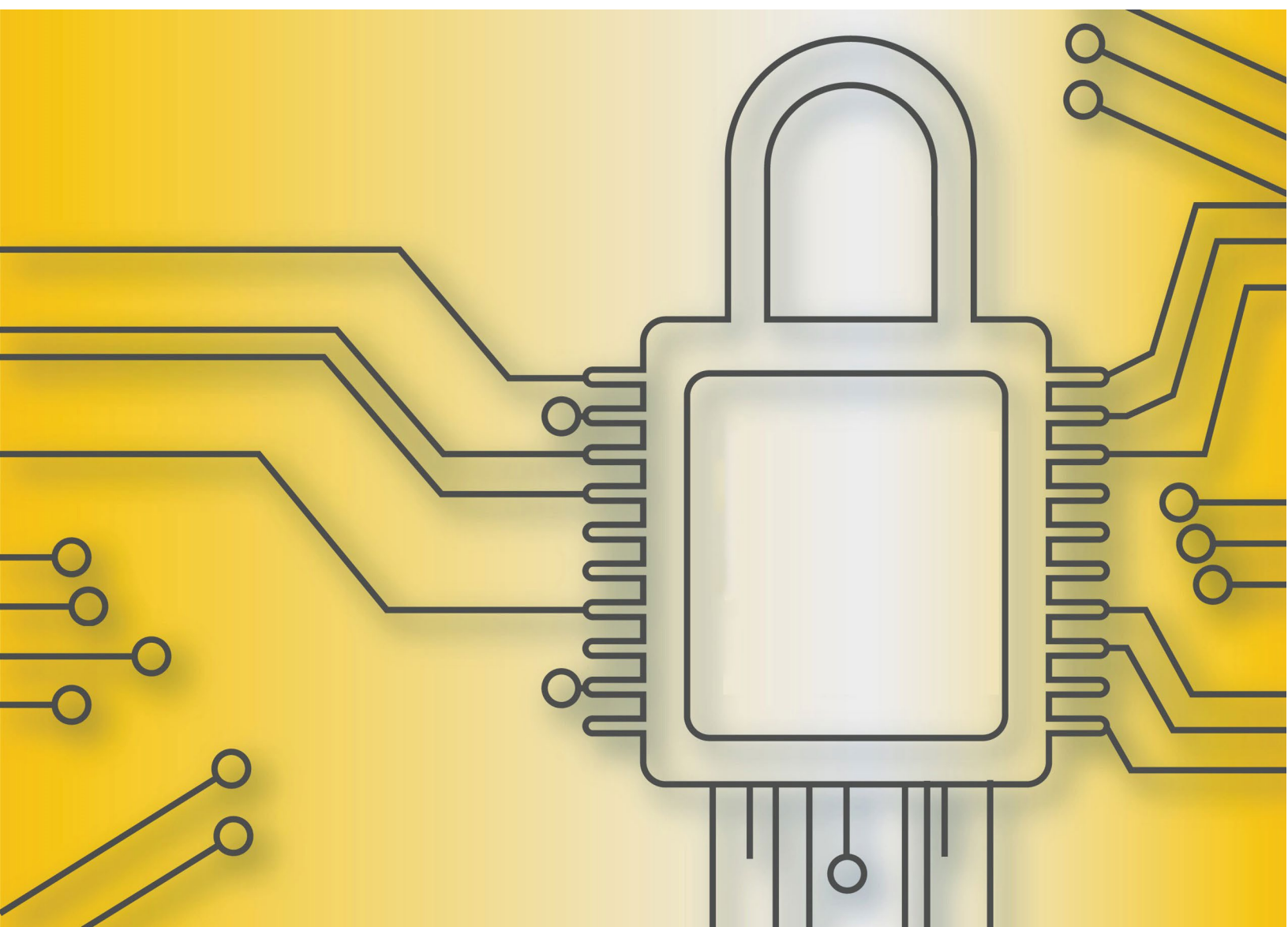




SecureVPE (Version 3) Software

User Manual



REPLIGEN CORPORATION

C Technologies Offices and Manufacturing Facility
685 Route 202/206 Bridgewater, NJ 08807 USA
International Telephone: +1 908-707-1009
International Fax: +1 908-707-1030
Email: analytics-support@repligen.com

The CTech™ Analytical Solutions homepage can be found at ctech.repligen.com

C Technologies, Inc. And/or its affiliates, to the extent allowed by law, disclaims, and in no event shall be liable for, any incidental or consequential damages in connection with user, instrument, or system performance in relation to all content contained in this document, including but not limited to fitness for location of use, specific purpose for use, or application.

© 2021 Repligen Corporation. All Rights Reserved. The trademarks mentioned herein are the property of Repligen Corporation or a Repligen affiliate, or their respective owners.

TABLE OF CONTENTS

1.	Background	4
2.	Introduction to SecureVPE	5
	2.1 Scope.....	5
3.	Approach to Achieving Compliance	6
4.	Glossary of Terms	7
5.	Installing/Upgrading the SecureVPE Software	8
	5.1 SecureVPE Application Pre-Installation & Verification	8
	5.2 Installing SecureVPE Software From Media.....	8
6.	Starting the SecureVPE Software	10
	6.1 SecureVPE and User Account Control Settings.....	10
7.	Enable SecureVPE Security Features	11
8.	Adding Users/Groups – SecureVPE Security Console	12
	8.1 Importing Domain User and Group Accounts into SecureVPE	13
9.	Working with Users and Groups	14
10.	Removing Domain User and Group Accounts From SecureVPE	15
11.	Global SecureVPE Settings	16
12.	Understanding SecureVPE Security Profiles	17
13.	Managing User and Group Permissions	18
14.	Secure Point Details by Application	18
15.	The Personalize Feature	25
16.	The Report Feature	26
17.	SoloVPE System Electronic Records (Batch Files)	27
18.	SoloVPE System E-Signatures	27
19.	SecureVPE Audit Logs	29
20.	Achieving Compliance – Considerations & Best Practices	32
21.	A Simple Three-Step Restricted Path Example Process	33
22.	SoloVPE Administration Program	33
	22.1 SoloVPE Administration - VPE System Service.....	33
	22.2 SoloVPE Administration - Device	34
	22.3 SoloVPE Administration - Solo	35
	22.4 SoloVPE Administration - Vessel.....	40
	22.5 SoloVPE Administration – UI Options	40
	22.6 SoloVPE Administration – Data Stores.....	40
	22.7 SoloVPE Administration – Licensing.....	41
23.	General Troubleshooting	42
24.	Getting Help	43
25.	Security Guidance for windows settings	44
26.	Notes	45

1. BACKGROUND

A successful implementation of the SoloVPE system requires a complete understanding of the capabilities of the Software. A complete understanding of the Software requires a comprehensive appreciation of the infrastructure of the Software environment. The SoloVPE Software platform is constructed from two major components:

1. The computer operating system: *Microsoft Windows®*
2. The variable pathlength application: *C Technologies, Inc. SoloVPE™ Software*

These two core components work cooperatively to create a complete interface for command and control of the SoloVPE hardware. User accounts and groups are controlled and maintained by the responsible IT function at the Operating System and/or Domain level.

For secured implementations of the SoloVPE System, C Technologies, Inc. recommends the implementation of the optional security module:

SecureVPE (C Technologies, Inc.)

The use of the SecureVPE module in conjunction with the security capabilities of the network environment and the workstation operating system creates a powerful yet flexible set of security tools. This collection of security features provides the individual or group assigned the task of implementing a secured system to achieve compliance. Compliance is achieved when the configuration of the Software works in conjunction with the organizations' policies and procedures while utilizing SecureVPE. Though a formal, independent certification of Software compliance does not exist, the security features of the SoloVPE System have demonstrated compliance through implementation efforts by multiple organizations around the world.

This document includes detailed information regarding how these components and the module work together, specific roles they each play, examples, and options of how they can be implemented to help companies achieve the desired level of security.

2. INTRODUCTION TO SECUREVPE

The SecureVPE Software package is an optional companion product for the SoloVPE Software. SecureVPE has been written to give users the tools needed to achieve compliance with their company and regulatory requirements.

Features in SecureVPE include:

- Windows 7/10 (32 and 64-Bit compliance)
- Eliminating dependence on the Agilent's Cary WinUV GLP Administration application
- Simplified User Interface
- Windows Active Directory Connection for Users and Groups
- Event Driven eSignatures
- User/Group Personalization Features
- Eliminating Microsoft Access® Runtime Architecture
- Secure Access Points for SoloVPE Software, SecureVPE Software, and SoloVPE Administration Software

The biggest change made in the SecureVPE V3 Software compared with V2 is the elimination of dependence on the *GLP Administration* application provided with Agilent's Cary WinUV Software suite. Prior implementations (Pre-V3) of SecureVPE depended on the Cary WinUV GLP Administrator application for User and Group maintenance, resulting in additional configuration and maintenance along with more burdensome administration. With the elimination of GLP Administrator, the new system architecture links directly to the Windows Active Directory data store for User and Group data at both the local machine and the domain level. This new active directory link allows single-user and group policies, password policies (complexity, aging, expiration, failed login attempts and lockout, etc.), and related local policies to be administered by the organization's IT and administrative staff. This provides customers with flexibility to craft policies, restrictions, and enhanced auditing options as is deemed necessary or appropriate for their organization.

Since company policies and protocols vary, it is important that customers fully understand the features and capability provided by the system. This manual is intended to provide a broad overview of the Software tools available to allow customers to fully understand the options that exist. Since many of the key features are controlled at the domain and workstation level, the involvement of Administrative IT staff on the implementation team is strongly recommended.

2.1 SCOPE

The V3 SecureVPE Software was released with the 3.0.159.0 software build. The software is compatible with 3.1.XXX.0 software builds as well as every version that was released in between the previously mentioned software versions.

3. APPROACH TO ACHIEVING COMPLIANCE

Compliance is achieved through the proper use of the security tools provided by the SoloVPE system. These tools must be used in combination with robust organizational policies. Standard operating procedures are training guidelines to create the necessary layers of security and achieve compliance with company and regulatory requirements. The various layers of security include network security (if applicable), workstation operating system security (login and file system), physical security and proper configuration of the SecureVPE Software package. No one tool or layer of security can provide every facet of required security. Each layer and feature must work together to deliver robust security. A Software product cannot be deemed compliant because it is one element of an overall system that includes policies, training, procedures, Software and ongoing proper use.

When properly implemented, these security tools provide a comprehensive way to control and log Software access, grant specific permissions, enforce eSignatures and secure file output. A global administrator or team of administrators need to establish the unique user and group identifications, set the Workstation, Domain and NTFS permissions, and implement appropriate local and group policies to achieve compliance. Since no two organizations have identical requirements and protocols it is up to the specific organization to design and properly implement a security scheme that achieves the required level of compliance using the tools provided. For more information on implementation, please see the Getting Help section 24 of this manual.

4. GLOSSARY OF TERMS

The following terms are defined as they refer to the SecureVPE Software package:

- **Administrator** – An individual with unlimited permissions to a device and/or Software application who facilitates the installation and configuration of the overall security plan.
- **Audit Trail** – A historical record of actions or events that takes place within the Software.
- **Cary WinUV** – Agilent’s suite of spectroscopy applications that are used to run the Cary series of spectrophotometer instruments.
- **Group ID** – A name for a collection of User ID’s that are related to each other through common attributes such as organization, authority, permissions etc.
- **Personalization** – A specific parameter in the SecureVPE Software that can be specified at the User/Group ID level.
- **Security Profile** – The complete list of permissions by Secure Point for a specific User ID or Group ID.
- **Secure Point** – A specific function, feature or object in the VPE Software environment for which access/authorization can be granted or revoked by User ID or Group ID as part of an overall security plan.
- **SecureVPE** – A Software application that is used to configure the added layer of security for VPE products beyond the Windows operating system.
- **User Account Control (UAC)** – A security infrastructure introduced with Microsoft Windows® to improve security. This is done by limiting software application to standard user privileges until an administrator authorizes an increase or elevation.
- **User ID** – A unique identifier for an individual that can be secured using password protection and permissions profiles with respect to a network, computer, or Software application.
- **VPE** – Variable Pathlength Extension product line.

5. INSTALLING/UPGRADING THE SECUREVPE SOFTWARE

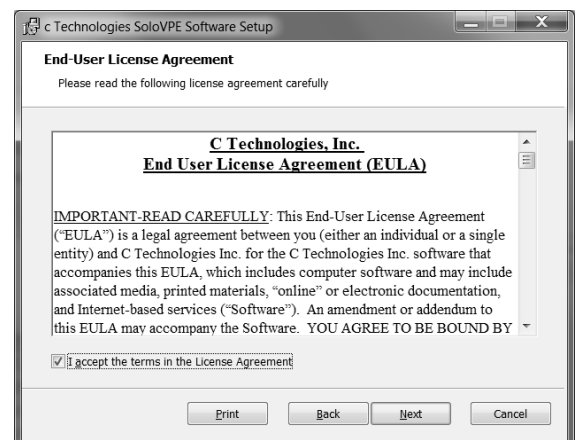
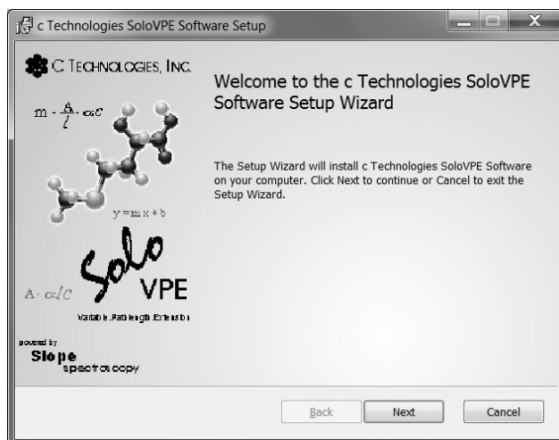
5.1 SECUREVPE APPLICATION PRE-INSTALLATION & VERIFICATION

Computers provided by C Technologies frequently have the SecureVPE Software pre-installed. To verify if the computer has SecureVPE installed and activated, click “**Windows Start Menu**” and type “**SecureVPE**” in the “*Search programs and files*” to find the application or view “*All Programs*” and browse to find the “*C Technologies*” program group which contains the shortcut to launch SecureVPE. Selecting the SecureVPE icon will run the Software, if the Software is not licensed, a message notifying you of the license status will appear. For questions about Software licenses please contact the Solo Service group at 908-707-1201 or your Authorized Service Provider.

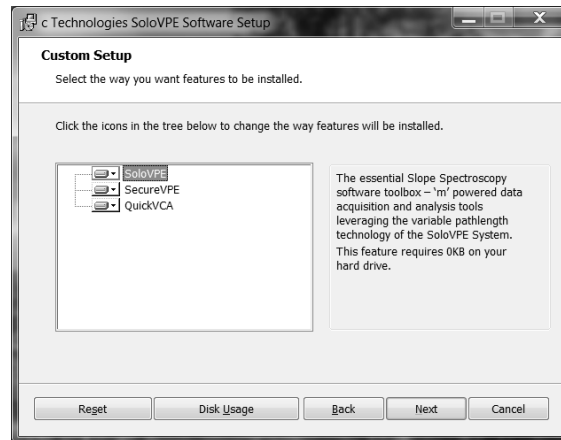
5.2 INSTALLING SECUREVPE SOFTWARE FROM MEDIA

The SecureVPE Software can be installed from the media (disc, flash drive, etc.) provided by a System Administrator or a user with Administrative privileges to the computer. The following procedure provides step by step guidance for installing SecureVPE on the SoloVPE computer system. **NOTE: It is strongly recommended that this installation is performed by or under the guidance of a trained SoloVPE Support Technician and if SecureVPE was not pre-installed by C Technologies, Inc.**

- 1) **Pre-Installation Steps:** Prior to installing the SecureVPE Software, the following conditions must be confirmed:
 - a. The SoloVPE Software Suite must be installed prior to or during the installation process.
 - b. Windows Update should have properly updated the Windows operating system.
 - c. The UAC must be set to “Default” or higher.
 - d. The SecureVPE Software package is typically pre-installed on SoloVPE Systems. If unsure of the system configuration please contact a SoloVPE representative or C Technologies, Inc.
- 2) **Insert Media:** To begin the installation process, insert the SecureVPE media (e.g. CD, DVD or USB Flash) into the SoloVPE system computer.
- 3) **Browse the Media to Find the SoloVPEPackage.exe File:** Use the My Computer applet or Windows Explorer browser for the SecureVPE installation media and locate the **SoloVPEpackage.exe** program. Double-click the **SoloVPEPackage.exe** file to begin the installation. Press the **Next** button to advance the installation process.
- 4) **End-User License Agreement:** Review and accept the terms of the license agreement. Press the **Next** button to advance the installation process.



- 5) **Setup:** From the Custom Setup screen, select SecureVPE to be installed on the device. Press the **Next** button to advance the installation process.



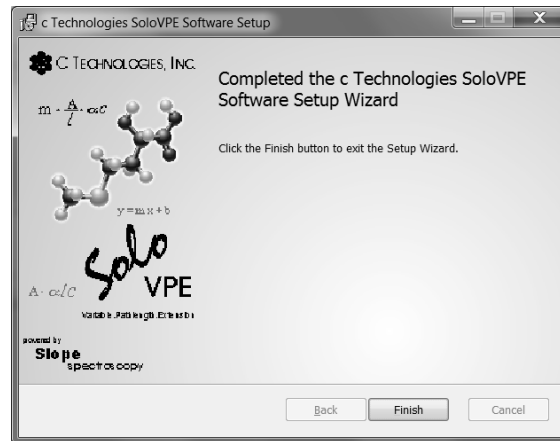
- 6) **Ready to Install:** The Software should now be properly configured for installation. Press the **Install** button to continue the installation process.



- 7) **Copy Files:** The installation will continue with files being installed to the system and the application being registered in Windows.



- 8) **Complete Installation:** Click **Finish** to complete installation. Please contact SoloVPE Service Direct for instructions on how to license the software for use. License registration is required to use the SecureVPE Software.”



6. STARTING THE SECUREVPE SOFTWARE

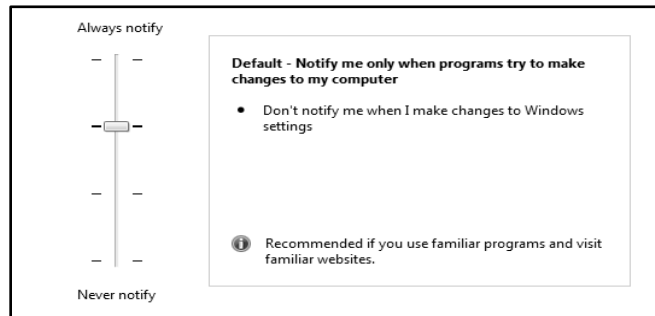


The SecureVPE icon will be visible on the Desktop and available in the C Technologies program group. Start the SecureVPE Software using one of the shortcuts provided. SecureVPE works in conjunction with the UAC Windows environment. This means that Local Administrator accounts and non-Local Administrator accounts can run the Software. Only Local Administrator accounts can have access to the Software if the UAC is set to “Default” or higher. In this case, when a non-local Administrator account is logged in, the attempts to run the Software will cause a prompt for elevated credentials to appear to prevent unauthorized use. However, if the UAC is set to “Never Notify,” Local Administrator accounts and non-Local Administrator accounts may have access to the Software. (See SecureVPE and User Account Control Settings).

6.1 SECUREVPE AND USER ACCOUNT CONTROL SETTINGS

The UAC functionality in Windows enhances security and protects user from the vulnerabilities associated with viruses and malware. The UAC makes it difficult for unauthorized users to change critical settings or gain control of the Windows and installed Software. The UAC is set at the workstation level, not by User Account or Group Account. The SoloVPE Software has been designed and built to leverage this powerful security feature. The UAC will prevent unauthorized changes to critical settings of the SoloVPE Software and computer system.

The UAC makes it possible to restrict and to run processes with different credentials. Most notably, UAC secured programs will require elevated credentials to be run. If the UAC has been set to “Default” or higher, users that have been designated as local or network Administrators will be able to run UAC secured programs such as SecureVPE and the SoloVPE Administration programs. Local Administration rights can be controlled by Network Administrators at the workstation level. When logged into the workstation, even Local Administrators will see a prompt alerting them to the fact that they are accessing a secured application. If the UAC has been set to “Default” or higher, users without Local Administrator rights will be prompted to enter elevated credentials to gain access to the Software. C Technologies has developed secure points to allow SecureVPE to function in an environment when the UAC is set to “Never Notify”. In this case, non-Local Administrator accounts can be configured to have access to secure programs.



C Technologies recommends that the UAC be set to Default on workstations running the SoloVPE Software with SecureVPE to fully

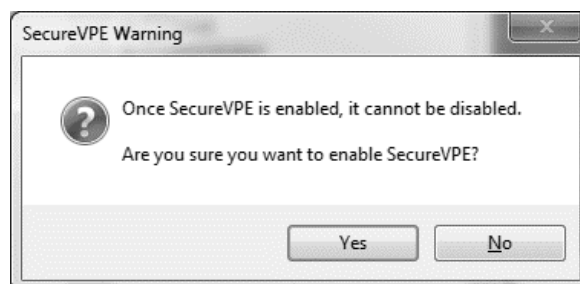
secure their SoloVPE System. Network Administrators should control the UAC setting through the interface provided in Windows under the Control Panel where User Accounts are maintained. **If UAC is turned on this point can only be accessed by the system admin. If UAC is turned off this point will need to be enabled to allow for use.**

7. ENABLE SECUREVPE SECURITY FEATURES

The security features of SecureVPE are disabled by default at the time of installation. SecureVPE must be enabled by an Administrator when the decision is made to go live with the enhanced security features of the system. SecureVPE has been designed to allow Administrators to configure users, groups, and permissions prior to enabling it. It is important to note that once SecureVPE has been enabled, it cannot be disabled. This is an irreversible action.

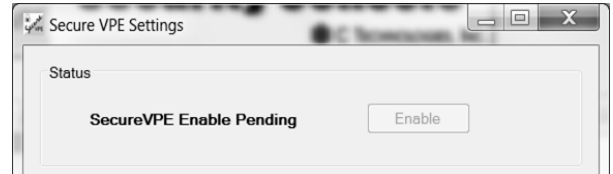
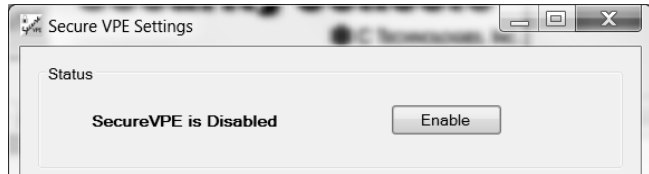


NOTE: By Default the SecureVPE Software is disabled, users can find out if the SecureVPE is enabled or disabled by viewing at the bottom of the SecureVPE Security Console. Once ENABLED, it cannot be DISABLED.



To enable SecureVPE, follow these steps:

- 1) Press the **Settings** button in the SecureVPE application window to open the SecureVPE Settings screen.
- 2) In the Status field, press the **Enable** button to arm the Software. Confirmation will still be required to commit the change. While the Enable action is pending it is still possible to abort the change by pressing the “Cancel” button in the SecureVPE Settings window.



- 3) Press the **OK** button to continue. A SecureVPE Warning will appear asking for confirmation that *SecureVPE* is to be enabled. Press **Yes** to Enable SecureVPE or **No** to abort this change.
- 4) After enabling the security features of SecureVPE, the status will continue to appear in the Status Bar at the bottom of the SecureVPE window.



8. ADDING USERS/GROUPS—SECUREVPE SECURITY CONSOLE

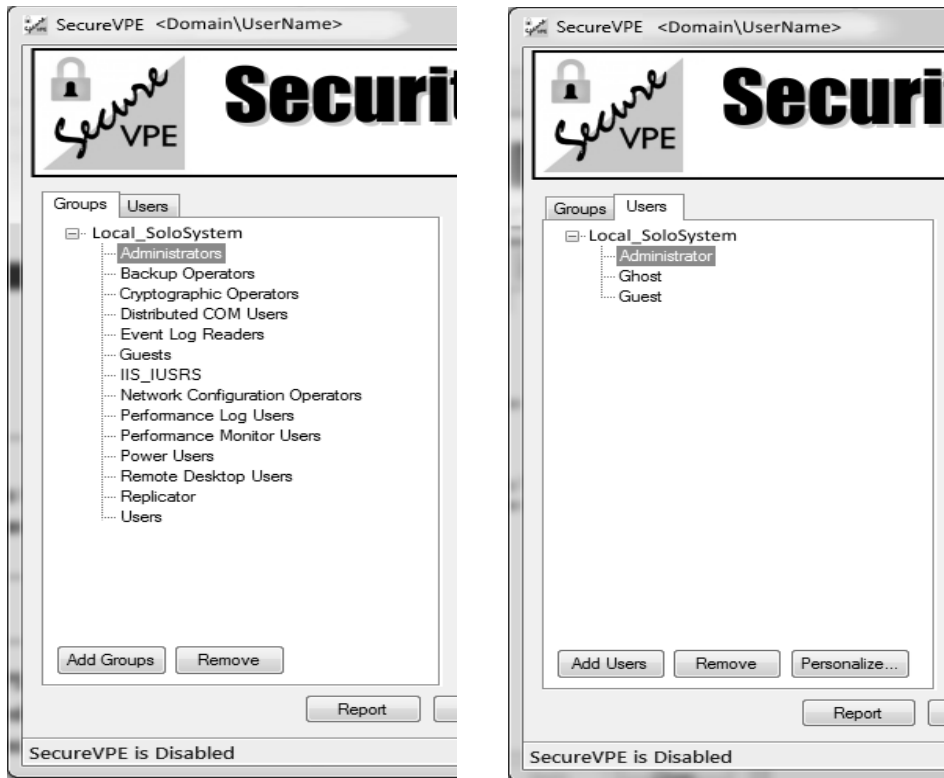
The Active Directory link allows Administrators to leverage familiar and powerful tools for managing users, groups, and passwords. *All the power and flexibility of Local and Group Policies to implement security structure that meets the needs of the organization.* It is important to include IT/Network Administration professionals as part of the implementation team to ensure a proper design plan is developed and properly configured at all layers of security infrastructure.



NOTE: *Users and Groups cannot be created or deleted in the SecureVPE environment.*

- ***Local Machine Users and Groups are pre-populated to SecureVPE by default.***
- ***Domain Users and Groups must be imported into SecureVPE***

When the SecureVPE application starts, it opens to the Security Console window. The Security Console is used to manage imported Users and Group and to create security profiles by granting and revoking rights to the various Secure Points available in the Software. When SecureVPE starts for the first-time the Users and Groups Tabs in the Security Console will display the Local Computer Name. Clicking the [+] sign to the left of the Computer Name will expand the list to show Local Users and Local Groups on each respective tab. Only the local objects are displayed because those are the only ones that are always available in Windows data store, whether the local machine is or is not connected to a network domain.



SecureVPE makes it easy to import Users and Groups from a connected Network Domain once the computer is connected to a network drive. The procedure for importing Users and Groups will be very familiar to Network Administrators. SecureVPE leverages the existing tools and techniques available in the Windows operating system and server Software. After the IT Administrator has connected the SoloVPE computer to the network domain, Users and Groups can be imported.

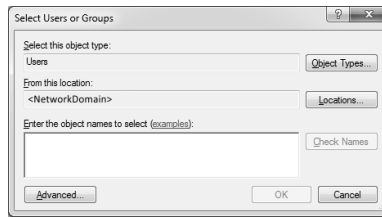
8.1 IMPORTING DOMAIN USER AND GROUP ACCOUNTS INTO SECUREVPE

1. Open the SecureVPE to display Security Console window by double-clicking from the Desktop shortcut or clicking the C Technologies Program Group icon.

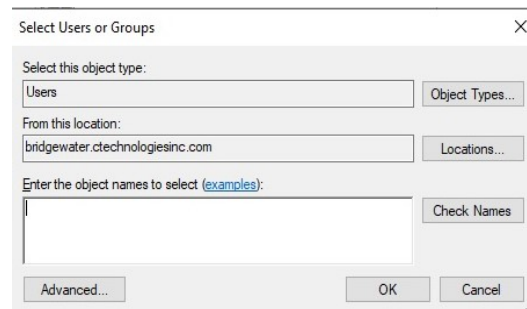


2. If the UAC is set to Default or higher you will be prompted to enter the credentials for a Local Administrator and acknowledge the security notification.
3. Select the **Users** tab.

4. Press the **Add Users** button at the bottom of the Users tab to display the **Select Users or Group** window.



5. Type either the User Name or Display Name of the account that you wish to import into SecureVPE and then press the **Check Names** button.
- 5.1 If the system finds the specified user account in the Active Directory collection then the fully resolved name will appear underlined in the form.
 - 5.2 If the information entered cannot resolve to a valid User account, the Name Not Found window will appear and provide an opportunity to correct the information or to search another way.
 - 5.3 Clicking the **Advanced** button opens a form that provides more flexible search options.



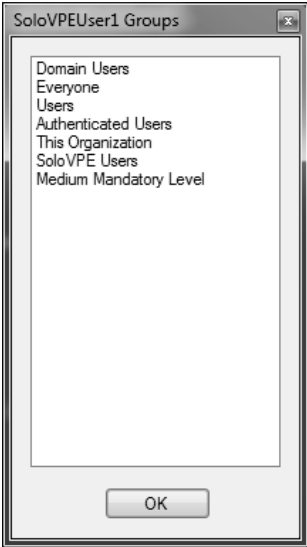

- 5.4 Once the desired User Account has been successfully found, press the **OK** button to import the User account into the SecureVPE environment. The User Name will appear under a Domain group in the Users tab



NOTE: The procedure for adding Groups is similar to the procedure for adding Users. Simply use the Groups Tab and the Add Groups button. The Select Users and Group window is the same but they are filtered for the different object types.

9. WORKING WITH USERS AND GROUPS

Network configurations can vary greatly from organization to organization based upon the size and sophistication of each company's IT architecture. This is one of many reasons why an IT Specialist / Administrator should be part of any secured SoloVPE Implementation team. A few helpful features have been included in the Software to make it easier to work with the User and Group objects.

Group Browser	User Browser
<p>The Group Browser feature provides an easy way to see the Groups to which a User belongs. Simply select a User from the <i>Users</i> tab (either Local Machine or Domain User) and double-click the User Name. The list of Groups to which that User belongs will appear in a pop-up window. Press the “OK” button to close the <i>Group Browser</i>.</p>	<p>The User Browser feature provides an easy way to see the Users that are members of a specific Group. Simply select a Group from the <i>Groups</i> tab (either Local Machine or Domain Group) and then double-click the Group Name. The list of Users that are members of the group will appear in a pop-up window.</p>
	
<p>Important: Depending on the size of the organization and the complexity of the Group and User Memberships, it may take a few seconds for the <i>User Browser</i> to appear. Press the “OK” button to close the <i>User Browser</i>.</p>	

The security profiles created in SecureVPE can be built at the User and/or the Group level. This can become a bit confusing and result in some unexpected behaviors when Users belong to multiple groups or security profiles existing at both the User and the Group level. To try and prevent these issues or help investigate them, SecureVPE includes both a Group Browser and User Browser feature.

10. REMOVING DOMAIN USER AND GROUP ACCOUNTS FROM SECUREVPE

The User and Group objects are created and maintained at the operating system and network domain level. There are limitations to the types of actions that can be taken in SecureVPE. For example, the Local Machine Users and Groups that appear on the respective tabs in SecureVPE cannot be removed from SecureVPE. If they exist on the Local Machine they will appear on these tabs. User and Group creation and deletion can only occur in their respective context (Local Machine or Network Domain).

Network Domain Level User and Group accounts that have been previously imported into SecureVPE can be removed from the SecureVPE environment. It is important to note that this does not delete or remove the account or any network privileges from the *Active Directory* data store. The “remove” action effectively revokes all SoloVPE Software permissions, deletes the associated security profile, and will n appear in the SecureVPE environment.

To remove a User or Group account from the SecureVPE environment, simply select the User or Group to be removed and press the **Remove** button at the bottom of the tab. A confirmation dialog will appear. To confirm the remove action, click **Yes**. To abort the remove action, click **No**. The User or Group security profile will be removed once the object is removed and the User and/or Group members will no longer have access to the SoloVPE Software.



NOTE: Users and Groups Objects CANNOT be deleted or modified from the Local Machine or a Network Domain using features in SecureVPE. SecureVPE merely connects to or disconnects from these objects which are created, managed and controlled by authorized Administration Personnel.

11. GLOBAL SECUREVPE SETTINGS

There are a few SecureVPE Global Settings that can be controlled from the SecureVPE Settings screen which is accessed by pressing the “Settings” button in the Security Console window. The most significant global setting is whether SecureVPE is Enabled or Disabled. The other settings are as follows:

Name	Value
LoginAttemptsAllowed	3
ESignatureAttemptsAllowed	3
ESignReasonRequired	True

- Datastore Location:** This setting indicates where the encrypted database file that stores the Security Profiles, Audit History, and Settings in SecureVPE is located. It is controlled by the system and cannot be changed in V3. It is recommended that this file be backed up routinely as part of the overall security plan and that the Network Administrator secure the file and folder to prevent unauthorized tampering or deletion. However, it is important to note that the system must be able to modify this file for proper functioning.
- LoginAttemptsAllowed:** This setting controls how many unsuccessful logins tries can be made during Perimeter Authentication before the system will lock.
- ESignatureAttemptsAllowed:** This setting controls how many unsuccessful E-Signature tries are allowed before the system will be forced into E-Signature Override mode.

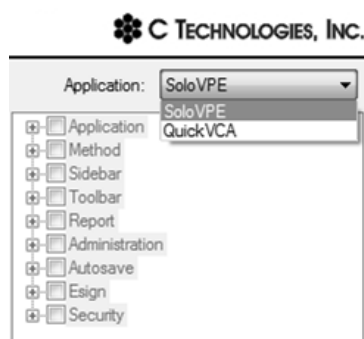
- d. **EsignReasonRequired:** This setting controls whether a “Reason” entry is required when an E-Signature is being executed.

In the event of a lock, an Administrator will have to enter their credentials to unlock the user.

12. UNDERSTANDING SECUREVPE SECURITY PROFILES

SecureVPE is the tool to control access to the SoloVPE and QuickVCA applications and features. Access is controlled by the User and/or the Group level through customizable Security Profiles. Security Profiles are created and managed using the Security Console window in SecureVPE. Only Local Administrators can access SecureVPE if the Windows UAC is set to “Default” or higher. Alternatively, the UAC must be set to “Never Notify” and permissions must be set within SecureVPE for non-Local Administrators to have access to SecureVPE Software.

Members of the Administrators group on the Local Machine can have User accounts on either the Local Machine and/or from a Network Domain. It is also possible to add entire Groups to the Local Administrators group. It is important to have experienced Network Administrators make these changes to ensure the User and Group design is implemented properly.



Security Profiles are created through two primary mechanisms in SecureVPE:

1. Granting permission to specific Secure Points available in the Software
2. Optionally setting User personalization's by using the Personalize feature

Secure Points are discrete features in the SoloVPE and QuickVCA Software that can be enabled or disabled by toggling permissions in SecureVPE. SecureVPE provides customers with the ability to control access to critical aspects of the system to achieve compliance. Available Secure Points will vary by application and are categorized into groups of related items in the Security Console for ease of use. The Security Console displays an Application drop-down list box allowing Administrators to toggle between the Secure Points of the SoloVPE Software and the QuickVCA Software.

Secure Points can control various aspects of the Software behaviors. A successful implementation requires that Administrators fully understand the details of each Secure Point to make sure it is used or not used in their security plan. A detailed list of all Secure Points, what they control, and recommendations for use are included in this manual. Please reference **KB16008 - VPE Software V3 - Security Configuration Windows 7-32-64 Cary WinUV Version 5** for additional Windows NTFS File configuration assistance.

It is important to note that security features in the Software consider all applicable Security Profiles when enforcing behaviors. It is possible that a Security Profile can be created for a specific user and that Security Profiles can be created for one or more Groups to which that User belongs as a member. When the system evaluates these collections of Secure Points it does so optimistically meaning, if a Secure Point is enabled in ANY of the applicable Security Profiles, the Secure Point will be enabled in the Software.

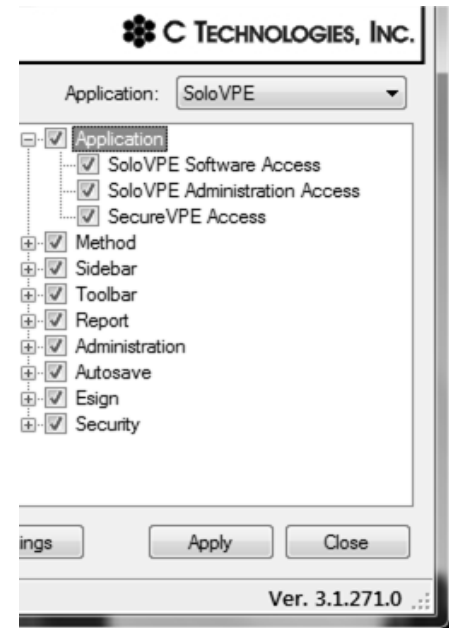
The optional Personalize feature is the final aspect of a complete Security Profile. Personalization is not required. It provides some user-specific parameters that can be controlled if a company decides that they should be included as part of the overall security plan. It is important to note that Personalization applies only at the User level and cannot be applied to Groups.

NOTE: If a Secure Point is Enabled in ANY of the Security Profiles or Group(s), applicable to a logged in user, the Secure Point will be Enabled for that User.

13. MANAGING USER AND GROUP PERMISSIONS

Security Profiles give Administrators control over the appearance of the Software interface and the features to which users have access to. The Security Console makes it very easy to configure Security Profiles by User and by Group. Enabling or disabling secure points in SecureVPE is as simple as selecting the Application, selecting the User or Group, and then clicking the appropriate checkbox Control

1. A User or Group object must be selected when toggling Secure Points. Actions taken apply only to the selected object.
2. When working with a specific Application (e.g. SoloVPE or Quick VCA), you must apply changes before you switch between the applications.
3. Changes are stored temporarily in the Software until the **Apply** button is pressed to implement the changes.
4. Closing the Software without pressing the **Apply** button discards the changes. The Software will notify the Administrator if changes are pending at the time the Software attempts to close.
5. All committed changes are logged in the SecureVPE Audit Trail.
6. You can quickly Enable all Secure Points by pressing Ctrl+A. You can quickly Disable all Secure Points by pressing Ctrl+D. You can enable or disable entire Groups of Secure Points by clicking the checkbox control at the top level of the Secure Point grouping.



Checking a Secure Point enables the security feature. Unchecking a Secure Point disables that security feature. It is important to note that all secure points are affirmative. Unchecking the secure point does not constitute a denial of that security feature. This means that when a User is active in multiple groups at the User level or based upon various Group memberships, an enabled Secure Point in any of the applicable Security Profiles means it will be enabled for that user.

14. SECURE POINT DETAILS BY APPLICATION

The following tables contain the security checkpoints associated with the SoloVPE Software. User access or authority is assigned by checking and unchecking permission on each secure point. This extra layer of security is application-specific to the installed VPE applications. The detailed list of available Secure Points by the application is presented in the following table.

SoloVPE Secure Points		
Group	Secure Point Name	Detailed Description & Guidance
Application	<i>SoloVPE Software Access</i>	Controls whether access to the SoloVPE software is allowed. This Secure Point is useful for permanently or temporarily preventing access to the SoloVPE software.
	<i>SoloVPE Administration Access</i>	Controls whether access to the SoloVPE Administration software is allowed. This Secure Point is useful for permanently or temporarily preventing access to the SoloVPE Administration software. UAC must be enabled
	<i>SecureVPE Access</i>	Controls whether access to the SecureVPE software is allowed. This Secure Point is useful for permanently or temporarily preventing access to the SecureVPE software. UAC must be enabled
Method	<i>Method Modification Rights Enabled</i>	Controls whether the users can create or modify methods using the various screen controls in the SoloVPE Software. Users for whom this Secure Point is disabled are prevented from creating or modifying methods but they can open existing methods and initiate data collection.
	<i>Advanced Setting Access Enabled</i>	Controls access to the Advanced screen and controls that are used to set parameters that control system operation at a more detailed level than the standard controls and parameters on the main software screens. Advanced parameters should generally only be used by more experienced individual involved with the development and validation of new methods.
	<i>DAQ View Enabled</i>	Controls whether the limited and compact Data Acquisition View of the Quick Slope feature is turned on and available for use. DAQ View is useful for limiting users to running existing Quick Slope methods in a simplified interface. It is not possible to create or modify methods in DAQ View.
	<i>DAQ View Optional</i>	Controls whether access to both the Data Acquisition View and the Full Quick Slope window is possible. When DAQ View is enabled and the DAQ View Optional is disabled, the user will ONLY have access to the DAQ View window of Quick Slope and not the full Quick Slope window. This is useful for Administrators and Method Developers to test and validate methods prior to deploying them to a DAQ View focused user group.
	<i>Quick Methods Enabled</i>	Controls whether the Quick Methods selector is visible in the Quick Slope feature. When Enabled the selector will be visible in both the DAQ View window and the full Quick Slope window. Quick Methods are useful for method developers but will have limited utility in tightly controlled method specific implementations.
	<i>Force Disable QSlope Alerts</i>	Controls whether the Quick Slope Alert Messages (e.g. Pathlength Shifted Up, Pathlength Shifted Down, High Abs, Low Abs, Low R ² etc.) are disabled. This notification is meant to give users important system information.
	Report	<i>Report Sidebar Button</i>
<i>Manual Sidebar Button</i>		Toggles visibility of the Manual button on the SoloVPE Sidebar controlling access to the SoloVPE Manual Control features.
<i>Section Sidebar Button</i>		Toggles visibility of the Section button on the SoloVPE Sidebar controlling access for users to create Section (Abs. vs. Pathlength) data from Spectral (Abs. vs. Wavelength) data.
<i>Analyze Sidebar Button</i>		Toggles visibility of the Analyze button on the SoloVPE Sidebar controlling access to the Section Data analysis tools available in the Analyze window.
<i>Quick Survey Sidebar Button</i>		Toggles visibility of the Quick Survey button on the SoloVPE Sidebar controlling access to generate spectral data for a broad wavelength and pathlength sampling. This is useful for characterizing unfamiliar samples.
<i>Quick Slope Sidebar Button</i>		Toggles visibility of the Quick Slope button on the SoloVPE Sidebar controlling access to rapidly acquiring Section data and making concentration measurements.
<i>Admin Sidebar Button</i>		Toggles visibility of the Admin button on the SoloVPE Sidebar controlling access to SoloVPE Administration program. The Admin button is effectively a shortcut to the SoloVPE Administration program like a Desktop of Start Menu shortcut. This Secure Point does not control access to the SoloVPE Administration, that is governed by the UAC feature, however, this provides quick access for Administrators that would require it.

	<i>EC Library Sidebar Button</i>	Toggles visibility of the EC Library button on the SoloVPE Sidebar quick access to the Extinction Coefficient Library application which is a standalone program accessible from the <i>Start Menu</i> . This Secure Point merely controls availability of the sidebar button, not access to the program itself. The ability to make changes to the EC Library data is controlled by a separate Secure Point.
	<i>Home Sidebar Button</i>	Toggles visibility of the Home button on the SoloVPE Sidebar controlling access to the command that sends the SoloVPE to the Home (Position / Fibrette loading position)
	<i>New Run Sidebar Button</i>	Toggles visibility of the New Run button on the SoloVPE Sidebar controlling User ability to clear both data and the report that is currently resident in the software.
	<i>Save Data Sidebar Button</i>	Toggles visibility of the Save Data button on the SoloVPE Sidebar controlling User ability to manually initiate a controlled Save Data event from the environment.
Toolbar	<i>Factor Scale Toolbar Button</i>	Toggles visibility of the Factor Scale button on the SoloVPE Toolbar controlling access to the graph scaling feature that forces the graph to display the entire selected trace from an ordinate value of zero.
	<i>Clear Rectangles Toolbar Button</i>	Toggles visibility of the Clear Rectangles button on the SoloVPE Toolbar controlling access to the feature that quickly removes the shaded bars Quick Slope uses to highlight the Slope optimization actions it takes.
	<i>Slope Tool Toolbar Button</i>	Toggles visibility of the Slope Tool button on the SoloVPE Toolbar controlling access to compact Slope Analysis tool that allows users to interrogate their data in inquiry mode.
	<i>Arrange Graph – VT Button</i>	Toggles visibility of the Arrange Graph – Vertical/Top button on the SoloVPE Toolbar controlling access to the feature that positions the current set of graphs. The <i>selected</i> graph is displayed prominently at the top of the graphics region with the unselected graphs distributed in a row across the bottom.
	<i>Arrange Graph – HL Button</i>	Toggles visibility of the Arrange Graph – Horizontal/Left button on the SoloVPE Toolbar controlling access to the feature that positions the current set of graphs. The <i>selected</i> graph is displayed prominently at the left side of the graphics region with the unselected graphs distributed in a column to the right.
	<i>Arrange Graph – VB Button</i>	Toggles visibility of the Arrange Graph – Vertical/Bottom button on the SoloVPE Toolbar controlling access to the feature that positions the current set of graphs. The <i>selected</i> graph is displayed prominently at the bottom of the graphics region with the unselected graphs distributed in a row across the top.
	<i>Arrange Graph – HR Button</i>	Toggles visibility of the Arrange Graph – Horizontal/Right button on the SoloVPE Toolbar controlling access to the feature that positions the current set of graphs. The <i>selected</i> graph is displayed prominently at the right side of the graphics region with the unselected graphs distributed in a column to the left.
	<i>Volume Calculator Toolbar Button</i>	Toggles visibility of the Volume Calculator button on the SoloVPE Toolbar controlling access to simple utility that lets users explore the relationship between the selected sample vessel, measurement pathlength and sample volume required to ensure that Fibrette remains in the sample during the run. Additional volume is never an issue and should be used when available.
	<i>Manual eSignature Toolbar Button</i>	Toggles visibility of the Manual eSignature button on the SoloVPE Toolbar controlling access to the feature that allows users to manually initiate eSignature events. When eSignatures are enabled it is important this button be accessible to make it easy to complete review and approval eSignatures which are not governed by software events.
	<i>Quick Check Toolbar Button</i>	Toggles visibility of the Quick Check button on the SoloVPE Toolbar controlling access to the Quick Check diagnostic utility that is useful for monitoring the help and cleanliness of the SoloVPE system. It is recommended that all users have access to this utility because it is a very useful verification check that can be run daily, weekly or in the event of troubleshooting action.
		<i>Plugins Enabled</i>
Report	<i>Report Modification Rights Enabled</i>	Controls whether the logged in user can make edits to the content in the report window in the SoloVPE software environment. It is recommended that Report Modification rights be denied for all users including Administrators, since the Agilent WinUV environment has no provisions for logging changes to report content.
	<i>QSlope Report Options Enabled</i>	Controls whether the logged in user can make changes to the configuration of the Quick Slope report using the report options that are available under the <i>Advanced</i> button in the Quick Slope window

Administration	<i>Measurement Continuation Allowed</i>	Controls whether the logged in user can continue performing sample measurement with the same sample and Fibrette after the first sample collection is complete. Once pressed “Done” in the Quick Slope screen the user will get a prompt confirming whether to continue taking measurement or go back to home position. If this option is set to “no” the system will automatically send the Fibrette to the Home position.
	<i>Set Zero Allowed</i>	Controls whether the logged in user has the authority to change/set the Zero Step Position in the Manual Control window of the SoloVPE software. This Secure Point does not impact the ability of a user to change the Zero Step Position in the <i>SoloVPE Administration</i> program, because access to that program is limited to Local Administrators via the UAC feature.
	<i>Quick Check Administrator Access</i>	Controls whether the logged in user has the authority to make changes to the Quick Check parameters accessible through the <i>Advanced</i> button in the Quick Check window. It is recommended that these settings be determined and set during the implementation process and then access can be limited to the system administrator(s).
	<i>Optimize Coupler Access</i>	Controls whether the logged in user has the authority to run the Optimize Coupler utility in the Manual Control window of the SoloVPE software.
	<i>Set Zero Wizard Access</i>	Controls whether the logged in user has the authority to run the Set Zero Wizard utility in the Manual Control window of the SoloVPE software. This application walks users through setting the zero position of the system. Not recommended and should only be accessed by trained Solo technicians or under C Technologies guidance.
	<i>Manual Limit Override Access</i>	Controls whether the logged in user has the authority to disable the motion control limit safety features in the Manual Control window of the SoloVPE software. Not recommended and should only be accessed by trained Solo technicians or under C Technologies guidance.
	<i>EC Edits Allowed</i>	Controls whether the logged in user has the authority to make edits, both new records and changes to existing records, in the Extinction Coefficient Library. Each company must determine if they wish to add the EC Library feature and if so, how they wish to implement it. Some organizations nominate one or more “librarians” to manage the EC Library. This is a decision that must be made by each organization based their needs as identified during the implementation process.
	<i>Allow Default Path Subfolders</i>	Used in conjunction with the all the forced pathing secure points, the Allow Default Path Subfolders controls whether Users can store save files in subfolders within the applicable Default folder. This feature provides users with a greater flexibility to organize batch files within the single Default file repository.
	<i>Force Data Save Default Path</i>	Controls Save Data events to the Default Pathing configured in the SoloVPE Admin Software. Does not apply to File Save events initiated from the Cary WinUV Menu. Subfolder are allowed based upon the setting of the Allow Default Path Subfolder Secure Point setting.
	<i>Force Method Save Default Path</i>	Controls Save Method events to the Default Pathing configured in the SoloVPE Admin Software. Does not apply to File Save events initiated from the Cary WinUV Menu. Subfolder are allowed based upon the setting of the Allow Default Path Subfolder Secure Point setting.
	<i>Coupler Check Access</i>	Controls whether the logged in user has the authority to access the coupler check in the Quick Check Application window of the SoloVPE software. Coupler check tests the overall system transmission independent of Fibrette use.
Autosave	<i>Autosave Optional</i>	Controls whether the logged in user has the authority to bypass or cancel the Autosave features in the SoloVPE software. <i>It is recommended that this permission be disabled for all users</i> because the Autosave feature plays a critical role in ensuring that all acquired data is saved, signed and secured while minimizing opportunities for user intervention that would compromise data integrity or result in data loss.
	<i>Incremental Autosave Enabled</i>	Controls whether the Increment Autosave feature is enabled in the SoloVPE software for the logged in user. This Secure Point should be set consistently for all Users. The benefit of Incremental Autosave comes from the intra-repetition saves that occur when the replicate features is being used in Quick Slope.
	<i>Force Autosave Default Path</i>	Creates a restriction during Autosave events that requires the Autosave file to be saved in the Default Path specified in the software. Attempts by a user to save to an alternate location prevent data acquisition until the required pathing target is met. Use of this Secure Point is recommended to ensure that Batch Files are saved to a network folder where they can be properly secured to prevent modification and /or deletion.
	<i>Prevent Save to Local Hard Drive</i>	Creates a restriction during save events that prevents saving the batch file to a hard drive on the local machine or in effect it forces the file to be saved to a network location. Attempts by a user to save to a folder on a local drive prevents data acquisition, in the

		event of an Autosave, until the pathing requirement is met. Use of this Secure Point is recommended to ensure that Batch files are saved to a network folder where they can be properly secured to prevent modification and /or deletion.
Esign	<i>E-Sign Override Rights Enabled</i>	Controls whether the user or group has the authority to execute an Override E-Signature action when required by the system
	<i>E-signatures Enabled</i>	Controls whether the electronic signature capabilities of the SoloVPE system are enabled for the user or group.
	<i>E-Sign Quick Check Event Optional</i>	Controls whether electronic signatures are required for Quick Check diagnostic test runs. When enabled for a user or group, those users can cancel the electronic signature event
	<i>Post Manual E-Sign Save Required</i>	Controls whether manually initiated electronic signature events are immediately followed by a non-optional save event.
	<i>E-Sign Pre-Save Event Optional</i>	Controls whether user initiated Save Actions require an electronic signature to proceed. When enabled for a user or group, those users can cancel the electronic signature event initiated by the pressing of a Save Data button (excludes menu driven File-Save events) in the SoloVPE software.
	<i>E-Sign Quick Methods Optional</i>	Currently Quick Methods cannot be created on demand by customers, however this Secure Point anticipates a potential software enhancement that would allow users to create Quick Methods from within the SoloVPE software. This Secure Point would control whether those Quick Method Creation Events would require electronic signatures
	<i>E-Sign EC Events Optional</i>	Controls whether actions taken in the Extinction Coefficient Library such as creating new records or modifying existing records require an electronic signature. It is recommended that customers disable this secure point if they decide to use the features of the Extinction Coefficient Library. This provides an added layer of security and audit logging to the routine maintenance of the EC Library. When enabled for a user or group, those users can cancel the electronic signature event initiated in response to extinction coefficient library records changes.
Security	<i>Inactivity Timer Enabled</i>	Controls whether the SoloVPE software inactivity timer feature is enabled by User and Group. The inactivity timer that is included with the SoloVPE software is provided as an optional failsafe for customers that do not want to implement a more robust Local or Group Policy at the workstation of the domain level.
	<i>Perimeter Authentication Enabled</i>	Controls whether a user must authenticate themselves again when the SoloVPE software is opened. When enabled for a user or group, those users will need to enter the credentials of the user currently logged into Windows whenever the SoloVPE software is run.

QuickVCA (QVCA) Secure Points

Group	Secure Point Name	Detailed Description & Guidance
Application	<i>QVCA Software Access</i>	Controls whether access to the QuickVCA software is allowed. This Secure Point is useful for permanently or temporarily preventing access to the QuickVCA software while still maintaining the Security Profile in SecureVPE.
ESign	<i>QVCA E-Sign Enabled</i>	Controls whether the electronic signature capabilities of the QuickVCA software are enabled for the user or group. For secured implementations, it is recommended that this feature be enabled for all groups and users of the QuickVCA software.
	<i>QVCA Post Manual E-Sign Save Required</i>	Controls whether manually initiated electronic signature events in QuickVCA are immediately followed by a non-optional save event. Since manual electronic signatures are frequently used to sign records for review and approval actions, it is recommended that this secure point be set to Enabled for all users and groups in secured implementations.
Method	<i>QVCA Method Modification Rights Enabled</i>	Controls whether the users can create or modify methods using the various screen controls in the QuickVCA Software. Users for whom this Secure Point is disabled are prevented from creating or modifying methods but they can open existing methods and initiate data collection.
Report	<i>QVCA Report Modification Rights Enabled</i>	Controls whether the logged in user can make edits to the content in the report window in the QuickVCA software environment. It is recommended that Report Modification rights be denied for all users including Administrators, since the Agilent WinUV environment has no provisions for logging changes to report content.
Autosave Autosave	<i>QVCA Autosave Optional</i>	Controls whether the logged in user has the authority to bypass or cancel the Autosave features in the QuickVCA software. <i>It is recommended that this permission be disabled for all users</i> because the Autosave feature plays a critical role in ensuring that all acquired data is saved, signed and secured while minimizing opportunities for user intervention that would compromise data integrity or result in data loss.
	<i>QVCA Incremental Autosave Enabled</i>	Controls whether the Increment Autosave feature is enabled in the QuickVCA software for the logged in user.
	<i>QVCA Force Autosave Default Path</i>	Creates a restriction during Autosave events that requires the Autosave file to be saved in the Default Path specified in the software. Attempts by a user to save to an alternate location prevent data acquisition until the required pathing target is met. Use of this Secure Point is recommended to ensure that Batch Files are saved to a network folder where they can be properly secured to prevent modification and /or deletion.
	<i>QVCA Prevent Save to Local Hard Drive</i>	Creates a restriction during save events that prevents saving the batch file to a hard drive on the local machine or in effect it forces the file to be saved to a network location. Attempts by a user to save to a folder on a local drive prevents data acquisition, in the event of an Autosave, until the save path requirement is met. Use of this Secure Point is recommended to ensure that Batch files are saved to a network folder where they can be properly secured to prevent modification and /or deletion.
Security	<i>QVCA Perimeter Authentication Enabled</i>	Controls whether a user must authenticate themselves again when the QuickVCA software is opened. When enabled for a user or group, those users will need to enter the credentials of the user currently logged into Windows whenever the QuickVCA software is run. Windows and Network Administrations have more powerful policy options at their disposal to make sure user sessions do not linger and create security vulnerabilities. Additionally, it is important to note that it is not recommended that a generic user log in be created for use by multiple users for secured implementations. While the prior architecture made that possible, the Active Directory link of the current architecture is significant more powerful and will create more secure implementations.
Administration	<i>QVCA Allow Default Path Subfolders</i>	Used in conjunction with the <i>Force Autosave Default Path</i> Secure Point, it controls whether Users can store save files in subfolders within the applicable Default folder.

	<i>QVCA Force Data Save Default Path</i>	Controls whether the Increment Autosave feature is enabled in the QVCA software for the logged in user. This Secure Point should be set consistently for all Users. The benefit of Incremental Autosave comes from the intra-repetition saves that occur when the replicate features is being used in QVCA.
	<i>QVCA Force Method Save Default Path</i>	Creates a restriction during Autosave events that requires the Autosave file to be saved in the Default Path specified in the software. Attempts by a user to save to an alternate location prevent data acquisition until the required pathing target is met. Use of this Secure Point is recommended to ensure that Batch Files are saved to a network folder where they can be properly secured to prevent modification and /or deletion.

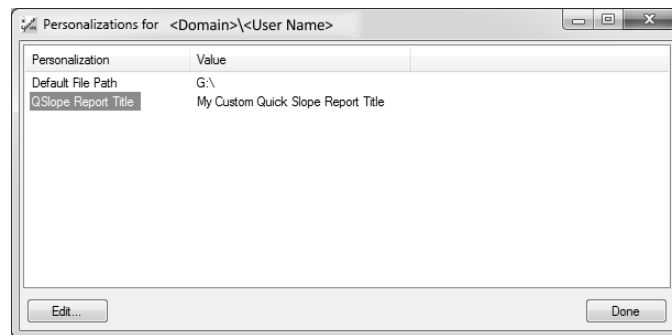
15. THE PERSONALIZE FEATURE

Personalization, or the Personalize feature in SecureVPE, allows Administrators to configure User Specific parameters as part of a User Security Profile. There are currently two Personalization parameters, though more may be added in future updates of the Software. It is important to note that these parameters are only available at the User level. They are not available for Groups. Setting values for these parameters results in specific behaviors in the SoloVPE Software that can be useful when creating an overall security implementation plan.

There are parameters that can currently be personalized are:

Default File Path: The Default File Path personalization has the power to be an important part of a secured implementation because it provides another tool to control where electronic records generated by the SoloVPE system are stored. Use of this personalized parameter, in conjunction with the Secure Points available in the Software, provides Administrators with the power to control where files are saved by User. This is a powerful option for implementation teams to consider when developing their security plan for the system.

Quick Slope Report Title: The *Quick Slope Report Title* personalization is a simple tweak but could have value for clearly identifying the user responsible for report generation. While the E-Signature feature allows the user to electronically sign their data and electronic records, it generally appears at the bottom of the report output. When a text value is set for this parameter, it replaces to default Quick Slope Report Titles with the personalized text.



The Personalize parameters are set using the following procedure:

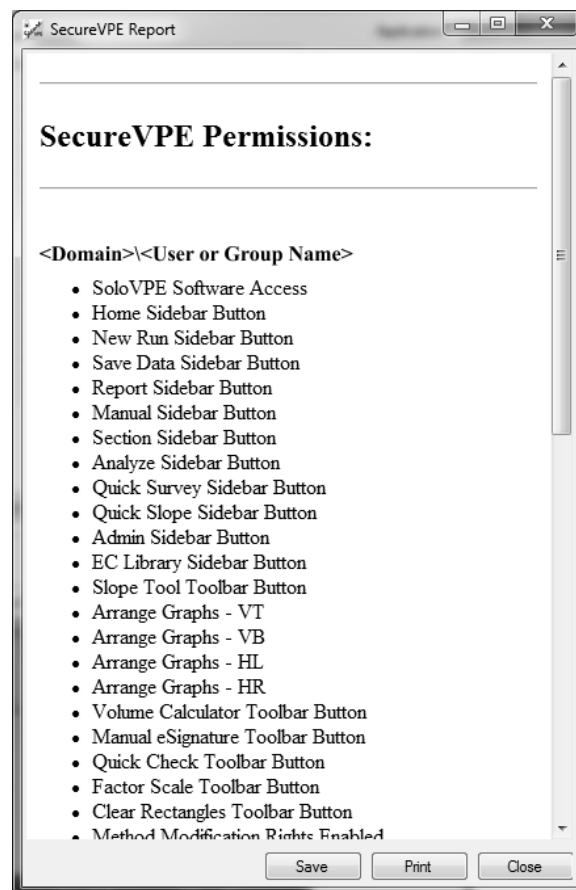
- 1) Select the *Users* tab in the *Security Console* window.
- 2) Select a User from the list.
- 3) Press the **Personalize...** button at the bottom of the *Users* tab to open the *personalization* window.
- 4) To set or edit a Personalization, double-click one of the personalizations from select the Personalization and press the **Edit** button to display the *Edit Personalization* window.
 - a. To set a *Quick Slope Report Title*, type the desired text into the field provided and press **OK**.
 - b. To set a *Default File Path*, either type the path if known or **Browse** for the desired path
 - c. Press **OK**.
- 5) Press **Done** to close the Personalization window.

16. THE REPORT FEATURE

The SecureVPE Software includes a reporting feature that allows Administrators to generate a SecureVPE Permissions report that summarizes all available Security Profiles by User and Group including the granted Secure Points and personalization. The report is provided as a way of documenting a snapshot of the current configurations.

Since Secure Points are either Enabled or Disabled, the report will list the enabled Secure Points by Domain and User or Group. If a Secure Point has been enabled for a User or Group, it will appear on the Report. Those that have not been granted simply do not appear on the report, the absence conveys status.

In addition to the Secure Point listings, Personalization settings are displayed for each User. If a User does not have personalization configured, then it will not be shown in the report.



17. SOLOVPE SYSTEM ELECTRONIC RECORDS (BATCH FILES)

The electronic records that are generated by the SoloVPE system are saved as Batch Files with the file extension (*.BVP). Batch files are a proprietary file structure created by the Agilent Cary WinUV Software. Batch files are independent objects stored on the computer or network file system. Batch files contain all information related to the analytical record including method and method log information, data and data audit logs, analysis results and report content, and E-Signature data.

C Technologies, Inc. strongly recommends that electronic records only be stored on a Network Drive to appropriately secure the electronic records created by the SoloVPE System. Specifically, it is recommended that Batch files be stored in secured network folders that will prevent any user from modifying or deleting files once they have been written. This recommendation is made primarily because of the way Microsoft handles file ownership on a local machine. While it is possible to configure NTFS file permission on files and folders stored locally, the rules that Microsoft uses to govern file ownerships create a vulnerability that is most readily addressed by storing files on a network drive. Owners retain modification and deletion rights on their own files, even when they are stored in folders that are configured to deny modification and deletion.

NOTE: File ownership includes some special permissions in the Windows environment that are beyond the control of the applications running in the environment. When the logged in user creates a new file that is saved to a local hard drive, the logged in user is given ownership of that file by default and ownership has its privileges. Owners retain unrestricted rights when it comes to modifying and deleting files they own, even when they are stored in folders that have NTFS file permission set to deny modification or deletion.

The most effective way to deal with the issue of Microsoft's file ownership rules is to save batch file, electronic records to a network location. By default, files saved to the network are owned by the Administrator of the domain rather than the logged in user that saved the file. This ensures that the NTFS file permissions that are set on the folder location and inherited by the newly created file are in force as soon as the initial write is complete. When NTFS permissions are properly configured by the IT Administrative staff to prevent modification or deletion of the files. The electronic records are preserved and protected.

The VPE System Service: An application in the SoloVPE Administrator called the VPE System Service has been introduced in Version 3.1.xyz and it provides an additional capability meant to address the issue of ownership. The VPE System Service is an optional feature accessible through the SoloVPE Administration application that can be implemented by the implementation team to create more flexibility should a customer wish to store files locally. When installed and running in the background, the VPE System Service watches for electronic records being created by the SoloVPE Software and when it detects a batch record creation event it immediately changes the ownership of the newly created file from the logged in user that created the file to the Administrator. In doing so, the VPE System Service reasserts the NTFS File permission settings and eliminates the issue of special permissions related to file ownership. For more information on the VPE System Service please see the SoloVPE User Manual.

18. SOLOVPE SYSTEM E-SIGNATURES

E-Signatures in the SoloVPE System are enabled by using the SecureVPE Software. The implementation team decides how to use the security features of the SecureVPE and SoloVPE system as part of the planning and development work required to implement the system. The Software is highly configurable out of the box, giving owners a lot of flexibility in deciding which features to implement. E-Signatures are made possible through SecureVPE.

The E-Signatures functionality in the SoloVPE Software gives users the ability to electronically sign the electronic records they generate by successfully authenticating their identity with their User ID and Password. By configuring the Secure Point in SecureVPE, Administrators can control when E-Signature prompts will appear. Many E-Signature events can be automatically triggered by actions such as configuring a method or acquiring data.

Some important attributes of E-Signatures in the SoloVPE System are as follows:

1. E-Signatures are not biometric.
2. E-Signatures are based upon two distinct components that together are used to ensure the uniqueness of the associated signer.
 - a. A Unique User ID controlled by the company through active directory
 - b. A Password of the logged in User
3. The Company is responsible for enacting policies and controls that ensure and verify the identity of the individual and meet the requirements of all applicable rules.
4. Electronic signature components are controlled, maintained and administered by the company (Active Directory Link) maintains responsibility for all rules and policies governing, uniqueness, format, complexity, aging etc.



The screenshot shows a dialog box titled "eSignature Required" with the SoloVPE logo and "e signature" text. It contains the following fields and controls:

- Time Stamp: 2018-06-05 10:40:14
- User Name: BRIDGEWATER\shaydu
- Type: Author (dropdown menu)
- Reason / Comments: A large empty text area.
- Password: A password input field.
- Locked: (unchecked)
- Override Required: (unchecked)
- eSign: A button.

E-signatures are stored in the Batch file with the electronic record, but there is also an E-Signature log that captures all E-Signature events attempted and completed on the system that is independent of the Batch file records. Successive failed E-Signature attempts will result in the Software locking until an authorized individual executes an E-Signature Override to clear the lock. The number of failed attempts is set in the SecureVPE Settings.

Esignature Audit Fields	Description
Date Time	Date: YYYY-MM-DD Time: hh:mm:ss
UserName	Computer or Network name/ username
PwdVerified	0= Failed 1=Success
Attempt	Number of attempts to verify the user
Locked	The system will lock due to multiple failed attempts, with the default being 3. After 3 failed attempts, the software requires credentials of an Administrator that is not the user.
Type	Author, Reviewer, Approval, Override
Class	It specifies the eSignature event in a specific section of the software (Module).
Reason	Reason or comments the user types into the text dialog box
Module	The area of the software the eSignature is being applied.
Override	After 3 failed attempts for an eSignature, the software requires an Admin (that is not the current user) to use their respective credentials for an ESignature. Providing those credentials and applying the ESign will be this Override. A 1 will indicate it was applied in the software.
ESignApplied	0= Failed 1=Success

eSignature Event List: When and how eSignatures are triggered/active within the SoloVPE Software

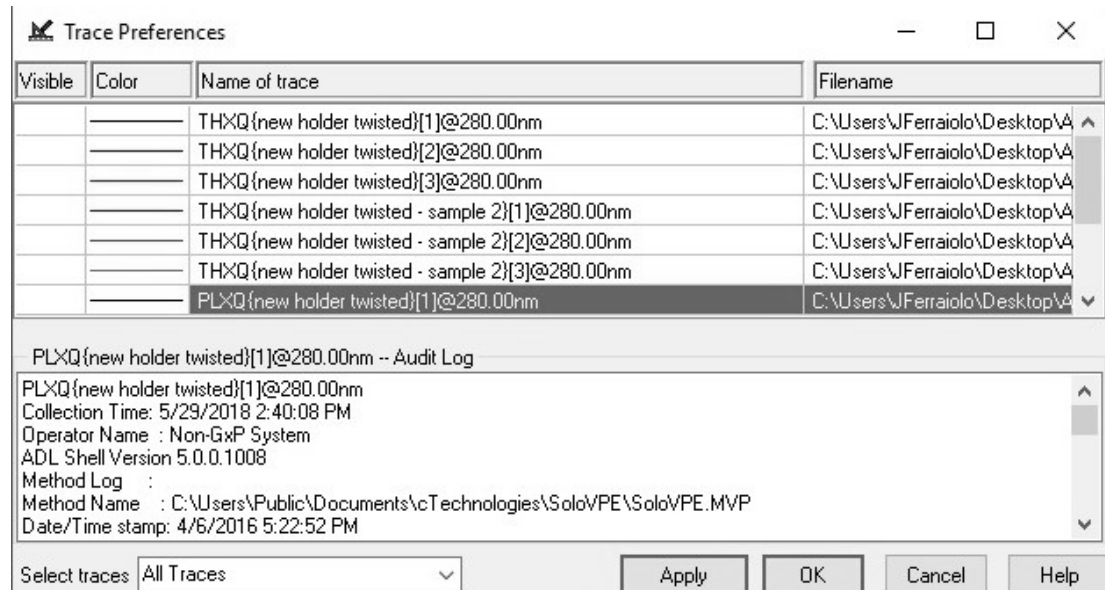
Class	Module	Description
Esign Data	SaveData	Button on the toolbar and when Quick Slope acquisition is completed
Esign Report	Report	Button on the toolbar
Esign Method	QSlope	Button on the toolbar
QuickCheck CouplerCheck	QCheck	Triggered when a Quick Check and Coupler Check are performed
Esign Data	EC Library	Edits add or modify (=# for the set that was edited)

19. SECUREVPE AUDIT LOGS

SecureVPE extensively logs actions taken within the application. Critical actions such as enabling the SecureVPE controls, and setting permission and personalization all get logged within the SecureVPE audit trail. The SecureVPE Audit Log (audit trail) is one of many audit logs that exist in the SoloVPE Software. Method Audit Logs, Data Audit Logs, SoloVPE Administration Audit Logs, Extinction Coefficient Library, the SoloVPE Software etc. all can provide significant insight into the user actions and system activities and be supportive of compliance actions and audit activities.

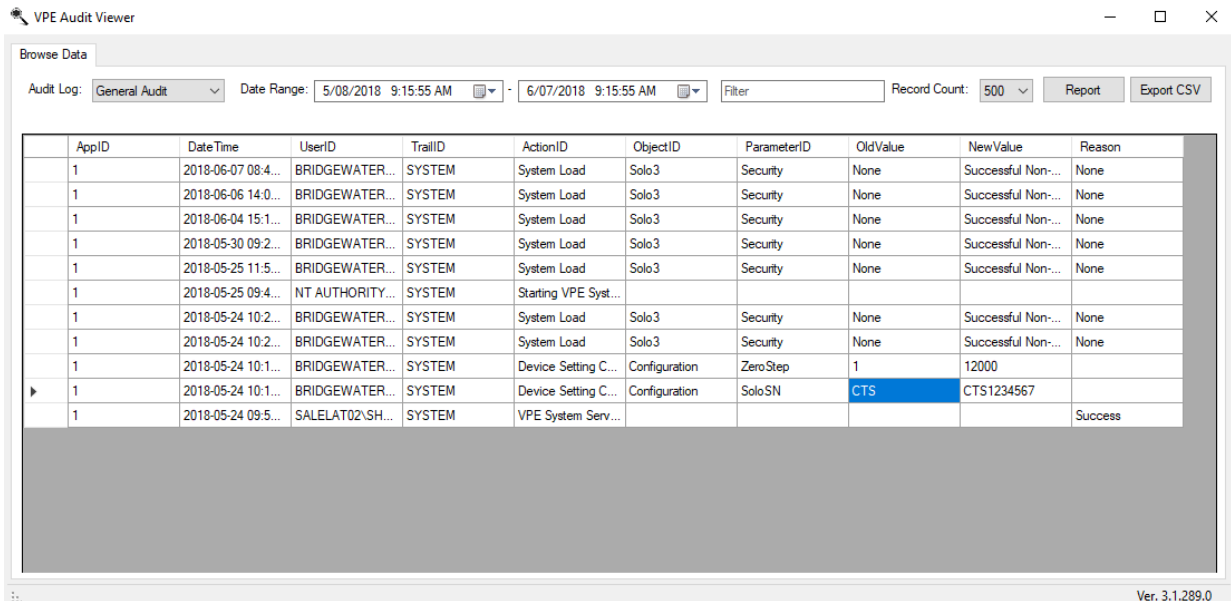
Audit trails related to the data or methods reside in the actual batch/method file. Batch files (*.BVP) and Method files (*.MVP) are the raw files saved by the software. The SoloVPE software is a file-based system. All raw data and method audit trails can be access by the following method:

1. Open the SoloVPE Software
2. Go to File/Open Data
3. Once the data file is open press the **Trace Preferences** button in the top Toolbar
4. Select trace for which you would like the audit trail Information



The SecureVPE Audit Logs can be accessed, viewed, filters and printed from the **VPE Audit Viewer** application. The VPE Audit Viewer is not secured via the UAC because the application provides read-only viewing of the audit trail information. It provides a single source for reviewing the SoloVPE specific audit trails and ensures accessibility even without Administrative privileges.

General Audit Viewer: Provides an overview of when, what, and who performed actions within the SoloVPE software. The audit viewer cannot be edited.



SecureVPE Audit Viewer: Provides an overview of when, what, and who performed actions within the SecureVPE software. Added user/groups and their access credentials are logged here. The audit viewer cannot be edited.

AppID	Date Time	UserID	TrailID	ActionID	ObjectID	ParameterID	OldValue	NewValue	Reason
1	2018-05-21 12:1...	BRIDGEWATER...	SYSTEM	Secure Point Assi...	SecureVPE	Security	SoloVPE Softwar...	SoloVPE Softwar...	None
1	2018-05-21 12:1...	BRIDGEWATER...	SYSTEM	Secure Point Assi...	SecureVPE	Security	SoloVPE Adminis...	SoloVPE Adminis...	None
1	2018-05-21 12:1...	BRIDGEWATER...	SYSTEM	Secure Point Assi...	SecureVPE	Security	SecureVPE Acce...	SecureVPE Acce...	None
1	2018-05-21 12:1...	BRIDGEWATER...	SYSTEM	Secure Point Assi...	SecureVPE	Security	Method Modificat...	Method Modificat...	None
1	2018-05-21 12:1...	BRIDGEWATER...	SYSTEM	Secure Point Assi...	SecureVPE	Security	Advanced Settlin...	Advanced Settlin...	None
1	2018-05-21 12:1...	BRIDGEWATER...	SYSTEM	Secure Point Assi...	SecureVPE	Security	DAQ View Enabl...	DAQ View Enabl...	None
1	2018-05-21 12:1...	BRIDGEWATER...	SYSTEM	Secure Point Assi...	SecureVPE	Security	DAQ View Option...	DAQ View Option...	None
1	2018-05-21 12:1...	BRIDGEWATER...	SYSTEM	Secure Point Assi...	SecureVPE	Security	Quick Methods E...	Quick Methods E...	None
1	2018-05-21 12:1...	BRIDGEWATER...	SYSTEM	Secure Point Assi...	SecureVPE	Security	Force Disable QS...	Force Disable QS...	None
1	2018-05-21 12:1...	BRIDGEWATER...	SYSTEM	Secure Point Assi...	SecureVPE	Security	Report Sidebar B...	Report Sidebar B...	None
1	2018-05-21 12:1...	BRIDGEWATER...	SYSTEM	Secure Point Assi...	SecureVPE	Security	Manual Sidebar ...	Manual Sidebar ...	None
1	2018-05-21 12:1...	BRIDGEWATER...	SYSTEM	Secure Point Assi...	SecureVPE	Security	Section Sidebar ...	Section Sidebar ...	None
1	2018-05-21 12:1...	BRIDGEWATER...	SYSTEM	Secure Point Assi...	SecureVPE	Security	Analyze Sidebar ...	Analyze Sidebar ...	None
1	2018-05-21 12:1...	BRIDGEWATER...	SYSTEM	Secure Point Assi...	SecureVPE	Security	Quick Survey Sid...	Quick Survey Sid...	None
1	2018-05-21 12:1...	BRIDGEWATER...	SYSTEM	Secure Point Assi...	SecureVPE	Security	Quick Slope Side...	Quick Slope Side...	None
1	2018-05-21 12:1...	BRIDGEWATER...	SYSTEM	Secure Point Assi...	SecureVPE	Security	Admin Sidebar B...	Admin Sidebar B...	None
1	2018-05-21 12:1...	BRIDGEWATER...	SYSTEM	Secure Point Assi...	SecureVPE	Security	EC Library Sideb...	EC Library Sideb...	None

Extinction Coefficient Audit Viewer: Provides an overview of when and who populated all extinction coefficients added to the EC database. The audit viewer cannot be edited. All Audit Viewer logs can be viewed, printed, or exported by custom date ranges or by user/group name and then pressing the Report or Export Buttons

Date Time	AppID	UserID	TrailID	ActionID	ObjectID	ParameterID	Reason	ECID	OldValue	New
2018-05-23 11:1...	1	BRIDGEWATER...	SYSTEM	active changed	test		None	4	False	True
2018-05-23 11:1...	1	BRIDGEWATER...	SYSTEM	EC Data Deleted	test		None	4	WL=236,EC=1	
2018-05-23 11:1...	1	BRIDGEWATER...	SYSTEM	EC Data Inserted	test		None	4		WL=2
2018-05-23 11:1...	1	BRIDGEWATER...	SYSTEM	active changed	test		None	4	True	False
2018-05-23 11:1...	1	BRIDGEWATER...	SYSTEM	EC Data Inserted	test		None	4		WL=2
2018-05-21 13:4...	1	BRIDGEWATER...	SYSTEM	EC Library Added	test		None	4		test
2018-05-21 13:4...	1	BRIDGEWATER...	SYSTEM	EC Data Inserted	test		None	4		WL=2
2018-05-21 12:1...	1	BRIDGEWATER...	SYSTEM	EC Data Inserted	test		None	3		WL=2
2018-05-21 12:1...	1	BRIDGEWATER...	SYSTEM	active changed	test		None	3	True	False
2018-05-21 12:1...	1	BRIDGEWATER...	SYSTEM	EC Library Added	test		None	3		test
2018-05-21 12:1...	1	BRIDGEWATER...	SYSTEM	EC Data Inserted	test		None	3		WL=2

Extinction Coefficient Event List: What parameters are tracked/logged within the Extinction Coefficient Audit Trail.

Audit Fields	Description
Date Time	Date: YYYY-MM-DD Time: hh:mm:ss
AppID	Always 1. 1 is the AppID for SoloVPE
UserID	Computer or Network name/ Username
TrailID	Always System
ActionID	This is action taken by the user within the EC Library - importing, exporting, and modifying.
ObjectID	This is the user-selected name of an Extinction Coefficient
ParameterID	This is always blank. No actions within the EC Library populate this field
Reason	Reason or comments the user types into the text dialog box
ECID	The ID of the Extinction Coefficient that was modified or added
OldValue	The old value will be listed here
NewValue	The newly edited/selected value will be listed here

20. ACHIEVING COMPLIANCE – CONSIDERATIONS & BEST PRACTICES

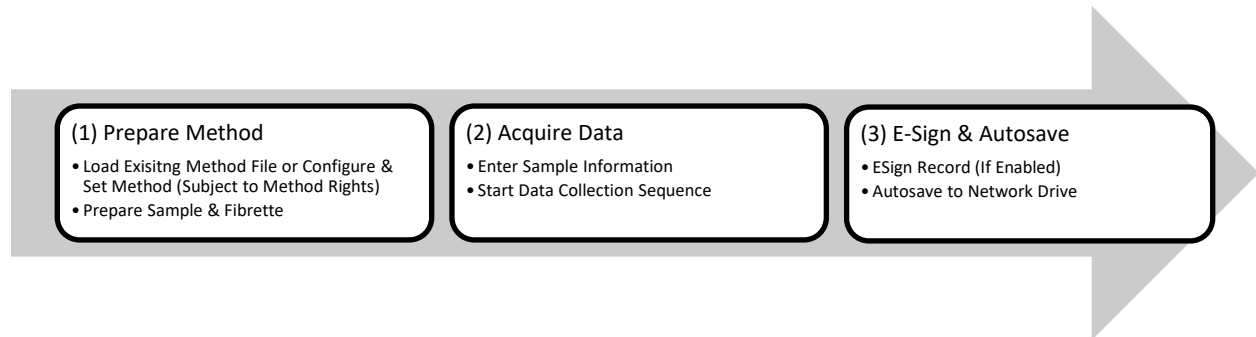
Each implementation has customer specific requirements and unique considerations there are common keys to success that have helped numerous customers with SoloVPE implementation. It is important to understand that every Software application will have unique attributes and behaviors that must be accounted for during implementation planning. Due to the SoloVPE's unique system architecture, which leverages the capabilities of the Agilent Cary 60 and the Cary WinUV environment, there are some important attributes to keep in mind. A flowchart of system info structure is provided below to assist with implementation efforts. Please see page 46.

The SoloVPE Software Interface exists within the Agilent Cary WinUV Software environment. Many of the fundamental interface options and logging activities are completely controlled by the Cary WinUV Software. The specific configurations that customers used are highly dependent on the organization's network infrastructure and use of local and group policies, but this list should be reviewed as part of the implementation planning.

- User ID & Password Controls:** Administration of User ID's and Passwords, as well as all associated policies (e.g. Uniqueness, Expiration & Aging, Complexity etc.), are managed and maintained by the in-house Administrator staff through active directory.
- Time-Out Behaviors:** Local and group policies implemented at the organization provide the greatest flexibility and control over system behavior when users walk away from the system without logging off. This feature can be enabled in the Security section of SecureVPE
- Save to Network Folders:** The configuration of SecureVPE should save files to secured network folders on which the NTFS file permissions and inheritance have been set to provide maximum protection of the electronic records. The most secure approach is to restrict any modification or deletion of electronic records.
- Autosave:** By using Autosave, user discretion is eliminated when it comes to the creation of electronic records. All data acquisition actions result in the creation of a batch file electronic record that cannot be modified or deleted.
- Hierarchy of Privileges:** When setting up Users and Groups it is important to create a spectrum of rights to prevent inadvertently getting locked out when a user forgets his or her password and the E-Signature override lock is triggered.
- Training:** The importance of adequate training for all personnel that are responsible for setting up, configuring, maintaining and using the SoloVPE System cannot be overstated. Having a User/Group that is both comfortable

with the science, the hardware and the Software of the SoloVPE System will certainly result in a successful implementation. Individuals that obtain advanced training that can act as internal support for the system and liaisons during interactions with C Technologies will help ensure quick issue resolution and overall satisfaction with the system. Please contact C Technologies for additional information.

7. **Backups:** As with any electronic system, routine and thorough backups are a critical element of secured (and unsecured) implementations.



21. A SIMPLE THREE-STEP RESTRICTED PATH EXAMPLE PROCESS

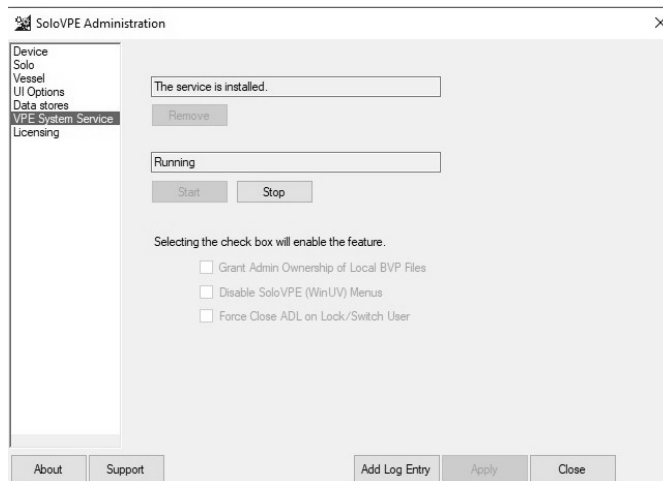
This example graphic shows a simple three-step process that is frequently used in compliant installations. The three steps include: (1) Prepare Method, (2) Acquire Data and (3) E-Sign and Autosave events. Within each step, the user options can be limited using Secure Points and personalization. Most importantly, once the data acquisition has been initiated the user cannot exit the process until the acquired data and report have been E-Signed (when enabled) and safely saved in a network folder via Autosave as is the recommended procedure.

22. SOLOVPE ADMINISTRATION PROGRAM

The SoloVPE Administration window contains device information, settings, support files, as well as Software licensing. It is through this window that configuration details specific to the organization, device, and details of the system can be configured. It is important to avoid making changes in any of the SoloVPE Administration modules without specific guidance from a Certified SoloVPE Support Specialist. Should a user require guidance on the proper use of SoloVPE Administration features please contact Support through established local or international channels.

22.1 SOLOVPE ADMINISTRATION - VPE SYSTEM SERVICE

The VPE System Service is an optional feature that is managed from within the UAC secured SoloVPE Administration application. An Administrator can install or remove the feature from within the application and to toggle its state between started and stopped. As a system level service, it runs in the background and contains no user interface. It acts as a sentry looking for events that require it to act.



The three main features the VPE System Service provides are as described as follows:

- 1) **Grant Admin Ownership of Local BVP Files** – This feature was integrated to overcome the Microsoft File Ownership permission vulnerability. As noted File Ownerships in Windows have permissions that cannot be overridden by NTFS settings on the Local Machine. Since File Ownership is determined by the logged in Windows user when a file is created, the VPE Local File Locking option looks for WinUV file creation event and when it detects them it will change the Ownership of the newly created file from the logged in user to the Administrator. This change gives Administrators the ability to set NTFS file permissions on local folders and protect files that could otherwise be subject to modification and deletion by the default owner.
- 2) **Disable SoloVPE (WinUV) Menus** – This feature was created to give Administrators the option of hiding the standard Agilent WinUV Menu Bar which simultaneously eliminates the SoloVPE Users’ ability to interact with unsecured WinUV features such as the standard File Save Dialogs and disables the WinUV Hot Keys which can cause unexpected behaviors.
- 3) **Force Close ADL on Lock/Switch User** – This feature will close the SoloVPE Software if the current user logs out of the software or switches account profiles while the software is still running under that User profile.

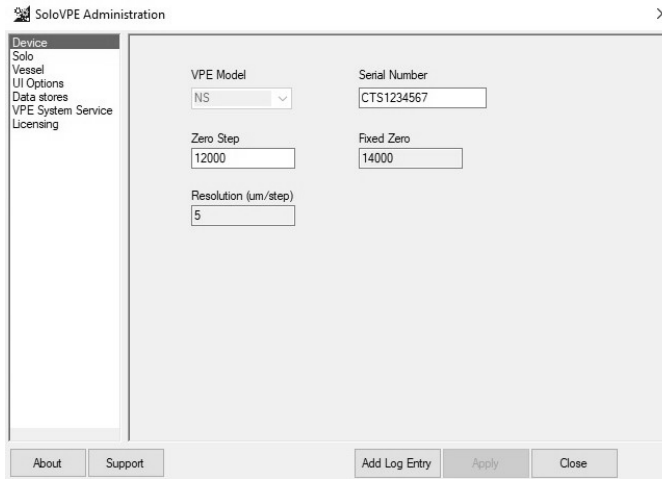


NOTE: Hiding the Cary WinUV menu bar does limit user ability to use unconstrained file pathing, however, it also eliminated access to standard Cary WinUV features that allow control of the Cary or quick access to the WinUV Audit Logs. These facts must be accounted for in the implementation.

As noted these features are accessible to all SoloVPE owners, even those that have not purchased SecureVPE. CTI does not recommend reliance on these measures exclusively to achieve compliance. The best practice recommendation is to save records to a network folder that more readily secured, mirrored and backed up.

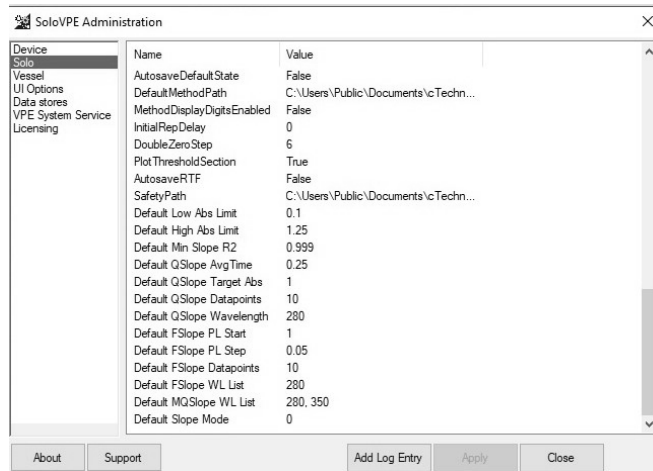
22.2 SOLOVPE ADMINISTRATION - DEVICE

Pressing the Device button displays a dialog window in which key system parameters such as the SoloVPE Model, Serial Number, Zero, Step Address, and Resolution information can be reviewed and updated.



22.3 SOLOVPE ADMINISTRATION - SOLO

The Solo Parameter list in the SoloVPE Administration tool is a list of settings that allow Administrators to fine tune and configure the SoloVPE environment and Software behavior. The full list of parameters and definitions can be found on pages 104 – 107 in DOC0126 SoloVPE User Manual – Software Version 3x.



SoloVPE Administration: Solo Parameter List

The Solo Parameter list in the SoloVPE Administration tool is a list of settings that allow Administrators to fine tune and configure the SoloVPE environment and Software behavior. Not all settings will be applicable to every implementation since not all features are used by all users. The following table lists the Solo Parameters and a brief description of their meaning and use.

Solo Parameter Name	Default Value	Description
VerboseLoggingEnabled	False	Low-Level System parameter intended to be used by trained service personnel for system maintenance and troubleshooting. Enables or disables more detailed event logging in the WinUV environment.

ExportLogWithCSV	False	Toggles the export of the Data Audit Log on and off when using the Save As *.CSV feature of the WinUV Save As Dialog.
DoubleZeroEnabled	True	Low-Level System parameter intended to be used by trained service personnel for system maintenance and troubleshooting. Should remain in the True state but is capable of reverting to a simpler Fibrette Zero action.
DefaultVessel	3	Specifies the Default Vessel type selected when the Software runs.
R2DisplayDigits	6	Broadly controls the number places displayed when the system display outputs R2 data to the screen and reports.
SlopeDisplayDigits	5	Broadly controls the number places displayed when the system display outputs slope data to the screen and reports.
ECDisplayDigits	5	Broadly controls the number places displayed when the system display outputs Extinction Coefficient data to the screen and reports.
ConcDisplayDigits	5	Broadly controls the number places displayed when the system display outputs Concentration data to the screen and reports.
AbsDisplayDigits	5	Broadly controls the number places displayed when the system display outputs Absorbance data to the screen and reports.
TransDisplayDigits	5	Broadly controls the number places displayed when the system display outputs Transmission data to the screen and reports.
StatsDisplayDigits	6	Broadly controls the number places displayed when the system display outputs Statistical data to the screen and reports.
WavelengthDisplayDigits	2	Broadly controls the number places displayed when the system display outputs Wavelength data to the screen and reports.
PathlengthDisplayDigits	3	Broadly controls the number places displayed when the system display outputs Pathlength data to the screen and reports.
SecondsDisplayDigits	2	Broadly controls the number places displayed when the system display outputs Seconds data to the screen and reports.
DefaultDateFormat	yyyy-mm-dd	Broadly controls the date formatting when the system displays date information on the screen and in reports.
DefaultDateTimeFormat	yyyy-mm-dd hh:nn:ss AMPM	Broadly controls the date formatting when the system displays time information on the screen and in reports.
DecimalDisplayDigits	5	Broadly controls the date formatting when the system displays date-time information on the screen and in reports.
DefaultMVPSeedFile	SoloVPE.MVP	Low-Level System parameter that should not be changed that specifies the generic Method File that is used by the SoloVPE Software when the Software opens.
DefaultSavePath	C:\Users\Public\Documents\cTechnologies\ SoloVPE\	The global Default Save Path that is used for Non-WinUV Save Dialog windows. This parameter is a global default that can be overridden by Personalization when the SecureVPE Software is enabled.

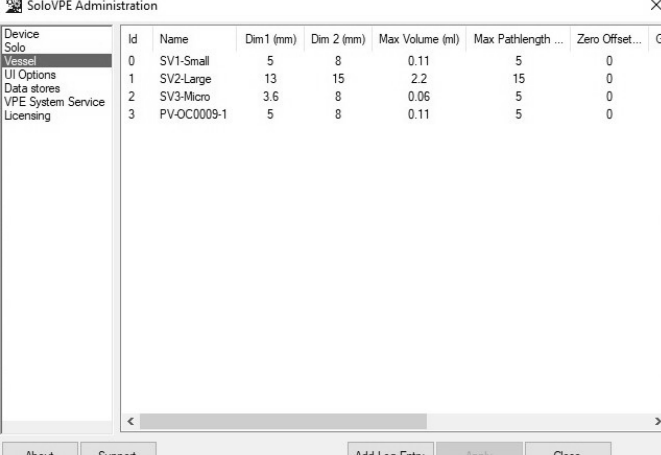
EnabledSessionLogging	False	Low-Level System parameter intended to be used by trained service personnel for system maintenance and troubleshooting. Enables or disables a detailed logging feature within the SoloVPE Software. When enabled performance is dramatically reduced due to the burden of this feature.
SessionLogType	Internal	Low-Level System parameter intended to be used by trained service personnel for system maintenance and troubleshooting. Parameters specify the output format of the session logs.
ReportGraph	False	Toggles whether the Graphics Region in the SoloVPE Software will print as its own region during hard copy output. When enabled wrapping and formatting can be negatively impacted which is why the default state is false.
ReportXScale	100	Low-Level System parameter that controls the output width percentage dedicated to the printing of the WinUV Graphics Region.
ReportYScale	100	Low-Level System parameter that controls the output height percentage dedicated to the printing of the WinUV Graphics Region.
Primary HGraphX	750	Low-Level System parameter that controls how the Horizontal Auto Arrange Graphs feature distributes the available graphs in the X-Axis
Primary HGraphY	950	Low-Level System parameter that controls how the Horizontal Auto Arrange Graphs feature distributes the available graphs in the Y-Axis
Primary VGraphX	1000	Low-Level System parameter that controls how the Vertical Auto Arrange Graphs feature distributes the available graphs in the X-Axis
Primary VGraphY	600	Low-Level System parameter that controls how the Vertical Auto Arrange Graphs feature distributes the available graphs in the Y-Axis
Default Section Graph	System Sections	Specifies the target Graph used for the display of System Generated Section Data
Default Spectra Graph	System Spectra	Specifies the target Graph used for the display of System Generated Spectral Data
ReplicateRetreatStep	6000	Low-Level System Parameter that specified how far the SoloVPE stage retreats during replicate measurements to allow for switching samples and Fibrettes to avoid returning all the way to the Home position.
Inactivity Threshold	10000	Specifies the latency time in seconds that the Inactivity monitor feature will allow before disabling Software features and requiring re-authentication of the current user.
RepLimit	6	Specifies the maximum number of replicates allowed to be made in the Quick Slope module.
MaxRepDelay	300	Specifies the maximum amount of time between replicate measurements in Quick Slope when the Rep Delay features is enabled in the Software.
QSlopeReportTitle	<Null>	A string value that overrides the Default Quick Slope Report Title. This Global Parameter can be changed for the system as the Quick Slope Report Title

IncrementalAutosaveFolder	True	Toggles whether the Incremental Autosave features create a subfolder for each data acquisition event or if it places all incremental auto-save files in a single folder.
IncrementalAutosavePath	C:\Users\Public\Documents\cTechnologies\SoloVPE\	A string value that specifies the path to which incremental auto-save files is saved.
AutosaveDefaultState	False	Toggles the Default state of the Autosave feature either Enabled by Default or Disabled by Default.
DefaultMethodPath	C:\Users\Public\Documents\cTechnologies\SoloVPE\	The default path that will be used when savings Method Files from within the SoloVPE and QuickVCA Software.
MethodDisplayDigitsEnabled	False	Enables or disables a Feature that allows users to specify the Concentration Display Digits as an independent parameter within a Quick Slope Method, independent of the other Concentration Display Digit parameter.
InitialRepDelay	0	A Low-Level System Feature that makes it possible to introduce a Pre-Acquisition Delay before the First or only data acquisition to allow for sample settling to occur post-Fibrette Zeroing.
DoubleZeroStep	6	A Low-Level System Parameter that makes it possible to control exactly how the Fibrette Zeroing Action occurs.
PlotThresholdSection	True	Enables or disables the plotting of the Quick Slope Search results used in the Quick Slope data acquisition routine.
AutosaveRTF	False	Enables or Disables the output of an RTF file in addition to the Autosave Batch File. The RTF file that is saved is the formatted content of the Cary WinUV Report Pane content.
SafetyPath	C:\Users\Public\Documents\cTechnologies\SoloVPE\	An Admin configurable path that the Software will use for Safety Save events in case of loss of network access.
Default Low Abs Limit	0.1	Override parameter that allows Administrators to change the default threshold value that controls the display of the Low Absorbance Alert in Quick Slope.
Default High Abs Limit	1.25	Override parameter that allows Administrators to change the default threshold value that controls the display of the High Absorbance Alert in Quick Slope.
Default Min Slope R2	0.999	Override parameter that allows Administrators to change the default threshold value that controls the display of the Low R2 Alert in Quick Slope.
Default QSlope AvgTime	0.25	Override parameter that allows Administrators to change the default Photometric Averaging Time value in Quick Slope.
Default QSlope Target Abs	1	Override parameter that allows Administrators to change the default Threshold Absorbance Target value in Quick Slope.
Default QSlope Datapoints	10	Override parameter that allows Administrators to change the default number of data points to be collected in Quick Slope.
Default QSlope Wavelength	280	Override parameter that allows Administrators to change the default wavelength value in Quick Slope.
Default FSlope PL Start	1	Override parameter that allows Administrators to change the default Starting Pathlength Value in Fixed Slope mode in Quick Slope.

Default FSlope PL Step	0.05	Override parameter that allows Administrators to change the default Pathlength Step Size Value in Fixed Slope mode in Quick Slope.
Default FSlopeWL List	280	Override parameter that allows Administrators to change the default wavelength value in Fixed Slope mode in Quick Slope.
Default MQSlope WL List	280, 350	Override parameter that allows Administrators to change the default wavelength value list in Multiple Quick Slope mode in Quick Slope.
Default Slope Mode	0	Override parameter that allows Administrators to change the Default Slope Acquisition mode in Quick Slope (0 = Quick, 1 = Fixed, 2 = Multi-Quick)

22.4 SOLOVPE ADMINISTRATION - VESSEL

This is where the vessel parameters can be viewed. Pressing the Vessel button displays the parameters of the Small, Micro, Large and Plastic vessel types in the SoloVPE Software.

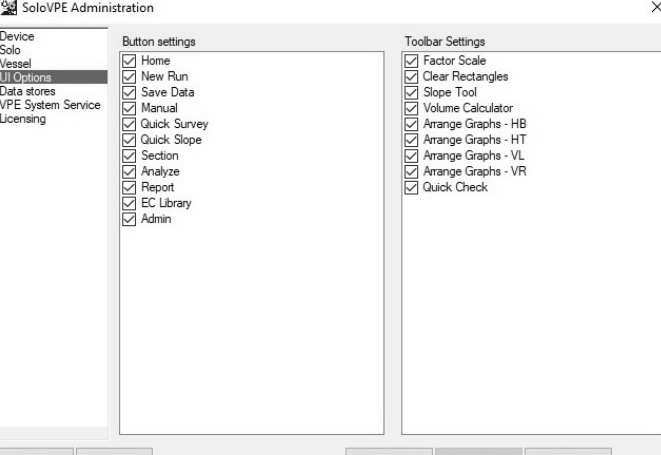


The screenshot shows the 'SoloVPE Administration' window with the 'Vessel' tab selected. A table displays the following data:

Id	Name	Dim1 (mm)	Dim 2 (mm)	Max Volume (ml)	Max Pathlength ...	Zero Offset ...	Gr
0	SV1-Small	5	8	0.11	5	0	
1	SV2-Large	13	15	2.2	15	0	
2	SV3-Micro	3.6	8	0.06	5	0	
3	PV-OC0009-1	5	8	0.11	5	0	

22.5 SOLOVPE ADMINISTRATION – UI OPTIONS

This is where features of the software can be enabled or disabled for users not using the SecureVPE program. Pressing the UI Options button displays a dialog window that contains controls to Grant or Revoke visibility to the SoloVPE side bar buttons. This is especially useful to users that do not have SecureVPE. **NOTE: This option will not appear when SecureVPE is installed.**

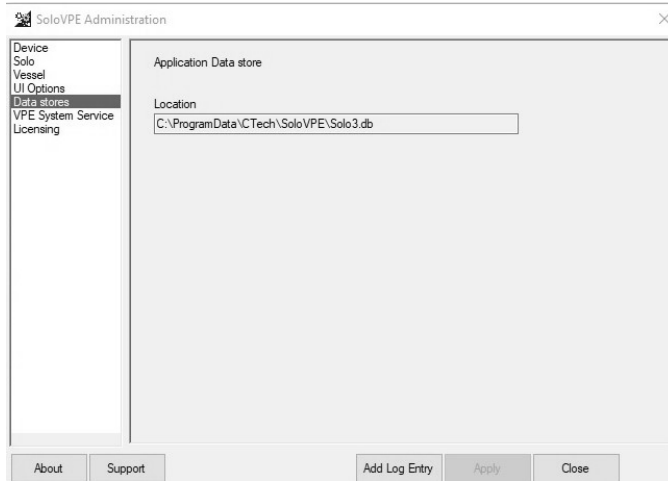


The screenshot shows the 'SoloVPE Administration' window with the 'UI Options' tab selected. It contains two columns of settings:

- Button settings:**
 - Home
 - New Run
 - Save Data
 - Manual
 - Quick Survey
 - Quick Slope
 - Section
 - Analyze
 - Report
 - EC Library
 - Admin
- Toolbar Settings:**
 - Factor Scale
 - Clear Rectangles
 - Slope Tool
 - Volume Calculator
 - Arrange Graphs - HB
 - Arrange Graphs - HT
 - Arrange Graphs - VL
 - Arrange Graphs - VR
 - Quick Check

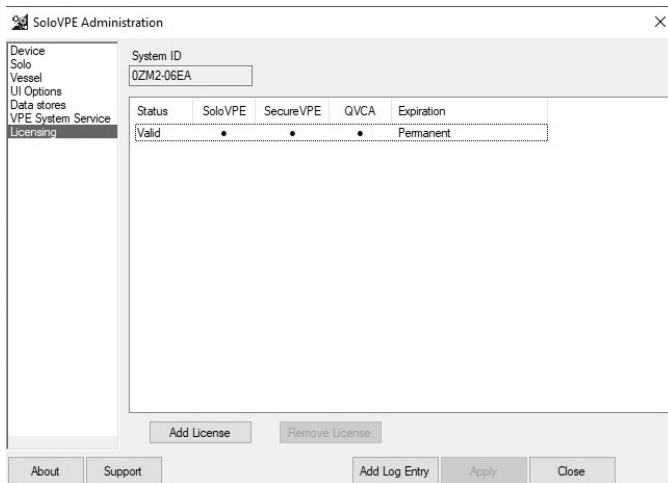
22.6 SOLOVPE ADMINISTRATION – DATA STORES

The SoloVPE software relies on a system level data object called a Datastore. It exists as a database in the system. All users must have read, write, and modify rights to this object. It contains vital system parameters, audit trails, and other important system information. Network Administrators should take necessary steps to enact appropriate security settings and backup protections on this important database as well as the rest of the system.



22.7 SOLOVPE ADMINISTRATION – LICENSING

This is where the Software System ID is located and the SoloVPE, SecureVPE, and QuickVCA software license status are displayed. Pressing the Licensing button allows the Admin to License the SoloVPE Software. Before shipment, the Software is typically licensed. It can be given a unique temporary license key or a permanent license key generated through the Admin Panel by using the system ID number.



23. GENERAL TROUBLESHOOTING

The following table provides common issues that may arise and their resolutions.

Issue	Resolution
Unable to Log into the SoloVPE Software	<ul style="list-style-type: none"> • Confirm the user password in Windows. If necessary, contact the System Administrator or IT to reset the user password. • If the Software fails to run, contact C Technologies, Inc. to confirm that the Software was properly licensed. • Run the SecureVPE Software to confirm that the user exists in the SecureVPE database. • Have the System Administrator confirm that the user has proper authority to run the SoloVPE Software in SecureVPE.
Unable to Open the SecureVPE Software	<ul style="list-style-type: none"> • The user trying to connect to the SecureVPE Software needs to be an Administrator with the correct privileges. • If UAC is on the user logged in must be a local Admin to open the application • Ensure the secure point is checked in the SecureVPE application
SoloVPE Permissions Appear Different Than Expected from the Profile.	<ul style="list-style-type: none"> • Check to see if there have been changes to the User's Group that may have overwritten any permissions for the User, and apply changes if necessary. • Ensure that there are no conflicts between User and Group settings and configurations.
Software Login Password Does Not Match the SoloVPE eSignature Password.	<ul style="list-style-type: none"> • Make sure the password is accurate. The SoloVPE Software login is controlled by the Windows Active Directory system.
The User is not prompted for Elevated Credentials when accessing the SecureVPE Software.	<ul style="list-style-type: none"> • Ensure that User Account Control Settings is turned on and set at the "Default" access level. (Global Network Admins may not be prompted for Elevated Credentials at any time).
Secure Point Permissions Changes Appear Not to take effect	<ul style="list-style-type: none"> • Check the permissions settings for the User and ALL Groups to which the user belongs. • SecureVPE uses a White List permission structure in which permissions are affirmatively granted and not denied. Therefore, a User assigned to multiple Groups will be granted permission if the Secure Point permissions are granted at the User level or any of the Group Memberships levels. Make sure to apply all changes

24. GETTING HELP

Implementing a GLP compliant security plan can be a complex and involved procedure. Because no two companies have the same policies, infrastructure, organization and procedures compliance can never be achieved by simply installing a Software package. Appropriate computer and network security profiles and standard operating procedures play a critical role in the implementation process and must be supported with training and verification.

Due to the complexity and critical importance of this process, most organizations rely on internal experts to properly design and implement their compliance schemes. C Technologies, Inc. is always willing to provide consultative support to customer personnel to ensure complete understanding and proper use of the tools provided. However, C Technologies, Inc is unable to take responsibility for the implementation and validity of the customer's security plan or the level of compliance.

If it is deemed beneficial to involve C Technologies personnel at any phase in the design or implementation of the security plan, please contact a C Technologies, Inc. representative to discuss options for remote or onsite consultative support. The contact information is as follows:

Customer Support

analytics-support@repligen.com

+1 908-707-1009

Repligen Corporation

C Technologies Offices and Manufacturing Facility

685 Route 202/206

Bridgewater, NJ 08807, USA

ctech.repligen.com

25. SECURITY GUIDANCE FOR WINDOWS SETTINGS

Variable Pathlength Security Guidance

NTFS Permission Recommendations (Subject to Validation During Implementation):

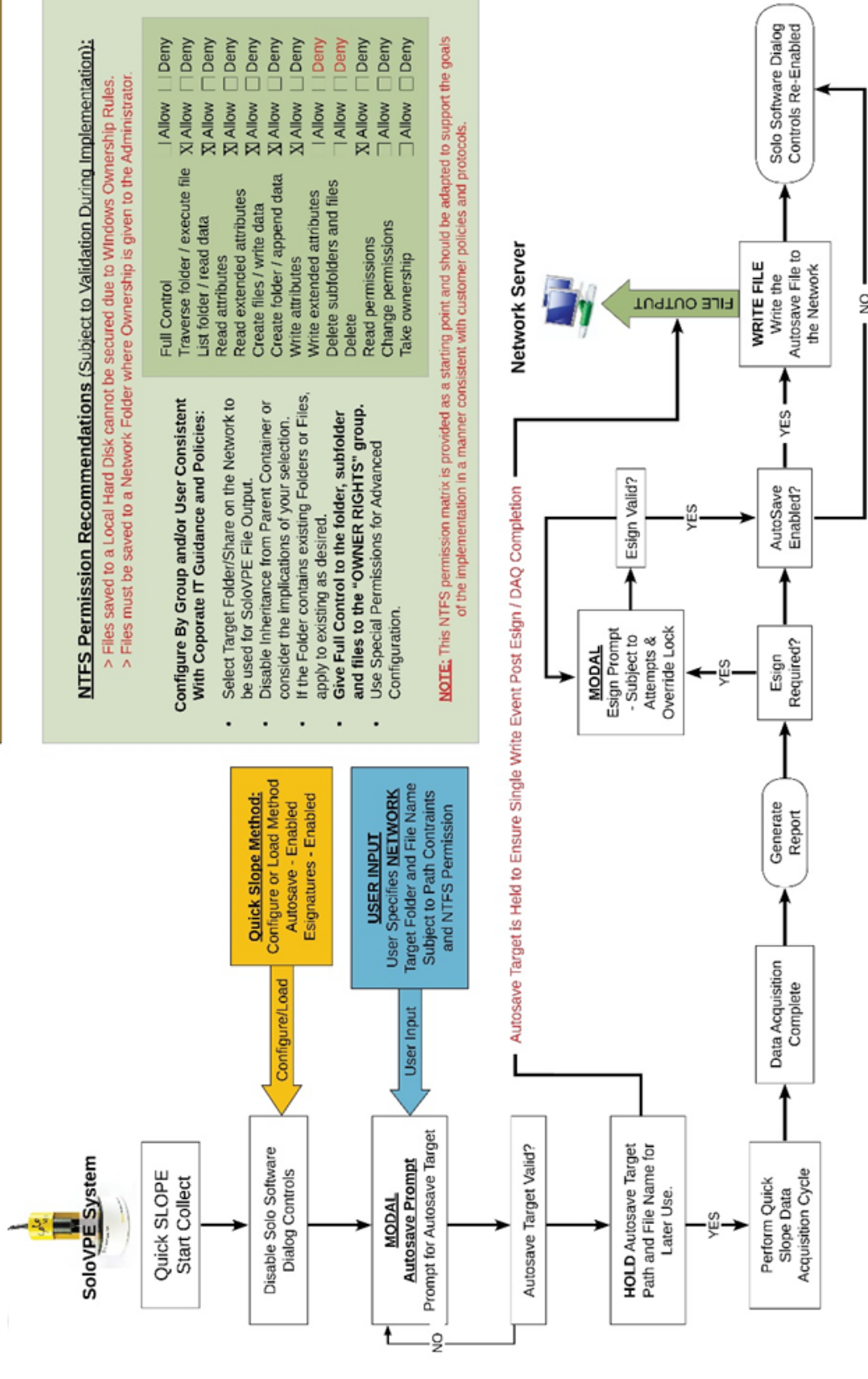
- > Files saved to a Local Hard Disk cannot be secured due to Windows Ownership Rules.
- > Files must be saved to a Network Folder where Ownership is given to the Administrator.

Configure By Group and/or User Consistent With Corporate IT Guidance and Policies:

- Select Target Folder/Share on the Network to be used for SoloVPE File Output.
- Disable Inheritance from Parent Container or consider the implications of your selection. If the Folder contains existing Folders or Files, apply to existing as desired.
- Give Full Control to the folder, subfolder and files to the "OWNER RIGHTS" group.
- Use Special Permissions for Advanced Configuration.

Full Control	/ Allow	/ Deny
Traverse folder / execute file	X Allow	Deny
List folder / read data	X Allow	Deny
Read attributes	X Allow	Deny
Read extended attributes	X Allow	Deny
Create files / write data	X Allow	Deny
Create folder / append data	X Allow	Deny
Write attributes	X Allow	Deny
Write extended attributes	/ Allow	Deny
Delete subfolders and files	/ Allow	Deny
Delete	X Allow	Deny
Read permissions	/ Allow	Deny
Change permissions	/ Allow	Deny
Take ownership	/ Allow	Deny

NOTE: This NTFS permission matrix is provided as a starting point and should be adapted to support the goals of the implementation in a manner consistent with customer policies and protocols.



26. NOTES