ASSURE ID

Administrator's Guide

PerkinElmer®

Release History

Part Number	Release	Publication Date
L1050019	J	August 2018

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

User Assistance
PerkinElmer, Inc.
710 Bridgeport Avenue
Shelton, Connecticut 06484-4794
U.S.A.

Or emailed to: http://www.perkinelmer.com/contactus/

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 © 2018 PerkinElmer, Inc.

Produced in the U.S.A.

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.
AssureID, Frontier, Spectrum Two, and Spectrum are trademarks of PerkinElmer, Inc.

Contents

Introduction

About this Guide

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

The AssureID software suite can be used with Frontier IR Systems, Spectrum Two, Spectrum 400 Series, Spectrum 100 Series, Spectrum One and Spectrum One NTS spectrometers.

AssureID can also be used to carry out data acquisition and analysis of samples using a Raman Triggered Fiber Optic Probe, with the appropriate instrument settings obtained from a .rex (Raman Experiment) file created using the Spectrum software and referenced as part of the method.

This *Administrator's Guide* is divided into the following sections:

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

AssureID Windows Administration – This section describes the tasks that need to be carried out to ensure that the Windows environment in which AssureID is used comply with the requirements of 21 CFR Part 11, for AssureID ES, and to establish routines for the backup and recovery of data.

AssureID Software Administration – This section describes the tasks that need to be carried out by a Software Administrator, using the AssureID software. These include:

- Establishing the login type
- Managing users and groups
- Configuring electronic signature points
- Viewing and managing audit trails

An Overview of AssureID – An introduction to the five main applications: Method Explorer, Method Editor, Analyzer, Results Browser and Database Tools.

Appendices – There are three appendices that describe the following:

- Configuring TCP/IP communications
- Administering the PerkinElmer security server Windows user account
- Enhanced Security Settings provided by the security server configuration utility

Further Information

For more detailed information on using AssureID software, access the on-screen help by selecting the **Contents and Index** option from the Help menu.

For more information on your spectrometer, consult the manuals and multimedia tutorials that come with the instrument.

Conventions Used in this Manual

Normal text is used to provide information and instructions.

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

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

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

Notes, Cautions and Warnings

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

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

CAUTION

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

WARNING

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

Folder Names

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

For example if you have a Windows 7, Windows 8 or Windows 10 operating system, because AssureID runs as a 32-bit application, on 64-bit systems the folder name will be C:\Program Files (x86).

Installation of AssureID

PC Requirements

The following pages detail the hardware and software requirements for the PC that will run the AssureID 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, 1.6 GHz processor.
- At least 1 GB of Random Access Memory (RAM).
- The capability of displaying at least High Color (16 bit) at 1280 x 1024 (normal) or 1280 x 900 (widescreen).
- 40 GB Hard disk with at least 1 GB free space as an NTFS drive.

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

- CD-ROM drive.
- Ethernet network connection (for Frontier FT-IR, Spectrum 100N, and Spectrum 400 Series instruments).
- A keyboard and PS/2®-style mouse.

Software Requirements

Operating System

This software requires that either Windows® 7 Professional (32-bit or 64-bit), or Windows® 8.x Pro (32-bit or 64-bit) , or Windows® 10(32-bit or 64-bit) operating system is installed on the PC before you install AssureID.

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

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

TCP/IP Communication

To operate Frontier IR Systems, Spectrum Two, Spectrum 400 Series, or Spectrum 100 Series spectrometers, you will need TCP/IP protocols established on the PC (see *Appendix 1: Configuring TCP/IP Communication* on page 82). We recommend that you do not install any software until this has been set up.

Previous versions of IR Software

We recommend that you purchase a new PC to run the software (see *PC Requirements* on page 10). If you are re-using a PC, we recommend that you re-format the hard disk on the PC (after backing up any important data) and re-install Windows before installing AssureID.

NOTE: AssureID ES will not install on a PC that already has installed Spectrum version 3.x, or later versions of the standard Spectrum software; that is, non-ES versions.

NOTE: If you have AssureID version 1.0 or version 2.1 already installed, you should backup your databases and then un-install before installing the latest version of AssureID. You can use the data migration tool to migrate the data to the new database. See *Using Database* Tools on page 28 for further information.

Installing AssureID Software

NOTE: We strongly suggest you read the hardware and software requirements given in *AssureID PC Requirements*, starting on page 10, before attempting to install your software.

NOTE: Before installing the software, we recommend that you read and print the release notes (AssureID Release Notes.rtf or AssureID Release Notes.pdf), which can be found in the Documentation folder of the AssureID CD, because they contain important information that may not be in this *Administrator's Guide* or the on-screen help.

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

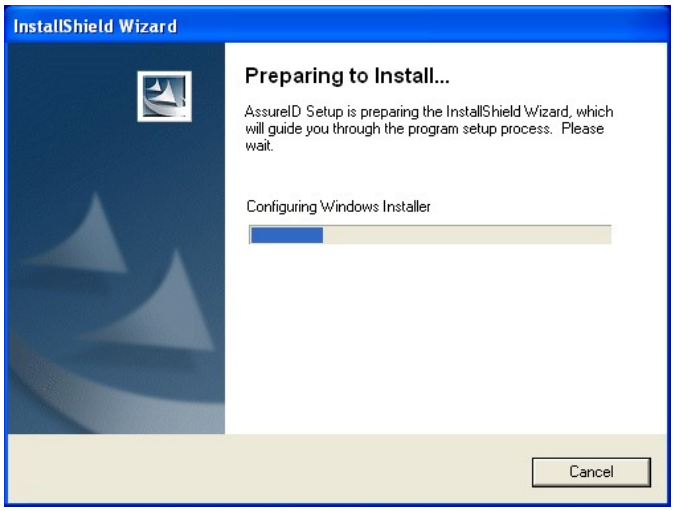
NOTE: You must be logged on to Windows as an Administrator before installing the software.

The AssureID CD contains an Installation Wizard to help you install the correct software on your PC.

1. Place your AssureID CD into your CD drive.

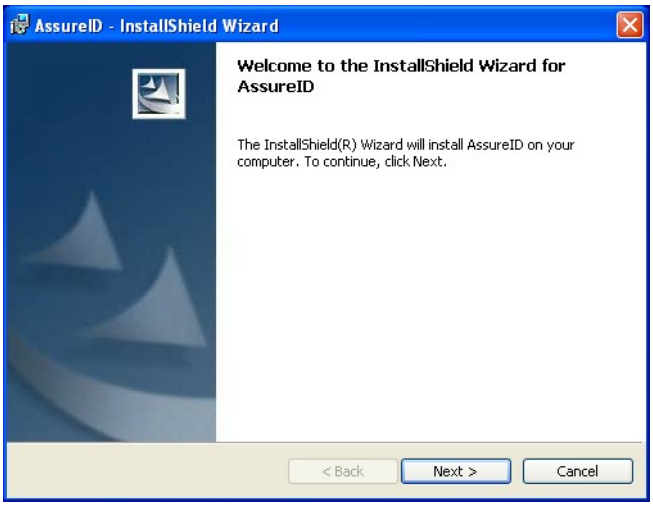
2. If the installation program does not start automatically, start the program **setup.exe** located in the root folder of the CD.

   The InstallShield Wizard starts.

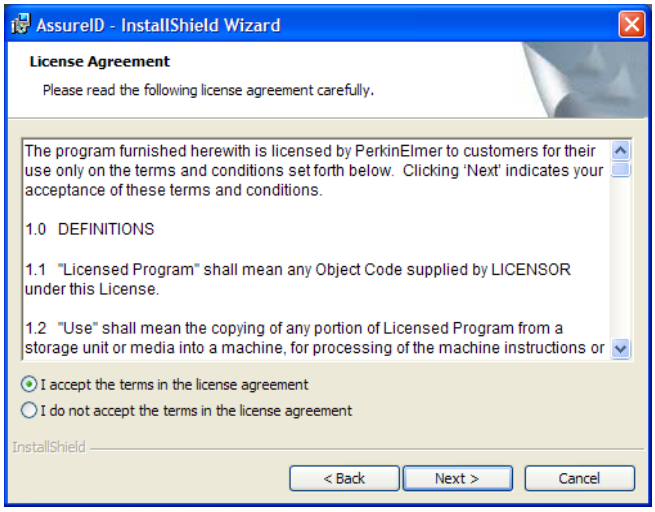


   If you have a previous version of the AssureID software installed, you will be required to uninstall AssureID. Select **Remove** and then click **Next** to uninstall the software. Do not attempt to repair the software as this will result in an error.

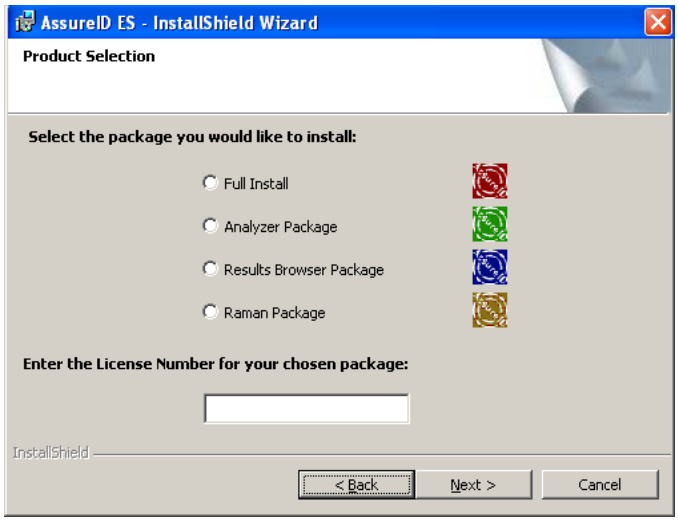
When the installer is ready, the Welcome dialog is displayed.



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



4. Read the license and if you accept the terms, select that option and then click **Next**.
   You will then be asked which type of installation you would like.



5. Select the package you would like to install.
   The options are described below.

Full Install

Installs Method Explorer, Method Editor, Analyzer, Results Browser and Database Tools. This option is suitable for installations where Method Developers develop methods for use by analysts.

Analyzer Package

Installs Method Explorer, Analyzer, Results Browser and Database Tools. This option will be suitable for installations where Analysts will analyze samples and validate instruments.

Results Browser Package

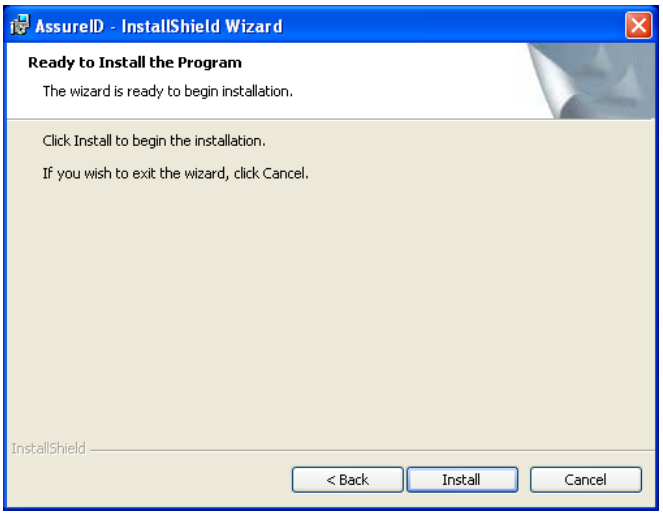
Installs Method Explorer, Results Browser and Database Tools. This option will be suitable for installations where Managers will view, review and approve results.

Raman Package

A full installation, but without IR-specific items. Suitable for Raman analyses where Method Developers will develop methods using a Raman Experiment (.rex) file and analysts will obtain sample data using a Triggered Fiber Optic Probe. Offline Raman analyses, in which all data will be obtained from disk files, are also supported.

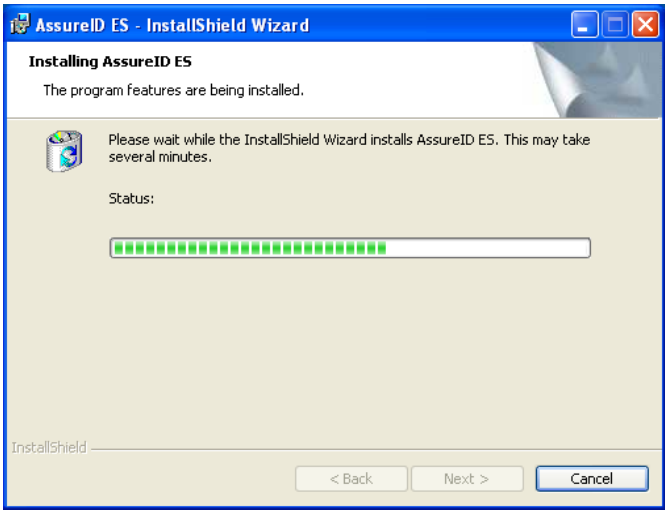
6. Enter the software license number printed on the certificate provided and then click **Next**.

   The Ready to Install page is displayed.

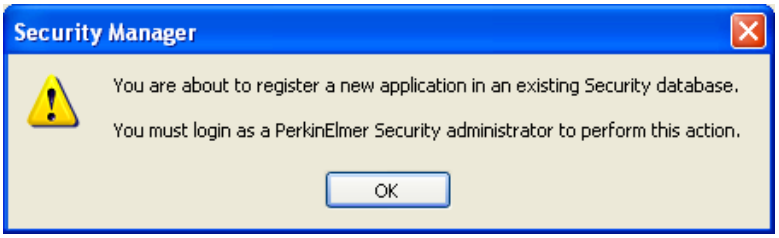


7. Click **Install** to begin installing AssureID.

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



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

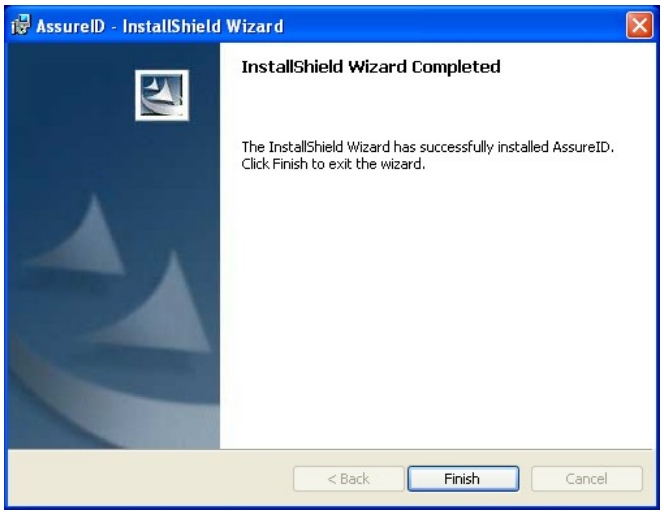


The PerkinElmer Login dialog is displayed.

Log in as a PerkinElmer Software Administrator.

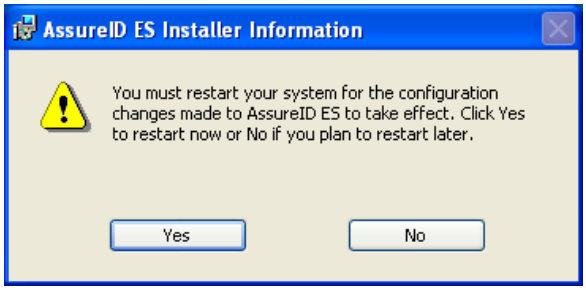
Use the Administrator **User name** and **Password** that you use for the PerkinElmer software that is already installed on the PC.

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



8. Click **Finish**.

   The restart dialog is displayed. You now have to restart your PC.



9. Click **Yes** to restart your PC immediately, or **No** if you want to restart your PC later.

   The installation is now complete.

Migrating from Earlier Versions of AssureID

Security Manager Database

The Security Manager database schema has changed since AssureID version 1.0 and cannot be used with AssureID version 4 or later. A new database must be created when installing AssureID 4.x.

NOTE: The user names of Analysts and Developers are recorded in the method and results databases and do not rely on the Security Manager database for reference.

The Security Manager database schema has also been changed since AssureID 2.x. However, this database can be used directly with AssureID 4.x. Use **Register Database** in Database Tools if you would like to use your AssureID 2.x Security Manager database. The AssureID 2.x database will be automatically updated the first time it is accessed by AssureID 4.x.

AssureID Databases

The AssureID method and result database schemas have changed since AssureID version 1.0. AssureID 1.0 databases can be migrated to AssureID 4.x using **Migrate Database** in Database Tools.

For further information on how to use Database Tools, see *Using Database Tools* on page 28.

Logging in to AssureID for the First Time

During the installation of AssureID a number of user names are created automatically, as follows.

Logins for AssureID ES

The default passwords for the five default user groups in AssureID ES are the same as the name of the group in lower case, as follows:

Login Name	Password	Group Membership
Administrator	administrator	Administrators
Developer	developer	Developers
Approver	Approver	Approvers
Analyst	Analyst	Analysts
Supervisor	supervisor	Supervisors

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

Further information about these groups is given in *Pre-defined groups in AssureID ES* on page 35.

NOTE: We recommend that you immediately create a second Administration level login for emergency use in case of a problem with the primary Administrator.

Logins for AssureID (Standard)

The default passwords and Group membership for the two default users in AssureID are as follows:

Login Name	Password	Group Membership
Administrator	administrator	Administrators
Analyst	analyst	Users

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

Further information about these groups is given in *Pre-defined groups in the Standard version of AssureID* on page 36.

NOTE: We recommend that you immediately create a second Administration level login for emergency use in case of a problem with the primary Administrator.

AssureID Windows Administration

Overview

Someone trained as a Windows Administrator should control the PC that the AssureID is installed on. They will be responsible for all Windows user/password settings; and in the Enhanced Security version they will also be responsible for 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.

  It is possible for users to login to AssureID using their Windows User Name and Password instead of having a separate AssureID User Name and Password. See *Setting up Windows Login* on page 31 for further information about setting this up.

In the Enhanced Security version of AssureID, they should also:

- Ensure that appropriate backup procedures are in place for data files and databases, as discussed in *File and Database Backups* on page 21.
- Manage the PKIUsers group. For details, see *Administering the PKIUsers Group* on page 23.
- Ensure that users only have access to folders and files that they need access to. This includes network drives.
- 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 (by using the security features in NTFS) files in the file locations where data is saved.
- 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.

File and Database Backups

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

- C:\ProgramData\PerkinElmer\AssureID (Windows 7 and 8 and 10) – This folder contains the database of methods and the database of analysis results.

- C:\ProgramData\PerkinElmer\Security System (Windows 7 and 8 and 10) – This folder contains the database of users.

- C:\Program Files (x86)\PerkinElmer\AssureID\Workflow Templates (Windows 7 and 8 and 10) – This folder contains sub-folders that hold files required to run the analysis workflows.

Windows Login Security

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

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

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

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

Default Windows Groups and Accounts

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

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

NOTE: It is recommended that the 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. This could be a way for an unauthorized person to access the system, if the default accounts are left unchanged (see *Appendix 2: Administering the PerkinElmer Security Server Windows User Account* on page 92).

Administering the PKIUsers Group

The Windows user group PKIUsers is created by AssureID during installation. This group is used to set permissions on files, folders and registry entries for AssureID to work correctly. All users of AssureID must be members of the PKIUsers group on their local PC.

NOTE: If the AssureID login type is set to Windows Login, users may also need to be made members of a separate Windows Login group. See *Setting up Windows Login* on page 31.

The PKIUsers group initially contains the global user, “Everyone”. However, to provide security, the Windows Administrator should identify the individual Windows users who are to be allowed to use AssureID, add them to this group, and then remove “Everyone”.

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

1. Log in to the PC as a Windows Administrator.
2. On the **Control Panel**, select **Administrative Tools** > **Computer Management** (Windows 7 and 8).
   The Computer Management dialog is displayed.
3. In the left-hand panel, click **Local Users and Groups**.
4. In the right-hand panel, double-click the **Groups** folder to see the list of available Groups on the PC.
5. Double-click **PKIUsers**.
   The PKIUsers Properties dialog is displayed.
6. To add a user to the Group, click **Add**.
   The Select Users, Computers, or Groups dialog is displayed.

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

   Click **OK**.

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

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

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

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

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

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

Administering PKIUsers When Using AssureID Across a Network

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

NOTE: For further information on using AssureID across a network, see *Sharing the PerkinElmer Security Database Across a Network* on page 27.

File Permissions

Members of the PKIUsers group are given the following permissions for the folders used by AssureID.

Folder	Permissions
C:\ProgramData\PerkinElmer\Security System (Windows 7 and 8 and 10)	Create Files, Create Folders, Read/Write Attributes, No delete.
C:\ProgramData\PerkinElmer\AssureID (Windows 7 and 8 and 10)	Create Files, Create Folders, Read/Write Attributes, No delete.

Folder	Permissions
C:\ProgramData\PerkinElmer\Reference Data (Windows 7 and 8 and 10)	All Permissions

NOTE: All sub-folders automatically inherit these permissions.

Windows Auditing

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

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

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

Login auditing is also available within Windows to monitor access to the system. For example, this may be used to look for failed attempts to log in. Login auditing can be set from the Control Panel by selecting **Audit Policy**.

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, and 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 AssureID 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.

Using Database Tools

There are three types of database used in AssureID:

Method Repositories – Store the methods as set up by the Method Editor and are accessed by the Method Explorer.

Result Stores – Hold the results of analyses and instrument validations completed through the Analyzer and are accessed by the Results Browser.

Security Database – Holds the information required for logins and is accessed by the Administration tools.

The Database Tools utility allows you to manage these databases.

1. Select **Database Tools** from the **AssureID** group in the **PerkinElmer Applications** under **Programs** on the Start menu.
   The Database Tools login dialog is displayed.

2. Enter your **User name** and **Password** and then click **OK**.
   You must be an AssureID Administrator to use Database Tools.
   The Database Tools application is started.

3. Select the required type of database by clicking on the icon in the left panel.
   The list of available databases of that type is displayed. The currently active database is indicated by a tick in a green circle .
   The database tools available depend on the type of database selected.

4. Click the button for the database tool required:

   - **Set Active Database** – Sets the selected database to be the active one.
   - **Compact Database** – Compacts the files to free up disk space.
   - **Create Database** – Creates a new database.
   - **Register Database** – Enables you to connect the PC to a database already in place on a network.
   - **Check Database** – Checks to see if a database has been tampered with or is corrupted.
   - **Migrate Database** – Migrates a database from version 1 of AssureID to work with the current version of the software.
   - **Un-Register Database** – Enables you to remove a database from the list of available databases. The database is not deleted from the hard disk on the PC. You cannot un-register the currently active database.

NOTE: All of the options are available for the Method Repositories and Result Stores. The Security Database only has the **Compact Database** and **Register Database** options.

AssureID Software Administration

Overview

The AssureID Software Administrator has privileges to set up and maintain the security of the AssureID software and, for AssureID ES, ensure technical compliance to 21 CFR Part 11. To do this, the Software Administrator is required to:

- Define how users login to AssureID, see *AssureID Login Types* on page 31.
- Administer the database of users, including adding new users and setting their group assignments. See *Creating New AssureID Users* on page 37 and *Assigning New Users to AssureID Groups* on page 39.

In the Enhanced Security version of AssureID, they should also:

- Define the Signature Points in the software, see *Configuring Electronic Signature Points* on page 40.
- Track the Login History, see *Viewing the Login History* on page 42.
- Track the Audit Trail, see *Viewing the Audit Trail* on page 43.

NOTE: The AssureID 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 AssureID software will automatically have the permissions required to administer any other PerkinElmer applications that have been installed and which use the PerkinElmer Security system.

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

However, although administrators and users are global in nature, groups and instruments assigned to the software are application specific.

AssureID Login Types

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

- PerkinElmer Login

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

- Windows Login

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

- No Passwords Login (AssureID Standard version only)

  This allows users to login to AssureID by selecting their User Name from a drop-down list in the Login dialog. No Password is required.

NOTE: Changing the login type within AssureID will automatically change the login type for all other PerkinElmer software installed on the same PC.

Setting up PerkinElmer Login

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

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

To setup the AssureID users and groups go to *Creating New AssureID Users* on page 37.

Setting up Windows Login

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

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

However, if appropriate, the Windows Administrator can create an alternative group, containing details of users who are to be allowed access using Windows Login. The software will then only allow members of the specified Windows group, who are also members of the PKIUsers group on the local PC, to access AssureID. For further details, see *Administering the PKIUsers Group* on page 23.

NOTE: All members of the Windows Login group must be members of PKIUsers on the local PC.

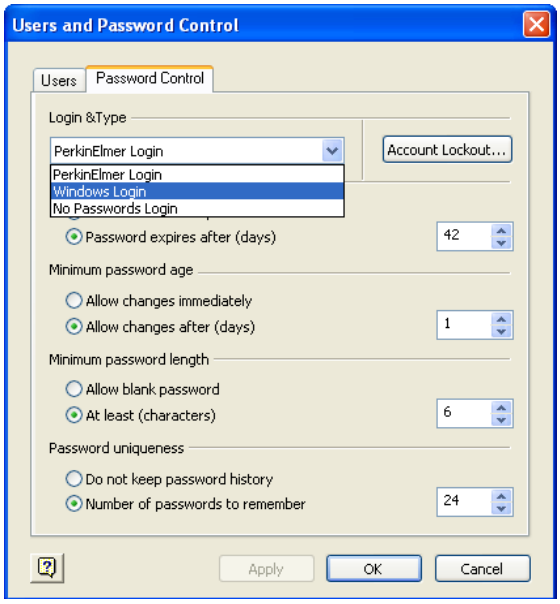
Depending on your company's security policy, you should consider whether to replace the default Windows Administrator account called 21cfr. This account is used by the Windows Login functionality. For a description of how to create a new account and then change the password, see *Appendix 2: Administering the PerkinElmer Security Server Windows User Account* on page 92.

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

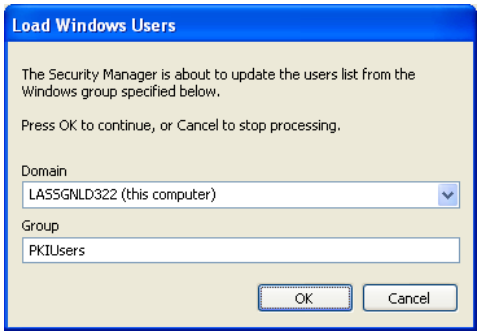
1. From within the Method Explorer, select **Administration** from the Tools menu.
   A sub-menu is displayed.

2. Select **Setup Users and Groups**.
   The dialog opens at the Users tab.

3. On the Password Control tab, change the Login Type to **Windows Login**.

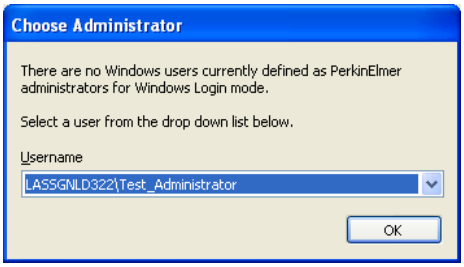


The Load Windows Users dialog is displayed.



4. If appropriate, select the Domain and Group containing the Windows users you want to be able to access the software.
   The default is the PKIUsers group on your local PC.

5. 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. Exit the AssureID 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 AssureID to configure all the other users who need access to the software.

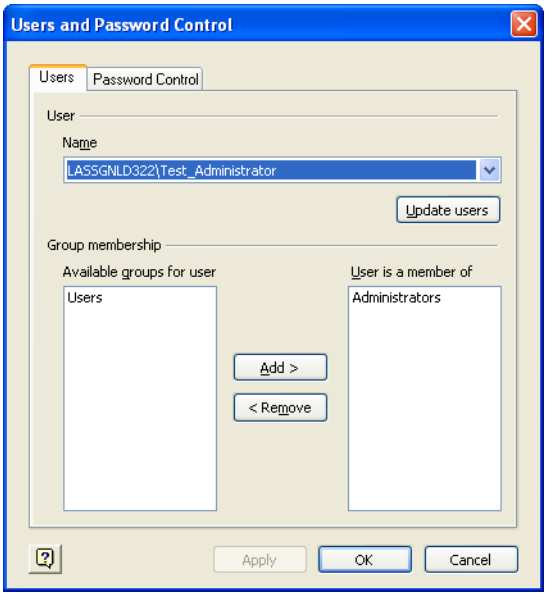
Additionally the administrator does not yet have permission to access instruments from AssureID software.

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

1. Start the AssureID software and log in using the administrator login.

2. From the Tools menu select **Setup Users and Groups**.

   On the Users tab, the Name drop-down contains all the users who are members of the Windows Login 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 AssureID software, including Instrument Access, needs to be a member of the **Users** group. In AssureID 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**.

Users should now have access to AssureID software.

Setting up No Passwords Login (AssureID Standard version only)

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

To set the login type to No Password login:

1. From within the Method Explorer, select Administration from the Tools menu.
   A sub-menu is displayed.
2. Select **Setup Users and Groups**.
   The dialog opens at the Users tab.
3. On the Password Control tab, change the Login Type to **No Passwords Login**.
4. Click **OK**.

Managing Users and Groups

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

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

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

Managing users and groups involves:

- Understanding the pre-defined groups. See *Pre-defined Groups* on page 35 for details.
- Creating new users and assigning them to groups; see *Creating New AssureID Users* on page 37 and *Assigning New Users to AssureID Groups* on page 39.

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

Pre-defined Groups

A number of groups are created automatically during the installation of AssureID or AssureID ES.

Pre-defined groups in AssureID ES

The following groups are pre-defined in AssureID ES: **Administrators**, **Analysts**, **Developers**, **Approvers** and **Supervisors**.

NOTE: It is possible to change the group membership of the default users. By default, the default users are only members of the default group with the same name. For example, the Analyst user is a member of the Analysts groups, and the Developer is a member of the Developers group.

NOTE: It is not possible to modify the Administrator Group permissions.

The following table lists what these groups of users are able to do:

Group	Member of the group is able to:
Administrators	The Administrator is only able to perform Administration tasks. This includes setup new users, create new groups and define signature points.
Analysts	Run methods and view results.
Developers	Read methods, develop methods, delete methods and folders, copy and move methods, configure instruments and accessories, set up and test instrument validation, and perform instrument validation.
Approvers	Read methods, copy and move methods, approve methods, view results and approve results.
Supervisors	Read methods, delete methods and folders, copy and move methods, and view results.

For more information on configuring users and groups see the on-screen help by selecting **Contents and Index** from the Help menu in the AssureID Method Explorer.

Pre-defined groups in the Standard version of AssureID

The following groups are pre-defined in AssureID: Users and Administrators.

The following table lists what these groups of users are able to do:

Group	Member of the group is able to:
Administrators	Administrators are only able to perform Administration tasks. This includes setup new users and passwords.
Users	Users are able to perform all tasks except setup new users and passwords.

For more information on configuring users and groups see the on-screen help by selecting **Contents and Index** from the Help menu in the AssureID Method Explorer.

Creating New AssureID Users

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

For PerkinElmer Login Type

To define new User names and Passwords:

1. From within the Method Explorer, select **Administration** from the Tools menu.
   A sub-menu is displayed.

2. Select **Setup Users and Groups**.
   In the Enhanced Security version of AssureID, the Users, Groups, Password Control and Summary dialog is displayed. In the Standard version of AssureID, 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 repeat the **Password** in the **Confirm password** entry field.
   The Password is case sensitive. It can consist of letters, numbers and single spaces only.

5. Select **Enabled** if you want the user to be able to login or **Disabled** if you do not want them to be able to login at the current time.
   If **Enabled** is selected, select **User must change password at next login** to force the user to change their password when they first log in.
   In the Enhanced Security version of AssureID, **User must change password at next login** is always selected when creating a new user, forcing them to change their password the first time they log in.

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.
   See *Assigning New Users to AssureID Groups* on page 39 for details.

For Windows Login Type

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

NOTE: Before you start, a Windows Administrator must have created the new Windows user and added that user to both the PKIUsers group and, if appropriate, to the group defined for Windows Login users. See *Administering the PKIUsers Group* on page 23 and *Setting up Windows Login* on page 31, for details.

1. Login to Method Explorer as an AssureID Administrator.
2. Select **Administration** from the Tools menu.
   A sub-menu is displayed.
3. Select **Setup Users and Groups**.
   In the Enhanced Security version of AssureID, the Users, Groups, Password Control and Summary dialog is displayed. In the Standard version of AssureID, the Users and Password Control dialog is displayed.
4. Select the Users tab and then click **Update Users**.
   The new user will now be able to login to AssureID.
5. Add the user to a group, to allow access to the software.
   See *Assigning New Users to AssureID Groups* on page 39 for details.

For No Passwords Login Type (AssureID Standard version only)

1. From within the Method Explorer, select **Administration** from the Tools menu.
   A sub-menu is displayed.
2. Select **Setup Users and Groups**.
   In the Enhanced Security version of AssureID, the Users, Groups, Password Control and Summary dialog is displayed. In the Standard version of AssureID, 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** and **Full name**.
5. Select **Enabled** if you want the user to be able to login or **Disabled** if you do not want them to be able to login at the current time.
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.
   See *Assigning New Users to AssureID Groups* on page 39 for details.

Assigning New Users to AssureID Groups

New users must be assigned to one or more AssureID groups. Each group is given access to particular applications and functionality within the AssureID software package, for example Administrators can access Method Explorer but cannot access Analyzer. Within these applications, users are able to perform specific operations such as “Perform instrument validation” or “Develop methods” as defined by the AssureID Administrator. If necessary, a group can be created for each user such that each user has their own specific set of access permissions.

To assign users to AssureID group(s):

1. From within the Method Explorer, select **Administration** from the Tools menu.
   A sub-menu is displayed.
2. Select **Setup Users and Groups**.
   The Users, Groups, Password Control and Summary dialog opens at the Users page.
3. Select the user from the **Name** drop-down list.
4. 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.
5. Click **OK** to close the Users, Groups, Password Control and Summary 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. This Administrator account replaces the default account which is disabled.

NOTE: 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.

Configuring Electronic Signature Points

NOTE: Signature Points are only available in the Enhanced Security version of AssureID.

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

A Signature Point is a point in the software that requires a signature. The Signature Points in AssureID are pre-defined. For example, one Signature Point is Lock Method, so when a method is locked it requires a Signature and a dialog automatically appears. The user has to enter their User name and Password. They may also be able to add additional comments if this option has previously been selected by the Administrator.

The Signature Points within the software are:

Software Area	Signature Point
Method Explorer	Save Instrument Validation
Method Editor	Save Method Lock Method Approve Method
Analyzer	Save Results Save IPV Results
Results Browser	Approve Results

The Administrator is able to define the settings (that is, whether a signature and comments are required) for each Signature Point individually or apply the same settings to all Signature Points.

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

To define the settings for each Signature Point:

1. From within the Method Explorer select **Administration** from the Tools menu and then select **Signature Points** from the sub-menu.

   The Signatures dialog is displayed.

2. Select the Signature Point **Name** from the drop-down list of available names.

3. If a Signature is required for a Signature Point, select **Signature required**.

4. If you want the user to be able to add comments if required, select **Prompt for comments**.

NOTE: Signature required and **Prompt for comments** are independent of each other. It is possible to select a signature point that requires only one or both of these options.

5. Repeat steps 2 to 4 for each Signature Point **Name**.

To define the same settings for each Signature Point:

1. From within the Method Explorer select **Administration** from the Tools menu and then select **Signature Points** from the sub-menu.

   The Signatures dialog is displayed.

2. To define the same settings for all Signature Points, click **Update All**.

   The Update All Signature Points dialog is displayed.

3. Select either **All Points require a signature**, **No Points require a signature**, or **Do not change the current settings**.

   If **Do not change the current settings** is selected, the settings selected for each **Name** will apply.

4. Select either **All Points require a prompt**, **No Points require a prompt**, or **Do not change the current settings**.

   If **Do not change the current settings** is selected, the settings selected for each **Name** will apply.

5. Click **OK**.

   The Update All Signature Points dialog closes and the Signatures dialog is re-displayed.

Viewing the Login History

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

The Login History can only be viewed by users who are members of the Administrators group.

1. From within the Method Explorer select **Administration** from the Tools menu and then select **View Audit Trail** from the sub-menu.

   The Login History and Audit Trail 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 the amount of disk space, but we recommend that all audit trails are regularly reviewed and archived to save disk space.

The Login History can be printed and exported as a comma-separated values (.csv) file, which can be opened, for example, in Microsoft Excel.

Viewing the Audit Trail

NOTE: Audit Trails are only available in the Enhanced Security version of AssureID.

The Administration 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. From within the Method Explorer select **Administration** from the Tools menu and then select **View Audit Trail** from the sub-menu.

   The Login History and Audit Trail 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 comma-separated values (.csv) file, which can be opened, for example, in Microsoft Excel.

An Overview of AssureID

Overview of AssureID

AssureID is a PerkinElmer software package that compares spectra against reference data to check the acceptability of materials. Qualitative and quantitative analyses can be performed.

For IR analyses, the AssureID software suite can be used with Frontier IR Systems, Spectrum Two, Spectrum 400 Series, Spectrum 100 Series, Spectrum One and Spectrum One NTS spectrometers; see *Using AssureID with FT-MIR and FT-NIR Instruments* on page 49 for details.

For Raman analyses, the AssureID software suite can be used in conjunction with a Raman Fiber Optic Probe. See *Using AssureID with a Raman Triggered Fiber Optic Probe* on page 50.

Offline working, for both Raman and IR analyses, is also supported, allowing spectra (both sample and reference spectra) to be imported from files; see *Using AssureID Without an Instrument* on page 51.

Starting AssureID Applications

There are five AssureID applications. These are Method Explorer, Method Editor, Analyzer, Results Browser and Database Tools. Method Editor is started from Method Explorer. The applications available will depend on the type of installation. For example, if you have the full installation all the applications will be available, but if you have the Results Browser installer you will only have the Method Explorer, Results Browser and Database Tools applications.

Using PerkinElmer Login

1. To start an AssureID application, from the Start menu select **Programs**, **PerkinElmer Applications** and then the relevant application from the **AssureID** group.

   The PerkinElmer Login dialog is displayed.

2. Enter your **User name** and **Password** as set up by the AssureID Administrator.

   See *Logins for AssureID ES* , and *Logins for AssureID (Standard)* on page 18 for details.

3. Click **OK**.

   If you have appropriate permissions assigned to you (Enhanced Security version of AssureID only), the software will start.

Using Windows Login

NOTE: You can only start AssureID applications using the Windows Login if this Login Type has been specified by the AssureID Administrator. For more information, see *Setting up Windows Login* on page 31.

1. From the Start menu select **PerkinElmer Applications**, then select **AssureID**, and then select the required application.

   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** or **Local PC (this computer)** from the **Log on to** drop-down list.

   By default, the Domain last 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**.

Using No Passwords Login (AssureID Standard version only)

1. From the Start menu select **Programs**, **PerkinElmer Applications** and then the relevant application from the **AssureID** group.

   The PerkinElmer Login dialog is displayed.

2. Select your **User name** from the drop-down list.

3. Click **OK**.

Using AssureID with FT-MIR and FT-NIR Instruments

When you use the AssureID software as part of a system which has an FT-MIR or FT-NIR instrument (or a dual-range instrument) attached, you specify the type of instrument and any accessory when you create a method using the AssureID Method Explorer New Method Wizard.

You then configure the instrument and any associated accessory; and specify the instrument validation required.

Once a method has been created, the AssureID Method Editor is used to build the method.

This will include:

- Defining instrument settings.
- Using the instrument to collect spectra of materials that will be used to test the identity of unknown samples subsequently supplied for analysis. Spectra of materials can also be imported from disk, if required.
- Using the instrument to collect spectra of validation samples that can be used to test the model. Spectra of validation samples can also be imported from disk, if required.
- Defining the Analysis Workflow.

When a method is run using the AssureID Analyzer, the Analysis Workflow determines the activities that must be carried out. Typically, these will include:

- Performing instrument background scans.
- Carrying out system suitability checks.

Then, for each sample:

- Entering sample details.
- Preparing the sample.
- Obtaining sample spectra.
- Analyzing results and reporting.

Using AssureID with a Raman Triggered Fiber Optic Probe

AssureID can be used to carry out data acquisition and analysis of samples using a Raman Triggered Fiber Optic Probe, with the appropriate instrument settings obtained from a .rex (Raman Experiment) file created using the Spectrum software and referenced as part of the method.

To do this, you should select the **Generic Raman** instrument type option, together with a Trigger Probe as an accessory, when you create a method using the AssureID Method Explorer New Method Wizard.

Once a method has been created, the AssureID Method Editor is used to build the method.

This will include:

- Importing spectra of materials that will be used to test the identity of unknown samples subsequently supplied for analysis.
- Importing spectra of validation samples that can be used to test the model.
- Defining the Analysis Workflow, including specifying the .rex file that contains the required Raman instrument settings.

NOTE: If you are using the Enhanced Security (ES) version of AssureID, you should consider storing the .rex files you create for use with AssureID in a read-only folder.

When a method is run using the AssureID Analyzer, the Analysis Workflow determines the activities that must be carried out. Typically, for each sample, these will include:

- Entering sample details.
- Using the probe to acquire a sample spectrum.
- Analyzing results and reporting.

NOTE: For full details of how to use a triggered fiber optic probe, refer to the *Raman Triggered Fiber Optic Probe* leaflet (L1321887).

Using AssureID Without an Instrument

AssureID can be used to carry out analysis of existing sample spectra, held on disk, without the use of an instrument. To do this, you specify a Generic instrument type when you create a method using the AssureID Method Explorer New Method Wizard.

NOTE: When you create a Generic MIR or Generic NIR method, you are given the option of selecting an accessory (Shuttle, HATR or UATR in the case of Generic MIR; NIRA in the case of Generic NIR). Any accessory selection you make here implies the accessory used when the sample data was acquired.

When you create a Generic Raman method, you are given the option of selecting a Trigger Probe as an accessory. Selecting the Trigger Probe accessory creates a method in which sample data will be acquired using a probe, rather than read from disk files. See *Using AssureID with a Raman Triggered Fiber Optic Probe* on page 50.

Once a method has been created, the AssureID Method Editor is used to build the method.

This will include:

- Importing spectra of materials that will be used to test the identity of unknown samples subsequently supplied for analysis.
- Importing spectra of validation samples that can be used to test the model.
- Defining the Analysis Workflow.

When a method is run using the AssureID Analyzer, the Analysis Workflow determines the activities that must be carried out. Typically, for each sample, these will include:

- Importing the sample spectrum, from disk.
- Analyzing results and reporting.

Offline and Online Working

AssureID allows spectra, both sample and reference data, to be obtained in two ways:

- Online – collecting spectra from an instrument attached to the PC running the AssureID software.
- Offline – importing spectral data from a file.

The way in which you obtain data will depend upon:

- Your license type – some licenses allow both collection and import of data; others only permit data to be imported.
- Where your license allows both offline and online working, that is both collection and import, the instrument type selected on the New Method Wizard defines how you will obtain data. In particular, a range of Generic instrument options have been provided specifically to enable offline working, with all data imported from files.

NOTE: For UV, only a Generic instrument type is provided. For Raman, a Generic instrument type is provided; but if a Trigger Probe is selected as an accessory, the probe can be used to acquire sample spectra using AssureID Analyzer. See *Using AssureID with a Raman Triggered Fiber Optic Probe* on page 50.

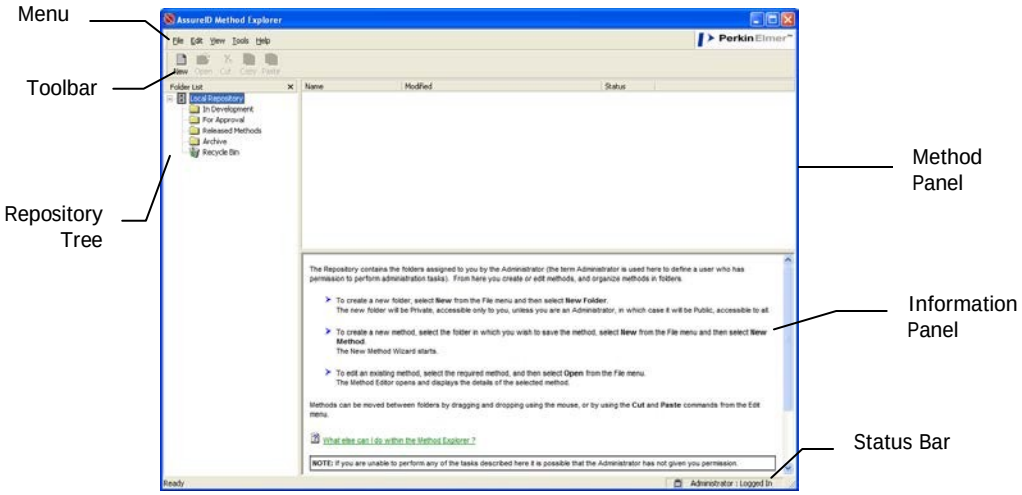
When working with an AssureID method created for a Generic instrument type, the following activities are not relevant and will not be included in the method:

- Defining instrument settings.
- System suitability checks.
- Collection of data (only Import options will be provided in the method).

Method Explorer

The AssureID Method Explorer is used for managing folders and methods. The Repository holds your folders, which in turn contain your methods. The folders you see are determined by your Login, which is defined by the Software Administrator (Enhanced Security version only).

The Method Explorer screen is divided into six areas:



- The menus give you access to the commands available from the Method Explorer, including the ability to create a new method, select and configure the instrument to be used, and set up the validation tests.
- The toolbar enables quick access to certain commands.
- The Repository Tree gives you access to the different folders of methods.
- The Method Panel lists the methods in the selected folder on the Repository Tree. Clicking on a method selects it and it can then be edited using the Method Editor as discussed on page 75.
- The Information Panel shows a description of the current folder or the description saved when a selected method was created. It can also give information about what you should do next and may contain links to the help file.
- The Status Bar displays context sensitive messages and shows who is currently logged into the system.

Creating a New Method

NOTE: If you are using AssureID ES you must have **Develop methods** permission. If you are using the standard version of AssureID you must be logged in with User group permissions. In both AssureID and AssureID ES it is not possible for the Administrator to create methods.

1. Highlight the folder in the Repository Tree where you want the new method to be saved once it has been created.

2. Select **New** and then **New Method** from the File menu.

   The New Method Wizard is displayed.

3. Work through the wizard, making selections as required and then clicking **Next** to move to the following page.

   When the wizard finishes the Method Editor starts with the new method loaded, which includes default instrument and pre-processing settings selected based on the information you provided.

Configuring an Instrument

Before collecting spectra you must add and configure an instrument. If there is only one instrument of a particular type available, this will be selected as the default instrument. However, if there is more than one instrument of the same type available (for example, over the network), you must select the required instrument and set it as the default instrument for data collection.

NOTE: This function is only relevant if you are using an FT-MIR or FT-NIR spectrometer.

NOTE: If you are using AssureID ES you must have **Configure instruments and accessories** permission. If you are using the standard version of AssureID you must be logged in as a member of the User group. In both AssureID and AssureID ES it is not possible for the Administrator to configure instruments.

Selecting an Instrument

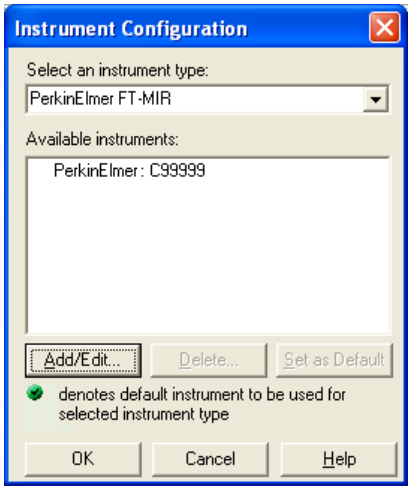
To select which instrument to use when collecting spectra:

1. From within the Method Explorer, select **Configure Instruments and Accessories** from the Tools menu.

   A sub-menu is displayed.

2. Select **Configure Instruments**.

   The Instrument Configuration dialog is displayed.



3. Select the instrument type from the drop-down list.

   The options are mid-infrared (FT-MIR) and near-infrared (FT-NIR) instruments. The list of **Available instruments** is updated for the selected instrument type.

4. Select the instrument to be the default and then click **Set as Default**.

   If only one instrument is listed, it is automatically set as the default. If more than one instrument is listed, the first instrument in the list is automatically set as the default. If the first instrument you added was a dual-range spectrometer, this will be the default for both FT-MIR and FT-NIR. A check mark in a green circle is displayed next to the default instrument.

5. Click **OK** to close the dialog.

   The selected default instrument will be used when collecting spectra.

Adding an Instrument

For a particular instrument type you may have access to several instruments across a network but you may want the user to only have access to one (or a restricted number) of these. Having the list of **Available instruments** within the Instrument Configuration dialog ensures that only the instruments you want to make available are actually available for use during method development.

To add an instrument to the list of available instruments:

1. From within the Method Explorer, select **Configure Instruments and Accessories** from the Tools menu.

   A sub-menu is displayed.

2. Select **Configure Instruments**.

   The Instrument Configuration dialog is displayed.

3. Click **Add/Edit**.

   The Instrument Install Wizard is displayed.

4. Select the **New Instrument** option and then click **Next**.

   The Instrument Details page is displayed.

5. Enter the **Instrument Name**.

   This may be any name to distinguish your instrument.

6. 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 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.

   The installation procedure for a Spectrum Two instrument continues at step 11.

7. When the Open dialog is displayed, insert the Instrument Configuration Disk that was shipped with the new instrument.

8. Navigate to the correct drive and then highlight the configuration file.

9. Click **Open**.

   When the files have been copied from the disk, **Completed** is displayed at the bottom of the page.

10. Click **Next**.

    The Test the performance of your instrument page is displayed.

11. Click **Skip** if you do not want to test the performance of the instrument now, or click **Next** if you want to continue with the tests.

    The Test Instrument Performance page is displayed. The performance tests start automatically. The result of each test is indicated as **Passed** or **Failed**.

12. When the tests are complete, click **Next**.

    The Collect ASTM Reference Spectra page is displayed.

13. Click **Skip** if you do not want to collect the spectra now, or click **Next** if you want to continue and collect the ASTM spectra.

    The Collecting ASTM Reference Spectra page is displayed. The collection starts automatically. This data is stored as reference spectra at C:\ProgramData\PerkinElmer\ Reference Data (Windows 7 and 8 and 10) to be used when ASTM validation tests are performed. The outcome is indicated as **Passed** or **Failed**.

14. When the collection is complete, click **Next**.

    The Install Accessories page is displayed.

15. Click **Skip** if you do not want to install any accessories now, or click **Next** if you want to continue with the accessory installation.

    The Testing your accessory page is displayed. The tests start automatically. The result of each test is indicated as **Passed** or **Failed**. If any of the tests fail, you cannot proceed.

16. When the tests are complete, click **Another Accessory** to install another accessory.

17. Click **Next** when you do not want to install any more accessories.

    The Finish page is displayed.

18. Click **Finish**.

    The Instrument Install Wizard closes and the new instrument is added to the list of available instruments.

    If you have added an FT-MIR/NIR dual-range spectrometer, it adds to both mid-infrared (FT-MIR) and near-infrared (FT-NIR) instrument types. If you have added an FT-MIR/FIR dual-range spectrometer, only a mid-infrared (FT-MIR) instrument type is added.

Deleting an Instrument

To delete an available instrument:

1. From within the Method Explorer, select **Configure Instruments and Accessories** from the Tools menu.

   A sub-menu is displayed.

2. Select **Configure Instruments**.

   The Instrument Configuration dialog is displayed.

3. Select the instrument from the list of Available instruments and then click **Delete**.

   You are asked to confirm the deletion.

4. Click **Yes**.

   The instrument is removed from the list of Available instruments.

Configuring an Accessory

Before collecting spectra you must install and test any accessories. This option should be used if you purchase a new accessory after installing the instrument.

NOTE: This function is only relevant if you are using an FT-MIR or FT-NIR instrument.

NOTE: To configure accessories you must have **Configure instruments and accessories** permission as set on the Groups tab of the Users, Groups, Password Control and Summary dialog.

1. From within the Method Explorer, select **Configure Instruments and Accessories** from the Tools menu.

   A sub-menu is displayed.

2. Select **Configure Accessories**.

3. If you have configured more than one instrument, use the drop-down list to select which instrument you would like to add the accessory to, and then click **OK**.

   The Instrument Install Wizard is displayed.

4. Click **Next**.

   The Instrument Install Wizard performs tests against all currently configured instruments.

5. Click **Another Accessory** if you want to install a new accessory.

6. Click **Next** if you do not want to install any more accessories.

   The Finish page is displayed.

7. Click **Finish**.

   The Instrument Install Wizard closes.

Setting up Instrument Validation

NOTE: If you are using AssureID ES you must have **Setup and test instrument validations** permission. If you are using the standard version of AssureID you must be logged in as a member of the User group. In both AssureID and AssureID ES it is not possible for the Administrator to setup and test instrument validations.

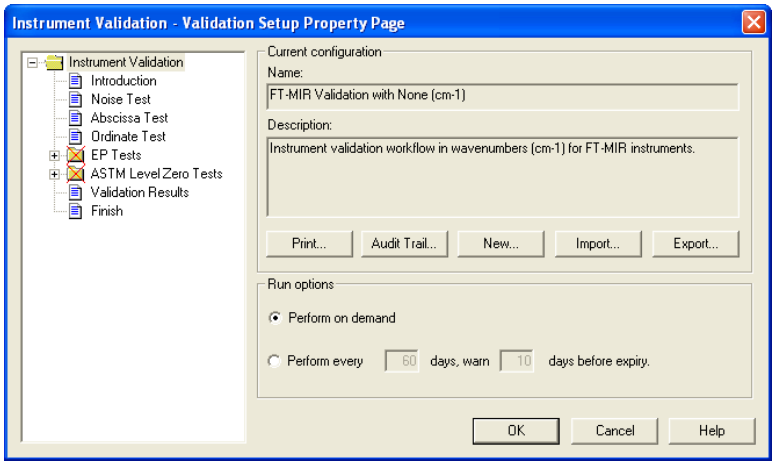
You need to set up the Validation workflow that will run when the Analyst clicks **Validate** on the Analysis page of the AssureID Analyzer, as shown on page 77.

NOTE: This function is only relevant if you are using an FT-MIR or FT-NIR instrument.

1. From the Tools menu within Method Explorer select **Instrument Validation**, and select **Setup**, then select the required validation setup or a **New Validation**.

2. If New Validation is selected, select the required template and then click **Open**.

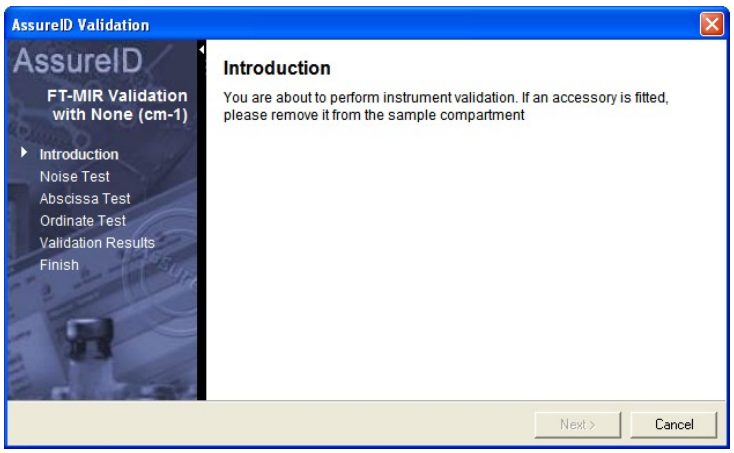
   The Validation Setup Property Page is displayed and the setup can be edited.



Once you have set up an instrument validation workflow you can test it from within the Method Explorer. This runs the validation workflow without saving any results in the Results database.

➢ From the Tools menu, select **Instrument Validation**, then **Test**, and select the required validation setup.

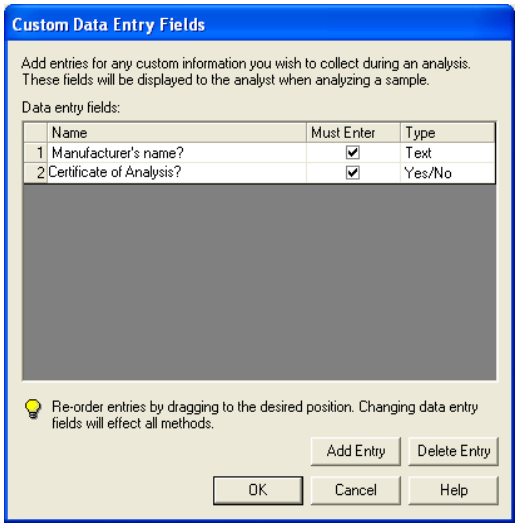
The validation workflow will run just as the Analyst will see it, but without saving the results.



Custom Fields

Analysis Options on the Tools menu enables the Developer to define custom fields that the Analyst will see as part of the Analysis Workflow. A custom field is a data entry field that is specific to your analysis requirements. For example, you may want the manufacturer's name to be included in the information saved when a sample is analyzed.

To do this, you create a custom field that requires the manufacturer's name to be entered.



There are two types of custom fields available:

- A text field – For example, to enter the manufacturer's name.
- Yes/No selector – For example, for the Analyst to say whether the sample has a Certificate of Analysis (COA).

The information entered in the custom field(s) is stored along with the result of the analysis and can be viewed using the Results Browser.

Printing a Method or Validation Audit Trail

It is not possible to export a Method Audit Trail or a Validation Audit Trail. Instead, the Audit Trail needs to be printed to a file. This is achieved by installing and selecting a suitable printer which should be selected from the Printer Setup icon in the Audit Trail window.

There are two possible methods for doing this:

- Printing to a generic text file.
- Printing to an Adobe PDF file.

Printing to a generic text file (txt format)

This is a driver which can be installed to the system from Windows. Printing from the audit trail window or the Print dialog to the generic text printer requests the user to enter a name for the file and will produce a text file in the \Program Files\PerkinElmer\AssureID or \ProgramFiles (x86)\PerkinElmer\AssureID folder. This text file can be opened in WordPad or a similar text program.

Printing to an Adobe file (PDF format)

Adobe Acrobat must be installed on your PC to be able to print a pdf file. When the printer is selected, the user is requested to enter a name and can also change the folder for the pdf file. The file can also be secured from modification at this stage. The file can be opened using Acrobat Reader which is freely available from the Adobe website or the Software Utilities CD.

Collecting Reference Spectra

AssureID requires the following reference spectra for setting up instrument validation and system suitability within methods:

Instrument Validation

NOTE: This function is only relevant if you are using an FT-MIR or FT-NIR instrument.

- ASTM MIR (%T) – Transmission for FT-MIR instrument test.
- ASTM NIR (%T) – Transmission for FT-NIR instrument test.
- ASTM NIR (%R) – Reflectance for use with the NIRA.
- USP Linearity – Set of reflectance spectra collected in Absorbance.

System Suitability

NOTE: This function is not relevant for Generic methods, developed for use without an instrument.

- Contamination and Throughput Check – This is a reference background for the accessory used in the method.

- Control Check – This is a spectrum of a designated material specifically for a particular method.

To collect a reference spectrum:

1. From within the Method Explorer, select **Instrument Validation** from the Tools menu.
   A sub-menu is displayed.

2. Select **Collect Reference Spectra**.
   The Reference Data Settings dialog is displayed. This displays the current instrument settings.

3. Click **Change Settings**.
   The Instrument Settings Properties dialog is displayed.

4. Change the instrument settings to those described below for your required reference spectrum, and then click **OK**.
   The instrument settings are updated to reflect the new values, and the Instrument Settings Properties dialog closes.

5. Click **Collect**.
   The Collect Reference Spectra dialog is displayed. A background spectrum is automatically collected. The **Scan Sample** and **Monitor** buttons remain grayed until the background spectrum has been collected.

6. Click **Save As**.
   The Save Reference Spectra dialog is displayed. The default folder is C:\ProgramData\PerkinElmer\Reference Data (Windows 7 and 8 and 10).

7. Navigate to the required folder if you do not want to save the background spectrum in the default location.

8. Click **Save**.
   The background spectrum is saved.

9. Enter the **Sample ID** and any **Comment**.
   The Comment will be saved with the spectrum.
   If a polystyrene reference is required, select the **Use APV Polystyrene** checkbox. This instructs the system to use the polystyrene sample in the instrument filterwheel.

NOTE: If your spectrometer does not have a filterwheel, the **Use APV Polystyrene** checkbox is not displayed. If you want to use a polystyrene sample, you should insert a polystyrene reference card in the sample area.

10. Click **Scan Sample**.
    A progress bar is displayed during scanning.
    When the spectrum has been collected it is displayed in the graph window of the dialog.

11. Click **Save As**.
    The Save Reference Spectra dialog is displayed.

12. Navigate to the required folder if you do not want to save the spectrum in the default location.

13. Click **Save**.
    The reference spectrum is saved.

ASTM MIR

The ASTM E1421 Level Zero Tests are intended for an open beam instrument.

➢ Use the following settings to collect the spectra listed below:
Scan Range – At least 4050 to 150 cm^{-1}
Resolution – 4 cm^{-1}
Number of Scans – 5
Scan Speed – 0.2 cm/s
Ensure CO_2/H_2O Suppression is switched off
It is assumed that all other settings are default.

Spectra required:

- An energy reference spectrum (named as, for example, ASTM E1421 Energy Reference.sp). This is a single beam or background spectrum generated under the above conditions.

- A polystyrene reference spectrum (named as, for example, ASTM E1421 Polystyrene Reference.sp). This is a sample spectrum generated under the above conditions with polystyrene in the beam.

The polystyrene spectrum may either be the polystyrene in the filter wheel (APV), if your instrument has one, or a card in the sample area.

Both (APV and sample area) may be recorded initially but when the ASTM test is set up in AssureID validation then the particular reference polystyrene spectrum must be stored. It is an important requirement of the ASTM test that the same sample is measured each time in the same orientation as when the reference spectrum was recorded from that same sample.

ASTM NIR in Transmission

The ASTM E1944 Level Zero Tests in transmission are intended for an open beam instrument.

➢ Use the following settings to collect the spectra listed below:
Scan Range – At least 12550 to 3950 cm^{-1}
Resolution – 4 cm^{-1}
Number of Scans – 5
Scan Speed – 0.2 cm/s
Ensure CO_2/H_2O Suppression is switched off
It is assumed that all other settings are default.

Spectra required:

- An energy reference spectrum (named as, for example, ASTM E1944 Energy Reference.sp).

- A reference material spectrum (named as, for example, ASTM E1944 Check Sample Reference.sp).

The check sample (reference) material specified by ASTM E 1944 is not specific (unlike ASTM E 1421 which specifically requires polystyrene), and recommends that it meets certain documented criteria. The polystyrene (1.2 mm thick) in the filter wheel (APV), or the polystyrene (1.2 mm) sample card can be used for the test.

ASTM NIR in Reflectance

The ASTM E1944 Level Zero Tests in reflectance are used for FT-NIR or FT-IR/NIR dual-range spectrometers fitted with a NIRA.

➢ Use the following settings to collect the spectra listed below:
Scan Range – At least 12550 to 3950 cm^{-1}
Resolution – 4 cm^{-1}
Number of Scans – 26 (equivalent to approximately 30 seconds)
Scan Speed – 1.0 cm/s
Ensure CO_2/H_2O Suppression is switched off
It is assumed that all other settings are default.

Spectra required:

- An energy reference spectrum (named as, for example, ASTM E1944 NIRA Energy Reference.sp) collected using the open beam.

- A reference material spectrum (named as, for example, ASTM E1944 NIRA Check Sample.sp) collected using the sample area.

The check sample (reference) material specified by ASTM E1944 is not specific (unlike ASTM E1421 which specifically requires polystyrene), and recommends that it meets certain documented criteria. A suitable reflectance material is required, for example NIST SRM 1920.

NOTE: The internal polystyrene sample in the filter wheel is not really suitable for this test but it is currently selected by default in the ASTM for FT-NIR and dual-range instruments with a NIRA fitted.

USP Linearity Spectra

The USP Linearity check (USP <1119> Vol 24, No 4) needs reference spectra collecting for the reflectance standards. The USP tests as a whole are conducted in absorbance.

These reference spectra must be collected with the NIRA fitted.

- Use the following settings to collect the spectra listed below:
  Ordinate Units – Absorbance
  Scan Range – 10000 to 4000 cm^{-1}
  Resolution – 16 cm^{-1}
  Number of Scans – 30
  Scan Speed – 1.0 cm/s
  It is assumed that all other settings are default.

One spectrum for each reflectance standard is required. These spectra are then imported into the USP Linearity test properties.

At run time, similar spectra are collected from the same reference reflectance samples and a plot of the observed absorbance against the stored reference absorbance is calculated to obtain the slope and intercept.

System Suitability Contamination and Throughput

NOTE: This function is not relevant for Generic methods, developed for use without an instrument.

The Contamination and Throughput Checks require a stored reference background spectrum to compare against during the System Suitability Checks.

The System Suitability Workflow settings for Contamination and Throughput Checks in an AssureID method will require a specific reference background for the accessory (and top plate) collected under the same instrument settings defined within the particular AssureID method.

System Suitability Control Check

NOTE: This function is not relevant for Generic methods, developed for use without an instrument.

The Control Check requires a reference spectrum of a known sample. The same sample is used at run-time, where a spectrum is collected and compared (using the Compare function) against the reference spectrum of that particular sample.

This System Suitability Control Check Reference Spectrum must be collected using the same instrument settings defined within the particular AssureID method.

Adjustments Toolbox

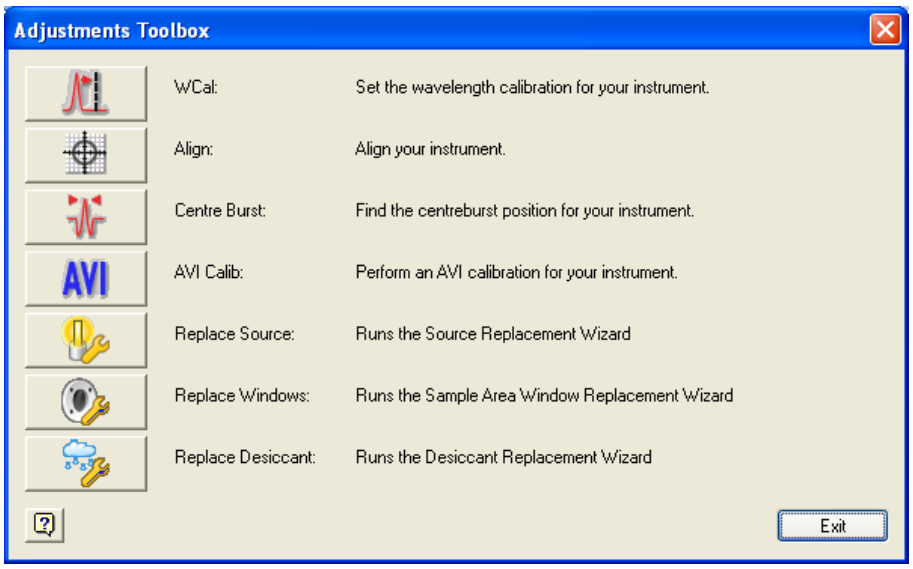
The Adjustments Toolbox enables access to the instrument adjustment commands.

NOTE: This function is only relevant if you are using an FT-MIR or FT-NIR instrument.

NOTE: To access the Adjustments Toolbox in the Enhanced Security version of AssureID, you must have **Configure instruments and accessories** permission as set on the Groups tab of the Users, Groups, Password Control and Summary dialog. To access the Adjustments Toolbox in the Standard version of AssureID, you must be logged in as a member of the User group.

1. From the Tools menu in the Method Explorer, select **Configure Instruments and Accessories**, and then select **Adjustments Toolbox**.

   The Adjustments Toolbox is displayed.



2. Click on the tool for the adjustment you want to make.

   A dialog will appear or the adjustment will be implemented, depending on the tool selected.

NOTE: The options available will depend upon your instrument type, and any accessories being used.

3. When you have finished making adjustments, click **Exit**.

   The Adjustments Toolbox closes.

Maintenance

The Maintenance dialog enables you to set and record desiccant change dates and routine service periods.

NOTE: This function is only relevant if you are using an FT-MIR or FT-NIR instrument.

The dialog enables you to:

- View the date of the last desiccant change or routine service.
- Set the interval for the desiccant and service warning messages to appear.
- Acknowledge that the desiccant has been changed or that a routine service has been performed.

To use this dialog:

1. From the Tools menu in the Method Explorer, select **ConfigureInstruments and Accessories**, and then select **Adjustments Toolbox**.
   The Adjustments Toolbox is displayed.
2. Click  .
   The Maintenance dialog is displayed.
3. Make the changes required.
   Click in the box,  , to set that the desiccant has been **Changed** or that the instrument has been **Serviced**.
4. Click **OK**.
   The changes are applied and the Maintenance dialog closes.

Wavenumber Calibration

A wavenumber shift may be observed as a result of sample effects. When the wavenumber calibration is re-defined, care should be taken when comparing spectra with previously-collected spectra or library spectra or performing instrument validation. Wavenumber calibration is controlled by the value of the stored laser wavenumber. You can adjust the calibration by up to 0.1% of the nominal laser value by entering expected and observed wavenumbers for a reference peak.

Changing the laser wavenumber only affects the interpolation of data collected subsequently. You cannot make the laser wavenumber different for sample and background spectra.

For information on when to recalibrate your instrument see the User's Guide supplied with your spectrometer. These are provided, in .PDF format, on the *IR & Raman Manuals CD* (part number L1050002).

NOTE: This function is only relevant if you are using an FT-MIR or FT-NIR instrument.

1. From the Tools menu in the Method Explorer, select **Configure Instruments and Accessories**, and then select **Adjustments Toolbox**.
   The Adjustments Toolbox is displayed.

2. Click  .
   The Wavenumber Calibration dialog is displayed.

3. Select **Calibrate from known band**.

4. Enter the expected position of a band in cm^{-1} in the **Expected position** text box.
   We recommend the reference band at 5669.3 cm^{-1} in the polystyrene spectrum.

5. Enter the observed position of that band in cm^{-1} in the **Observed position** text box.

6. Click **OK**.
   If the correction to the laser wavenumber correction is greater than 0.1% (this is very unlikely) the following error message is displayed:
   Delta is too big
   In this case we recommend that you make sure that the positions of the bands entered in the **Observed position** and **Expected position** text boxes are correct.
   If a correction to the laser wavenumber greater than 0.1% is required, we recommend that you:

   - Select **Set laser wavenumber** and then reset the laser by clicking **Reset** and then **OK**.
   - Repeat the calibration using your standard.

   If a correction greater than 0.1% is still required, we recommend that you contact your local PerkinElmer Service Department.

7. Choose **OK**.
   The laser wavenumber in the instrument is reset.

Aligning the Instrument

Alignment is the adjustment of the interferometer mirror angles to optimize the amplitude of the interferogram centerburst. This is achieved by maximizing the energy of the region of the interferogram around the centerburst.

The Align function aligns one mirror in the interferometer to achieve this.

NOTE: This function is only relevant if you are using an FT-MIR or FT-NIR instrument.

1. Make sure that the sample compartment is empty.

2. From the Tools menu in the Method Explorer, select **Configure Instruments and Accessories**, and then select **Adjustments Toolbox**.
   The Adjustments Toolbox is displayed.

3. Click  .
   Alignment of the instrument begins.

4. To stop the alignment, click **Cancel**.

5. When alignment is complete, click **OK**.
   The Instrument Alignment dialog closes.

NOTE: If significant absorption occurs in the sample area, the beam energy reaching the detector may not be sufficient to enable alignment. During alignment, do not disturb the instrument by, for example, obstructing the infrared beam in the sample compartment.

Relocating the Centerburst

The Relocate Centerburst function is used to find the position of the scanning mirrors in the interferometer such that there is zero path difference between the two beams when they recombine. In this position the infrared radiation interferes constructively at all wavelengths, so the amplitude of the interferogram is at its maximum.

Relocate Centerburst is implemented automatically as part of the initialization process.

NOTE: This function is only relevant if you are using an FT-MIR or FT-NIR instrument.

To manually relocate the centerburst after initialization:

1. From the Tools menu in the Method Explorer, select **ConfigureInstruments and Accessories**, and then select **Adjustments Toolbox**.
   The Adjustments Toolbox is displayed.

2. Click  .
   The centerburst is relocated.

3. To stop the process before completion, click **Cancel**.

4. Click **OK**.
   The Finding Centreburst dialog closes.

Instrument Display

The Instrument Display adjustment is only available when you are connected to Frontier IR Systems, Spectrum 400 Series, or Spectrum 100 Series spectrometers. It enables you to adjust the brightness and contrast of the instrument display.

To use the Instrument Display tool:

1. From the Tools menu in the Method Explorer, select **Configure Instrumentsand Accessories**, and then select **Adjustments Toolbox**.
   The Adjustments Toolbox is displayed.

2. Click  .
   The Display Settings dialog is displayed.

3. Adjust the **Brightness** and **Contrast** to suit your working environment, and then click **OK**.
   The Display Settings dialog closes.

Fiber Probe Display

The Fiber Probe Display adjustment is only available when you are using a spectrometer with an Triggered Fiber Optic Probe accessory connected. It enables you to adjust the brightness and contrast of the Fiber Probe display.

NOTE: This function is only relevant if you are using an FT-NIR instrument.

To use the Fiber Probe Display tool:

1. From the Tools menu in the Method Explorer, select **Configure Instruments and Accessories**, and then select **Adjustments Toolbox**.
   The Adjustments Toolbox is displayed.

2. Click  .
   The Display Settings dialog is displayed.

3. Adjust the **Brightness** and **Contrast** to suit your working environment, and then click **OK**.
   The Display Settings dialog closes.

AVI Calibration

AVI calibration is a routine that takes a spectrum of a methane standard, and calculates the correction needed for the current sampling configuration.

NOTE: This function is not relevant for Generic methods, developed for use without an instrument.

NOTE: You cannot perform an AVI calibration if you are using a spectrometer with an accessory fitted in the sample area.

1. From the Tools menu in the Method Explorer, select **Configure Instruments and Accessories**, and then select **Adjustments Toolbox**.
   The Adjustments Toolbox is displayed.

2. Click 

.
   The AVI calibration routine begins.

3. Make sure that the sample area is clear and nothing is blocking the beam, then click **OK**.

NOTE: If your instrument has a filterwheel with a methane cell, this is used as the reference sample.

If your instrument does not have a filterwheel, or if the filterwheel does not have a methane cell, you are prompted to insert one in the sample area by the software. Click **Continue** to start the calibration.

At the end of the calibration a confirmation message is displayed.

4. Click **OK**.

You can now use AVI correction for this instrument configuration.

Replace Source

The Replace Source wizard guides you through the process of changing your spectrometer source.

NOTE: This function is only relevant for Spectrum Two instruments.

1. From the Tools menu in the Method Explorer, select **Configure Instruments and Accessories**, and then select **Adjustments Toolbox**.

   The Adjustments Toolbox is displayed.

2. Click  .

   The Replace Source wizard starts.

For further information on the Replace Source wizard, see the *Spectrum Two User's Guide* (L1050228).

Replace Windows

The Replace Windows wizard guides you through the process of changing your spectrometer windows.

NOTE: This function is only relevant for Spectrum Two instruments.

1. From the Tools menu in the Method Explorer, select **Configure Instruments and Accessories**, and then select **Adjustments Toolbox**.

   The Adjustments Toolbox is displayed.

2. Click  .

   The Replace Windows wizard starts.

For further information on the Replace Windows wizard, see the *Spectrum Two User's Guide* (L1050228).

Replace Desiccant

The Replace Desiccant wizard guides you through the process of changing the desiccant packs in your spectrometer.

NOTE: This function is only relevant for Spectrum Two instruments.

1. From the Tools menu in the Method Explorer, select **Configure Instruments and Accessories**, and then select **Adjustments Toolbox**.
   The Adjustments Toolbox is displayed.
2. Click  .
   The Replace Desiccant wizard starts.

For further information on the Replace Desiccant wizard, see the *Spectrum Two User's Guide* (L1050228).

NIRA II Corrections

If you have a NIRA II accessory installed in your instrument, there will be two further options in the Adjustments Toolbox:

	Reference Correction	Standardize a reference material for the NIRA II accessory.
	Stray Light Correction	Correct for any stray light in the NIRA II accessory.

These options run wizards to collect spectra and apply the corrections. Refer to the *NIRA II User's Guide* (L1050086) for further information.

Quant Import

The legacy Spectrum Quant+ and Spectrum Beer's Law applications do not form part of the 21 CFR Part 11 compliant PerkinElmer software. It is therefore likely that they are not installed on the same PC as AssureID. To use methods from these applications in AssureID, you will have to export the method from the Quant PC as a zip file, and then import the method onto the AssureID PC.

Exporting the Quant Method

The Quant Method is exported as a zip file. It is then unzipped when it is imported.

1. From the Start menu select **PerkinElmer Applications** and then select **Quant Export**.
   The Quant Transfer Utility dialog is displayed.
2. Select the Methods Directory that contains the Method you want to export.
3. Select the **Quant type** from the drop-down list.
   The list of available Methods is displayed.

4. Highlight the Method(s) to be exported.
5. Select the **Destination Path** for the zipped method(s).
6. Click **Next**.
   The Methods are zipped and exported to the selected folder.
7. Click **Exit** to close the Quant Transfer Utility dialog.
8. Copy the zipped files from the Quant PC to the AssureID PC.

Importing the Quant Method

1. From the Tools menu in the Method Explorer, select **Administration** and then select **Quant Import**.
   The Quant Import dialog is displayed.
2. Click **Add Zipfile to List**.
3. Select the zip files to be extracted.
   The file extension is .qmz.
4. Click **Next**.
   The zip files are extracted.
5. View the Log file to determine where the files have been extracted to.
6. Click **Exit** to close the Quant Import dialog.
   The Quant Methods are now available to be imported into AssureID.

NOTE: This procedure is not required when using quantitative methods generated in Spectrum Quant which use Beer's Law, PLS or PCR algorithms. These methods can be imported into AssureID directly.

Legacy File Converter

NOTE: Legacy File Converter is only available in AssureID ES.

21 CFR Part 11 technical compliance mandates very high levels of data integrity and security. To ensure that AssureID 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 Administration tools. This allows users to add a data security checksum to all spectra in a folder 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. Select **Legacy File Converter** from the Administration sub-menu under the Tools menu within the Method Explorer.

   The Legacy File Converter is displayed.

2. For the Source Path, click **Browse** and on the file selector displayed, select the **Source Path** for the folder containing the legacy data.

   The default path is C:\Users*<your Windows user name>*\CheckSumInput (Windows 7 and 8 and 10).

3. For the **Destination Path**, click **Browse** and on the file selector displayed, select the Destination Path for the folder containing the converted data.

   The default path is C:\Users*<your Windows user name>*\CheckSumOutput (Windows 7 and 8 and 10).

4. Click **Next**.

   The data is copied and a checksum is added to each file, then the new files are written to the destination folder, leaving the original data untouched. The default text _cs is appended to each filename.

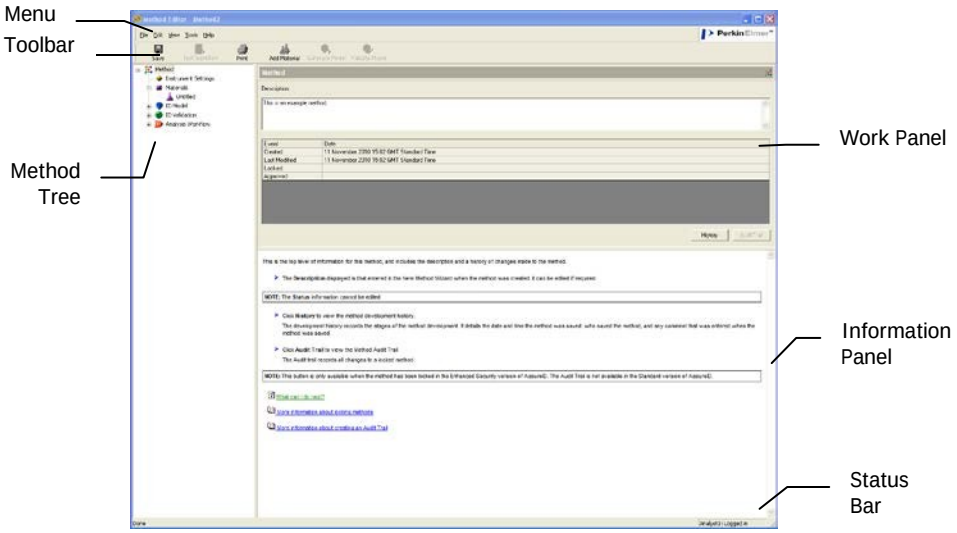
5. To view information about the conversion, click **View Log**.

   A log file is displayed.

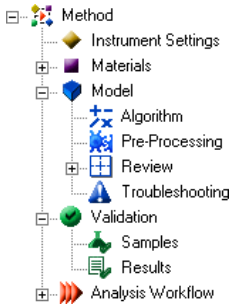
Method Editor

The AssureID Method Editor is used to edit your methods including changing the instrument settings, adding materials and sample spectra to define the materials, setting the algorithm and pre-processing parameters, reviewing the model, troubleshooting any problems, validating the model, and setting up the workflow.

The Method Editor screen is divided into six areas:



- The menus give you access to the commands available from the Method Editor.
- The toolbar enables quick access to certain commands.
- The Method Tree gives you access to the different aspects of a method as shown below.



- The Work Panel displays the details for the selected step on the Method Tree and enables you to set up the method as required.
- The Information Panel shows information about the selected step. It can also give information about what you should do next and may contain links to the help file.
- The Status Bar displays context sensitive messages and shows who is currently logged into the system.

Editing a Method

To edit a method:

1. Select the required step from the Method Tree.
   The Work Panel displays the information for that step.

2. Edit the details as required.
   Information to help you is displayed in the Information Panel.

When you have finished editing the method, select **Save** from the File menu to save the method under the same name and overwrite the previous version, or select **Save As** from the File menu and save the method under a new name.

Locking and Approving Methods

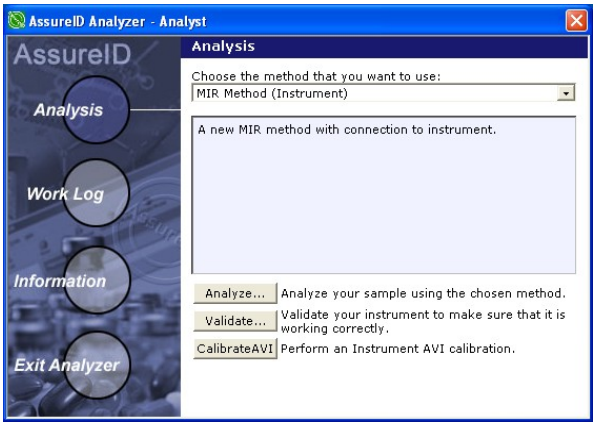
Personnel with the appropriate levels of access to the system can lock methods to prevent editing and can sign methods off as approved before they are released to analysts.

These options are found on the Tools menu.

NOTE: Approving methods is only available in AssureID ES.

Analyzer

The Analyst (or any person who has permission to run methods) will use the AssureID Analyzer to analyze samples and, in the Enhanced Security version of AssureID, to sign off their results.



The **Analysis** part of the Analyzer can be used to run sample analyses, validate the instrument to make sure that it is working correctly (where appropriate) and perform an AVI Calibration (again, where appropriate).

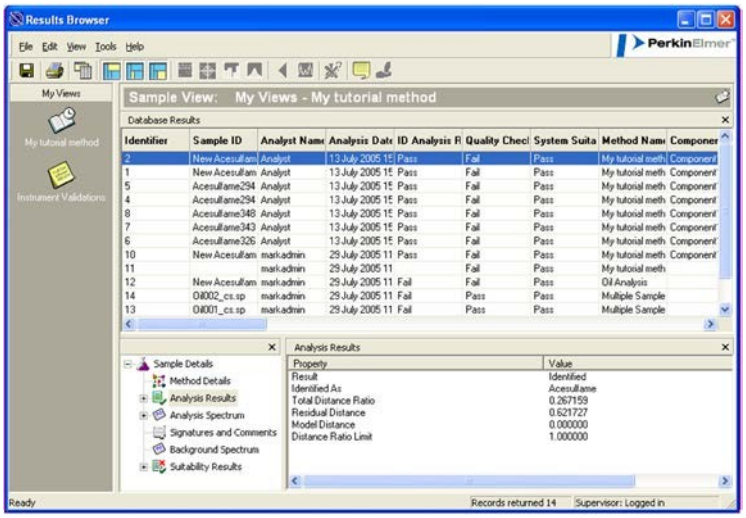
When performing a sample analysis, the Analyst selects the correct method from the list of available methods and then clicks **Analyze** and follows the Analysis Workflow that has been previously defined by the Developer. The steps and messages that the Analyst will see are set by the Developer in the Analysis Workflow section of the Method Tree in AssureID Method Editor. As part of the Analysis Workflow, after the sample has been analyzed, the Analyst is able to view the spectrum, and view and print the report of the analysis.

You can also **Validate** the instrument. You will be informed if the instrument needs validating before the next analysis can be performed. In the Enhanced Security version of AssureID, when the results of any analyses or validations have been signed they are saved to the results database and can be accessed by users with permission to access the Results Browser. In the Standard version of AssureID, the results of analyses and validations are directly saved to the results database and are available in the Results Browser.

To perform an Absolute Virtual Instrument (AVI) calibration, click **Calibrate AVI**. The AVI calibration routine involves collecting a spectrum of the methane in the cell in the filterwheel, and then calculating the correction needed for the current sampling configuration.

NOTE: If your instrument does not have a filterwheel, or if the filterwheel does not have a methane cell, you are prompted to insert one in the sample area by the software. Click **Continue** to start the calibration.

Results Browser



The AssureID Results Browser is used to investigate and manage the results generated from the AssureID Analyzer.

All sample analysis results and instrument validation results are stored in a database. The Results Browser provides the means to investigate and manage these results.

The Results Browser is used in two ways; the Sample Analysis View and the Instrument Validation View. The selected view is generated by using the Query Editor dialog to specify the requirements to use when searching the results database.

Approving Results

NOTE: It is only possible to approve results in AssureID ES.

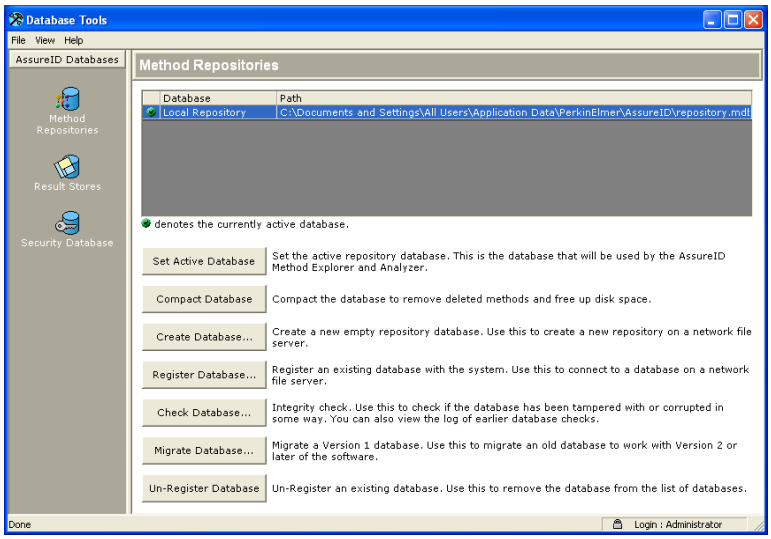
Only users who are members of groups who have the permission to **Approve results** are able to approve results in the Results Browser.

1. Select the result from the Results Table that you want to approve.
2. From the Tools menu select **Approve**.
   The Add Approver Signature dialog is displayed as specified by the Signature Point settings. See *Configuring Electronic Signature Points* on page 40.
3. Enter your **User name** and **Password**.
4. Enter any **Comment** you want saved with the file.
5. Click **OK**.
   The approval is stored

NOTE: It is possible for more than one person to approve a result.

Database Tools

The AssureID Database Tools is used to manage the databases which store the methods, the results and the security information. The databases are listed in the **AssureID Databases** pane.

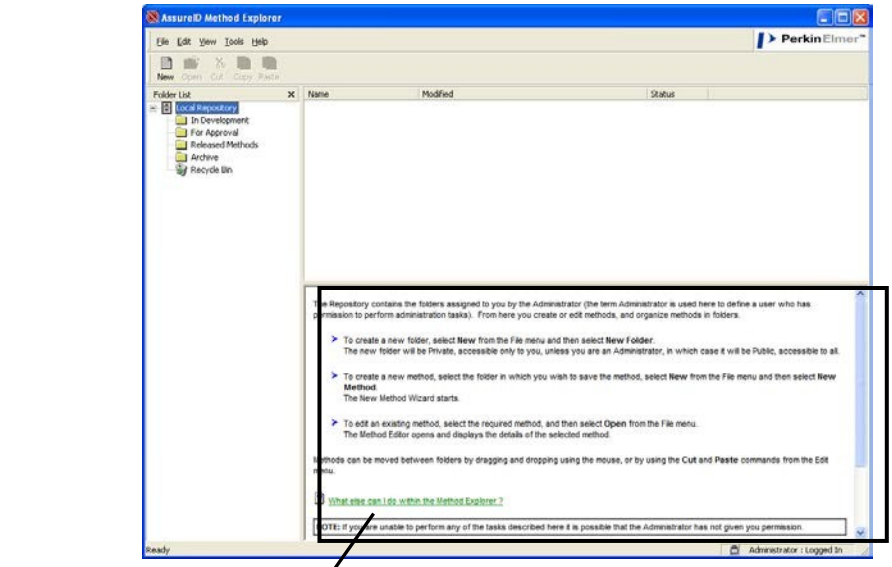


NOTE: You must be logged in as an Administrator to use Database Tools.

For more information see *Using Database Tools* on page 28, and the on-screen Database Tools Help.

Information Panel

Both the Method Explorer and the Method Editor use an Information Panel to provide extra information to help you work with the AssureID software.



The Information Panel displays three types of information:

- Information to help you work with the currently displayed screen is shown at the top of the panel.
- Information to help you decide what to do next is available as hidden text viewed by clicking on What can I do next ? . The text will be displayed and can be hidden by clicking on the link again.
- Further background information relevant to the task at hand is displayed from the on-screen help by clicking a link called **More information**, for example.
  More information about Analysis Workflows .

Appendices

Appendix 1: Configuring TCP/IP Communication

TCP/IP is the communications protocol used by Frontier IR Systems, Spectrum Two, Spectrum 400 Series and Spectrum 100 Series spectrometers 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.

Before you Start (Spectrum Two only)

If you are using AssureID with Spectrum software and the Spectrum software was installed for use with a Spectrum Two instrument, TCP/IP configuration will have been carried out automatically during installation. No further action is required.

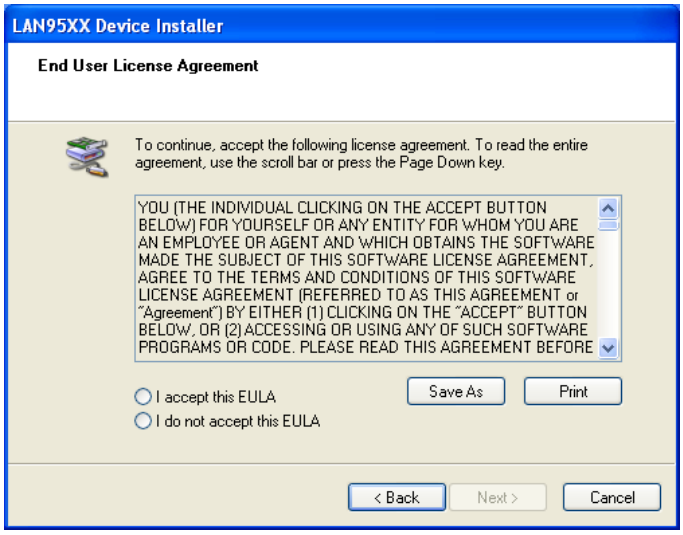
However, if you are using AssureID as standalone software, without Spectrum, or if Spectrum software was installed for use with another type of instrument, a Frontier IR spectrometer for example, you should follow the steps below **before** you configure TCP/IP.

1. Navigate to the folder C:\Program Files\PerkinElmer\ServiceIR\LAN9500 or C:\Program Files (x86)\PerkinElmer\ServiceIR\LAN9500, as applicable.

2. Double-click **install.exe**

   The LAN95XX Device Installer starts.

3. Click **Next**.
   The LAN95XX Device End User Licence Agreement page is displayed.



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

5. Click **Finish**.

6. Connect your Spectrum Two to the PC, using the USB cable supplied with the instrument.

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

8. Click **Network Connections**.
   The Network Connections dialog is displayed.

9. Right-click on **PerkinElmer Spectrum Two** and then select **Properties**.

You can now configure TCP/IP communications for use with your Spectrum Two.

TCP / IP Configuration Procedure

To configure the TCP/IP settings for your PC:

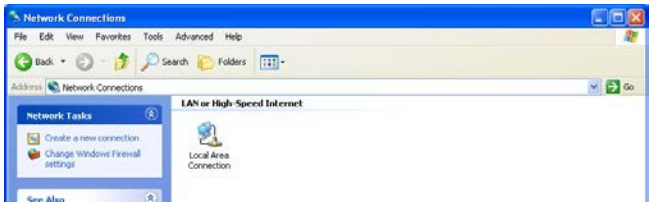
1. For Windows 7, from the Start menu, select **Settings** and then **Control Panel**.
   For Windows 8, right-click at the bottom of the Start screen to display the Apps toolbar, and click the All Apps icon to display the Apps. For Windows 8.1, click the down arrow on the Start screen to display the Apps. Double-click the Control Panel icon in the **Windows System** group.
   The Control Panel dialog is displayed.

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

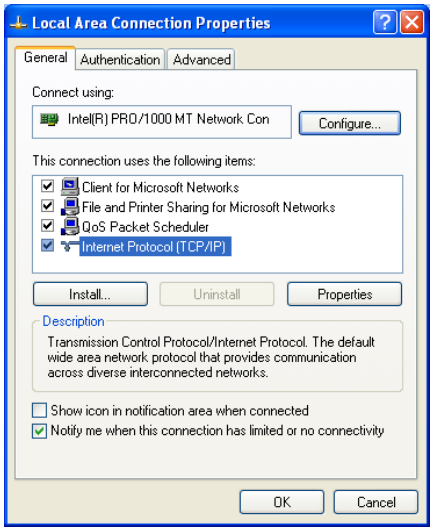
   OR

   For Windows 10, right click "**Start**" button, from the prompted menu, select **Network Connections**. Settings dialog is displayed. Click "**Change adapter options**".

   The Network Connections dialog is displayed.



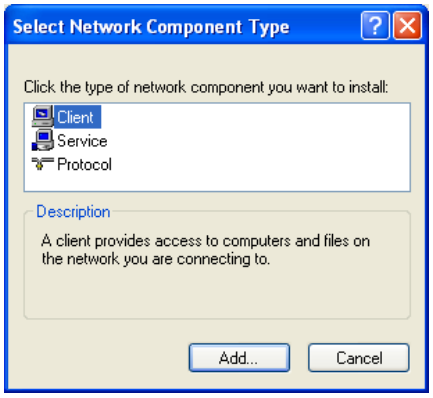
3. Select the Local Area Connection you want to use, right-click and then select **Properties**.
   The Local Area Connecton Properties dialog is displayed.



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

5. If **Internet Protocol (TCP/IP)** or **Internet Protocol (TCP/IPv4)** is not listed on the dialog, click **Install**.

   The Select Network Component Type dialog is displayed.



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

   The Select Network Protocol dialog is displayed.

7. Select **Internet Protocol (TCP/IP)** and then click **OK**.

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

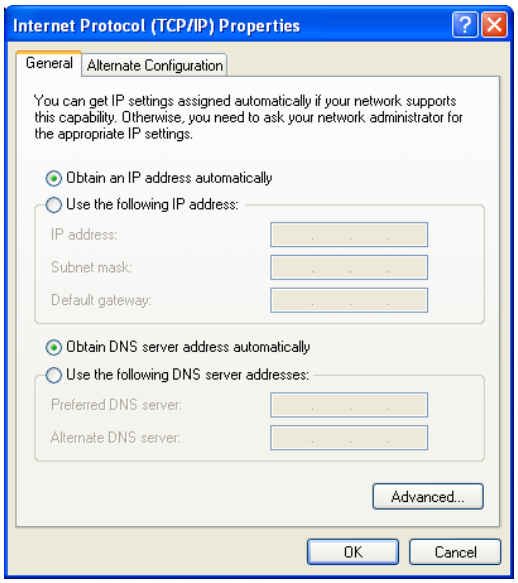
8. For Windows 7 and 8 and 10, select **Internet Protocol Transfer 4 (TCP/IPv4)** and then click **Properties**.

   The Internet Protocol Version 4 (TCP/IPv4) Properties dialog is displayed.

   OR

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

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



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

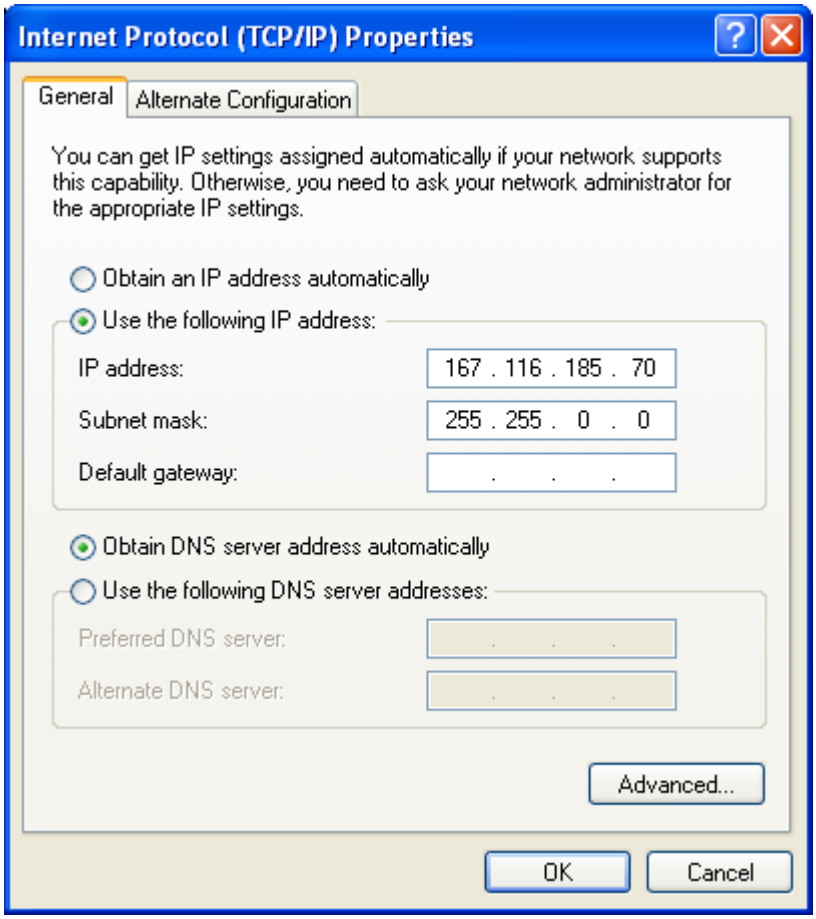
10. Enter the IP address and Subnet mask.

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

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

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

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



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

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

Changing the IP Address of your Instrument

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

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

If you are unable to connect to your Spectrum Two instrument because you do not know the IP address, refer to the Spectrum Two Support website:
www.perkinelmer.com/SpectrumTwoSupport

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

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

If you have not yet installed the instrument

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

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

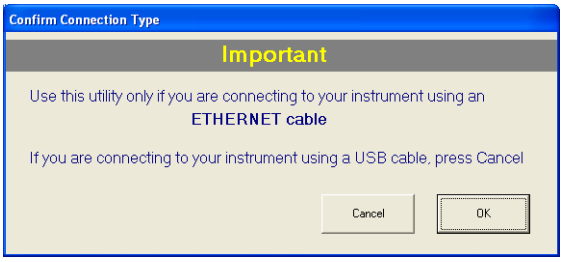
2. Connect the instrument to mains power and turn it on.

   For details of how to connect up your FT-IR spectrometer, refer to the User's Guide supplied with your instrument.

NOTE: The PC's TCP/IP address must be compatible with the instrument's IP address so that you can connect to the instrument. Refer to *TCP/IP Configuration Procedure* on page 84.

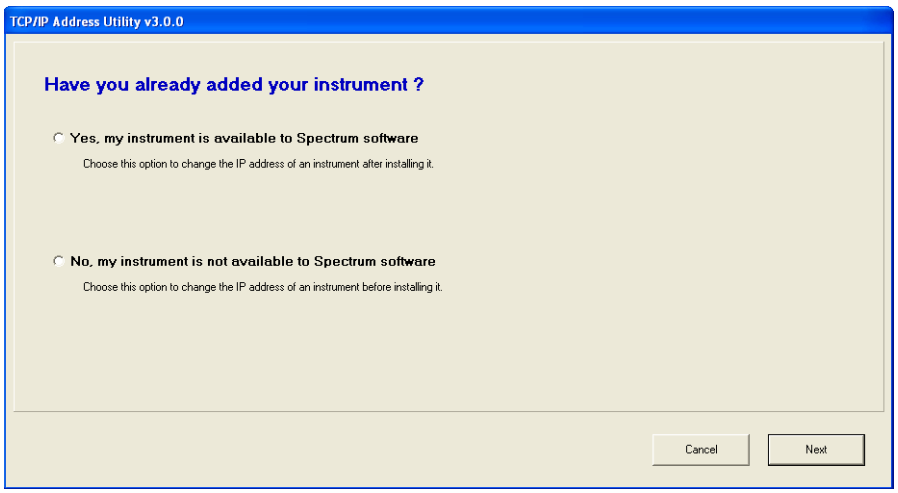
3. Open Windows Explorer and double-click the **Set IP Address** shortcut, which is found in the C:\Program Files\PerkinElmer\ServiceIR or C:\Program Files (x86)\PerkinElmer\ServiceIR directory.

   The Confirm Connection Type dialog is displayed.

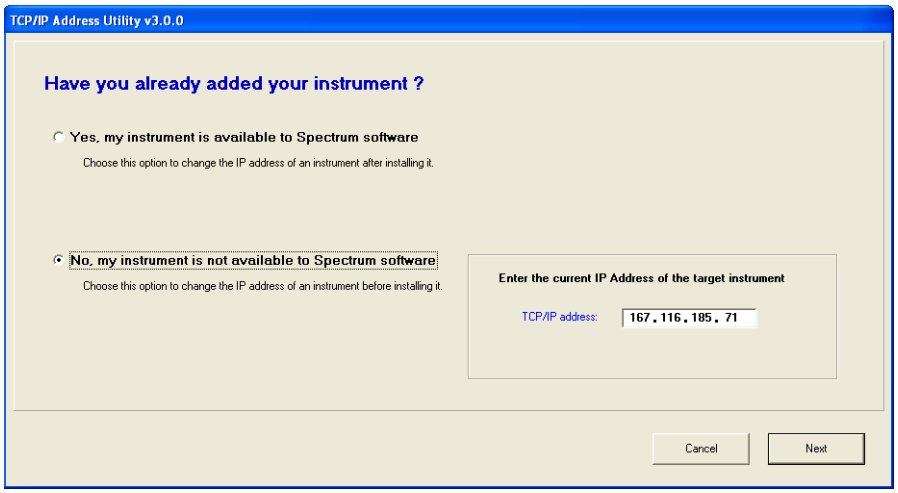


4. Ensure that you are connected using an Ethernet cable, and then click **OK**.

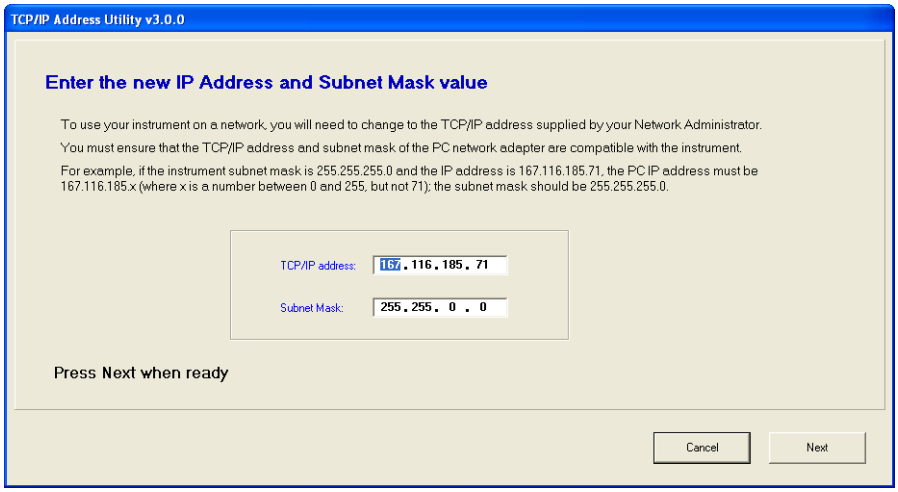
   The Set IP Address program starts.



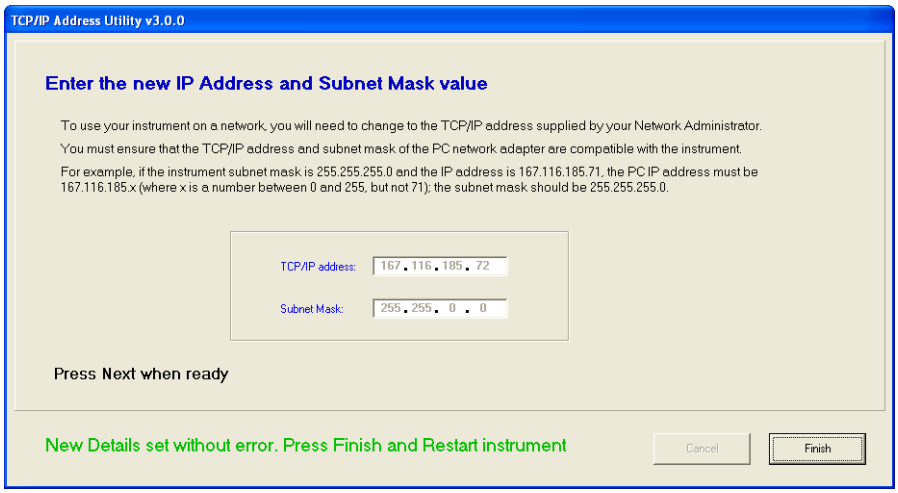
5. Select **No, my instrument is not available to Spectrum software**.
   The dialog updates to show the factory default IP address for instruments.



6. Enter the current IP address for the instrument and then click **Next**.
   The Enter the new IP Address and Subnet Mask value dialog is displayed. Refer to the instructions on the dialog.



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



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

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

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

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

The instrument will not be recognized by AssureID until it has been installed, in either AssureID or Spectrum.

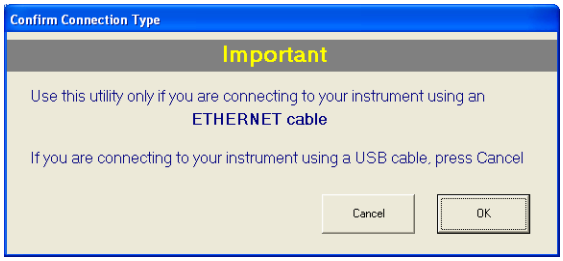
If you have already installed the instrument

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

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

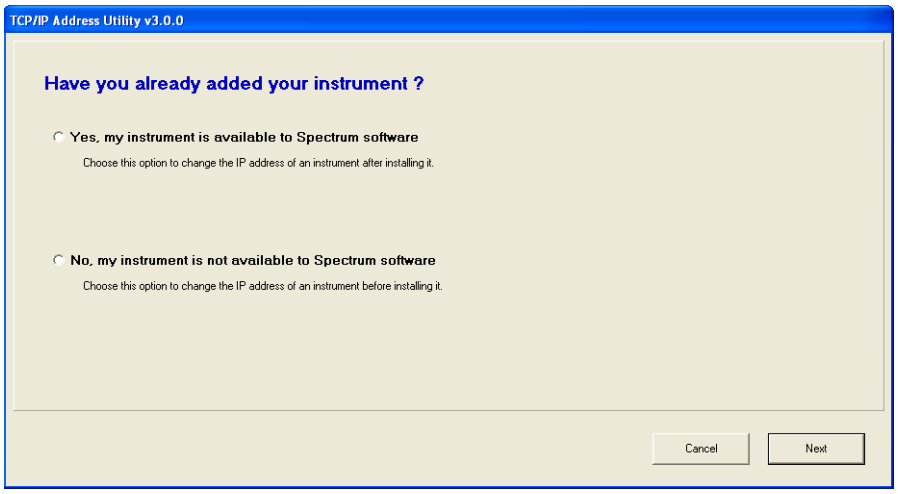
3. Open Windows Explorer and double-click the **Set IP Address** shortcut, which is found in the C:\Program Files\PerkinElmer\ServiceIR or C:\Program Files (x86)\PerkinElmer\ServiceIR directory.

   The Confirm Connection Type dialog is displayed.



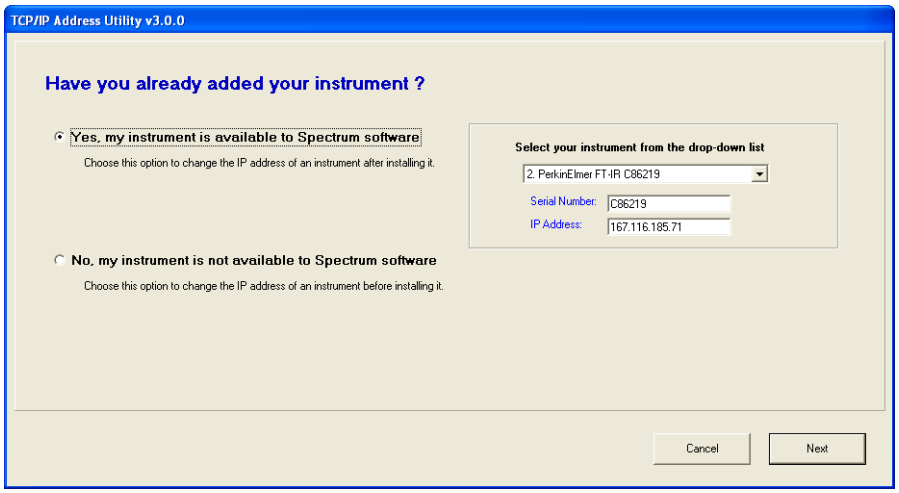
4. Ensure that you are connected using an Ethernet cable, and then click **OK**.

   The Set IP Address program starts.



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

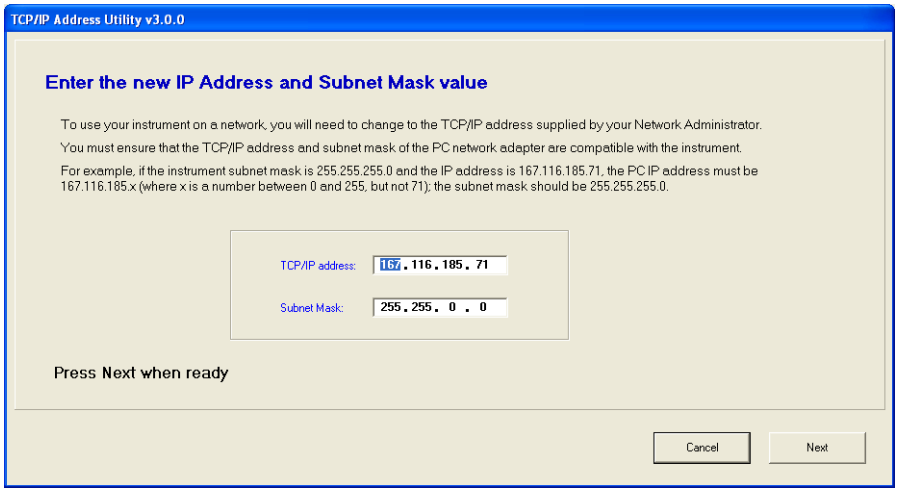
   The dialog updates to display a drop-down list of instruments installed in Spectrum software. The Serial Number and current IP Address for the currently selected instrument are also displayed.



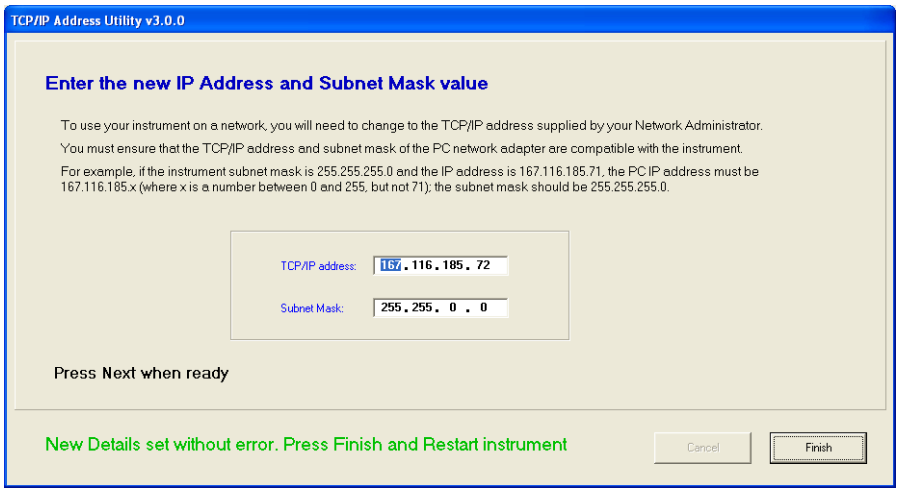
6. Select the instrument you connected to in step 1 from the drop-down list.
   The Serial Number and current IP Address of the instrument are displayed.

7. Click **Next**.

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



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



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

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

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

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

Appendix 2: 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 set up 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 AssureID security system. The 21cfr account will then be disabled.

4. Browse to the program C:\Program Files\PerkinElmer\PE21CFR\config21cfr.exe or C:\Program Files (x86)\PerkinElmer\PE21CFR\config21cfr.exe.

5. If your computer is using Windows XP, double-click the file to run the program.

   OR

   If your computer is using Windows 7 and 8 and 10, right-click the file and select **Run as administrator**.

   This provides the elevated permission level required to run the program in Windows 7 and 8. If you are not already logged on as a Windows administrator, the software will request you to do so.

NOTE: For further information on the **config21cfr.exe** utility, see *Appendix 3: Administering the PerkinElmer Enhanced Security Application Account* on page 94.

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

   The Enhanced Security Configuration program 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 AssureID 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. Start the program C:\Program Files\PerkinElmer\PE21CFR\config21cfr.exe or C:\Program Files (x86)\PerkinElmer\PE21CFR\config21cfr.exe.

2. Login using the Local_Administrator account **User name** and **Password** identified/created in step 1 of the previous instructions.
   The Enhanced Security Configuration program is displayed.

3. Select the Passwords tab.

4. Select **Update password in this program after changing in Operating System**.

5. Leave the Enhanced Security Configuration program open at the Passwords tab.

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

7. Double-click **User Accounts**.
   The User Accounts dialog opens.

8. Select the AssureID security system account (New_21cfr), and then click **Reset Password**.
   The Reset Password dialog is displayed.

9. Enter the new password, confirm the new password, and then click **OK**.
   You should remember this password.

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

11. Click **Save** to save the changes to the Enhanced Security Configuration program.
    You will have to restart the PC after making the changes, then you will be able to run AssureID using Windows Logins again.

Appendix 3: Administering the PerkinElmer Enhanced Security Application Account

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

The Security Server functions as an extension of the computer's operating system and is used by the Windows Login functionality of AssureID ES 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 the PerkinElmer Enhanced Security Application Account used by the Windows Login functionality.

To run the Enhanced Security Configuration program:

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

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

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

For details of how to change the account see *Changing the Enhanced Security Application Account* on page 95. For details of how to change the account password, see *Using the Passwords Tab* on page 97.

The Enhanced Security Configuration program is displayed.

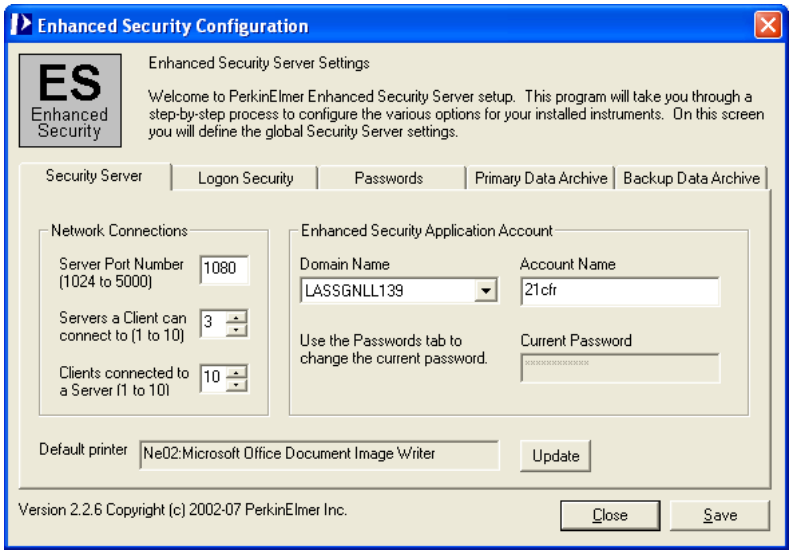
There are five tabs, only two of which are applicable to AssureID ES users:

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

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

Using the Security Server Tab

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



Changing the Enhanced Security Application Account

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

1. Create a new Administrator account in Windows.

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

2. Enter the name of the new account in the **Account Name** field.

3. Ensure that the **Domain Name** is correct.

   The domain name is most likely to be the local PC.

4. Click **Update**.

5. Enter the password of the new account in the **Current Password** field.

6. Click **Save** to save the changes to the Enhanced Security Configuration program.

Changing the Network Connection settings

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

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

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

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

   The default value is 10.

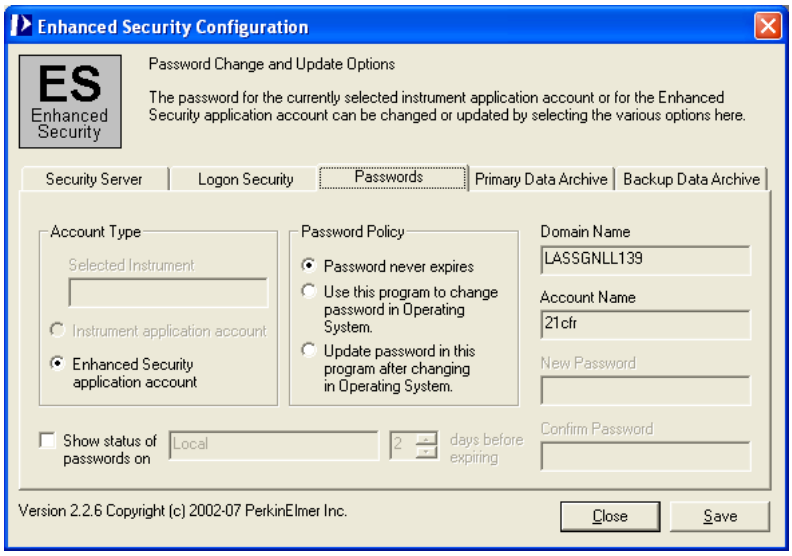
Changing the printer

To change the default printer:

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

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

Using the Passwords Tab



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

Changing the password for the Enhanced Security Application Account

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

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

Troubleshooting the Enhanced Security Configuration Program

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

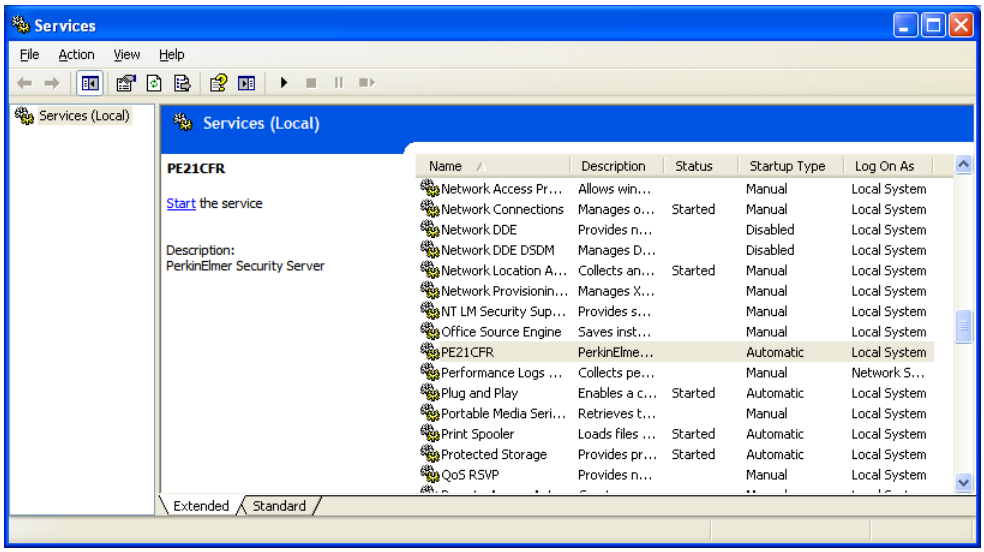
Server error message

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

To resolve this issue:

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

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

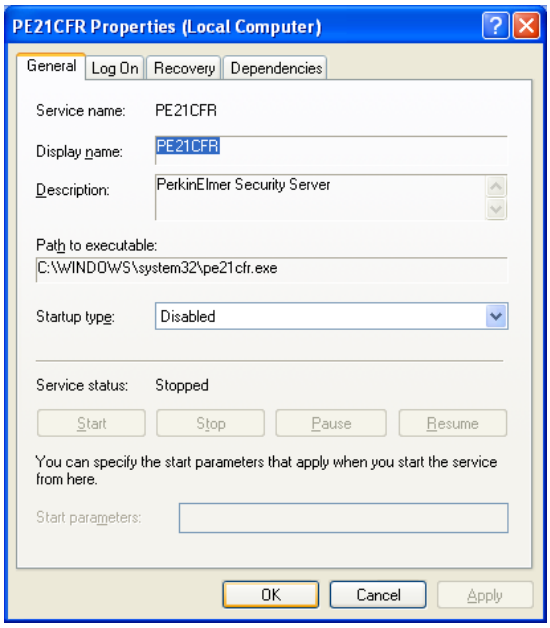


4. At this point:
   - If the Startup Type is Automatic, click **Start the service**. The Security Server should start running.
   - If the Startup Type is either Manual or Disabled, you must change this to Automatic, and then click **Start the service**. This change may require the intervention of your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

To change the Startup Type:

1. Right-click **PE21CFR**.

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



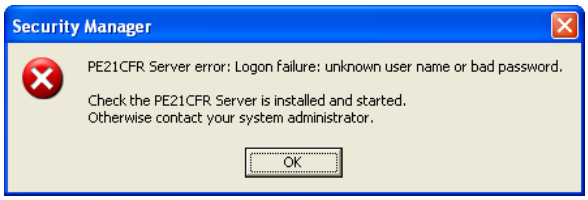
3. Select **Automatic** from the **Startup type** drop-down list.

4. Click **OK**.

5. Press **Start** in the Services window.

Logon failure message

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



To resolve the problem, follow the instructions in *Changing the Enhanced Security Application Account* on page 95, and *Changing the password for the Enhanced Security Application Account* on page 97 that describe how to change the account name and password respectively.

Installation error message

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

This message is displayed in response to the following circumstances:

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

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

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

- The Enhanced Security Configuration program will not run.

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

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

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

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

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

Status Monitor

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

Starting the Status Monitor

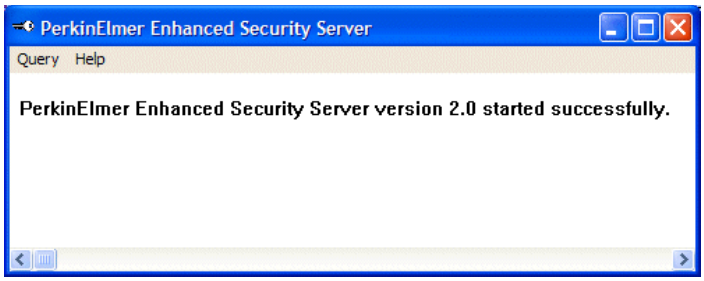
If you have enabled Password Notification with the Enhanced Security Configuration program, the Status Monitor should start automatically. If it does not, follow the steps below to start it manually:

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

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

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

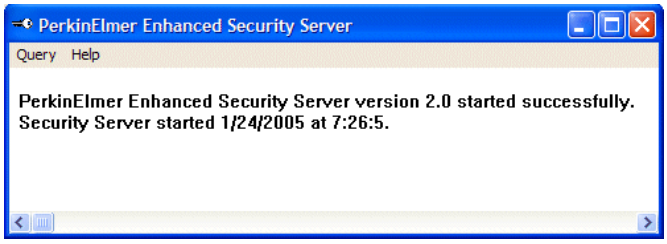
   

The Query menu allows you to view:

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

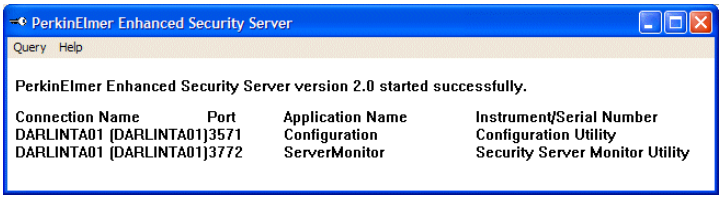
Status

This indicates when the Security Server starts and stops running.



Connections

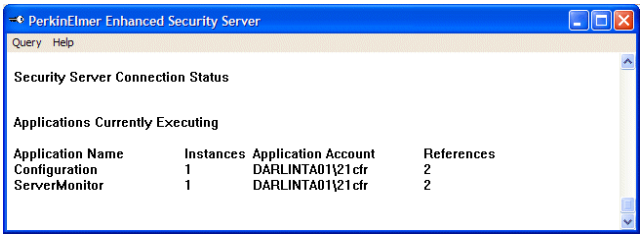
This shows the computer name, application name, and the instrument and serial number that are connected to the Security Server. It also shows the name and port number of the connection.



Applications

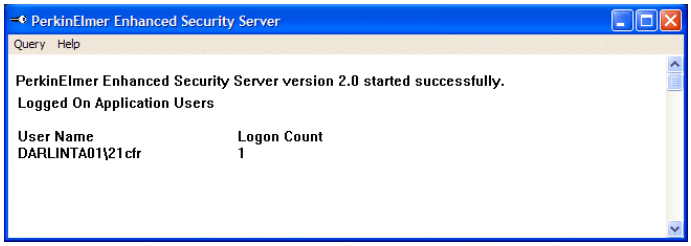
This shows the software applications that are connected to the Security Server. It also shows the number of instances of these applications, the names of the Application accounts, and the name of the computer on which each Application account is stored. It also shows the References; that is, the number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

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



Users

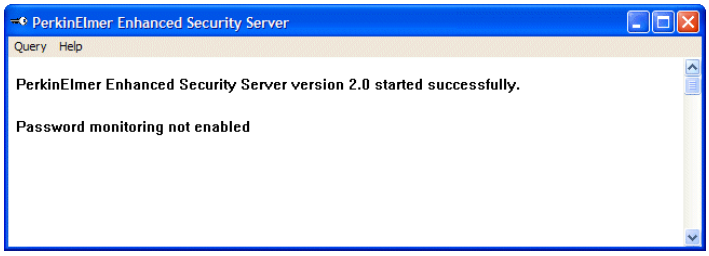
This shows the name of the user(s) that have logged onto the Security Server. In the example shown below, the user named DARLINTA01 has logged on to the Security Server. The Logon Count is the number of logon sessions for the user DARLINTA01.



Passwords

This shows the Application account(s) password status.

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



You can change the status of the password on the Passwords tab of the Enhanced Security Configuration program. See *Changing the password for the Enhanced Security Application Account* on page 97 for details.