VPE Software: SoloVPE Software Security Configuration

Abstract: This document details the preferred security configuration for the SoloVPE software, specifically the security permissions for the files and folders associated with the SoloVPE Software Suite and the SecureVPE Application. These security settings are a part of an overall security plan to be defined by each customer to achieve their desired level of compliance.

Applicability: This article applies to the SoloVPE Software running in the Agilent Cary WinUV (Version 5) environment on a computer running the **Windows 7 Professional (32 bit / 64 bit)** operating system with an NTFS file system on the system hard disk.

Symptom: Not Applicable

Cause: Not Applicable

Detailed Info:

Different organization and groups have been found to require different levels of security and control over their SoloVPE system. In order to provide guidance on the preferred security configuration on the SoloVPE software the matrix below has been prepared. It is up to the customer's Information Technology group to properly implement and administer the desired level of security on their system following installation. *C Technologies, Inc. will provide support to customers as they implement their security plan, but given the broad array of customer specific requirements, it cannot be responsible for implementation and compliance of the customer specific security plan.*

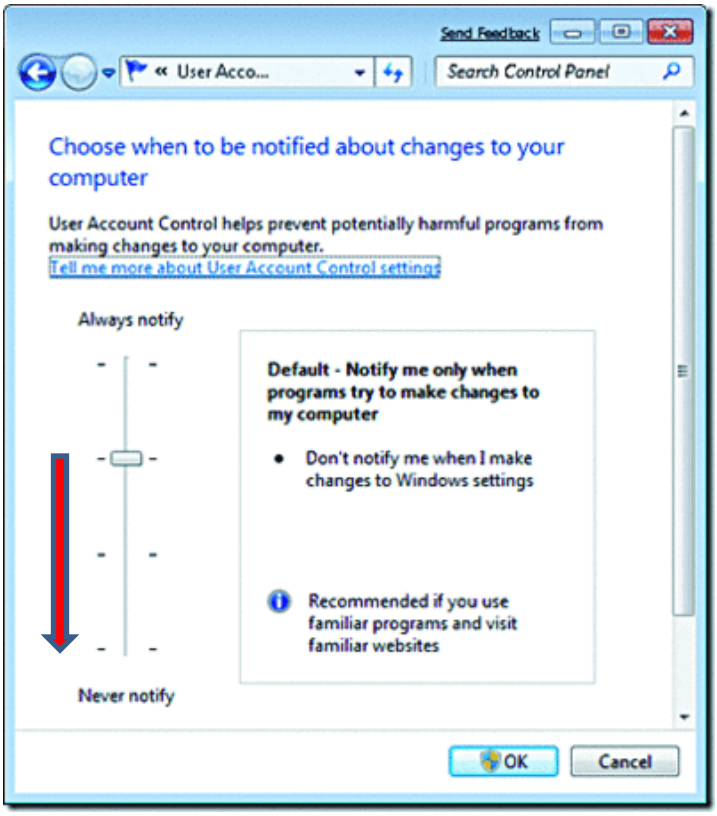
The following matrix lists and describes the standard installed folders and sub-folders required by the SoloVPE software. The permissions noted are for non-Administrative personnel. For each folder and/or file the preferred security permissions are listed that provide the appropriate level of protection for the SoloVPE Software, but Administrative privileges will be required to perform updates of the SoloVPE system will ensure proper functionality.

Additional folders may need to be created at the discretion of the user and/or the IT group for storage and backup of Method Files and Data Files.

Do to the introduction of the UAC (User Access Control) in Windows Vista and Windows 7, particular program and account permissions might demonstrate unpredictable behavior. As a result, "access denied" errors might occur when running the SoloVPE/SecureVPE software. Consult Microsoft's TechNet article http://technet.microsoft.com/en-us/library/2009.07.uac.aspx for detailed information of the UAC.

There are two suggested methods to address this behavior:

Option 1: Disable UAC (Default SoloVPE system setting)
Completely turn off UAC by moving the "slider" to **"Never notify"** position (See graphic below). Windows 7 will emulate a Windows XP Professional type of installation with no alerts or security checks. Create your own security objects by running **Control Panel-> Administrative Tools-> Computer Management.** Grant account permissions according to the security matrix listed below. Keep in mind your company's security policy might restrict access to this control. If this applies to your configuration, please proceed to Option 2.



Option 2: Custom Account Permissions

<u>This only applies if user(s) are a member of the local Administrator's Group!</u>

When the UAC is set to its default position, members of the local Administrator's group with Full NTFS permissions may encounter *"access denied"* or *"write permissions"* errors when running the SoloVPE software. As a work around, a SoloVPE Windows 7 installation is setup with the default Administrator account **<u>disabled</u>**. In turn, the first account created during installation is assigned administrator rights. This account is called "VPELocalAdmin." The VPELocalAdmin account will function as the "Administrator" of the system with full NTFS access to the SoloVPE software.

<u>Local Account Permissions (non-domain)</u>

Note: If the computer system was purchased from C Technologies, Inc., accounts with administrator and standard permissions are created by default. The following information should be used as an NTFS security template for customers with proprietary systems.

Administrative User/Groups

Create a local group called ***"VPELocalAdmins"*** and add the ***"VPELocalAdmin"*** user to this group. Assign permissions to the "VPELocalAdmins" group by following the matrix specified below. These are the **minimum** NTFS permissions that are to be granted to the"VPELocalAdmins" group. Full NTFS permissions can be assigned to the group simulate administrative privileges. Any additional users that function at an administrator level should be and added to the "VPELocalAdmins" group.

Standard User/Groups

Create a local user called ***"VPELocalUser"*** and a group called "VPELocalUsers" and the ***VPELocalUser*** user account to this group. Assign permissions to the VPELocalUsers group by following the matrix specified below. Keep in mind these are minimum permissions for a standard user to run the SoloVPE software and should not have any elevated permissions! Add any additional standard users (non-administrator) to this group.

Domain Level Permissions

Create domain level users and add them to the appropriate security groups in Active Directory. If the user is to operate at an administrative level, add the user or group to the local VPELocalAdmins group. If the user is a standard domain user (non-administrator), add the user or group to the local VPELocalUsers group. Domain level users will inherit the required permissions to operate the SoloVPE/SecureVPE software simplifying account permissions. If you do not wish to use the default groups, grant permissions to your domain accounts following the matrix listed below.

File – Folder Security Map

File or Folder	Description	NTFS Security
C:\CTECH	**Legacy Installation Folder**	***Read & Execute*** ***List Folder Contents*** ***Read***
C:\CTECH\SoloVPE	**Legacy SoloVPE Installation Folder**	***Read & Execute*** ***List Folder Contents*** ***Read***
C:\CTECH\SoloVPE\Hooks *(If Applicable)*	**SoloVPE Hooks Folder**	***Read & Execute*** ***List Folder Contents*** ***Read*** ***Write***
C:\Program Files\CTECH\SoloVPE\Documents	**SoloVPE Documentation Folder**	***Read & Execute*** ***List Folder Contents*** ***Read***
C:\Program Files\CTECH\SoloVPE\Hooks *(If Applicable)*	**SoloVPE Hooks Folder**	***Read & Execute*** ***List Folder Contents*** ***Read*** ***Write***
C:\Program Files\CTECH\SoloVPE\Help	**SoloVPE Help Folder**	***Read & Execute*** ***List Folder Contents*** ***Read***
C:\Program Files\CTECH\SoloVPE\Images	**SoloVPE Image Folder**	***Read & Execute*** ***List Folder Contents*** ***Read***
C:\ProgramData\CTECH\SoloVPE	**SoloVPE System Configuration Data**	***Folder Attribute=Uncheck Hidden*** ***Read & Execute*** ***List Folder Contents*** ***Read*** ***Write***
ValidateVPE Configuration Information		
C:\CTECH\ValidateVPE\System	**Validate VPE System Folder**	***Read & Execute*** ***List Folder Contents*** ***Read*** ***Write***
C:\CTECH\ValidateVPE\Module	**Validate VPE Module Folder**	***Read & Execute*** ***List Folder Contents*** ***Read***
C:\CTECH\ValidateVPE\img	**Validate VPE Graphic Library**	***Read & Execute*** ***List Folder Contents*** ***Read***

SecureVPE Configuration Information (Optional)		
C:\Program Files\CTECH\SecureVPE	**SecureVPE Interface Application**	***Read & Execute*** ***List Folder Contents*** ***Read*** ***Write, Delete***
C:\ProgramData\CTECH\SecureVPE	**SecureVPE Configuration Data**	***Read & Execute*** ***List Folder Contents*** ***Read*** ***Write***

NOTE: The Agilent/Varian Cary WinUV software also has some constraints regarding security configuration. There are some files that the Agilent software places in the "C:\ProgramData\Agilent" Folder and the "C:\Windows" directory that require the ability to read, write and delete. The application also makes use the Windows API and may require specific access to the associated controls and drivers stored in the Windows folder structure.

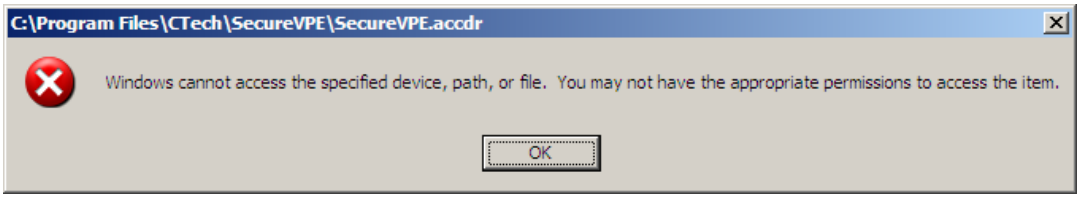
Addendum: Troubleshooting Specific Permission / Access Related Issues

10051 Error could not open file / 10021 Error could not open file

This error message is caused by improper permission settings on the following folder:
C:\ProgramData\CTech\SoloVPE

Please refer to Appendix B and apply permission criteria as per which operating system / software version for which this system is configured for.

Access Runtime Error

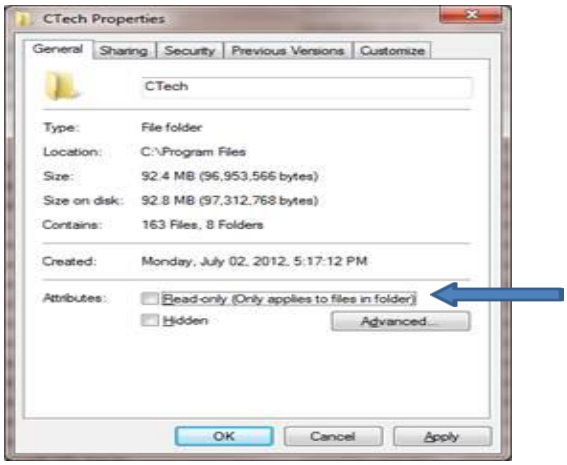


The following error will occur when a company computer policy is restricting Access or Access Runtime from running.

SecureVPE is compatible with Access 2007 Runtime only! **Do not install Access 2010 Runtime**.

Word Reporting Error

Folder and file attributes will override NTFS permissions. Please verify "Read-only" attributes are **unchecked** on your destination folder when configuring the directories below.



Document Info:

Prepared By: C Technologies, Inc.
757 Route 202/206
Bridgewater, NJ 08807
(P) 908-707-1009
(F) 908-707-1030
(E) support@solovpe.com

Version: 04/2018-04-13