

UV WINLAB ES



Administrator's Guide

Release History

Part Number	Release	Publication Date
L6050012	D	November 2014

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

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

Or emailed to: info@perkinelmer.com

Notices

The information contained in this document is subject to change without notice.

Except as specifically set forth in its terms and conditions of sale, PerkinElmer makes no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

PerkinElmer shall not be liable for errors contained herein for incidental consequential damages in connection with furnishing, performance or use of this material.

Copyright Information

This document contains proprietary information that is protected by copyright.

All rights are reserved. No part of this publication may be reproduced in any form whatsoever or translated into any language without the prior, written permission of PerkinElmer, Inc.

Copyright © 2014 PerkinElmer, Inc.

Produced in the UK.

Trademarks

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

PerkinElmer is a registered trademark of PerkinElmer, Inc.

Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and other countries.

Table of Contents

Introduction.....	5
Overview	6
Further Information	6
Conventions	7
Installation	9
PC Requirements.....	10
Software Requirements.....	10
Installing UV WinLab ES Software	12
Using the VeriTest-Rational Installation Analyzer™	12
Software installation	13
Security and Audit Trails	21
Windows Administration	22
Windows Configuration.....	23
Default Windows groups and accounts.....	23
Administering the UV WinLab Users Group	24
File permissions.....	25
Active Directory	25
Administration of UV WinLab ES.....	27
UV WinLab ES Software Administration.....	28
UV WinLab ES Permissions.....	29
UV WinLab ES login security.....	29
Setting up PerkinElmer Login.....	29
Setting up Windows Login.....	29
Users and Groups	32
Default Users	33
Adding a new user.....	34
Pre-defined Groups.....	34
Permissions.....	36
Assigning a user to a group.....	38
Creating a new group	38
Defining what members of a group are able to do	38
Passwords.....	39
Defining when users must change their password.....	40
Defining the minimum length of time that users must retain the same password.....	40
Defining the length of a password	40
Re-using a password.....	40
Account Lockout.....	41
Disabling an existing individual user.....	42
Security Summary	42
Folder Visibility	44
Public.....	44
Private	44
Restricted	45
Setting up Electronic Signature Points	46
UV WinLab ES Login History.....	48
Security System Audit Trail	49
Other Audit Trails.....	50
Method Audit Trail	50
IPV Setup Audit Trail	50
Legacy File Converter	52
Database Management.....	53
Database Tools.....	53

Backing up and Recovering Databases and Files	55
Recovering from Checksum Failures.....	56
UVWinLab database	56
Security database	56
Data files.....	57
Overview of UV WinLab ES	59
Starting UV WinLab ES.....	60
Adding an Instrument	60
Appendices.....	65
Appendix 1: The link between Windows Login security and UV WinLab security...	66
Appendix 2: Administering the PerkinElmer Enhanced Security Application	
Account	67
Using the Security Server Tab.....	68
Using the Passwords Tab.....	69
Troubleshooting the Enhanced Security Configuration Program.....	70
Status Monitor	73

Introduction

Overview

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

Installation – the step-by-step procedure for installing the software.

Administration of UV WinLab ES – full details of what it means to be an Administrator for the software, how to use both the in-built security of the Windows operating system and the UV WinLab ES software to maintain 21 CFR Part 11 technical compliance, and how to work with the databases in UV WinLab ES.

An Overview of UV WinLab ES – an introduction to starting the application and configuring an instrument.

Appendix – a table shows the link between Windows Logon Security and UV WinLab Security.

Further Information

For more information on your Lambda instrument, consult the manual that comes with the instrument.

A full HTML Help system is provided with the UV WinLab ES software and can be accessed by selecting **Contents and Index** from the Help menu. A version of the help file in .pdf format, for viewing away from the PC, can be accessed by clicking on the **User's Guide pdf** button on the toolbar in the Help window.

Conventions

The following conventions are 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.

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

The procedures described in this document assume that the software has been installed to the C: drive. The appropriate drive letter should be substituted, as applicable.



Installation

PC Requirements

The following pages detail the software requirements for the PC that will run the UV WinLab ES software and communicate with the instrument. To ensure successful installation of the software, please check these requirements before starting the installation.

Software Requirements

Operating System

This software requires that one of the following versions of the Windows operating system is installed on your PC before you install UV WinLab ES software.

- Windows XP Professional (Service Pack 3, or later)
- Windows 7 Professional
- Windows 8.x Pro

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

Internet Explorer

UV WinLab ES requires Internet Explorer 5.5 or later. This must be installed on the PC before you install the UV WinLab ES software.

Previous Versions of UV Software

If you do not have any version of UV WinLab currently installed:

UV WinLab must be installed on a clean PC.

If you are upgrading from UV WinLab 2.x or 3.x:

UV WinLab must be installed on a clean PC. You must not install UV WinLab on a PC with UV WinLab 2.x or 3.x already installed.

If you are upgrading from UV WinLab 4 or later:

NOTE: You must remove the current version of UV WinLab before installing this version of UV WinLab.

NOTE: Your current databases will not be removed, and you can continue to use them with this latest version of UV WinLab, providing that you are using the same format of UV WinLab (for example upgrading from UV WinLab Standard 5.2 to UV WinLab Standard 6.0). If you are upgrading from the Standard version of UV WinLab to the Enhanced Security version, you must remove your databases, as well as the software, as they are not compatible. If you want to use Methods that you have previously created, then these can be exported before the software is deleted. Please see the on-screen Help for further information about exporting methods.

To remove UV WinLab from your PC (Windows XP operating system):

1. From the Start menu select **Control Panel**.
2. Select **Add or Remove Programs**.
3. Select **Remove a Program**.
4. Select **PerkinElmer UV WinLab** and then click **Remove**.
UV WinLab is removed.
5. Reboot the PC before proceeding with the installation.
If you want to backup your databases before deleting them or before installing the new version of UV WinLab, please refer to *Database Management* on page 53, and *Backing up and Recovering Databases and Files* on page 55.

To remove UV WinLab from your PC (Windows 7 operating system):

1. From the Start menu select **Control Panel**.
2. Select **Programs and Features**.
3. Select **PerkinElmer UV WinLab** and then click **Uninstall**.
4. Select **Yes** when prompted.
UV WinLab is uninstalled.
5. Reboot the PC before proceeding with the installation.
If you want to backup your databases before deleting them or before installing the new version of UV WinLab, please refer to *Database Management* on page 53, and *Backing up and Recovering Databases and Files* on page 55.

To remove UV WinLab from your PC (Windows 8.x operating system):

1. Use the Search function to locate the **Control Panel** under **Settings**.
2. Select **Programs and Features**.
3. Select **PerkinElmer UV WinLab** and then click **Uninstall**.
4. Select **Yes** when prompted.
UV WinLab is uninstalled.
5. Reboot the PC before proceeding with the installation.
If you want to backup your databases before deleting them or before installing the new version of UV WinLab, please refer to *Database Management* on page 53, and *Backing up and Recovering Databases and Files* on page 55.

Installing UV WinLab ES Software

NOTE: You must be logged on to Windows at Administrator level before installing the software.

The installation will make the following operating system checks to ensure 21 CFR Part 11 technical compliance.

- An appropriate version of the Windows operating system;
- At least one NTFS drive.

It will also check whether there are any non-compliant PerkinElmer UV software programs installed.

Using the VeriTest-Rational Installation Analyzer™

NOTE: VeriTest-Rational Installation Analyzer is a third-party software package available on the *Software Utilities CD* shipped with UV WinLab ES. PerkinElmer is not responsible for any errors or issues arising from use of this software.

Installation Analyzer (IA) detects changes made to the drives and registry of a Windows system, typically before and after the installation of a product. IA does this by creating "snapshots" of the system both before and after the desired operations, and then performing a comparison of the two snapshots.

The compare operation will generate an HTML report detailing the changes made to the drives and registry. The information will include all added, deleted and changed: files, directories and executables. It will also include all added, deleted and changed: registry entries, 16-bit executables and kernel mode drivers added to the system and extensions properly or improperly added to the system.

NOTE: If you do not want to use VeriTest-Rational Installation Analyzer™ omit the next section, and Step 20 of the UV WinLab and UV WinLab Data Processor and Viewer (DPV) installation.

To use the VeriTest-Rational Installation Analyzer™ during the installation:

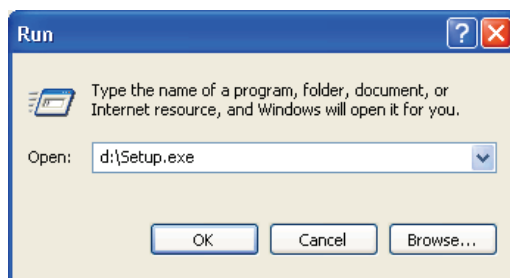
6. Install by copying the Analyzer directory from the *Software Utilities CD* shipped with UV WinLab, to your hard drive.
7. Read the directions found in Using.htm in the Analyzer directory.
8. Create a snapshot of the PC.

Software installation

To install UV WinLab ES or UV WinLab Data Processor and Viewer (DPV):

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

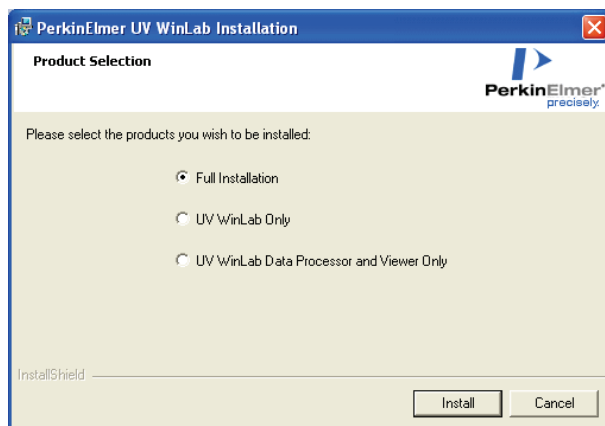
The Run dialog is displayed.



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

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

After the start-up picture, the Wizard is set up and the Product Selection dialog is displayed.

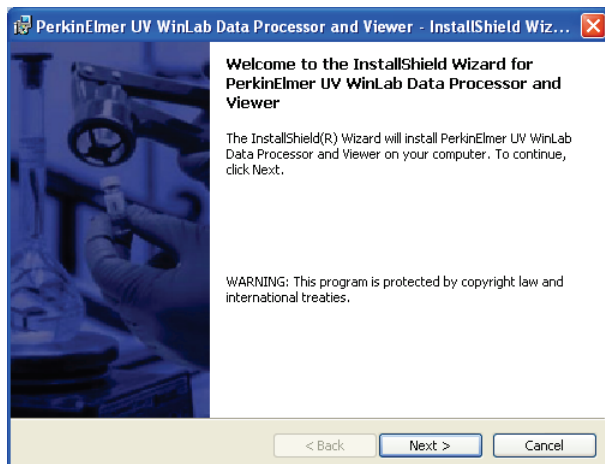


4. Select the products you want to be installed and then click **Install**.

NOTE: If your PC is running under the Windows 7 operating system AND you have another PerkinElmer application already installed, the **UV WinLab Only** option is not made available until after you have installed the UV WinLab DPV software.

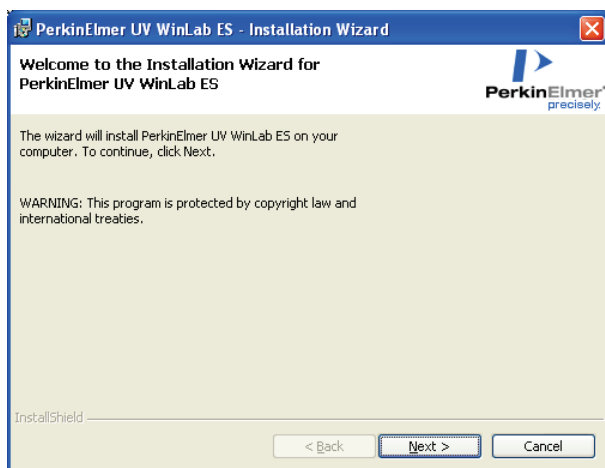
If you want to install UV WinLab, you are advised to select the **Full Installation** option. Alternatively, you can select **UV WinLab Data Processor and Viewer Only** and then subsequently re-run the installation process to install UV WinLab.

If you select **Full Installation**, both UV WinLab and UV WinLab DPV will be installed. In this case, UV WinLab DPV software is installed before the UV WinLab software. The Welcome page for UV WinLab Data Processor and Viewer (DPV) is displayed. Go to Step 5.



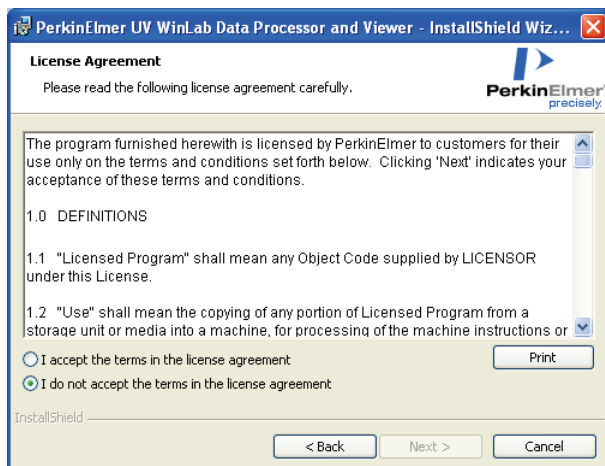
OR

If you select **UV WinLab Only**, the UV WinLab Welcome page is displayed. Go to Step 9.



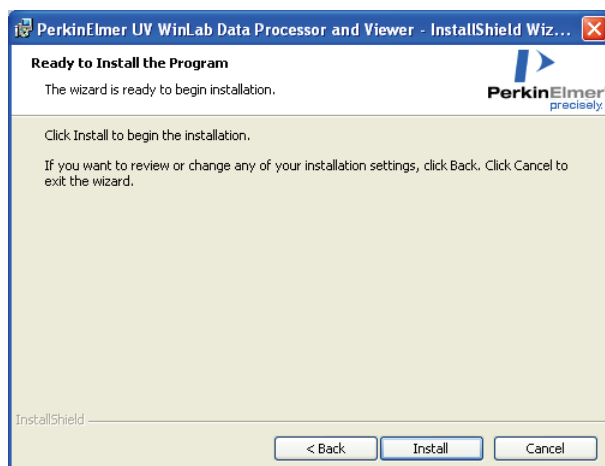
5. Click **Next**.

If your PC does not meet any of the requirements you will be informed of the problem and will need to correct it before the installation can be performed. Otherwise, the UV WinLab DPV License Agreement will be displayed.



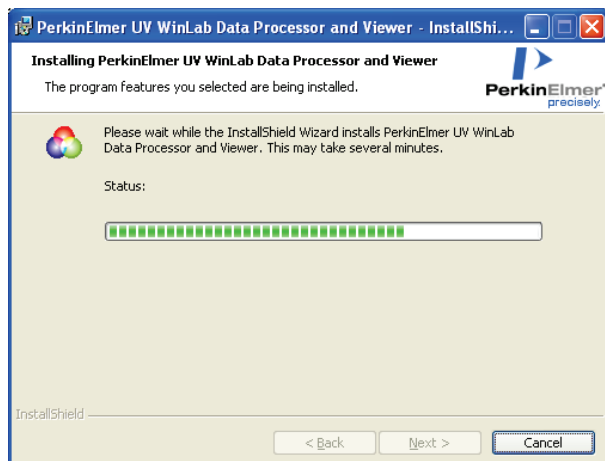
6. Read the License Agreement and if you accept the terms, select that option and then click **Next**.

The Ready to Install the Program page is displayed.

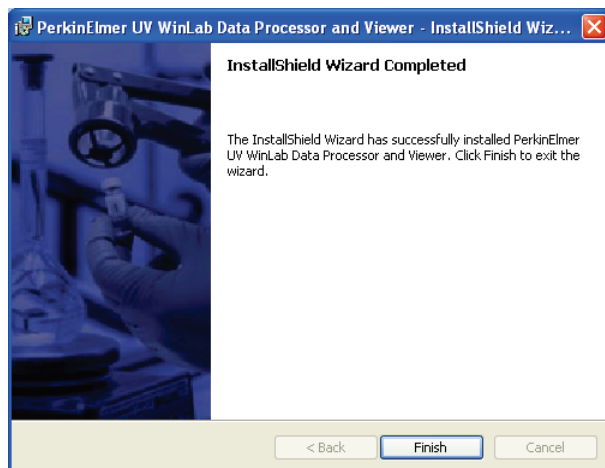


7. Click **Install**.

The Installation begins.

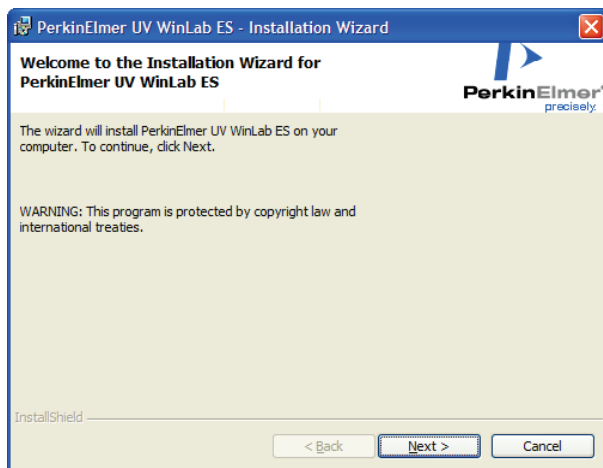


When the installation is complete a confirmation message is displayed.



8. Click **Finish**.

If you selected **Full Installation** in Step 4, the UV WinLab installer will now run. After a few seconds, the UV WinLab Welcome page is displayed. Go to Step 9.



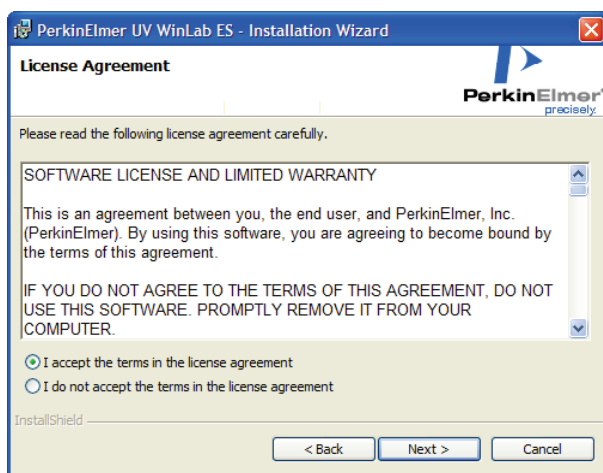
OR

If you selected **UV WinLab Data Processor and Viewer Only**, the installation is now complete.

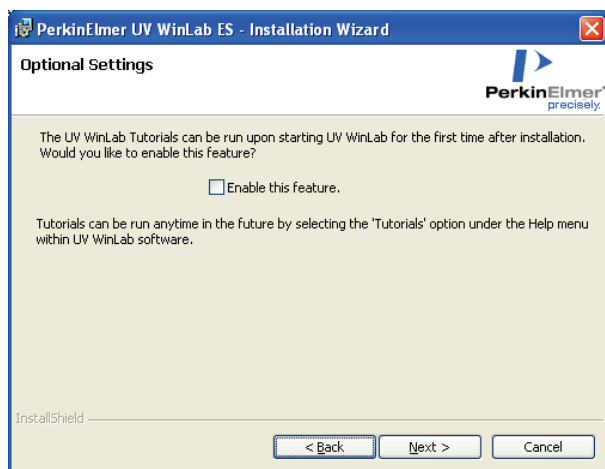
UV WinLab DPV is now ready to be used. You do not need to restart your computer.

9. Click **Next**.

If your PC does not meet any of the requirements you will be informed of the problem and will need to correct it before the installation can be performed. Otherwise, the UV WinLab License Agreement will be displayed.



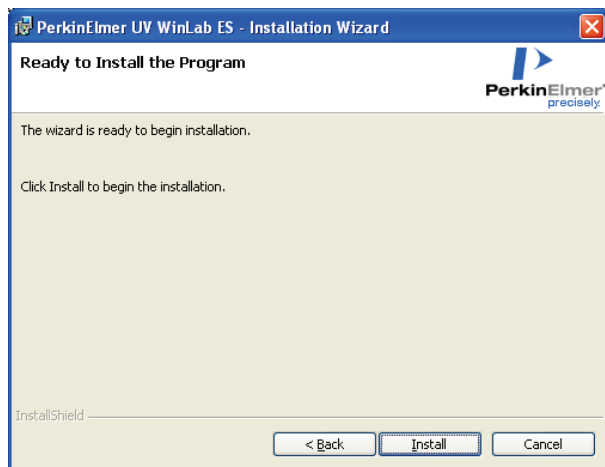
10. Read the license and if you accept the terms, select that option and then click **Next**.
The Optional Settings page is displayed.



11. Select the check box if you want the Getting Started Tutorial to start up the first time you run the UV WinLab software after installation.
The option is disabled as default.

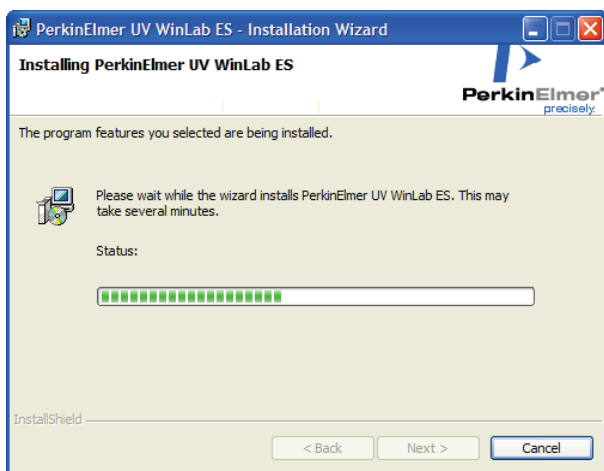
NOTE: The Getting Started Tutorial is designed to be a quick introduction to UV WinLab version 6 to help you to start collecting your data as soon as possible. The Getting Started Tutorial and other tutorials covering a range of UV WinLab functions can be accessed at any time. Select **Tutorials** from the Help menu within the UV WinLab Explorer.

12. Click **Next**.
The Ready to Install the Program page is displayed.



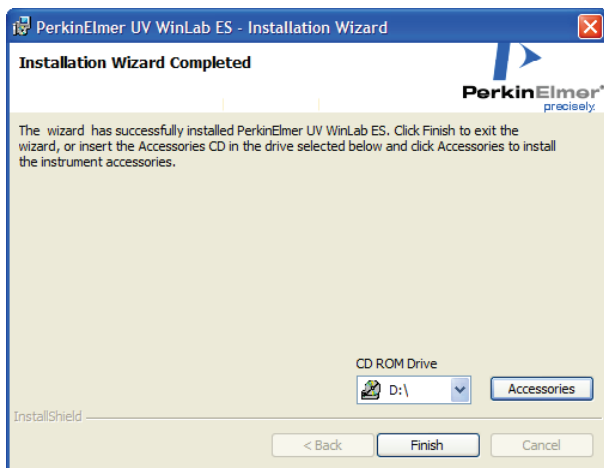
13. Click **Install**.

The Installation begins.



If you are upgrading UV WinLab, or installing the application onto a system with other PerkinElmer applications already installed, then the PerkinElmer Login dialog may be displayed. In this case, login as a PerkinElmer software Administrator. Use the Administrator User name and password that you use for the PerkinElmer software that is already installed on the PC.

When the installation is complete a confirmation message is displayed.

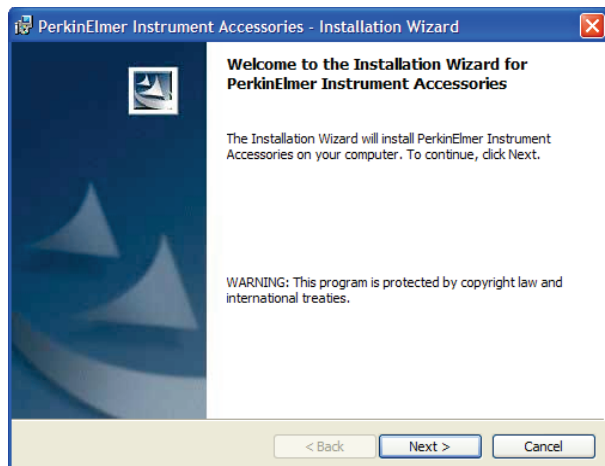


14. If you do not want to install any accessories, go to Step 18.

OR

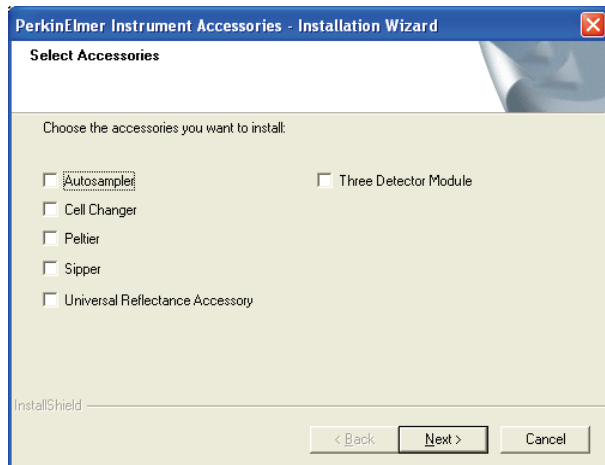
If you want to install accessories, insert the accessory CD in the CD drive, select the drive from the drop-down list and then click **Accessories**.

The Accessory Wizard starts.



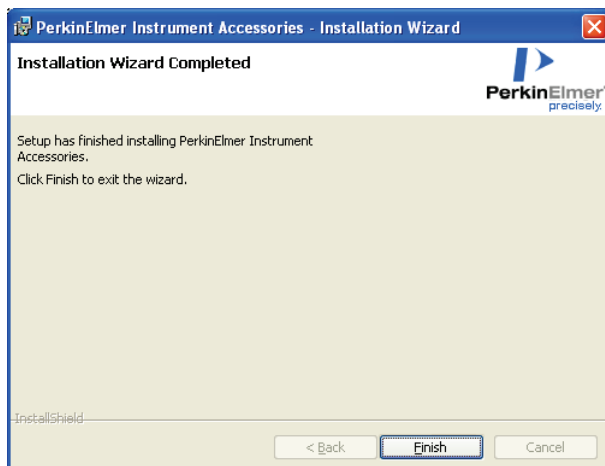
15. Click **Next**.

The Select Accessories page is displayed.



16. Select the accessories you want to install and then click **Next**.

Each of the selected accessories is installed in turn using the Accessory Wizard. Follow the instructions on the screen. When all the selected accessories have been installed, the Installation Wizard Completed page is displayed.

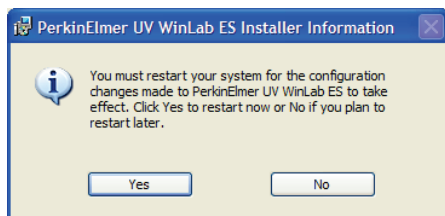


17. Click **Finish**.

The main Installation Wizard Completed dialog is re-displayed.

18. Click **Finish**.

A message is displayed prompting you to restart your computer.



19. Click **Yes**.

The computer will restart and the installation is now complete.

20. Create a second snapshot using VeriTest-Rational Installation Analyzer™ and compare with the first to generate an installation report.

NOTE: The HTML report that is produced for UV WinLab is approximately 1000 pages long.

NOTE: After installing the software, we recommend that you read and print the release notes (UV WinLab ES Release Notes.pdf), which can be found in the UV WinLab Documentation folder under UV WinLab, from the PerkinElmer Applications section of the Start menu. They contain important information that may not be in this Administrator's Guide or the on-screen Help.

NOTE: The following sections of this manual give important information on recommended procedures for maintaining the security of the system and should be read thoroughly.

Security and Audit Trails

There are two main security systems used by the software:

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

These security features give maximum flexibility, allowing the customer to very tightly restrict what a day-to-day user is able to do and to fit easily with the company procedures designed to adhere to 21 CFR Part 11 compliance.

Each security system has an Administrator who has full access, so it is important that whoever takes this role has been fully trained in that particular area.

NOTE: We strongly recommend that at least one more Administrator is created. If the Administrator forgets their password, it is very serious as there is no “back door” into the software. This is to ensure 21 CFR Part 11 compliance.
It is a very good idea to create a dummy administrator whose log-in is stored in a secure location (such as a safe).

Day-to-day users of the system will not typically be allowed to delete, change or rename data files. Their access to UV WinLab ES functionality will be determined by the permissions of the group to which they are assigned.

Windows Administration

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

NOTE: We recommend that 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:

- Review the directory and file security permissions set during installation and consider whether further changes are required.
- Set up Password and User Name policies according to the company's internal security policy.
- Ensure that Users only have access to folders and files that they need access to. This includes network drives.
- Consider whether the floppy drive or CD Writer should be disabled.
- Make sure that Users are prevented from deleting any files in the file locations where data is saved (by using the security features in NTFS).
- Use the auditing features of Windows to track attempts to log in and attempts to delete files from the PC.
- Consider whether to set up a password protected screen saver to guard against unauthorized use of the system when unattended.
- Ensure that appropriate backup procedures are in place for data files and databases, as discussed in *Database Management* on page 53.

Windows Configuration

During installation, PerkinElmer software will set directory and file security permissions so that UV WinLab will run on an NTFS system on Windows.

The Windows administrator should review what has been set and consider whether further changes are required.

Default Windows groups and accounts

NOTE: The Administrator account is already present on the PC and is the standard Windows administrator account. This gives the administrator full access to the whole system, including the ability to Delete and Rename files, and run any application, and change user and file/folder permissions. Clearly the administrator has great power, and so the person acting in this role should be suitably trained and qualified in Windows. We recommend that this person is not the same person who will be using the instrument on a day-to-day basis.

The install sets up the following default Windows accounts:

- UV WinLab User – <password: UV WinLab user> – an ordinary Windows User account.
- PEService and PEDeveloper – two Windows Administrator accounts for use by PerkinElmer (the default password for these accounts are only available to PerkinElmer engineers).
- UV WinLab Users group – this group is used to set permissions on files, folders and registry entries required for UV WinLab ES to work correctly. See below for details of how to administer this group.
- 21CFR_Admin group – a group used for Windows login functionality. This contains the Windows Administrator account, 21cfr, used by Windows login functionality to authenticate Windows user names and passwords.

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

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

Administering the UV WinLab Users Group

All users of UV WinLab ES must be members of the UV WinLab Users group on their local PC.

NOTE: If the UV WinLab ES login type is set to Windows Login, users may also need to be made members of a separate Windows Login group. See *Setting up Windows Login* on page 29.

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

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

1. Log in to the PC as a Windows Administrator.
2. On the Control Panel, open **Computer Management**.
The Computer Management dialog is displayed.
In Windows 7/8, you will need to open **Administrative Tools** first and then select Computer Management.
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 **UV WinLab Users**.
The UV WinLab Users 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 UV WinLab Users Properties dialog.
10. Click **OK** and then close all the Control Panel dialog boxes.

File permissions

NOTE: By default, UV WinLab is installed to the C: drive.

The installer sets the following folder permissions, which are required for UV WinLab execution:

Directory	"UV WinLab Users" group
...\PerkinElmer\Security System	Generic Write, Create Files, Create Folders, No delete.
...\PerkinElmer\UVWinLab	Create Files, Create Folders, Read/Write Attributes, No delete.

Where "... " represents:

- For Windows XP, C:\Documents and Settings\All Users\Application Data
- For Windows 7/8, C:\ProgramData

NOTE: All subdirectories automatically inherit these permissions.

Active Directory

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

If the target computer for PerkinElmer ES software is on an Active Directory network, then this may be a preferable way of managing computer and Windows settings.



Administration of **UV WinLab ES**

UV WinLab ES Software Administration

There is a need to have someone with Administrator privileges in UV WinLab ES to set up and maintain the security of UV WinLab ES Software for the technical compliance to 21 CFR Part 11.

The UV WinLab ES Software Administrator is required to:

- Administer the users, including setting their access and permissions to UV WinLab; see *UV WinLab ES Permissions* on page 29.
- Set Account lockout and Passwords; see *Adding a new user* on page 34.
- View the Login History; see *UV WinLab ES Login History* on page 48.
- View the Audit trails; see *Security System Audit Trail* on page 49 and *Other Audit Trails* on page 50.

NOTE: The UV WinLab ES Software Administrator does not need to be a Windows Administrator. They can be a Windows User if required.

UV WinLab ES Permissions

UV WinLab ES login security

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

- **PerkinElmer Login**
This involves creating a user name and password for each UV WinLab ES user, in addition to their Windows login on the PC. This provides much greater flexibility to tailor the software to a User's individual needs and level of training. It also allows the PC to be used by different people and different compliant applications more easily.
- **Windows Login**
This allows Windows users to log in to UV WinLab ES using their Windows user name and password, instead of having a separate UV WinLab ES user name and password.

The level of access available to users of UV WinLab ES software depends on the permissions set by the Software Administrator. Part of the planning process for establishing UV WinLab 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.

Setting up PerkinElmer Login

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

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

To set up the UV WinLab ES users and groups, see *Users and Groups* on page 32.

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 UV WinLab ES.

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

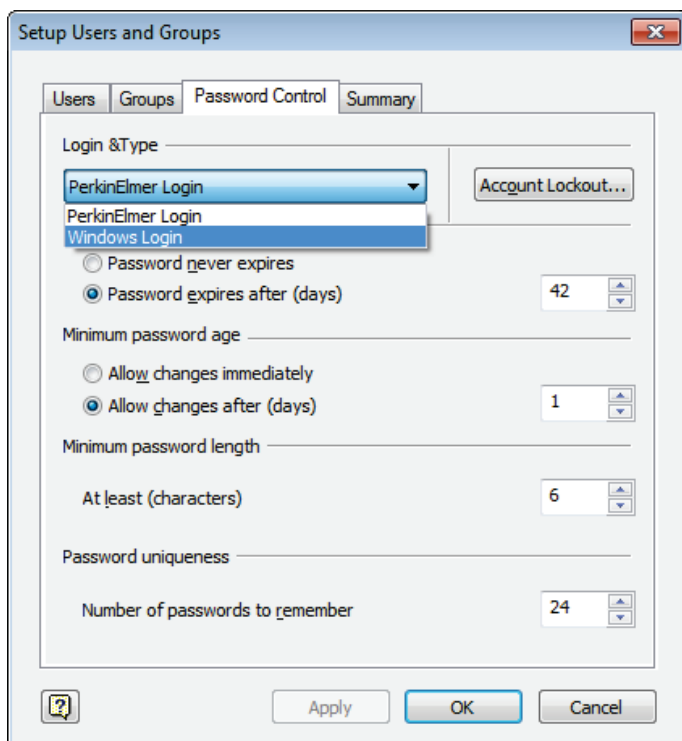
When you set the UV WinLab ES login type to Windows Login, you must specify the name of a Windows group whose members are to be allowed to use the Windows Login facility. By default this is the UV WinLab Users group on the local PC, created when the software was installed.

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 UV WinLab Users group on the local PC, to access UV WinLab ES. For further details, see *Administering the UV WinLab Users Group* on page 24.

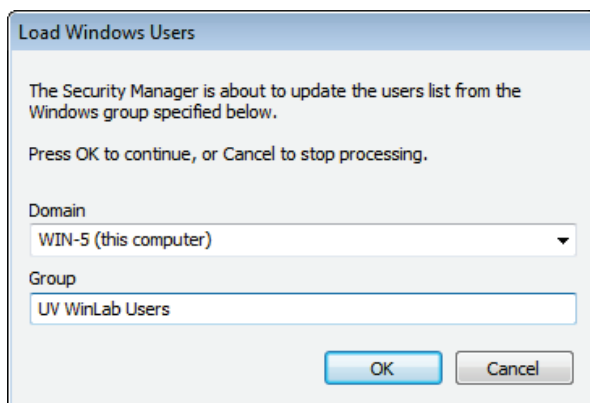
NOTE: All members of the Windows Login group must be members of UV WinLab Users on the local PC they are going to use.

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

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



The Load Windows Users dialog is displayed.

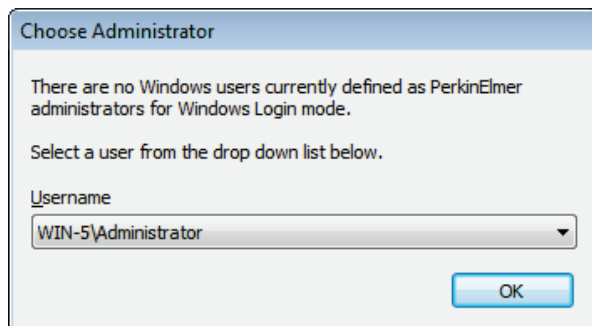


4. If appropriate, select the Domain and Group containing the Windows users you want to be able to access the software.

If you want to use the default Windows Login group, make sure that **UV WinLab Users** is entered in the Group text box. If you want to use another Windows login group, it must contain at least one individual Windows user. See *Administering the UV WinLab Users Group* on page 24.

5. Click **OK**.

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

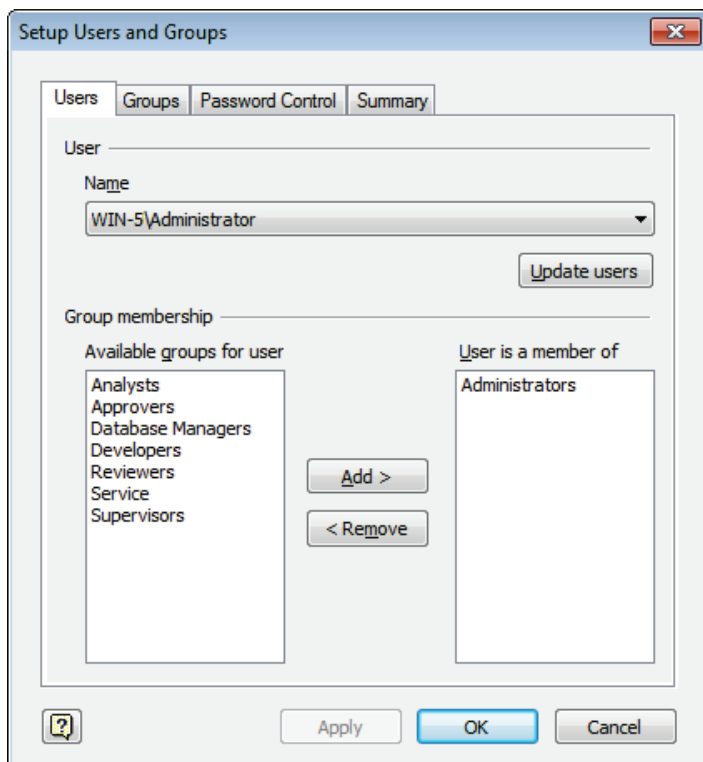


6. Use the drop-down to select the user who is to be the PerkinElmer Software Administrator and then click **OK**.
7. Click **OK** again to close the Setup Users and Groups dialog.
8. Exit the UV WinLab ES software.

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

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

1. Log in to UV WinLab ES software as the Software Administrator.
2. From the Administration 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 must be assigned to the appropriate group or groups within UV WinLab ES.



- Any user required to be a UV WinLab ES Software Administrator must be made a member of the Administrators group. We recommend that at least two users are set up as Software Administrators, for emergency use.
 - Any user requiring access to UV WinLab ES software must be made a member of at least one group.
3. Select each user in turn from the **Name** drop-down and configure them appropriately. See *Assigning a user to a group* on page 38 for details.
 4. When you are finished, click **OK**.

Users can now access the UV WinLab ES software.

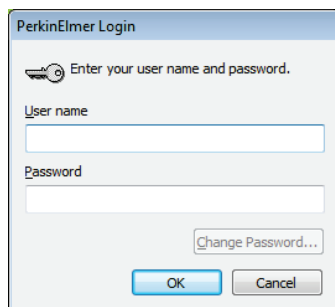
Users and Groups

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

The Users and Groups setup is used to define the users, groups and password control. Users of UV WinLab ES must be set up by a UV WinLab ES Administrator. Each User must have a Password to login to UV WinLab. Users are assigned to one or more groups. Each group is able to perform a series of operations such as Editing methods or Approving results, as defined by the permissions allocated to the group.

Default groups are provided. However, a UV WinLab ES Administrator can create custom groups as required.

1. To start UV WinLab ES, select **PerkinElmer UV WinLab** from the **UV WinLab** group under **PerkinElmer Applications** from the **Programs** section of the Start menu. The PerkinElmer Login dialog is displayed.



2. Enter your **User name (Administrator)** and **Password (administrator)**.
The software will start and you will be prompted to change your password.
3. Change your password.
4. Select **Setup Users and Groups** from the Administration menu within the UV WinLab Explorer.

Default Users

UV WinLab ES contains the following default users and their passwords:

User name	Password	Member of Group
Administrator	administrator	Administrators
Database Manager	database manager	Database Managers
Supervisor	supervisor	Supervisors
Reviewer	reviewer	Reviewers
Developer	developer	Developers
Approver	approver	Approvers
Analyst	analyst	Analysts

NOTE: We recommend that you change these passwords immediately or disable the accounts to stop any unauthorized access to the software.

NOTE: The User name PEService is also available, but is intended for use by PerkinElmer Service Engineers. PEService is a member of the Administrators and Service groups. The User name PEDeveloper is also available, but is intended for use by PerkinElmer. PEDeveloper is a member of the Developer group.

Further information about these groups is given in *Pre-defined Groups* on page 34.

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

NOTE: We recommend that you immediately create another user who is a member of the Administrators group for emergency use in case of a problem with the primary Administrator.

Adding a new user

1. If the Setup Users and Groups dialog is not displayed, select **Setup Users and Groups** from the Administration menu.
2. Select the Users tab and then click **New**.
The New User dialog is displayed.
3. Enter the **User name**, **Full name**, **Password**, and repeat the **Password** in the **Confirm password** entry field.
The password length is defined on the Password Control tab. By default it is at least six characters.

NOTE: A **User name** must be unique.

NOTE: The Password is case-sensitive. It can consist of letters, numbers and single spaces only.

4. 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.
5. Click **OK**.
The **User name** drop-down list is updated with the new user.

NOTE: When the new user logs in for the first time they will be forced to change their password.

Pre-defined Groups

The following pre-defined groups are provided in UV WinLab ES: Administrators, Database Managers, Analysts, Supervisors, Developers, Reviewers, Approvers and Service.

The Administrator is able to set up new groups and define what members or the groups are able to do.

NOTE: It is possible to change the group membership of the pre-defined users. By default, the pre-defined users are only members of the default group with the same name. For example, the Analyst user is a member of the Analysts group, and the Developer is a member of the Developers group. The exception to this is the PEService user, who is a member of the Administrators and Service groups.

The following table lists the permissions of the pre-defined groups:

Group	Member of the group is able to:
Administrators	<p>The permissions for the Administrator are not listed. The Administrator is only able to perform Administration tasks – set up users, groups and passwords. They can also undelete reports and report templates.</p> <div> NOTE: This group cannot be edited. </div>
Database Manager	Create and edit methods and IPV set-ups, Manage and delete methods and IPV set-ups, Manage tasks, Manage the database.
Analysts	Continue task, Run calibrations, Run methods, Run queries.
Supervisors	Configure instruments, Continue tasks, Edit and save calibrations, Edit queries, Print reports, Run instrument performance verifications, Run methods, Run queries, Run calibrations.
Developers	Create and edit methods and IPV set-ups, Edit calibrations, Edit queries, Edit report templates, Manage and delete methods and IPV set-ups, Print reports, Reprocess results, Run instrument performance verifications, Run methods, Run queries.
Reviewers	Edit and save calibrations, Edit queries, Edit report templates, Manage and delete methods and IPV set-ups, Print reports, Review method and IPV set-ups, Review report templates, Review reports, Review results, Run calibrations, Run instrument performance verifications, Run methods, Run queries.
Approvers	Approve methods and IPV set-ups, Approve report templates, Approve reports, Approve results, Edit and save calibrations, Edit queries, Edit report templates, Manage and delete methods and IPV set-ups, Print reports, Run calibrations, Run instrument performance verifications, Run methods, Run queries.
Service	Configure instruments, Create and edit methods and IPV set-ups, Edit queries, Edit report templates, Manage the database, Print reports, Re-process results, Run calibrations, Run instrument performance verifications, Run methods, Run queries, Service.

Permissions

All the available permissions that can be assigned to groups in UV WinLab are listed below, together with an overview of what the permission enables the user to do within the software.

Permission	Description
Approve methods and IPV set-ups	Approve locked methods and locked IPV set-ups.
Approve own results	Allows a user to approve their results within the Workspace or Results Browser. NOTE: Run Queries permission is needed in addition if you want to approve results from within the Results Browser.
Approve report templates	Approve report templates. (This sets the status of the report template to Approved.)
Approve reports	Approve reports. (This sets the status of the report to Approved.)
Approve results	Approve a task. (This sets the status of the task to Approved.) NOTE: Run Queries permission is needed in addition if you want to approve results from within the Results Browser.
Configure instruments	Add new instruments, delete instruments, enables instrument calibration for High Performance instruments, apply an IPV setup to an instrument, set a default instrument, edit instrument.
Continue task	Re-open tasks and continue running them, add new samples to sample table.
Create and edit methods and IPV set-ups	Create, edit, copy, paste, lock and unlock methods; import and export methods, create IPV setup and apply to an instrument, re-perform failed IPV, postpone an IPV, perform an IPV on demand.
Delete reports	Delete reports.
Edit and save calibrations	Modify and save existing calibrations.
Edit queries	Create, edit and run results queries; cut, paste, delete and restore queries.
Edit report templates	Opens Communiqué report creator to create, edit and save report templates; Delete user created report templates (default templates cannot be deleted).
Manage and delete methods and IPV set-ups	Delete, restore, cut and paste methods; move methods between folders.
Manage tasks	Rename and delete folders, rename folder items, cut and paste tasks between folders.

Permission	Description
Manage the database	Run database utilities, use legacy file converter, determine the visibility of folders, empty recycle bin.
Print reports	Print preview and print reports.
Reprocess results	<p>Enables a completed task to be re-processed (a copy of the task is created and can be renamed).</p> <p>NOTE: Only the Reporting, Processing, Quant and Rate pages in the Workspace can be edited.</p>
Review methods and IPV set-ups	Review a locked method or locked IPV setup.
Review report templates	Review report templates.
Review reports	Review reports.
Review results	<p>Review a task. (This sets the status of the task to Reviewed.)</p> <p>NOTE: Run Queries permission is needed in addition if you want to review results from within the Results Browser.</p>
Run calibrations	Create and save calibrations.
Run instrument performance verifications	Perform instrument performance verifications.
Run methods	Run methods to create tasks, enables Autozero, add comments to sample table.
Run queries	<p>Run pre-defined results queries.</p> <p>NOTE: The Run queries permission does not allow you to create a new query, only run a previously setup query against the current database.</p>
Service	Access the Instrument filter properties in the Explorer and access the filter table on the Instrument page in the workspace (High Performance instruments).

Assigning a user to a group

Users can be assigned to one or more groups. The user would then have the permissions assigned to all the groups of which they are a member.

1. Select the user from the **Name** drop-down list on the Users tab.
2. 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.

If you want to create more than one new user and assign each of them to a group/groups you must click **Apply** after assigning the groups to the first user before creating the next new user, otherwise the group assignments for the currently selected user will be lost.

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

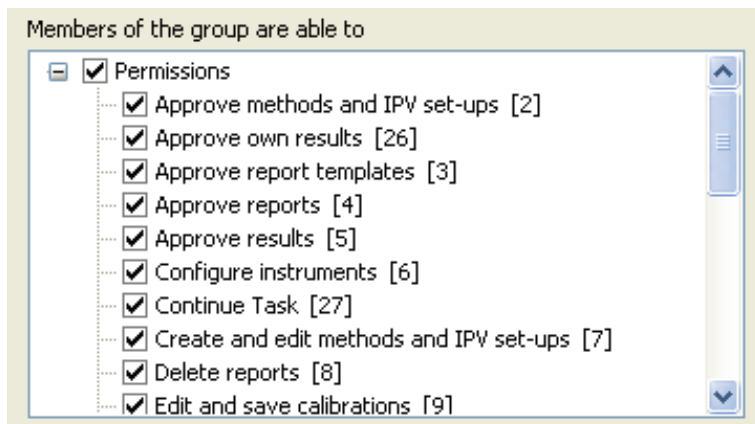
Creating a new group

1. From the Administration menu, select **Setup Users and Groups**.
The Setup Users and Groups dialog is displayed.
2. Select the Groups tab and then click **New**.
The New Group dialog is displayed.
3. Enter a **Group name** and then click **OK**.
The drop-down list is updated to include the new group.
By default, none of the options in the **Permissions** list are selected.

Defining what members of a group are able to do

The permissions available to each group are selected on the Groups tab. The permissions are listed as a tree structure. When a new group is created, none of the permissions are selected by default.

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



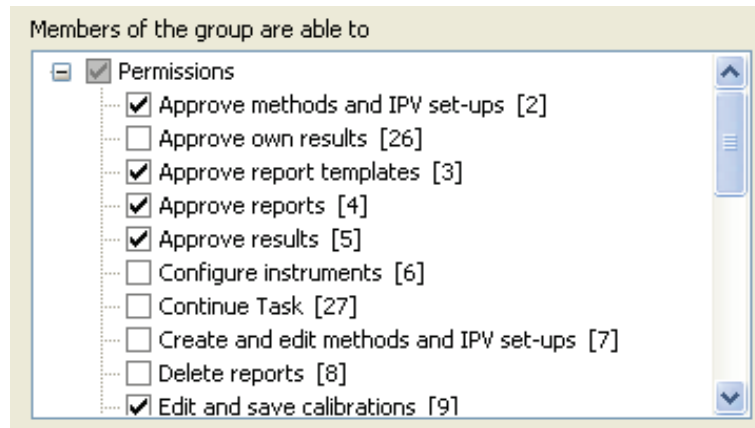
All the permissions are automatically checked.

OR

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

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

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



2. When all the required permissions are selected, click **Apply**.
The available options for the group are updated.

NOTE: The numbers at the end of each permission relate to the database. When you view the audit trail, it is these numbers that are listed rather than the description of the permission. You will need to refer back to the list of permissions on the Groups tab to find the number that relates to a particular permission, or look at the summary where the permission together with the number is given.

For more information on configuring users and groups, and the available permissions, see the on-screen Help by selecting **Contents and Index** from the Help menu in the UV WinLab Explorer.

Passwords

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

Changing a password

1. From the Administration menu in the UV WinLab Explorer, select **Setup Users and Groups**.
The Setup Users and Groups dialog is displayed.
2. Select the Users tab.
3. To change a user's password, select the user from the **Name** drop-down list on the User's tab and then click **Edit**.
The Edit User dialog is displayed.
4. Enter the new **Password** and repeat it in the **Confirm password** entry field.

5. Click **OK**.

The new password is implemented. The next time the user logs in they will be forced to use the new password.

Defining when users must change their password

NOTE: The settings on the Password Control tab apply to all users. It is not possible to define individual Password controls for each user.

On the Password Control tab, **Maximum password age** defines the maximum number of days that users can retain the same password before they must change it. By default the password expires after **42 days**. The minimum is **1 day** and the maximum is **999 days**.

The **Maximum password age** cannot be set less than or equal to the **Minimum password age**.

NOTE: If you want to set the **Maximum password age** to **1 day** the **Minimum password age** must first be set to **Allow changes immediately**.

NOTE: Users are forced to change their password the first time they login.

Defining the minimum length of time that users must retain the same password

On the Password Control tab, **Minimum password age** defines the number of days that users must retain the same password before being allowed to change it. The default is **Allow changes after 1 days**. **Allow changes after 1 days** prevents users from changing their password several times in a short space of time in order to return to a previous password. The minimum is **1 day** and the maximum is **999 days**.

To allow users to be able to change their password immediately, select **Allow changes immediately**.

The **Minimum password age** cannot be set greater than or equal to the **Maximum password age**.

Defining the length of a password

Minimum password length on the Password Control tab defines the minimum number of characters that must be used in the password. The default is **At least 6 characters**. The minimum is 1 and the maximum is 16 characters.

Re-using a password

Users are able to reuse a previous password. **Password uniqueness** on the Password Control tab defines the number of new passwords that must be used before a previous password can be reused. For example, if the first password is "security", and **Number of passwords to remember** is set to three entries, users must use three other passwords in addition to their current password before they are able to reuse "security" as their password. The minimum is 1 and the maximum is 24. By default, **Number of passwords to remember** is set to **24**.

Account Lockout

Clicking **Account Lockout** on the Permissions tab of the Setup Users and Groups dialog displays the Account Lockout dialog. The dialog allows you to define the **Number of failed logins allowed before lockout**.

For example, if **Number of failed logins allowed before lockout** is set to five failed login attempts, the user is allowed five failed attempts at login. On the fifth failed attempt they are locked out until the Administrator allows them access again (Permanent) or for a specified period of time (Duration). The default is lockout after five failed login attempts for both Enhanced Security and Standard Security. The minimum number of failed login attempts before a user is locked out is 1. The maximum number of allowed failed login attempts before a user is locked out is 10.

You can select the Lockout Duration as **Permanent, until Administrator unlocks**, or **Duration**. If you select **Duration**, enter the time (in minutes) for the lockout.

NOTE: If **Number of failed logins allowed before lockout** is set to **1** the user will be locked out when they have one incorrect login attempt. That is, they are not allowed an incorrect login attempt, otherwise they will be immediately locked out.

Permanent until administrator unlocks means that the user will be unable to login again until the administrator has unlocked their account and assigned a new password. **Duration** prevents the user being able to login again until the time specified has elapsed. **Duration** is grayed if Permanent is selected.

If **Duration** is selected, the default is 60 minutes. The minimum **Duration** is 1 minute and the maximum **Duration** is 32767 minutes (22.75 days).

NOTE: In the Enhanced Security version of UV WinLab, details of failed login attempts are recorded in the Login History.

If the Lockout is set to **Permanent until administrator unlocks** and the user has failed to login correctly within the allowed number of attempts, the administrator must assign a new password before they are able to login again.

When the administrator next logs in after a user has been locked out, a list of Locked Out Users is displayed.

To reinstate locked out users:

1. Highlight the name of the user that you want to reinstate and then click **Edit**.
The Edit User dialog is displayed.
2. Enter a new **Password** and repeat it in the **Confirm password** field.
3. Click **OK**.
The user is removed from the list of Locked Out Users.
4. Click **OK** to close the Locked Out Users dialog.
The previously locked out user will now be able to login using the new password, which they will be forced to change if they are using the Enhanced Security version of UV WinLab. In the Standard version of UV WinLab, users are only forced to change their password if **User must change password at next login** has been selected.

NOTE: If you click **OK** rather than **Edit** when the list of Locked Out Users is displayed, the list is closed and the Explorer starts. Any locked out users will remain locked out. The list will be redisplayed each time you login until any locked out users have each been assigned a new password.

NOTE: Users locked out for a specified duration can be unlocked by the administrator in the same manner.

Disabling an existing individual user

Disabling a user is useful as it ensures that during extended periods when a user will not be using UV WinLab (for example during a vacation), the User name and Password cannot be used.

1. From the Administration menu, select **Setup Users and Groups**.
The Setup Users and Groups dialog is displayed.
2. Select the Users tab.
3. Select the **Name** of the user from the drop-down list and then click **Edit**.
The Edit User dialog is displayed.
4. To disable the user, select **Disabled**.
5. Click **OK**.

The **User** is disabled.

If the disabled user attempts to login, an error message will displayed informing them that their login failed.

NOTE: To enable the user, select **Enabled** on this dialog. You must also enter and confirm a new password when enabling a user.

NOTE: You cannot disable yourself.

Security Summary

NOTE: The Summary can only be viewed by a member of the Administrators group.

The Summary records all information about the security settings:

Password control – it records maximum password age, minimum password age, minimum password length, password uniqueness, lockout count and lockout duration.

Permissions – it records the number of permissions and lists all the permissions with their associated number.

Users – it records the number of users. For each user it records the username, full name, status, last login, the groups the user belongs to, and the permissions of the groups.

Groups – it records the number of groups. For each group it records the group name, the users in the group, and the group permissions.

Viewing the Summary

1. From the Administration menu in the Explorer select **Setup Users and Groups**.
The Setup Users and Groups dialog is displayed.
2. Select the Summary tab.
The summary is displayed.

Printing the Summary

- To print the Summary click **Print**.
All the information is printed.

Exporting the Summary

1. To export the Summary click **Export**.
The Save As dialog is displayed.
2. Select the required destination and enter a filename.
The summary is exported as a *.csv file and can be opened, for example, in Microsoft Excel.

Folder Visibility

Anybody can create a folder. This folder is private to the person who created it and any person with **Manage the database** permission can also see it.

NOTE: Only a person with **Manage the database** permission is able to configure folders, that is, determine the level of access of the folder to users.

To create a new folder:

1. Click the right mouse button in the Main Pane of the Explorer Window.
2. From the menu select **New** and then select **Folder** from the sub-menu.
A new folder is added and the name is highlighted so that it can be edited.
3. Enter a new name for the folder and then click outside the name to save it.

NOTE: When a person with **Manage the database** permission (for example the default Database Manager) logs into the Explorer, any private folders that have been created have the name of the user appended so that the Database Manager can see who the folder belongs to.

There are three levels of access to folders: Public, Private and Restricted.

Public

All users are able to see Public folders.

To assign a folder as **Public**:

1. Click the right mouse button on the folder and then select **Properties**.
The Folder Properties dialog is displayed.
2. Select the Permissions tab.
3. Select **Public** and then click **OK**.
All users are able to see the Public folder.

Private

A Private folder can only be seen by the person who created the folder, and a Database Manager. A Database Manager can re-assign a private folder to another user.

To re-assign a Private folder:

1. Select the folder, click the right mouse button on the folder and then select **Properties**.
The Folder Properties dialog is displayed.
2. Select the Permissions tab.
3. Select **Private**.

4. Select the new **Owner** from the drop-down list.
5. Click **OK**.
The private folder is assigned to the new owner. Only the Database Manager and the new owner are now able to see the folder.

Restricted

A Restricted folder can only be seen by members of the group(s) that are given access to the folder by a Database Manager.

To assign groups to a folder:

1. Select the folder, click the right mouse button on the folder and then select **Properties**.
The Folder Properties dialog is displayed.
2. Select the Permissions tab.
3. Select **Restricted**.
A list of **Available Groups** is displayed.
4. Select a group from the **Available groups** list and then click **Add**.
The group is added to the Groups with access to this folder list.
5. Repeat Step 3 to add further groups to the **Groups with access to this folder** list, as required.
6. Click **OK**.
All groups in the **Groups with access to this folder** list will have access to the Restricted folder.
7. To remove a group from the **Groups with access to this folder** list, select the group and then click **Remove**.
The group is removed from the **Groups with access to this folder** list and added to the **Available Groups** list.

NOTE: If you have permission to **Manage the database**, and want to alter a folder description and the visibility of a folder, enter any necessary changes on the General tab of the folder's Properties dialog and then click **Apply** before selecting the Permissions tab and making the necessary changes. This ensures that the changes made on the General tab are saved when the Permissions tab is selected.

Setting up Electronic Signature Points

Within UV WinLab ES there is the option to select Signature Points. A Signature Point is a point in the software that requires an electronic signature, usually when a specific action such as saving is performed. The Signature Points are pre-defined within UV WinLab. For example, one Signature Point is Lock Method, so when a method is locked it requires an electronic signature and a dialog automatically appears. The user has to enter their User name, Password (if this option has been selected) and Reason for locking the method. They may also be able to add additional comments that are then saved with the signature if this option has previously been selected by the UV WinLab ES software Administrator.

The UV WinLab ES software Administrator is able to define the settings (that is, whether an electronic signature and comments are required) for each Signature Point individually or apply the same settings to all Signature Points. In addition, the software Administrator defines the list of reasons that may have caused each Signature Point to occur. The user then selects a reason from this pre-defined list in the Signature Point dialog.

For a full list of Signature Points, see the on-screen Help which can be accessed by selecting **Contents and Index** from the Help menu within the UV WinLab Explorer.



Defining the settings for each Signature Point

1. From the Administration menu in the Explorer, select **Signature Points**.
The Signature Points dialog is displayed.
2. Select the Signature Point **Name** from the drop-down list of available names.
3. If an electronic signature is required for a Signature Point, select **Signature required**.
4. If you want the user to be able to add comments if required, select **Prompt for comments**.

When the Signature Point dialog is displayed in the software, the user will be prompted to select a reason. For example, if they are reviewing a report the **Review Report** signature point is displayed. The user must then select a reason from the drop-down list of available reasons.

The list of reasons is also defined on this tab.

5. To add a new reason, click **New** and use the New Reason dialog to enter the new Reason.
6. To delete a reason, select the Reason from the **Text** list and click **Delete**.
7. To edit a reason, select the Reason from the **Text** list, click **Edit** and modify the text.

8. To change the order of the reasons, select a reason and click  or  to move it in the list.

Defining the same settings for all Signature Points

1. From the Administration menu in the UV WinLab Explorer, select **Signature Points**.
The Signature Points 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. In the Require Signature section, 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, no change will be made to the **Signature required** settings.
4. In the Prompt for comments, 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, no change will be made to the **Prompt for Comments** settings.
5. Click **OK**.
The Update All Signatures dialog closes and the Signature Points dialog is re-displayed.

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

UV WinLab ES Login History

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

1. From within the UV WinLab Explorer select **View Audit Trail** from the Administration menu.

The View Audit Trail dialog is displayed.

2. Select the Login History tab.

The login history is displayed. It details every login attempt, since the history was last cleared. It lists:

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

NOTE: If an incorrect **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 .csv file.

Security System Audit Trail

The Security System 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. Passwords are not displayed to ensure security is maintained.

1. From within the UV WinLab Explorer select **View Audit Trail** from the Administration menu.
The View Audit Trail Properties 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, except where this is a password;
 - **Current Value** – the new state, except where this is a password;
 - **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;
 - **Date Modified** – the date and time of the change.

The Audit Trail can be printed and exported as a .csv file.

Other Audit Trails

Method Audit Trail

When a method has been locked an Audit Trail commences for the method. The Audit Trail records:

- The software version;
- Date/Time;
- User Login ID and Full Name;
- Method name;
- Method type;
- Method Revision Details – Method revision, Method ID, Created on, Created by, Revision locked on, Revision locked by, Method description;
- Property, Previous Values and Actual Values.

To view the Method Audit Trail:

1. Open the method whose Audit Trail you want to view.
2. Double-click on the method in the Explorer to open it in the Workspace.
3. From the Tools menu select **Audit Trail**.

The Audit Trail report is displayed in the Print Preview window of Communiqué Report Creator.

IPV Setup Audit Trail

When an IPV setup has been locked an Audit Trail commences. The Audit Trail records:

- Name, Revision and Description;;
- Event History – Event, Date/Time, User Name, Full Name, Revision, Comments/Reason;
- Tests and Settings – Revision number, Tests Added, Tests Deleted, and for each test the Parameter Name, Initial Value and Final Value.

To view the IPV Setup Audit Trail:

1. From the Tools menu in the UV WinLab Explorer, select **Instrument Performance Verification**, and then from the sub-menu select **Create IPV Setup**.
The IPV Setup dialog is displayed.
2. Select the **Name** of the IPV Setup whose Audit Trail you want to view.
3. Click **Audit Trail**.
The Audit Trail report is displayed in the Print Preview window of Communiqué Report Creator.

Legacy File Converter

21 CFR Part 11 technical compliance mandates very high levels of data integrity and security. To ensure that UV WinLab 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.

Spectra collected on a previous version of UV WinLab, with the exception of data collected using UV WinLab 4.x ES or later, will not be read into the system and cannot be processed as they do not have the checksum. 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 called the Legacy File Converter has been included as part of the Administration tools. This utility allows the Administrator to add a data security checksum to a legacy spectrum.

NOTE: Use of the utility should be highly controlled and spectra that are processed should have full supporting GxP provenance as part of their Audit Trail.

NOTE: You must be a member of the Database Managers group or have **Manage the database** permission to be able to access the Legacy File Converter.

1. Select **Legacy File Converter** from the Administration menu within the 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 directory containing the legacy data.
3. For the Destination Path, click **Browse** and on the file selector displayed, select the **Destination Path** for the directory containing the converted data.
4. Click **Next**.
The data is copied and a checksum is added to each file, then the new files are written to the destination directory, leaving the original data untouched. The default text `_cs` is appended to each filename.
5. To view information about the conversion, click **View Log**.
A log file is displayed.

Database Management

You must be a member of the Database Managers group or have **Manage the database permission** to have access to the Database Tools.

There are three databases used in UV WinLab ES:

UVWinLab.mdb – holds information about methods and tasks

Users.mdb – holds the information required for logins

Communique.mdb – holds information about reports and report templates.

We recommend that you make regular backups of your databases. See *Backing up and Recovering Databases and Files* on page 55.

Database Tools

1. From the Start menu select Programs\PerkinElmer Applications\UV WinLab\Database Tools.
The Database Tools application starts.
2. 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 with a tick in a green circle showing the current database.
3. Click the button for the database tool required:
 - **Set Active Database** – Set the selected database to be the active one that will be used by UV WinLab.
 - **Compact Database** – Compact the database to remove deleted methods and free up disk space.
 - **Create Database** – Create and register a new empty database. Use this to create a new database on a network file server.
 - **Register Database** – Register an existing database with the system. Use this to connect to a database on a network file server.
 - **Check Database** – Enables you to perform an integrity check to see if the database has been tampered with or corrupted in some way. You can also view the log of previous database checks.
 - **Partial Archive** – Allows you to archive the database but leave the methods available for future use.
 - **Archive Utilities** – Loads the Communiqué archiving utility. Use this to archive or restore templates, reports and event logs.

<p>NOTE: The availability of the database tools listed above depend on the database selected.</p>
--

The table below lists the database tools available for each database. "X" indicates the operation is possible.

	UVWinLab.mdb	Users.mdb	Communique.mdb
Set Active Database	X		X
Compact Database	X	X	X
Create Database	X		X
Register Database	X		X
Check Database	X		
Partial Archive	X		
Archive Utilities			X

NOTE: Users.mdb is called **Security** in the left pane of the Database Tools application.

Backing up and Recovering Databases and Files

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

The following files/directories must be backed up regularly:

- ...\\PerkinElmer\\SecuritySystem\\Users.mdb
This is the security database of users, groups, passwords and permissions.
- ...\\PerkinElmer\\SecuritySystem\\backup\\Users.bak
This is a backup of the security database automatically created by UV WinLab. A maximum of three backup files are maintained: users.bak1, users.bak2, and users.bak3. These are replaced in sequence, with users.bak1 always being the most recent and users.bak3 the oldest.
- ...\\PerkinElmer\\UVWinLab\\Communique.mdb
This is the database of reports and report templates.
- ...\\PerkinElmer\\UVWinLab\\UVWinLab.mdb
This is the database of methods and tasks.

Where "... " represents:

For Windows XP, C:\\Documents and Settings\\All Users\\Application Data

For Windows 7/8, C:\\ProgramData

NOTE: Backups of Users.mdb and UVWinLab.mdb should be made at the same time to ensure that they are synchronized. If they are not synchronized and a problem occurs that means a backed-up database needs to be restored, there may be issues when attempting to use the UV WinLab Explorer.

Recovering from Checksum Failures

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

- Hard disk failure;
- Power failure;
- Software crash, either the application or Windows or another application;
- Deliberate attempt to falsify data.

If they occur then the reasons for them should be investigated and the reasons understood, before simply recovering from the problem.

The only remedy to an error message stating there is a checksum failure, and preventing you from accessing UV WinLab, is to restore from a backup database.

UVWinLab database

If the UVWinLab database gets a checksum failure the software will continue operating but the data in error will not be accessible. You will receive an error message if you try to open an invalid task or method.

It is essential that backups are regularly made of the Repository in order to recover from a checksum failure. The Windows Administrator can restore from this backup if the Repository becomes corrupt as follows:

1. Log in as Windows Administrator.
2. Rename or move UVWinLab.mdb from:
For Windows XP, C:\Documents and Settings\All Users\Application Data\PerkinElmer\UVWinLab
OR
For Windows 7/8, C:\ProgramData\PerkinElmer\UVWinLab
3. Copy your backup file as UVWinLab.mdb to replace the old one.

It should then be possible to view all the data again. Data collected after the last backup will be lost when the backup is restored.

Security database

It is essential that backups are regularly made of the security database in order to recover from a possible database failure. This should be done at the same time as the UVWinLab.mdb database is backed up.

In addition, the security system automatically backs up the Users.mdb database at the end of a session, and on exit from the administration dialog, in a subdirectory called \Backup as ...\\PerkinElmer\\SecuritySystem\\Backup\\Users.bak

Where “...” represents:

For Windows XP, C:\\Documents and Settings\\All Users\\Application Data

For Windows 7/8, C:\\ProgramData

A maximum of three backup files are maintained: users.bak1, users.bak2, and users.bak3. These are replaced in sequence, with users.bak1 always being the most recent and users.bak3 the oldest.

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

1. Log in as Windows Administrator.
2. Rename or move Users.mdb from ...\\PerkinElmer\\SecuritySystem.
3. Copy the most recent backup file ...\\PerkinElmer\\SecuritySystem\\Backup\\Users.bak as ...\\PerkinElmer\\SecuritySystem\\Users.mdb to replace the old one.

It should then be possible to log on again. Some data may be lost if there were any changes to the database that were not backed up.

Data files

These are discrete files, exported from UV WinLab, with extensions .sp and .td.

These files are all checksummed and when the files are loaded into UV WinLab, their integrity is checked. If the checksum is not present or is incorrect, then an error message is produced and the file will not load.

It is possible to use the Legacy File Converter to convert non-checksummed .sp and .td files collected in UV WinLab version 2.85 or earlier, version 4.x Standard, version 5.x Standard or version 6.x Standard. See *Legacy File Converter* on page 52.



Overview of UV WinLab ES

Starting UV WinLab ES

1. To start UV WinLab ES, select **PerkinElmer UV WinLab** from the **UV WinLab** group under **PerkinElmer Applications** from the **Programs** section of the Start menu.

The PerkinElmer Login dialog is displayed.



2. Enter your **User name** and **Password** as set up by the Administrator (see *UV WinLab ES Permissions* on page 29).

The software will start.


Adding an Instrument

Before collecting spectra you must add your instrument.

NOTE: You must have the **Configure instruments** permission to be able to add an instrument. See *UV WinLab ES Permissions* on page 29 for further information.

NOTE: You must switch the instrument on and allow it to initialize before adding it to the software.

Adding a Medium Performance instrument (Lambda 25, 35, 45, 20, 40, 40P, 20Bio and 40Bio)

1. Select **Instruments** from the Folder List in the Explorer window.
2. In the Main pane double-click **Add New Instrument** .
The New Instrument Wizard starts.
3. Select **Medium Performance UV/Vis instrument** from the Choose the type of instrument drop-down list.
The **Description** below the drop-down list details the available instruments.
4. Click **Next**.
The Select Instrument Type page is displayed.
5. Select the Instrument type from the drop-down list and, if required, select **Make this the default instrument**.

6. Click **Next**.

The Setup Communications page is displayed.

7. From the drop-down list, select the **Port** to which the instrument is connected.

OR

If you want to use a Simulation (if you are not connected to a real instrument), select **Simulation**.

The drop-down list becomes grayed.

NOTE: If you want to use a Simulated Medium Performance instrument, you must also setup the Simulator. See the on-screen Help for further information

8. Click **Next**.

NOTE: Clicking **Next** will automatically run a check to see if the correct instrument is attached to the selected port and switched on, and will display a Warning message if not.

9. Enter the **Name** and **Serial Number** of the instrument.

The Name will be displayed in the Explorer beneath the instrument icon.

The Serial Number can be found on the rear of the instrument. It can be edited in future if required. The Serial Number will be grayed and state **Simulation** if simulation was selected in Step 7.

10. Click **Next**.

The Method Shortcuts page is displayed.

11. Select your shortcut options.

If you want to add shortcuts to the basic methods to the Start Menu or the Desktop, select the appropriate options here.

All the options are selected as default.

12. Click **Next**.

The Example Methods dialog is displayed.

13. Select the group(s) of Example Methods that you would like to install.

The groups include: **Biochemistry & Molecular Biology**, **Clinical and Healthcare**, **Environmental**, **Food & Drink** and **General QC**.


14. Click **Next**.

The Finished page displays all the selected settings.

15. If all the settings are correct click **Finish** to close the wizard and add the instrument.

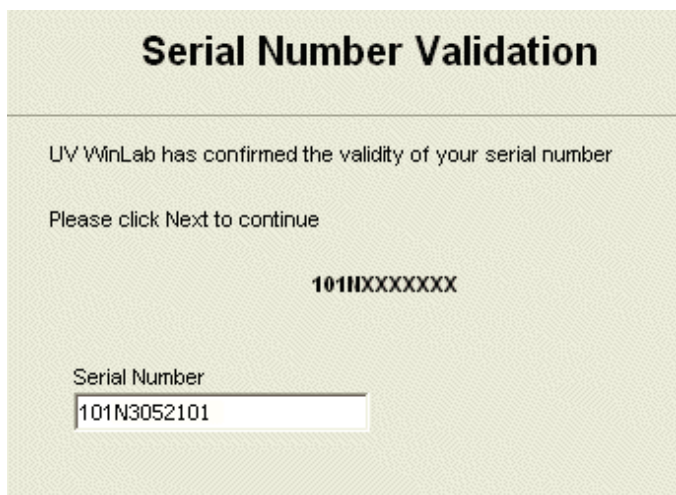
The Wizard closes, a confirmation message that the instrument has been successfully installed is displayed, and the instrument is displayed in the Explorer. If you have selected to make this the default instrument, a tick mark is displayed next to the instrument icon.

Adding a High Performance Instrument (Lambda 650, 750, 850, 800, 950, 900 and 1050)

1. Select **Instruments** from the **Folder List** in the Explorer window.
2. In the main pane, double-click **Add New Instrument** .
The New Instrument Wizard starts.
3. Select **High Performance UV/Vis/NIR instrument** from the Choose the type of instrument drop-down list.
The **Description** below the drop-down list details the available instruments.
4. Click **Next**.
The Select Instrument Type page is displayed.
5. Select the instrument type from the drop-down list and, if required, select **Make this the default instrument**.
6. Click **Next**.
The Setup Communications page is displayed.
7. From the drop-down list, select the **Port** the instrument is connected to.

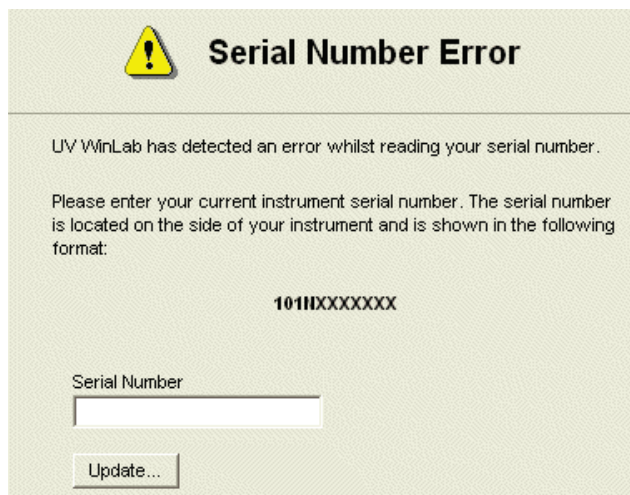
OR

If you are not connected to an instrument, select **Offline instrument**.
8. Click **Next**.
The software will try to detect the serial number of the attached instrument. The next wizard screen you see depends on whether the serial number is successfully detected.
9. If the Serial Number is correct, click **Next** to continue.



OR

If the Serial Number is not correctly detected, you must enter the **Serial Number** and then click **Update**. When the Serial Number has been updated, click **Next** to continue.



Serial Number Error

UV WinLab has detected an error whilst reading your serial number.

Please enter your current instrument serial number. The serial number is located on the side of your instrument and is shown in the following format:

101HXXXXXX

Serial Number

Update...

NOTE: You will not be able to proceed with the instrument installation until you have updated the Serial Number.

NOTE: If you have selected **Offline** instrument, you will not need to change the serial number displayed.

10. Enter the **Name** of your instrument.
The **Name** you enter will be used for identification throughout UV WinLab.
The **Serial Number** previously detected or entered is displayed but cannot be edited.
11. Select whether the instrument has a **Common Beam Depolarizer installed, Double Polarizer/Depolarizer installed**, and/or **Sample/Reference Beam Attenuators** installed.

NOTE: The option **Sample / Reference Beam Attenuators** is not available for the Lambda 650 or Lambda 750.

12. Click **Next**.
The Method Shortcuts page is displayed.
13. Select your shortcut options.
If you want to add shortcuts to the basic methods to the Start Menu or the Desktop, select the appropriate options here.
All the options are selected as default.
14. Click **Next**.
The Example Methods dialog is displayed.
15. Select the group(s) of Example Methods that you would like to install.
The groups include: **Color, Materials, Optics** and **Solar Reflectance**.
16. Click **Next**.
The Finished page displays all the selected settings.

17. If all the settings are correct click **Finish** to close the wizard and add the instrument.

The Wizard closes, the basic methods are created and a confirmation message that the instrument has been successfully installed is displayed, and the instrument is displayed in the Explorer. If you have selected to make this the default instrument, a tick mark is displayed next to the instrument icon.

NOTE: For further information on using UV WinLab, see the on-screen Help or Tutorials. To access the Help or Tutorials, select **Contents and Index** or **Tutorials** from the Help menu within the UV WinLab Explorer.

Appendices

Appendix 1: The link between Windows Login security and UV WinLab security

As there are two security systems it is important for the system administrator to understand the link between the Windows login system and the UV WinLab system. A table of the possible combinations and the implications and typical roles is given below:

Login to Windows as	Login to UV WinLab as	Can do	Can't do	Comment	Typical role
Administrator	Administrator	Anything to Windows; Perform Administration tasks in UV WinLab.	Collect Data; Manage the UV WinLab Databases.	Must be a suitably trained qualified person, knowledgeable in Windows.	Lab manager trained in Windows administration.
Administrator	User (Supervisor, Developer, Analyst, Approver, Reviewer)	Anything to Windows including datafiles, adding new applications; Access to UV WinLab depends on the group permissions.	Depends on permission in UV WinLab.	Must be a suitably trained qualified person.	IT department staff.
User	Administrator	Perform Administration tasks in UV WinLab; Run any other applications for which they have permission.	Can't delete/change data files.	Does not need to be qualified in Windows admin.	Lab manager, chief scientist, supervisor.
User	Database Manager	Perform Database Management tasks in UV WinLab; Run any other applications for which they have permission.	Depends on permission in UV WinLab.	Essential that back-ups are regularly taken.	IT department or Supervisor.
User	User (Supervisor, Developer, Analyst, Approver, Reviewer)	Run UV WinLab; Access to UV WinLab depends on the group permissions.	Can't change Windows settings; Can't delete/change datafiles	UV WinLab user who uses the system on a day-to-day basis within a 21 CFR Part 11 compliant environment.	System technician, operator.

Appendix 2: Administering the PerkinElmer Enhanced Security Application Account

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

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

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

To run the Enhanced Security Configuration program:

1. Ensure that the Enhanced Security Application Account is a member of the Administrators, Users and 21CFR_Admin groups on your PC.
2. Start the program C:\Program Files\PerkinElmer\PE21CFR\config21cfr.exe or C:\Program Files (x86)\PerkinElmer\PE21CFR\config21cfr.exe, and log in using the Enhanced Security Application Account name and password.

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

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

For details of how to change the account see *Changing the Enhanced Security Application Account* on page 68. For details of how to change the account password, see *Using the Passwords Tab* on page 70.

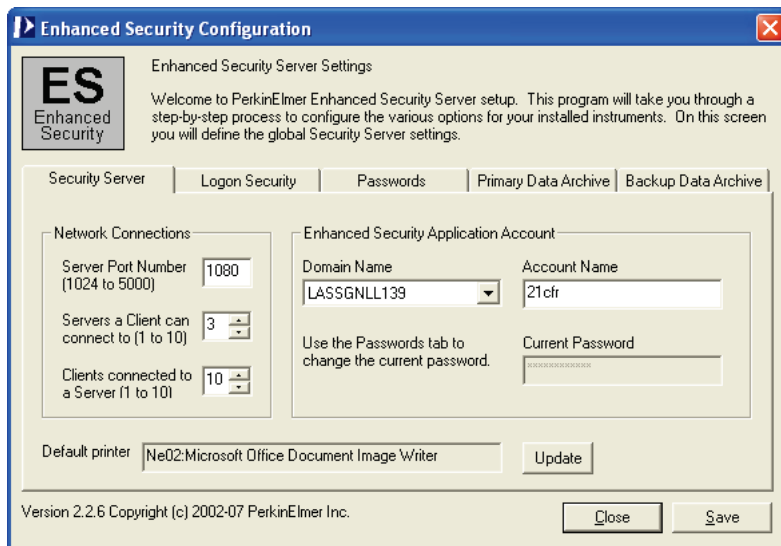
The Enhanced Security Configuration program is displayed.

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

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

Using the Security Server Tab

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



Changing the Enhanced Security Application Account

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

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

Changing the Network Connection settings

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

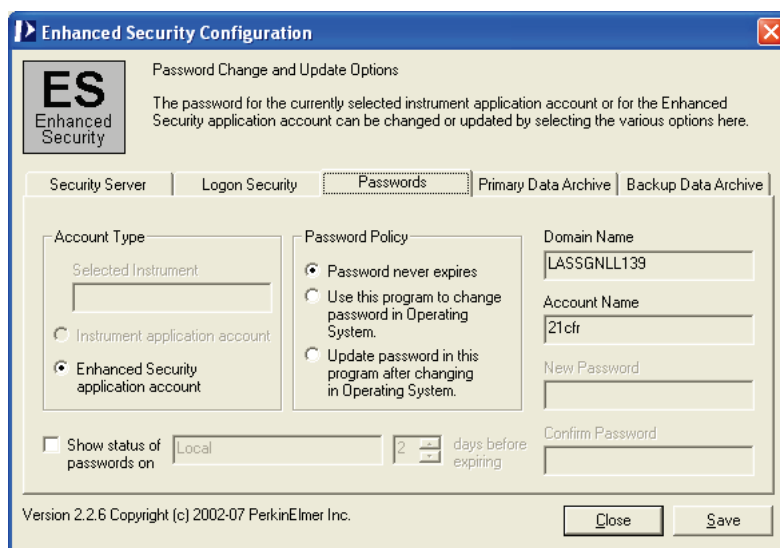
1. If you have installed an application that has the same TCP/IP server port number as that shown in the **Server Port Number** field, change the server port number.
The **Servers a Client can connect to** field represents the maximum number of Security Servers (including the local computer) that a client application can be connected to at any one time. This value will be greater than one if an application must start programs on other computers on the network.
2. The **Clients connected to a Server** field represents the number of applications that a server can have connected at any one time.
The default value is 10.

Changing the printer

To change the default printer:

1. Change the printer using the Windows operating system tools.
2. Return to this tab and click **Update**.

Using the Passwords Tab



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

Changing the password for the Enhanced Security Application Account

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

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

Troubleshooting the Enhanced Security Configuration Program

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

Server error message

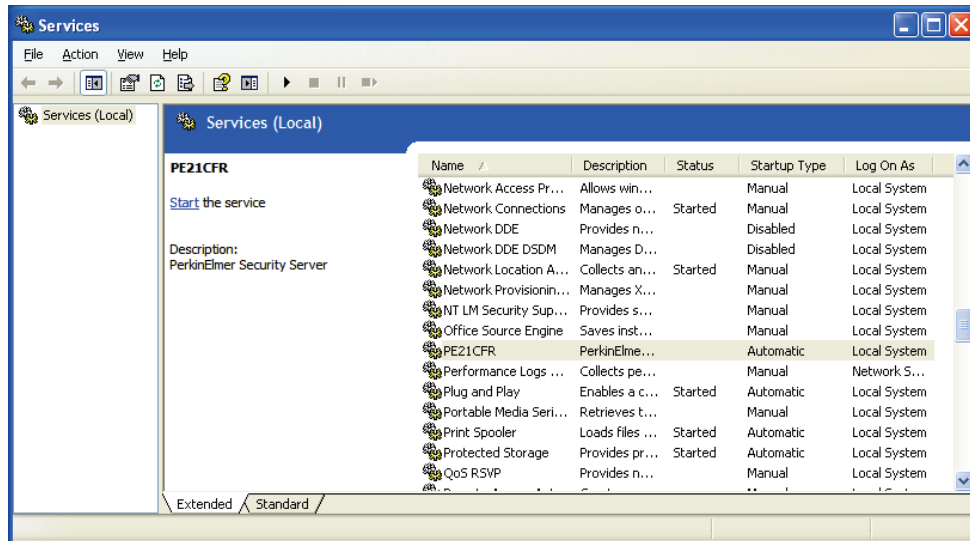
The Server error message, shown below, is typically displayed when you try to run the Enhanced Security Configuration program when the Security Server is not running.



To resolve this issue:

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

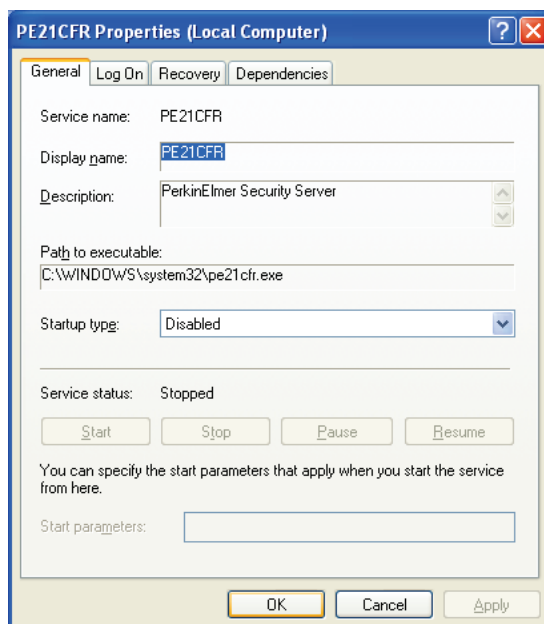
3. Under **Services**, select **PE21CFR**.
The Services dialog is displayed.



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

To change the Startup Type:

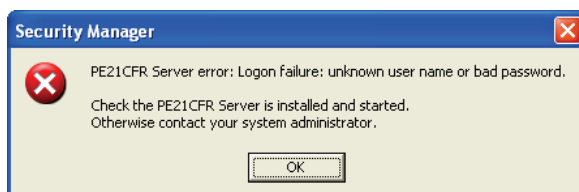
1. Right-click **PE21CFR**.
2. Select **Properties** from the menu.
The PE21CFR Properties (Local Computer) dialog is displayed.



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

Logon failure message

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



To resolve the problem, follow the instructions in *Changing the Enhanced Security Application Account* on page 68, and *Changing the password for the Enhanced Security Application Account* on page 69 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 UV WinLab ES will work correctly once the PC has been restarted.

Status Monitor

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

Starting the Status Monitor

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

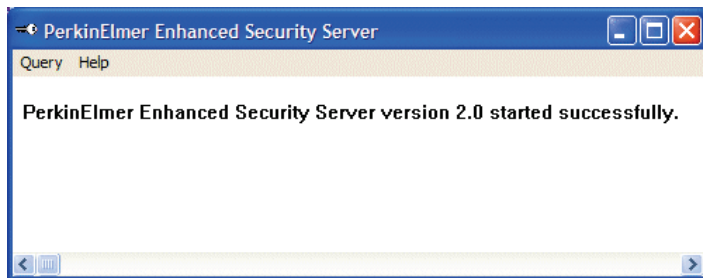
1. Start the program C:\Program Files\PerkinElmer\PE21CFR\pe21cfrsvr.exe or C:\Program Files (x86)\PerkinElmer\PE21CFR\pe21cfrsvr.exe.

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



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

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

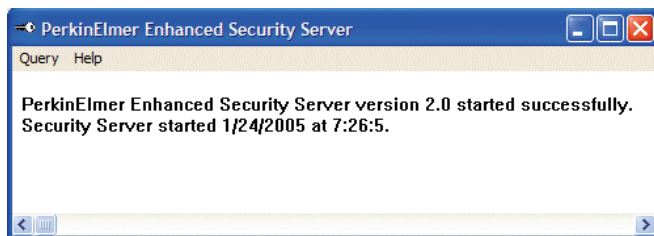


The Query menu allows you to view:

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

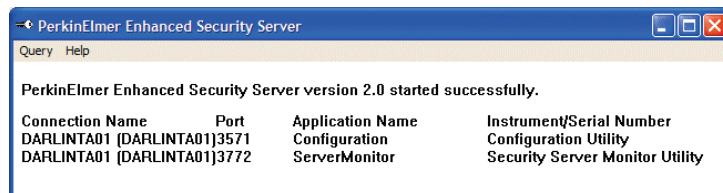
Status

This indicates when the Security Server starts and stops running.



Connections

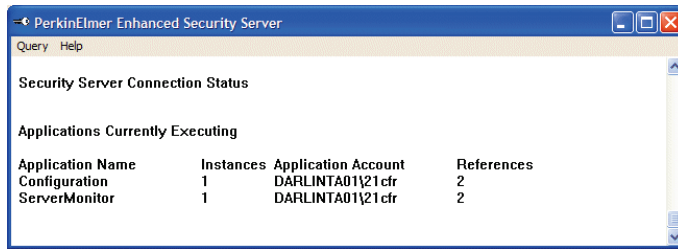
This shows the computer name, application name, and the instrument and serial number that are connected to the Security Server. It also shows the name and port number of the connection.



Applications

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

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



PerkinElmer Enhanced Security Server

Query Help

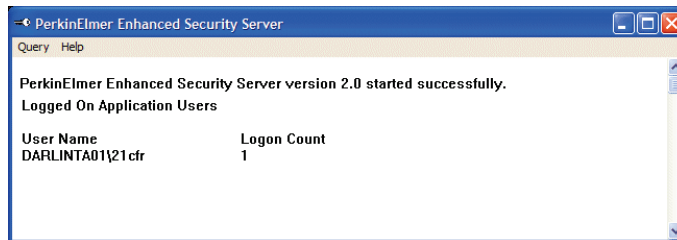
Security Server Connection Status

Applications Currently Executing

Application Name	Instances	Application Account	References
Configuration	1	DARLINTA01\21cfr	2
ServerMonitor	1	DARLINTA01\21cfr	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.



PerkinElmer Enhanced Security Server

Query Help

PerkinElmer Enhanced Security Server version 2.0 started successfully.

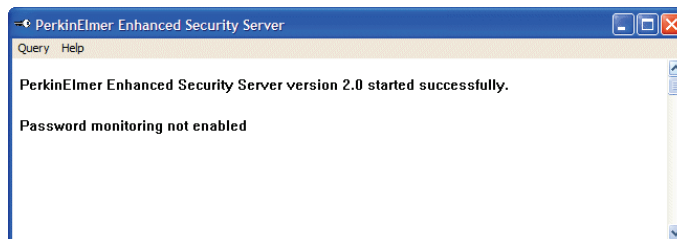
Logged On Application Users

User Name	Logon Count
DARLINTA01\21cfr	1

Passwords

This shows the Application account(s) password status.

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



PerkinElmer Enhanced Security Server

Query Help

PerkinElmer Enhanced Security Server version 2.0 started successfully.

Password monitoring 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 70 for details.

