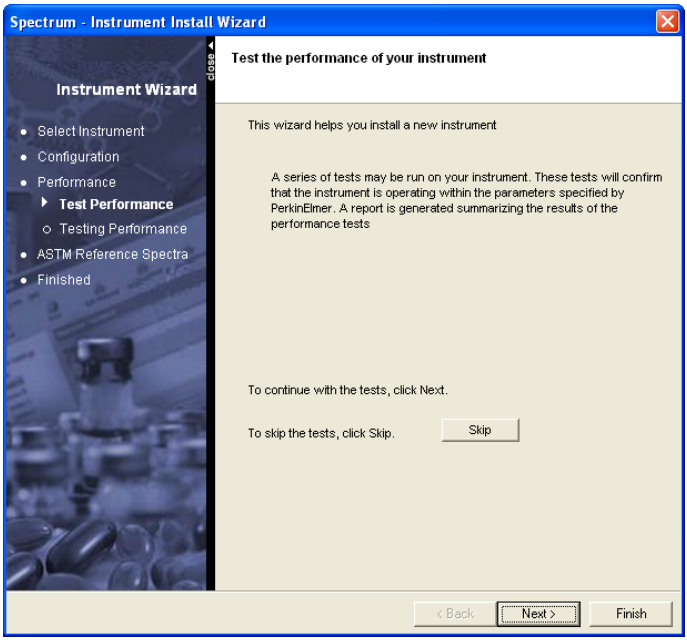


Assuming the **Connection** is working, this page displays the **Serial Number** and **Firmware Version** reported by your instrument, confirms that the installation of the **Instrument Configuration** is complete, and displays the **Instrument Type** recognized by the Spectrum software.

9. When the Test Configuration page displays **Completed**, check that the information is correct.

10. Remove the configuration CD and then click **Next**.

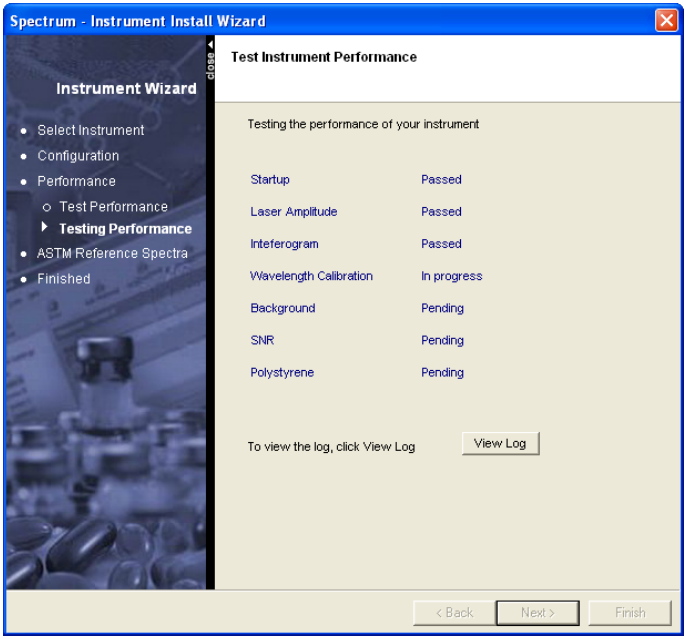
    The **Test the performance of your instrument** page is displayed.



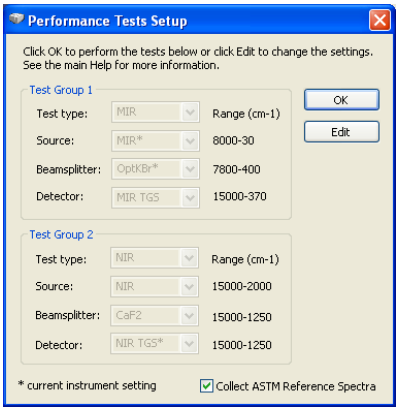
11. If you want to test the performance of the instrument, click **Next**.

    If you do not want to test the performance of the instrument, click **Skip**.

    If your instrument is a Spectrum 100 Series, the software performs a series of instrument performance tests.



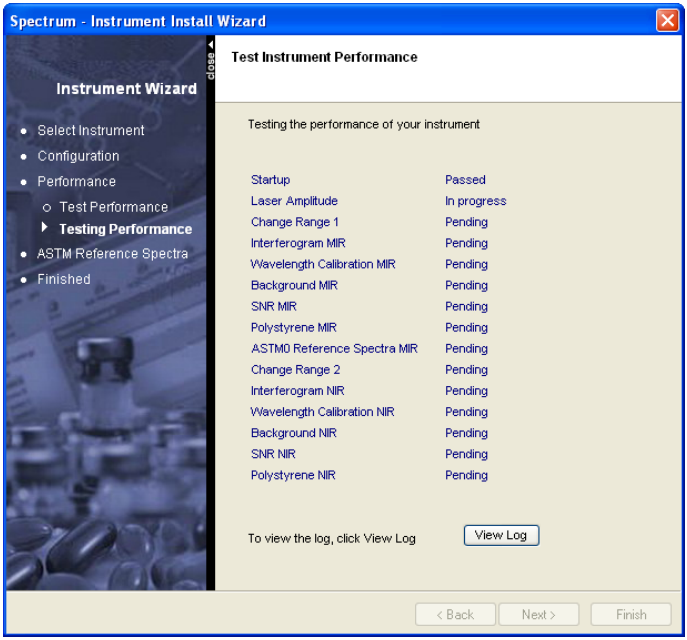
If your instrument is a Spectrum 400 Series, the Performance Tests Setup dialog is displayed.



By default, the performance tests in Test Group 1 are for the current instrument setup, and those in Test Group 2 require the instrument to select the alternate source, detector and beamsplitter (that is, perform a complete automated range change). If you want to perform the tests in a particular order, to perform tests for a particular configuration, or to cancel some tests, edit the settings using the drop-down lists, and then click **OK**.

The wizard works through the Test Group 1 instrument performance tests, performs an automated range change, and then continues with the Test Group 2 instrument performance tests.

A current instrument setting is marked by a *. ASTM reference spectra are collected by default.



12. When the tests are complete, click **View Log** if you want to see the results of the performance tests in more detail.

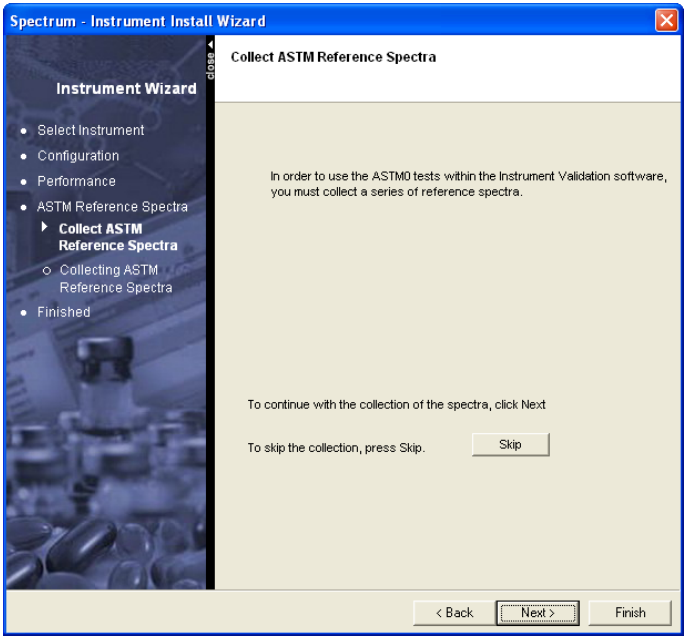
    If you want to view the results of the performance tests later, the log is stored at C:\Program Files\PerkinElmer\ServiceIR\<Instrument Serial Number>\Performance Tests xxx\PerformanceTests.log (where xxx is an incremental number).

13. Click **Next**.

    If your instrument is a Spectrum 100 Series, the **Collect ASTM Reference Spectra** page is displayed.

If your instrument is a Spectrum 400 Series, the **Collect ASTM Reference Spectra** page is not displayed if the ASTM spectra were collected during the Performance Tests.

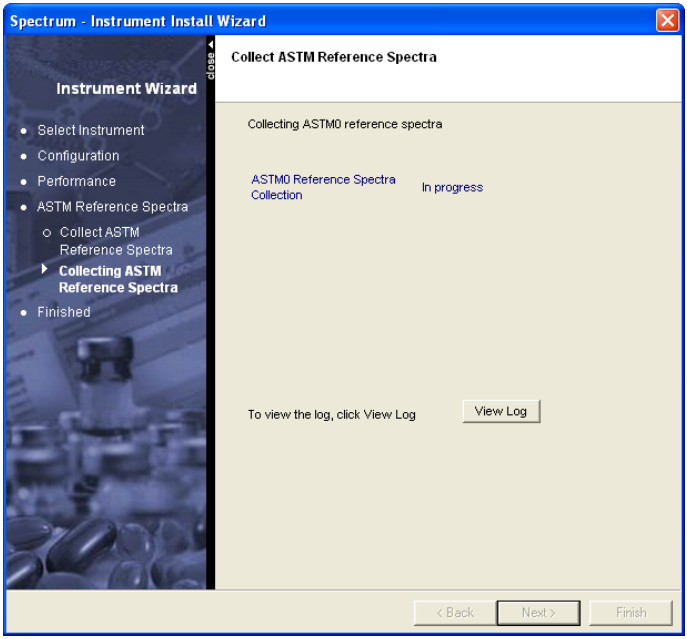
These spectra are used when ASTM validation tests are performed. For more information about ASTM level 0 tests, see the Spectrum Help file.



14. To collect ASTM Reference Spectra, click **Next**.

    If you do not want to collect ASTM Reference Spectra, click **Skip** to move to the Finish page.

    If your instrument is a Spectrum 400 Series, it may need to change the data collection range before collecting spectra.

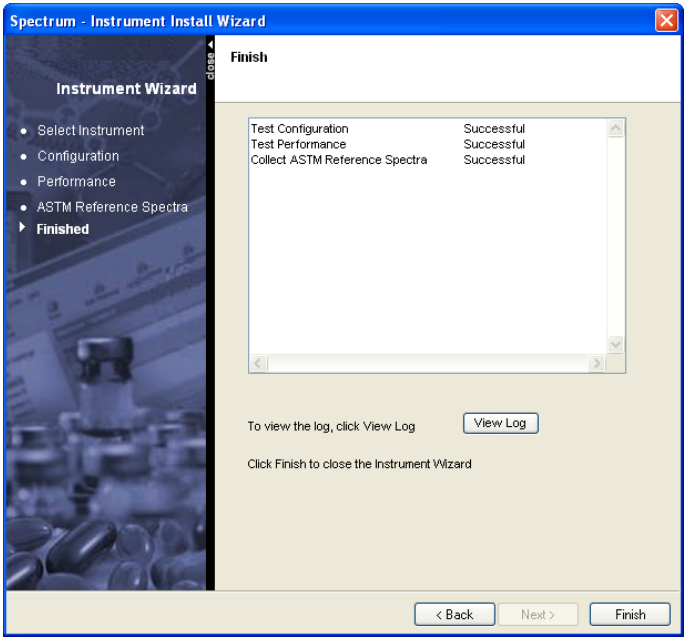


15. When the ASTM0 Reference Spectra Collection is complete, click **View Log** if you want to see the results in more detail.

    If you want to view the results later, the log is stored at C:\Program Files\PerkinElmer\ServiceIR\<Instrument Serial Number>\Performance Tests xxx\PerformanceTests.log (where xxx is an incremental number).

16. Click **Next**.

    The **Finish** page is displayed.



The Finish page provides a summary of the instrument configuration. In this case the configuration and performance have been tested successfully, and the ASTM Reference Spectra have been collected successfully.

You can also click **View Log** to see the results of the configuration and performance tests in more detail.

17. Click **Finish** to complete the installation.

    If the source, beamsplitter, or detector on your Spectrum 400 was changed to facilitate testing, you are given an opportunity to return the instrument to its original setup.

18. Click **Yes** or **No** as required.

In the Enhanced Security version of Spectrum you can now assign which groups have access to the instrument. For more information see *Assigning the Group to an Instrument* on page 54.

If you want to use this instrument to collect data you must close Spectrum, start Spectrum again, and then select this instrument in the Spectrum Login dialog.

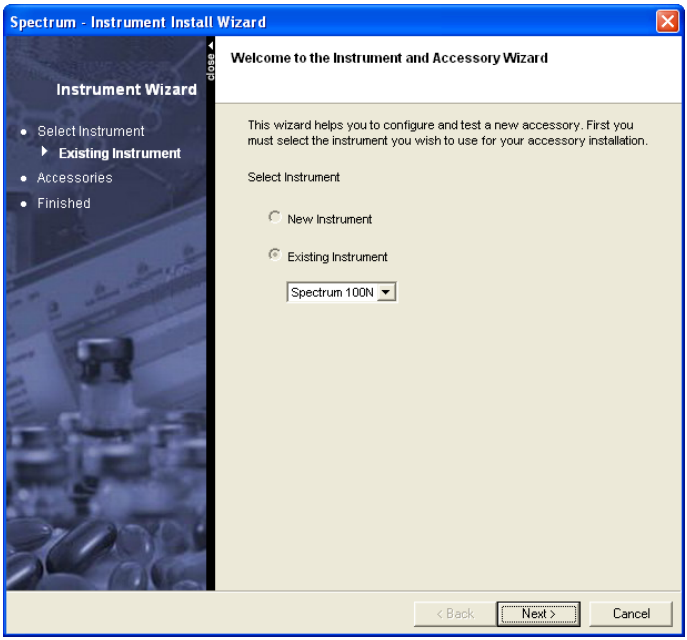
Adding an Accessory

To add an accessory:

1. Login to Spectrum as an Administrator.
2. Select Instrument and Accessory Configuration from the Administration menu.

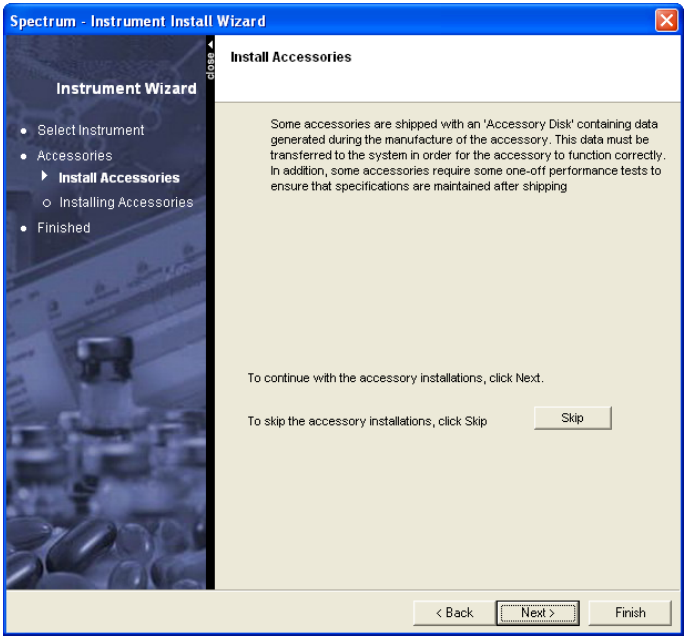
   A sub-menu is displayed.
3. Select Add Accessories.

   The Instrument Install Wizard Welcome page is displayed. The Instrument and Accessory Wizard will lead you through the installation procedure.



4. Select the instrument on which the accessory will be installed, and then click **Next**.

   The **Install Accessories** page is displayed.

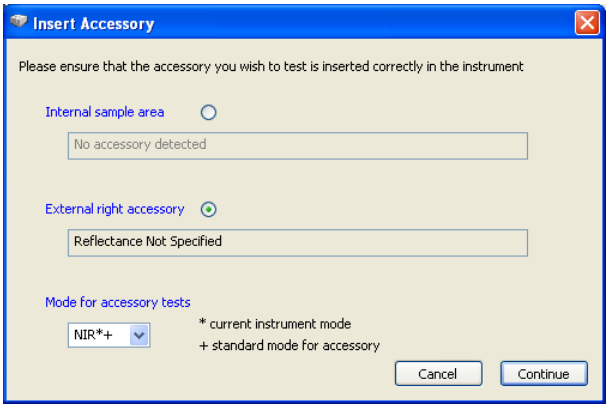


5. Fit the accessory you want to install into the instrument as described in its User's Guide.

   Typically, you remove the current accessory from the instrument, then slide in the new accessory, making sure that it is properly connected. When an accessory has been fitted into the instrument it is automatically recognized by the Spectrum software.

6. Click **Next**.

   The Insert Accessory dialog is displayed. In this case the current accessory is an external reflectance accessory on a Spectrum 400. If your instrument is a Spectrum 100, or a Spectrum 400 with no external accessory fitted, a simplified dialog is displayed.



7. If an external accessory is fitted, select the accessory you want to install.

8. Select the Mode (wavelength range), in which you want to test the accessory.

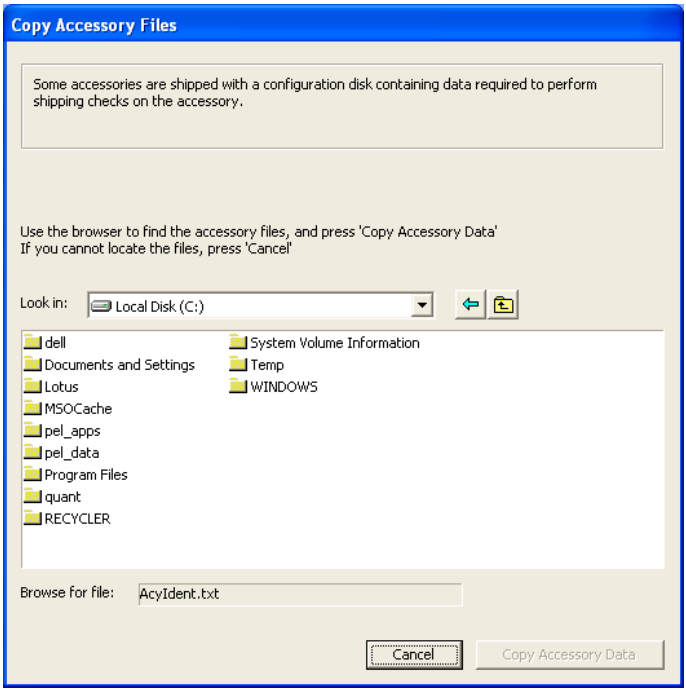
   The current instrument mode is marked by a ***** and the standard operating mode of the accessory by a **+**.

   If you do not select the current wavelength range, a wavelength range change will be performed before testing begins.

NOTE: Depending on the beamsplitters and detectors fitted, the instrument requires some time to equilibrate after changing ranges and before Performance Testing can continue.

9. Click Continue.

   Some accessories (for example the Universal ATR), are shipped with a CD containing, for example, reference spectra generated during manufacture. In these cases the **Copy Accessory Files** page is displayed, which prompts you for the configuration CD supplied with the accessory.

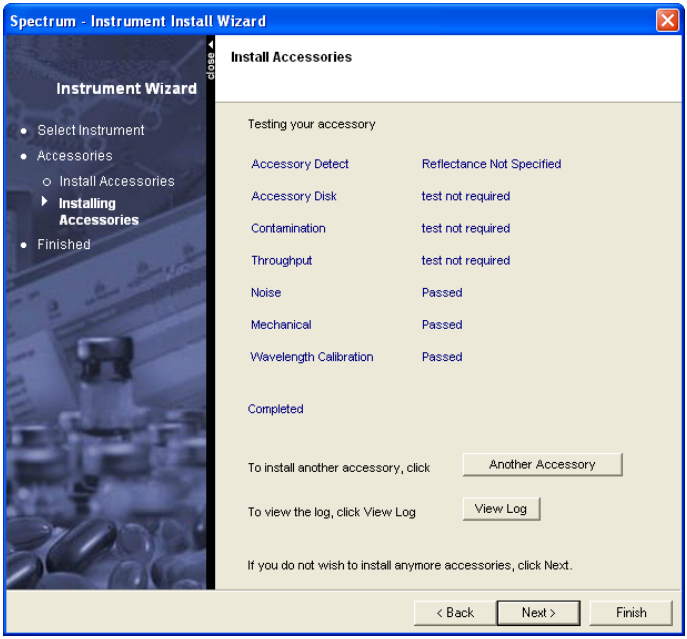


10. Navigate to the configuration file, and then click **Copy Accessory Data**.

    The Install Accessories page is displayed.

    The software performs a series of accessory performance tests. You may be prompted to remove the accessory briefly, and then replace it. This is to clear the beam path while a background spectrum is collected.

    If your instrument is a Spectrum 400 Series, it may need to change the data collection range before collecting spectra.



11. When the accessory tests and calibrations tests are complete you can install another accessory, if required, by clicking **Another Accessory**.

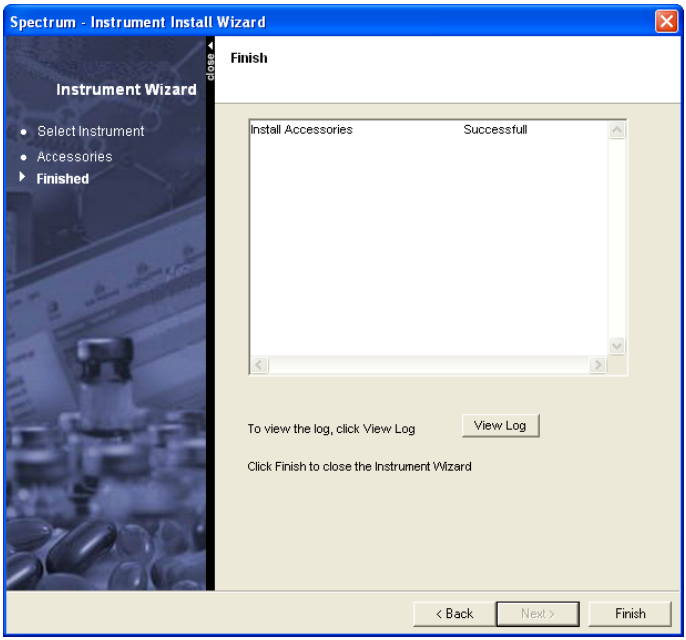
    You are returned to the start of the installation wizard.

12. Click **View Log** if you want to see the test results in more detail.

    If you want to view the results of the accessory tests later, the log is stored at C:\Program Files\PerkinElmer\ServiceIR\<Instrument Serial Number>\Performance Tests xxx\PerformanceTests.log (where xxx is an incremental number).

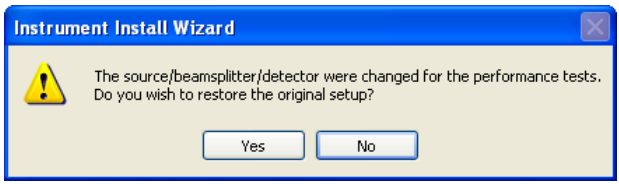
13. Click **Next**.

    The **Finish** page is displayed.



14. Click **Finish** to complete the installation.

    If the source, beamsplitter, or detector on your Spectrum 400 was changed to facilitate testing, you are given an opportunity to return the instrument to its original setup.



15. Click **Yes** or **No** as required.

Removing an Instrument

To remove an instrument:

1. In Spectrum, select **Instrument and Accessory Configuration** from the Administration menu.

   A sub-menu is displayed.

2. Select Remove Instrument.

   The Remove Instrument dialog is displayed.

3. Select the instrument that you wish to remove from the drop-down list.

4. Click **OK**.

   The instrument is removed.

Other Considerations

Sharing the PerkinElmer Security Database Across a Network

If you have multiple installations of PerkinElmer software that use the Security Database, you should consider whether to share the database across a network.

The advantages of sharing the database are:

- PerkinElmer User names and Passwords are global so can be re-used with multiple products;
- The security policies for all PerkinElmer applications using the security system can be consistently applied;
- The Audit Trails and Login History are 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.

However, if the network is not reliable it might be better to keep the database on the local PC.

When Spectrum is installed, the Security Database is installed on the local PC. You can use Database Tools to create a new database on the network, or register with an existing database on the network. For instructions see the Database Tools Help.

NOTE: In the Standard version of Spectrum, you must copy the [username].ini and [username].cfg configuration files to all PCs as they cannot be shared. In the Enhanced Security version of Spectrum, you must copy the [groupname].ini, [groupname].cfg and [groupname].bci configuration files to all PCs as they cannot be shared.

Shut Down of Windows with Spectrum Still Running

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

Removing Accessories During a Scan

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

Appendices

Appendix I – Configuring TCP/IP Communication

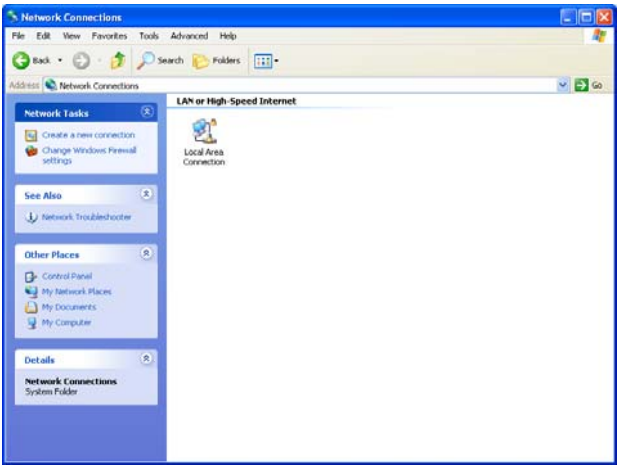
TCP/IP is the communications protocol used by the Spectrum 400, the Spectrum 100, and the Spectrum 100N to connect to the PC. If TCP/IP communication is not configured on your PC you will need to do so before you can establish communications between the PC and your instrument.

NOTE: You must be logged on at Windows Administrator level to configure TCP/IP.

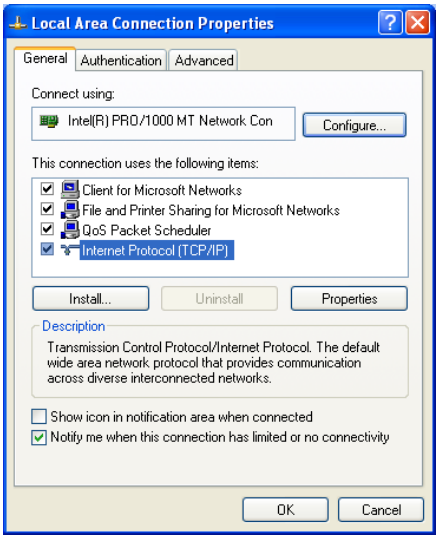
NOTE: The dialogs shown below are typical examples of a straightforward installation: they should not be taken as exact representations of what you will see on your PC. If you need assistance, please talk to your network administrator.

1. From the Start menu, select **Settings** and then **Control Panel**.
   The Control Panel dialog is displayed.

2. Click Network Connections.
   The Network Connections dialog is displayed.

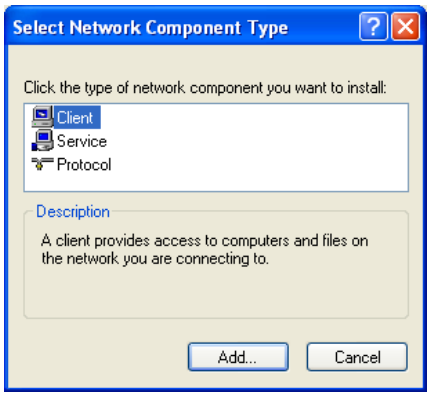


3. Right click on Local Area Connection and then select **Properties**.
   The Local Area Connection Properties dialog is displayed.



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

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



6. Select **Protocol** and then click **Add**.

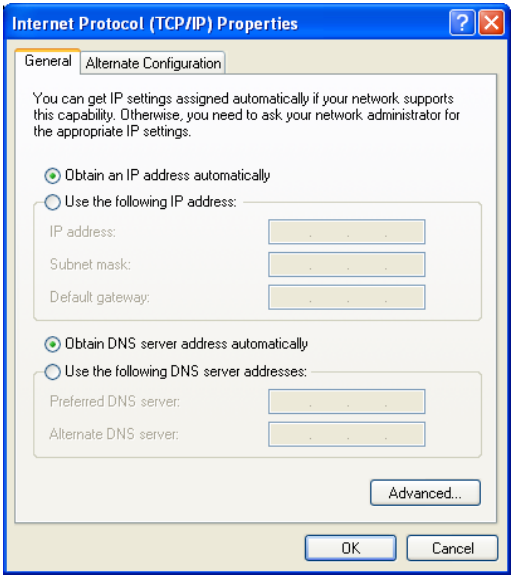
   The Select Network Protocol dialog is displayed.

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. Select Internet Protocol (TCP/IP) and then click Properties.

   The Internet Protocol (TCP/IP) Properties dialog is displayed.

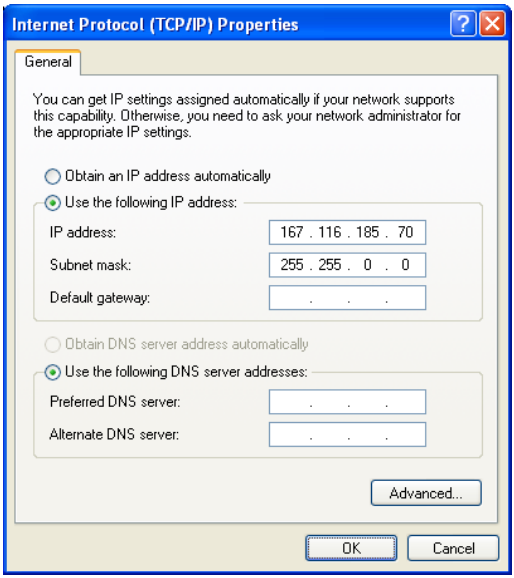


9. Select Use the following IP address and then type in the IP address and Subnet mask for the PC.

   If your PC is on a network, you will need to consult your network administrator to get an IP address. If your PC is not on a network, you should enter the numbers shown on the next page.

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'.

NOTE: If you use the settings shown overleaf you must not connect the PC to an Internet enabled network.



10. Click **OK**.

    You will be prompted to restart the PC.

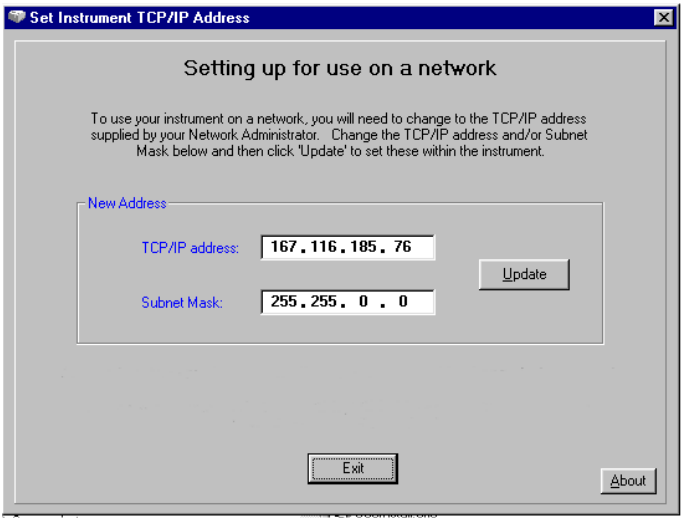
Using the SetIP Utility

The SetIP utility may be used to change the TCP/IP address of a Spectrum 400, Spectrum 100 or Spectrum 100N instrument, especially if the computer is connected to a network. To access SetIP and change the TCP/IP address follow the procedure as outlined below.

NOTE: Ensure that the Spectrum software is not running while using this utility as SetIP may not run correctly.

1. Open Windows Explorer and double-click **SetIP.exe** which is found in the C:\Program Files\PerkinElmer\ServiceIR directory.

   The SetIP program starts.



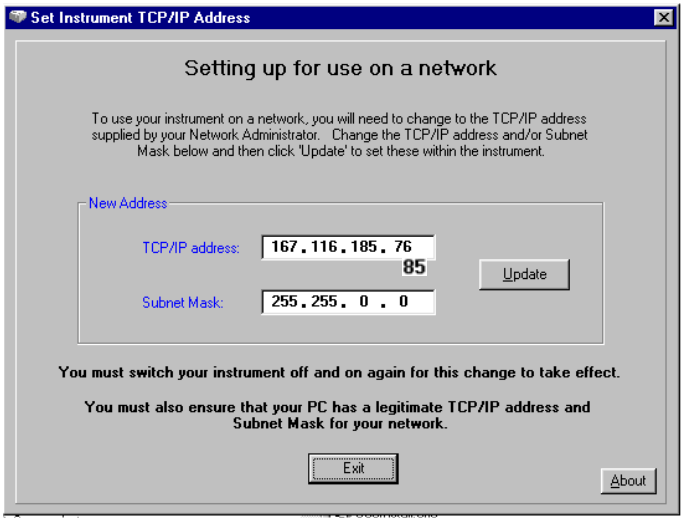
   The SetIP program displays the current address of the default instrument connected to the PC.

   The address shown above is only an example and may not reflect the TCP/IP address that you are using.

2. Enter the new address in **TCP/IP address** and **Subnet Mask** and then click **Update**.

   Further on-screen instructions below **New Address** will be displayed, which serves as confirmation that the new TCP/IP address has been conditionally accepted.

If the new TCP/IP address is not accepted then an error dialog will be presented.



3. Click **Exit** to close the SetIP utility.

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

   The TCP/IP address of the instrument is successfully changed.

Appendix II – Windows Configuration Script

NOTE: The Windows Configuration Script is only available on the *Spectrum ES Software CD*.

For 21 CFR Part 11 systems further security is recommended to make sure, for example, that data files cannot be deleted or tampered with. The lockdown script will set the essential security permissions automatically, but the Windows administrator should review what has been set and consider whether further changes are required.

Running the Lockdown Script

To run the lockdown script:-

1. Insert the *Spectrum ES CD* in the drive.
   The software installation program may start automatically.
2. Using Windows Explorer, double-click on the \Security\ directory.
3. Double-click on **Lockdown.vbe** to run the script.

What the Lockdown Script Does

The Lockdown Script sets directory and file permissions, sets up default windows groups and accounts and “locks down” the desktop.

Directory and File Permissions

The Lockdown script sets the following restricted permissions on these directories and files:

NOTE: c in each case refers to the drive Spectrum ES is installed to.

Directory	Windows Administrator	‘Everyone’
C:\pel_apps\.....	Full Control	Modify
C:\pel_data\.....	Full Control	Modify
C:\pel_data\reports\	Full Control	Write once, Read
C:\pel_data\docs\	Full Control	Write once, Read
C:\pel_data\spectra\	Full Control	Write once, Read
C:\pel_data\igram\	Full Control	Write once, Read
C:\pel_data\chrom\	Full Control	Write once, Read
C:\pel_data\pktables\	Full Control	Write once, Read

C:\windows\temp	Full Control	Full Control

Files	Windows Administrator	'Everyone'
C:\windows\pel_inst.ini	Full Control	Modify
C:\windows\pel_apps.*	Full Control	Modify
C:\windows\pe_sopb.ini	Full Control	Modify

In addition, the lockdown configures the following:

- Restricts permission to Microsoft Management Console (MMC).

  MMC is a feature of Windows 2000 and XP that allows a user to configure security policies for their PC. If a user were to run this, they could potentially undo parts of the lockdown script. Refer to *Management Console and Active Directory* on page 96 for more details.

- Lifts permission to Internet Explorer.
- Disables Windows XP Guest account.
- Sets the PerkinElmer logo as the backdrop for all new users.
- Configures the restricted Start menu.

  This uses registry policy settings to disable items including Control Panel, My Computer, My Network Places.

NOTE: Applications installed on the PC after the Lockdown Script has been run do not appear on the Start menu. The Windows Administrator must copy the application shortcuts to the Start menu (or desktop) as required.

- Creates the SpectrumES group and the SpectrumES User
- Creates the PEService user.

Write Once directories allow files to be created but they cannot be deleted, edited, renamed or moved.

If operating in a 21 CFR Part 11 environment it is highly recommended that permissions of this type are used to protect key data, such as spectrum files and reports.

Default Windows groups and accounts

The script then sets up the following default accounts:

SpectrumES User <password: SpectrumES User>
which is an ordinary Windows User account.

PEService <password: peservice>
and is for use by PerkinElmer service engineers.

The lockdown script sets these permissions for the Windows group called Everyone. This is the windows default group that has all users as members. Additionally the minimum Windows password length is set to six characters.

IR Assistant / Quant Import

In addition to setting up default groups and accounts the script also sets the correct Registry permissions for IR assistant and Quant Import to run.

However, if you wish to set up IR Assistant and Quant Import to run on a restricted system without running the lockdown script, then do the following:

1. Log onto Windows as an Administrator.
2. Click **Run** from the Start menu.
3. Enter the following text precisely (with the quotations marks as written)
   cmd /c ""d:\security\regini" "d:\security\irasst.txt""

NOTE: The letter d refers to the letter assigned to the CD-ROM drive. It should be replaced with the appropriate letter for your CD-ROM drive.

4. Click **OK**.
5. Enter cmd /c ""d:\security\regini" "d:\security\Quant_import.txt""
6. Click **OK**.
   IR Assistant and Quant Import will now run on a restricted system.

Background Wallpaper

The script sets the background wallpaper.

Locking down the desktop

Examples of the settings are:

- No Control Panel available
- No Find
- No Network Neighborhood
- No Right mouse button click menus

NOTE: The full list of settings made can be found in \windows\system32\policy.txt. These settings can be edited if required before running the lockdown script. The settings will apply to ordinary Windows Users (for example, *SpectrumES User*), not to the existing Windows administrator.

Management Console and Active Directory

The management console is a Windows 2000/XP feature that allows the Windows administrator the facility to set many features in Windows, in particular security features. The list of choices is huge but all the ones set by the Lockdown scripts can be set or unset via the Management Console (and its Snap-ins).

The Windows administrator may wish to review the options available from the console in light of the 21 CFR Part 11 requirements.

Active Directory is a feature in Windows that manages computer settings from a central place and allows security and other settings to be centrally managed by an Active Directory server usually on a Windows domain server.

If the target computer for PerkinElmer ES software is on an Active Directory network, then this may be a preferable way of managing computer/windows settings than by using the lockdown script.

Appendix III – Backup and Recovery

Backing up and Recovering Databases and Files

It is essential that backups are regularly made of key files and databases in order to secure the data in case of computer failure or accidental loss or damage.

The following directories (including subdirectories) must be backed up regularly:

C:\pel_data\

The following files must be backed up regularly:

C:\Documents and Settings\All Users\Application Data\PerkinElmer\Security System\Users.mdb

C:\Documents and Settings\All Users\Application Data\PerkinElmer\Security System\Backup\Users.bak

C:\Windows\Pel_inst.ini

C:\Windows\Pel_apps.ini

C:\Windows\pe_sopb.ini

In Spectrum ES only, you must also backup the following:

C:\Documents and Settings\All Users\Application Data\PerkinElmer\SpectrumES\audit.mdb

C:\Windows\Pel_apps.bci

Recovering from Checksum Failures

Spectrum ES uses a variety of security techniques to ensure that files cannot be tampered with either accidentally or deliberately – one of these is to use Checksums to ensure the data has not been tampered with. Under normal operation checksums are used in the application to validate the data security, however a checksum failure can occur after a number of situations:

- Hard disk failure
- Power failure
- Software crash, either the application or Windows or another application
- Falsification of data

The only remedy to an error message stating there is a checksum failure is to restore from a backup database. Checksum warnings will not occur during normal operation of Spectrum ES software. If they occur then the reasons for them should be investigated and the reasons understood, before simply recovering from the problem.

Security database (includes the Spectrum ES Administrator's Audit Trail)

The security system automatically backs up the Users.mdb database each time the software is closed, in a subdirectory called \Backup:

C:\Documents and Settings\All Users\Application Data\PerkinElmer\Security System\Backup\Users.bak

The Windows Administrator can restore from this database if the active database becomes corrupt and gives a checksum failure:

1. Log on as Windows Administrator.
2. Rename, Move or Delete Users.mdb
3. Copy \backup\Users.bak as Users.mdb to replace the old one.

Any changes to the users and groups made since the last time the software was closed will be lost.

Spectrum ES Audit Trail database

If the database (audit.mdb) fails for one of the above reasons, then replacing the corrupt database with a backup will usually cure any problem and allow the application to run again.

To work with the audit trail, login as a Spectrum Administrator, and then from the Administration menu select **View Spectrum Audit Trail**.

Checksums and .bci & .ini files

A security feature of Spectrum ES is that all PerkinElmer .ini files (e.g. pel_apps.ini) which contain important system information can no longer be altered by directly changing the text in the files. **Changes must not be attempted**. (they will in fact be ignored).

Although the .ini files still remain, they have been superseded by equivalent .bci files, which contain the same data and are encrypted and checksummed.
Any attempt to change a .bci file will cause a checksum failure and Spectrum will issue an error message similar to "**Checksum failure on …..bci file**" or "**Incorrect checksum value in file \pel_data\…..*.bci**". Spectrum can no longer be used if that happens.

- To recover from this, your administrator should move or delete the .bci file and then run the following utility:
  C:\Program Files\PerkinElmer\ServiceIR\BCItranslate.exe

This utility will restore the .bci file to a clean state and Spectrum will run again. The utility will ask you to log in and you must log in as a Spectrum Administrator. The .bci files will be checked to make sure they have valid checksums, and any that fail the check can be repaired. A record of this action is placed in the Audit trail database.

Spectra files

These are discreet files, usually stored in the c:\pel_data\spectra\ subdirectory with extensions .sp.

These files are all checksummed and when files are loaded into Spectrum ES, their integrity is checked.

If the checksum isn't present or is wrong, then an error message is produced and the file will not load.

It is possible to use the Legacy File converter to convert non-checksummed files. See *Appendix IV*.

Appendix IV – Legacy File Converter

NOTE: The Legacy File Converter is only available in the Enhanced Security version of Spectrum.

21 CFR Part 11 technical compliance mandates very high levels of data integrity and security. To ensure that Spectrum ES only accesses and uses data acquired on a 21 CFR Part 11 compliant system, a data security checksum has been added to the spectrum data file generated from an Enhanced Security software application.

Spectra without this 21 CFR Part 11 checksum will not be read into the Enhanced Security software and cannot be processed. This feature stops data from older data systems from being automatically used in new compliant systems.

To allow users access to their legacy data a Conversion Utility has been included as Part of the Spectrum ES Administration tools. This utility allows the Administrator to add a data security checksum to all spectra in a directory of legacy spectra.

NOTE: Use of the utility should be highly controlled and spectra that are converted should have full supporting GxP provenance as Part of their audit trail.

1. Login to Spectrum as an Administrator.
2. Select **Legacy File Converter** from the Administration menu.

   The Legacy File Converter is displayed.
3. Click the appropriate **Browse** and on the file selectors displayed, select the **Source Path** and **Destination Path** for the directory containing the legacy data.

NOTE: Ensure that the appropriate Write permissions for the destination directory are set before attempting to carry out the conversion.

4. Click **Next**.

   The data is copied and a checksum is added to each file, then the new files are written to the destination directory, leaving the original data untouched.
5. To view information about the conversion, click **View Log**.

   A log file is displayed.

Appendix V – Quant Import Utility

NOTE: The Quant Import Utility is only available in the Enhanced Security version of Spectrum.

The Quant Import utility allows the administrator to include legacy Quant method(s) from PerkinElmer's Quant C, Quant+ or Beer's Law applications into Spectrum ES. The legacy methods and calibration files need to be exported from the Quant PC using the Quant Export tools supplied with the Quant applications before it can be imported onto the Spectrum ES PC. Exported Quant methods are saved as a zipped file with a .qmz extension.

NOTE: Use of the utility should be highly controlled and imported methods should have full supporting GxP provenance as Part of their audit trail.

1. Login to Spectrum as an **Administrator**.
2. Select **Quant Import** from the Administration menu.
   The Quant Import dialog is displayed.
3. Click **Add Zipfile To List** and then navigate to the .qmz files to be added.
   File(s) chosen in this manner will be listed within **Source Files**.
4. Click **Next**.
   The .qmz files are extracted. The **Progress** of the extraction process is indicated by **Zip files extracted**, **Zip files remaining**, **Number Of Errors** and status bar. A checksum is added to each file before being written to the destination directory.
5. Once notification is given that extraction is complete, **View Log** should be clicked to ascertain which Quant methods were successfully extracted to the appropriate quant directory.

NOTE: The destination directory for the extracted methods cannot be changed and it is important to ensure that the appropriate Write permissions are assigned before attempting this procedure.

6. Close the Import Log and then click **Exit** to close the Quant Import dialog.

Appendix VI – Windows Login Security, NTFS Permissions and Spectrum Security

Since there are two security systems it is important for the system administrator to understand the link between the Windows login system and the Spectrum system. Here is a table of the possible combinations and the implications and typical roles:

Login to Windows as	Login to Spectrum as	Can do	Cannot do	Comment	Typical role
Administrator	Administrator	Anything	No restrictions	Must be a suitably trained qualified person, knowledgeable in both Windows and Spectrum.	Lab manager trained in Windows administration
Administrator	User	Anything to Windows including datafiles, adding new applications. Reviewing Windows audit trails (ES), setting up user accounts etc Running Spectrum.	Change Spectrum settings. Access certain menus within Spectrum, depending on given permissions.	Must be a suitably trained qualified person, but might be from the IT dept, who do not need to understand Spectrum.	IT department staff
User	Administrator	Run Spectrum, typically managing Spectrum access. They can run other applications on the PC for which they have permission.	Cannot delete/change data files.	Must be trained in Spectrum, but does not need to be qualified in Windows administration.	Lab manager, chief scientist, supervisor

Login to Windows as	Login to Spectrum as	Can do	Cannot do	Comment	Typical role
User	User	Run Spectrum, typically taking scans and saving data. They can run other applications on the PC if allowed.	Cannot change Windows or Spectrum settings. Cannot delete/change datafiles.	Spectrum user who uses the system on a day-to-day basis. Could be within a 21 CFR Part 11 compliant environment (ES).	System technician, operator Scientist

Appendix VII – Administering the PerkinElmer Security Server Windows User Account

The default PerkinElmer Security Server Windows User Account is called 21cfr. This account is used by the Windows Login functionality.

However, your company's security policy may require you to use some other account. This appendix describes how to create a new account and then change the password of the account.

Creating a New Account

To setup Windows login you should create a new Windows Administrator account, and use it to replace the default Windows Administrator account called 21cfr:

1. Identify or create a new general purpose Windows Administrator account (called for example Local_Administrator).

   To create a new account, use the **User Accounts** dialog which can be opened from the **Control Panel**.

   The new account must be made a member of the local Administrators, Users, and 21CFR_Admin groups.

2. If you are not already logged on using this account, then log out and back in to Windows using this account.

3. Create another new Windows Administrator account.

   As an example you could enter the User name **New_21cfr**, however we recommend that you use a different User name and Password.

   The new account must be made a member of the Administrators, Users, and 21CFR_Admin groups.

   This new account will replace the account called 21cfr, which is used by the Spectrum security system. The 21cfr account will then be disabled.

4. From the Start menu, select **Run**.

   The Run dialog is displayed.

5. Enter C:\Program Files\PerkinElmer\PE21CFR\config21cfr.exe.

NOTE: For further information on the **config21cfr.exe** utility, see *Appendix VIII – Enhanced Security Settings* on page 107.

6. Login using the Local_Administrator account **User name** and **Password** identified/created in step 1.

   The Enhanced Security Configuration dialog is displayed.

7. Enter the User name of the account created in step 3 into the **Account Name** field.

   In our case we would enter **New_21cfr**. You must enter the User name defined when creating the account.

8. Click **Update**.

9. Enter the Password of the account created in step 3 into the **Current Password** field.

10. Click **Save**.

11. When the information has been successfully updated, select to restart the computer.

12. When the computer has restarted, login as the Local_Administrator.

Changing the Account Password

Your company's internal security policy may require you to regularly change the password of the Spectrum security system account (New_21cfr). If so, it is essential that you follow the procedure below exactly.

To change the password of the account:

1. From the Start menu, select **Run**.

   The Run dialog is displayed.

2. Enter C:\Program Files\PerkinElmer\PE21CFR\config21cfr.exe

3. Login using the Local_Administrator account **User name** and **Password** identified/created in step 1 of the previous instructions.

   The Enhanced Security Configuration dialog is displayed.

4. Select the **Passwords** tab.

5. Select Update password in this program after changing in Operating System.

6. Leave the Enhanced Security Configuration dialog open at the Passwords tab.

7. From the Start menu, select **Settings** and then select **Control Panel**.

8. Double-click **User Accounts**.

   The User Accounts dialog opens.

9. Select the Spectrum security system account (New_21cfr), and then click **Reset Password**.

   The Reset Password dialog is displayed.

10. Enter the new password, confirm the new password, and then click **OK**.

    You should remember this password.

11. In the Enhanced Security Configuration dialog, enter the password in the **New Password** and **Confirm Password** fields.

12. Click **Save** to save the changes to the Enhanced Security Configuration dialog.

    You will have to restart the PC after making the changes, then you will be able to run Spectrum using Windows Logins again.

Appendix VIII – Enhanced Security Settings

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 software. The Security Server passes to the Windows operating system the account credentials of any user that attempts to log on 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 on to the software and sign-off signatures.

The Enhanced Security Configuration program allows the Windows Administrator (Local_Administrator) to set preferences and maintain accounts for software applications.

To run the Enhanced Security Configuration program:

1. Log on to Windows using the Local_Administrator account.

   This user name must be a member of the local Administrators, Users, and 21CFR_Admin groups.

2. From the Start menu, select **Run**.

   The Run dialog is displayed.

3. Enter C:\Program Files\PerkinElmer\PE21CFR\config21cfr.exe

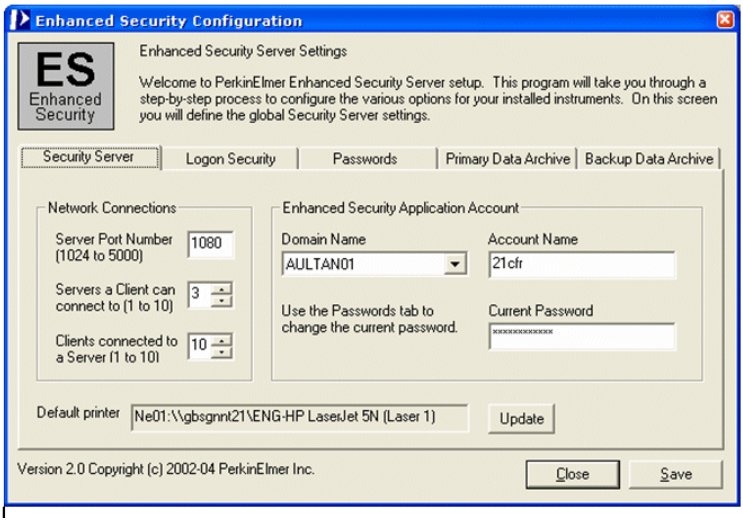
   The Enhanced Security Configuration program is displayed.

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

Security Server – Allows you to enter the account name and password for the Enhanced Security Application Account, change the Server Port Number, Network Connections, and default printer.

Passwords – Allows the password for the Enhanced Security Application Account to be changed.

Security Server Tab



The default name of the Enhanced Security Application Account is **21cfr**.

To change the **Account Name**:

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.

It is unlikely that it will be necessary to change the Network Connection settings, however if there are problems connecting to the security server or an instrument then the following steps may be necessary:

7. Change the **Server Port Number** only if you have installed an application that has the same TCP/IP server port number as you see in the **Server Port Number** field.

   The **Servers a Client can connect to** field represents the maximum number of Security Servers, including the local computer, to which 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.

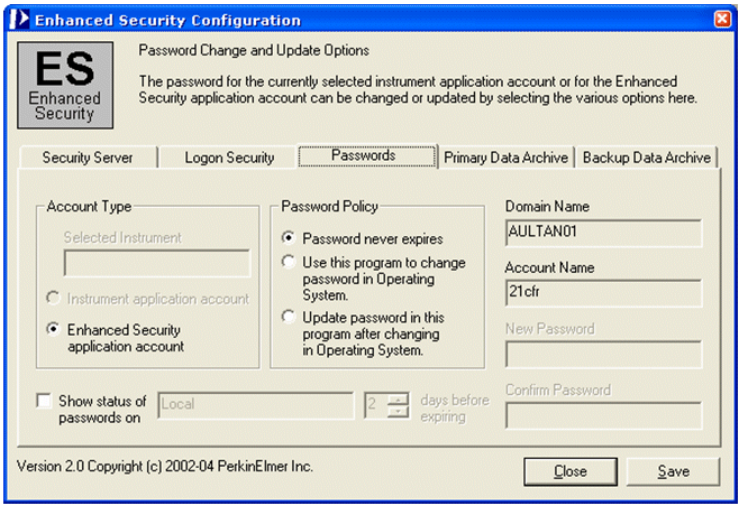
8. The **Clients connected to a Server** field represents the number of applications that a server can have connected at any one time.

   The default value is 10.

To change the default printer:

You must first change the printer using the operating system tools. After you have made this change in the operating system, you can return to this tab and click **Update** (beside the Default printer field).

Passwords Tab



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

To change the password of the Enhanced Security Application Account:

1. Leave the Enhanced Security Configuration program open at the Passwords tab.
2. From the Start menu, select **Settings** and then select **Control Panel**.
3. Double-click **User Accounts**.

   The User Accounts dialog opens.
4. 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.
5. Enter the new password, confirm the new password, and then click **OK**.
6. 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.
7. Enter the new password in the **New Password** and **Confirm Password** fields.
8. Click **Save** to save the changes to the Enhanced Security Configuration program.

   You will have to restart your PC after making any changes.

Troubleshooting

The information below details how to troubleshoot common runtime and installation errors that you may encounter with the Enhanced Security Configuration program. It also describes the Status Monitor. The Status Monitor is a tool that you can use to assess the status of the Enhanced Security Configuration program.

Common errors and fixes

Here is the common error message, followed by a description of the problems that cause it and the probable fixes. You will see different error messages depending on the type of instrument you have equipped with the Enhanced Security Configuration program.

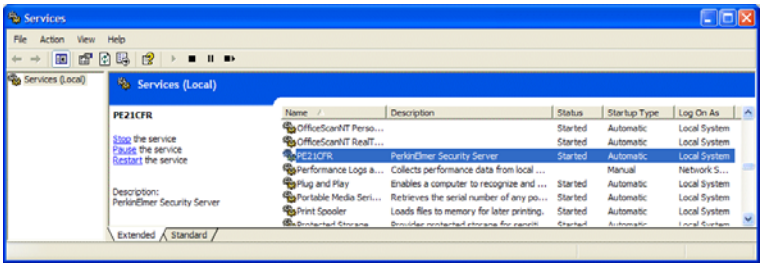
You will see the error message shown above if any of the following problems are occurring:

Problem A: The Security Server is not running.

Fix A: If you cannot run the Enhanced Security Configuration program, then the Security Server is not running. Try the following:

1. Restart the computer. If restarting does not resolve the problem, try this:
2. From the Start menu, select **Settings** and then select **Control Panel**.
3. Double click on Administrative Tools and then Services.

4. Under **Services**, select **PE21CFR.**
   You should see the following:

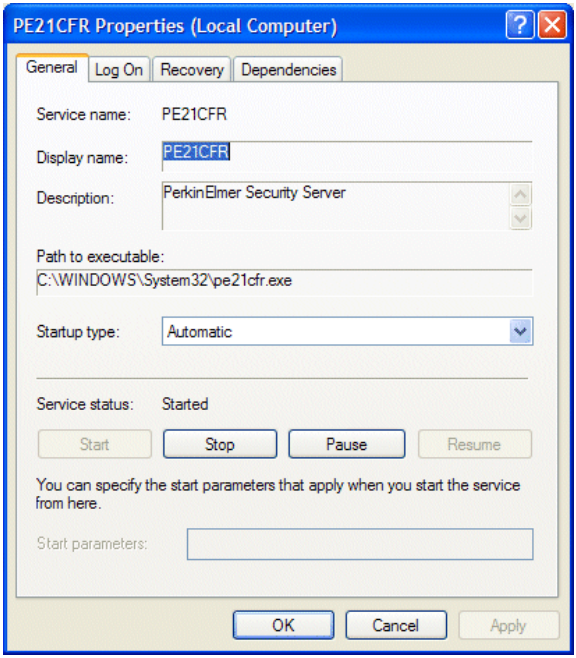


   Note that the **Startup Type** for PE21CFR is **Automatic**.

   - 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**. The System Administrator will probably have to make this change.

To change the Startup Type:

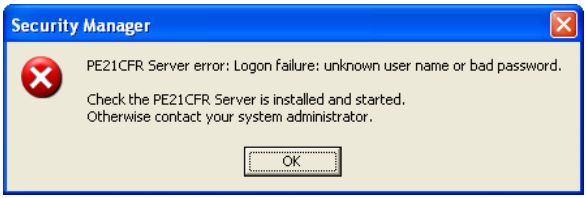
1. Right-click on **PE21CFR**.
2. Select **Properties** from the menu.
   The PE21CFR Properties (Local Computer) dialog is displayed.



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

Logon Error Message

If the following error message appears before the Spectrum login screen, then this is probably because 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.



To resolve the problem, follow the instructions in *Security Server Tab* on page 108, and *Passwords Tab* on page 109 that describe how to change the Account Name and change the 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**.

You will see this error message if any of the following problems are occurring:

Problem A: 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 will allow the Enhanced Security Application Account credentials to be verified correctly.

Fix A: Delete the Enhanced Security Application Account. Reinstall the Enhanced Security program.

Problem B: The Enhanced Security Configuration program will not run. The local operating system "Administrators" users group may have been deleted.

Fix B: 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 (the default password is 21CFR) has been changed via Windows but not updated in the Enhanced Security Configuration program.

To resolve the problem, carefully enter the new password in the **Enhanced Security Administrator Password** field, and then click **Restart**. The Enhanced Security Configuration program and Spectrum will work correctly after the PC has 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 into it.

Starting the Status Monitor

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

1. Locate the PE21CFR directory on the computer's hard drive.
2. In the PE21CFR directory, locate the file **pe21cfrsvr.exe**.
3. Double-click the file.

   This will start the Status Monitor.
4. When the key icon is in the system tray, the Status Monitor is running. To view the Status Monitor, double-click the key icon in the system tray.

   The Status Monitor is displayed.

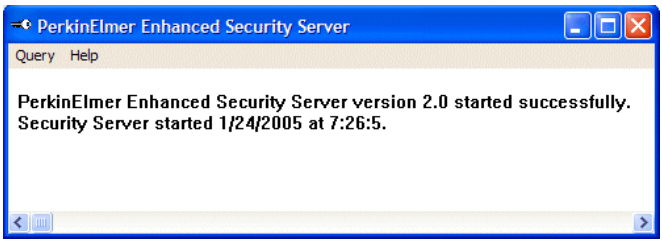
From the **Query** menu, the Status Monitor allows you to view:

- 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.

We will now take a closer look at each of these features:

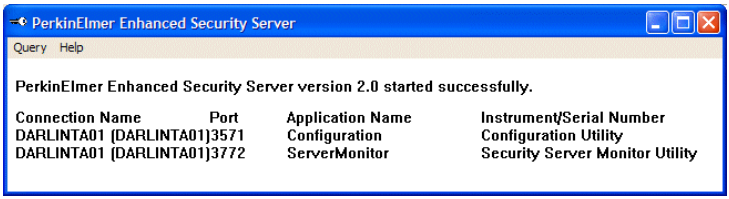
Status

This is the status of the Security Server. It tells you when the Security Server starts and stops running. You can view the status of the Security Server by selecting **Status** from the Query menu.



Connections

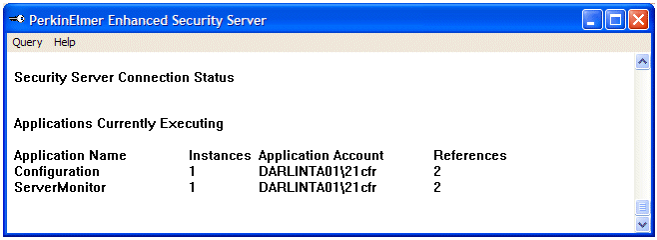
This shows you the computer name, application name, and the instrument and serial number that are connected to the Security Server. It also shows you the name and port number of the connection. You can view the connections to the Security Server by selecting **Connections** from the Query menu.



Applications

This shows you the software applications that are connected to the Security Server. It also shows you 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". This is the number of applications that are using an Application account.

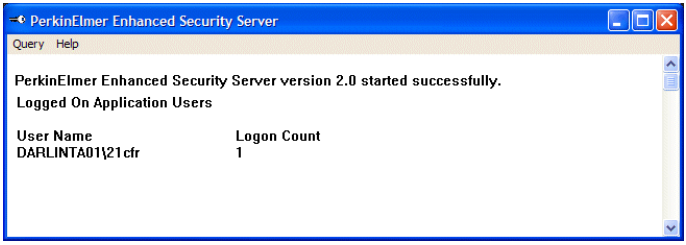
In the example shown below, there are two software applications running; **Configuration** and **ServerMonitor**. There is one instance of each application. The name of the computer on which the Application account is stored is **DARLINTA01**. The name of the Application account is **21cfr**. The number 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 onto the Security Server. The **Logon Count** is the number of logon sessions for the user **DARLINTA01**.

To view the users logged onto the Security Server, select **Users** from the Query menu.



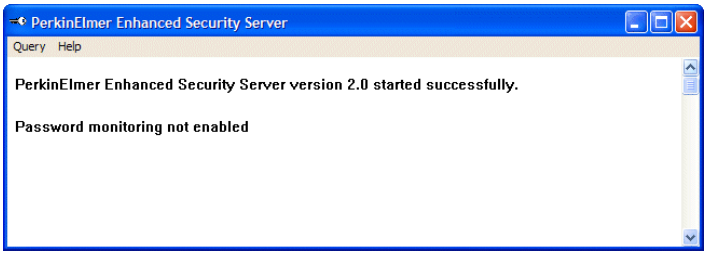
Passwords

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.

To view the Application account password status, select **Passwords** from the Query menu.



Index

R

S

U